

(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 9 月 3 日 (03.09.2020)



(10) 国际公布号
WO 2020/173276 A1

(51) 国际专利分类号:
G06Q 20/02 (2012.01) **G06Q 20/08** (2012.01)
G06Q 20/40 (2012.01)

(21) 国际申请号: PCT/CN2020/073753

(22) 国际申请日: 2020 年 1 月 22 日 (22.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910140872.0 2019 年 2 月 26 日 (26.02.2019) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛
大开曼资本大厦一座四层 847 号邮箱,
Grand Cayman (KY)。

(72) 发明人: 孙玉星 (SUN, Yuxing); 中国浙江省杭州市
余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴
集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市
海淀区上地三街 9 号嘉华大厦 B 座 409,
Beijing 100085 (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: RISK PAYMENT PROCESSING METHOD AND APPARATUS, AND DEVICE

(54) 发明名称: 风险支付的处理方法、装置及设备

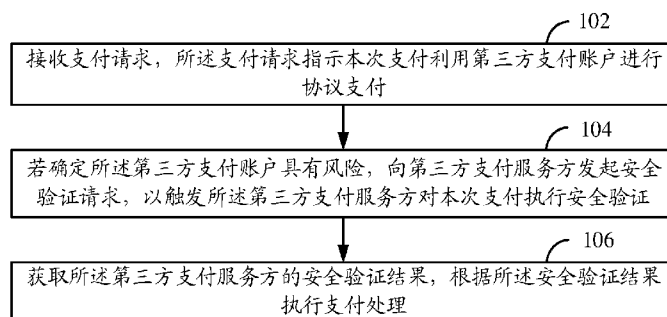


图 1A

102 Receive a payment request, the payment request indicating that protocol payment is performed on this payment by using a third-party payment account
104 If it is determined that the third-party payment account is risky, initiate a security verification request to a third-party payment service party to trigger the third-party payment service party to execute security verification on this payment
106 Obtain a security verification result of the third-party payment service party, and perform payment processing according to the security verification result

(57) Abstract: A risk payment processing method and apparatus, and a device. If a transaction platform side finds out that a third-party payment account is risky, a security verification request can be initiated to a third-party payment service party to trigger the third-party payment service party to execute security verification on this payment. An embezzlement risk can be released in the payment process by introducing an identity verification capability of a third-party payment service side, on one hand, payment security can be ensured, and on the other hand, payment experience of a user can be ensured, and a payment success rate is improved.

(57) 摘要: 一种风险支付的处理方法、装置及设备, 交易平台侧若发现第三方支付账户具有风险, 可以向第三方支付服务方发起安全验证请求, 以触发所述第三方支付服务方对本次支付执行安全验证。通过引入第三方支付服务侧的核身能力, 能够在支付过程中释放盗用风险, 一方面可以保证支付的安全性, 另一方面可以保证用户的支付体验, 提升支付成功率。

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, 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))。

风险支付的处理方法、装置及设备

技术领域

[01] 本说明书涉及互联网技术领域，尤其涉及风险支付的处理方法、装置及设备。

背景技术

- 5 [02] 随着互联网技术的发展，人们越来越多地使用各种基于网络的服务，也越来越多地采用移动支付手段进行支付，例如各种电子钱包。网购等交易平台可以接入各服务方提供的电子钱包，用户可以在需要支付时，可以根据需要选取其中一种电子钱包进行支付。但这种支付处理方式也可能存在一定的风险，在可能存在风险的情况下，如何既保证安全性、又不影响用户的支付体验，成为亟待解决的技术问题。

10 发明内容

[03] 为克服相关技术中存在的问题，本说明书提供了风险支付的处理方法、装置及设备。

[04] 根据本说明书实施例的第一方面，提供一种风险支付的处理方法，包括：

[05] 接收支付请求，所述支付请求指示本次支付利用第三方支付账户进行协议支付；

- 15 [06] 若确定所述第三方支付账户具有风险，向第三方支付服务方发起安全验证请求，以触发所述第三方支付服务方对本次支付执行安全验证；

[07] 获取所述第三方支付服务方的安全验证结果，根据所述安全验证结果执行支付处理。

[08] 可选的，所述方法还包括：

- 20 [09] 若确定所述第三方支付账户未具有风险，执行协议支付流程，完成本次支付处理。

[10] 可选的，所述安全验证请求携带有本次支付的支付信息，以供所述第三方支付服务方在确定所述第三方支付账户未具有风险后、利用所述支付信息触发扣款流程。

[11] 可选的，所述根据所述安全验证结果执行支付处理，包括：

[12] 若安全验证结果指示本次支付未通过安全验证，阻止本次支付。

- 25 [13] 可选的，所述向第三方支付服务方发起安全验证请求，以触发所述第三方支付服

务方对本次支付执行安全验证, 包括:

[14] 调用所述第三方支付服务方提供的安全验证接口, 获取第三方支付服务方的页面链接信息, 根据所述页面链接信息访问所述第三方支付服务方的安全验证页面, 以使所述第三方支付服务方通过所述安全验证页面对本次支付执行安全验证。

5 [15] 可选的, 所述向第三方支付服务方发起安全验证请求, 以触发所述第三方支付服务方对本次支付执行安全验证, 包括:

[16] 触发启动第三方支付应用, 以使所述第三方支付应用跳转至安全验证页面, 通过所述安全验证页面对本次支付执行安全验证。

[17] 根据本说明书实施例的第二方面, 提供一种风险支付的处理方法, 包括:

10 [18] 接收交易平台侧发送的对本次支付的安全验证请求, 所述安全验证请求是交易平台侧在用户利用第三方支付账户进行协议支付后、确定所述第三方支付账户具有风险后发起的;

[19] 对所述本次支付执行安全验证流程;

15 [20] 确定所述安全验证流程执行后的验证结果, 将所述验证结果发送给所述交易平台侧。

[21] 根据本说明书实施例的第三方面, 提供一种风险支付的处理装置, 包括:

