

# (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局

(43) 国际公布日  
2019 年 8 月 8 日 (08.08.2019)



(10) 国际公布号  
**WO 2019/148783 A1**

- (51) 国际专利分类号:  
**G06Q 20/38** (2012.01)
- (21) 国际申请号: PCT/CN2018/096807
- (22) 国际申请日: 2018 年 7 月 24 日 (24.07.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201810090202.8 2018 年 1 月 30 日 (30.01.2018) CN
- (71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518052 (CN)。
- (72) 发明人: 吴贞海 (WU, Zhenhai); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518052 (CN)。
- (74) 代理人: 广州华进联合专利商标代理有限公司 (ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区珠江东路 6 号 4501 房 (部位: 自编 01-03 和 08-12 单元) (仅限办公用途), Guangdong 510623 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

(54) **Title:** TRANSACTION PROCESSING METHOD AND DEVICE, COMPUTER DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 交易处理方法、装置、计算机设备和存储介质

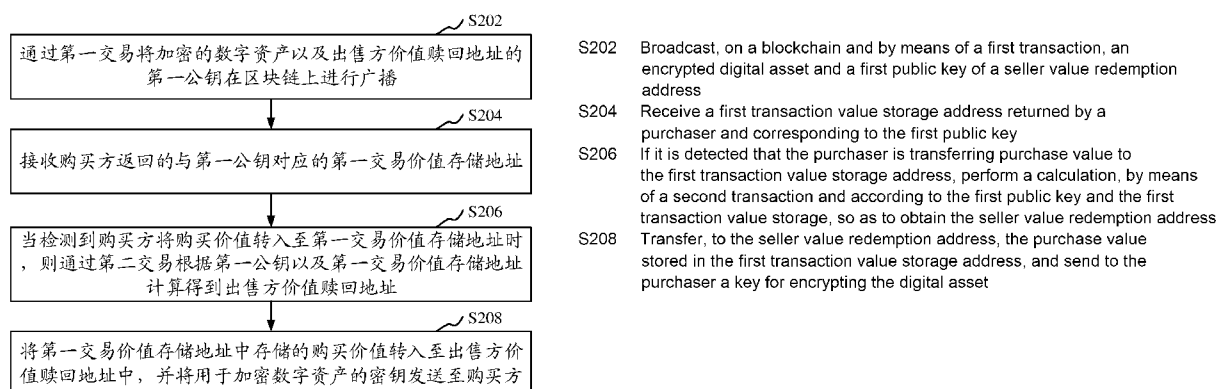


图 2

(57) **Abstract:** A transaction processing method comprises: broadcasting, on a blockchain and by means of a first transaction, an encrypted digital asset and a first public key of a seller value redemption address; receiving a first transaction value storage address returned by a purchaser and corresponding to the first public key; if it is detected that the purchaser is transferring purchase value to the first transaction value storage address, performing a calculation, by means of a second transaction and according to the first public key and the first transaction value storage address, so as to obtain the seller value redemption address; and transferring, to the seller value redemption address, the purchase value stored in the first transaction value storage address, and sending to the purchaser a key for encrypting the digital asset.

(57) **摘要:** 一种交易处理方法, 包括: 通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播; 接收购买方返回的与第一公钥对应的第一交易价值存储地址; 当检测到所述购买方将购买价值转入至第一交易价值存储地址时, 则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址; 将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中, 并将用于加密所述数字资产的密钥发送至所述购买方。

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,  
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,  
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明，要求每一种可提供的地区  
保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,  
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,  
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,  
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,  
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,  
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,  
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

- 包括国际检索报告 (条约第21条(3))。

**发明名称：交易处理方法、装置、计算机设备和存储介质****相关申请的交叉引用**

本申请要求于 2018 年 1 月 30 日提交中国专利局，申请号为 2018100902028，申请名称为“交易处理方法、装置、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

**技术领域**

本申请一种交易处理方法、装置、计算机设备和存储介质。

**背景技术**

随着计算机技术的发展，出现了网上交易，该网上交易一般是用于进行数字化资产的交易，该数字化资产可以是一部电影、一份电子版芯片设计手册、一份查询列表等，网上交易一般是设置一个中心化的结算系统，该结算系统用于对出售方和购买方进行控制，以实现交易。

然而，发明人意识到，目前的交易方式需要设置一个结算系统，出售方和购买方均需要在该结算系统进行注册登记等，而没有在结算中心进行注册登记的出售方或购买方则不能进行交易，形成了中心化处理结算系统，造成结算系统压力大。

**发明内容**

根据本申请公开的各种实施例，提供一种交易处理方法、装置、计算机设备和存储介质。

一种交易处理方法，包括：

通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；

接收购买方返回的与所述第一公钥对应的第一交易价值存储地址；

当检测到所述购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址；及

将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中，并将用于加密所述数字资产的密钥发送至所述购买方。

一种交易处理装置，包括：

广播模块，用于通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；

接收模块，用于接收购买方返回的与所述第一公钥对应的第一交易价值存储地址；

计算模块,用于当检测到所述购买方将购买价值转入至第一交易价值存储地址时,则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址;及

交易模块,用于将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中,并将用于加密所述数字资产的密钥发送至所述购买方。

一种计算机设备,包括存储器和一个或多个处理器,所述存储器中储存有计算机可读指令,所述计算机可读指令被所述处理器执行时,使得所述一个或多个处理器执行以下步骤:通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播;接收购买方返回的与所述第一公钥对应的第一交易价值存储地址;当检测到所述购买方将购买价值转入至第一交易价值存储地址时,则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址;及将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中,并将用于加密所述数字资产的密钥发送至所述购买方。

一个或多个存储有计算机可读指令的非易失性计算机可读存储介质,计算机可读指令被一个或多个处理器执行时,使得一个或多个处理器执行以下步骤:通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播;接收购买方返回的与所述第一公钥对应的第一交易价值存储地址;当检测到所述购买方将购买价值转入至第一交易价值存储地址时,则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址;及将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中,并将用于加密所述数字资产的密钥发送至所述购买方。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征和优点将从说明书、附图以及权利要求书变得明显。

## 附图说明

为了更清楚地说明本申请实施例中的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其它的附图。

图1为根据一个或多个实施例中交易处理方法的应用场景图。

图2为根据一个或多个实施例中交易处理方法的流程示意图。

图3为根据一个或多个实施例中区块结构示意图。

图4为根据一个或多个实施例中区块链的示意图。

图5为根据一个或多个实施例中的交易处理方法的时序图。

图6为根据一个或多个实施例中交易处理装置的结构框图。

图7为根据一个或多个实施例中计算机设备的内部结构图。

## 具体实施方式

为了使本申请的技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

本申请提供的交易处理方法，可以应用于如图 1 所示的应用环境中。出售方和购买方均与区块链进行通信。出售方可以将待出售的数字资产加密后在区块链上进行广播，从而购买方可以获得到该数字资产，购买方在获取到该数字资产后，首先根据出售方的出售方价值赎回地址的第一公钥构造合约，并将购买价值转入到该合约指定的第一交易价值存储地址中，当出售方检测到购买方将购买价值转入至第一交易价值存储地址，则提取该第一交易价值存储地址中存储的购买价值，并将加密数字资产的密钥发送给购买方以完成交易。出售方和购买方对应的终端可以但不限于各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备。

在其中一个实施例中，如图 2 所示，提供了一种交易处理方法，以该方法应用于图 1 中的出售方为例进行说明，包括以下步骤：

S202：通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播。

具体地，数字化资产的样式多样，可以包括一部电影（movie），一份电子版芯片设计手册（datasheet），一份查询列表（query list）等等。第一交易是出售方将待出售的数字资产在区块链上进行广播的交易，区块链在接收到该第一交易后，区块链中的节点可以竞争性地挖矿，以计算该第一交易的有效性。

