

(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
2021 年 11 月 4 日 (04.11.2021)



(10) 国际公布号
WO 2021/219086 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) **H04L 9/32** (2006.01)
- (21) 国际申请号: PCT/CN2021/091038
- (22) 国际申请日: 2021 年 4 月 29 日 (29.04.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202010353842.0 2020 年 4 月 29 日 (29.04.2020) CN
- (71) 申请人: 青岛海尔滚筒洗衣机有限公司(QINGDAO HAIER DRUM WASHING MACHINE CO., LTD.) [CN/CN]; 中国山东省青岛市崂山区高科技工业园海尔路 1 号, Shandong 266101 (CN)。杭州甘道智能科技有限公司(HANGZHOU GANDAO INTELLIGENT

TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市滨江区丹凤路 399 号 2 号楼 A 楼 1703 室, Zhejiang 310051 (CN)。海尔智家股份有限公司(HAIER SMART HOME CO., LTD.) [CN/CN]; 中国山东省青岛市崂山区海尔路 1 号, Shandong 266101 (CN)。

(72) 发明人: 辛耀东(XIN, Yaodong); 中国山东省青岛市崂山区高科技工业园海尔路 1 号, Shandong 266101 (CN)。张纯锋(ZHANG, Chunfeng); 中国山东省青岛市崂山区高科技工业园海尔路 1 号, Shandong 266101 (CN)。王正涛(WANG, Zhengtao); 中国山东省青岛市崂山区高科技工业园海尔路 1 号, Shandong 266101 (CN)。宋军(SONG, Jun); 中国山东省青岛市崂山区高科技工业园海尔路 1 号, Shandong 266101 (CN)。马百义(MA, Baiyi); 中国山东省青岛市崂山

(54) Title: DATA TRANSMISSION METHOD AND SYSTEM BASED ON BLOCKCHAIN

(54) 发明名称: 基于区块链的数据传输方法和系统

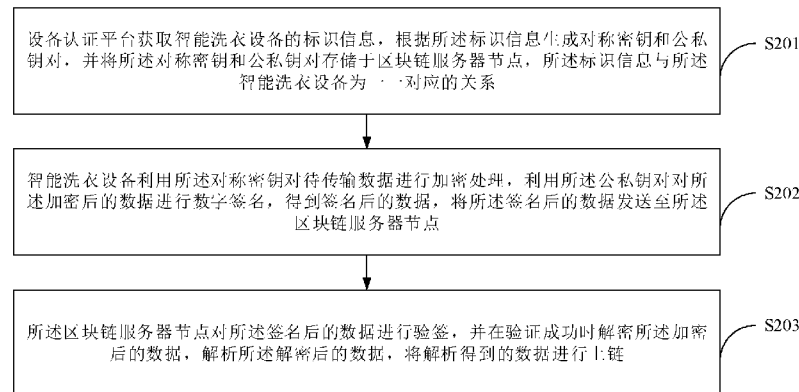


图2

- S201 A device authentication platform obtains identifier information of an intelligent laundry device, generates a symmetric key and a public and private key pair according to the identifier information, and stores the symmetric key and the public and private key pair in a blockchain server node, wherein the identifier information and the intelligent laundry device are in one-to-one correspondence
- S202 The intelligent laundry device performs, by using the symmetric key, encryption processing on data to be transmitted, performs digital signature on the encrypted data by using the public and private key pair to obtain signed data, and sends the signed data to the blockchain server node
- S203 The blockchain server node performs signature verification on the signed data, decrypts the encrypted data if the verification is successful, analyzes the decrypted data, and stores the analyzed data on a blockchain

(57) Abstract: Embodiments of the present invention provide a data transmission method and system based on a blockchain. The method comprises: a device authentication platform obtains identifier information of an intelligent laundry device, generates a symmetric key and a public and private key pair according to the identifier information, and stores the symmetric key and the public and private key pair in a blockchain server node, wherein the identifier information and the intelligent laundry device are in one-to-one correspondence; the intelligent laundry device performs, by using the symmetric key, encryption processing on data to be transmitted, performs digital

区高科技工业园海尔路1号, Shandong 266101 (CN)。张勇杰(ZHANG, Yongjie); 中国浙江省杭州市滨江区丹凤路399号2号楼A楼1703室, Zhejiang 310051 (CN)。宋学武(SONG, Xuewu); 中国山东省青岛市崂山区高科技工业园海尔路1号, Shandong 266101 (CN)。

(74) 代理人: 北京同立钧成知识产权代理有限公司(LEADER PATENT & TRADEMARK FIRM); 中国北京市海淀区西直门北大街32号枫蓝国际A座8F-6, Beijing 100082 (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, IT, 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, 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))。

signature on the encrypted data by using the public and private key pair to obtain signed data, and sends the signed data to the blockchain server node; and the blockchain server node performs signature verification on the signed data, decrypts the encrypted data if the verification is successful, analyzes the decrypted data, and stores the analyzed data on the blockchain. According to the embodiments of the present invention, the data transmission process is more safe and reliable, and the confidentiality and authenticity of the data are improved.