[22] 接收模块, 用于: 接收支付请求, 所述支付请求指示本次支付利用第三方支付账户进行协议支付;

20 [23] 安全验证模块, 用于: 若确定所述第三方支付账户具有风险, 向第三方支付服务方发起安全验证请求, 以触发所述第三方支付服务方对本次支付执行安全验证;

[24] 支付处理模块, 用于: 获取所述第三方支付服务方的安全验证结果, 根据所述安全验证结果执行支付处理。

[25] 可选的, 所述支付处理模块, 还用于:

[26] 若确定所述第三方支付账户未具有风险, 执行协议支付流程, 完成本次支付处理。

25 [27] 可选的, 所述安全验证请求携带有本次支付的支付信息, 以供所述第三方支付服务方在确定所述第三方支付账户未具有风险后、利用所述支付信息触发扣款流程。

[28] 可选的, 所述支付处理模块, 还用于:

[29] 若安全验证结果指示本次支付未通过安全验证，阻止本次支付。

[30] 可选的，所述安全验证模块，还用于：

[31] 调用所述第三方支付服务方提供的的安全验证接口，获取第三方支付服务方的页面链接信息，根据所述页面链接信息访问所述第三方支付服务方的安全验证页面，以使所述第三方支付服务方通过所述安全验证页面对本次支付执行安全验证。

[32] 可选的，所述安全验证模块，还用于：

[33] 触发启动第三方支付应用，以使所述第三方支付应用跳转至安全验证页面，通过所述安全验证页面对本次支付执行安全验证。

[34] 根据本说明书实施例的第四方面，提供一种风险支付的处理装置，包括：

10 [35] 接收模块，用于：接收交易平台侧发送的对本次支付的安全验证请求，所述安全验证请求是交易平台侧在用户利用第三方支付账户进行协议支付后、确定所述第三方支付账户具有风险后发起的；

[36] 安全验证模块，用于：对所述执行安全验证流程；

15 [37] 发送模块，用于：确定所述安全验证流程执行后的验证结果，将所述验证结果发送给所述交易平台侧。

[38] 根据本说明书实施例的第五方面，提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现前述风险支付的处理方法的实施例。

[39] 本说明书的实施例提供的技术方案可以包括以下有益效果：

20 [40] 本说明书实施例中，交易平台侧若发现第三方支付账户具有风险，可以向第三方支付服务方发起安全验证请求，以触发所述第三方支付服务方对本次支付执行安全验证；本实施例通过引入第三方支付服务侧的核身能力，能够在支付过程中释放盗用风险，一方面可以保证支付的安全性，另一方面可以保证用户的支付体验，提升支付成功率。

25 [41] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书。

附图说明

[42] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实

施例，并与说明书一起用于解释本说明书的原理。

[43] 图 1A 是本说明书根据一示例性实施例示出的一种风险支付的处理方法的流程图。

[44] 图 1B 是本说明书根据一示例性实施例示出的另一种风险支付的处理方法的流程图。

[45] 图 2A 是本说明书根据一示例性实施例示出的另一种风险支付的处理方法的流程图。

[46] 图 2B 是本说明书根据一示例性实施例示出的应用页面示意图。

[47] 图 3 是本说明书根据一示例性实施例示出的风险支付的处理方法装置所在设备的框图。

[48] 图 4 是本说明书根据一示例性实施例示出的一种风险支付的处理方法装置的框图。

10 [49] 图 5 是本说明书根据一示例性实施例示出的另一种风险支付的处理方法装置的框图。

具体实施方式

[50] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实
15 施例中所描述的实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

[51] 在本说明书使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[52] 应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为
25 “在……时”或“当……时”或“响应于确定”。

[53] 电商支付场景下，电商交易平台通常可以引入其他第三方电子钱包，以丰富用户支付渠道，用户使用电商交易平台的交易服务时，可以选择采用第三方电子钱包进行支

付。为了提升用户体验，一些基于网络服务的交易平台推出了代扣服务（也称为协议支付），用户需要将第三方的电子钱包账户与交易平台的账户进行绑定，并签订代扣协议。当用户购买交易平台的产品或服务时，交易平台会直接向第三方电子钱包发起扣款请求，进行消费记账，而不需要用户输入密码，从而提高用户体验。例如电商公司 Lazada 的交易平台可以接入马来西亚的 TnG 钱包。其中，Lazada 与 TnG 可以采用协议支付的形式，交易平台可以直接向 TnG 钱包发起扣款请求，TnG 钱包无需用户在支付时进行支付密码验证等支付验证操作，可以根据扣款请求直接对用户账户进行扣款操作。

[54] 支付场景中，交易平台通常配置有风险决策系统，以评判本次支付是否存在风险。由于协议支付的场景下未进行支付密码的验证，并且是涉及第三方电子钱包，交易平台若发现第三方电子钱包具有风险，可以是直接拦截支付以保证安全性，但此种方式会影响到用户的支付体验，可能会造成用户流失。交易平台也可以出于支付体验的考虑，令本次支付通过风险决策，但此种方式则引入了一定风险，有可能放过真实的风险支付，给平台或用户带来损失。

[55] 基于此，本说明书实施例提供一种风险支付的处理方法，一方面可以保证支付的安全性，另一方面可以保证用户的支付体验，提升支付成功率。其中，该风险支付的处理方案涉及交易平台侧的处理方法，也涉及在第三方支付产品（即第三方电子钱包）侧的处理方法。

[56] 首先从交易平台侧描述该风险支付的处理方法，如图 1A 所示，是本说明书根据一示例性实施例示出的风险支付的处理方法的流程图，包括如下步骤：

[57] 在步骤 102 中，接收支付请求，所述支付请求指示本次支付利用第三方支付账户进行协议支付；

[58] 在步骤 104 中，若确定所述第三方支付账户具有风险，向第三方支付服务方发起安全验证请求，以触发所述第三方支付服务方对本次支付执行安全验证；

[59] 在步骤 106 中，获取所述第三方支付服务方的安全验证结果，根据所述安全验证结果执行支付处理。

[60] 本实施例中，用户可以在交易平台侧注册有交易账户，通过该交易账户获得交易平台方提供的交易服务；另外，用户在第三方支付服务方侧也注册有账户（本实施例中称为第三方支付账户），通过该账户获得第三方支付服务方通过的支付服务；交易平台方与第三方支付服务方具有合作关系，第三方支付服务方提供的第三方支付钱包可以接

