



## (12) 实用新型专利

(10) 授权公告号 CN 205068404 U

(45) 授权公告日 2016. 03. 02

(21) 申请号 201520778703. 7

(22) 申请日 2015. 10. 09

(73) 专利权人 北京大明五洲科技有限公司

地址 100192 北京市海淀区北京海淀区黑泉  
路8号1幢康健宝胜广场C座八层8001

(72) 发明人 谭云龙

(51) Int. Cl.

G06F 21/35(2013. 01)

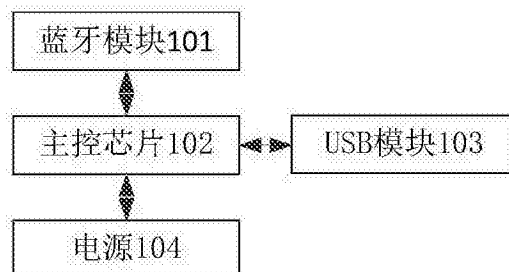
权利要求书1页 说明书6页 附图2页

### (54) 实用新型名称

无线转接装置以及安全认证系统

### (57) 摘要

本申请公开了一种无线转接装置以及安全认证系统,无线转接装置,其包括:无线模块、主控芯片、USB模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述USB模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互。本申请解决了具有蓝牙通讯功能的移动终端与 USBKEY 进行配合,以及保证了网络购物的交易敏感数据的安全。



1. 一种无线转接装置,其特征在于,包括:无线模块、主控芯片、USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互。

2. 根据权利要求 1 所述的无线转接装置,其特征在于,还包括:充电接口,用于向所述电源充电。

3. 根据权利要求 2 所述的无线转接装置,所述充电接口为 micro-usb 母头。

4. 根据权利要求 1 所述的无线转接装置,其特征在于,还包括升压单元,用于当所述主控芯片处于 host 模式时向所述 USB 模块提供需要的电压。

5. 根据权利要求 1 所述的无线转接装置,其特征在于,所述 USB 模块为 USB 2.0typeA 母头。

6. 根据权利要求 1 所述的无线转接装置,其特征在于,所述无线模块包括蓝牙 3.0 或 ble 蓝牙中任意一种或两者都包含。

7. 一种安全认证系统,其特征在于,包括移动终端、转接装置以及安全认证设备,无线转接装置包括:无线模块、主控芯片、USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互。

8. 根据权利要求 7 所述的安全认证系统,其特征在于,所述充电接口为 micro-usb 母头。

9. 根据权利要求 7 所述的安全认证系统,其特征在于,还包括升压单元,用于当所述主控芯片处于 host 模式时向所述 USB 模块提供需要的电压。

10. 根据权利要求 7 所述的安全认证系统,其特征在于,所述 USB 模块为 USB 2.0typeA 母头。

## 无线转接装置以及安全认证系统

### 技术领域

[0001] 本申请属于信息安全技术领域,具体地说,涉及一种无线转接装置以及安全认证系统。

### 背景技术

[0002] 随着智能化移动终端设备的流行,以及移动互联网的迅速发展,网络购物、金融交易逐渐除了可以在 PC 机端上实现,也可在到移动终端上,换言之,网络购物、金融交易移动化程度越来越高。

[0003] 为了保证交易的安全,在 PC 机端要依赖于 USBKEY,对交易相关数据进行加解密等处理。类似地,当在移动终端上进行交易时,通过将传统的 USBKEY 进行技术拓展,变为可为移动交易所用的安全认证工具。

[0004] 但是,随着移动互联网的发展,移动终端的硬件配置和软件功能越来越丰富。相比于之前,主要通过 PC 机端进行交易数据的传输和处理,在移动终端也可以实现电子购物等交易数据的处理。目前,已经出现了可与其他外设直接进行无线通讯的手机。为了保证在 PC 机端上网络购物等金融交易数据的安全,使用了 USBKEY,但是,现有的 USBKEY 无法直接与移动终端进行直接数据通讯,从而无法保证网络购物的交易敏感数据的安全。

