

(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
2020 年 5 月 7 日 (07.05.2020)



(10) 国际公布号
WO 2020/087736 A1

(51) 国际专利分类号:
G06Q 20/00 (2012.01)

(21) 国际申请号: PCT/CN2018/124203

(22) 国际申请日: 2018 年 12 月 27 日 (27.12.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811265616.6 2018年10月29日 (29.10.2018) CN

(71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518033 (CN)。

(72) 发明人: 高立志(GAO, Lizhi); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518033 (CN)。

(74) 代理人: 北京市京大律师事务所(BEIJING JINGDA LAW FIRM); 中国北京市海淀区海淀中街 16 号 7 层 2 单元 703, Beijing 100080 (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, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: BLOCKCHAIN-BASED OFFLINE PAYMENT METHOD AND APPARATUS, AND DEVICE AND STORAGE MEDIUM

(54) 发明名称: 一种基于区块链的离线支付方法、装置、设备和存储介质

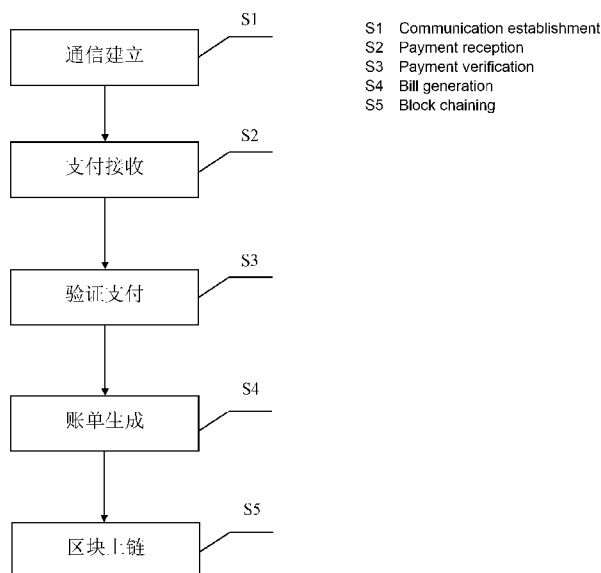


图 1

(57) Abstract: A blockchain-based offline payment method and apparatus, and a device and a storage medium. The method comprises: when offline, establishing a connection for communication; verifying transaction information and completing payment processing; generating billing information; and when online, generating a transaction block from the billing information, payment account information and collection account information. According to the method, a series of processing on transaction information in an offline state can be completed by means of short-distance connection and communication, and the processing mode is simple and convenient;

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))。

moreover, the problem that mobile payment cannot be completed in the offline state is solved, and the method has the characteristics of being efficient, secure and convenient.

(57) 摘要: 一种基于区块链的离线支付方法、装置、设备和存储介质, 所述方法包括: 离线状态时, 建立连接进行通信; 验证交易信息, 完成支付处理; 生成账单信息; 在线状态时, 将账单信息、付款账户信息和收款账户信息生成交易区块。本方法可以通过近距离连接通信, 完成离线状态下交易信息的一系列处理, 处理方式简单、便捷, 同时解决了离线状态无法完成移动支付的问题, 具备高效、安全、便捷的特点。

一种基于区块链的离线支付方法、装置、设备和存储介质

本申请要求于 2018 年 10 月 29 日提交中国专利局、申请号为
5 201811265616.6、发明名称为“一种基于区块链的离线支付方法、装置、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

本申请涉及移动支付领域，特别涉及一种基于区块链的离线支付方法、装
10 置、设备和存储介质。

背景技术

移动支付以便捷、简单的操作方式快速风靡支付市场，不仅打破传统的支付模式，更是给金融业、服务业等各领域带来了翻天覆地的变化。越来越多的
15 单位和个人通过移动终端、互联网等方式直接或间接向银行金融机构发送支付指令产生货币支付与资金转移行为，从而实现了无现金生活、办公的快速便捷，但是由于移动支付必须建立在互联网的基础上完成交易，这就给网络信号受限的地区带来了极大的不便，也降低了支付成功的几率，给用户带来了诸多困扰。

目前市面上绝大多数的移动支付多采用在线支付的方式完成，无法满足无
20 网络状态下的支付交易，而且无网络状态下经常会造成支付失败、重复支付、支付信息无法匹配等情况的发生，给用户造成了诸多不便。

发明内容

基于此，有必要针对无网络状态下经常会造成支付失败、重复支付、支付
25 信息无法匹配等问题，提供一种基于区块链的离线支付方法、装置、设备和存储介质。

一种基于区块链的离线支付方法，包括：

当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

5 所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

10 基于相同的技术构思，本申请还提供了一种基于区块链的离线支付装置，包括：

通信建立模块，设置为当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

15 支付接收模块，设置为所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

验证支付模块，设置为所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

20 账单生成模块，设置为所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

区块上链模块，设置为当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

25 基于相同的构思，本申请还提供一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

5 所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

10 基于相同的构思，本申请还提供一种存储有计算机可读指令的存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