(57) 摘要: 本发明实施例提供一种基于区块链的数据传输方法和系统, 该方法包括: 设备认证平台获取智能洗衣设备的标识信息, 根据标识信息生成对称密钥和公私钥对, 并将对称密钥和公私钥对存储于区块链服务器节点, 标识信息与智能洗衣设备为一一对应的关系; 智能洗衣设备利用对称密钥对待传输数据进行加密处理, 利用公私钥对对所述加密后的数据进行数字签名得到签名后的数据, 将签名后的数据发送至区块链服务器节点; 区块链服务器节点对签名后的数据进行验签, 并在验证成功时解密所述加密后的数据, 并解析解密后的数据, 将解析得到的数据进行上链。本发明实施例使得数据传输过程更加安全可靠, 且提高了数据的机密性和真实性。

基于区块链的数据传输方法和系统

本申请要求于2020年04月29日提交中国专利局、申请号为202010353842.0、申请名称为“基于区块链的数据传输方法和系统”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

[0001] 本发明属于信息安全技术领域，具体涉及一种基于区块链的数据传输方法和系统。

背景技术

[0002] 随着物联网技术的发展，越来越多的物联网设备连接到互联网中。许多物联网驱动的共享设备也发展非常迅速，比如共享单车、共享充电宝、共享智能洗衣设备等。

[0003] 相关技术中，洗护物联云平台为每一个运营商家分配共享智能洗衣设备接口，共享智能洗衣设备通过接口洗护物联云平台上进行认证，然后用户需要使用共享智能洗衣设备时，由相应的共享智能洗衣设备向洗护物联云平台发送用户身份信息，以使洗护物联云平台控制用户的访问权限。

[0004] 但是，智能洗衣设备与洗护物联云平台之间的数据传输均是直接进行的，或者进行一些简单加密之后再传输，如此很容易导致传输的数据被拦截并破解传输协议，从而导致数据传输的安全可靠性大大降低。

发明内容

[0005] 为了解决现有技术中的上述问题，本发明提供一种基于区块链的数据传输方法和系统，通过基于智能洗衣设备的唯一标识信息生成一个对称密钥和一对公私钥对，对称密钥给待传输的数据加密，并且，对称密钥和公私钥对存储在区块链服务器节点中，并且智能洗衣设备相关的数据也都保存在区块链服务器中，利用区块链签名机制进行智能洗衣设备身份认证，保证了设备的有效性，通过对称加密保

证待传输数据的机密性，利用区块链的共识机制、不可篡改特性保证了待传输数据的真实性和安全性。

[0006] 本发明实施例的第一方面提供一种基于区块链的数据传输方法，包括：

[0007] 设备认证平台获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，并将所述对称密钥和公私钥对存储于区块链服务器节点，所述标识信息与所述智能洗衣设备为一一对应的关系；

[0008] 智能洗衣设备利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点；

[0009] 所述区块链服务器节点对所述签名后的数据进行验签，并在验证成功时解密所述加密后的数据，解析所述解密后的数据，将解解析得到的数据进行上链。

[0010] 可选的，所述智能洗衣设备利用所述对称密钥对待传输数据进行加密处理之前，所述方法还包括：

[0011] 智能洗衣设备接收业务云平台发送的设备指令，并对所述设备指令进行处理，得到待传输数据。

[0012] 可选的，所述智能洗衣设备的安全芯片中存储有软件开发工具包 SDK；所述智能洗衣设备利用所述对称密钥对待传输数据进行加密处理之前，所述方法还包括：

[0013] 利用所述 SDK 根据所述公私钥对生成区块链交易信息，所述区块链交易信息包括所述公私钥对；

[0014] 将所述区块链交易信息和所述对称密钥存储至所述安全芯片中。

[0015] 可选的，所述利用所述公私钥对对所述加密后的数据进行数字签名，包括：

[0016] 通过所述公私钥对中的公钥对所述加密后的数据进行数据签名，得到签名后的数据。

[0017] 可选的，所述区块链服务器节点对所述签名后的数据进行验签，包括：

[0018] 所述区块链服务器节点在链上获取所述智能洗衣设备对应的公私钥对，并通过所述公私钥对中的私钥对所述签名后的数据进行验签。

[0019] 可选的，所述解析所述解密后的数据，包括：

[0020] 获取所述智能洗衣设备对应的设备协议；

[0021] 根据所述设备协议对所述解密后的数据进行解析。

[0022] 可选的，所述将所述签名后的数据发送至所述区块链服务器节点，包括：

[0023] 调用所述安全芯片中的 SDK 中的接口，通过所述接口将所述签名后的数据发送至所述区块链服务器节点。

[0024] 本发明实施例的第二方面提供一种基于区块链的数据传输系统，包括：设备认证平台，区块链服务器节点以及智能洗衣设备；

[0025] 所述设备认证平台用于：获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，并将所述对称密钥和公私钥对存储于区块链服务器节点，所述标识信息与所述智能洗衣设备为一一对应的关系；

[0026] 所述智能洗衣设备用于：利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点；

[0027] 所述区块链服务器节点用于：对所述签名后的数据进行验签，并在验证成功时解密所述加密后的数据，解析所述解密后的数据，将解析得到的数据进行上链。

[0028] 本发明实施例的第三方面提供一种计算机设备，包括：至少一个处理器和存储器；

[0029] 所述存储器存储计算机执行指令；

[0030] 所述至少一个处理器执行所述存储器存储的计算机执行指令，使得所述至少一个处理器执行本发明实施例第一方面所述的基于区块链的数据传输方法。

[0031] 本发明实施例的第四方面提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当处理器执行所

述计算机执行指令时，实现本发明实施例第一方面所述的基于区块链的数据传输方法。

[0032] 本发明实施例的第五方面提供一种芯片，所述芯片包括存储器、处理器，所述存储器中存储代码和数据，所述存储器与所述处理器耦合，所述处理器运行所述存储器中的程序使得所述芯片实现本发明实施例第一方面所述的基于区块链的数据传输方法。

[0033] 本发明实施例的第六方面提供一种程序产品，包括：计算机程序，当所述程序产品在计算机上运行时，使得所述计算机实现本发明实施例第一方面所述的基于区块链的数据传输方法。