入至交易平台方的交易产品中，用户使用交易平台测的产品、在需要支付时，用户可以选择使用第三方支付产品执行支付操作。其中，本实施例中的第三方支付服务方可以采用协议支付的方式，因此用户在支付时可以无需在第三方支付服务方侧进行如密码或生物特征识别等支付验证。

5 [61] 实际应用中，交易平台方可以通过多种方式接收支付请求，例如，用户可以利用交易平台方提供的客户端获得交易服务，客户端中提供有交易功能及支付功能等，作为例子，客户端可以提供有支付方式的选择入口，在用户支付时，可以供用户选择触发其中一种支付方式；客户端通过获取用户的触发操作，进而确定用户选择了哪种支付方式。通过触发操作可以确定用户选择了预先签订有协议支付的第三方支付方式，客户端可以
10 令支付请求中携带指示本次支付利用第三方支付账户进行协议支付的信息，使得交易平台方接收到支付请求后，可以对本次支付进行风险决策。

[62] 在另一些例子中，交易平台可以提供有页面站点，用户可以通过浏览器登录交易平台提供的服务页面，同样，服务页面提供有交易功能及支付功能等，在用户支付时，可以供用户选择触发其中一种支付方式；通过获取用户的触发操作，进而确定用户选择
15 了哪种支付方式。通过触发操作确定用户选择了预先签订有协议支付的第三方支付方式，服务页面可以令支付请求中携带指示本次支付利用第三方支付账户进行协议支付的信息，使得交易平台方可以对本次支付进行风险决策。实际应用中，支付请求中可能还携带有如交易订单相关信息、交易金额或交易时间等等其他自定义信息，本实施例对此不作限定。

20 [63] 交易平台侧可以配置有风险控制系统，以在用户发起支付时判断本次支付是否具有风险。其中，支付风险可能有多种类型，例如可能是用户在交易平台侧的账户被盗用，此种情况下，交易平台方可以对用户账户执行安全验证。实际应用中，也有可能是用户在第三方支付侧的账户被盗用，此种情况下，本实施例中由第三方支付服务方进行安全验证。

25 [64] 具体的，风险控制系统能识别出的风险类型可能有多种，因为在本实施例的支付场景中，涉及了用户的两个账户：在交易平台侧的交易账户，以及在第三方支付侧的支付账户，风险的存在有可能是用户在交易平台侧的交易账户被盗用，盗用者可能利用该交易账户登录交易平台，并利用该交易账户关联的支付账户进行支付，此种情况下，由于涉及的是本侧的交易账户，交易平台可以对该交易账户执行风控控制及安全验证。然
30 而，风险的存在也有可能是用户在第三方支付侧的支付账户被盗用，面对第三方的支付

账户，交易平台执行风控控制及安全验证的方式较为有限，因此本实施例方案中，交易平台方可以请求第三方支付服务方对该第三方支付账户的本次支付行为进行安全验证。

[65] 其中，本实施例对风险控制系统的风险判定过程并无限定，作为例子，风险控制系统可以结合多种因素确定第三方支付账户是否具有盗用风险，例如，可以根据用户的常用地址、历史支付金额、历史支付频率等历史特征，并结合最近 N 笔支付的地址、金额及频率等判断是否具有盗用风险。

[66] 若确定所述第三方支付账户未具有风险，交易平台侧可以执行协议支付流程，完成本次支付处理。若确定第三方支付账户具有风险的情况下，由于涉及的是其他服务方的账户，为了保证安全，交易平台可以告知第三方支付服务方，通过向第三方支付服务方发起安全验证请求，以触发所述第三方支付服务方对本次支付执行安全验证。

[67] 可选的，交易平台方可以与第三方支付服务方约定有调用接口，在交易平台方发现第三方支付账户具有盗用风险后，交易平台方可以调用该接口，以告知第三方支付服务方，并向第三方支付服务方发起安全验证请求。第三方支付服务方在接收到安全验证请求后执行安全验证流程。

[68] 其中，由于用户是在使用交易平台侧的产品进行交易支付，为了保证用户操作的流畅性、减少操作复杂度，一种可选的方式是用户在当前所使用的交易平台侧的产品中进行安全验证。基于此，本实施例提供了一个可选的实现方式，可以在交易平台侧的产品中直接展示第三方支付服务方的安全验证页面，具体的，交易平台侧可以获取第三方支付服务方的页面链接信息，该页面链接信息可以包括第三方支付服务方的安全验证页面的页面地址或 URL（Uniform Resource Locator，统一资源定位符）。其中，该 URL 地址可以是第三方支付服务方在接口被调用后返回给交易平台侧，也可以是第三方支付服务方预先提供给交易平台侧，根据该信息，可以在交易平台中直接访问所述第三方支付服务方的安全验证页面，以使所述第三方支付服务方通过所述安全验证页面对本次支付执行安全验证。可选的，该安全验证页面可以是符合 HTML5 标准实现的页面，在本实施例中，由于可以在交易平台侧的产品中直接展示第三方支付服务方的安全验证页面，用户可以方便地进行安全验证，该方案可以提升用户体验，提高支付处理的效率。

[69] 在另一些例子中，用户设备中可能同时安装有交易平台提供的应用和第三方支付侧提供的支付应用，也可以是直接跳转至第三方支付应用的安全验证页面，具体的，可以是触发启动第三方支付应用，以使第三方支付应用直接跳转至安全验证页面，通过所述安全验证页面对本次支付执行安全验证。