15 所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

20 所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

25 上述一种基于区块链的离线支付方法、装置、设备和存储介质，通过建立离线状态近距离通信，接收支付数据和收款账户信息，完成离线状态下交易账单的处理，同时将账单信息、收款账户信息、付款账户信息上传至区块链系统，完成离线状态下的移动支付。本申请完成了离线状态下移动支付的顺利开展，保障了移动支付在无网络情况的正常进行，简单、便捷、易操作，不仅解决了移动支付的历史难题，更给用户的便捷生活提供了安全保障，避免了支付失败、

重复支付的情况发生。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本申请的限制。

图 1 为本申请一个实施例中一种基于区块链的离线支付方法的流程图；

图 2 为本申请一个实施例中步骤 S3 验证支付的流程图；

图 3 为本申请一个实施例中步骤 S5 区块上链的流程图；

10 图 4 为本申请一个实施例中步骤 S6 广播更新的流程图；

图 5 为本申请一个实施例中一种基于区块链的离线支付装置的示意图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请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仅用以解释本申请，并不用于限定本申请。

本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本申请的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。

图 1 为本申请一种基于区块链的离线支付方法的流程图，如图 1 所示，一种基于区块链的离线支付方法，包括以下步骤：

25 步骤 S1，通信建立：当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信。

本步骤是在收款终端或付款终端存在至少一个处于离线状态的情况下实施的，包括所述收款终端或所述付款终端同时处于离线状态的情况，具体通信连接的方法选用：NFC 近距离无线传输或蓝牙连接。

近距离通信，是一种新兴的技术，使用了 NFC 技术的设备，例如手机、平

板等可以在彼此靠近的情况下进行数据交换，是由非接触式射频识别及互连互通技术整合演变而来，通过在单一芯片上集成感应式读卡器、感应式卡片和点对点通信的功能，利用移动终端实现移动支付、电子票务、门禁、移动身份识别、防伪等应用，可以用于网络断开，终端处于离线状态下数据的传输。

- 5 在具体设计时，例如在乘坐公交或地铁时，手机终端利用 NFC 功能，不管是否处于在线状态，均可以完成移动支付，目前常见的应用终端：Apple Pay、华为支付、小米移动钱包。

10 本实施例通过采用非接触式近距离传输，实现了离线状态下支付的进行，补全了移动支付处于离线状态下的短板，同时简单、易操作，使用方式灵活、高效。

步骤 S2，支付接收：所述付款终端接收所述收款终端发送的支付数据和收款账户信息。

- 15 在具体设计时，假如超市购物使用移动支付，当超市收银员收款时，使用扫描枪扫描顾客移动终端的二维码或条形码后，收款终端就会将支付数据和收款账户信息传送给付款终端。

本实施例采用移动支付，大大提高了收银的效率，降低了交易成本，促进了无现金支付的快速发展，使人们的生活更加便捷，也带动了传统交易方式的转型升级。

- 20 步骤 S3，验证支付：所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端。

在实施本步骤之前需要确保交易信息的合法性，因此所述收款终端和所述付款终端必须为实名认证终端。

- 25 当所述付款终端或所述收款终端初次使用时，通过预设的实名认证界面获取用户上传的实名认证信息，完成实名认证，所述实名认证信息包括但不限于所述用户身份证明、终端名称、所述用户指纹信息、支付账号信息或支付协议中的至少一种。

已实名认证的收款终端和付款终端可进行移动支付，图 2 为本申请一个实施例中步骤 S3 验证支付的流程图，如图 2 所示，步骤 S3 可包括如下具体步骤：

步骤 S301, 支付反馈: 所述付款终端接收所述支付数据和所述收款账户信息并显示在所述付款终端的信息确认界面上;

步骤 S302, 验证处理: 所述付款终端提请用户验证所述支付数据与所述收款账户是否一致, 当接收到所述用户反馈验证一致时, 所述付款终端完成支付
5 处理并反馈支付结果至所述收款终端, 当接收到所述用户反馈验证不一致时, 所述付款终端拒绝支付并将支付失败反馈至所述收款终端。

本步骤在所述付款终端设置显示屏, 用于由用户查看具体所述支付数据和所述收款账户信息, 具体可选用 LED 显示屏、多触点触摸屏、液晶显示屏等。具体能否完成交易需要经用户查看后给出所述付款设备确认信息, 所述付款设
10 备依据确认后反馈的信息进行支付。

在具体设计时, 当超市购物扫描支付时, 支付数据和收款账户信息都会在用户的手机终端显示, 用户在手机终端可查看具体的交易信息, 确认无误后方可完成交易。

本实施例实施过程必须是在终端已经实名认证的情况下进行, 保障了信息的可追溯性, 同时将支付信息显性化, 由用户确认后方可完成交易, 保障了用
15 户的知情权和合法权益, 给移动支付提供了双重安全保障。