[0034] 本发明实施例的第七方面提供一种计算机程序，当所述计算机程序被处理器执行时，用于实现本发明实施例第一方面所述的基于区块链的数据传输方法。

本领域技术人员能够理解的是，本发明实施例提供一种基于区块链的数据传输方法和系统，通过设备认证平台获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，将所述对称密钥和公私钥对存储于区块链服务器节点，标识信息与所述智能洗衣设备为一一对应的关系；智能洗衣设备利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点；所述区块链服务器节点对所述签名后的数据进行验签，并在验证成功时解密所述加密后的数据，解析所述解密后的数据，将解析得到的数据进行上链。由于每台智能洗衣设备对应唯一的标识信息，因此产生的每台洗衣设备的对称密钥和公私钥对都各不相同，大大增加了其破解难度，利用对称密钥对待传输的数据进行加密保证了用户隐私不被泄露，使用对称钥对利用区块链的签名机制进行智能洗衣设备数字身份的验证，保证了设备的有效性，并且智能洗衣设备的相关数据都加密后上链存储在区块链服务器节点中，使得数据透明且不可篡改，从而大大增加了数据传输的可靠性。

附图说明

[0035] 下面参照附图来描述本发明的基于区块链的数据传输方法和系统的优选实施方式。附图为：

[0036] 图1是本发明一示例性实施例示出的基于区块链的数据传输方法的应用场景图；

[0037] 图2是本发明一示例性实施例示出的基于区块链的数据传输方法的流程示意图；

[0038] 图3是本发明一示例性实施例示出的基于区块链的数据传输系统的结构示意图；

[0039] 图4是本发明一示例性实施例示出的计算机设备的结构示意图。

具体实施方式

[0040] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0041] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0042] 随着物联网技术的发展，越来越多的物联网设备连接到互联网中。许多物联网驱动的共享设备也发展非常迅速，比如共享单车、共享充电宝、共享智能洗衣设备等。

[0043] 相关技术中，洗护物联云平台为每一个运营商家分配共享智能洗衣设备接口，共享智能洗衣设备通过接口洗护物联云平台上进行认证，然后用户需要使用共享智能洗衣设备时，由相应的共享智能

洗衣设备向洗护物联云平台发送用户身份信息，以使洗护物联云平台控制用户的访问权限。

[0044] 但是，智能洗衣设备与洗护物联云平台之间的数据传输均是直接进行的，或者进行一些简单加密之后再传输，如此很容易导致传输的数据被拦截并破解传输协议，从而导致数据传输的安全可靠性大大降低。并且，传统的智能洗衣设备的相关数据（比如设备的使用记录，用户使用智能洗衣设备时填写的个人身份信息）都是存储于普通的关系型数据库中，然而普通的关系型数据库中的数据信息很容易被黑客窃取和篡改，从而威胁存储数据的真实性和安全性。

[0045] 针对此缺陷，本申请的主要技术方案包括：基于区块链分布式数据存储、共识机制以及不可篡改的特性，提供一种基于区块链的数据传输方法。基于智能洗衣设备唯一硬件序列号生成一个对称密钥以及一对公私钥对，对称密钥用于对待传输的数据进行加密或解密，公私钥对用于智能洗衣设备身份认证。且对称密钥和公私钥对存在于区块链的服务器节点上，对于智能洗衣设备而言，这两种密钥存放在安全芯片中，黑客几乎难以破解，并且每台智能洗衣设备用于加密的对称密钥各不相同，破解难度更是大大提高。另外，由于智能洗衣设备相关数据都保存在区块链服务器节点上，由于区块链节点共识的特性，保证了数据传输的安全性和真实性。

[0046] 下面结合上述附图阐述本发明的基于区块链的数据传输方法和系统的优选技术方案。

[0047] 图1是本发明一示例性实施例示出的基于区块链的数据传输方法的应用场景图。

[0048] 如图1所示，本实施例提供的应用场景的基本架构主要包括：智能洗衣设备认证平台101，至少一台智能洗衣设备102，区块链服务器103，客户端设备104；其中，智能洗衣设备均在智能洗衣设备认证平台上进行注册认证，以使智能洗衣设备认证平台获取设备的管理权；用户通过客户端设备（比如手机）向智能洗衣设备发送申请使用请求，并在请求通过时使用该智能洗衣设备；其中，智能洗衣设备认证平台、智能洗衣设备以及用户通过客户端设备发送的相关信息均发送至区块链服务器中进行上链，以存储在区块链中。

[0049] 图2是本发明一示例性实施例示出的基于区块链的数据传输方法的流程示意图。

[0050] 如图2所示，本实施例提供的方法可以包括以下步骤。

[0051] S201，设备认证平台获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，并将所述对称密钥和公私钥对存储于区块链服务器节点，所述标识信息与所述智能洗衣设备为一一对应的关系。

[0052] 其中，标识信息可以但不限于包括智能洗衣设备的唯一硬件序列号(device id)以及洗衣物联SIM卡的卡号(Integrate circuit card identity, ICCID)，每台智能洗衣设备均对应唯一的硬件序列号和ICCID。

[0053] 具体的，智能洗衣认证平台为每个商家提供智能洗衣设备绑定接口，通过绑定每台洗衣设备的硬件序列号和ICCID获得设备的管理权，并根据每台设备的硬件序列号和ICCID为每台智能洗衣设备生成对称密钥和公私钥对，且每台智能洗衣设备的对称密钥和公私钥对都是唯一的，不同智能洗衣设备的对称密钥和公私钥对各不相同。其中的对称密钥用于对传输数据进行加密或解密，公私钥对用于进行智能洗衣设备身份认证。然后将生成的每台智能洗衣设备的对称密钥和公私钥对存储到区块链服务器节点中。

