(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 106559211 B
(45)授权公告日 2019.12.13

(21)申请号 201611029339.X

(22)申请日 2016.11.22

(65)同一申请的已公布的文献号
申请公布号 CN 106559211 A

(43)申请公布日 2017.04.05

(73)专利权人 中国电子科技集团公司第三十研究所
地址 610000 四川省成都市高新区创业路6号

(72)发明人 刘杰 安红章 李大双 刘尚麟 吴开均

(74)专利代理机构 成都九鼎天元知识产权代理有限公司 51214
代理人 郭彩红

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)
G06Q 20/40(2012.01)

(56)对比文件
CN 106022917 A,2016.10.12,
CN 105976231 A,2016.09.28,
CN 105956923 A,2016.09.21,
US 2016210710 A1,2016.07.21,

审查员 陈露

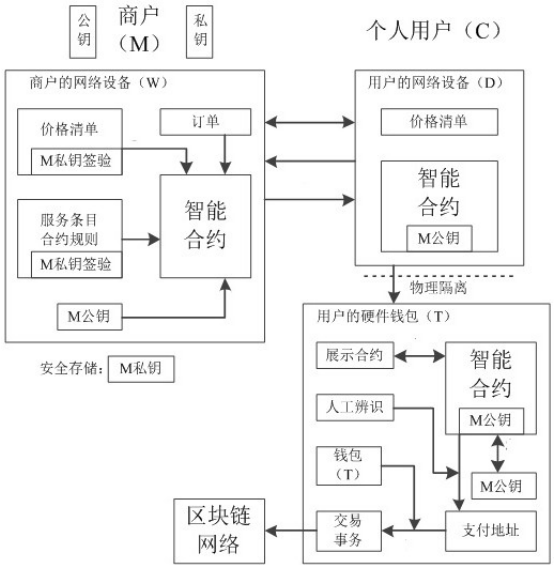
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种区块链中隐私保护智能合约方法

(57)摘要

本发明提供了一种区块链中隐私保护智能合约方法,在智能合约中加密数字资产交易参与方的内容信息,并进行密文处理;所述智能合约x采用Merkle树结构,Merkle树的叶子节点通过公钥进行加密,并采用哈希摘要值来替代区块头原始数据。与现有技术相比,使具有数据隐私保护要求的区块链中,具备数字资产交易数据和过程隐私保护功能,只有智能合约交易参与方可以查看交易信息,能够用于任何具有数据隐私保护要求的区块链应用场景。



CN 106559211 B

1.一种区块链中隐私保护智能合约方法,具体方法为:在智能合约x中加密数字资产交易参与方的内容信息,并进行密文处理;所述智能合约x采用Merkle树结构, Merkle树的叶子节点通过公钥进行加密,从而使密文的哈希值被用在Merkle树中,并采用哈希摘要值来替代区块头原始数据,从而隐藏Merkle树中的分支的内容;

所述智能合约方法,包括个人用户C和商户M;商户M收到个人用户C发来的订单后,通过商户M的私钥签验生成一个智能合约x;该智能合约x能够通过商户M的公钥的验证,并同商户M的公钥一同返回给个人用户C;将商户M的信息分为静态信息和动态信息;所述静态信息通过私钥签验进智能合约形成智能合约签验版本;商户M的设备W采用商户M的公钥验证所述智能合约签验版本的合法性,签验合法后,所述智能合约签验版本加上商户M的公钥被填充进智能合约模板存储在设备W中;当有订单产生时,商户M将订单和其收款的支付地址通过用户M的私钥一起签验,生成账单,并将该账单返回给设备W,商户M的设备W将订单细节填入智能合约模板,生成智能合约x,并返回给个人用户C的网络设备D;所述静态信息是指针对不同交易事务,智能合约中相同的部分;所述动态信息是指针对不同交易事务,智能合约中变化的部分。