步骤 S4, 账单生成: 所述收款终端依据所述支付结果和所述付款账户信息生成账单信息, 并将所述账单信息发送至所述付款终端。

本步骤在已完成支付的基础上将已经完成的交易数据进行整理, 将具体的
20 支付内容、支付数据、付款账户信息和收款账户信息统一为一张账单, 发送至付款终端作为核对和收款凭证。

在具体设计时, 使用移动支付的终端, 比如支付宝、微信、银联支付等客户端均可以看到已完成交易的具体详情, 用户可直接在客户端查看交易记录。

本实施例将具体交易内容做电子化处理, 便于用户随时查看消费信息, 同
25 时若用户固定使用某些支付客户端, 可详细了解个人的使用习惯和交易详情, 便于用户合理安排个人的资金周转。

步骤 S5, 区块上链: 当所述收款终端或所述付款终端任一处于在线状态时, 处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块, 将所述交易区块在区块链系统中上链,

形成新的区块链。

区块链系统是一个分布式的链接账本，每一个账本就是一个区块，区块是很多交易数据的集合，它被标记上时间戳和之前一个区块的独特标记，有效的区块获得全网络的共识认可后会被追加到主区块链中，区块链是有包含交易信息
5 信息的区块从后向前有序链接的数据结构。

图 3 为本申请一个实施例中步骤 S5 区块生成的流程图，如图 3 所示，在一个实施例中，步骤 S5 可包括如下具体步骤：

步骤 S501，数据上传：当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款
10 账户信息、所述收款账户信息上传至区块链系统中的离线支付交易节点。

步骤 S502，哈希值计算：所述离线交易节点依据所述账单信息、所述付款账户信息、所述收款账户信息计算目标哈希值。

哈希值又称“散列”，是把任意长度的输入通过散列算法变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，哈希值简单地理解成是一段数据的 DNA，或者身份证，通过一定的哈希算法，将一段较长的数据映射
15 为较短小的数据，这段小数据就是大数据的哈希值。哈希值是唯一的，一旦大数据发生了变化，哪怕是一个微小的变化，哈希值也会发生变化，保证了没有两个数据的哈希值是完全相同的。正是因为这样的特点，哈希值常常用来区分两个不同的文件，以哈希函数为基础构造的哈希算法，常用于实现数据完整性和
20 和实体认证，同时也构成多种密码体制和协议的安全保障。本步骤通过计算哈希值将离线交易节点区分开，是作为节点区分的标记。

本实施例有效利用哈希值算法将离线交易节点区分，避免了不同区块出现重复的可能性，保证了数据区块的唯一性了，避免了数据的混淆，也保证了数据的安全性。

步骤 S503，区块生成：所述离线支付交易节点引用区块链记录列表中前一
25 区块的哈希值，将所述前一区块的哈希值、时间戳、所述目标哈希值生成区块头，将所述账单信息、所述支付账户信息、所述收款账户信息生成区块体，所述区块头和所述区块体形成交易区块。

区块链系统中每一个数据区块一般包含区块头和区块体两部分，区块头中

封装了前一区块的哈希值、时间戳、随机数、当前区块的目标哈希值等信息，区块体则包含交易详情。区块的数据如果没有上链，百分之百就是伪区块链项目，只有将区块的内容上传至区块链系统，才能实现区块链系统的链接，实现数据资源的共享和使用，也更能发挥区块链系统的信用价值。

5 本实施例采用区块链技术记录交易信息，具备颠覆性的价值，由于区块链技术是参与方之间通过共享共识的方式建立的公共账本，因此区块链中的信息天然就是参与方认可的、唯一的、可溯源、不可篡改的信息源，原来许多重复验证的流程和操纵就可以简化，提升了效率；基于区块链的交易同时与传统交易需要信任交易对手不同，区块链技术可以使用智能合约等方式，保证交易多
10 方自动完成相应义务，确保交易安全，从而降低对手的信用风险；区块链技术可以实现实时的交易结算和清算，减少时间，提高效率。

图 4 为本申请一个实施例中步骤 S6 广播更新的流程图，如图 4 所示，在一个实施例中，步骤 S6 可包括如下具体步骤：

15 步骤 S601，区块广播：所述离线交易节点将已上链的所述交易区块在所述区块链系统中广播。

步骤 S602，列表更新：所述区块链系统中的各节点将所述交易区块的记录信息更新至自身节点的区块链记录列表中。

针对已完成数据存储的区块，将区块之间是实现互联互通，与互联网一样，实现各区块的链接，从而形成大的区块链网络。区块链广播是建立在点与点之间存在互通的基础上的，在区块链系统中，每个节点会记住它最近成功链接的网络节点，当重新启动后它可以迅速地与先前的对等节点重新建立链接，当出现新的链接或失去已有链接时，节点会建立一个或多个新的链接，节点也将一条包含自身 IP 地址消息发送给她相邻节点，相邻节点会再将此消息依次转发给它们各自的相邻节点，从而保证节点信息被多个节点所接收、保证链接更稳定。
20 本步骤中节点就是在交易区块成功链接区块链网络的基础上成功将消息发送至
25 链接的节点，再通过已完成链接的节点传送给其他节点，实现信息的广播。

