

(19) 中华人民共和国国家知识产权局



(12) 发明专利申请

(10) 申请公布号 CN 103927656 A

(43) 申请公布日 2014. 07. 16

(21) 申请号 201410185649. 5

(22) 申请日 2014. 05. 05

(71) 申请人 宋骊平

地址 710000 陕西省西安市太白南路 2 号西安电子科技大学 133 信箱

(72) 发明人 宋骊平 赵万明

(74) 专利代理机构 西安亿诺专利代理有限公司

61220

代理人 康凯

(51) Int. Cl.

G06Q 20/36(2012. 01)

G06Q 20/10(2012. 01)

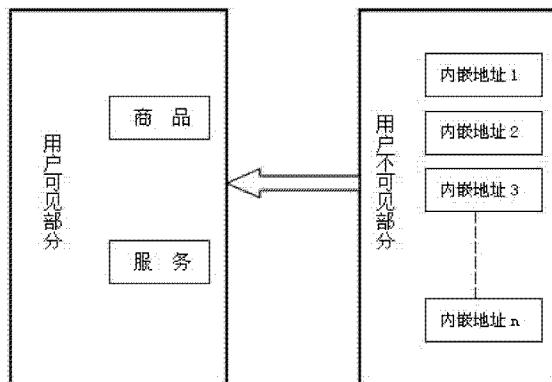
权利要求书1页 说明书4页 附图1页

(54) 发明名称

一种内嵌固定收款地址的比特币终端钱包及其比特币支付方法

(57) 摘要

一种内嵌固定收款地址的比特币终端钱包及其比特币支付方法，该比特币手机钱包内嵌比特币收款地址；所述比特币收款地址即为比特币公钥，由一串二进制代码组成，还有与所述比特币公钥相适应的比特币私钥，只有获得比特币私钥，才能支付比特币公钥上的比特币；所述比特币公钥和比特币私钥通过椭圆曲线加密算法成对生成。本发明内嵌了固定收款地址的比特币手机钱包可以用来作为一种比特币支付工具，实现购买各种商品和服务；公司、企业、商家或者个人可以按照自己要求开发出内嵌固定收款地址的比特币手机钱包，然后消费者可以很方便的安装到终端上用来购买商品或者服务。



1. 一种内嵌固定收款地址的比特币终端钱包,其特征在于:所述比特币手机钱包内嵌比特币收款地址;所述比特币收款地址即为比特币公钥,由一串二进制代码组成,还有与所述比特币公钥相适应的比特币私钥,只有获得比特币私钥,才能支付比特币公钥上的比特币;所述比特币公钥和比特币私钥通过椭圆曲线加密算法成对生成。

2. 根据权利要求1所述内嵌固定收款地址的比特币终端钱包,其特征在于:所述内嵌的比特币地址就是提供比特币付费服务的公司、企业或者个人的比特币收款帐号。

3. 一种利用权利要求2所述比特币终端钱包的比特币支付方法,其特征在于,包括以下步骤:

1) 提供一个处理器,该处理器将比特币与相应的商品和服务按照既定的汇率转换和相应运行;

2) 比特币终端钱包内嵌比特币收款地址,按照该比特币收款地址,终端使用者能将比特币支付到提供比特币付费服务的公司、企业或者个人;

3) 按照既定的汇率转换和相应运行是指处理器接受和处理提供比特币付费服务的公司、企业或者个人收到相应比特币后,按照既定的汇率转换提供给终端相应的商品和服务;实际是在终端点击相应购买按钮时,处理器调用发送比特币的函数,该函数首先嵌入固定的比特币地址,其后生成一个包含比特币数量和该固定比特币地址的请求,然后把这个请求广播出去,至此处理器完成比特币的发送;

4) 将相应的商品和服务信息的结果链接到终端,完成支付的过程。

4. 根据权利要求3所述比特币支付方法,其特征在于,在步骤4)之后还包括步骤5):如果支付出错,处理器应终端的请求调用发送比特币的函数,该函数首先生成一个请求,该请求包含终端支付的比特币数量和支付该笔比特币的地址,然后把这个请求广播出去,可实现比特币的退还。