[0005] 因此,亟待提供一种技术方案,用以解决具有无线通讯功能的移动终端与 USBKEY 进行配合时,网络购物的交易敏感数据的安全。

### 实用新型内容

[0006] 本申请所要解决的技术问题是提供一种无线转接装置以及安全认证系统,用于解决或缓解现有技术中的上述技术问题。

[0007] 为了解决上述技术问题,本申请提供了一种无线转接装置,其包括:无线模块、主控芯片、USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互。

[0008] 优选地,在本申请无线转接装置的一实施例中,其还包括:充电接口,用于向所述电源充电。

[0009] 优选地,在本申请无线转接装置的一实施例中,所述充电接口为 micro-usb 母头。

[0010] 优选地,在本申请无线转接装置的一实施例中,还包括升压单元,用于当所述主控芯片处于 host 模式时向所述 USB 模块提供需要的电压。

[0011] 优选地,在本申请无线转接装置的一实施例中,所述 USB 模块为 USB 2.0typeA 母头。

[0012] 优选地,在本申请无线转接装置的一实施例中,所述无线模块包括蓝牙 3.0 或 ble

蓝牙中任意一种。

[0013] 为了解决上述技术问题,本申请提供了一种安全认证系统,其包括移动终端、转接装置以及安全认证设备,无线转接装置包括:无线模块、主控芯片、USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互。

[0014] 优选地,在本申请安全认证系统的一实施例中,所述充电接口为 micro-usb 母头。

[0015] 优选地,在本申请安全认证系统的一实施例中,还包括升压单元,用于当所述主控芯片处于 host 模式时向所述 USB 模块提供需要的电压。

[0016] 优选地,在本申请安全认证系统的一实施例中,所述 USB 模块为 USB 2.0typeA 母头。

[0017] 与现有的方案相比,由于无线转接装置包括:无线模块、主控芯片、USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互,解决了具有无线通讯功能的移动终端与 USBKEY 进行配合,以及保证了网络购物的交易敏感数据的安全。

## 附图说明

[0018] 图 1 为本申请无线转接装置实施例一的结构示意图;

[0019] 图 2 为本申请无线转接装置实施例二的结构示意图;

[0020] 图 3 为本申请无线转接装置实施例三的结构示意图;

[0021] 图 4 为本申请安全认证系统实施例一的结构示意图。

## 具体实施方式

[0022] 以下结合附图和优选实施例对本申请的技术方案进行详细地阐述。应该理解,以下列举的实施例仅用于说明和解释本申请,而不构成对本申请技术方案的限制。

[0023] 下述实施例中,由于无线转接装置包括:无线模块、主控芯片、USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互,解决了具有无线通讯功能的移动终端与 USBKEY 进行配合,以及保证了网络购物的交易敏感数据的安全。

[0024] 本申请的核心思想之一:

[0025] 本申请提供了一种无线转接装置,其核心思想在于,包括:无线模块、主控芯片、

USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互。

[0026] 本申请的核心思想之二:

[0027] 本申请提供的安全认证系统,其核心思想在于,包括移动终端、转接装置以及安全认证设备,无线转接装置包括:无线模块、主控芯片、USB 模块以及电源,所述无线模块与所述主控芯片连接,所述电源与所述主控芯片连接;所述 USB 模块与安全认证设备连接;所述电源用于向所述主控芯片供电;所述无线模块用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块用于所述移动终端与所述安全认证设备之间进行数据交互。

[0028] 需要说明的是,本申请下述实施例中的移动终端包括并不限于智能手机、平板电脑、智能化穿戴设备等。

[0029] 下述实施例中,蓝牙模块作为无线模块。

[0030] 实施例一

[0031] 图 1 为本申请无线转接装置实施例一的结构示意图;如图 1 所示,其可以包括:蓝牙模块 101、主控芯片 102、USB 模块 103 以及电源 104,所述蓝牙模块 101 与所述主控芯片 102 连接,所述电源 104 与所述主控芯片 102 连接;所述 USB 模块 103 与安全认证设备连接;所述电源 104 用于向所述主控芯片 102 供电;所述蓝牙模块 101 用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片 102 用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块 103 用于所述移动终端与所述安全认证设备之间进行数据交互。

