(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114651252 A
(43)申请公布日 2022.06.21

(21)申请号 202080077447.2

(22)申请日 2020.11.19

(30)优先权数据
10-2019-0169407 2019.12.18 KR

(85)PCT国际申请进入国家阶段日
2022.05.06

(86)PCT国际申请的申请数据
PCT/KR2020/016341 2020.11.19

(87)PCT国际申请的公布数据
WO2021/125586 KO 2021.06.24

(71)申请人 权五京
地址 韩国首尔市麻浦区世界杯北路44街22,501号

(72)发明人 权五京

(74)专利代理机构 北京锺维联合知识产权代理有限公司 11579
专利代理师 罗银燕

(51)Int.Cl.
G06F 21/34(2006.01)
G06F 21/46(2006.01)
G06F 21/70(2006.01)
G06F 21/10(2006.01)

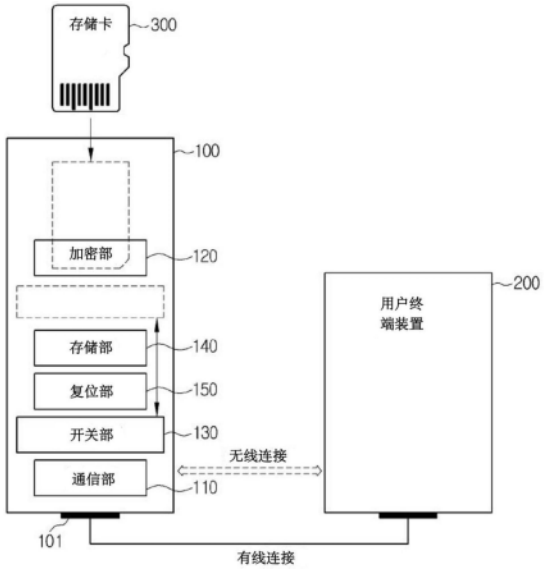
权利要求书1页 说明书10页 附图8页

(54)发明名称

内容钱包装置及利用其的自我主权身份及版权认证系统

(57)摘要

本发明公开内容钱包装置。与存储内容的存储装置连接的内容钱包装置包括:通信部,用于内容钱包装置与用户终端装置之间的通信;加密部,为了内容钱包装置与用户终端装置之间的认证而生成包含用户身份(ID)及密码的加密数据;开关部,用于控制存储装置与通信部之间的电连接;以及复位部,若通过开关部解除存储装置与通信部之间的电连接,则将所生成的密码初始化。由此,在用户销售内容的过程中,在中心管理系统未经授权的情况下,用户和购买方可以直接买卖内容,每当用户认证内容所有权时生成新密码,由此,可以通过防止第三方的盗取来防止内容无故泄露。



CN 114651252 A

1.一种内容钱包装置,与存储内容的存储装置连接,其特征在于,包括:

通信部,用于上述内容钱包装置与用户终端装置之间的通信;

加密部,为了上述内容钱包装置与用户终端装置之间的认证而生成包含用户身份及密码的加密数据;

开关部,用于控制上述存储装置与上述通信部之间的电连接;以及

复位部,若通过上述开关部解除上述存储装置与上述通信部之间的电连接,则将所生成的上述密码初始化。

2.根据权利要求1所述的内容钱包装置,其特征在于,

若通过上述开关部使上述存储装置与上述通信部电连接,则上述加密部生成第一随机密码,

若通过上述开关部解除上述存储装置与上述通信部之间的电连接,则上述复位部将上述第一随机密码初始化,

若通过上述开关部使上述存储装置与上述通信部再次电连接,则上述加密部生成第二随机密码。

3.根据权利要求1所述的内容钱包装置,其特征在于,若通过上述开关部使上述存储装置与上述通信部电连接,则上述通信部向上述用户终端装置传输用于断开上述用户终端装置的网络的信号。

4.根据权利要求3所述的内容钱包装置,其特征在于,若断开上述用户终端装置的网络,则通过由上述加密部生成的加密数据来执行上述内容钱包装置与用户终端装置之间的认证。

5.根据权利要求1所述的内容钱包装置,其特征在于,若通过上述开关部使上述存储装置与上述通信部电连接,则上述加密部加密上述内容来向上述通信部传递。

6.根据权利要求1所述的内容钱包装置,其特征在于,上述加密部向上述内容插入用户固有的识别码。

7.一种系统,包括内容钱包装置及用户终端装置,其特征在于,

上述内容钱包装置为了上述内容钱包装置与上述用户终端装置之间的认证而向上述用户终端装置传输包含用户身份及密码的加密数据,

若根据用户操作输入的密码与所传输的上述密码匹配,则上述用户终端装置执行上述内容钱包装置与用户终端装置之间的认证。

8.根据权利要求7所述的系统,其特征在于,每当与上述用户终端装置执行认证时,上述内容钱包装置随机生成用于上述认证的密码来传输。

9.根据权利要求8所述的系统,其特征在于,

若上述存储装置与上述内容钱包装置电连接,则上述内容钱包装置向上述用户终端装置传输用于断开上述用户终端装置的网络的信号,

若输入与所传输的上述信号对应的用户操作,则上述用户终端装置断开网络。

内容钱包装置及利用其的自我主权身份及版权认证系统

技术领域

[0001] 本发明涉及内容钱包装置及利用其的系统，更详细地，涉及新生成自我主权身份认证所需密码来强化内容信息的安全的内容钱包装置及利用其的系统。

背景技术

[0002] 通常，需要运营在线平台的民间企业家向数据库的运营商进行委托来运营事业，对会员注册时所需个人信息及与平台使用详情有关的数据管理以及对相应信息的使用权限进行集中化。

[0003] 当通过以此集中的数据库运营的私人在线平台被第三方入侵时，存在共享此平台的其他用户的数据有可能容易泄露的问题。

[0004] 并且，若运营个人在线平台的民间企业家使用私人在线平台，则需要支付昂贵的使用费用，不仅如此，当个人数据管理出现问题时，存在当事人无法迅速对应的问题等。

发明内容

[0005] 技术问题

[0006] 本发明的目的在于，提供如下的内容钱包装置及利用其的系统，即，在没有中央管理服务器的介入的情况下用户可以直接向需要购买存储在存储装置的内容的购买方传输，每当需要用户认证时新生成密码，以防止被轻松盗取或泄漏，由此强化安全。

[0007] 解决问题的方案

[0008] 用于实现这种目的的本发明一实施例的与存储内容的存储装置连接的内容钱包装置可包括：通信部，用于上述内容钱包装置与用户终端装置之间的通信；加密部，为了上述内容钱包装置与用户终端装置之间的认证而生成包含用户身份(ID)及密码的加密数据；开关部，用于控制上述存储装置与上述通信部之间的电连接；以及复位部，若通过上述开关部解除上述存储装置与上述通信部之间的电连接，则将所生成的上述密码初始化。

[0009] 在此情况下，若通过上述开关部使上述存储装置与上述通信部电连接，则上述加密部生成第一随机密码，若通过上述开关部解除上述存储装置与上述通信部之间的电连接，则上述复位部将上述第一随机密码初始化，若通过上述开关部使上述存储装置与上述通信部再次电连接，则上述加密部生成第二随机密码。

[0010] 并且，若通过上述开关部使上述存储装置与上述通信部电连接，则上述通信部可向上述用户终端装置传输用于断开上述用户终端装置的网络的信号。

[0011] 其中，若断开上述用户终端装置的网络，则可通过由上述加密部生成的加密数据来执行上述内容钱包装置与用户终端装置之间的认证。

[0012] 进而，若通过上述开关部使上述存储装置与上述通信部电连接，则上述加密部加密上述内容来向上述通信部传递。

[0013] 并且，上述加密部可向上述内容插入用户固有的识别码。

[0014] 另一方面，在本发明一实施例的包括内容钱包装置及用户终端装置的系统中，上

述内容钱包装置可以为了上述内容钱包装置与上述用户终端装置之间的认证而向上述用户终端装置传输包含用户身份及密码的加密数据，若根据用户操作输入的密码与所传输的上述密码匹配，则上述用户终端装置可执行上述内容钱包装置与用户终端装置之间的认证。