出售方可以将要出售的数字资产通过密钥进行加密后再在区块链上进行广播，从而购买方不能直接获取到该数字资产的明文，只有在出售方将加密该数字资产的密钥提供给购买方后，购买方才能获取到数字资产的明文。且由于存储在区块链上的数据均是需要通过私钥进行加密的，其是为了保护数据的安全性，因此为了保证出售方价值赎回地址的安全性，出售方将出售方价值赎回地址的第一公钥在区块链上进行广播，从而可以防止区块链上的非法分子获取到出售方价值赎回地址，进而获取到该出售方价值赎回地址中的价值。

S204：接收购买方返回的与第一公钥对应的第一交易价值存储地址。

具体地，当存在购买方想要购买该数字资产时，则获取到出售方广播的加密的数字资产以及出售方价值赎回地址的第一公钥，并根据该第一公钥和购买方的购买方价值赎回地址生成一合约，例如该合约的内容可以表示为当购买方提供购买该数字资产的购买价值时，则给出售方的出售方价值赎回地址，从而可以将购买价值转入到出售方价值赎回地址中，出售方在收到购买价值后则可以将加密数字资产的密钥转发给对应的购买方，当购买方未提供购买该数字资产的购买价值，或者是所提供的购买价值不是针对该数字资产的时候，则将该购买价值退回至购买方价值赎回地址中。

在获得到该合约后，可以对该合约按照预设规则进行计算得到第一交易价值存储地

址，例如可以对合约进行二次摘要计算得到第一交易价值存储地址。为了防止出售方在获取到价值后不将数字资产转给购买方，因此可以购买方先将购买价值转入到第一交易价值存储地址中，并在购买方获取到该第一交易价值存储地址中的购买价值后，区块链主动将出售方用于加密数字资产的密钥提供给购买方。且购买方在向第一交易价值存储地址转入购买价值后，可以对该次交易进行签名，以确保交易的安全性，并实现对第一交易价值存储地址中的价值的锁定，从而只有验证成功的才可以从该第一交易价值存储地址中获取到购买价值。

S206：当检测到购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据第一公钥以及第一交易价值存储地址计算得到出售方价值赎回地址。

具体地，当出售方检测到购买方将购买价值转入至第一交易价值存储地址时，即出售方检测到购买方将购买价值转入至公共价值存储地址时，则可以提供自身的出售方价值赎回地址，以便于将区块链中第一交易价值存储地址中的购买价值转入至自身的出售方价值赎回地址中，其中该出售方价值赎回地址由于在区块链上是以第一公钥的形式存在的，因此需要根据第一公钥以及第一交易价值存储地址计算得到。具体地可以是对通过出售方自身的第一私钥进行验证，只有验证成功的第一公钥，才会得到正确的出售方价值赎回地址。从而可以根据第一交易价值存储地址中的购买价值转入至出售方价值赎回地址。

S208：将第一交易价值存储地址中存储的购买价值转入至出售方价值赎回地址中，并将用于加密数字资产的密钥发送至购买方。

具体地，在获取到出售方价值赎回地址后，则出售方可以将第一交易价值存储地址中存储的购买价值转入至出售方价值赎回地址中，并在获取到购买价值后，将用于加密数字资产的密钥发送给购买方，从而购买方可以根据获取到的用于加密数字资产的密钥对加密的数字化资产进行解密得到数字资产的明文。且可选地，在出售方将用于加密数字资产的密钥发送至购买方的时候，可以预先与购买方约定加密密钥的加密方式，从而可以方式密钥在传输的过程中被非法分子获取到，或者可以将密钥存储至区块链上的一存储地址中，从而购买方可以直接从该存储地址中获取到相应的密钥。

出售方在区块链上广播的是加密的数字资产以及用于加密数字资产的密钥的摘要，从而购买方无法解密得到该数字资产，保证了数字资产的安全性，且在交易过程中不需要交易局的参与，去中心化，提高了交易的实效性。

上述交易处理方法，不需要中心化的结算系统，出售方和购买方可以通过区块链自由地进行交易，出售方可以将出售的资产进行加密后在区块链上进行广播，从而需要购买该数字资产的购买方可以根据出售方的价值赎回地址的第一公钥构造合约，并购买价值转入到该合约指定的第一交易价值存储地址中，当出售方检测到购买方将购买价值转入至第一交易价值存储地址，则提取该第一交易价值存储地址中存储的购买价值，并将加密数字资产的密钥发送给购买方以完成交易。

在其中一个实施例中，该交易处理方法还可以包括：通过第一交易将用于加密数字

资产的密钥的第一摘要在区块链上进行广播；接收购买方返回的第一摘要。从而通过第二交易根据第一公钥以及第一交易价值存储地址计算得到出售方价值赎回地址的步骤，即上述步骤 S206 可以包括：通过第二交易获取用于加密数字资产的密钥，并计算密钥的第二摘要；当第二摘要与第一摘要相同时，则通过出售方价值赎回地址的第一私钥验证第一公钥；当验证成功时，则获取到出售方价值赎回地址。

具体地，在本实施例中，出售方不仅将加密的数字资产在区块链上进行广播，还将用于加密数字资产的密钥的第一摘要在区块链上进行广播，即出售方想要出售某一数字资产时，首先将该数字资产通过密钥进行加密，然后计算密钥的第一摘要，并将加密的数字资产、第一摘要以及出售方价值赎回地址的第一公钥在区块链上进行广播。从而购买方可以获取到该加密的数字资产、第一摘要以及出售方价值赎回地址的第一公钥，购买方在获取到第一公钥后，还可以获取到购买方价值赎回地址的第二公钥，并根据第一公钥以及第二公钥生成一合约，根据该合约可以生成第一交易价值存储地址，并将自己的购买价值转入到该第一交易价值存储地址中后，通知出售方购买价值已经转入到第一交易价值存储地址中，并通过第一摘要来确定其所要购买的数字资产是哪一个，即第一摘要可以唯一地确定数字资产。

其中，在出售方接收到购买方已经将购买价值转入到第一交易价值存储地址中后，可以开启一第二交易，通过该第二交易向区块链提供用于加密数字资产的密钥，并按照预设的算法计算密钥的第二摘要，当第二摘要与第一摘要相同时，则可以确定购买方所要购买的数字资产，并通过与该数字资产对应的出售方价值赎回地址的第一私钥验证第一公钥，只有验证成功后，第一交易价值存储地址中的购买价值才可以转入到该出售方价值赎回地址中，即出售方可以提供出该出售方价值赎回地址。

其中，购买方还需要预先将一定的价值转入到区块链的购买方价值存储地址中，该购买方价值存储地址可以与购买方价值赎回地址相同，从而购买方在交易时，可以直接将购买方价值存储地址中的价值转入到第一交易价值存储地址中，以顺利地完成交易。

上述实施例中，引入了第一摘要，通过第一摘要来确定购买方所购买的数字资产，并且在第一摘要验证成功后，通过出售方价值赎回地址的第一私钥验证第一公钥，保证了交易的安全性。

在其中一个实施例中，该交易处理方法还可以包括：接收购买方返回的与第一公钥对应的赎回脚本。从而通过第二交易获取用于加密数字资产的密钥的步骤之前，还可以包括：通过第二交易根据赎回脚本计算得到第二交易价值存储地址；当第二交易价值存储地址与第一交易价值存储地址一致时，则继续通过第二交易获取用于加密数字资产的密钥的步骤。

在其中一个实施例中，赎回脚本是由购买方根据第一公钥以及购买方价值赎回地址的第二公钥生成的，第一交易价值存储地址是购买方根据赎回脚本生成的。

具体地，赎回脚本是根据出售方价值赎回地址的第一公钥和购买方价值赎回地址的

第二公钥生成的，其本质上为本次交易的合约。即购买方将在获取到第一公钥和第二公钥后，通过脚本虚拟机生成赎回脚本，并通过对赎回脚本按照预设规则进行计算得到第一交易价值存储地址，然后购买方将购买方资金转入到该第一交易价值存储地址中，其中预设规则可以是二次摘要计算等，但是需要保证购买方和出售方的预设规则相同，从而购买方和出售方根据同一个赎回脚本得到的交易价值存储地址是相同的。