[0032] 本实施例中,蓝牙 3.0 的传输速度相对于蓝牙 2.0 来说自然更高,而技术原因就在 802.11 无线协议上。通过集成“802.11PAL”(协议适应层),蓝牙 3.0 的数据传输率提高了大约 24Mbps(即可在需要的时候调用 802.11WIFI 用于实现高速数据传输),是蓝牙 2.0 的八倍。

[0033] 蓝牙 4.0 即 BLE 蓝牙最重要的特性是省电科技,极低的运行和待机功耗可以使一粒纽扣电池连续工作数年之久。此外,低成本和跨厂商互操作性,3 毫秒低延迟、100 米以上超长距离、AES-128 加密等诸多特色,可以用于计步器、心律监视器、智能仪表、传感器物联网等众多领域,大大扩展蓝牙技术的应用范围。

[0034] BLE 低功耗蓝牙有 2 个主要组成:OSAL 操作系统抽象层和 HAL 硬件抽象层,多个 Task 任务和事件在 OSAL 管理下工作,而每个任务和事件又包括 3 个组成:BLE 协议栈,profiles 和应用程序。

[0035] 低功耗蓝牙只用 3 个信道做广播信道,允许毫秒级快速建立连接,效率远高于传统蓝牙的 32 个信道方式。

[0036] 少的数据频道和宽频道间隔:传统蓝牙有 79 个数据信道,频道间隔是 1MHz;低功耗蓝牙有 40 个数据信道,频道间隔是 2MHz。

[0037] 传统蓝牙的工作峰值电流一般是 35mA,睡眠状态电流是 0.01mA。

[0038] 而低耗能蓝牙的工作峰值电流是小于 15mA,睡眠状态电流是 0.004mA。

[0039] 本实施中,蓝牙 BLE 连接的过程:

[0040] 1、作为外围设备的移动终端发送具体的广告数据,以让任何中央设备知道外围设备是一个可连接的设备,广告内容包含设备地址,还可以包含一些额外的数据,比如设备名称、服务 ID 等。

[0041] 2、作为中央设备 (Center) 的转接装置接收到广告数据后发送一个搜索请求给外围设备 (Peripheral),外围设备移动终端 (Peripheral) 返回扫描响应给中央设备 (Center),如此中央设备可判定外围设备是一个可连接的设备。

[0042] 3、中央设备可以发送一个建立连接的请求给外围设备,进行配对连接,必要时进行绑定操作 (连接可以被从机或者主机任一方终止)。

[0043] 配对 (Pairing):建立连接,配对完成后可以进行数据通信。

[0044] 绑定 (Banding):将配对信息记录下来,如设备地址,这样下次连接时就不需要再次配对的过程 (快速连接)。

[0045] 实施例二

[0046] 图 2 为本申请无线转接装置实施例二的结构示意图;如图 2 所示,其可以包括:蓝牙模块 101、主控芯片 102、USB 模块 103 以及电源 104,所述蓝牙模块 101 与所述主控芯片 102 连接,所述电源 104 与所述主控芯片 102 连接;所述 USB 模块 103 与安全认证设备连接;所述电源 104 用于向所述主控芯片 102 供电;所述蓝牙模块 101 用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据;所述主控芯片 102 用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号;所述 USB 模块 103 用于所述移动终端与所述安全认证设备之间进行数据交互。

[0047] USB 设备分为 HOST (主设备) 和 SLAVE (从设备),只有当一台 HOST 与一台 SLAVE 连接时才能实现数据的传输。简单的说,如果一个数码设备支持 USB HOST,那么它就可以从另外一个 USB 设备中取得数据。因此,在与移动终端通过蓝牙通讯时,转接装置作为主设备,即主控芯片 102 处于 host 模式来实现。