5. 根据权利要求3或4所述比特币支付方法,其特征在于:所述既定的汇率是比特币终端钱包开发者制定的比特币和相应的商品和服务的价值比率。

6. 根据权利要求5所述比特币支付方法,其特征在于:所述将结果链接到终端是指终端支付相应数量的比特币应该得到相应的商品和服务,并生成到终端。

7. 根据权利要求6所述比特币支付方法,其特征在于:所述相应的商品和服务包括购物网站上各种商品和话费充值、Q币兑换。

8. 根据权利要求7所述比特币支付方法,其特征在于:所述比特币收款地址为物理地址或虚拟地址。

9. 根据权利要求8所述比特币支付方法,其特征在于:所述物理地址或虚拟地址为物理地址1~n或虚拟地址1~n。

10. 根据权利要求9所述比特币支付方法,其特征在于:所述终端包括手机、平板计算机以及计算机。

一种内嵌固定收款地址的比特币终端钱包及其比特币支付方法

技术领域

[0001] 本发明属于软件技术领域，具体涉及内嵌固定收款地址的比特币手机钱包及其支付方法。

背景技术

[0002] 比特币诞生于 2009 年，是一种基于 P2P 网络的虚拟货币，比特币手机钱包是一种在手机上运行的用来管理比特币的软件。现有的比特币钱包软件功能比较基础，只是用来保存用户的比特币地址和私钥信息、接收他人发送的比特币、将自己帐户上的比特币发送给他人，是一种一对一式的支付方式。近年来，移动终端支付作为一种快捷便利的支付手段，已经得到了广泛的应用，比特币作为一种虚拟货币也越来越为人们所接受，一些商家开始接受比特币作为支付货币，但现有的比特币钱包功能单一，只能实现一对一式的支付方式，难以和现有的移动终端支付结合，进而难以被商家或个人专门用来作为一种支付工具使用。因此，将比特币和移动支付终端结合实现类似于货币的支付方式是一种全新的需求。

发明内容

[0003] 本发明的目的在于提供一种内嵌固定收款地址的比特币终端钱包及其比特币支付方法，其针对现有比特币终端钱包的不足，将固定收款地址内嵌于比特币终端钱包，将比特币和终端结合实现类似于货币的支付，购买各种商品和服务。

[0004] 本发明的技术解决方案是：

一种内嵌固定收款地址的比特币终端钱包，其特殊之处在于：所述比特币手机钱包内嵌比特币收款地址；所述比特币收款地址即为比特币公钥，由一串二进制代码组成，还有与所述比特币公钥相适应的比特币私钥，只有获得比特币私钥，才能支付比特币公钥上的比特币；所述比特币公钥和比特币私钥通过椭圆曲线加密算法(ECC :Elliptic Curves Cryptography)成对生成。椭圆曲线加密算法属于公钥加密算法的一种。

[0005] 上述内嵌的比特币地址就是提供比特币付费服务的公司、企业或者个人的比特币收款帐号。

[0006] 一种利用上述比特币终端钱包的比特币支付方法，其特殊之处在于，包括以下步骤：

- 1) 提供一个处理器，该处理器将比特币与相应的商品和服务按照既定的汇率转换和相应运行；
- 2) 比特币终端钱包内嵌比特币收款地址，按照该比特币收款地址，终端使用者能将比特币支付到提供比特币付费服务的公司、企业或者个人；
- 3) 按照既定的汇率转换和相应运行是指处理器接受和处理提供比特币付费服务的公司、企业或者个人收到相应比特币后，按照既定的汇率转换提供给终端相应的商品和服务；实际是在终端点击相应购买按钮时，处理器调用发送比特币的函数，该函数首先嵌入固定

的比特币地址,其后生成一个包含比特币数量和该固定比特币地址的请求,然后把这个请求广播出去,至此处理器完成比特币的发送;

上述函数可根据使用者的需求在完成上述功能的条件下,自行编程设计。

[0007] 例如,在 Java 中,这个函数的核心代码如下:

```
function (String adress, String amount)
{
    Address inlineAddress = new Address (Constants.NETWORK_PARAMETERS,
"adress");
    // 将固定的比特币地址嵌入
    final SendRequest sendRequest = SendRequest.to(inlineaddress, amount);
    // 生成包含比特币数量和固定比特币地址的请求
    Transaction transaction = wallet.sendCoinsOffline(sendRequest);
    // 将该请求广播出去,完成比特币的发送
}
```

4) 将相应的商品和服务信息的结果链接到终端,完成支付的过程。

[0008] 上述比特币支付方法,其特殊之处在于,在步骤 4) 之后还包括步骤 5):如果支付出错,处理器应终端的请求调用发送比特币的函数,该函数首先生成一个请求,该请求包含终端支付的比特币数量和支付该笔比特币的地址,然后把这个请求广播出去,可实现比特币的退还。