2.根据权利要求1所述的智能合约方法,还包括个人用户C的可信路径设备T;个人用户C使用可信路径设备T来验证智能合约的签名,检查包含商户M的公钥的智能合约。

3.根据权利要求2所述的智能合约方法,所述C的可信路径设备T中存储有个人用户C的私钥,个人用户C发送的智能合约信息通过其私钥进行签验后发送出去,并通过个人用户C的网络设备D上包含的C的公钥签验合法后,随C的公钥一起发送给商户M。

4.根据权利要求1所述的智能合约方法,所述方法还包括,可信路径设备T永久存储智能合约x,该智能合约x同时也是给个人用户C的收据。

5.根据权利要求1所述的智能合约方法,所述方法还包括,商户M将静态信息中的价格列表作为一个签验项进行签验,并填充进智能合约,将服务种类和合约条件作为一个签验项进行签验,并填充进智能合约。

6.根据权利要求1所述的智能合约方法,智能合约的工作流程为:

定义:K是私钥,P是公钥,公私钥对(K,P)是商户M作为商家的表征,H是加密哈希函数;假设有一对函数d-addr()和d-priv(),其中,d-addr(P,H(x))是针对P和H(x)的唯一区块链地址,d-priv(K,x)是与d-addr(P,H(x))相对应的私钥;d-priv(K,x)需要根据K计算得出;定义b=d-addr(P,H(x))作为智能合约x的支付地址,则个人用户C能够计算出地址b,并且只有M能够获取b上面的资金;由于H(x)编码在输出地址b的内部,所以智能合约x是能够附着在支付交易上的;

商户M的设备W收到个人用户C的网络设备D发来的订单后,生成一个智能合约x,并且将智能合约x发送给网络设备D;针对不同交易事务,智能合约x中相同的部分被称为静态信息,静态信息按照M的需要进行改变,改变周期常常跨越若干个订单;智能合约x中,在不同交易事务中都变化的部分被称为动态信息;

假设智能合约x包含商户M的公钥P,所有的静态信息通过商户M的私钥K签验,所有的动态信息不用签验;当收到智能合约x时,网络设备D检查智能合约x是否与其要提出的订单信息相一致,如果一致,则将智能合约x转发给到可信路径设备T;然后可信路径设备T验证智能合约x中的所有签名,并且将公钥P和智能合约x展示给个人用户C;当个人用户C交互式的

同意该合约,则可信路径设备T计算b= d-addr(P,H(x)),并且生成并广播一个交易事务,通过该事务将用户添加到合约中的资金数目发送到地址b;最后,可信路径设备T永久的存储x。

一种区块链中隐私保护智能合约方法

技术领域

[0001] 本发明涉及一种区块链中隐私保护智能合约方法,特别是涉及一种适用于数字资产保护体系的区块链中隐私保护智能合约方法。

背景技术

[0002] 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。

[0003] 当前,区块链上数据的隐私保护是其在应用中遇到的一个实际问题。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。同态加密是一种无需对加密数据进行解密就可以执行计算的方法。它提供了一种重要的方法,能够在原有基础上使用区块链技术。通过使用同态加密技术在区块链上存储数据不会对区块链属性造成任何重大的改变。同态加密技术不仅提供了隐私保护,它同样会允许随时访问区块链上的加密数据进行审计或实现其他目的。

发明内容

[0004] 本发明要解决的技术问题是提供一种区块链中隐私保护智能合约方法,使具有数据隐私保护要求的区块链中,具备数字资产交易数据和过程隐私保护功能。

[0005] 本发明采用的技术方案如下:一种区块链中隐私保护智能合约方法,具体方法为:在智能合约中加密数字资产交易参与方的内容信息,并进行密文处理;所述智能合约x采用Merkle树结构, Merkle树的叶子节点通过公钥进行加密,并采用哈希摘要值来替代区块头原始数据。