[0015] 其中，每当与上述用户终端装置执行认证时，上述内容钱包装置可随机生成用于上述认证的密码来传输。

[0016] 而且，若上述存储装置与上述内容钱包装置电连接，则上述内容钱包装置可向上述用户终端装置传输用于断开上述用户终端装置的网络的信号，若输入与所传输的上述信号对应的用户操作，则上述用户终端装置可断开网络。

[0017] 发明的效果

[0018] 根据如上所述的本发明的多种实施例，在用户销售内容的过程中，在中央管理系统未经授权的情况下，用户和购买方可以直接买卖内容，每当用户欲认证内容所有权时生成新的密码，由此，可以通过防止第三方的盗取来防止内容无故泄露。

附图说明

[0019] 图1为示出本发明一实施例的内容钱包装置的结构的图。

[0020] 图2为示出本发明另一实施例的内容钱包装置的结构的图。

[0021] 图3为用于说明图2的内容钱包装置的剖视图。

[0022] 图4为用于说明本发明另一实施例的内容钱包装置内置在用户终端装置的状态的图。

[0023] 图5为用于说明本发明另一实施例的多种存储装置与内容钱包装置的连接状态的图。

[0024] 图6为用于说明利用本发明一实施例的内容钱包装置的系统的图。

[0025] 图7为用于说明利用图6的内容钱包装置的系统的流程的图。

[0026] 图8为用于说明利用本发明另一实施例的内容钱包装置的系统的图。

具体实施方式

[0027] 以下，参照附图，更加详细说明本发明。而且，在说明本发明的过程中，在判断为对于相关的公知功能或结构的具体说明使本发明的主旨不清楚的情况下，将省略对其的详细说明。而且，后述的术语作为考虑在本发明中的功能来定义的术语，可根据用户、运营人员的意图或管理等改变。因此，上述定义应以本说明书中的整体内容来下达。

[0028] 本发明的存储装置300可以为包括能够存储内容的外置硬盘、USB、CD、存储卡等存储功能的独立的存储装置，以下，以存储卡(以下，以存储装置的附图标记300记述)进行说明，但并不局限于此。

[0029] 图1为示出本发明一实施例的内容钱包装置的结构的图。

[0030] 参照图1，内容钱包装置100可以与存储内容的存储卡300连接，可向用户终端装置200传输存储于存储卡300的内容。

[0031] 在此情况下，用户终端装置200可以为移动终端装置，此外，可以为平板PC、个人数据助理(PDA，Personal Digital Assistant)、可穿戴设备、笔记本电脑、台式PC及数字摄像

头等可以电通信的多种电子设备。

[0032] 并且,内容钱包装置100为了传输内容而可以包括通信部110、加密部120、开关部130、存储部140及复位部150。

[0033] 通信部110可以实现内容钱包装置100及用户终端装置200之间的通信,可通过基于有线的直接连接或规定范围内的基于无线的间接连接实现通信。

[0034] 例如,用户终端装置200及内容钱包装置100的基于有线的连接可以利用与通常使用的充电端子连接的方式。并且,此外可以利用与插入外置硬盘、USB、耳机等的端子等连接的方式来直接连接。

[0035] 若内容钱包装置100及用户终端装置200位于规定范围内,则基于无线的连接可以利用近场通信(NFC,Near Field Communication)、射频无线通信(RFID,Radio Frequency identification)、蓝牙(Bluetooth)及红外线通信等来间接连接。

[0036] 如上所述,内容钱包装置100及用户终端装置200通过通信部110连接,由此,存储在向内容钱包装置100插入的存储卡300的内容可以向用户终端装置200移动,并且,为了在内容钱包装置100中进行认证而随机生成的密码可以向用户终端装置200移动。

[0037] 不仅如此,通信部110还可以向用户终端装置200传输用于断开用户终端装置200的网络的信号,以下,进行详细说明。

[0038] 加密部120为了内容钱包装置100及用户终端装置200之间的认证而可以生成包含用户身份(ID,identification)及密码(password、pass-code)的加密数据(Encryption data)。

[0039] 具体地,若存储卡300及通信部110电连接,则加密部120可以生成加密数据。

[0040] 包含在加密数据的用户身份可以为存储在存储部140的用户认证身份,例如,可以为基于去中心化身份(DID,Decentralized identity)的身份认证身份。

[0041] 去中心化身份为基于分布式存储系统的自我主权身份证明技术,是如下的方法,即,分布式存储系统并非向如特定机构或企业的中央集中系统委托可区分个人身份的信息的所有权,身份验证所需信息也由网络的终端成员进行分割存储并管理。

[0042] 即,自我主权身份证明技术为每个人自己证明对于身份验证信息的主权的方式。

[0043] 加密部120从存储部140读取这种去中心化身份,由此可以与密码一同生成为加密数据。

[0044] 而且,包含在所生成的加密数据的密码可以为混合数字、文字或符号等来生成或者利用触摸次数、图案、触摸区域指定等来生成的密码。

[0045] 例如,若所生成的密码的可输入位数为十位数,则当用户终端装置为台式PC时,数字、文字或符号可仅混合数字0至9中的数字来生成密码,或者混合在打字机中的韩文、英文及数字一同并记的符号来生成密码。

[0046] 并且,在内容钱包装置中,作为台式PC画面,可以使用直线或曲线等来以图案形态生成密码。

[0047] 进而,在存储于存储卡300的内容向用户终端装置200传输之前,加密部120可以加密内容来向通信部110传递。若通过开关部130,存储卡300及通信部110电连接,则加密部120加密内容。

[0048] 例如,加密部120可以利用预先存储的机制来通过模拟方式加密内容,或者通过利

用预先存储的逻辑算法的数字方式加密内容。

[0049] 加密的内容根据公钥加密方式或私钥加密方式加密，加密部120可以一同生成解密密钥来向通信部110传递，以可再次解密以此加密的内容。

[0050] 并且，加密部120为了简化内容加密过程，除内容的加密之外，仅可向内容插入用户固有的识别码，以可以识别内容的原作者。

[0051] 例如，用户的固有识别码可通过水印实现。水印为插入只有内容的原作者知道的标记(Mark)的方式，当未经授权的第三者非法复制或流通内容时，可提取向内容插入的水印，由此，可以知道是否为原作者的内容，不仅如此，也可以追踪复制的路径。

[0052] 开关部130可以控制存储卡300及通信部110之间的电连接。

[0053] 例如，开关部130可以为能够位置变化的按钮形式，可包括拨动开关、推动开关、滑动按钮开关等。

[0054] 以此可实现物理位置变化的开关部130可在插入存储卡300之后向插入存储卡300的方向移动开关部130来使存储卡300及通信部110电连接，与此相反，可向存储卡300插入的方向和相反方向移动开关部130的位置来解除存储卡300及通信部110之间的电连接。

[0055] 只是，这为用于说明本发明的实施例，可实施若实现内容钱包装置100及用户终端装置200之间的通信，则存储卡300及通信部110在内容钱包装置100内自动连接的方式，而并非实施通过物理调节位置来连接存储卡300及通信部110的方式。

[0056] 并且，若通过开关部130，存储卡300及通信部110电连接，则通信部110可以向用户终端装置200传输用于断开用户终端装置200的网络的信号。

[0057] 在用户终端装置200为移动终端装置的情况下，通信部110可以向移动终端装置发送询问是否转换为飞行模式的消息，可通过用户的操作选择是否转换为飞行模式。