[0009] 上述既定的汇率是比特币终端钱包开发者制定的比特币和相应的商品和服务的价值比率。

[0010] 上述将结果链接到终端是指终端支付相应数量的比特币应该得到相应的商品和服务,并生成到终端。

[0011] 上述相应的商品和服务包括购物网站上各种商品和话费充值、Q 币兑换。

[0012] 上述比特币收款地址为物理地址或虚拟地址。

[0013] 上述物理地址或虚拟地址为物理地址 1 ~ n 或虚拟地址 1 ~ n。

[0014] 上述终端包括手机、平板计算机以及计算机。

[0015] 本发明的有益效果是:内嵌了固定收款地址的比特币手机钱包可以用来作为一种比特币支付工具,实现购买各种商品和服务;公司、企业、商家或者个人可以按照自己要求开发出内嵌固定收款地址的比特币手机钱包,然后消费者可以很方便的安装到终端上用来购买商品或者服务。

附图说明

[0016] 图 1 内嵌固定收款地址的比特币手机钱包原理图;

图 2 基于 Bitcoin Wallet 的具有手机话费充值功能的比特币钱包软件界面;

图 3 基于 Bitcoin Wallet 的具有手机话费充值功能的比特币钱包软件充值界面。

具体实施方案

[0017] 为了使本发明所要解决的技术问题、技术方案及有益效果更加清楚明白,以下结

合附图及实施实例,对本发明进行详细的说明。应当说明的是,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0018] 比特币是一种P2P形式的虚拟货币。点对点的传输意味着一个去中心化的支付系统。比特币不依靠特定货币机构发行,它通过特定算法的大量计算产生,比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。

[0019] 参见图1,比特币公钥和比特币私钥通过椭圆曲线加密算法成对生成,只有掌握比特币私钥,才能支付比特币公钥上的比特币,内嵌的地址就是比特币公钥,由一串二进制代码组成,例如:“14WoGxg1ba8VfKeniqGWm8tYgR6h4m53aG”即代表一个比特币地址,比特币数量记录在这一地址上,只有拥有这一地址对应的比特币私钥才拥有该地址上的比特币,因此这一地址可以看作是公司、企业或者个人的银行帐号。内嵌就是把一个或多个比特币地址固化到程序里,在点击相应购买按钮时,调用发送比特币的函数,可产生一个发送比特币的请求,该请求中包含了固化的比特币地址。

[0020] 例如在java中实现程序如下:

```
final Address inlineAddress = new Address (Constants.NETWORK_PARAMETERS,  
"adress");
```

```
final SendRequest sendRequest = SendRequest.to(address, amount);
```

```
Transaction transaction = wallet.sendCoinsOffline(sendRequest);
```

其中Address是bitcoinj库中定义的存放比特币地址的类。bitcoinj是利用java实现Bitcoin协议并且开源的库。

[0021] 而adress就是所谓的内嵌的比特币地址,例如“14WoGxg1ba8VfKeniqGWm8tYgR6h4m53aG”。

[0022] 当客户端使用者购买商品或者服务时,就自动把比特币发到这个内嵌的地址上。

[0023] 实施例1:

在此以“基于Bitcoin Wallet的具有手机话费充值功能的比特币钱包软件”为例说明本发明。参见图2,在Bitcoin Wallet中新增一个“手机充值”菜单项,参见图3,当用户点击此菜单项时会显示话费充值的界面。用户输入充值号码,选择充值面值后,点击确定按钮,程序就会把用户钱包中同等价值的比特币发送到内嵌的比特币地址上。内嵌就是写入程序中的一个或多个固定的比特币地址,内嵌的比特币地址就是提供比特币充话费服务的公司、企业或者个人的比特币收款帐号。当比特币发送出去后,提供比特币充话费服务的公司、企业或者个人就会把话费充到用户手机上。最后提供比特币充话费服务的公司、企业或者个人把软件发布出去,人们就可以使用这个软件实现比特币充话费。

[0024] 实施例2:

Q币是腾讯公司发行的虚拟游戏货币,只能在腾讯公司的游戏中使用,腾讯公司的游戏玩家需要Q币参与游戏,因此Q币充值的需求很大,为了给这些游戏玩家提供方便的充值途径,可以应用本发明开发出Q币充值比特币手机钱包。在Bitcoin Wallet中新增一个“Q币充值”菜单项,当用户点击此菜单项时会显示Q币充值的界面。用户输入需要充值的账