[70] 其中，第三方支付服务方可以通过多种方式实现安全验证，作为例子，可以通过验证支付密码的方式，在该安全验证页面中可以提供有支付密码输入接口，以供用户输入支付密码完成验证；在另一些例子中，可以采用短信 OTP（One Time Password，一次性密码）验证；或者，还可以采用生物特征识别进行安全验证，例如识别用户的指纹或人脸等方式，本实施例对此不做限定。

[71] 本实施例中，为了提高支付处理效率，交易平台侧在调用接口发起安全验证请求时，安全验证请求可以携带有本次支付的支付信息，该支付信息可以包括用户账户、订单相关信息、支付金额、支付地址等多种信息，以供所述第三方支付服务方在确定所述第三方支付账户未具有风险后、利用该支付信息触发扣款流程。在需要安全验证的情况下，本实施例通过令安全验证请求中携带支付信息，可以使第三方支付服务方在验证成功的情况下及时触发扣款，从而可提到支付处理效率，减少支付处理时间。

[72] 接下来从第三方支付产品侧描述该风险支付的处理方法，如图 1B 所示，是本说明书根据一示例性实施例示出的风险支付的处理方法的流程图，包括如下步骤：

[73] 在步骤 112 中、接收交易平台侧发送的对本次支付的安全验证请求，所述安全验证请求是交易平台侧在用户利用第三方支付账户进行协议支付后、确定所述第三方支付账户具有风险后发起的。

[74] 在步骤 114 中、对所述本次支付执行安全验证流程。

[75] 在步骤 116 中、确定所述支付验证流程执行后的验证结果，将所述验证结果发送给所述交易平台侧。

[76] 本实施例从第三方支付产品侧描述该风险支付的处理过程，与前述实施例相对应，在接收到交易平台侧发起的安全验证请求后，可以对本次支付执行安全验证流程。作为例子，可以通过验证支付密码的方式，在该安全验证页面中可以提供有支付密码输入接口，以供用户输入支付密码完成验证；在另一些例子中，可以采用短信 OTP（One Time Password，一次性密码）验证；或者，还可以采用生物特征识别进行安全验证，例如识别用户的指纹或人脸等方式，本实施例对此不做限定。在确定所述支付验证流程执行后的验证结果后，将所述验证结果发送给所述交易平台侧，以供交易平台侧执行后续的支付处理。

[77] 接下来再通过一实施例对本说明书的风险支付的处理方案进行说明，如图 2A 所示，本实施例方案中涉及电商交易平台 Lazada，以及交易平台侧所配置的支付处理系统

ECPay, 第三方支付侧的产品包括 TnG 钱包。Lazada 可以与 TnG 钱包签订协议支付, 即 Lazada 直接向 TnG 发起扣款请求, TnG 根据扣款请求直接执行扣款操作, 在扣款时无需执行用户输入密码等支付验证操作。这种协议支付未需要由第三方支付侧 TnG 执行支付验证, 本实施例提供了一种在出现风险交易的情况下, 如何保证支付安全的支付处理方案。

[78] 本实施例中, 交易平台 Lazada 使用 ECPay 支付系统处理用户的支付事项, 当用户在交易平台侧交易并发起支付请求后, 由 ECPay 支付系统调用 ECPay 风控系统进行风险决策。若 ECPay 风控系统识别安全时, 则输出协议支付决策, ECPay 支付系统触发协议支付流程, 完成本次支付处理。若 ECPay 风控系统识别出 TnG 账户存在盗用风险后, 输出安全验证决策。

[79] ECPay 支付系统在接收到安全验证决策后, 可以使用跳转支付验证方式请求 TnG 对本次支付进行安全验证。可选的, Lazada 侧可以调用 TnG 侧提供的安全验证接口, 在 Lazada 侧的产品中直接跳转到 TnG 侧的安全验证页面, 如图 2B 所示, 是本说明书根据一示例性实施例示出的安全验证页面的示意图, 在该页面中, 用户可以输入支付密码或短信 OTP, 以供 TnG 钱包进行安全验证; 若安全验证通过, 则 TnG 钱包执行扣款流程, Lazada 订单支付成功。若安全验证通过, 则 TnG 钱包发出验证失败给 Lazada 侧, Lazada 侧的订单支付失败。

[80] 本实施例中, 在电商场景下使用 TnG 钱包支付时, 传统方案在支持协议支付的情况下, ECPay 系统在发现第三方支付账户具有盗用风险后, 通常是拦截交易或者放过交易。在引入本实施例的跳转支付验证的决策后, 可以利用 TnG 的核身能力, 释放 TnG 盗用风险。对于 Lazada 订单支付成功率, 以及用户支付体验, 均有大幅提升。电商场景下通常接入有多种第三方支付产品, 本实施例方案利用第三方支付服务方的核身能力, 能够释放盗用风险。在风险可控的情况下, 可提升用户支付体验, 提升支付成功率。

[81] 与前述风险支付的处理方法的实施例相对应, 本说明书还提供了风险支付的处理装置及其所应用的终端的实施例。

[82] 本说明书风险支付的处理装置的实施例可以应用在计算机设备上, 例如服务器或终端设备。装置实施例可以通过软件实现, 也可以通过硬件或者软硬件结合的方式实现。以软件实现为例, 作为一个逻辑意义上的装置, 是通过其所在文件处理的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言, 如图 3 所示, 为本说明书风险支付的处理装置所在计算机设备的一种硬件结构图, 除了图 3

所示的处理器 310、内存 330、网络接口 320、以及非易失性存储器 340 之外，实施例中装置 331 所在的服务器或电子设备，通常根据该计算机设备的实际功能，还可以包括其他硬件，对此不再赘述。