[0048] 与上述实施例不同的是,本实施例中转接装置还包括:充电接口 105,所述充电接口 105 用于向所述电源 104 充电。

[0049] 优选地,所述充电接口 105 为 micro-usb 母头,Micro USB 是 USB 2.0 标准的一个便携版本,比部分手机使用的 Mini USB 接口更小,Micro-USB 是 Mini-USB 的下一代规格,Micro-USB 比标准 USB 和 Mini-USB 连接器更小,节省空间,具有高达 10000 次的插拔寿命和强度,盲插结构设计。Micro-USB 标准支持目前 USB 的 OTG 功能,即在没有主机 (例如个人电脑) 的情况下,便携设备之间可直接实现数据传输,兼容 USB1.1 (低速:1.5Mb/s,全速:12Mb/s) 和 USB 2.0 (高速:480Mb/s),同时提供数据传输和充电,特别适用于高速 (HS) 或更高速率的数据传输,是连接小型设备 (如手机, PDA, 数码相机, 数码摄像机和便携数字播放器等等) 的最佳选择。

[0050] 实施例三

[0051] 图 3 为本申请无线转接装置实施例三的结构示意图;如图 3 所示,与上述实施例一相同的是,其可以包括:蓝牙模块 101、主控芯片 102、USB 模块 103 以及电源 104,所述蓝牙模块 101 与所述主控芯片 102 连接,所述电源 104 与所述主控芯片 102 连接;所述 USB 模

块 103 与安全认证设备连接 ; 所述电源 104 用于向所述主控芯片 102 供电 ; 所述蓝牙模块 101 用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据 ; 所述主控芯片 102 用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号 ; 所述 USB 模块 103 用于所述移动终端与所述安全认证设备之间进行数据交互。

[0052] 本实施例中, 所述 USB 模块 103 为 USB 2.0typeA 母头。

[0053] 与上述实施例二相同的是, 本实施例中转接装置还包括 : 充电接口 105, 所述充电接口 105 用于向所述电源 104 充电。

[0054] 与上述实施例一和二不同的是, 本实施例中, 还包括升压单元 106, 用于当所述主控芯片 102 处于 host 模式时向所述 USB 模块 103 提供需要的电压。

[0055] 简单的升压单元 106 通常用一个电容和一个二极管, 电容存储电荷, 二极管防止电流倒灌, 频率较高的时候, 升压单元 106 的电压就是电路输入的电压加上电容上的电压, 起到升压的作用。

[0056] 常用的升压单元 106 还有开关直流升压电路 (即所谓的 boost 或者 step-up 电路), 其 the boost converter, 或者叫 step-up converter, 是一种开关直流升压电路, 它可以是输出电压比输入电压高, 主要由三极管或者 mos 管组成。

[0057] 在充电过程中, 开关闭合 (三极管导通), 开关 (三极管) 处用导线代替。这时, 输入电压流过电感。二极管防止电容对地放电。由于输入是直流电, 所以电感上的电流以一定的比率线性增加, 这个比率跟电感大小有关。随着电感电流增加, 电感里储存了一些能量。

[0058] 当开关断开 (三极管截止) 时的等效电路。当开关断开 (三极管截止) 时, 由于电感的电流保持特性, 流经电感的电流不会马上变为 0, 而是缓慢的由充电完毕时的值变为 0。而原来的电路已断开, 于是电感只能通过新电路放电, 即电感开始给电容充电, 电容两端电压升高, 此时电压已经高于输入电压了。升压过程就是一个电感的能量传递过程。充电时, 电感吸收能量, 放电时电感放出能量。如果电容量足够大, 那么在输出端就可以在放电过程中保持一个持续的电流。如果这个通断的过程不断重复, 就可以在电容两端得到高于输入电压的电压。