[0054] 本步骤中，为每台智能洗衣设备生成各不相同的对称密钥和公私钥对，并且对称密钥和公私钥对均存储在区块链服务器节点中，大大提高了破解难度。

[0055] S202，智能洗衣设备利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点。

[0056] 其中，待传输数据包括设备使用记录、用户使用智能洗衣设备是填写的身份信息等。

[0057] 具体的，每台智能洗衣设备的对称密钥和公私钥对预先烧录进每台设备模组额外的安全芯片中；然后由智能洗衣设备中的安全芯片对待传输数据进行加密，得到加密数据，然后再根据公私钥对中的公钥对加密数据进行数字签名，将签名后的数据上链存储至区块链服务器节点中。

[0058] 本步骤中，将每台智能洗衣设备的对称密钥和公私钥对存储在安全芯片中，进一步提高了破解难度，并且将待传输数据加密、签名后进行传输，保证了数据传输过程中的可靠性和机密性，将加密、签名的数据存储在区块链中，基于区块链的共识机制和不可篡改特性保证了数据的安全性和真实性。

[0059] S203，所述区块链服务器节点对所述签名后的数据进行验签，并在验证成功时解密所述加密后的数据，解析所述解密后的数据，将解析得到的数据进行上链。

[0060] 具体的，区块链服务器节点在链上获取该智能洗衣设备对应的公私钥对，并通过所述公私钥对中的私钥对所述签名后的数据进行验签，若验证失败，则说明该数据是伪造的；若验证成功，则在链上获取该智能洗衣设备的对称密钥，采用对称密钥对加密后的数据进行解密，然后对解密后的数据进行解析，得到解析后的数据，将解析后的数据上链。

[0061] 本实施例中，由于每台智能洗衣设备对应唯一的标识信息，因此产生的每台洗衣设备的对称密钥和公私钥对都各不相同，大大增加了其破解难度，利用对称密钥对待传输的数据进行加密保证了用户隐私不被泄露，使用对称钥对利用区块链的签名机制进行智能洗衣设备数字身份的验证，保证了设备的有效性，并且智能洗衣设备的相关数据都加密后上链存储在区块链服务器节点中，使得数据透明且不可篡改，从而大大增加了数据传输的可靠性。

[0062] 为了更清楚的理解本申请，下面在图 2 所示实施例的基础上，对智能洗衣设备传输数据的过程进一步详细描述。

[0063] 首先，设备认证平台获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，并将所述对称密钥和公私钥对存储于区块链服务器节点，所述标识信息与所述智能洗衣设备为一一对应的关系。

[0064] 其中，标识信息可以但不限于包括智能洗衣设备的唯一硬件序列号(device id)以及洗衣物联 SIM 卡的卡号(Integrate circuit card identity, ICCID)，每台智能洗衣设备均对应唯一的硬件序列号和 ICCID。

[0065] 具体的，智能洗衣认证平台为每个商家提供智能洗衣设备绑定接口，通过绑定每台洗衣设备的硬件序列号和 ICCID 获得设备的

管理权。智能洗衣设备在向智能洗衣认证平台绑定注册时，获取并存储每台设备的硬件序列号和 ICCID，根据每台设备的为每台智能洗衣设备生成对称密钥和公私钥对，且每台智能洗衣设备的对称密钥和公私钥对都是唯一的，不同智能洗衣设备的对称密钥和公私钥对各不相同。其中的对称密钥用于对传输数据进行加密或解密，公私钥对用于进行智能洗衣设备身份认证。然后将生成的每台智能洗衣设备的对称密钥和公私钥对存储到区块链服务器节点中。

[0066] 进一步的，所述智能洗衣设备的安全芯片中存储有软件开发工具包 SDK；利用所述 SDK 根据所述公私钥对生成区块链交易信息，所述区块链交易信息包括所述公私钥对；将所述区块链交易信息和所述对称密钥存储至所述安全芯片中。

[0067] 具体的，区块链服务器节点上部署有 hyperchain hvm 智能合约，为每台智能洗衣设备提供适配的操作智能合约的 SDK，其运行在每台智能洗衣设备的安全芯片中，利用 SDK 根据每台智能洗衣设备的公私钥对生成一个 Account 字符串，该字符串包含公私钥对以及交易信息，Account 字符串是发起区块链交易的主体，然后将 Account 字符串和对称密钥烧录进每台设备模组额外的安全芯片中。

[0068] 进一步的，所述方法还包括：智能洗衣设备接收业务云平台发送的设备指令，并对所述设备指令进行处理，得到待传输数据。

[0069] 具体的，SDK 区别于智能洗衣设备本身的嵌入式程序，该 SDK 为嵌入式程序提供有限的接口，供其进行设备状态上报，或者使用记录上报。嵌入式程序用于接收业务云平台下发的设备指令，并对接收到的设备指令进行处理，得到待传输数据，该待传输数据可能包括设备的使用记录数据、用户使用该设备时填写的身份信息或者设备的状态信息等。

[0070] 进一步的，智能洗衣设备利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点。

[0071] 具体的，该智能洗衣设备的安全芯片中操作 hvm 智能合约的 SDK 将待传输数据通过该设备的对称密钥进行加密，得到加密数据；然后通过公私钥对中的公钥对加密数据进行数字签名；调用安全芯片