[0006] 本发明方法使得只有智能合约交易参与方可以查看交易信息,能够用于任何具有数据隐私保护要求的区块链应用场景。采用哈希摘要值来替代区块头原始数据,从而隐藏Merkle树中的某个分支的内容;在智能合约内容中设置Merkle树的叶子节点通过公钥进行加密,从而使密文的哈希值被用在Merkle树中。

[0007] 智能合约是一组情景-应对型的程序化规则和逻辑,是部署在区块链上的去中心化、可信共享的程序代码。智能合约的运作机理如图1所示:通常情况下,智能合约经各方签验后,以程序代码的形式附着在区块链数据 (例如一笔区块链代币交易)上,经区块链网络传播和节点签验后记入区块链的特定区块中。智能合约封装了预定义的若干状态及转换规则、触发合约执行的情景(如到达特定时间或发生特定事件等)、特定情景下的应对行动等。区块链可实时监控智能合约的状态,并通过核查外部数据源和确认满足特定触发条件后激活并执行智能合约。

[0008] 包括个人用户C和商户M;商户M收到个人用户C发来的订单后,通过商户M的私钥签

验生成一个智能合约x;该智能合约x能够通过商户M的公钥的验证,并同商户M的公钥一同返回给个人用户C。

[0009] 每一个智能合约x有一个专有地址,并且有一个支付的公开证明。任何了解智能合约x交易方都可以验证x是否被支付。

[0010] 还包括个人用户C的可信路径设备T;个人用户C使用可信路径设备T来验证智能合约的签名,检查包含商户M的公钥的智能合约。

[0011] 个人用户C需要有一个可信的路径设备T,T可以显示所有x的敏感内容。

[0012] 所述可信路径设备T中存储有个人用户C的私钥,个人用户C发送的智能合约信息通过其私钥进行签验后发送出去,并通过个人用户C的网络设备D上存储的C的公钥验签合法后,随C的公钥一起发送给商户M。

[0013] 所述方法还包括,将商户M的信息分为静态信息和动态信息;所述静态信息通过M的私钥签验并填充进智能合约形成智能合约签验版本;商户M的设备W采用商户M的公钥验证所述智能合约签验版本的合法性,签验合法后,所述智能合约签验版本加上商户M的公钥被填充进智能合约模板存储在设备W中;当有订单产生时,商户M将订单和其收款的支付地址通过用户M的私钥一起签验,生成账单,并将该账单返回给设备W,商户M的设备W将订单细节填入智能合约模板,生成智能合约x,并返回给个人用户C的网络设备D;所述静态信息是指针对不同交易事务,智能合约中相同的部分;所述动态信息是指针对不同交易事务,智能合约中变化的部分。

[0014] 协议主要部分可以在非可信设备上执行(D或W)。特别的,D和W的通信链路不用要求是安全的(加密的或是认证的)。它可以是未加密的邮件。

[0015] 所述方法还包括,可信路径设备T永久存储智能合约x,该智能合约x同时也是给个人用户C的收据。因此M不能否认收到针对d-addr(P,x)的一笔支付。

[0016] 所述方法还包括,商户M将静态信息中的价格列表作为一个签验项进行签验,并填充进智能合约,将服务种类和合约条件作为一个签验项进行签验,并填充进智能合约。

[0017] 其工作流程为:

[0018] 定义:K是私钥,P是公钥,公私钥对(K,P)是商户M作为商家的表征,H是加密哈希函数;假设有一对函数d-addr()和d-priv(),其中,d-addr(P,H(x))是针对P和H(x)的唯一区块链地址,d-priv(K,x)是与d-addr(P,x)相对应的私钥;d-priv(K,x)需要根据K计算得出;定义b=d-addr(P,H(x))作为智能合约x的支付地址,则个人用户C能够计算出地址b,并且只有M能够获取b上面的资金;由于H(x)编码在输出地址b的内部,所以智能合约x是能够附着在支付交易上的;

[0019] 商户M的设备W收到个人用户C的网络设备D发来的订单后,生成一个智能合约x,并且将智能合约x发送给网络设备D;针对不同交易事务,智能合约x中相同的部分被称为静态信息,静态信息可以按照M的需要进行改变,这个周期常常跨越若干个订单;智能合约x中,在不同交易事务中都变化的部分被称为动态信息;