[0058] 进而，若断开用户终端装置200的网络，则可通过包含通过加密部120生成的用户身份及密码的加密数据执行内容钱包装置100及用户终端装置200之间的认证。

[0059] 接着，举例说明移动终端装置，在用户选择转换飞行模式的情况下，断开移动终端装置的网络，可向移动终端装置传输通过加密部120生成的加密数据。

[0060] 在此情况下，用户可向移动终端装置输入包含在所传输的加密数据的密码，当与在内容钱包装置100中生成的密码相同时，针对所存储的内容，与著作权识别信息有关的数据可附加记录在内容钱包装置100。

[0061] 并且，可通过确认通过用户的操作向移动终端装置输入的密码及在内容钱包装置100中生成的密码是否相同，执行对于加密的内容的用户的认证，基于此，可以实现自我主权身份认证。

[0062] 如上所述，当用户终端装置为台式PC时，台式PC接收在数字、文字或符号中混合仅从数字0至9中的数字来生成的密码、混合在包含在打字机的韩文、英文及数字一同并记的符号来生成的密码并通过打字机或此外的输入装置输入与所传输的密码响应的密码来执行认证。

[0063] 并且，在基于图案的密码的情况下，根据向用户终端装置的鼠标或可触摸的画面传输的图案密码写入，由此输入密码来执行认证。

[0064] 其中，通过加密部120传输的密码及用户通过用户终端装置200输入的密码的相同与否可以在形成于内容钱包装置100的存储部140中执行。

[0065] 例如，可通过存储在存储部140的密码认证模块或密码认证程序来执行用户传输的密码及用户通过用户终端装置200输入的密码之间是否相同。

[0066] 存储部140可以包括ROM、RAM、EPROM、EEPROM、硬盘等中的至少一个，此外，可以为包括能够存储的非易失性存储器的存储介质。

[0067] 如上所述，若通过存储部140，在内容钱包装置100中生成的密码及用户向用户终端装置200输入的密码相同，则作为用户身份的所有者的用户可以查询存储在通过用户终端装置200认证的内容钱包装置100的存储卡300的内容。

[0068] 并且，当需要向其他外部终端装置传输内容时，可在选择所查询的内容来从内容钱包装置100向用户终端装置200传输之后，向其他外部终端装置传输用户终端装置200所接收的内容。

[0069] 其中，当所选择的内容从内容钱包装置100向用户终端装置200传输时，可以执行加密来传输。

[0070] 另一方面，内容钱包装置100可以包括处理器(未图示)，在此情况下，上述加密部120的工作可以由处理器(未图示)执行，在此情况下，加密部120可以被处理器(未图示)代替。

[0071] 处理器(未图示)可算出读取存储在密码认证模块的程序来生成的密码及通过用户的操作向用户终端装置200输入的密码是否相同，上述密码认证模块存储在存储部140。

[0072] 并且，处理器(未图示)可读取存储在内容加密模块的程序来以如上所述的方式加密内容，上述内容加密模块存储在存储部140。

[0073] 若通过开关部130解除存储卡300及通信部110之间的电连接，则复位部150可以将所生成的密码初始化。

[0074] 例如，若向内容钱包装置100插入存储卡300，且开关部130向插入的方向移动，则存储卡300及通信部110电连接，由此加密部120可以生成第一随机密码。

[0075] 之后，若开关部130向与插入存储卡300的方向相反的方向移动，则存储卡300及通信部100之间的电连接将被解除并通过复位部150来将第一随机密码初始化。

[0076] 当然，在此情况下，通过加密部120生成的第一随机密码可存储在存储部140，通过开关部130解除存储卡300及通信部100之间的电连接，存储在存储部140的第一随机密码可通过复位部150初始化。

[0077] 若开关部130再次向插入存储卡300的方向移动，则存储卡300及通信部110再次电连接，加密部120可以生成与初始化的第一随机密码不同的第二随机密码，第二随机密码也可存储在存储部140。

[0078] 如上所述，每当内容钱包装置100及用户终端装置200连接时，加密部120随机生成新密码，之前随机生成的密码可通过复位部150初始化，由此可以防止被第三者盗取的危险。

[0079] 图2为示出本发明另一实施例的内容钱包装置的结构的图，图3为用于说明图2的内容钱包装置的剖视图。

[0080] 其中，已对通信部110、加密部120、开关部130、存储部140及复位部150进行了说明，因此，将省略对其的详细说明。

[0081] 参照图2，内容钱包装置100还可包括输入部160。

[0082] 输入部160用于接收用户操作，在内容钱包装置100中生成的密码可通过用户操作输入到输入部160来生成。

[0083] 换句话说，作为一实施例，对于随机生成的密码，随着存储卡300及通信部110通过图1所示的开关部130电连接，可通过加密部120随机生成密码，作为另一实施例，通过图2所示的输入部160输入基于用户操作的密码，由此可以随时生成。

[0084] 当然，通过用户的操作生成密码，因此，通过复位部150初始化之前的密码和初始化之后的密码必然相同。

[0085] 在此情况下，图2所示的加密部120可加密存储在存储卡300的内容，并可生成对其进行解密的解密秘钥。

[0086] 并且，以可以使内容的原作者识别的方式能够生成用户固有的识别码。

[0087] 参照图3，说明的内容钱包装置100的工作，在内容钱包装置100可插入存储卡300，所插入的存储卡300可以与加密部120连接。

[0088] 在此情况下，开关部130的位置向插入存储卡300的方向移动，则存储卡300及通信部110电连接，加密部120可读取存储在存储部140的用户身份来生成用户身份。

[0089] 而且，可以随机生成用户通过输入部160随意输入的密码，同时随机生成密码可存储在存储部140。

[0090] 如上所述，通过输入部160生成的密码及通过加密部120生成的用户身份可传递到通信部110。

[0091] 向通信部110传递的随机生成的密码可传输到用户终端装置200，若用户通过用户终端装置200输入随机生成的密码，则内容钱包装置100通过通信部110接收用户输入的密码，存储部140存储所传递的密码。

[0092] 如上所述，存储部140可以确认在内容钱包装置100中随机生成的密码及向用户终端装置200输入的密码是否相同。

[0093] 当所存储的密码相互匹配时，用户可通过用户终端装置200查询存储在存储卡300内的内容。并且，当向外部终端装置传输内容时，加密部120可加密存储在存储卡300的内容来向通信部110传递，通信部110可向外部终端装置传输在用户终端装置200中加密的内容。

[0094] 若开关部130的位置向插入存储卡300的相反方向移动，则可通过复位部150将存储在存储部140的密码初始化。

[0095] 但是，图3所示的内容钱包装置100为用于实施本发明的一个例示，在内容钱包装置100中所包括的结构要素的位置可根据用户的利用及便利改变。

[0096] 图4为用于说明本发明另一实施例的内容钱包装置内置于用户终端装置的状态的图。

[0097] 参照图4，内容钱包装置100可处于内置于用户终端装置200的形态。

[0098] 在此情况下，内容钱包装置100及用户终端装置200的通信可以在内容钱包装置100插入于用户终端装置200的过程中实现，若内容钱包装置100完全插入于用户终端装置200，则内容钱包装置100及用户终端装置200电连接。

[0099] 以如上方式实现电连接，同时，内容钱包装置100向用户终端装置200传输外部通信网中断的消息。

[0100] 若用户向用户终端装置200输入中断外部通信网的选择，则内容钱包装置100可随

机生成密码，读取存储于内容钱包装置100的用户身份来与所生成的密码一同向用户终端装置200传输。

[0101] 因此，用户输入向用户终端装置200传输的密码，内容钱包装置100对所输入的密码与在内容钱包装置100中随机生成的密码进行匹配并确认是否相同之后，将存储在存储卡300的内容加密来向用户终端装置200传输。

