(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108389046 B
(45)授权公告日 2020.08.28

(21)申请号 201810124778.1

(22)申请日 2018.02.07

(65)同一申请的已公布的文献号
申请公布号 CN 108389046 A

(43)申请公布日 2018.08.10

(73)专利权人 西安交通大学
地址 710049 陕西省西安市碑林区咸宁西路28号

(72)发明人 王晨旭 姜一鸣 秦栋 陶敬 秦涛 马小博 管晓宏

(74)专利代理机构 西安通大专利代理有限责任公司 61200
代理人 安彦彦

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 40/04(2012.01)
G06F 21/64(2013.01)

(56)对比文件
CN 107346491 A,2017.11.14
CN 106982205 A,2017.07.25
CN 105976231 A,2016.09.28
US 2017155515 A1,2017.06.01
CN 106559211 A,2017.04.05
杨兴寿.电子商务环境下的信用和信任机制研究.《中国博士学位论文全文数据库 经济与管理科学辑》.2017,
汪传雷.基于区块链的供应链物流信息生态圈模型.《情报理论与实践》.2017,第40卷(第7期),

审查员 甘晶萌

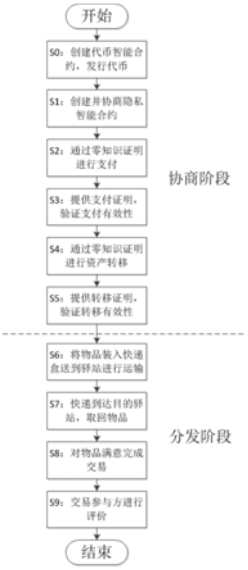
权利要求书2页 说明书6页 附图4页

(54)发明名称

一种电子商务中基于区块链技术的隐私保护交易方法

(57)摘要

一种电子商务中基于区块链技术的隐私保护交易方法,采用包括隐私智能合约和零知识证明在内的区块链技术保护用户的私人信息;隐私智能合约在交易期间作为买家和卖家之间的桥梁;采用零知识证明来发行保密代币并创建保密交易;将区块链、工业数据空间和物联网技术结合在一起,建立一个基础架构,以分布式的方式为管理物流业务建立一个综合平台。本发明不仅对快递员隐藏隐私信息,还可以对卖家隐藏诸如身份、地址、电话号码等隐私信息,而且还能够用于其他具有数据隐私保护要求的区块链应用场景,另外还能够充分利用区块链特性,使得电子商务平台的评价问题得以改善。



CN 108389046 B

1.一种电子商务中基于区块链技术的隐私保护交易方法,其特征在于,该方法包括以下两个阶段:

协商阶段:采用包括隐私智能合约和零知识证明在内的区块链技术保护用户的私人信息;隐私智能合约在交易期间作为买家和卖家之间的桥梁;采用零知识证明来发行保密代币并创建保密交易,以提供所有权证明;

分发阶段:将区块链、工业数据空间和物联网技术结合在一起,建立一个基础架构,以分布式的方式为管理物流业务建立一个综合平台;其中,区块链用于记录、存储数据并运行隐私智能合约;工业数据空间用于物流链各方之间的安全数据交换;物联网技术用于物流网络上的实时数据传输;

包括交易参与方卖家A和买家B以及托管方M;

所述协商阶段包括如下步骤:

S0:假设最初没有涉及卖家A拥有的某资产的交易,卖家A在贸易链上创建一个资产代币智能合约,并为自己发行资产的保密代币;与此同时,买家B在支付链上用法币代币智能合约来为自己生成法币代币;其中,贸易链用于添加或更改资产代币智能合约,以及物流链用于维护物流信息;支付链用于记录法币交易;

S1:卖家A和买家B通过加密通信信道对隐私智能合约内容进行协商;买家B发送给隐私智能合约一个消息表示接受此合约内容;

S2:隐私智能合约提示买家B进行支付,买家B通过零知识证明支付法币代币给卖家A;其中,买家B实际上将法币代币放入托管地址;买家B的客户端接收并排序隐私智能合约的指令,当接收到支付指令时,买家B产生零知识证明并将其发送到法币代币合约来将相应数量的法币代币支付到托管方M的托管地址;买家B的法币代币余额相应减少;

S3:买家B向隐私智能合约提供支付证明,隐私智能合约在支付链上验证是否已支付;

S4:当验证有效,隐私智能合约提示卖家A进行资产转移,卖家A通过零知识证明将资产所有权转移给买家B;

S5:卖家A向隐私智能合约提供转移证明,隐私智能合约在贸易链上验证是否转移成功;其中,卖家A向隐私智能合约证明资产转移已完成;隐私智能合约验证是否有效,如果有效,将状态更改为转移完成,并将买家B的地址哈希发送给卖家A的客户端,并指示卖家A将实物发送给买家B;

所述分发阶段包括如下步骤:

S6:卖家A将资产实物放入运用具有唯一编号的快递盒中,并把快递盒送到智能物流驿站;其中,快递盒结合了物联网技术具有唯一编号;由物流公司负责检查和监督物品的合法性;卖家A的客户端将买家B的地址哈希发送到这个快递盒,并把这个快递盒的号码发送给隐私智能合约,然后隐私智能合约将快递盒的号码发送给买家B的客户端;智能驿站接收并解析快递盒中的哈希,指示快递员发货;智能驿站在区块链网络内发送交易,并在物流链中记录快递盒的加密运输历史;其中物流过程中的数据交换通过工业数据空间连接器完成,由工业数据空间技术负责分发阶段的安全隐私数据交换;在发货后,隐私智能合约状态变更为已发货;

S7:当快递盒到达目的地,买家B的客户端指示买家B去取快递盒;

S8:买家B向隐私智能合约发送一个表明交易已经完成的交易。

2.根据权利要求1所述的一种电子商务中基于区块链技术的隐私保护交易方法，其特征在于：所述步骤S1中隐私智能合约指定卖家A和买家B之间资产对法币的价格；隐私智能合约引用资产代币和法币代币智能合约的地址；卖家A和买家B发送给隐私智能合约双方的公钥和支付地址包括物理地址哈希；隐私智能合约在初始化后状态变更为协商，在买家B接收合约内容后状态变更为确认。

3.根据权利要求1所述的一种电子商务中基于区块链技术的隐私保护交易方法，其特征在于：所述步骤S3中买家B通过向隐私智能合约发送法币支付零知识证明的输出来证明相应数额的法币代币已经被置于托管方M托管中；隐私智能合约通过使用买家B提供的输出在法币代币智能合约上调用函数来验证法币代币是否被置于托管方M托管，法币代币智能合约用一个二进制值来响应隐私智能合约，该二进制值指示承诺是否在法币代币智能合约的承诺累加器中；如果有效，隐私智能合约状态更改为支付完成。

4.根据权利要求1所述的一种电子商务中基于区块链技术的隐私保护交易方法，其特征在于：所述步骤S4中卖家A的客户端接收并排序隐私智能合约的指令；卖家A通过产生零知识证明将相应的资产代币发送到托管方M的地址，并将零知识证明的输出发送给资产代币智能合约；卖家A的资产代币余额相应减少。

5.根据权利要求1所述的一种电子商务中基于区块链技术的隐私保护交易方法，其特征在于：所述步骤S7中当快递盒到达最接近买家B地址的驿站时，驿站认为快递盒已经到达目的地，将快递盒的状态在物流链上由运输中变更为已到达；买家B的客户端指示买家B去取快递盒中的实物并将快递盒的状态改变为空闲中；隐私智能合约状态变更为已取货。

一种电子商务中基于区块链技术的隐私保护交易方法

技术领域

[0001] 本发明涉及智能电子商务技术以及隐私保护领域，特别涉及一种电子商务中基于区块链技术的隐私保护交易方法。

背景技术

[0002] 电子商务是以信息网络技术为手段，以商品交换为中心的商务活动，是传统商业活动各环节的电子化、网络化、信息化。电子商务由于产品丰富，交易快速，不受时间，地点，门店等的限制，变得越来越受欢迎。但是，用户的个人信息如身份、地址、电话号码等的泄露已经成为电子商务的一大关注点。实际上，它已经形成了一个严重危害用户安全和隐私的“灰色产业”。另外，卖家威胁或强制买家做出、修改或删除违反其意愿的评论也是常见的。而且，网络购物网站也遭受恶意差评或虚假好评的影响，这严重影响了用户体验。

[0003] 为了解决电商物流中的隐私问题，一些电商发明了“隐私面单”来隐藏消费者的信息，使得隐私信息不会出现在快递单上。虽然这种技术在一定程度上阻止了个人信息的泄露，但是这种技术不能对卖家隐藏来自买家的地址，电话号码等信息。

[0004] 区块链是数字资产保护体系的核心支撑技术。区块链技术的核心优势是去中心化，在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作。智能合约是区块链的核心构成要素，能够实现控制和管理区块链上数字资产的功能。智能合约为静态的底层区块链数据赋予了灵活可编程的机制和算法，并且，其自动化和可编程特性使其可封装分布式区块链系统中各节点的复杂行为。

[0005] 隐私性一直是区块链领域一个重要的话题。区块链作为一门新兴的技术，必要的隐私保护是推广的关键。绝大部分的应用场景，都需要有弹性的隐私保护。对于某些区块链上的参与方，他们并不希望任何人都可以查看其数字资产交易的账本。零知识证明技术不需要第三方就可以对交易信息实现强大的匿名性，而且可以防止对区块链交易历史的有效分析。IDS技术可以让各方一起工作，而不会泄露彼此的机密信息，可以保证在物流过程中的数据安全。

发明内容

[0006] 鉴于此，针对电子商务中用户隐私保护的问题，本发明的目的是提出一种电子商务中基于区块链技术的隐私保护交易方法。

[0007] 为实现上述目的，本发明采用如下的技术方案：

[0008] 一种电子商务中基于区块链技术的隐私保护交易方法，该方法包括以下两个阶段：

[0009] 协商阶段：采用包括隐私智能合约和零知识证明在内的区块链技术保护用户的私人信息；隐私智能合约在交易期间作为买家和卖家之间的桥梁；采用零知识证明来发行保密代币并创建保密交易，以提供所有权证明；