[0020] 假设智能合约x包含商户M的公钥P,所有的静态信息通过商户M的私钥K签验,所有的动态信息不用签验;当收到智能合约x时,网络设备D检查智能合约x是否与其要提出的订单信息相一致,如果一致,则将智能合约x转发给到可信路径设备T;然后可信路径设备T验证智能合约x中的所有签名,并且将公钥P和智能合约x展示给个人用户C;当个人用户C交互

式的同意该合约,则可信路径设备T计算b=d-addr(P,x),并且生成并广播一个交易事务,通过该事务将用户添加到合约中的资金数目发送到地址b;最后,可信路径设备T永久的存储x,因为该合约同时也是给个人用户C的收据。

[0021] 例如,M的服务和价格清单往往是固定的,为静态信息。例如,一个订单中D提供的所有信息,如服务类别、数量、地址等,都属于动态信息。

[0022] 第三方不能监控M所有的收入支付,因为它们不知道x的内容。如果x的随机化(哈希计算)处理做得很好,那么不论P[x]还是d-addr(P,x)都不能够通过商户M的公钥P与M连接。

[0023] 对于重复订单,C能够在不与M直接交互的情况下,完全依靠自身创造x。只有在交易事务结束后,C才需要将x提交给M。并且,交易事务的验证从网络浏览器层面(基于SSL/TLS证书的信任机制)转移到了支付层面(基于密钥P的信任机制)。在支付基础地址(例如P)上构建在线商家,是比在SSL/TLS证书上构建更为通用的一种方法。

[0024] 与现有技术相比,本发明的有益效果是:使具有数据隐私保护要求的区块链中,具备数字资产交易数据和过程隐私保护功能,只有智能合约交易参与方可以查看交易信息,能够用于任何具有数据隐私保护要求的区块链应用场景。

附图说明

[0025] 图1为智能合约运作机理示意图。

[0026] 图2为本发明其中一实施例的智能合约工作流程示意图。

具体实施方式

[0027] 为了使本发明的目的、技术方案及优点更加清楚明白,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。

[0028] 本说明书(包括摘要和附图)中公开的任一特征,除非特别叙述,均可被其他等效或者具有类似目的的替代特征加以替换。即,除非特别叙述,每个特征只是一系列等效或类似特征中的一个例子而已。

[0029] 具体实施例1

[0030] 一种区块链中隐私保护智能合约方法,具体方法为:在智能合约中加密数字资产交易参与方的内容信息,并进行密文处理;所述智能合约x采用Merkle树结构,Merkle树的叶子节点通过公钥进行加密,并采用哈希摘要值来替代区块头原始数据。

[0031] 本发明方法使得只有智能合约交易参与方可以查看交易信息,能够用于任何具有数据隐私保护要求的区块链应用场景。采用哈希摘要值来替代区块头原始数据,从而隐藏Merkle树中的某个分支的内容;在智能合约内容中设置Merkle树的叶子节点通过公钥进行加密,从而使密文的哈希值被用在Merkle树中。

[0032] 在本具体实施例中,包括个人用户C和商户M;商户M收到个人用户C发来的订单后,通过商户M的私钥签验生成一个智能合约x;该智能合约x能够通过商户M的公钥的验证,并同商户M的公钥一同返回给个人用户C。

[0033] 作为收据,用户C能够显示智能合约x的部分内容。极端情况下,用户C仅仅需要显

示其发起的某一个交易事务有一个受M控制的事务输出。其他情况下，用户C需要显示除了地址信息之外，智能合约的其余内容。

[0034] 用户C可以显示明文、密文或者哈希值。合约中交易事务的参与方用户C可以接收有加密域的合约，并能够验证该合约已经在区块链上进行支付，并可以将其发送给商户M。同时，所有人都不能看到加密域的明文。