[0102] 若加密的内容向用户终端装置200的传输全部完成，则所插入的内容钱包装置100可以从用户终端装置200向外部分离。

[0103] 在此情况下，内容钱包装置100可从用户终端装置200分离并将随机生成的密码初始化。

[0104] 作为内容钱包装置100内置在用户终端装置200来实施的另一例，若内容钱包装置100插入于用户终端装置200，则在所插入的向外部露出的一面可包括能够改变位置的开关单元(未图示)。

[0105] 这种开关单元可以为拨动开关、推动开关、滑动按钮开关等，可通过移动上述开关来控制内容钱包装置100及用户终端装置200的电连接。

[0106] 图5为用于说明本发明另一实施例的多种存储装置与内容钱包装置的连接状态的图。

[0107] 参照图5，内容钱包装置100可包括多个输入端口、输出端口，可通过端口连接多种存储装置。

[0108] 在此情况下，包括多个输入端口、输出端口的钱包装置100可以为如USB或雷电接口等的能够支持坞站的装置。

[0109] 图6为用于说明利用本发明一实施例的内容钱包装置的系统的图。

[0110] 参照图6，利用内容钱包装置的系统10可包括内容钱包装置100及用户终端装置200。

[0111] 内容钱包装置100可以向用户终端装置200传输包含为了内容钱包装置100及用户终端装置200之间的认证的用户身份及随机生成的密码的加密数据。

[0112] 若根据用户操作输入的密码与所传输的密码匹配，则用户终端装置200可执行内容钱包装置100及用户终端装置200之间的认证。

[0113] 例如，内容钱包装置100可以向用户终端装置200传输随机生成的密码，用户通过用户终端装置200输入所传输的密码，由此，接收所输入的密码的内容钱包装置100可以确认是否与随机生成的密码匹配并相同。

[0114] 其中，每当内容钱包装置100及用户终端装置200执行认证时，可以新生成随机生成的密码，每当进行认证时，内容钱包装置100可以确认新生成的密码是否相同。

[0115] 若匹配的密码相同，则向用户终端装置200传递内容钱包装置100的内容及用户身份，向需要购买上述内容及用户身份的其他用户的用户终端装置200-1直接传输加密的内容、解密秘钥及内容及用户身份。

[0116] 在此情况下，用户终端装置200可向其他用户的用户终端装置200-1传输从内容钱包装置100传输的用户身份，由此，可以相互执行基于去中心化身份(Decentralized identity)的身份认证。

[0117] 例如，若从供给内容的用户终端装置200向其他用户终端装置200-1传输从内容钱

包装置100传输的非激活的用户身份(去中心化身份)及加密的内容,则在其他用户终端装置200-1中传输自我身份认证值(SSI,Self-Sovereign identity),由此可以针对供给方执行对于对应个别需要的用户身份认证。

[0118] 当然,与此相反,其他用户可向用户终端装置200-1输入通过自己的内容钱包装置100-1随机生成的密码,若从内容钱包装置100-1传递的密码及通过用户终端装置200-1的用户输入的密码相同,则可以向用户终端装置200-1传输自己所有的内容,可以向其他用户终端装置200直接传输。

[0119] 如上所述,针对不同用户所有的内容,以通过内容钱包装置100、100-1及用户终端装置200、200-1随机生成的密码证明是否为正当的用户之后,可直接传输用户身份及内容,由此可以防止第三方的盗取及内容的非法流出。

[0120] 参照图1及图6,若存储卡300及内容钱包装置100电连接,则包括内容钱包装置100的系统10可以向用户终端装置200传输用于断开用户终端装置200的网络的信号,若输入与所传输的信号对应的用户操作,则用户终端装置200可断开网络。

[0121] 在此情况下,断开的网络可以为用户终端装置200的外部通信网,例如,近距离通信(LAN,Local Area Network)、城域网(MAN,Metropolitan Area Network)、广域网(WAN,Wide Area Network)等。

[0122] 具体地,例如,当用户终端装置200为移动终端装置时,通信部110可以向移动终端装置传输询问是否转换飞行模式的消息,可通过用户的操作选择是否转换为飞行模式。

[0123] 在此情况下,若用户选择转换为飞行模式,则断开作为移动终端装置的外部通信网的网络,可通过基于有线的直接连接或在规定范围内基于无线的间接连接仅执行内容钱包装置100及用户终端装置200之间的通信。

[0124] 图7为用于说明利用图6的内容钱包装置的系统的流程的图。

[0125] 参照图7,利用内容钱包装置的系统10可依次进行如下步骤:步骤S100,向内容钱包装置插入存储卡;步骤S200,判断所插入的存储卡是否与内容钱包装置连接;步骤S300,从内容钱包装置向用户终端装置传输用于断开网络的信号;步骤S400,判断是否断开用户终端装置的网络;步骤S500,从内容钱包装置向用户终端装置传输加密数据;步骤S600,确认内容钱包装置与用户终端装置之间随机生成的密码是否相同;以及步骤S700,在内容钱包装置中加密内容来向用户终端传输。

[0126] 向内容钱包装置插入存储卡的步骤S100为向内容钱包装置插入存储内容的存储卡的步骤,之后可进行所插入的存储卡与内容钱包装置是否连接的步骤S200。

[0127] 在此情况下,所插入的存储卡与内容钱包装置是否连接的步骤S200可以为通过物理变化来判断存储卡与内容钱包装置是否电连接的步骤。

[0128] 当存储卡与内容钱包装置并未电连接时,利用内容钱包装置的系统不进行向用户终端传输内容的步骤。

[0129] 相反,当存储卡与内容钱包装置电连接时,可进行从内容钱包装置向用户终端装置传输用于断开网络的信号的步骤S300。

[0130] 从内容钱包装置向用户终端装置传输用于断开网络的步骤S300可以为如下步骤,即,可以传输断开作为用户终端装置为了与其他电子设备的通信而使用的外部通信网的网络。

[0131] 若向用户终端装置正常传递断开网络的信号，则可通过用户操作选择是否断开网络。

[0132] 判断是否断开用户终端装置的网络的步骤S400可以为如下的步骤，即，若通过用户操作选择网络断开，则判断用户终端装置的网络是否正常断开。

[0133] 若用户终端装置的网络并未正常断开，则回到判断所插入的存储卡是否与内容钱包装置连接的步骤S200来判断存储卡与内容钱包装置是否电连接。

[0134] 相反，若用户终端装置的网络被正常断开，则可以进行从内容钱包装置向用户终端装置传输加密数据的步骤S500。

[0135] 在此情况下，加密数据可以为包含用户身份及随机生成的密码的数据。

[0136] 从内容钱包装置向用户终端装置传输随机生成的密码的步骤S500可以为如下步骤，即，若存储卡及内容钱包装置之间正常连接，则在内容钱包装置中所包括的加密部随机生成密码，向用户终端装置传输随机生成的密码。

[0137] 在此情况下，随机生成的密码和用户身份也可一同传输到用户终端装置。

[0138] 如上所述，若向用户终端装置传输随机生成的密码，则进行确认内容钱包装置与用户终端装置之间的随机生成的密码是否相同的步骤S600。

[0139] 在确认在内容钱包装置与用户终端装置之间的随机生成的密码是否相同的步骤S600中，若向用户终端装置传输的随机生成的密码通过用户的操作输入到用户终端装置，则所输入的密码传输到内容钱包装置，并匹配所传输的密码及在内容钱包装置中随机生成的密码。

[0140] 若所匹配的密码不相同，则进行判断所插入的存储卡与内容钱包装置是否连接的步骤S200，在存储卡与内容钱包装置重新电连接的过程中将之前随机生成的密码初始化并随机生成其他密码。