其中为了保证购买方发送的第一交易价值存储地址与赎回脚本是相对应的，出售方在获取到购买方返回的赎回脚本后，按照与购买方相同的预设规则根据赎回脚本计算得到第二交易价值存储地址，当第二交易价值存储地址与第一交易价值存储地址一致，则说明购买方的赎回脚本与其转入资金的第一交易价值存储地址相同，因此可以继续交易。

上述实施例中，对赎回脚本和第一交易价值存储地址进行了再一次的验证，进一步提高了交易的安全性。

在其中一个实施例中，该交易处理方法还包括一购买方价值赎回步骤，即当出售方不进行交易的情况下，购买方可以赎回相应的购买价值，该步骤可以包括：当第二摘要与第一摘要不相同，则获取预设区块数量；获取参与计算第二交易的区块的数量；当参与计算第二交易的区块的数量大于预设区块数量时，则根据第一交易价值存储地址得到第二公钥；当购买方提供的购买方价值赎回地址的第二私钥与第二公钥验证成功时，将第一交易价值存储地址中存储的购买价值转入至购买方价值赎回地址中。

具体地，区块链作为一种新型的使用分布式的计算设备产生共识（节点间相互可信的数据和计算行为）的方法，也被称作分布式账本。其中核心的设计思想包括使用工作量证明机制保护账本可信。具体的过程描述如下：分布式网络中的记账节点计算机（俗称矿工），通过网络收集市场的转账交易信息，矿工以特定的格式打包若干个数量的交易信息到一个区块的数据结构中（block），这个时候矿工节点再按照固定的一个格式生成一个对应于这个block的区块头部（block header），这个区块头部中除了基本的描述当前block信息之外，还有2个重要的属性，一个是关于所有交易的一个特殊摘要值（hash，从所有序列化的交易中通过merkle-tree方法构造），另一个是一个位置的随机数字段nonce。有了这个区块头部以后，矿工开始一下步骤搜索一个特定的随机数：计算初始值随机数对应的header结构的hash，检测该hash是否满足区块链对当前区块的难度设定。如果满足，结束搜索，将该随机数nonce写入区块头部，向网络中的其他节点广播这个区块，等待其他节点把这个block接受，并写入各自的区块链。如果不满足设定工作量证明，继续递增随机数nonce，计算hash，检查难度。直到找到一个合适的难度，该区块计算完成，并继续寻找下一区块进行计算。具体的区块的结构请参阅图3，其中一个区块包括区块头部和区块主体，其中区块头部包括前一个区块的摘要、本区块的摘要。时间、版本、初始随机数、交易构造的默克树的根（相当于预设工作量难度），交易主体则涉及多个交易。具体的区块链的结构请参阅图4。

其中，当第二交易中所计算的第二摘要与第一摘要不相同，即购买方所提供的用

于加密数字资产的密钥的摘要与出售方的一致时，则可以获取到参与第二交易计算的区块的数量，当区块数量大于预设区块数量时，则认为交易超时，即出售方不会完成本次交易，则根据第一交易价值存储地址得到第二公钥，例如首先根据第二交易存储地址得到赎回脚本，再获取到赎回脚本中的第二公钥，从而当购买方提供的购买方价值赎回地址的第二私钥与第二公钥验证成功时，将第一交易价值存储地址中存储的购买价值转入至购买方价值赎回地址中，以结束交易。

上述实施例中，引入区块链的计算机制，通过区块链的计算机制来判断交易是否超时，如果超时则可以将第一交易价值存储地址中的价值返回至购买方价值赎回地址中，以完成交易。

参阅图 5，图 5 为一实施例中的交易处理方法的时序图，该交易处理方法可以包括：出售方将加密的数字资产，加密数字资产的密钥的第一摘要以及出售方价值赎回地址的第一公钥发送至区块链上进行广播，购买方根据想要购买的数字资产，获取到出售方在区块链上广播的加密的数字资产，加密数字资产的密钥的第一摘要以及出售方价值赎回地址的第一公钥，并根据购买方价值赎回地址的第二公钥生成赎回脚本，然后根据该赎回脚本生成第一交易价值存储地址，并将购买价值转入到该第一交易价值存储地址中，其中，购买方可以预先将一定的价值转入到区块链的购买方价值存储地址中，从而购买时可以直接将购买方价值存储地址中的价值转入到第一交易价值存储地址中，且购买方在价值转入成功后，向出售方发送携带有第一交易价值存储地址的消息以及生成的赎回脚本，从而出售方可以按照与购买方相同的预设规则对赎回脚本进行计算得到第二交易价值存储地址，并比较该第一交易价值存储地址以及第二交易价值存储地址，只有该第一交易价值存储地址以及第二交易价值存储地址相同时，才会继续交易。

为了方便，出售方在接收到赎回脚本以及价值转入成功的消息后，可以开启一第二交易以完成购买价值的转移和加密数字资产的密钥的转移。其中，在实际应用过程中，可以通过堆栈的形式实现第二交易的过程。该第二交易的输入可以为加密数字资产的密钥、赎回脚本、出售方价值赎回地址的第一私钥，输出为出售方价值赎回地址。该第二交易的具体处理过程是：首先将出售方价值赎回地址的第一私钥压入到堆栈中，将加密数字资产的密钥压入堆栈中，然后计算加密数字资产的密钥的第一摘要，并通过该第一摘要与出售方返回的第二摘要进行比对，如果相同，则在堆栈的头部压入 true，从而根据第一私钥对赎回脚本中出售方价值赎回地址的第一公钥进行验证，如果验证成功，则输出出售方价值赎回地址。从而出售方可以将第一交易价值存储地址中的交易价值转入到出售方价值赎回地址中，并将加密数字资产的密钥发送给对应的购买方，从而购买方可以根据该密钥对加密的数字资产进行解密得到数字资产的明文以完成交易。

此外，在第二交易过程中，如果第一摘要和第二摘要不相同，则在堆栈的头部压入 false，并将超时参数压入到堆栈中，该超时参数即预设区块的数量，从而购买方可以检测参与计算第二交易的区块是否达到预设的区块数量，如果是，则将购买方的购买方价值赎

回地址的第二公钥压入到堆栈中，从而购买方提供正确的第二私钥后，区块链通过第二公钥验证该第二私钥后，可以将第一交易价值存储地址中的购买价值返回给购买方以结束交易。

应该理解的是，虽然图 2 和图 5 的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图 2 和图 5 中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

在其中一个实施例中，如图 6 所示，提供了一种交易处理装置，包括：广播模块 100、接收模块 200、计算模块 300 和交易模块 400，其中：

广播模块 100，用于通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播。

接收模块 200，用于接收购买方返回的与第一公钥对应的第一交易价值存储地址。

计算模块 300，用于当检测到购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据第一公钥以及第一交易价值存储地址计算得到出售方价值赎回地址。

交易模块 400，用于将第一交易价值存储地址中存储的购买价值转入至出售方价值赎回地址中，并将用于加密数字资产的密钥发送至购买方。

在其中一个实施例中，广播模块 100 还可以用于通过第一交易将用于加密数字资产的密钥的第一摘要在区块链上进行广播。

接收模块 200 还用于接收购买方返回的第一摘要；

计算模块 300 可以包括：

摘要计算单元，用于通过第二交易获取用于加密数字资产的密钥，并计算密钥的第二摘要。

验证单元，用于当第二摘要与第一摘要相同时，则通过出售方价值赎回地址的第一私钥验证第一公钥。

地址获取单元，用于当验证成功时，则获取到出售方价值赎回地址。

在其中一个实施例中，接收模块 200 还可以用于接收购买方返回的与第一公钥对应的赎回脚本。

装置还可以包括：

比较模块，用于通过第二交易根据赎回脚本计算得到第二交易价值存储地址；当第二交易价值存储地址与第一交易价值存储地址一致时，则继续通过第二交易获取用于加密数字资产的密钥。