[0035] 具体实施例2

[0036] 在具体实施例1的基础上，还包括个人用户C的可信路径设备T；个人用户C使用可信路径设备T来验证智能合约的签名，检查包含商户M的公钥的智能合约。

[0037] 具体实施例3

[0038] 在具体实施例1的基础上，所述可信路径设备T中存储有个人用户C的私钥，个人用户C发送的智能合约信息通过其私钥进行签验后发送出去，并通过个人用户网络设备上的公钥签验合法后，随公钥一起发送给商户M。

[0039] 合约中交易事务的参与方用户C能够验证该合约已经在区块链上进行支付，并可以将其发送给商户M。

[0040] 具体实施例4

[0041] 在具体实施例1到3之一的基础上，所述方法还包括，将商户M的信息分为静态信息和动态信息；所述静态信息通过私钥签验进智能合约形成智能合约签验版本；商户M的设备W采用商户M的公钥验证所述智能合约签验版本的合法性，签验合法后，所述智能合约签验版本加上商户M的公钥被编译进智能合约模板存储在设备W中；当有订单产生时，商户M将订单和其收款的支付地址通过用户M的私钥一起签验，生成账单，并将该账单返回给设备W，商户M的设备W将订单细节填入智能合约模板，生成智能合约x，并返回给个人用户的网络设备D；所述静态信息是指在不同智能合约中都相同的部分；所述动态信息是指不同智能合约中都变化的部分。

[0042] 商户M能够控制智能合约的内容设置。同时，为了使智能合约签验的过程更加自动化，将合约内容划分为静态信息和动态信息两个部分，这主要是根据智能合约涉及的订单是否发生变化来决定的。如果订单发生变化，则为动态信息；反之，则为静态信息。

[0043] 在基于隐私保护智能合约的实施过程中，定义：个人用户C，C拥有一个网络设备D，用户C与一个可信的路径设备T进行交互，T可以是可以签验交易事务的硬件钱包。T能够获取区块链上所用代币钱包的私钥，这里假设T没有被入侵。例如，在某个场景中T被安全的启动，从D通过无线链路获取数据，并且利用单向信道来向区块链网络广播已经签验的交易事务。此外，定义：商户M，M拥有一个设备W来接收和处理订单。处理一个订单要求至少生成一个支付地址，并且将此地址返回给个人用户C。因此，M需要将其钱包分割为两部分，地址钱包L和密钥钱包。地址钱包L存放在W上，而密钥钱包离线安全存储。

[0044] 具体实施例5

[0045] 在具体实施例2到4之一的基础上，所述方法还包括，可信路径设备T永久存储智能合约x，该智能合约x同时也是给个人用户C的收据。

[0046] 在完成支付后，C需要能够证明：(1)M已经同意在收到一定数量的代币支付后，完成订单；(2)对于该笔订单，一定数量的代币支付给了M，并且M已经收到。

[0047] 具体实施例6

[0048] 在具体实施例1到5之一的基础上，在基于书面形式的用户-商户交易流程如下：(1)M首先签验这个账单；(2)M通过收据签验该笔资金的交易，该收据通常包含账单信息。

[0049] 在基于区块链上智能合约的交易事务中，账单是由M签验的一个合约x，用户C加入这个合约并同意合约包含的支付条款。如果x的哈希值被附着在区块链的交易事务上，那么这个交易事务就可以证明M通过收据签验了该笔资金的交易，并且该收据包含账单信息。

[0050] 智能合约x包含了C加入合约需要遵循的合约条款。x包含了支付地址，并且被M签验。本专利描述的带隐私保护的智能合约不仅对合约内容进行隐私保护，还对交易事务中的支付地址进行隐私保护。