本实施例将交易信息在区块链系统中进行公开，由于区块链技术可以更好地将所有交易和智能合约进行实时监控，并且以不可撤销、不可抵赖、不可篡改方式留存，方便监管机构实现实时监控和监管，也方便参与方实现自动化合

规处理，从而提升透明度，实现了更高效地实时监管，避免了欺诈行为。

步骤 S5，所述交易区块在所述区块链系统中上链的过程还包括以下两种情况：

5 当所述收款终端在线时，将所述交易区块上链至所述区块链系统中的收款侧链；

当所述付款终端在线时，将所述交易区块上链至所述区块链系统中的付款侧链。

10 从链与链的关系，区块链可以分为主链和侧链，本步骤中依据收款终端和付款终端上链的节点不同，将区块链分为了收款侧链和付款侧链，不同的上传节点上传的侧链也不同。侧链之间设有防火墙，一条侧链上的数据或上传节点的错误造成链上资产的丢失或增加不会影响到另一条链上的资产的丢失或增加，即使在资产的转移过程中发生区块链的重组，也不会出现问题，任何因区块链重组造成的终端，局限在本条侧链上不会影响其他区块链，通常侧链之间能相互独立，用户可以从其他链条提供数据。

15 本实施例将区块链中的数据通过侧链的方式区分开，有效降低因数据错误或节点上传错误导致大面积区块重组的成本，同时可以将数据从不同的侧链之间进行区分备份，防止了数据的和资产的丢失。

20 本申请基于区块链建立离线支付系统，在于能够以非常低的成本解决网络交易的身份识别和个人征信问题，以及使用点对点的交易避免了传统集中式的清算结构，从而能够大大提高金融系统甚至整个经济体系的运行效率，创造性地使用技术地方式为交易双方建立信用，而无需第三方机构参与，从而极大地降低了交易成本，也降低了价值交换地信用成本。

在一个实施例中，提出了一种基于区块链的离线支付装置，如图 5 所示，其包括：

25 通信建立模块，设置为当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

支付接收模块，设置为所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

验证支付模块，设置为所述付款终端依据所述支付数据和所述收款账户信

息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

账单生成模块，设置为所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

- 5 区块生成模块，设置为当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

10 在一个实施例中，所述通信建立模块的所述收款终端与所述付款终端之间采用的连接方式为 NFC 近距离无线传输或蓝牙连接。

在一个实施例中，一种基于区块链的离线支付装置，还包括：

15 实名认证模块，设置为当所述付款终端或所述收款终端初次使用时，通过预设的实名认证界面获取用户上传的实名认证信息，完成实名认证，所述实名认证信息包括但不限于所述用户身份证明、终端名称、所述用户指纹信息、支付账号信息或支付协议中的至少一种。

在一个实施例中，所述验证支付模块，包括：

信息展示单元，设置为所述付款终端接收所述支付数据和所述收款账户信息并显示在所述付款终端的信息确认界面上；

20 账户验证单元，设置为所述付款终端提请用户验证所述支付数据与所述收款账户是否一致，当接收到所述用户反馈验证一致时，所述付款终端完成支付处理并反馈支付结果至所述收款终端，当接收到所述用户反馈验证不一致时，所述付款终端拒绝支付并将支付失败反馈至所述收款终端。

在一个实施例中，所述区块上链模块，包括：

25 信息上传单元，设置为当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息、所述收款账户信息上传至区块链系统中的离线支付交易节点；

哈希值计算单元，设置为所述离线交易节点依据所述账单信息、所述付款账户信息、所述收款账户信息计算目标哈希值；

区块形成单元，设置为所述离线支付交易节点引用区块链记录列表中前一

区块的哈希值，将所述前一区块的哈希值、时间戳、所述目标哈希值生成区块头，将所述账单信息、所述支付账户信息、所述收款账户信息生成区块体，所述区块头和所述区块体形成交易区块。

在一个实施例中，一种基于区块链的离线支付装置，还包括：

- 5 区块广播模块，设置为所述离线交易节点将已上链的所述交易区块在所述区块链系统中广播；

列表更新模块，设置为所述区块链系统中的各节点将所述交易区块的记录信息更新至自身节点的区块链记录列表中。

在一个实施例中，所述区块上链模块，还包括：

- 10 收款侧链上链单元，设置为当所述收款终端在线时，将所述交易区块上链至所述区块链系统中的收款侧链；

付款侧链上链单元，设置为当所述付款终端在线时，将所述交易区块上链至所述区块链系统中的付款侧链。

- 15 在一个实施例中，提出了一种计算机设备，包括存储器和处理器，存储器中存储有计算机可读指令，计算机可读指令被处理器执行时，使得处理器执行计算机可读指令时实现上述各实施例里一种基于区块链的离线支付方法中的步骤。