[83] 如图 4 所示，图 4 是本说明书根据一示例性实施例示出的一种风险支付的处理装置 5 的框图，所述装置包括：

[84] 接收模块 41，用于：接收支付请求，所述支付请求指示本次支付利用第三方支付账户进行协议支付；

[85] 安全验证模块 42，用于：若确定所述第三方支付账户具有风险，向第三方支付服务方发起安全验证请求，以触发所述第三方支付服务方对本次支付执行安全验证；

10 [86] 支付处理模块 43，用于：获取所述第三方支付服务方的安全验证结果，根据所述安全验证结果执行支付处理。

[87] 可选的，所述支付处理模块，还用于：

[88] 若确定所述第三方支付账户未具有风险，执行协议支付流程，完成本次支付处理。

15 [89] 可选的，所述安全验证请求携带有本次支付的支付信息，以供所述第三方支付服务方在确定所述第三方支付账户未具有风险后、利用所述支付信息触发扣款流程。

[90] 可选的，所述支付处理模块，还用于：

[91] 若安全验证结果指示本次支付未通过安全验证，阻止本次支付。

[92] 可选的，所述安全验证模块，还用于：

20 [93] 调用所述第三方支付服务方提供的安全验证接口，获取第三方支付服务方的页面链接信息，根据所述页面链接信息访问所述第三方支付服务方的安全验证页面，以使所述第三方支付服务方通过所述安全验证页面对本次支付执行安全验证。

[94] 可选的，所述安全验证模块，还用于：

[95] 触发启动第三方支付应用，以使所述第三方支付应用跳转至安全验证页面，通过所述安全验证页面对本次支付执行安全验证。

25 [96] 如图 5 所示，图 5 是本说明书根据一示例性实施例示出的一种风险支付的处理装置的框图，所述装置包括：

[97] 接收模块 51，用于：接收交易平台侧发送的对本次支付的安全验证请求，所述安

全验证请求是交易平台侧在用户利用第三方支付账户进行协议支付后、确定所述第三方支付账户具有风险后发起的；

[98] 安全验证模块 52，用于：执行安全验证流程；

[99] 发送模块 53，用于：确定所述安全验证流程执行后的验证结果，将所述验证结果
5 发送给所述交易平台侧。

[100] 相应的，本说明书还提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现风险支付的
10 处理方法的实施例。

[101] 上述风险支付的处理装置中各个模块的功能和作用的实现过程具体详见上述风险
10 支付的处理方法中对应步骤的实现过程，在此不再赘述。

[102] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实
15 施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部
件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也
可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根
据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技
术人员在不付出创造性劳动的情况下，即可以理解并实施。

[103] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。
20 在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执
行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺
序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是
可以的或者可能是有利的。

[104] 本领域技术人员在考虑说明书及实践这里申请的发明后，将容易想到本说明书的
25 其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变
型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未申请的本技术领
域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正
范围和精神由下面的权利要求指出。

[105] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，
并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来
限制。

[106] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

权利要求书

1、一种风险支付的处理方法，包括：

接收支付请求，所述支付请求指示本次支付利用第三方支付账户进行协议支付；

若确定所述第三方支付账户具有风险，向第三方支付服务方发起安全验证请求，以

5 触发所述第三方支付服务方对本次支付执行安全验证；

获取所述第三方支付服务方的安全验证结果，根据所述安全验证结果执行支付处理。

2、根据权利要求1所述的方法，所述方法还包括：

若确定所述第三方支付账户未具有风险，执行协议支付流程，完成本次支付处理。

3、根据权利要求1所述的方法，所述安全验证请求携带有本次支付的支付信息，

10 以供所述第三方支付服务方在确定所述第三方支付账户未具有风险后、利用所述支付信息触发扣款流程。

4、根据权利要求1所述的方法，所述根据所述安全验证结果执行支付处理，包括：

若安全验证结果指示本次支付未通过安全验证，阻止本次支付。

5、根据权利要求1所述的方法，所述向第三方支付服务方发起安全验证请求，以

15 触发所述第三方支付服务方对本次支付执行安全验证，包括：

调用所述第三方支付服务方提供的安全验证接口，获取第三方支付服务方的页面链接信息，根据所述页面链接信息访问所述第三方支付服务方的安全验证页面，以使所述第三方支付服务方通过所述安全验证页面对本次支付执行安全验证。

6、根据权利要求1所述的方法，所述向第三方支付服务方发起安全验证请求，以

20 触发所述第三方支付服务方对本次支付执行安全验证，包括：

触发启动第三方支付应用，以使所述第三方支付应用跳转至安全验证页面，通过所述安全验证页面对本次支付执行安全验证。

7、一种风险支付的处理方法，包括：

接收交易平台侧发送的对本次支付的安全验证请求，所述安全验证请求是交易平台

25 侧在用户利用第三方支付账户进行协议支付后、确定所述第三方支付账户具有风险后发起的；

对所述本次支付执行安全验证流程；

确定所述安全验证流程执行后的验证结果，将所述验证结果发送给所述交易平台侧。

8、一种风险支付的处理装置，包括：

30 接收模块，用于：接收支付请求，所述支付请求指示本次支付利用第三方支付账户进行协议支付；

安全验证模块，用于：若确定所述第三方支付账户具有风险，向第三方支付服务方发起安全验证请求，以触发所述第三方支付服务方对本次支付执行安全验证；

支付处理模块，用于：获取所述第三方支付服务方的安全验证结果，根据所述安全验证结果执行支付处理。

5 9、一种风险支付的处理装置，包括：

接收模块，用于：接收交易平台侧发送的对本次支付的安全验证请求，所述安全验证请求是交易平台侧在用户利用第三方支付账户进行协议支付后、确定所述第三方支付账户具有风险后发起的；

