权利要求书

1、一种基于近场通信NFC便携设备的支付方法，包括:

所述NFC便携设备获取NFC写入信息，所述NFC写入信息包括密钥对标识和对应的公钥;

当进入消费机具的NFC通信范围时，接收所述消费机具发送的消费金额信息;

利用所述公钥，对所述消费金额信息加密得到加密信息;

将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

2、如权利要求1所述的方法，所述密钥对标识及其对应的密钥对由所述服务端预先生成，并下发所述密钥对标识和所述密钥对中的所述公钥，再由NFC写入端将所述下发的信息写入所述NFC便携设备中。

3、如权利要求1所述的方法，所述NFC写入信息还包括关联于所述密钥对标识的用户账户的账户识别信息;

所述将所述加密信息和所述密钥对标识发送给所述消费机具，还包括:

将所述账户识别信息发送给所述消费机具，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

4、如权利要求1所述的方法，所述利用所述公钥，对所述消费金额信息加密得到加密信息，具体包括:

获取当前时间;

利用所述公钥，对所述消费金额信息和所述当前时间加密得到加密信息;

其中，所述当前时间用于所述服务端在所述扣款前进行时效性校验。

5、如权利要求1~4任一项所述的方法，所述NFC便携设备为支持NFC的可穿戴设备或者卡片。

6、一种针对近场通信 NFC 便携设备的写入方法，包括:

NFC 写入端获取用户账户关联的密钥对标识和对应的密钥对中的公钥;

将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

7、如权利要求 6 所述的方法，所述获取用户账户关联的密钥对标识和对应的密钥对中的公钥，具体包括:

请求服务端生成关联于用户账户的密钥对标识和对应的密钥对;

接收所述服务端返回的所述密钥对标识和所述密钥对中的公钥;

其中，当所述 NFC 便携设备通过所述用户账户支付时，由所述服务端扣款。

8、如权利要求 7 所述的方法，所述获取用户账户关联的密钥对标识和对应的密钥对中的公钥，还包括:

获取所述用户账户的账户识别信息;

所述将所述密钥对标识和所述公钥写入所述 NFC 便携设备中,还包括:

将所述账户识别信息写入所述 NFC 便携设备中，以用于所述服务端查找所述密钥对中的私钥用于所述扣款。

9、如权利要求 6 所述的方法，所述方法还包括:

请求所述服务端解除所述用户账户与所述密钥对标识之间的关联关系，若所述关联关系解除，则所述 NFC 便携设备不能够基于所述密钥对标识成功支付。

10、一种基于近场通信 NFC 便携设备的支付方法，包括:

消费机具当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息;

接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中;

将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端

解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

11、如权利要求 10 所述的方法，所述接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，还包括:

接收所述 NFC 便携设备发送的所述用户账户的账户识别信息，所述账户识别信息被预先写入所述 NFC 便携设备中;

所述将所述加密信息和所述密钥对标识发送给服务端，还包括:

将所述账户识别信息发送给所述服务端，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

12、如权利要求 10 所述的方法，所述将所述加密信息和所述密钥对标识发送给服务端，还包括:

将相应的业务场景信息发送给所述服务端，以用于生成相应的业务单据。

13、一种基于近场通信 NFC 便携设备的支付方法，包括:

服务端接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述 NFC 便携设备利用所述密钥对标识对应的公钥加密生成，并通过 NFC 通信方式发送给所述消费机具;

根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息;

根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

14、如权利要求 13 所述的方法，所述接收消费机具发送的密钥对标识和包含消费金额信息的加密信息前，所述方法还包括:

预先生成所述密钥对标识及其对应的密钥对，并与所述用户账户进行关联;

下发所述密钥对标识和所述密钥对中的所述公钥，以用于 NFC 写入端

将所述下发的信息写入所述NFC便携设备中。

15、如权利要求14所述的方法，所述接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，还包括:

接收所述消费机具发送的所述用户账户的账户识别信息，所述账户识别信息由NFC便携设备通过NFC通信方式发送给所述消费机具;

所述根据所述密钥对标识，确定所述密钥对标识对应的私钥，具体包括:

根据所述账户识别信息，确定所述用户账户对应的各密钥对标识;

根据所述各密钥对标识和所述消费机具发送的密钥对标识，确定所述消费机具发送的密钥对标识对应的私钥。

16、如权利要求13所述的方法，所述加密信息中还包括所述NFC便携设备获取的当前时间;

所述根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款前，所述方法还包括:

根据服务端时间确定所述当前时间尚具有时效性。

17、一种基于近场通信NFC便携设备的支付装置，所述装置位于所述NFC便携设备，包括:

获取模块，获取NFC写入信息，所述NFC写入信息包括密钥对标识和对应的公钥;

接收模块，当进入消费机具的NFC通信范围时，接收所述消费机具发送的消费金额信息;

加密模块，利用所述公钥，对所述消费金额信息加密得到加密信息;

发送模块，将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

18、如权利要求17所述的装置，所述密钥对标识及其对应的密钥对由所述服务端预先生成，并下发所述密钥对标识和所述密钥对中的所述公钥，

再由 NFC 写入端将所述下发的信息写入所述 NFC 便携设备中。

19、如权利要求 17 所述的装置，所述 NFC 写入信息还包括关联于所述密钥对标识的用户账户的账户识别信息;