- 20 在一个实施例中，提出了一种存储有计算机可读指令的存储介质，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上述各实施例里一种基于区块链的离线支付方法中的步骤。

- 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，是可以通过计算机程序来指令相关的硬件来完成，该计算机程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，前述的存储介质可为磁碟、光盘、只读存储记忆体(ReA/D-Only Memory, ROM)等非易失性存储介质，或随机存储记忆体(Random Access Memory, RAM)等。
- 25

以上所述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本申请专利范围的限制。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

5 权利要求为准。

权 利 要 求 书

1. 一种基于区块链的离线支付方法，包括：

当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

5 所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

10 当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

2. 如权利要求 1 所述的一种基于区块链的离线支付方法，其中，所述收款终端与所述付款终端之间采用的连接方式为 NFC 近距离无线传输或蓝牙连接。

3. 如权利要求 1 所述的一种基于区块链的离线支付方法，其中，还包括：

20 当所述付款终端或所述收款终端初次使用时，通过预设的实名认证界面获取用户上传的实名认证信息，完成实名认证，所述实名认证信息包括但不限于所述用户身份证明、终端名称、所述用户指纹信息、支付账号信息或支付协议中的至少一种。

4. 如权利要求 1 所述的一种基于区块链的离线支付方法，其中，所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果反馈至所述收款终端，包括：

所述付款终端接收所述支付数据和所述收款账户信息并显示在所述付款终端的信息确认界面上；

所述付款终端提请用户验证所述支付数据与所述收款账户是否一致，当接收到所述用户反馈验证一致时，所述付款终端完成支付处理并反馈支付结

果至所述收款终端，当接收到所述用户反馈验证不一致时，所述付款终端拒绝支付并将支付失败反馈至所述收款终端。

5 5. 如权利要求 1 所述的一种基于区块链的离线支付方法，其中，当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链，包括：

10 当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息、所述收款账户信息上传至区块链系统中的离线支付交易节点；

所述离线交易节点依据所述账单信息、所述付款账户信息、所述收款账户信息计算目标哈希值；

15 所述离线支付交易节点引用区块链记录列表中前一区块的哈希值，将所述前一区块的哈希值、时间戳、所述目标哈希值生成区块头，将所述账单信息、所述支付账户信息、所述收款账户信息生成区块体，所述区块头和所述区块体形成交易区块。

6. 如权利要求 5 所述的一种基于区块链的离线支付方法，其中，还包括：

所述离线交易节点将已上链的所述交易区块在所述区块链系统中广播；

20 所述区块链系统中的各节点将所述交易区块的记录信息更新至自身节点的区块链记录列表中。

25 7. 如权利要求 5 所述的一种基于区块链的离线支付方法，其中，所述当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链，还包括：

当所述收款终端在线时，将所述交易区块上链至所述区块链系统中的收款侧链；

当所述付款终端在线时，将所述交易区块上链至所述区块链系统中的付款侧链。

8. 一种基于区块链的离线支付装置，包括：

通信建立模块，设置为当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

5 支付接收模块，设置为所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

验证支付模块，设置为所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

10 账单生成模块，设置为所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

区块上链模块，设置为当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

15 9. 根据权利要求 8 所述的一种基于区块链的离线支付装置，其中，所述通信建立模块的所述收款终端与所述付款终端之间采用的连接方式为 NFC 近距离无线传输或蓝牙连接。

10. 根据权利要求 8 所述的一种基于区块链的离线支付装置，其中，还包括：

20 实名认证模块，设置为当所述付款终端或所述收款终端初次使用时，通过预设的实名认证界面获取用户上传的实名认证信息，完成实名认证，所述实名认证信息包括但不限于所述用户身份证明、终端名称、所述用户指纹信息、支付账号信息或支付协议中的至少一种。

25 11. 根据权利要求 8 所述的一种基于区块链的离线支付装置，其中，所述验证支付模块，包括：

支付反馈单元，设置为所述付款终端接收所述支付数据和所述收款账户信息并显示在所述付款终端的信息确认界面上；

验证处理单元，设置为所述付款终端提请用户验证所述支付数据与所述收款账户是否一致，当接收到所述用户反馈验证一致时，所述付款终端完成

支付处理并反馈支付结果至所述收款终端，当接收到所述用户反馈验证不一致时，所述付款终端拒绝支付并将支付失败反馈至所述收款终端。

12. 根据权利要求 8 所述的一种基于区块链的离线支付装置，其中，所述区块上链模块，包括：

5 数据上传单元，设置为当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息、所述收款账户信息上传至区块链系统中的离线支付交易节点；