号,选择充值多少个 Q 币后,点击确定按钮,程序就会把用户钱包中同等价值的比特币发送到内嵌的比特币地址上。内嵌就是写入程序中的一个或多个固定的比特币地址,内嵌的比特币地址就是提供比特币充 Q 币服务的公司、企业或者个人的比特币收款帐号。当比特币发送出去后,提供比特币充 Q 币服务的公司、企业或者个人就会把 Q 币充值到用户账号上。

[0025] 实施例 3 :

公司,商家或个人可以开设自己的购物网站,网站可以提供各种商品,除了每种商品的介绍,描述和价格之外,同时提供每个商品对应的二维码供用户扫码支付,用户使用商家提供的内嵌固定收款地址的手机钱包可以购买这些商品。

[0026] 在 Bitcoin Wallet 中新增一个“购物”菜单项,当用户点击此菜单项时会显示购物的界面。用户点击“二维码扫描”,将手机摄像头对准购物网站上自己准备购买的商品的二维码,扫码成功后,在手机界面上,会显示商品名称,货号,价格等信息,以及文本输入框,用户在文本输入框中填写收货地址,点击确定按钮,程序就会把用户钱包中同等价值的比特币发送到内嵌的比特币地址上,内嵌的比特币地址就是购物网站的比特币收款帐号,商家在收到比特币后,即可将指定商品寄往用户填写的收货地址。这样,用户可以省去在购物网站注册个人信息,设置密码,登录,退出等一系列复杂麻烦的手续,使得网上购物更加方便快捷。推出这样免费的内嵌固定收款地址的手机钱包可以使商家迅速赢得口碑,占领市场,增强用户粘性,为用户提供方便快捷的购物体验。

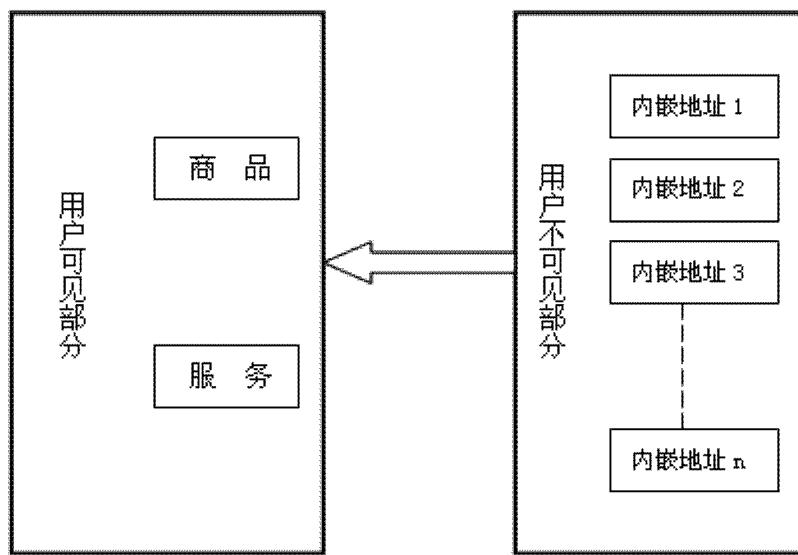


图 1



图 2

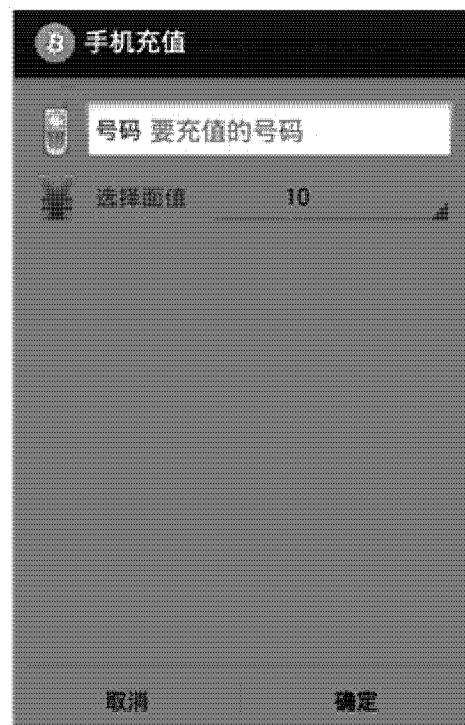


图 3