[0141] 相反，若所匹配的密码相同，则进行在内容钱包装置中加密内容并向用户终端传输的步骤S700。

[0142] 在内容钱包装置中加密内容来向用户终端传输的步骤S700可以为如下的步骤，即，加密存储在存储卡的内容，同时，以使内容的原作者需要传输的其他用户或正常购买内容的用户可以正常利用内容的方式可一同传输能够解密所加密的内容的解密秘钥。

[0143] 在此情况下，加密的内容为了区分内容的原作者而插入用户固有的识别码来传输。

[0144] 图8为用于说明利用本发明另一实施例的内容钱包装置的系统的图。

[0145] 参照图8，利用内容钱包装置的系统10可以向具有用户终端装置200、200-1、200-2、200-3、200-4、200-5的用户之间直接无偿或有偿传输内容，在多个用户终端装置200、200-1、200-2、200-3、200-4、200-5利用内容钱包装置100、100-1、100-2、100-3、100-4、100-5，由此可以轻松接收用户所需要的内容。

[0146] 在此情况下，在多个用户终端装置200、200-1、200-2、200-3、200-4、200-5中的一个用户终端装置200中，通过内容钱包装置100执行用户认证之后，若向网络传输加密的内容，则网络可以提供加密内容的预览或相关信息。

[0147] 因此，当观察通过多个用户所具有的用户终端装置200-1、200-2、200-3、200-4、200-5加密的内容的预览或相关信息来需要购买时，支付加密的内容有关的费用，若支付完

费用，则具有加密的内容的原作者可以向其他用户终端装置200-1、200-2、200-3、200-4、200-5一同传输加密的内容及解密秘钥。

[0148] 其中，可以在分布式账本中制作使用内容钱包装置100、100-1、100-2、100-3、100-4、100-5的用户终端装置200、200-1、200-2、200-3、200-4、200-5之间的购买历史及传输历史等。

[0149] 分布式账本可基于通常使用的区块链，通过使用分布式账本，可利用本发明的内容钱包装置100来存储收发内容的所有历史。

[0150] 并且，分布式账本可存储一个用户通过从各个内容钱包装置100、100-1、100-2、100-3、100-4、100-5传输的用户身份的购买历史及传输历史等。

[0151] 在此情况下，如上所述，所使用的用户身份为各个内容钱包装置100、100-1、100-2、100-3、100-4、100-5的用户自身所有的用户认证身份，即，去中心化身份。

[0152] 由此，各个用户可以阅览通过分布式账本存储的所有历史，并可轻松了解由哪个用户购买及传输等，从而可以实现透明的交易。

[0153] 并且，由于使用去中心化身份，由此，用户本人可以直接管理用户认证方法，而并非由中心服务器管理身份信息。

[0154] 换句话说，例如，若存储在存储卡的内容为视频，则可从需要供给上述视频的用户终端装置200向需要购买的用户终端装置200-1、200-2、200-3、200-4、200-5传输用户的身份认证所需要的去中心化身份。

[0155] 之后，若从需要购买的用户终端装置200-1、200-2、200-3、200-4、200-5传输身份认证值(SSI)并成立用户身份认证，则被加密成并未完全公开的形态的视频将与解密秘钥一同传输到需要购买的用户终端装置200-1、200-2、200-3、200-4、200-5。

[0156] 在这种过程中，供给视频的用户终端装置200的供给记录、需要购买的用户终端装置200-1、200-2、200-3、200-4、200-5的购买历史等均可存储在各个用户终端装置200、200-1、200-2、200-3、200-4、200-5的分布式账本数据。

[0157] 以上，虽然示出并说明了本发明的优选实施例，本发明并不局限于上述特定实施例，在不超出发明要求保护范围所保护的本发明的主旨的情况下，本发明所属技术领域的普通技术人员可进行多种变形实施，这种变形实施应不能从本发明的技术思想或展望单独理解。