10 哈希值计算单元，设置为所述离线交易节点依据所述账单信息、所述付款账户信息、所述收款账户信息计算目标哈希值；

 区块生成单元，设置为所述离线支付交易节点引用区块链记录列表中前一区块的哈希值，将所述前一区块的哈希值、时间戳、所述目标哈希值生成区块头，将所述账单信息、所述支付账户信息、所述收款账户信息生成区块体，所述区块头和所述区块体形成交易区块。

15 13. 根据权利要求 12 所述的一种基于区块链的离线支付装置，其中，还包括：

 区块广播模块，设置为所述离线交易节点将已上链的所述交易区块在所述区块链系统中广播；

20 列表更新模块，设置为所述区块链系统中的各节点将所述交易区块的记录信息更新至自身节点的区块链记录列表中。

14. 根据权利要求 12 所述的一种基于区块链的离线支付装置，其中，所述区块上链模块，还包括：

 收款侧链上链单元，设置为当所述收款终端在线时，将所述交易区块上链至所述区块链系统中的收款侧链；

25 付款侧链上链单元，设置为当所述付款终端在线时，将所述交易区块上链至所述区块链系统中的付款侧链。

15. 一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

16. 根据权利要求 15 所述的计算机设备，其中，所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果反馈至所述收款终端，使得所述处理器执行以下步骤：

所述付款终端接收所述支付数据和所述收款账户信息并显示在所述付款终端的信息确认界面上；

所述付款终端提请用户验证所述支付数据与所述收款账户是否一致，当接收到所述用户反馈验证一致时，所述付款终端完成支付处理并反馈支付结果至所述收款终端，当接收到所述用户反馈验证不一致时，所述付款终端拒绝支付并将支付失败反馈至所述收款终端。

17. 根据权利要求 15 所述的计算机设备，其中，当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链，使得所述处理器执行以下步骤：

当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息、所述收

款账户信息上传至区块链系统中的离线支付交易节点；

所述离线交易节点依据所述账单信息、所述付款账户信息、所述收款账户信息计算目标哈希值；

5 所述离线支付交易节点引用区块链记录列表中前一区块的哈希值，将所述前一区块的哈希值、时间戳、所述目标哈希值生成区块头，将所述账单信息、所述支付账户信息、所述收款账户信息生成区块体，所述区块头和所述区块体形成交易区块。

18. 一种存储有计算机可读指令的存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

10 当收款终端或付款终端中至少一个处于离线状态时，所述收款终端与所述付款终端建立连接进行通信；

所述付款终端接收所述收款终端发送的支付数据和收款账户信息；

15 所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果和付款账户信息反馈至所述收款终端；

所述收款终端依据所述支付结果和所述付款账户信息生成账单信息，并将所述账单信息发送至所述付款终端；

20 当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链。

25 19. 根据权利要求 18 所述的存储介质，其中，所述付款终端依据所述支付数据和所述收款账户信息验证交易信息，所述付款终端依据所述交易信息验证结果完成支付处理并将支付结果反馈至所述收款终端，使得一个或多个所述处理器执行以下步骤：

所述付款终端接收所述支付数据和所述收款账户信息并显示在所述付款终端的信息确认界面上；

所述付款终端提请用户验证所述支付数据与所述收款账户是否一致，当接收到所述用户反馈验证一致时，所述付款终端完成支付处理并反馈支付结

果至所述收款终端，当接收到所述用户反馈验证不一致时，所述付款终端拒绝支付并将支付失败反馈至所述收款终端。

5 20. 根据权利要求 18 所述的存储介质，其中，当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息和所述收款账户信息生成交易区块，将所述交易区块在区块链系统中上链，形成新的区块链，使得一个或多个所述处理器执行以下步骤：

10 当所述收款终端或所述付款终端任一处于在线状态时，处于在线状态的所述收款终端或所述付款终端将所述账单信息、所述付款账户信息、所述收款账户信息上传至区块链系统中的离线支付交易节点；

所述离线交易节点依据所述账单信息、所述付款账户信息、所述收款账户信息计算目标哈希值；

15 所述离线支付交易节点引用区块链记录列表中前一区块的哈希值，将所述前一区块的哈希值、时间戳、所述目标哈希值生成区块头，将所述账单信息、所述支付账户信息、所述收款账户信息生成区块体，所述区块头和所述区块体形成交易区块。