[0010] 分发阶段：将区块链、工业数据空间和物联网技术结合在一起，建立一个基础架

构,以分布式的方式为管理物流业务建立一个综合平台;其中,区块链用于记录、存储数据并运行隐私智能合约;工业数据空间用于物流链各方之间的安全数据交换;物联网技术用于物流网络上的实时数据传输。

[0011] 本发明进一步的改进在于,包括交易参与方卖家A和买家B以及托管方M;

[0012] 所述协商阶段包括如下步骤:

[0013] S0:假设最初没有涉及卖家A拥有的某资产的交易,卖家A在贸易链上创建一个资产代币智能合约,并为自己发行资产的保密代币;与此同时,买家B在支付链上用法币代币智能合约来为自己生成法币代币;其中,贸易链用于添加或更改资产代币智能合约,以及物流链用于维护物流信息;支付链用于记录法币交易;

[0014] S1:卖家A和买家B通过加密通信信道对隐私智能合约内容进行协商;买家B发送给隐私智能合约一个消息表示接受此合约内容;

[0015] S2:隐私智能合约提示买家B进行支付,买家B通过零知识证明支付法币代币给卖家A;

[0016] S3:买家B向隐私智能合约提供支付证明,隐私智能合约在支付链上验证是否已支付;

[0017] S4:当验证有效,隐私智能合约提示卖家A进行资产转移,卖家A通过零知识证明将资产所有权转移给买家B;

[0018] S5:卖家A向隐私智能合约提供转移证明,隐私智能合约在贸易链上验证是否转移成功;

[0019] 所述分发阶段包括如下步骤:

[0020] S6:卖家A将资产实物放入运用具有唯一编号的快递盒中,并把快递盒送到智能物流驿站;

[0021] S7:当快递盒到达目的地,买家B的客户端指示买家B去取快递盒;

[0022] S8:买家B向隐私智能合约发送一个表明交易已经完成的交易。

[0023] 本发明进一步的改进在于,所述步骤S1中隐私智能合约指定卖家A和买家B之间资产对法币的价格;隐私智能合约引用资产代币和法币代币智能合约的地址;卖家A和买家B发送给隐私智能合约双方的公钥和支付地址包括物理地址哈希;隐私智能合约在初始化后状态变更为协商,在买家B接收合约内容后状态变更为确认。

[0024] 本发明进一步的改进在于,所述步骤S2中买家B实际上将法币代币放入托管地址;买家B的客户端接收并排序隐私智能合约的指令,当接收到支付指令时,买家B产生零知识证明并将其发送到法币代币合约来将相应数量的法币代币支付到托管方M的托管地址;买家B的法币代币余额相应减少。

[0025] 本发明进一步的改进在于,所述步骤S3中买家B通过向隐私智能合约发送法币支付零知识证明的输出来证明相应数额的法币代币已经被置于托管方M托管中;隐私智能合约通过使用买家B提供的输出在法币代币智能合约上调用函数来验证法币代币是否被置于托管方M托管,法币代币智能合约用一个二进制值来响应隐私智能合约,该二进制值指示承诺是否在法币代币智能合约的承诺累加器中;如果有效,隐私智能合约状态更改为支付完成。

[0026] 本发明进一步的改进在于,所述步骤S4中卖家A的客户端接收并排序隐私智能合

约的指令;卖家A通过产生零知识证明将相应的资产代币发送到托管方M的地址,并将零知识证明的输出发送给资产代币智能合约;卖家A的资产代币余额相应减少。

[0027] 本发明进一步的改进在于,所述步骤S5中卖家A向隐私智能合约证明资产转移已完成;隐私智能合约验证是否有效,如果有效,将状态更改为转移完成,并将买家B的地址哈希发送给卖家A的客户端,并指示卖家A将实物发送给买家B。

[0028] 本发明进一步的改进在于,所述步骤S6中快递盒结合了物联网技术具有唯一编号;由物流公司负责检查和监督物品的合法性;卖家A的客户端将买家B的地址哈希发送到这个快递盒,并把这个快递盒的号码发送给隐私智能合约,然后隐私智能合约将快递盒的号码发送给买家B的客户端;智能驿站接收并解析快递盒中的哈希,指示快递员发货;智能驿站在区块链网络内发送交易,并在物流链中记录快递盒的加密运输历史;其中物流过程中的数据交换通过IDS连接器完成,由IDS技术负责分发阶段的安全隐私数据交换;在发货后,隐私智能合约状态变更为已发货。

[0029] 本发明进一步的改进在于,所述步骤S7中当快递盒到达最接近买家B地址的驿站时,驿站认为快递盒已经到达目的地,将快递盒的状态在物流链上由运输中变更为已到达;买家B的客户端指示买家B去取快递盒中的实物并将快递盒的状态改变为空闲中;隐私智能合约状态变更为已取货。