中的 SDK 提供的接口进行数据上链操作，即将签名后的数据通过 SDK 提供的接口发送至区块链服务器节点。

[0072] 进一步的，区块链服务器节点对签名后的数据进行验签，并在验证成功时解密所述加密后的数据，解析所述解密后的数据，将解析得到的数据进行上链。

[0073] 具体的，所述区块链服务器节点在链上获取所述智能洗衣设备对应的公私钥对，并通过所述公私钥对中的私钥对所述签名后的数据进行验签。若验证失败，则说明该数据是伪造的；若验证成功，则在链上获取该智能洗衣设备的对称密钥，采用对称密钥对加密后的数据进行解密；然后获取该智能洗衣设备的设备协议，通过该设备协议对解密后的数据进行解析，得到解析后的数据，最终将解析后的数据上链。

[0074] 进一步的，用户通过客户端应用程序 APP 注册的所有信息均利用对称密钥进行加密后发送至区块链服务器节点进行存储。

[0075] 本实施例中，利用区块链的数字签名机制进行智能洗衣设备身份认证，实现了设备数字身份的严格验证，保证了智能洗衣设备的有效性；进一步的，利用对称加密算法对用户信息进行脱敏处理，保证了数据传输过程中不被拦截导致信息泄露；并且，智能洗衣设备的相关数据全部加密后上链存储在区块链中，基于区块链分布式数据存储、共识机制以及不可篡改的特性，实现了数据公开透明且不可篡改，保证了数据的真实性和可靠性

[0076] 图 3 是本发明一示例性实施例示出的基于区块链的数据传输系统的结构示意图。

[0077] 如图 3 所示，本实施例提供的系统包括：智能洗衣设备认证平台 301，区块链服务器节点 302，智能洗衣设备 303；所述智能洗衣设备认证平台用于：获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，并将所述对称密钥和公私钥对存储于区块链服务器节点，所述标识信息与所述智能洗衣设备为一一对应的关系；所述智能洗衣设备用于：利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点；所述区块链服务器节点用于：对所述签名后的数据进行验签，并在验

证成功时解密所述加密后的数据，解析所述解密后的数据，将解析得到的数据进行上链。

[0078] 其中，智能洗衣设备的数量为至少一个。

[0079] 进一步的，参见图 3，本实施例提供的系统还包括：业务云平台 304，用于给智能洗衣设备调用接口，并向智能洗衣设备发送设备指令；所述智能洗衣设备还用于：接收业务云平台发送的设备指令，并对所述设备指令进行处理，得到待传输数据。

[0080] 进一步的，所述智能洗衣设备的安全芯片中存储有软件开发工具包 SDK；所述智能洗衣设备认证平台还用于：利用所述 SDK 根据所述公私钥对生成区块链交易信息，所述区块链交易信息包括所述公私钥对；将所述区块链交易信息和所述对称密钥存储至所述安全芯片中。

[0081] 进一步的，所述智能洗衣设备具体用于：通过所述公私钥对中的公钥对所述加密后的数据进行数据签名，得到签名后的数据。

[0082] 进一步的，所述区块链服务器节点具体用于：所述区块链服务器节点在链上获取所述智能洗衣设备对应的公私钥对，并通过所述公私钥对中的私钥对所述签名后的数据进行验签。

[0083] 进一步的，所述区块链服务器节点具体用于：获取所述智能洗衣设备对应的设备协议；根据所述设备协议对所述解密后的数据进行解析。

[0084] 进一步的，所述智能洗衣设备具体用于：调用所述安全芯片中的 SDK 中的接口，通过所述接口将所述签名后的数据发送至所述区块链服务器节点。

[0085] 本实施例中各个模块的详细功能描述请参考有关该方法的实施例中的描述，此处不做详细阐述说明。

[0086] 图 4 为本发明实施例提供的计算机设备的硬件结构示意图。如图 4 所示，本实施例提供的计算机设备 40 包括：至少一个处理器 401 和存储器 402。其中，处理器 401、存储器 402 通过总线 403 连接。

[0087] 在具体实现过程中，至少一个处理器 401 执行所述存储器 402 存储的计算机执行指令，使得至少一个处理器 401 执行上述方法实施例中的基于区块链的数据传输方法。

[0088] 处理器 401 的具体实现过程可参见上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

[0089] 在上述的图 4 所示的实施例中，应理解，处理器可以是中央处理单元（英文：Central Processing Unit，简称：CPU），还可以是其他通用处理器、数字信号处理器（英文：Digital Signal Processor，简称：DSP）、专用集成电路（英文：Application Specific Integrated Circuit，简称：ASIC）等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合发明所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

[0090] 存储器可能包含高速 RAM 存储器，也可能还包括非易失性存储 NVM，例如至少一个磁盘存储器。

[0091] 总线可以是工业标准体系结构（Industry Standard Architecture，ISA）总线、外部设备互连（Peripheral Component Interconnect，PCI）总线或扩展工业标准体系结构（Extended Industry Standard Architecture，EISA）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，本申请附图中的总线并限定仅有一根总线或一种类型的总线。

[0092] 本申请的另一实施例提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当处理器执行所述计算机执行指令时，实现上述方法实施例中的基于区块链的数据传输方法。

[0093] 上述的计算机可读存储介质，上述可读存储介质可以是由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。可读存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0094] 一种示例性的可读存储介质耦合至处理器，从而使处理器能够从该可读存储介质读取信息，且可向该可读存储介质写入信息。当然，可读存储介质也可以是处理器的组成部分。处理器和可读存储介质可以位于专用集成电路(Application Specific Integrated Circuits，简

称：ASIC)中。当然，处理器和可读存储介质也可以作为分立组件存在于设备中。

[0095] 本实施例还提供一种芯片，所述芯片包括存储器、处理器，所述存储器中存储代码和数据，所述存储器与所述处理器耦合，所述处理器运行所述存储器中的程序使得所述芯片用于执行上述各种实施方式提供的基于区块链的数据传输方法。