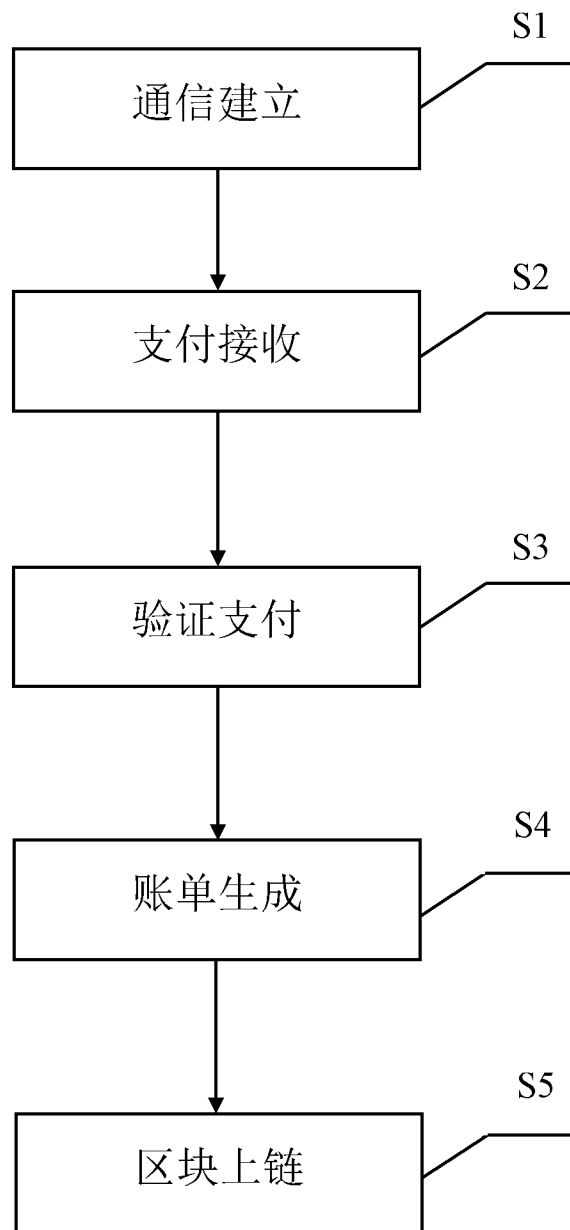


图 1

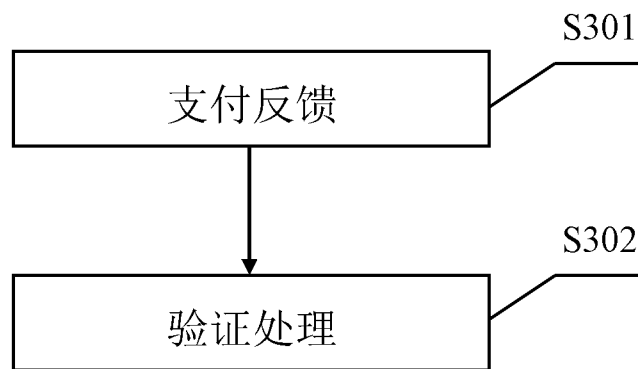


图 2

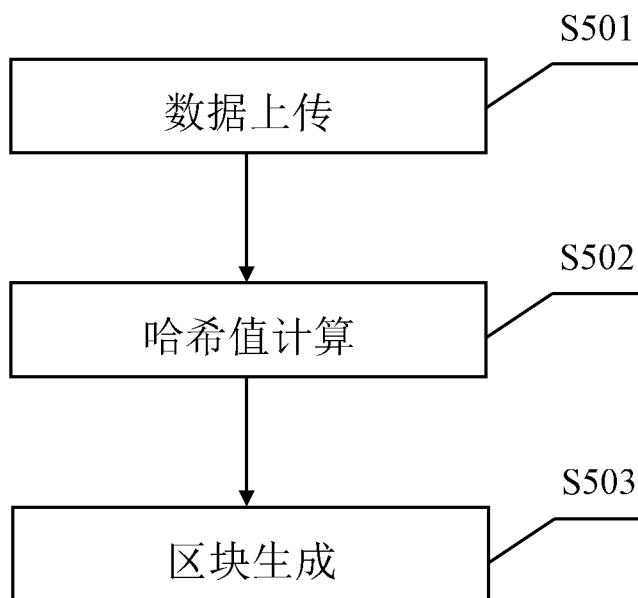


图 3

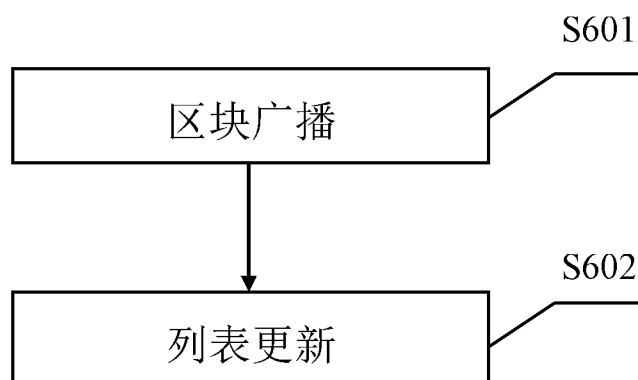


图 4

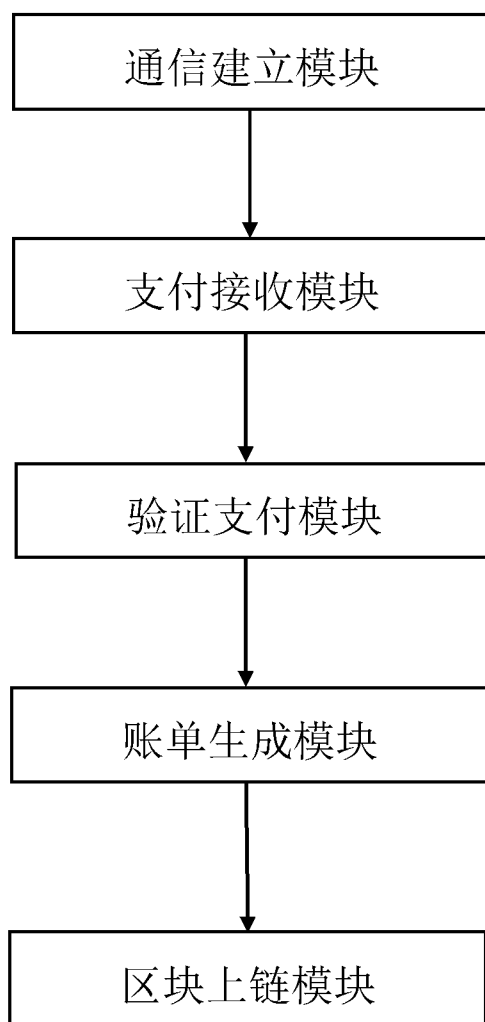


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/124203

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/00(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; G06F

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)

WPI, EPODOC, CNPAT, CNKI: 离线, 在线, 支付, 上链, 交易, 账单, 区块链, 账户, 交易区块, offline, online, block chain, payment

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 107665427 A (ALIBABA GROUP HOLDING LIMITED) 06 February 2018 (2018-02-06) description, paragraphs [0158]-[0214]	1-20
Y	CN 108701296 A (MASTERCARD INTERNATIONAL, INC.) 23 October 2018 (2018-10-23) description, paragraphs [0028]-[0078]	1-20
A	CN 108256867 A (XIDIAN UNIVERSITY) 06 July 2018 (2018-07-06) entire document	1-20
A	CN 106910072 A (GIESECKE & DEVRIENT (CHINA) INFORMATION TECHNOLOGIES CO., LTD.) 30 June 2017 (2017-06-30) entire document	1-20
A	CN 107688938 A (SHANGHAI YUDE TECHNOLOGY CO., LTD.) 13 February 2018 (2018-02-13) 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

“&” document member of the same patent family

Date of the actual completion of the international search

16 July 2019

Date of mailing of the international search report

31 July 2019

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/124203

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107665427	A	06 February 2018	WO	2019037650	A1	28 February 2019
				HK	1248893	A0	19 October 2018
CN	108701296	A	23 October 2018	WO	2017139060	A1	17 August 2017
				EP	3414718	A1	19 December 2018
				US	2017236121	A1	17 August 2017
				IN	201817004152	A	13 April 2018
CN	108256867	A	06 July 2018	None			