[0030] 与现有技术相比,本发明具有的有益效果:本发明中区块链由于采用了安全隔离通道实现的隐私智能合约,并结合零知识证明以及IDS与IoT技术,再加上一定的权限管理功能,因此能进行安全的数据交换,并达到在整个电子商务过程中保护隐私的要求。在具有数据隐私保护要求的电子商务中,具备资产交易数据和过程隐私保护功能,且具有资产所有权证明的功能,只有隐私智能合约交易参与方可以查看限定的交易信息,相较于传统电子商务,不仅对快递员隐藏隐私信息,还可以对卖家隐藏诸如身份、地址、电话号码等隐私信息,而且还能够用于其他具有数据隐私保护要求的区块链应用场景,另外还能够充分利用区块链特性,使得电子商务平台的评价问题得以改善。

[0031] 进一步的,为了保护用户身份和保证所有权证明,本发明采用了零知识证明技术。其允许一方(证明者)向另一方(验证者)不泄露任何其他信息的情况下证明给定的陈述是真实的。为了保护用户的地址,本发明用一个哈希字符串来索引地址,并将其加密记录在物流链上。为了保护电话号码,我们使用结合物联网技术的快递盒和智能物流驿站。当快递盒发送的物联网数据表明已经到达智能物流驿站时,隐私智能合约将快递盒的号码发送给买方客户端。客户端指示买家在快递盒中取货。与一般惯例不同,买家不需要提供用于短信通知的电话号码。本发明解决了电子商务中用户隐私信息如身份,地址,电话号码等泄露的问题。

附图说明

[0032] 图1为本发明中的协商阶段的示意图。

[0033] 图2为本发明中的分发阶段的示意图。

[0034] 图3为本发明的交易方法的流程图。

[0035] 图4为本发明中的隐私智能合约状态变更示意图。

[0036] 图5为本发明中的快递盒状态变更示意图。

[0037] 图6为本发明中的分发阶段技术组件示意图。

具体实施方式

[0038] 以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0039] 本发明交易参与方可以超过2个,托管方也可以为多个形成托管组,链也可以继续扩展。

[0040] 所述交易是指通过调用智能合约来改变账本的状态;用户可以通过发送交易请求来使区块链账本记录信息。

[0041] 所述保密交易是指将代币从一方转移到另一方;发送者,接收者和正在转移的数量对于第三方观察者是不可见的。

[0042] 所述承诺相当于未使用的交易输出;也被用来描述代币的接收者必须拥有以便使用该代币的数据。

[0043] 所述代币智能合约指在链上可见的智能合约,支持代币的发行,保密交易。

[0044] 所述隐私智能合约通过安全隔离通道来实现,隐私智能合约将实施一个有限状态机来追踪贸易生命周期的进展;只有在特定的交易事件发生时,才能从一个交易状态转移到下一个交易状态。

[0045] 所述托管方是指与监管机构类似的角色,也是隐私智能合约的参与方,他们可以独立验证保密交易和代币转移。

[0046] 参见图3和图4,本发明的方法包括以下两个阶段:

[0047] 协商阶段:在协商阶段通过采用包括隐私智能合约和零知识证明在内的区块链技术保护用户的私人信息。具体而言,每笔交易都由隐私智能合约代表,其中定义了业务逻辑,交易类型,交易参与方,依赖的资产,价格以及任何其他相关信息。隐私智能合约在交易期间作为买家和卖家之间的桥梁并且不会泄露私人信息。本发明使用零知识证明来发行保密代币并创建保密交易,以提供所有权证明。由于零知识证明的零知识属性,代币化资产和保密交易阻止了买方私人信息的泄露。代币化资产可以是现金或其他可交易货物。有关保密交易的信息在交易过程中是保密的。

[0048] 分发阶段:在分发阶段将区块链,工业数据空间(IDS)和物联网(IoT)技术结合在一起,建立一个基础架构,以分布式的方式为管理物流业务建立一个可靠的综合平台。区块链技术以分散的方式处理各方之间的交易历史和合同。区块链网络用于可靠的记录,存储数据并运行智能合约。IDS技术允许物流链各方之间的安全数据交换。IDS连接器是IDS技术的核心,可确保数据的隐私性和机密性。物联网技术使物流网络上的实时数据传输成为可能。通过物联网技术监控快递盒位置等状态。如果发生纠纷,物联网数据将作为事件触发和仲裁证明记录在区块链中。

[0049] 本发明中包括交易参与方卖家A和买家B以及托管方M;包括支付链用于记录法币交易,贸易链用于添加或更改资产代币智能合约,以及物流链用于维护物流信息。

[0050] 图1显示了本发明所述的协商阶段的流程。如图1所示,协商阶段包括步骤:

[0051] 步骤S0.假设最初没有涉及卖家A拥有的某资产的交易。卖家A必须在贸易链上为该资产创建资产代币合约并为自己发放保密的代币,即图1中的创建资产代币智能合约。现

在,卖家A拥有该资产代币。如果该资产或者法币代币智能合约已存在,则不需要再创建。

[0052] 与此同时,买家B在支付链上用法币代币合约为自己发放了一些法币代币,即图1中的发行法币代币。

[0053] 步骤S1.卖家A在隐私通道中与买家B建立隐私智能合约,即图1中的建立隐私智能合约。隐私智能合约指定卖家A和买家B之间以某法币特定价格进行交易,即隐私智能合约指定卖家A和买家B之间资产对法币的价格。隐私智能合约引用该资产代币合约和该法币代币合约的地址。此外,隐私智能合约还接收双方相应的公钥和支付地址包括物理地址哈希。当卖家A初始化合同时,隐私智能合约状态变为协商;而后买家B可以向隐私智能合约发送表示接受条款的交易,即图1中的接受合约内容,此时隐私智能合约状态变为确认。