[0059] 实施例四

[0060] 图 4 为本申请安全认证系统实施例一的结构示意图 ; 如图 4 所示, 其包括转接装置 100、移动终端 200 以及安全认证设备 300, 无线转接装置 100 包括 : 蓝牙模块 101、主控芯片 102、USB 模块 103 以及电源 104, 所述蓝牙模块 101 与所述主控芯片 102 连接, 所述电源 104 与所述主控芯片 102 连接 ; 所述 USB 模块 103 与安全认证设备连接 ; 所述电源 104 用于向所述主控芯片 102 供电 ; 所述蓝牙模块 101 用于与具有蓝牙功能的移动终端无线连接并获取蓝牙数据 ; 所述主控芯片 102 用于处于 host 模式以对所述蓝牙数据进行转换生成 USB 信号 ; 所述 USB 模块 103 用于所述移动终端 200 与所述安全认证设备 300 之间进行数据交互。

[0061] 优选的, 在本申请安全认证系统的一实施例中, 所述主控芯片可以是意法半导体的 stm32f10x 系列中带 OTG 功能的主控芯片, 如 STM32F105RBT6, 或者是 microchip 公司的 PIC 系列单片机中带 OTG 功能的主控芯片, 如 PIC24FJ128GB202。

[0062] 优选地, 在本申请安全认证系统的一实施例中, 所述 USB 模块 103 为 USB 2.0typeA

母头。

[0063] 优选地,本实施例中,还包括充电接口 105,所述充电接口 105 为 micro-usb 母头。

[0064] 优选地,在本申请安全认证系统的一实施例中,还包括升压单元 106,用于当所述主控芯片 102 处于 host 模式时向所述 USB 模块 103 提供需要的电压。

[0065] 本实施例中的移动终端除了具有蓝牙功能外,还具有 OTG 功能,即即插即用功能,在跟安全认证设备建立有效连接后,相互之间可以之间进行点对点的通讯。

[0066] 有关对交易数据进行安全处理包括:主控芯片 102 通过从对从移动终端产生的交易数据,它利用存储在安全认证设备上的用户的私钥以及数字证书,利用内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中,理论上使用任何方式都无法读取,因此保证了用户认证的安全性。

[0067] 实施例五

[0068] 图 5 为本申请上述图 4 中安全认证系统实施例一的具体结构示意图,如图 5 所示,在结构的组成上与图 4 相同,在此不再详细赘述。安全认证系统包括:蓝牙模块,与蓝牙模块连接的主控芯片,蓝牙模块与主控芯片的 IO\_RX 端以及 IO\_TX 端连接;与主控芯片连接得 USBTYPE 母头,主控芯片与 USBTYPE 对应 DM 连接、DP 连接;USBTYPE 母头与升压案源连接,升压单元的输出电压可以是 5V;升压单元与电池连接,具体与电池的 VBAT 端连接,电池还与主控芯片连接,向主控芯片供电,主控芯片具体与电池的 VBAT 端连接;充电电路与电池连接,具体与充电电路的 VCHG 端连接;充电电路与 microusb 母头连接。需要说明的是,各个模块之间的工作关系同图 4,详细不再赘述。

[0069] 上述说明示出并描述了本申请的若干优选实施例,但如前所述,应当理解本申请并非局限于本文所披露的形式,不应看作是对其他实施例的排除,而可用于各种其他组合、修改和环境,并能够在本文所述申请构想范围内,通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本申请的精神和范围,则都应在本申请所附权利要求的保护范围内。