[0051] 所述方法还包括，商户M将静态信息中的价格列表作为一个签验项进行签验进智能合约，将服务种类和合约条件作为一个签验项进行签验进智能合约。

[0052] 具体实施例7

[0053] 在具体实施例1到6之一的基础上，如图2所示，其工作流程为：

[0054] 定义:K是私钥，P是公钥，公私钥对(K,P)是M作为商家的表征，H是加密哈希函数；假设有一对函数d-addr()和d-priv()，其中，d-addr(P,H(x))是针对P和H(x)的唯一区块链地址，d-priv(K,x)是与d-addr(P,x)相对应的私钥；d-priv(K,x)需要根据K计算得出；定义b=d-addr(P,H(x))作为智能合约x的支付地址，则用户C能够计算出地址b，并且只有M能够获取b上面的资金；由于H(x)编码在输出地址b的内部，所以智能合约x是能够附着在支付交易上的。

[0055] 商户M的设备W收到用户C的网络设备D发来的订单后，生成一个智能合约x，并且将智能合约x发送给网络设备D；智能合约x在不同合约中都相同的部分被称为静态信息；静态信息能够按照M的需要进行改变，这个周期常常跨越若干个订单；例如，M的服务和价格清单往往是固定的，为静态信息。智能合约x中，在每一笔交易事务都变化的部分被称为动态信息。例如，一个订单中D提供的所有信息，如服务类别、数量、地址等，都属于动态信息。

[0056] 假设x包含M的公钥P，所有的静态信息通过商户M的私钥K签验，所有的动态信息不用签验；当收到智能合约x时，网络设备D检查智能合约x是否与其要提出的订单信息相一致，如果一致，则将智能合约x转发给可信路径设备T；然后可信路径设备T验证智能合约x中的所有签名，并且将公钥P和智能合约x展示给用户C；当用户C交互式的同意该合约，则可信路径设备T计算b=d-addr(P,x)，并且生成并广播一个交易事务，通过该事务将用户添加到合约中的资金数目发送到地址b；最后，可信路径设备T永久的存储x，因为该合约同时也是给C的收据。

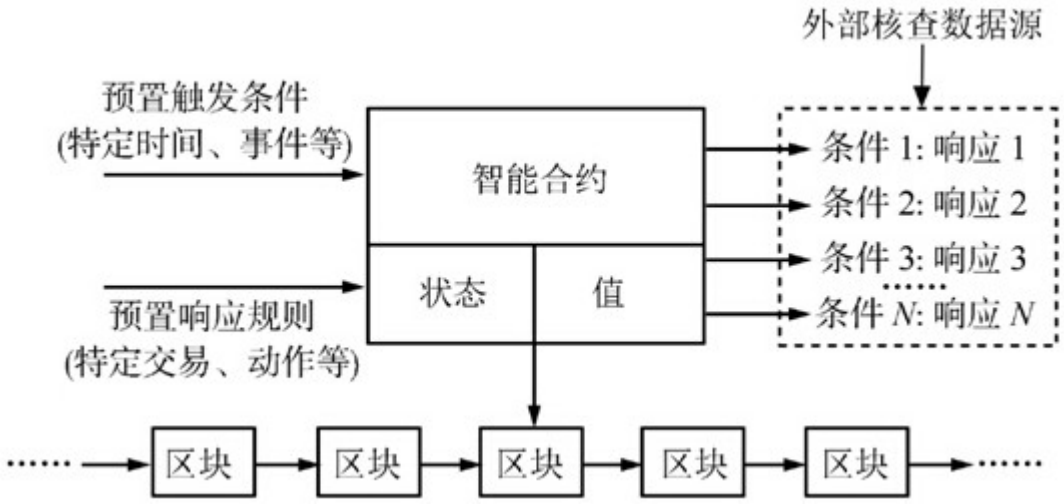

外部核查数据源
预置触发条件
(特定时间、事件等)
智能合约
状态
值
预置响应规则
(特定交易、动作等)
条件 1: 响应 1
条件 2: 响应 2
条件 3: 响应 3
条件 N: 响应 N
区块
区块
区块
区块
区块