[0096] 本实施例还提供一种计算机程序，当所述计算机程序被处理器执行时，用于执行前述各种实施方式提供的基于区块链的数据传输方法。

[0097] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0098] 至此，已经结合附图所示的优选实施方式描述了本发明的技术方案，但是，本领域技术人员容易理解的是，本发明的保护范围显然不局限于这些具体实施方式。在不偏离本发明的原理的前提下，本领域技术人员可以对相关技术特征作出等同的更改或替换，这些更改或替换之后的技术方案都将落入本发明的保护范围之内。

权 利 要 求 书

1、一种基于区块链的数据传输方法，其特征在于，包括：

设备认证平台获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，并将所述对称密钥和公私钥对存储于区块链服务器节点，所述标识信息与所述智能洗衣设备为一一对应的关系；

智能洗衣设备利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点；

所述区块链服务器节点对所述签名后的数据进行验签，并在验证成功时解密所述加密后的数据，解析所述解密后的数据，将解析得到的数据进行上链。

2、根据权利要求1所述的方法，其特征在于，所述智能洗衣设备利用所述对称密钥对待传输数据进行加密处理之前，所述方法还包括：

智能洗衣设备接收业务云平台发送的设备指令，并对所述设备指令进行处理，得到待传输数据。

3、根据权利要求1或2所述的方法，其特征在于，所述智能洗衣设备的安全芯片中存储有软件开发工具包SDK；所述智能洗衣设备利用所述对称密钥对待传输数据进行加密处理之前，所述方法还包括：

利用所述SDK根据所述公私钥对生成区块链交易信息，所述区块链交易信息包括所述公私钥对；

将所述区块链交易信息和所述对称密钥存储至所述安全芯片中。

4、根据权利要求1至3任一项所述的方法，其特征在于，所述利用所述公私钥对对所述加密后的数据进行数字签名，包括：

通过所述公私钥对中的公钥对所述加密后的数据进行数据签名，得到签名后的数据。

5、根据权利要求1至4任一项所述的方法，其特征在于，所述区块链服务器节点对所述签名后的数据进行验签，包括：

所述区块链服务器节点在链上获取所述智能洗衣设备对应的公私钥对，并通过所述公私钥对中的私钥对所述签名后的数据进行验签。

6、根据权利要求1至5任一项所述的方法，其特征在于，所述解析所述解密后的数据，包括：

获取所述智能洗衣设备对应的设备协议；

根据所述设备协议对所述解密后的数据进行解析。

7、根据权利要求1至6任一项所述的方法，其特征在于，所述将所述签名后的数据发送至所述区块链服务器节点，包括：

调用所述安全芯片中的SDK中的接口，通过所述接口将所述签名后的数据发送至所述区块链服务器节点。

8、一种基于区块链的数据传输系统，其特征在于，包括：设备认证平台，区块链服务器节点以及智能洗衣设备；

所述设备认证平台用于：获取智能洗衣设备的标识信息，根据所述标识信息生成对称密钥和公私钥对，并将所述对称密钥和公私钥对存储于区块链服务器节点，所述标识信息与所述智能洗衣设备为一一对应的关系；

所述智能洗衣设备用于：利用所述对称密钥对待传输数据进行加密处理，利用所述公私钥对对所述加密后的数据进行数字签名，得到签名后的数据，将所述签名后的数据发送至所述区块链服务器节点；

所述区块链服务器节点用于：对所述签名后的数据进行验签，并在验证成功时解密所述加密后的数据，解析所述解密后的数据，将解析得到的数据进行上链。

9、一种计算机设备，其特征在于，包括：至少一个处理器和存储器；

所述存储器存储计算机执行指令；

所述至少一个处理器执行所述存储器存储的计算机执行指令，使得所述至少一个处理器执行如权利要求1至7任一项所述的基于区块链的数据传输方法。

10、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机执行指令，当处理器执行所述计算机执行指令时，实现如权利要求1至7任一项所述的基于区块链的数据传输方法。

11、一种芯片，其特征在于，所述芯片包括存储器、处理器，所述存储器中存储代码和数据，所述存储器与所述处理器耦合，所述处理器运行所述存储器中的程序使得所述芯片用于执行上述权利要求1至7任一项所述的基于区块链的数据传输方法。