在其中一个实施例中，赎回脚本是由购买方根据第一公钥以及购买方价值赎回地址

的第二公钥生成的，第一交易价值存储地址是购买方根据赎回脚本生成的。

在其中一个实施例中，装置还可以包括：

预设区块数量获取模块，用于当第二摘要与第一摘要不相同，则获取预设区块数量。

5 当前区块数量获取模块，用于获取参与计算第二交易的区块的数量。

第二公钥获取模块，用于当参与计算第二交易的区块的数量大于预设区块数量时，则根据第一交易价值存储地址得到第二公钥。

赎回模块，用于当购买方提供的购买方价值赎回地址的第二私钥与第二公钥验证成功时，将第一交易价值存储地址中存储的购买价值转入至购买方价值赎回地址中。

10 关于交易处理装置的具体限定可以参见上文中对于交易处理方法的限定，在此不再赘述。上述交易处理装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

在其中一个实施例中，提供了一种计算机设备，该计算机设备可以是终端，其内部结构图可以如图 7 所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口、显示屏和输入装置。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机可读指令。该内存储器为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机可读指令被处理器执行时以实现一种交易处理方法。该计算机设备的显示屏可以是液晶显示屏或者电子墨水显示屏，该计算机设备的输入装置可以是显示屏上覆盖的触摸层，也可以是计算机设备外壳上设置的按键、轨迹球或触控板，还可以是外接的键盘、触控板或鼠标等。

本领域技术人员可以理解，图 7 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

一种计算机设备，包括存储器和一个或多个处理器，存储器中储存有计算机可读指令，计算机可读指令被处理器执行时，使得一个或多个处理器执行以下步骤：通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；接收购买方返回的与第一公钥对应的第一交易价值存储地址；当检测到购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据第一公钥以及第一交易价值存储地址计算得到出售方价值赎回地址；及将第一交易价值存储地址中存储的购买价值转入至出售方价值赎回地址中，并将用于加密数字资产的密钥发送至购买方。

在其中一个实施例中，处理器执行计算机可读指令时还实现以下步骤：通过第一交易将用于加密数字资产的密钥的第一摘要在区块链上进行广播；接收购买方返回的第一摘

要；处理器执行计算机可读指令时所实现的通过第二交易根据第一公钥以及第一交易价值存储地址计算得到出售方价值赎回地址的步骤，可以包括：通过第二交易获取用于加密数字资产的密钥，并计算密钥的第二摘要；当第二摘要与第一摘要相同时，则通过出售方价值赎回地址的第一私钥验证第一公钥；及当验证成功时，则获取到出售方价值赎回地址。

5 在其中一个实施例中，处理器执行计算机可读指令时还实现以下步骤：接收购买方返回的与第一公钥对应的赎回脚本；处理器执行计算机可读指令时所实现的通过第二交易获取用于加密数字资产的密钥的步骤之前，还可以包括：通过第二交易根据赎回脚本计算得到第二交易价值存储地址；及当第二交易价值存储地址与第一交易价值存储地址一致时，则继续通过第二交易获取用于加密数字资产的密钥的步骤。

10 在其中一个实施例中，处理器执行计算机可读指令时所提到的赎回脚本是由购买方根据第一公钥以及购买方价值赎回地址的第二公钥生成的，第一交易价值存储地址是购买方根据赎回脚本生成的。

在其中一个实施例中，处理器执行计算机可读指令时还实现以下步骤：当第二摘要与第一摘要不相同，则获取预设区块数量；获取参与计算第二交易的区块的数量；当参与计算第二交易的区块的数量大于预设区块数量时，则根据第一交易价值存储地址得到第二公钥；及当购买方提供的购买方价值赎回地址的第二私钥与第二公钥验证成功时，将第一交易价值存储地址中存储的购买价值转入至购买方价值赎回地址中。

15 一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；接收购买方返回的与第一公钥对应的第一交易价值存储地址；当检测到购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据第一公钥以及第一交易价值存储地址计算得到出售方价值赎回地址；及将第一交易价值存储地址中存储的购买价值转入至出售方价值赎回地址中，并将用于加密数字资产的密钥发送至购买方。

20 在其中一个实施例中，计算机可读指令被处理器执行时还实现以下步骤：通过第一交易将用于加密数字资产的密钥的第一摘要在区块链上进行广播；接收购买方返回的第一摘要；计算机可读指令被处理器执行时所实现的通过第二交易根据第一公钥以及第一交易价值存储地址计算得到出售方价值赎回地址的步骤，可以包括：通过第二交易获取用于加密数字资产的密钥，并计算密钥的第二摘要；当第二摘要与第一摘要相同时，则通过出售方价值赎回地址的第一私钥验证第一公钥；及当验证成功时，则获取到出售方价值赎回地址。

25 在其中一个实施例中，计算机可读指令被处理器执行时还实现以下步骤：接收购买方返回的与第一公钥对应的赎回脚本；在其中一个实施例中，计算机可读指令被处理器执行时所实现的通过第二交易获取用于加密数字资产的密钥的步骤之前，还可以包括：通过第二交易根据赎回脚本计算得到第二交易价值存储地址；及当第二交易价值存储地址与第

一交易价值存储地址一致时，则继续通过第二交易获取用于加密数字资产的密钥的步骤。

在其中一个实施例中，计算机可读指令被处理器执行时所提到的赎回脚本是由购买方根据第一公钥以及购买方价值赎回地址的第二公钥生成的，第一交易价值存储地址是购买方根据赎回脚本生成的。

- 5 在其中一个实施例中，计算机可读指令被处理器执行时还实现以下步骤：当第二摘要与第一摘要不相同，则获取预设区块数量；获取参与计算第二交易的区块的数量；当参与计算第二交易的区块的数量大于预设区块数量时，则根据第一交易价值存储地址得到第二公钥；及当购买方提供的购买方价值赎回地址的第二私钥与第二公钥验证成功时，将第一交易价值存储地址中存储的购买价值转入至购买方价值赎回地址中。
- 10 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一非易失性计算机可读存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器
- 15 (ROM)、可编程 ROM (PROM)、电可编程 ROM (EPROM)、电可擦除可编程 ROM (EEPROM) 或闪存。易失性存储器可包括随机存取存储器 (RAM) 或者外部高速缓冲存储器。作为说明而非局限，RAM 以多种形式可得，诸如静态 RAM (SRAM)、动态 RAM (DRAM)、同步 DRAM (SDRAM)、双数据率 SDRAM (DDRSDRAM)、增强型 SDRAM (ESDRAM)、同步链路 (Synchlink) DRAM (SLDRAM)、存储器总线 (Rambus) 直接
- 20 RAM (RDRAM)、直接存储器总线动态 RAM (DRDRAM)、以及存储器总线动态 RAM (RDRAM) 等。

以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

## 权利要求书

1、一种交易处理方法，包括：

通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；

接收购买方返回的与所述第一公钥对应的第一交易价值存储地址；

5 当检测到所述购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址；及

将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中，并将用于加密所述数字资产的密钥发送至所述购买方。

2、根据权利要求1所述的方法，其特征在于，所述方法还包括：

10 通过第一交易将用于加密所述数字资产的密钥的第一摘要在区块链上进行广播；

接收所述购买方返回的所述第一摘要；

所述通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址，包括：

通过第二交易获取用于加密所述数字资产的密钥，并计算所述密钥的第二摘要；

15 当所述第二摘要与所述第一摘要相同时，则通过所述出售方价值赎回地址的第一私钥验证所述第一公钥；及

当验证成功时，则获取到出售方价值赎回地址。

3、根据权利要求2所述的方法，其特征在于，所述方法还包括：

接收所述购买方返回的与所述第一公钥对应的赎回脚本；

20 所述通过第二交易获取用于加密所述数字资产的密钥之前，还包括：

通过第二交易根据所述赎回脚本计算得到第二交易价值存储地址；及

当所述第二交易价值存储地址与所述第一交易价值存储地址一致时，则继续通过第二交易获取用于加密所述数字资产的密钥的步骤。

25 4、根据权利要求3所述的方法，其特征在于，所述赎回脚本是由所述购买方根据所述第一公钥以及所述购买方价值赎回地址的第二公钥生成的，所述第一交易价值存储地址是所述购买方根据所述赎回脚本生成的。