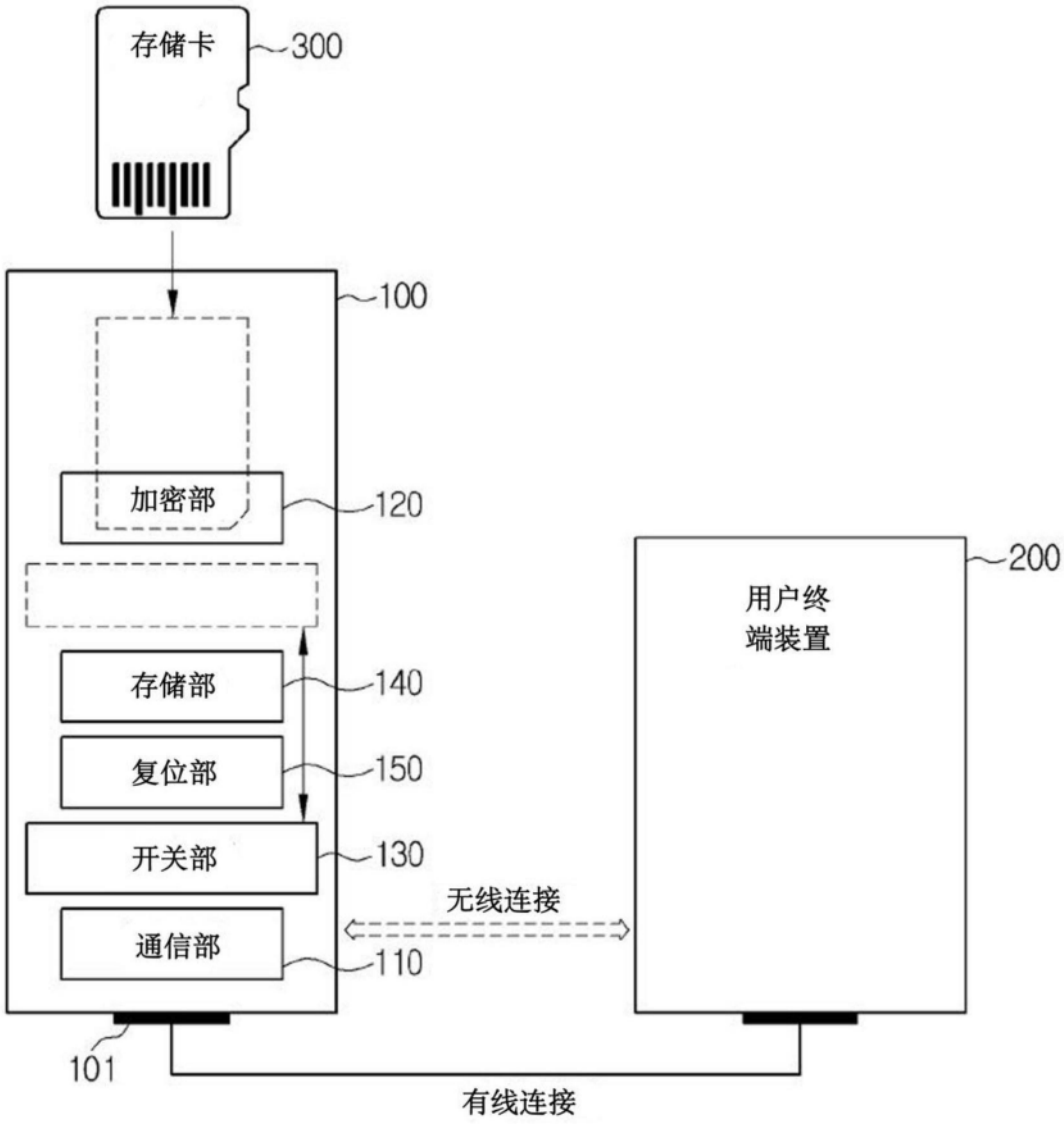

存储卡
300
100
加密部
120
200
用户终
端装置
存储部
140
复位部
150
开关部
130
无线连接
通信部
110
101
有线连接

图1

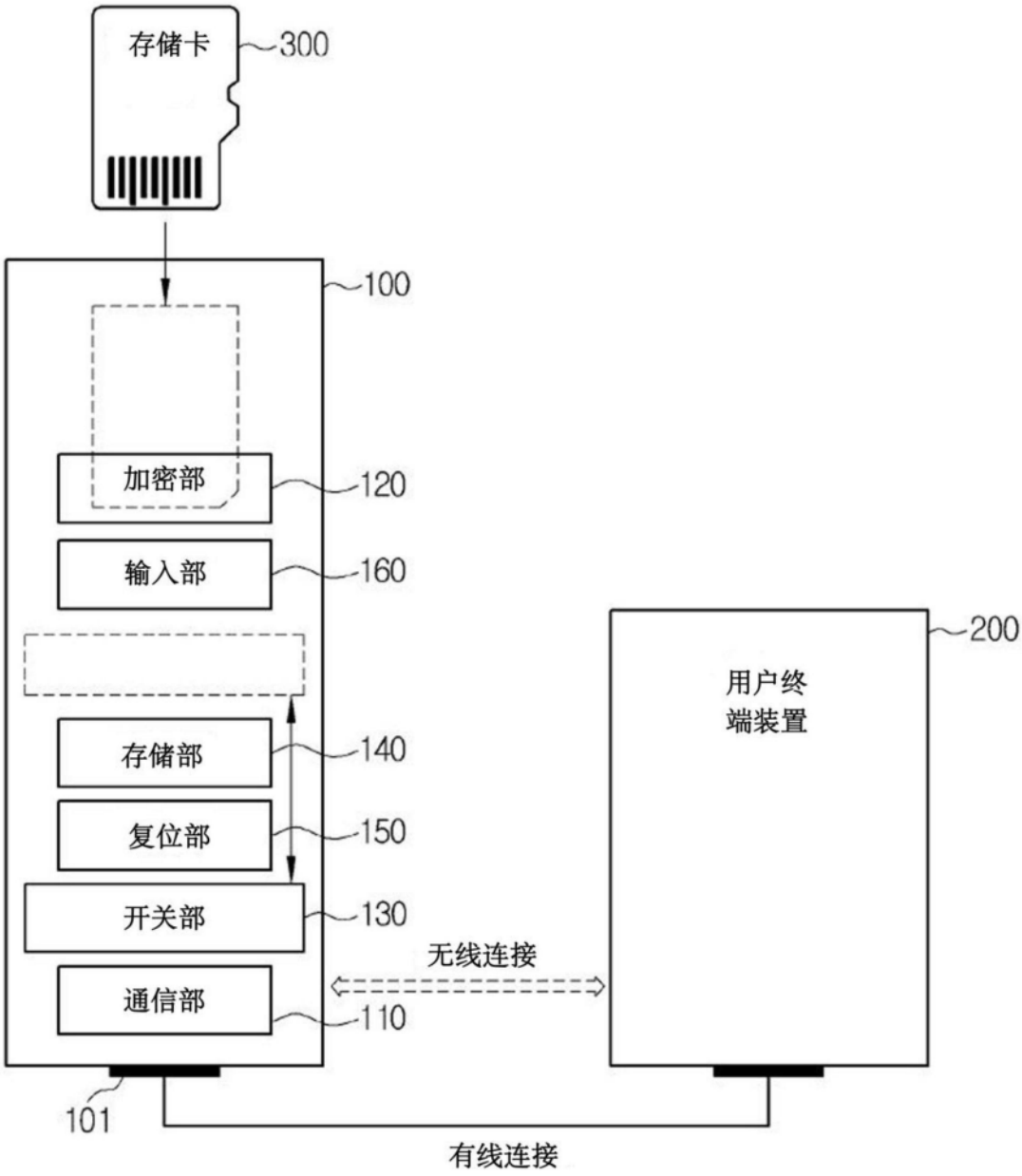
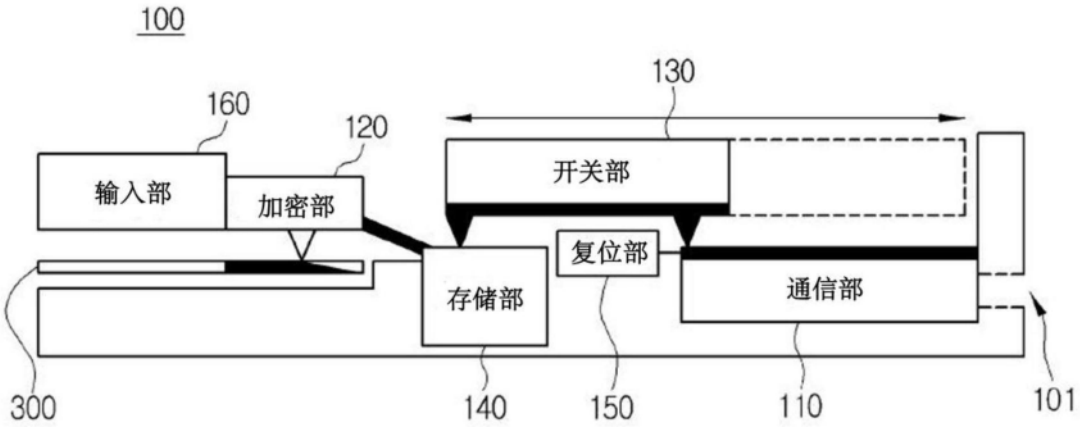
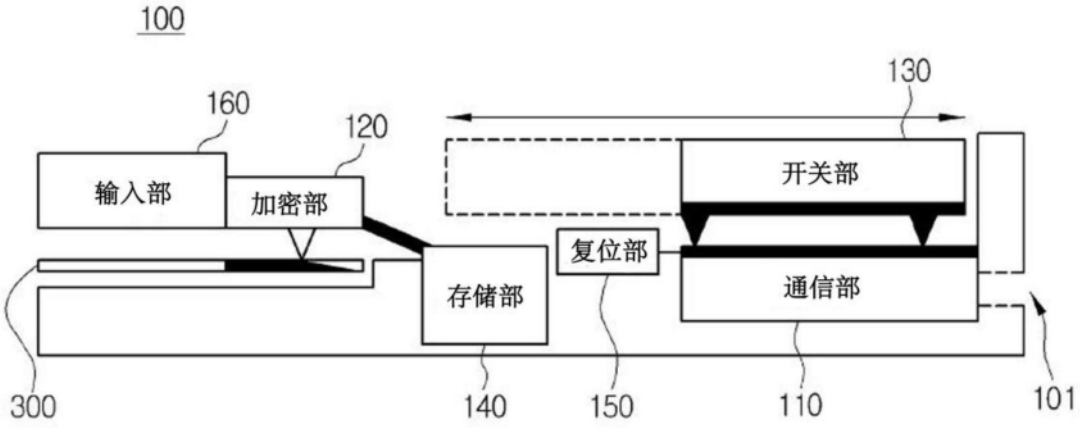

存储卡
300
100
加密部
120
输入部
160
存储部
140
复位部
150
开关部
130
通信部
110
101
无线连接
200
用户终
端装置
有线连接

图2


100
160
120
130
输入部
加密部
开关部
复位部
存储部
通信部
300
140
150
110
101

(a)


100
160
120
130
输入部
加密部
开关部
复位部
存储部
通信部
300
140
150
110
101

(b)