12、一种程序产品，其特征在于，包括：计算机程序，当所述程序产品在计算机上运行时，使得所述计算机执行上述权利要求1至7任一项所述的基于区块链的数据传输方法。

13、一种计算机程序，其特征在于，当所述计算机程序被处理器执行时，用于执行上述权利要求1至7任一项所述的基于区块链的数据传输方法。

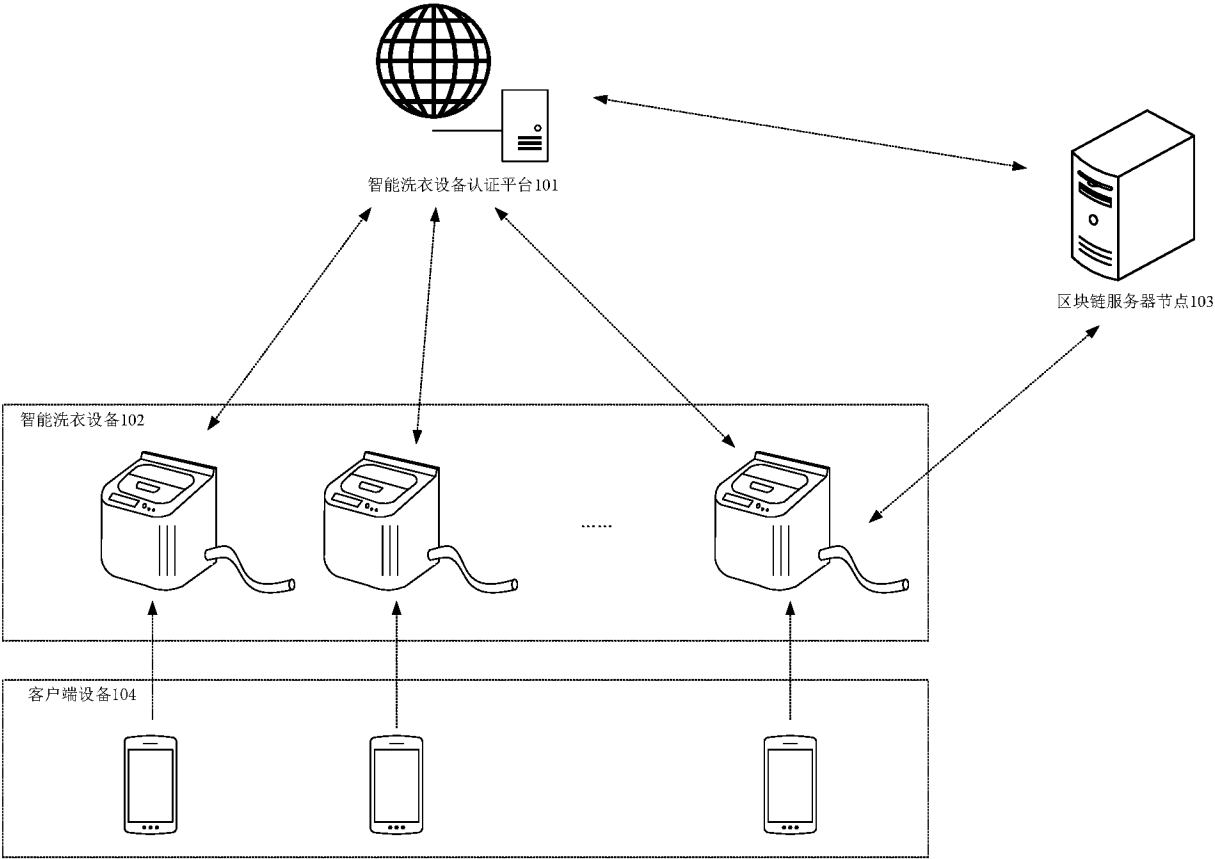


图1

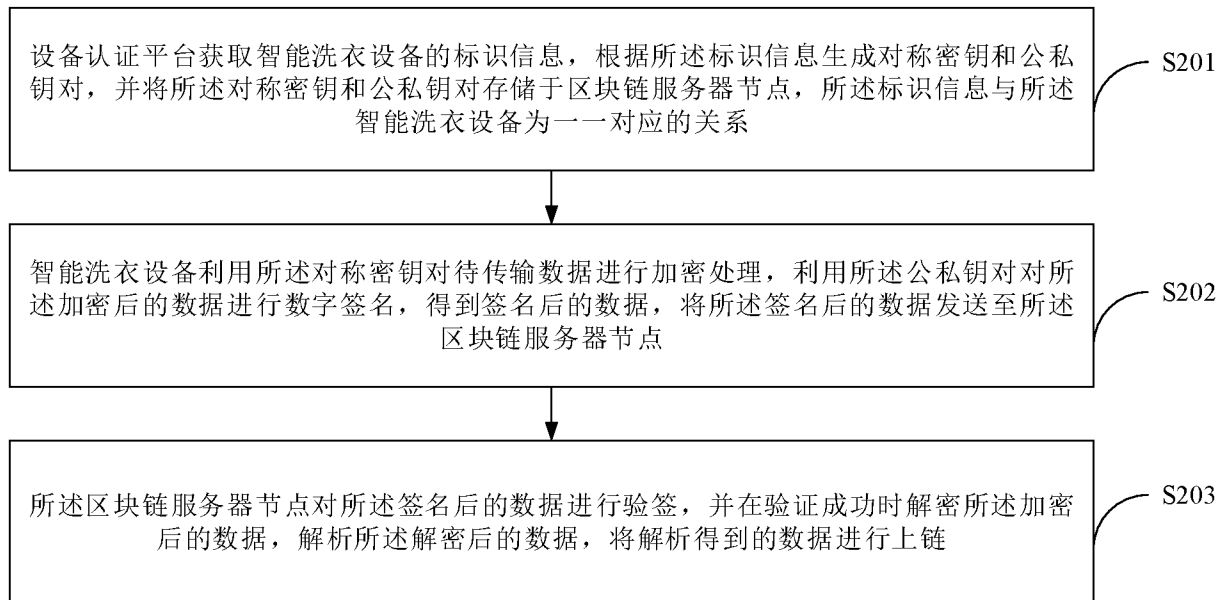


图2

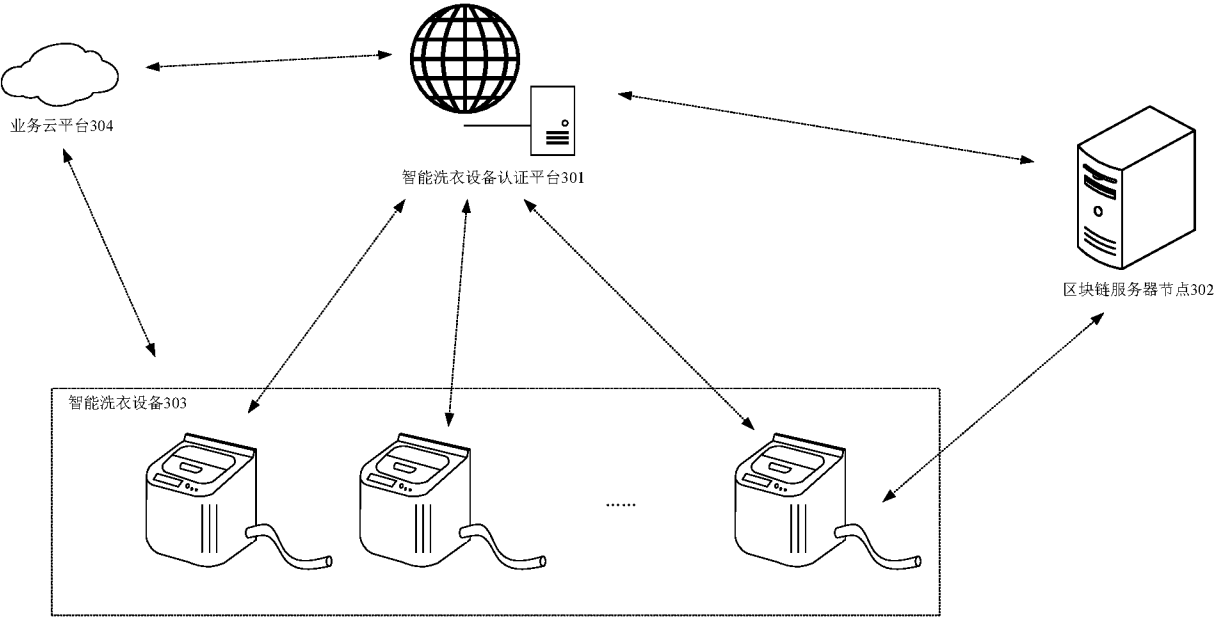


图3

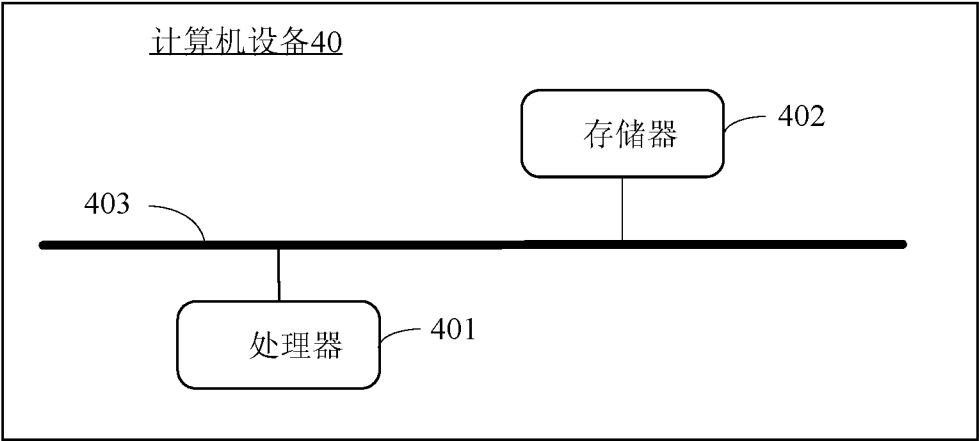


图4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/091038

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/32(2006.01)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)

H04L

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)

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 二次, 双重, 两次, 加密, 区块链, 上链, 对称密钥, 验签, 验证签名, double, encrypt+, block chain, key, verif+, signature

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 110061845 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 26 July 2019 (2019-07-26) description paragraphs [0023]-[0124], [0149]-[0186]	1-13
X	CN 110599322 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 20 December 2019 (2019-12-20) description paragraphs [0070]-[0072], [0126]-[0130]	1-13
A	US 2020084027 A1 (BANK OF MONTREAL et al.) 12 March 2020 (2020-03-12) entire document	1-13



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

24 June 2021

Date of mailing of the international search report

21 July 2021

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/CN2021/091038