图1

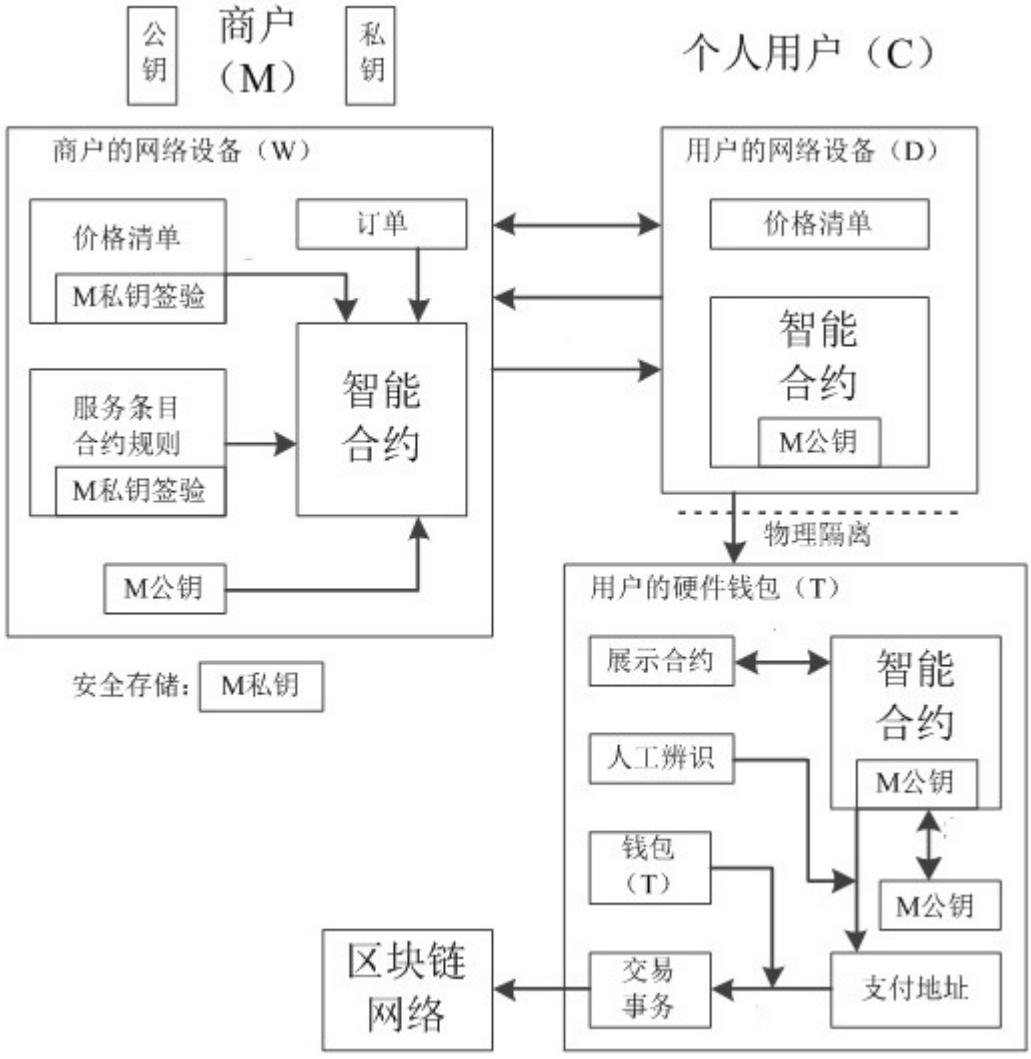

公钥
商户
（M）
私钥
个人用户（C）
商户的网络设备（W）
价格清单
M私钥签验
订单
服务条目
合约规则
M私钥签验
智能
合约
M公钥
安全存储：M私钥
用户的网络设备（D）
价格清单
智能
合约
M公钥
物理隔离
用户的硬件钱包（T）
展示合约
智能
合约
人工辨识
M公钥
钱包
（T）
M公钥
区块链
网络
交易
事务
支付地址

图2