安全验证模块，用于：对所述本次支付执行安全验证流程；

10 发送模块，用于：确定所述安全验证流程执行后的验证结果，将所述验证结果发送给所述交易平台侧。

10、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现权利要求1至7任一所述的方法。

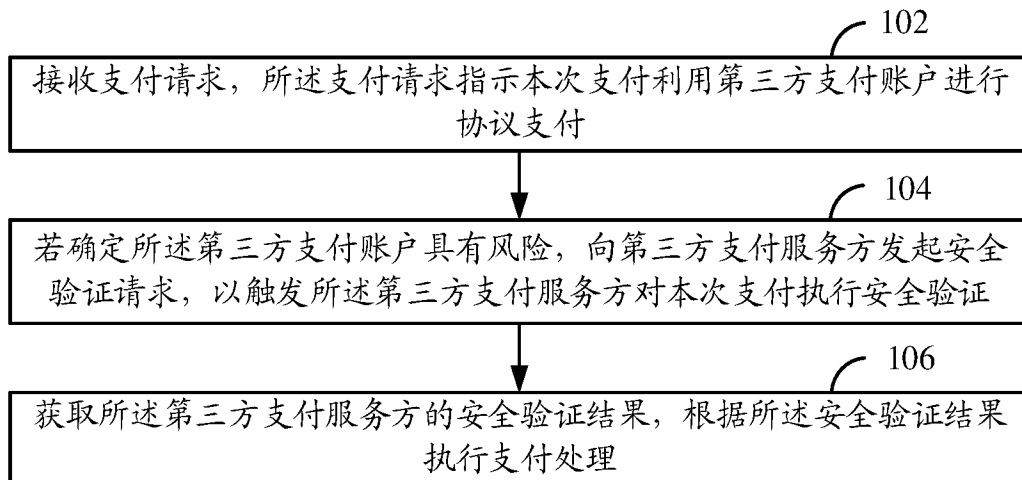


图 1A

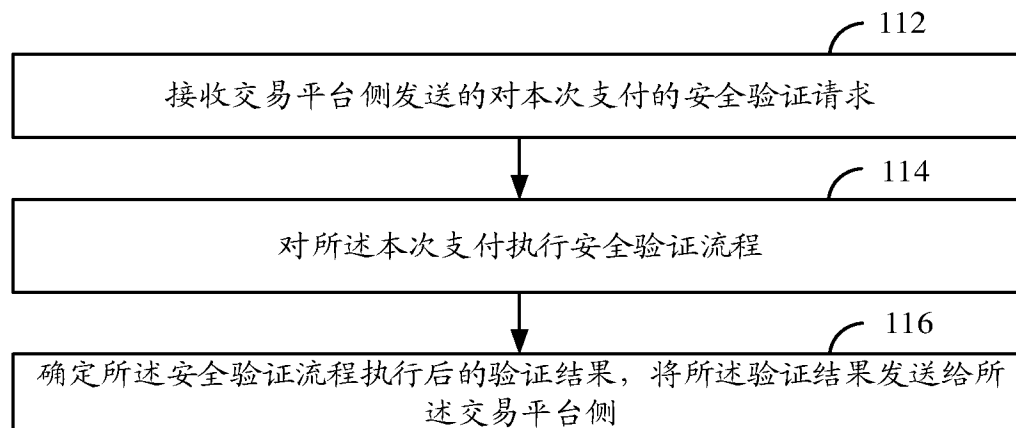


图 1B

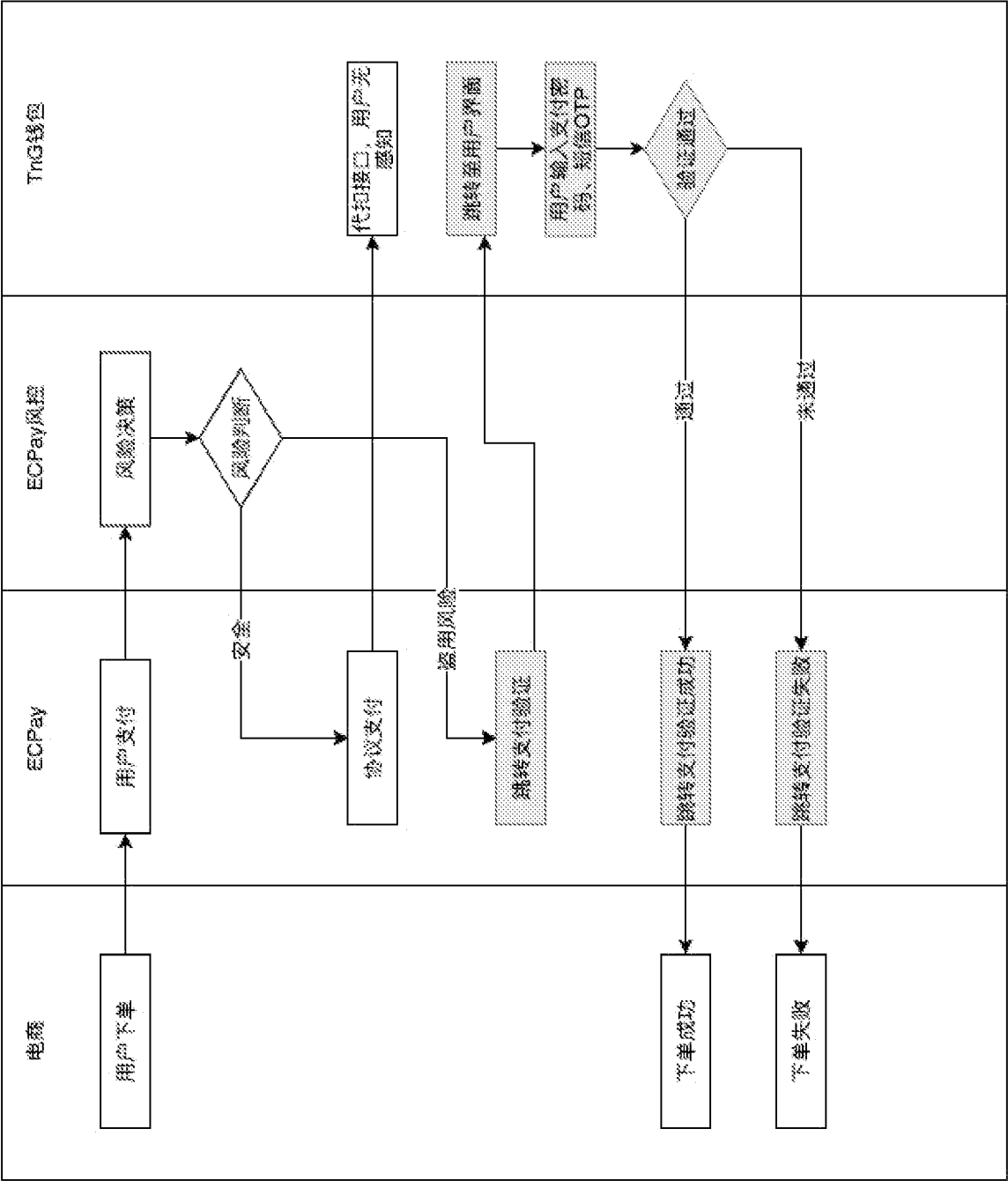


图 2A

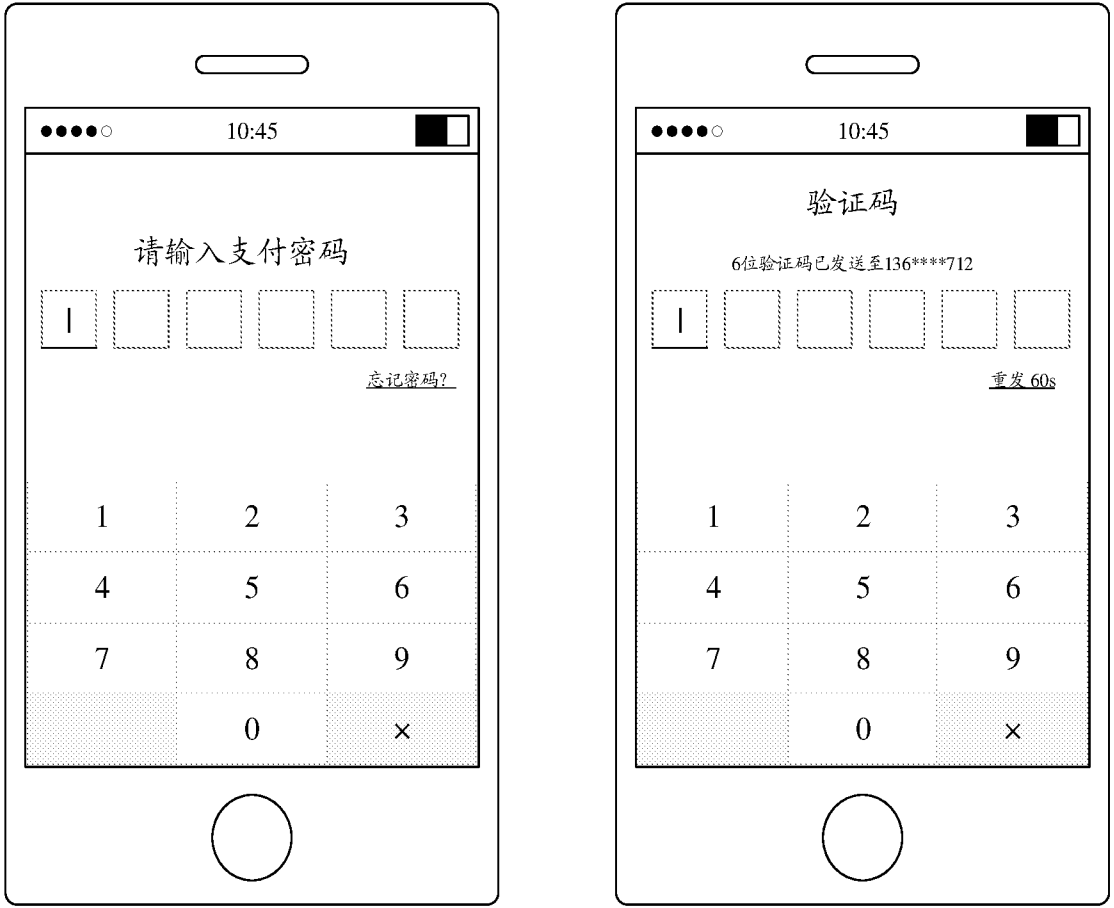


图 2B

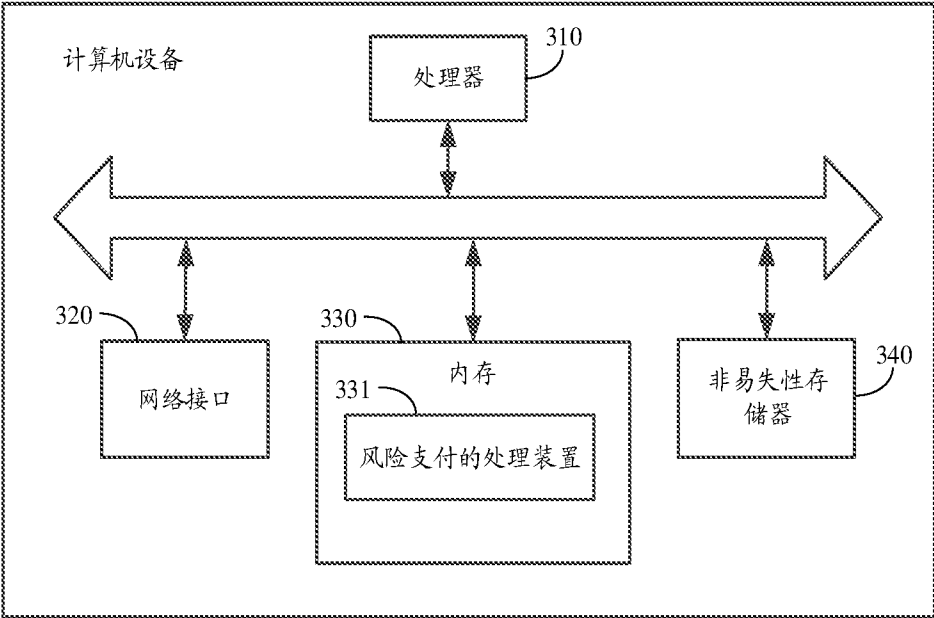


图 3

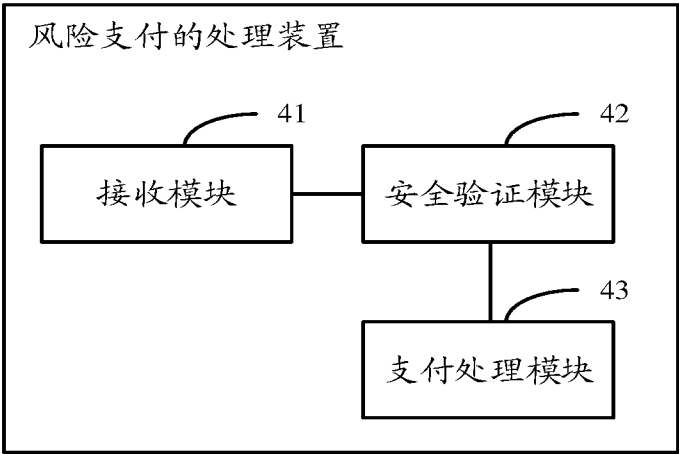


图 4

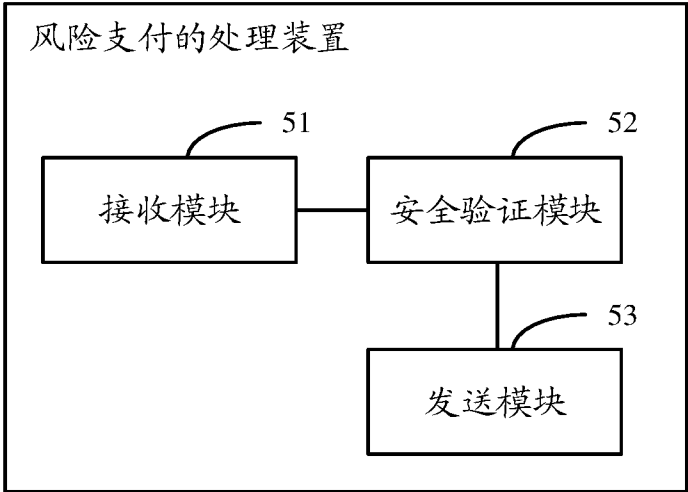


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/073753

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/02(2012.01)i; G06Q 20/40(2012.01)i; G06Q 20/08(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)

CNPAT, CNKI, WPI, EPODOC: 风险, 第三方, 支付, 协议, 安全, 验证, risk, third party, pay, agreement, protocol, safety, security, validate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110060035 A (ALIBABA GROUP HOLDING LIMITED) 26 July 2019 (2019-07-26) description, paragraphs 4-38	1-10
Y	CN 103489095 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 01 January 2014 (2014-01-01) description, paragraphs 34-38, 48-51, 53-60	1-10
Y	CN 107808289 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 16 March 2018 (2018-03-16) description, paragraphs 16-19, 60-70, 73-74, 81-99	1-10