[0054] 步骤S2.隐私智能合约向买家发出指令,向卖家A支付相应的法币代币,即图1中的指示B进行支付。买家B的客户端接收并排序该指令,指示买家B进行保密交易。买家B使用托管协议通过产生必要的零知识证明并将其输出发送到法币代币智能合约来将相应数量的法币代币支付给托管方的地址,即图1中的将证明输出发送给法币代币智能合约。此时保密交易完成,并在法币代币智能合约内创建承诺。买家B的代币余额相应减少。

[0055] 步骤S3.买家B通过向隐私智能合约发送法币支付零知识证明的输出来证明相应数额的法币代币已经被置于托管方M托管中,即图1中的向隐私智能合约提供支付证明。隐私智能合约通过使用买家B提供的输出在法币代币智能合约上调用函数来验证法币代币是否被置于托管方M托管,即图1中的验证支付有效性。法币代币智能合约用一个二进制值来响应隐私智能合约,该二进制值指示承诺是否在法币代币智能合约的承诺累加器中。如果有效,隐私智能合约状态更改为支付完成。

[0056] 步骤S4.如果有效,隐私智能合约指示卖家A将资产代币放入托管地址,即图1中的指示A转移资产所有权。卖家A的客户端接收并排序隐私智能合约的指令,指令提示她进行资产代币转移,卖家A通过产生必要的零知识证明将相应的资产代币发送到托管地址,并将零知识证明输出发送给资产代币智能合约,即图1中的转移资产代币。此时保密交易发生,并在资产代币智能合约内创建一个承诺。卖家A的资产代币余额相应减少。

[0057] 步骤S5.卖家A通过向隐私智能合约提交输出,提供资产代币已完成转移的证据,即图1中的向隐私智能合约提供转移证明。然后,隐私智能合约验证资产代币已经存入托管地址,即图1中的验证转移有效性,如果有效,将状态更改为转移完成,并将买家B的物理地址哈希发送给卖家A的客户端,指示她将资产实物发送给买家B,即图1中的指示A进行发货。

[0058] 图2显示了本发明所述的分发阶段的流程。如图2所示,分发阶段包括如下步骤:

[0059] 步骤S6.卖家A将物品放入具有唯一编号的快递盒中。然后卖家A将快递盒送到智能物流驿站,即图2中的将物品放到快递盒送到驿站。物流公司负责检查和监督物品的合法性。参见图6,卖家A的客户端通过IDS连接器将买家B的地址哈希发送到快递盒,并将该盒子的号码发送给隐私智能合约,即图2中的发送快递盒编号。然后隐私智能合约将快递盒的号码发送给买家B的客户端,即图2中的将快递盒编号发给B。驿站接收并解析快递盒中的地址哈希,并指示快递员运输。驿站在区块链网络内发送交易,并在物流链中记录快递盒的加密运输历史,即图2中的记录物流信息。在发货后,隐私智能合约状态变更为已发货。快递盒的状态参见图5。

[0060] 步骤S7.当快递盒到达最接近买家B地址的驿站时,驿站认为快递盒已经到达目的

地，并将快递盒的状态在物流链中从运输中改变为已到达，即图2中的查询物流盒状态。当箱子的状态为已到达时，买家B的客户端指示买家B取出快递盒中的物品，即图2中的取回快递盒中的物品，并将快递盒的状态改变为空闲中，即图2中的更改快递盒状态。隐私智能合约状态变更为已取货。

[0061] 步骤S8.如果买家B对实物感到满意，买家B就会向隐私智能合约发送一个表明交易已经完成的交易，即图2中的指示交易已完成。然后，隐私智能合约使用托管协议将可签署有效交易的双方密钥发送给卖家A和买家B，即图2中的发送密钥。现在，卖家A和买家B可以向托管方发送有效的交易，以获取相应的法币代币(即图2中的取回法币代币所有权)和资产代币(即图2中的取回资产代币所有权)的所有权。隐私智能合约变更状态为交易完成。

[0062] 步骤S9.交易完成后，买家和卖家可以向私人合约发送评论，所有评论将被记录在区块链中。其他用户可以通过评论来查看双方的信誉。买家B现在获得了实物和该物品的代币。如果买家B把他们卖给C这样的第三方，C将无法确定该代币的来源。卖家A将无法确定买家B何时将代币发送给其他人以及接收人是谁。卖家A只能看到交易已经发生，因为交易被写入到卖家A可以访问的贸易链上的资产代币智能合约。