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110061845	A	26 July 2019	WO	2020181845	A1	17 September 2020
CN	110599322	A	20 December 2019	None			
US	2020084027	A1	12 March 2020	WO	2020049357	A1	12 March 2020

国际检索报告

国际申请号

PCT/CN2021/091038

A. 主题的分类

H04L 29/06 (2006.01) i; H04L 9/32 (2006.01) 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)

H04L

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))

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT; 二次, 双重, 两次, 加密, 区块链, 上链, 对称密钥, 验签, 验证签名, double, encrypt+, block chain, key, verif+, signature

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
X	CN 110061845 A (深圳壹账通智能科技有限公司) 2019年 7月 26日 (2019 - 07 - 26) 说明书第[0023]-[0124]、[0149]-[0186]段	1-13
X	CN 110599322 A (腾讯科技深圳有限公司) 2019年 12月 20日 (2019 - 12 - 20) 说明书第[0070]-[0072]、[0126]-[0130]段	1-13
A	US 2020084027 A1 (BANK OF MONTREAL 等) 2020年 3月 12日 (2020 - 03 - 12) 全文	1-13

☐ 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

2021年 6月 24日

国际检索报告邮寄日期

2021年 7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

受权官员

苏星晔

电话号码 86-(512)-88996074

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/091038

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	110061845	A	2019年 7月 26日	W0	2020181845	A1	2020年 9月 17日
CN	110599322	A	2019年 12月 20日	无			
US	2020084027	A1	2020年 3月 12日	W0	2020049357	A1	2020年 3月 12日