A	CN 103530764 A (BEIJING BAIDU NETCOM SCIENCE AND TECHNOLOGY CO., LTD.) 22 January 2014 (2014-01-22) entire document	1-10
A	CN 108038686 A (ALIBABA GROUP HOLDING LIMITED) 15 May 2018 (2018-05-15) entire document	1-10
A	CN 106934606 A (ALIBABA GROUP HOLDING LIMITED) 07 July 2017 (2017-07-07) entire document	1-10



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

10 April 2020

Date of mailing of the international search report

21 April 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
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/CN2020/073753

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	110060035	A	26 July 2019	None		
CN	103489095	A	01 January 2014	JP	2016523417 A	08 August 2016
				EP	3057049 A1	17 August 2016
				WO	2015051727 A1	16 April 2015
				US	2016117681 A1	28 April 2016
CN	107808289	A	16 March 2018	None		
CN	103530764	A	22 January 2014	None		
CN	108038686	A	15 May 2018	HK1254020	A0	12 July 2019
CN	106934606	A	07 July 2017	HK1238763	A0	04 May 2018

国际检索报告

国际申请号

PCT/CN2020/073753

A. 主题的分类

G06Q 20/02(2012.01)i; G06Q 20/40(2012.01)i; G06Q 20/08(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

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))