图3

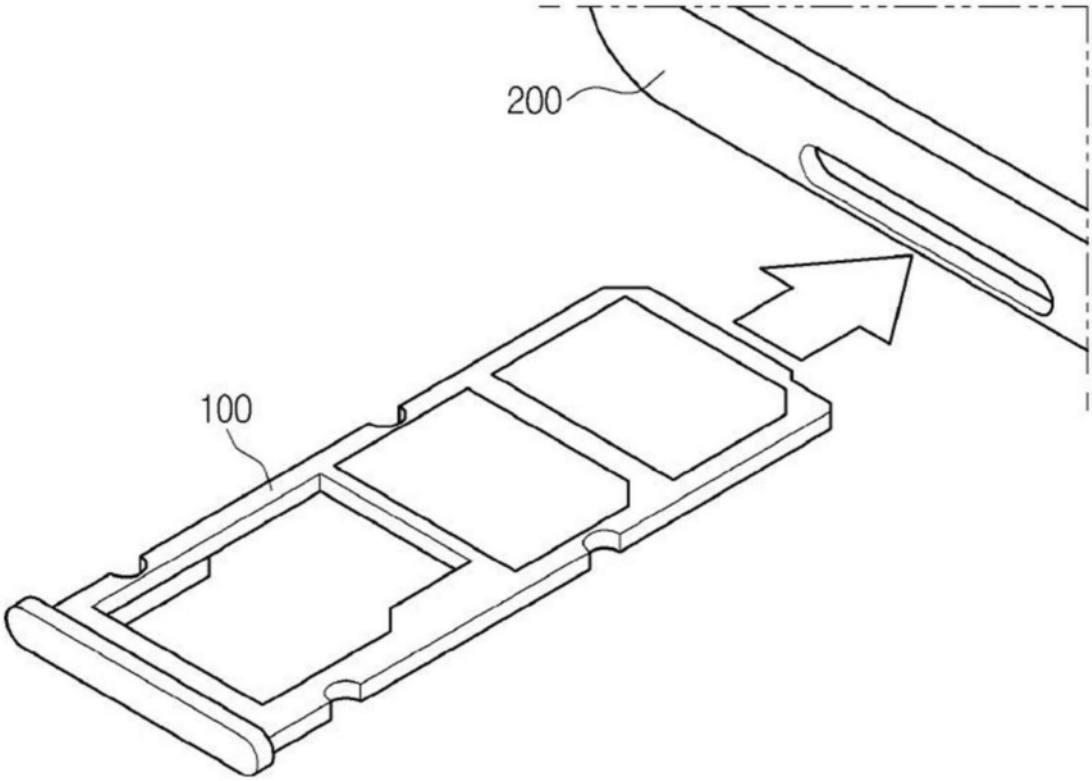


图4

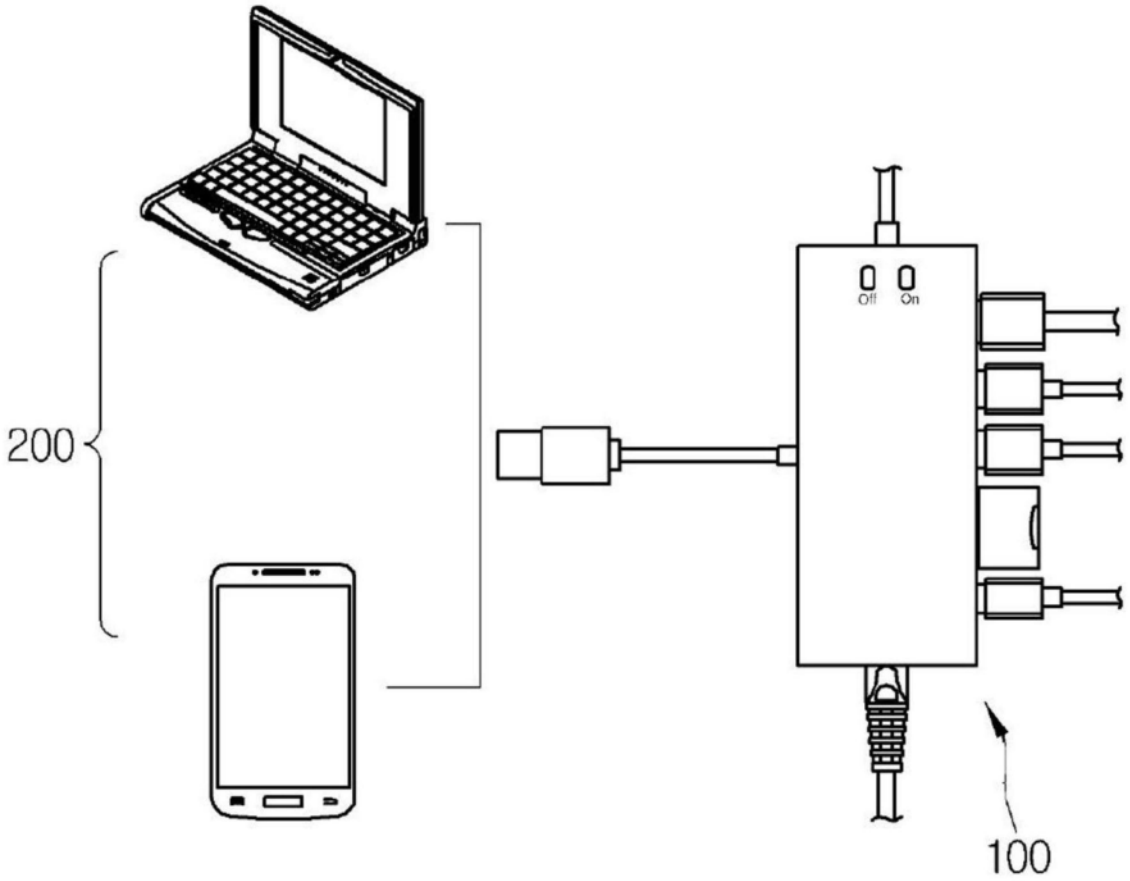


图5

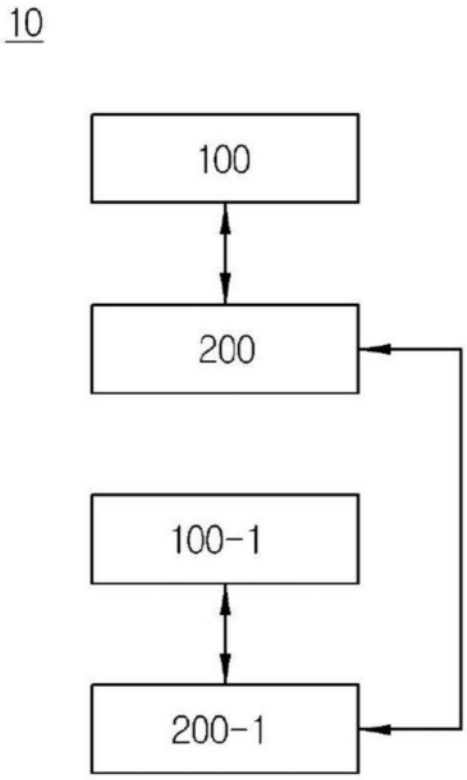


图6

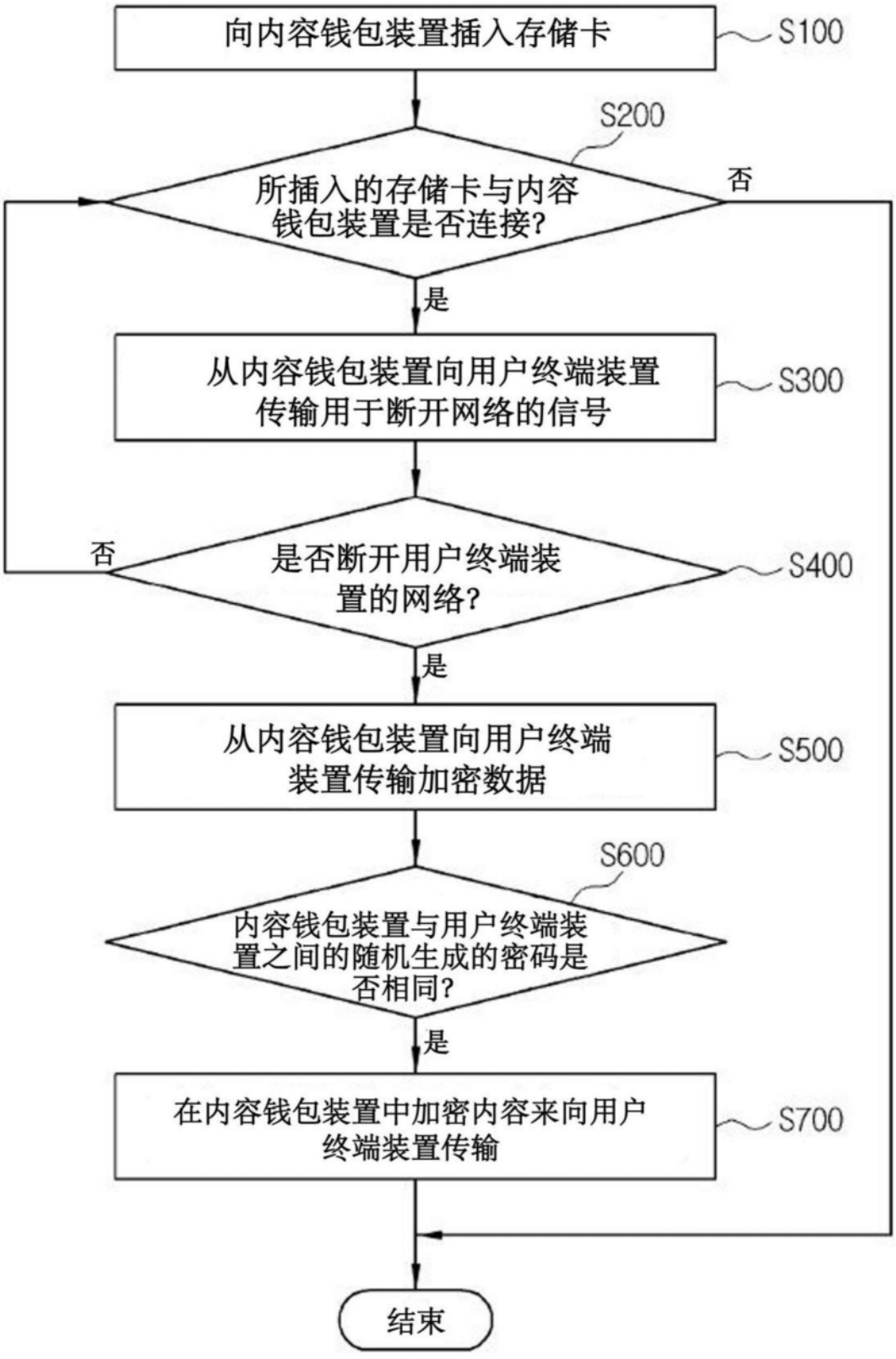

向内容钱包装置插入存储卡
S100
S200
所插入的存储卡与内容钱包装置是否连接?
否
是
从内容钱包装置向用户终端装置传输用于断开网络的信号
S300
否