5、根据权利要求4所述的方法，其特征在于，所述方法还包括：

当所述第二摘要与所述第一摘要不相同，则获取预设区块数量；

获取参与计算所述第二交易的区块的数量；

30 当参与计算所述第二交易的区块的数量大于所述预设区块数量时，则根据所述第一交易价值存储地址得到第二公钥；及

当所述购买方提供的购买方价值赎回地址的第二私钥与所述第二公钥验证成功时，将所述第一交易价值存储地址中存储的购买价值转入至所述购买方价值赎回地址中。

6、一种交易处理装置，包括：

广播模块，用于通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；

接收模块，用于接收购买方返回的与所述第一公钥对应的第一交易价值存储地址；

5 计算模块，用于当检测到所述购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址；及

交易模块，用于将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中，并将用于加密所述数字资产的密钥发送至所述购买方。

10 7、根据权利要求6所述的装置，其特征在于，所述广播模块还用于通过第一交易将用于加密所述数字资产的密钥的第一摘要在区块链上进行广播；

所述接收模块还用于接收所述购买方返回的所述第一摘要；

所述计算模块包括：

15 摘要计算单元，用于通过第二交易获取用于加密所述数字资产的密钥，并计算所述密钥的第二摘要；

验证单元，用于当所述第二摘要与所述第一摘要相同时，则通过所述出售方价值赎回地址的第一私钥验证所述第一公钥；及

地址获取单元，用于当验证成功时，则获取到出售方价值赎回地址。

20 8、根据权利要求7所述的装置，其特征在于，所述接收模块还用于接收所述购买方返回的与所述第一公钥对应的赎回脚本；

所述装置还包括：

比较模块，用于通过第二交易根据所述赎回脚本计算得到第二交易价值存储地址；当所述第二交易价值存储地址与所述第一交易价值存储地址一致时，则继续通过第二交易获取用于加密所述数字资产的密钥。

25 9、根据权利要求8所述的装置，其特征在于，所述赎回脚本是由所述购买方根据所述第一公钥以及所述购买方价值赎回地址的第二公钥生成的，所述第一交易价值存储地址是所述购买方根据所述赎回脚本生成的。

10、根据权利要求9所述的装置，其特征在于，所述装置还包括：

30 预设区块数量获取模块，用于当所述第二摘要与所述第一摘要不相同，则获取预设区块数量；

当前区块数量获取模块，用于获取参与计算所述第二交易的区块的数量；

第二公钥获取模块，用于当参与计算所述第二交易的区块的数量大于所述预设区块数量时，则根据所述第一交易价值存储地址得到第二公钥；及

35 赎回模块，用于当所述购买方提供的购买方价值赎回地址的第二私钥与所述第二公钥验证成功时，将所述第一交易价值存储地址中存储的购买价值转入至所述购买方价值赎回

地址中。

11、一种计算机设备，包括存储器及一个或多个处理器，所述存储器中储存有计算机可读指令，所述计算机可读指令被所述一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：通过第一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；接收购买方返回的与所述第一公钥对应的第一交易价值存储地址；当检测到所述购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址；及将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中，并将用于加密所述数字资产的密钥发送至所述购买方。

12、根据权利要求 11 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：通过第一交易将用于加密所述数字资产的密钥的第一摘要在区块链上进行广播；接收所述购买方返回的所述第一摘要；所述处理器执行所述计算机可读指令时所实现的所述通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址，包括：通过第二交易获取用于加密所述数字资产的密钥，并计算所述密钥的第二摘要；当所述第二摘要与所述第一摘要相同时，则通过所述出售方价值赎回地址的第一私钥验证所述第一公钥；及当验证成功时，则获取到出售方价值赎回地址。

13、根据权利要求 12 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：接收所述购买方返回的与所述第一公钥对应的赎回脚本；所述处理器执行所述计算机可读指令时所实现的所述通过第二交易获取用于加密所述数字资产的密钥之前，还包括：通过第二交易根据所述赎回脚本计算得到第二交易价值存储地址；及当所述第二交易价值存储地址与所述第一交易价值存储地址一致时，则继续通过第二交易获取用于加密所述数字资产的密钥的步骤。

14、根据权利要求 13 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时所涉及的所述赎回脚本是由所述购买方根据所述第一公钥以及所述购买方价值赎回地址的第二公钥生成的，所述第一交易价值存储地址是所述购买方根据所述赎回脚本生成的。

15、根据权利要求 14 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：当所述第二摘要与所述第一摘要不不同时，则获取预设区块数量；获取参与计算所述第二交易的区块的数量；当参与计算所述第二交易的区块的数量大于所述预设区块数量时，则根据所述第一交易价值存储地址得到第二公钥；及当所述购买方提供的购买方价值赎回地址的第二私钥与所述第二公钥验证成功时，将所述第一交易价值存储地址中存储的购买价值转入至所述购买方价值赎回地址中。

16、一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：通过第

一交易将加密的数字资产以及出售方价值赎回地址的第一公钥在区块链上进行广播；接收购买方返回的与所述第一公钥对应的第一交易价值存储地址；当检测到所述购买方将购买价值转入至第一交易价值存储地址时，则通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址；及将所述第一交易价值存储地址中存储的购买价值转入至所述出售方价值赎回地址中，并将用于加密所述数字资产的密钥发送至所述购买方。

17、根据权利要求 16 所述的存储介质，其特征在于，所述计算机可读指令被所述处理器执行时还执行以下步骤：通过第一交易将用于加密所述数字资产的密钥的第一摘要在区块链上进行广播；接收所述购买方返回的所述第一摘要；所述计算机可读指令被所述处理器执行时所实现的所述通过第二交易根据所述第一公钥以及所述第一交易价值存储地址计算得到出售方价值赎回地址，包括：通过第二交易获取用于加密所述数字资产的密钥，并计算所述密钥的第二摘要；当所述第二摘要与所述第一摘要相同时，则通过所述出售方价值赎回地址的第一私钥验证所述第一公钥；及当验证成功时，则获取到出售方价值赎回地址。

18、根据权利要求 17 所述的存储介质，其特征在于，所述计算机可读指令被所述处理器执行时还执行以下步骤：接收所述购买方返回的与所述第一公钥对应的赎回脚本；所述计算机可读指令被所述处理器执行时所实现的所述通过第二交易获取用于加密所述数字资产的密钥之前，还包括：通过第二交易根据所述赎回脚本计算得到第二交易价值存储地址；及当所述第二交易价值存储地址与所述第一交易价值存储地址一致时，则继续通过第二交易获取用于加密所述数字资产的密钥的步骤。

19、根据权利要求 18 所述的存储介质，其特征在于，所述计算机可读指令被所述处理器执行时所涉及的所述赎回脚本是由所述购买方根据所述第一公钥以及所述购买方价值赎回地址的第二公钥生成的，所述第一交易价值存储地址是所述购买方根据所述赎回脚本生成的。

20、根据权利要求 19 所述的存储介质，其特征在于，所述计算机可读指令被所述处理器执行时还执行以下步骤：当所述第二摘要与所述第一摘要不不同时，则获取预设区块数量；获取参与计算所述第二交易的区块的数量；当参与计算所述第二交易的区块的数量大于所述预设区块数量时，则根据所述第一交易价值存储地址得到第二公钥；及当所述购买方提供的购买方价值赎回地址的第二私钥与所述第二公钥验证成功时，将所述第一交易价值存储地址中存储的购买价值转入至所述购买方价值赎回地址中。