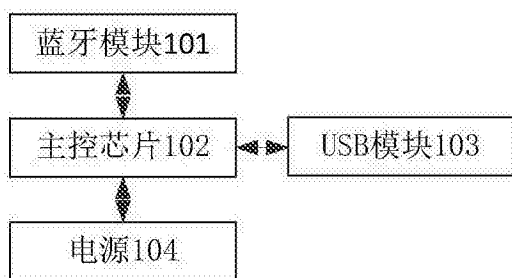


图 1

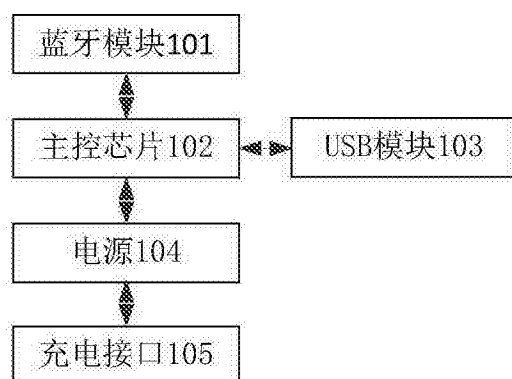


图 2

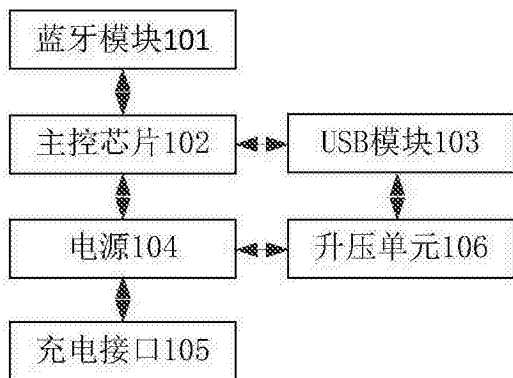


图 3

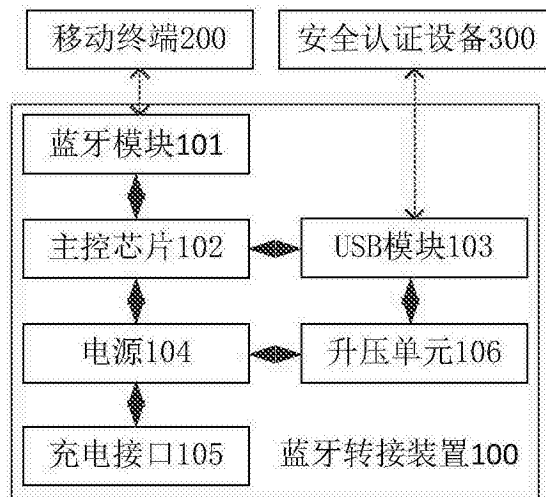


图 4

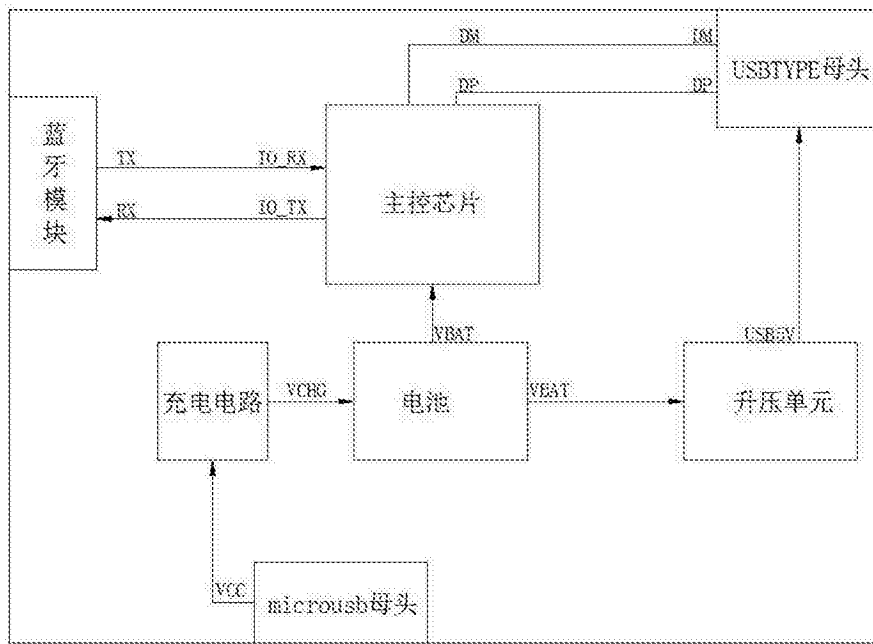


图 5