CNPAT, CNKI, WPI, EPDOC: 风险, 第三方, 支付, 协议, 安全, 验证, risk, third party, pay, agreement, protocol, safety, security, validate

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
PX	CN 110060035 A (阿里巴巴集团控股有限公司) 2019年 7月 26日 (2019 - 07 - 26) 说明书第4-38段	1-10
Y	CN 103489095 A (百度在线网络技术北京有限公司) 2014年 1月 1日 (2014 - 01 - 01) 说明书第34-38, 48-51, 53-60段	1-10
Y	CN 107808289 A (腾讯科技深圳有限公司) 2018年 3月 16日 (2018 - 03 - 16) 说明书第16-19, 60-70, 73-74, 81-99段	1-10
A	CN 103530764 A (百度在线网络技术北京有限公司) 2014年 1月 22日 (2014 - 01 - 22) 全文	1-10
A	CN 108038686 A (阿里巴巴集团控股有限公司) 2018年 5月 15日 (2018 - 05 - 15) 全文	1-10
A	CN 106934606 A (阿里巴巴集团控股有限公司) 2017年 7月 7日 (2017 - 07 - 07) 全文	1-10

☐ 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

2020年 4月 10日

国际检索报告邮寄日期

2020年 4月 21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

授权官员

杨春雨

电话号码 86-(10)-53961437

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/073753

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	110060035	A	2019年 7月 26日	无			
CN	103489095	A	2014年 1月 1日	JP	2016523417	A	2016年 8月 8日
				EP	3057049	A1	2016年 8月 17日
				WO	2015051727	A1	2015年 4月 16日
				US	2016117681	A1	2016年 4月 28日
CN	107808289	A	2018年 3月 16日	无			
CN	103530764	A	2014年 1月 22日	无			
CN	108038686	A	2018年 5月 15日	HK1254020	A0		2019年 7月 12日
CN	106934606	A	2017年 7月 7日	HK1238763	A0		2018年 5月 4日