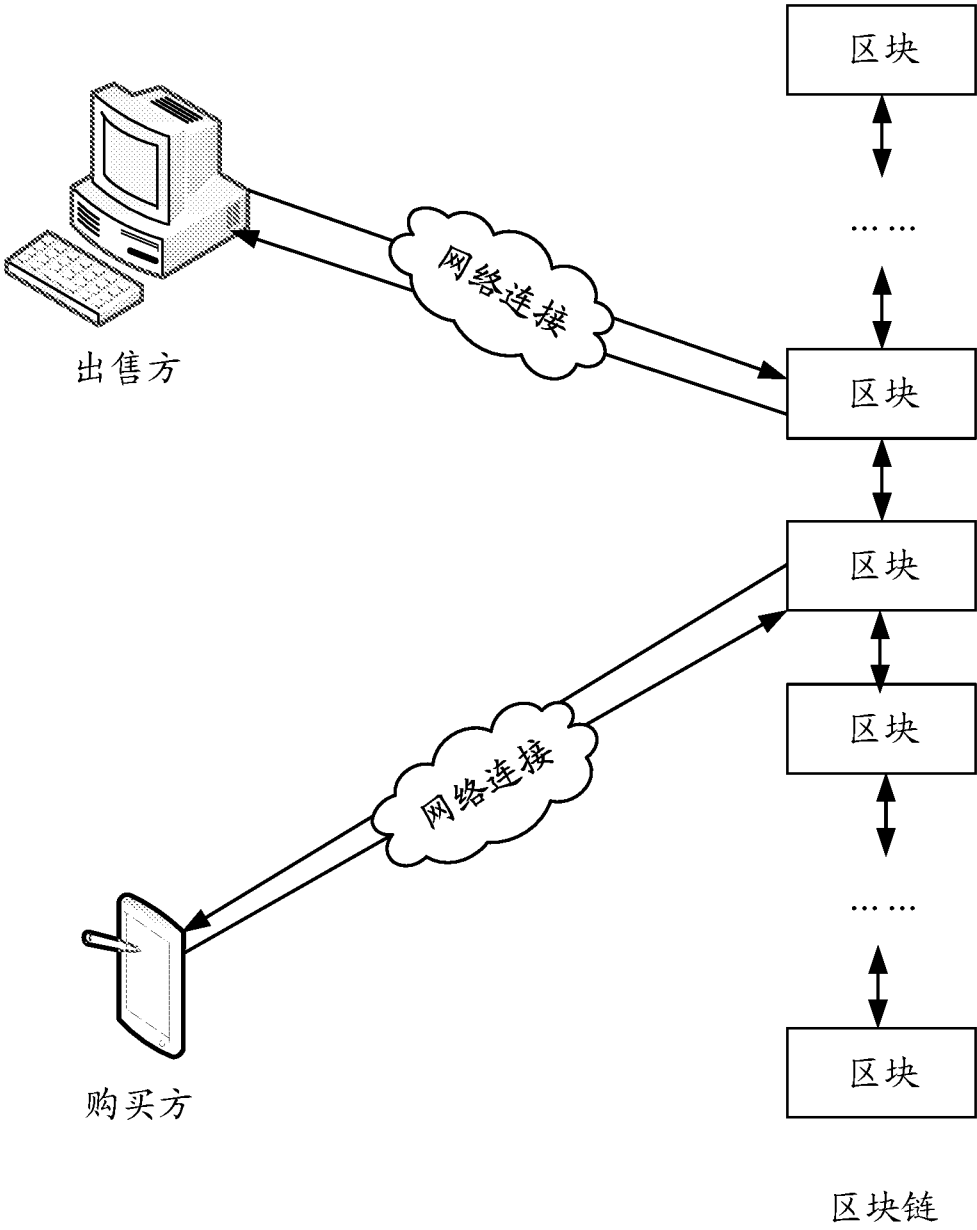


图 1

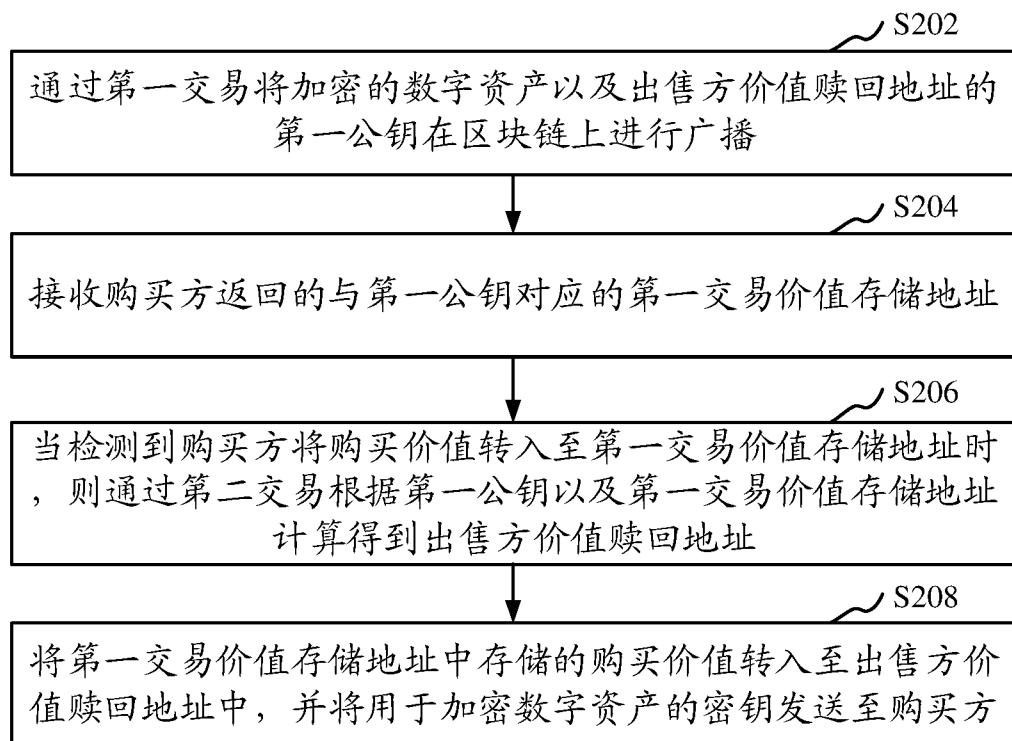


图 2

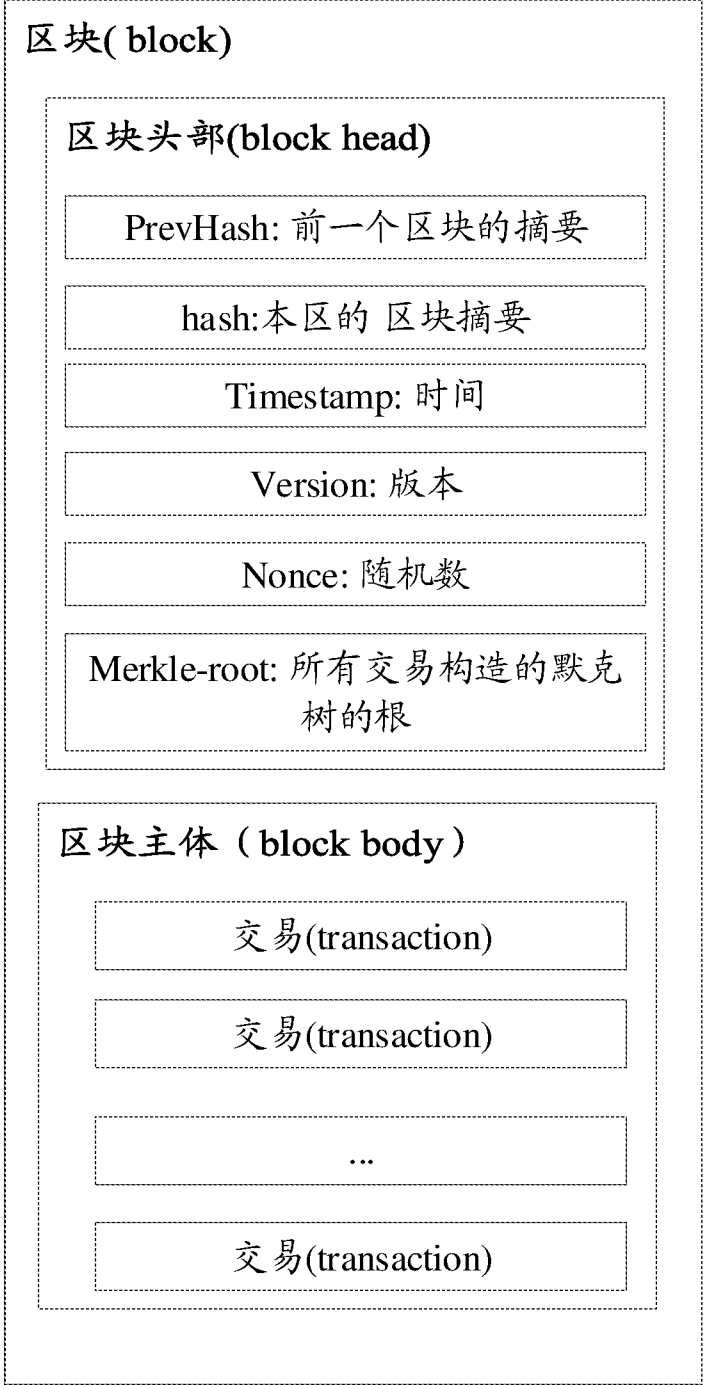


图 3

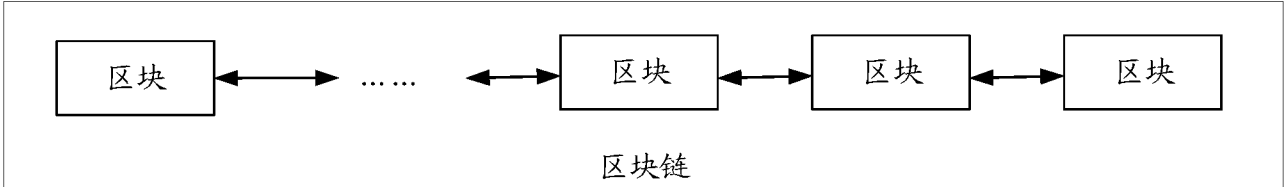


图 4

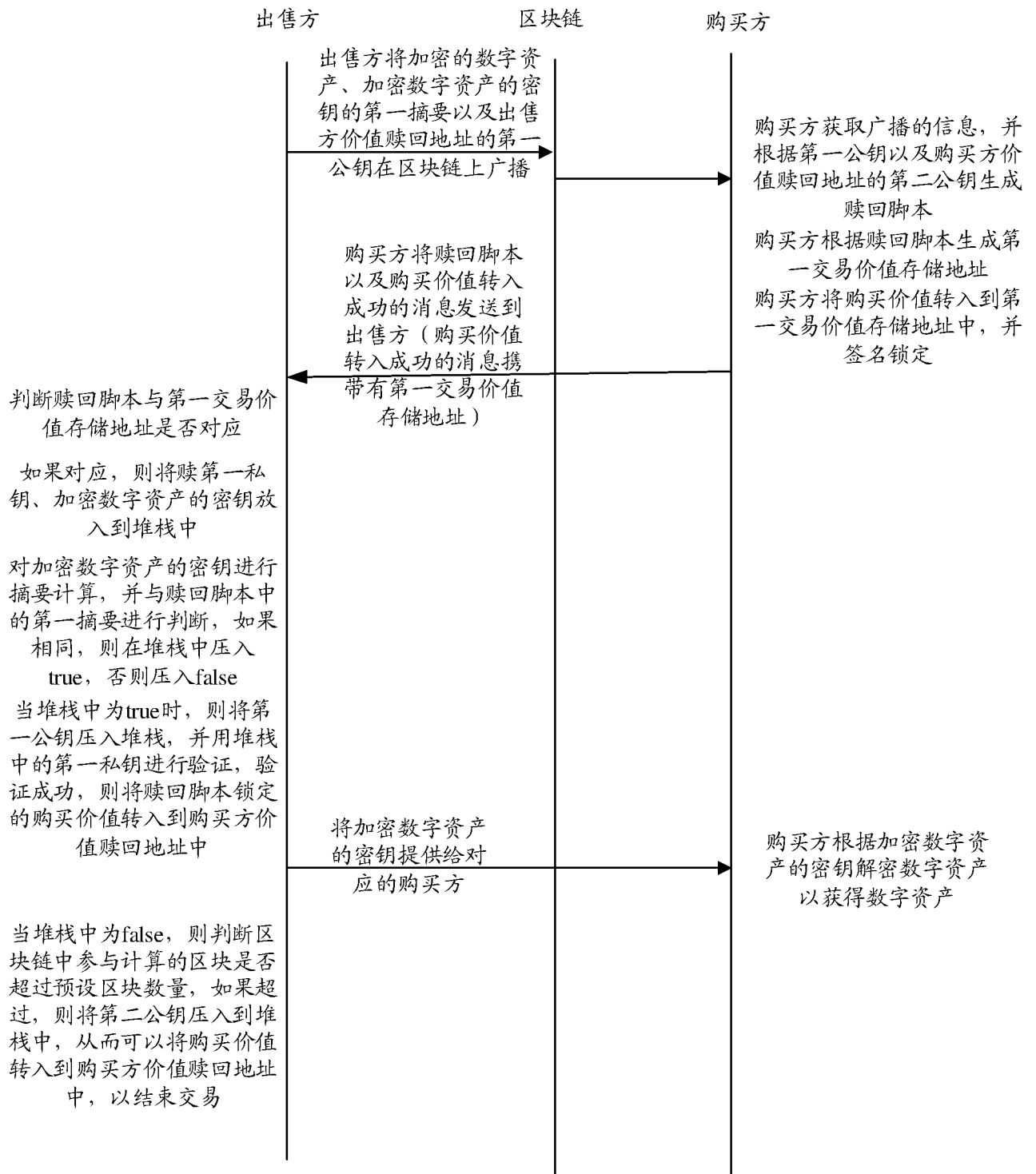


图 5

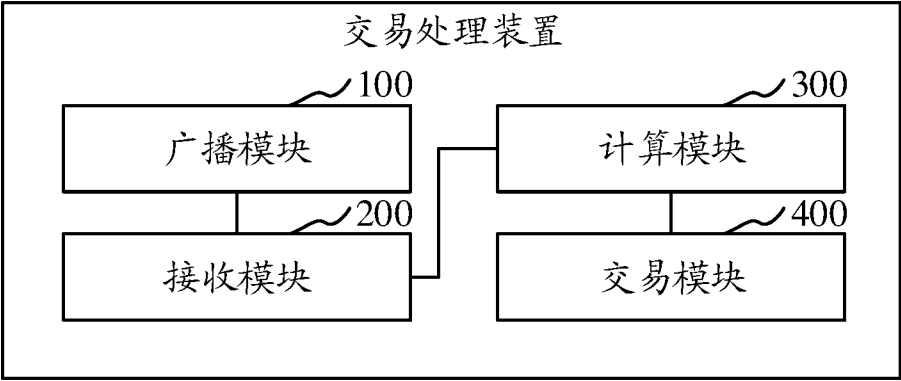


图 6