[0063] 本发明解决了电子商务中用户隐私信息如身份，地址，电话号码等泄露的问题。为了保护用户身份和保证所有权证明，本发明采用了零知识证明技术。其允许一方(证明者)向另一方(验证者)不泄露任何其他信息的情况下证明给定的陈述是真实的。为了保护用户的地址，本发明用一个哈希字符串来索引地址，并将其加密记录在物流链上。为了保护电话号码，我们使用结合物联网技术的快递盒和智能物流驿站。当快递盒发送的物联网数据表明已经到达智能物流驿站时，隐私智能合约将快递盒的号码发送给买方客户端。客户端指示买家在快递盒中取货。与一般惯例不同，买家不需要提供用于短信通知的电话号码。

[0064] 本发明所述的区块链，由于其采用了安全隔离通道实现的隐私智能合约，并结合零知识证明以及IDS与IoT技术，再加上一定的权限管理功能，因此能进行安全的数据交换，并达到在整个电子商务过程中保护隐私的要求。与现有技术相比，本发明的有益效果是：在具有数据隐私保护要求的电子商务中，具备资产交易数据和过程隐私保护功能，且具有资产所有权证明的功能，只有隐私智能合约交易参与方可以查看限定的交易信息，相较于传统电子商务，不仅对快递员隐藏隐私信息，还可以对卖家隐藏诸如身份、地址、电话号码等隐私信息，而且还能够用于其他具有数据隐私保护要求的区块链应用场景，另外还能够充分利用区块链特性，使得电子商务平台的评价问题得以改善。

[0065] 可以理解的是，对于本领域的普通技术人员来说，可以根据本发明的技术构思做出其它各种相应的改变与变形，而所有这些改变与变形都应属于本发明权利要求的保护范围。

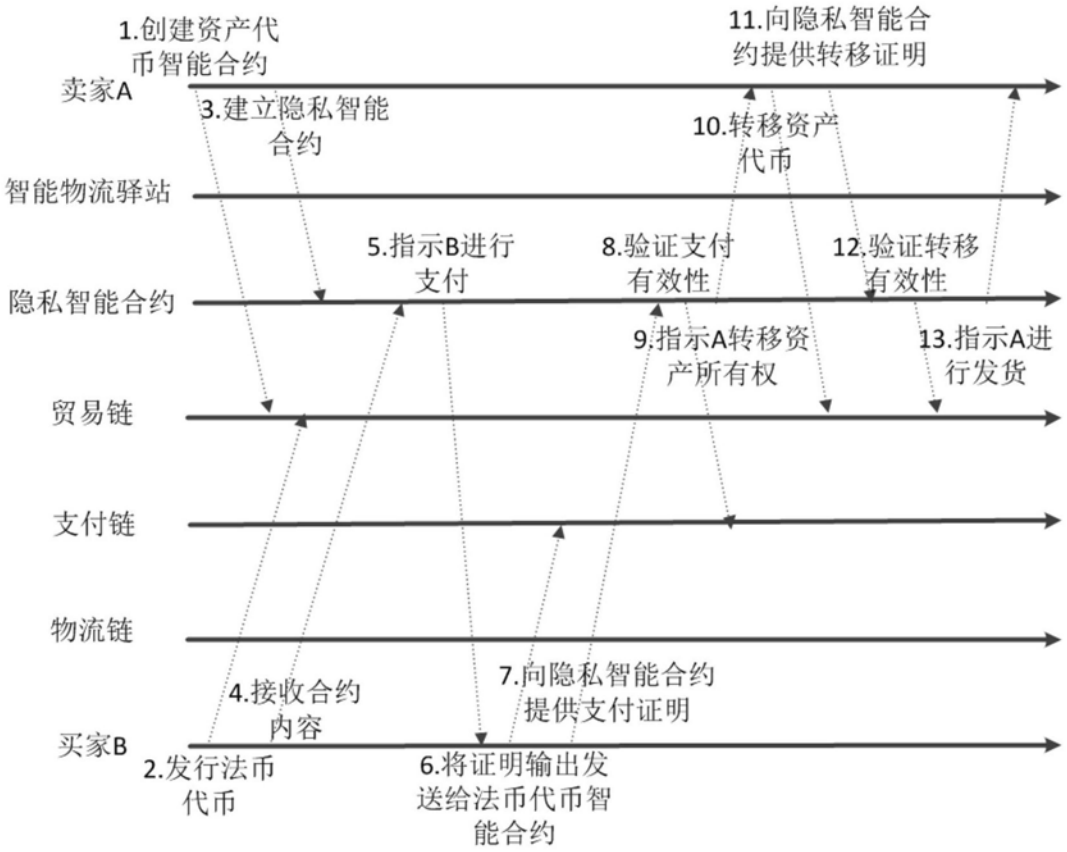

1.创建资产代币智能合约
11.向隐私智能合约提供转移证明
卖家A
3.建立隐私智能合约
10.转移资产代币
智能物流驿站
5.指示B进行支付
8.验证支付有效性
12.验证转移有效性
隐私智能合约
9.指示A转移资产所有权
13.指示A进行发货
贸易链
支付链
物流链
4.接收合约内容
7.向隐私智能合约提供支付证明
买家B
2.发行法币代币
6.将证明输出发送给法币代币智能合约