是否断开用户终端装置的网络?
S400
是
从内容钱包装置向用户终端装置传输加密数据
S500
S600
内容钱包装置与用户终端装置之间的随机生成的密码是否相同?
是
在内容钱包装置中加密内容来向用户终端装置传输
S700
结束

图7

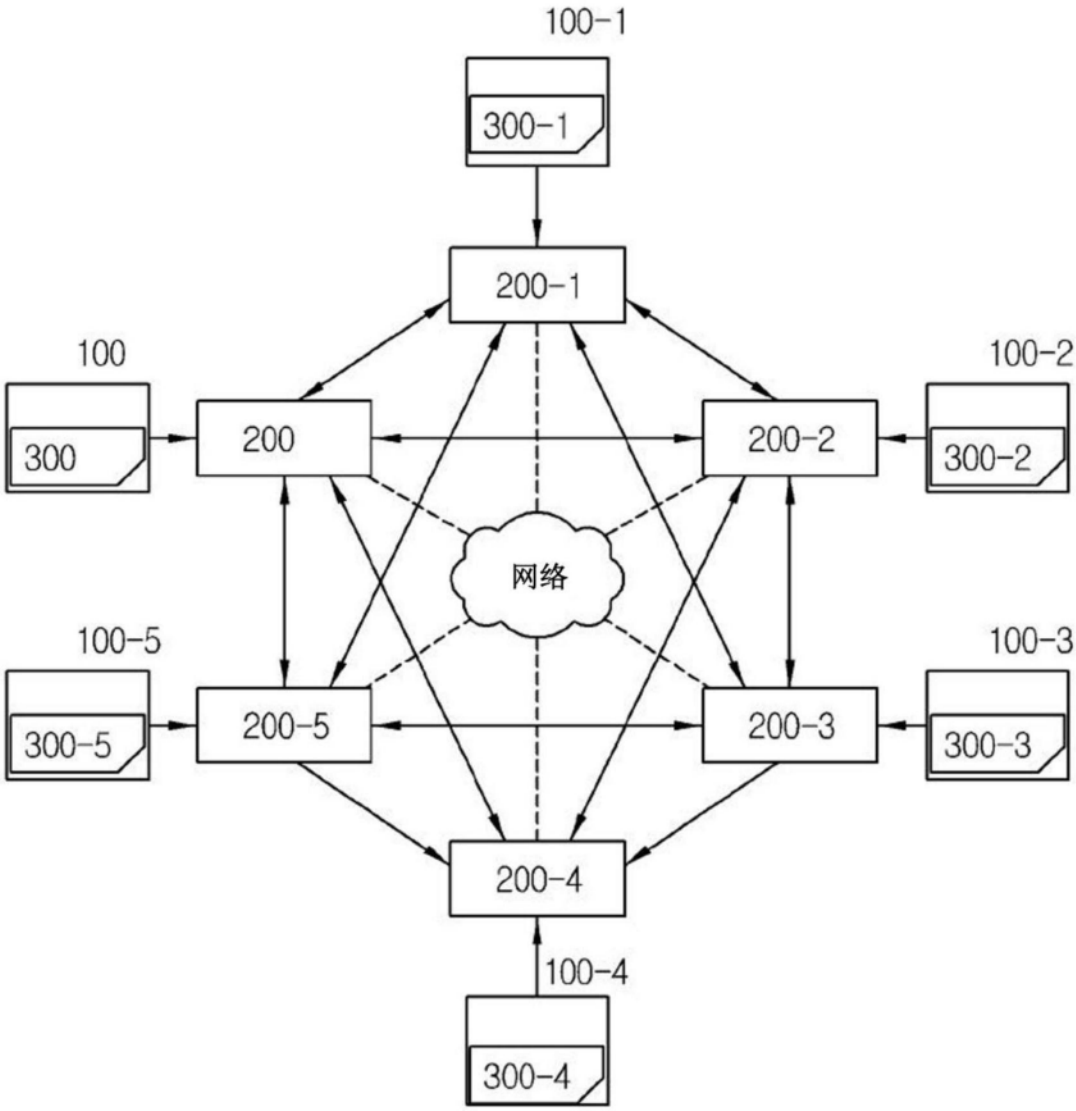

100-1
300-1
200-1
100
300
200
100-2
200-2
300-2
网络
100-5
300-5
200-5
100-3
200-3
300-3
200-4
100-4
300-4

图8