CN	106910072	A	30 June 2017	None			
CN	107688938	A	13 February 2018	None			

国际检索报告

国际申请号

PCT/CN2018/124203

A. 主题的分类

G06Q 20/00 (2012.01) i

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. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

G06Q; G06F

包含在检索领域中的除最低限度文献以外的检索文献

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))

WPI, EPDOC, CNPAT, CNKI: 离线, 在线, 支付, 上链, 交易, 账单, 区块链, 账户, 交易区块, offline, online, block chain, payment

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 107665427 A (阿里巴巴集团控股有限公司) 2018年 2月 6日 (2018 - 02 - 06) 说明书第[0158]-[0214]段	1-20
Y	CN 108701296 A (万事达卡国际股份有限公司) 2018年 10月 23日 (2018 - 10 - 23) 说明书第[0028]-[0078]段	1-20
A	CN 108256867 A (西安电子科技大学) 2018年 7月 6日 (2018 - 07 - 06) 全文	1-20
A	CN 106910072 A (捷德中国信息科技有限公司) 2017年 6月 30日 (2017 - 06 - 30) 全文	1-20
A	CN 107688938 A (上海与德科技有限公司) 2018年 2月 13日 (2018 - 02 - 13) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“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)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“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

“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

“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

“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

“&” 同族专利的文件

国际检索实际完成的日期

2019年 7月 16日

国际检索报告邮寄日期

2019年 7月 31日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

丁文勃

电话号码 86-(10)-53961330

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/124203

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107665427	A	2018年 2月 6日	WO	2019037650	A1	2019年 2月 28日
				HK	1248893	A0	2018年 10月 19日
CN	108701296	A	2018年 10月 23日	WO	2017139060	A1	2017年 8月 17日
				EP	3414718	A1	2018年 12月 19日
				US	2017236121	A1	2017年 8月 17日
				IN	201817004152	A	2018年 4月 13日
CN	108256867	A	2018年 7月 6日	无			
CN	106910072	A	2017年 6月 30日	无			
CN	107688938	A	2018年 2月 13日	无			