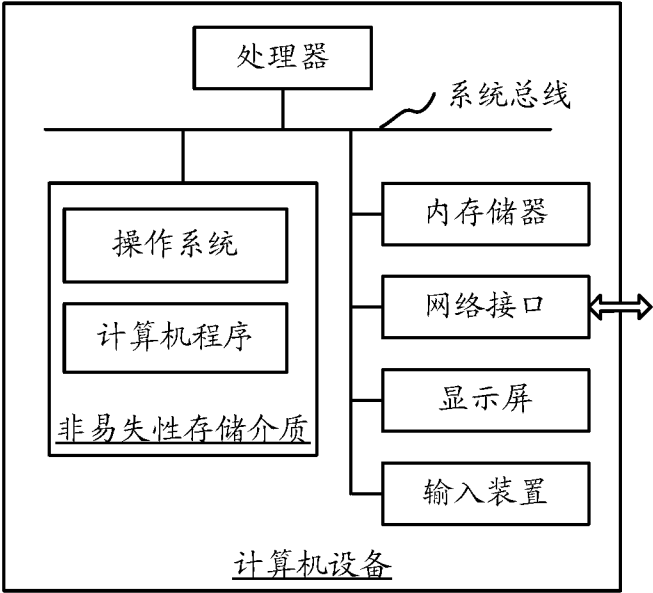


图 7

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/096807

**A. CLASSIFICATION OF SUBJECT MATTER**

G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; VEN; CNTXT; CNKI: 区块链, 交易, 出售, 购买, 地址, block chain, transaction, trade, buy, deal, sell, purchase, address,