图1

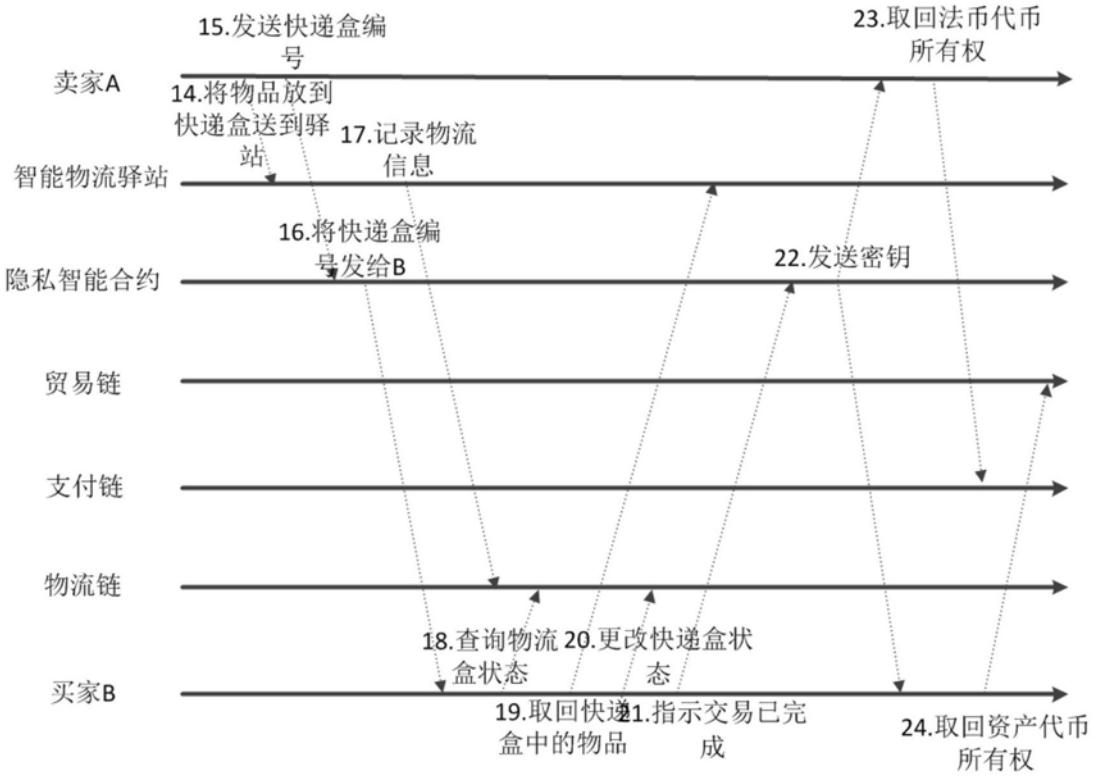

15.发送快递盒编号
23.取回法币代币所有权
卖家A
14.将物品放到快递盒送到驿站
17.记录物流信息
智能物流驿站
16.将快递盒编号发给B
22.发送密钥
隐私智能合约
贸易链
支付链
物流链
18.查询物流盒状态
20.更改快递盒状态
买家B
19.取回快递盒中的物品
21.指示交易已完成
24.取回资产代币所有权