所述发送模块将所述加密信息和所述密钥对标识发送给所述消费机具，还包括:

所述发送模块将所述账户识别信息发送给所述消费机具，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

20、如权利要求 17 所述的装置，所述加密模块利用所述公钥，对所述消费金额信息加密得到加密信息，具体包括:

所述加密模块获取当前时间;

利用所述公钥，对所述消费金额信息和所述当前时间加密得到加密信息;

其中，所述当前时间用于所述服务端在所述扣款前进行时效性校验。

21、如权利要求 17~20 任一项所述的装置，所述 NFC 便携设备为支持 NFC 功能的可穿戴设备或者卡片。

22、一种针对近场通信 NFC 便携设备的写入装置，所述装置位于 NFC 写入端，包括:

获取模块，获取用户账户关联的密钥对标识和对应的密钥对中的公钥;

写入模块，将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

23、如权利要求 22 所述的装置，所述获取模块获取用户账户关联的密钥对标识和对应的密钥对中的公钥，具体包括:

所述获取模块请求服务端生成关联于用户账户的密钥对标识和对应的密钥对;

接收所述服务端返回的所述密钥对标识和所述密钥对中的公钥;

其中，当所述 NFC 便携设备通过所述用户账户支付时，由所述服务端扣款。

24、如权利要求 23 所述的装置，所述获取模块获取用户账户关联的密钥对标识和对应的密钥对中的公钥，还包括:

所述获取模块获取所述用户账户的账户识别信息;

所述写入模块将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，还包括:

所述写入模块将所述账户识别信息写入所述 NFC 便携设备中，以用于所述服务端查找所述密钥对中的私钥用于所述扣款。

25、如权利要求 22 所述的装置，所述装置还包括:

解除模块，请求所述服务端解除所述用户账户与所述密钥对标识之间的关联关系，若所述关联关系解除，则所述 NFC 便携设备不能够基于所述密钥对标识成功支付。

26、一种基于近场通信 NFC 便携设备的支付装置，所述装置位于消费机具，包括:

第一发送模块，当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息;

接收模块，接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中;

第二发送模块，将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

27、如权利要求 26 所述的装置，所述接收模块接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，还包括:

所述接收模块接收所述 NFC 便携设备发送的所述用户账户的账户识别信息，所述账户识别信息被预先写入所述 NFC 便携设备中;

所述第二发送模块将所述加密信息和所述密钥对标识发送给服务端，

还包括:

所述第二发送模块将所述账户识别信息发送给所述服务端，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

28、如权利要求 26 所述的装置，所述第二发送模块将所述加密信息和所述密钥对标识发送给服务端，还包括:

所述第二发送模块将相应的业务场景信息发送给所述服务端，以用于生成相应的业务单据。

29、一种基于近场通信 NFC 便携设备的支付装置，所述装置位于服务端，包括:

接收模块，接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述 NFC 便携设备利用所述密钥对标识对应的公钥加密生成，并通过 NFC 通信方式发送给所述消费机具;

确定模块，根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息;

扣款模块，根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

30、如权利要求 29 所述的装置，所述装置还包括:

关联下发模块，在所述接收模块接收消费机具发送的密钥对标识和包含消费金额信息的加密信息前，预先生成所述密钥对标识及其对应的密钥对，并与所述用户账户进行关联;

下发所述密钥对标识和所述密钥对中的所述公钥，以用于 NFC 写入端将所述下发的信息写入所述 NFC 便携设备中。

31、如权利要求 30 所述的装置，所述接收模块接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，还包括:

所述接收模块接收所述消费机具发送的所述用户账户的账户识别信息，所述账户识别信息由所述NFC便携设备通过NFC通信方式发送给所述消费机具;

所述确定模块根据所述密钥对标识，确定所述密钥对标识对应的私钥，具体包括:

所述确定模块根据所述账户识别信息，确定所述用户账户对应的各密钥对标识;

根据所述各密钥对标识和所述消费机具发送的密钥对标识，确定所述消费机具发送的密钥对标识对应的私钥。

32、如权利要求 29 所述的装置，所述加密信息中还包括所述 NFC 便携设备获取的当前时间;

所述扣款模块根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款前，还执行:

所述扣款模块根据服务端时间确定所述当前时间尚具有时效性。

33、一种基于近场通信 NFC 便携设备的支付设备，所述设备为所述 NFC 便携设备，包括:

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够:

获取NFC写入信息，所述NFC写入信息包括密钥对标识和对应的公钥;

当进入消费机具的 NFC 通信范围时，接收所述消费机具发送的消费金额信息;

利用所述公钥，对所述消费金额信息加密得到加密信息;

将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

34、一种针对近场通信 NFC 便携设备的写入设备，所述设备为 NFC 写入端，包括:

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

获取用户账户关联的密钥对标识和对应的密钥对中的公钥；

将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

35、一种基于近场通信 NFC 便携设备的支付设备，所述设备为消费机具，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息；

接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中；

将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

36、一种基于近场通信 NFC 便携设备的支付设备，所述设备为消费机具，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所

述加密信息由所述NFC便携设备利用所述密钥对标识对应的公钥加密生成，并通过NFC通信方式发送给所述消费机具；

根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息；

根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。