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                            | Relevant to claim No. |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| PX        | CN 108305074 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 20 July 2018 (2018-07-20)<br>claims 1-10, and description, paragraphs [0053]-[0118] | 1-20                  |
| A         | CN 107038578 A (ZHEJIANG SHUQIN TECHNOLOGY CO., LTD.) 11 August 2017 (2017-08-11)<br>entire document                                          | 1-20                  |
| A         | CN 107409123 A (T0. COM, INC.) 28 November 2017 (2017-11-28)<br>entire document                                                               | 1-20                  |
| A         | CN 107240001 A (BEIJING HUITONG JINCAI INFORMATION TECHNOLOGY CO., LTD. ET AL.) 10 October 2017 (2017-10-10)<br>entire document               | 1-20                  |
| A         | CN 107622385 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 23 January 2018 (2018-01-23)<br>entire document                           | 1-20                  |
| A         | WO 2016178990 A1 (MONEGRAPH, INC.) 10 November 2016 (2016-11-10)<br>entire document                                                           | 1-20                  |



Further documents are listed in the continuation of Box C.



See patent family annex.

\* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&amp;” document member of the same patent family

Date of the actual completion of the international search

26 October 2018

Date of mailing of the international search report

14 November 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China (ISA/  
CN)  
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing  
100088  
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CN2018/096807**

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                               | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------|-----------------------|
| A         | JP 2017220710 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 14<br>December 2017 (2017-12-14)<br>entire document | 1-20                  |

**INTERNATIONAL SEARCH REPORT**  
**Information on patent family members**

International application No.

**PCT/CN2018/096807**

| Patent document<br>cited in search report |            |    | Publication date<br>(day/month/year) | Patent family member(s) |              |    | Publication date<br>(day/month/year) |
|-------------------------------------------|------------|----|--------------------------------------|-------------------------|--------------|----|--------------------------------------|
| CN                                        | 108305074  | A  | 20 July 2018                         | None                    |              |    |                                      |
| CN                                        | 107038578  | A  | 11 August 2017                       | None                    |              |    |                                      |
| CN                                        | 107409123  | A  | 28 November 2017                     | CA                      | 2975528      | A1 | 01 December 2016                     |
|                                           |            |    |                                      | SG                      | 11201706289W | A  | 28 September 2017                    |
|                                           |            |    |                                      | AU                      | 2016266567   | A1 | 24 August 2017                       |
|                                           |            |    |                                      | JP                      | 2018505633   | A  | 22 February 2018                     |
|                                           |            |    |                                      | WO                      | 2016190922   | A3 | 29 December 2016                     |
|                                           |            |    |                                      | WO                      | 2016190922   | A2 | 01 December 2016                     |
|                                           |            |    |                                      | EP                      | 3257012      | A2 | 20 December 2017                     |
|                                           |            |    |                                      | KR                      | 20170117096  | A  | 20 October 2017                      |
|                                           |            |    |                                      | US                      | 2016234026   | A1 | 11 August 2016                       |
| CN                                        | 107240001  | A  | 10 October 2017                      | None                    |              |    |                                      |
| CN                                        | 107622385  | A  | 23 January 2018                      | None                    |              |    |                                      |
| WO                                        | 2016178990 | A1 | 10 November 2016                     | US                      | 2016321434   | A1 | 03 November 2016                     |
|                                           |            |    |                                      | US                      | 2016321435   | A1 | 03 November 2016                     |
|                                           |            |    |                                      | US                      | 2016321769   | A1 | 03 November 2016                     |
| JP                                        | 2017220710 | A  | 14 December 2017                     | None                    |              |    |                                      |

## 国际检索报告

国际申请号

PCT/CN2018/096807

|                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                       |                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------|
| <b>A. 主题的分类</b><br>G06Q 20/38 (2012.01) i<br><br>按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类                                                                                                                                                                                                                                                                                                              |                                                                                       |                                 |
| <b>B. 检索领域</b><br>检索的最低限度文献 (标明分类系统和分类号)<br>G06Q<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))<br>CPRSABS; VEN; CNTXT; CNKI: 区块链, 交易, 出售, 购买, 地址, block chain, transaction, trade, buy, deal, sell, purchase, address,                                                                                                                                             |                                                                                       |                                 |
| <b>C. 相关文件</b>                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                       |                                 |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                              | 引用文件, 必要时, 指明相关段落                                                                     | 相关的权利要求                         |
| PX                                                                                                                                                                                                                                                                                                                                                                                                | CN 108305074 A (深圳壹账通智能科技有限公司) 2018年 7月 20日 (2018 - 07 - 20)<br>权利要求1-10, 说明书第53-118段 | 1-20                            |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 107038578 A (浙江数秦科技有限公司) 2017年 8月 11日 (2017 - 08 - 11)<br>全文                       | 1-20                            |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 107409123 A (缙零网股份有限公司) 2017年 11月 28日 (2017 - 11 - 28)<br>全文                       | 1-20                            |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 107240001 A (北京汇通金财信息科技有限公司 等) 2017年 10月 10日 (2017 - 10 - 10)<br>全文                | 1-20                            |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 107622385 A (南京邮电大学) 2018年 1月 23日 (2018 - 01 - 23)<br>全文                           | 1-20                            |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | WO 2016178990 A1 (MONEGRAPH INC) 2016年 11月 10日 (2016 - 11 - 10)<br>全文                 | 1-20                            |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | JP 2017220710 A (NIPPON TELEGRAPH & TELEPHONE) 2017年 12月 14日 (2017 - 12 - 14)<br>全文   | 1-20                            |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                              |                                                                                       |                                 |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“P” 公布日先于国际申请日但迟于所要求的优先权日的文件<br>“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件<br>“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性<br>“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性<br>“&” 同族专利的文件 |                                                                                       |                                 |
| 国际检索实际完成的日期                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                       | 国际检索报告邮寄日期                      |
| 2018年 10月 26日                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                       | 2018年 11月 14日                   |
| ISA/CN的名称和邮寄地址                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                       | 受权官员                            |
| 中华人民共和国国家知识产权局 (ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10) 62019451                                                                                                                                                                                                                                                                                                                       |                                                                                       | 徐琳<br><br>电话号码 (86-10) 62089885 |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2018/096807

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 |              |    | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|------|--------------|----|----------------|
| CN          | 108305074  | A  | 2018年 7月 20日   | 无    |              |    |                |
| CN          | 107038578  | A  | 2017年 8月 11日   | 无    |              |    |                |
| CN          | 107409123  | A  | 2017年 11月 28日  | CA   | 2975528      | A1 | 2016年 12月 1日   |
|             |            |    |                | SG   | 11201706289W | A  | 2017年 9月 28日   |
|             |            |    |                | AU   | 2016266567   | A1 | 2017年 8月 24日   |
|             |            |    |                | JP   | 2018505633   | A  | 2018年 2月 22日   |
|             |            |    |                | WO   | 2016190922   | A3 | 2016年 12月 29日  |
|             |            |    |                | WO   | 2016190922   | A2 | 2016年 12月 1日   |
|             |            |    |                | EP   | 3257012      | A2 | 2017年 12月 20日  |
|             |            |    |                | KR   | 20170117096  | A  | 2017年 10月 20日  |
|             |            |    |                | US   | 2016234026   | A1 | 2016年 8月 11日   |
| CN          | 107240001  | A  | 2017年 10月 10日  | 无    |              |    |                |
| CN          | 107622385  | A  | 2018年 1月 23日   | 无    |              |    |                |
| WO          | 2016178990 | A1 | 2016年 11月 10日  | US   | 2016321434   | A1 | 2016年 11月 3日   |
|             |            |    |                | US   | 2016321435   | A1 | 2016年 11月 3日   |
|             |            |    |                | US   | 2016321769   | A1 | 2016年 11月 3日   |
| JP          | 2017220710 | A  | 2017年 12月 14日  | 无    |              |    |                |