图2

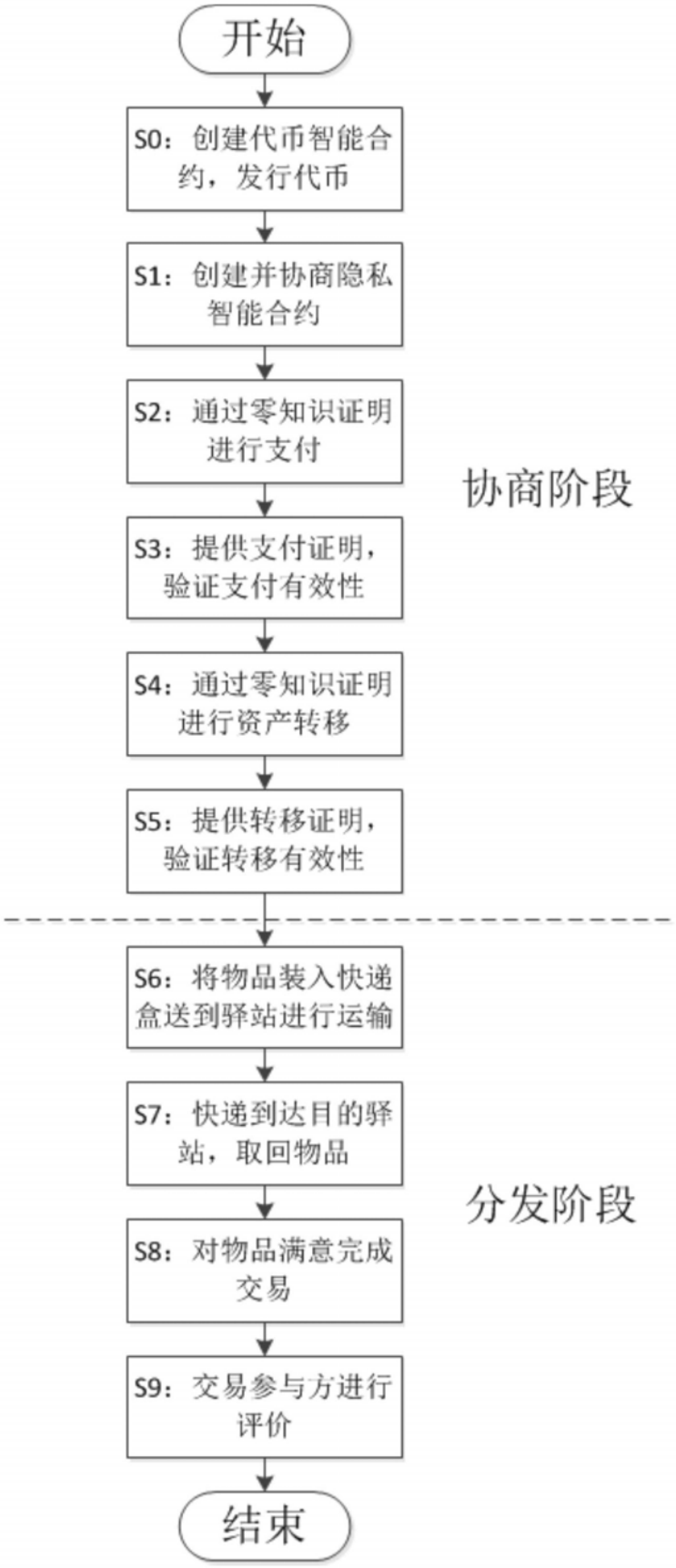

开始
S0：创建代币智能合约，发行代币
S1：创建并协商隐私智能合约
S2：通过零知识证明进行支付
协商阶段
S3：提供支付证明，验证支付有效性
S4：通过零知识证明进行资产转移
S5：提供转移证明，验证转移有效性
S6：将物品装入快递盒送到驿站进行运输
S7：快递到达目的驿站，取回物品
分发阶段
S8：对物品满意完成交易
S9：交易参与方进行评价
结束

图3

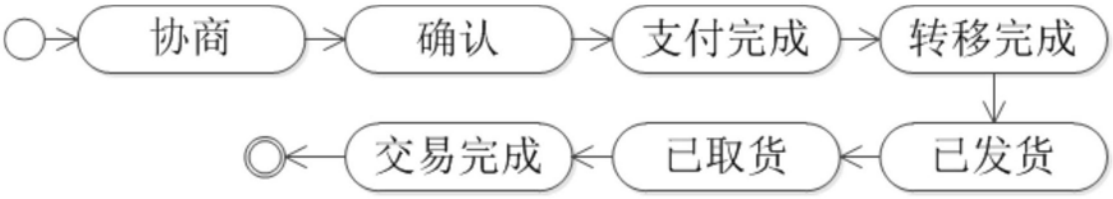

协商
确认
支付完成
转移完成
已发货
已取货
交易完成

图4

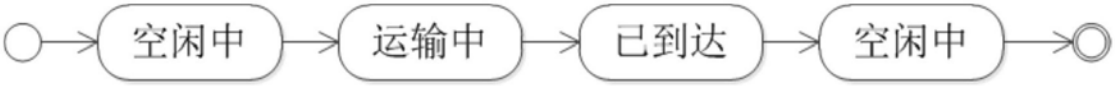

空闲中
运输中
已到达
空闲中

图5

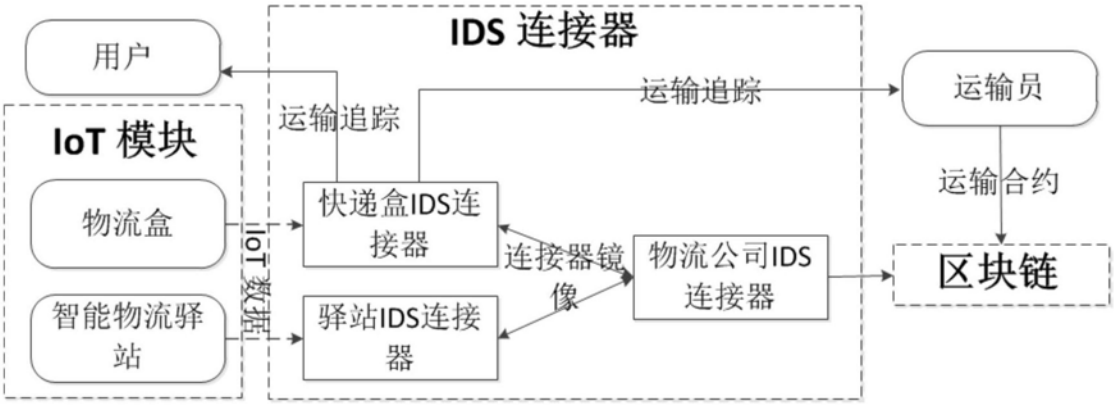

IDS 连接器
用户
运输追踪
运输追踪
运输员
IoT 模块
运输合约
物流盒
快递盒IDS连接器
连接器镜像
物流公司IDS连接器
区块链
IoT 数据
智能物流驿站
驿站IDS连接器

图6