**一款更安全便携实用的硬件钱包设计**

1. **技术领域：支持虚拟货币不触网签名的安全硬件钱包**
2. **现有技术：现有硬件钱包大部分是将安全芯片内置在手机硬件中，或者是将硬件钱包设计成信用卡形状。同时现有硬件钱包只支持蓝牙一种信息传输形式。**
3. **目的：现有硬件钱包大部分是将安全芯片内置在手机硬件中，这样导致硬件钱包与手机设备完全耦合，几乎没有兼容性。满足手机兼容性的硬件钱包又因为小巧的外观设计，寡少的传输协议。使得硬件钱包在携带方面，不易丢失方面，传输安全方面有着诸多的不足。 同时市面上的现有钱包大多千篇一律，在美观性方面差强人意。为了解决当前硬件钱包的不足，我们设计了一款全新的硬件钱包。**
4. **技术方案及发明要点（重点）：**

**本技术方案设计了一款不触网（互联网）手机壳外观并支持多种传输协议的硬件钱包。**

**本硬件钱包要点如下：**

**为了保证虚拟货币交易的安全性，本硬件钱包在设计中满足如下特点：**

**1）私钥永远不会暴露并传递到任何计算机网络。与区块链网络所有的签名交互都通过安全的传输协议，使用银行金融级安全芯片, 不使用非安全的缓存芯片,保证私钥不会流出芯片,暴露在非安全环境中。即使丢失或者被盗,甚至落入黑客手中,也不会被破解。**

**2）双端分离,用独立的显示屏,通过在硬件钱包的显示屏上确认交易信息,有效防止交易被伪造。**

**3） 所有硬件钱包的固件信息锁死在安全芯片中，无法被篡改，也就没有了伪造指令的风险。**

**4）硬件钱包与外界环境通过蓝牙或者usb 连接等安全的传输协议连接。杜绝计算机病毒的影响。**

**5）在使用币种交易之前由本人物理确认设备上的交易（而不是计算机上的应用程序）。**

**6）同时满足蓝牙与usb 连接进行交易信息交互，使得硬件钱包签名的安全性，进一步提升。**

**2为了解决安全芯片与手机完全耦合，导致兼容性不足的问题。本发明设计中将安全芯片，与私钥存储环境与手机设备解耦。使得本硬件钱包在与手机适配的兼容性方面有了极大的提升。**

**3：为了解决现有技术方案中，将硬件钱包设计为信用卡小巧形状。不易携带，容易丢失的问题。我们将硬件钱包设计成手机壳的形状，使得硬件钱包从物理角度与手机绑定。大大降低了现有设计中硬件钱包不易携带，容易丢失的问题。**

**4：为了解决硬件钱包千篇一律美观性不足的问题，本发明设计中手机壳的设计，将在外观层面大大提升硬件钱包美观性不足的问题。使得硬件钱包又实用，又美观。**

**5：同时我们将nfc 功能与硬件钱包集成，这使得我们的硬件钱包在功能上满足虚拟货币的离线支付场景。**

1. **有益效果：**

**与旧有硬件钱包相比我们有如下有益特点。**

**1：与许多将安全芯片内置在手机中的硬件钱包相比，我们手机壳外观的硬件钱包可以与不同型号，不同操作系统的手机设配。更具有软件钱包安装设备的兼容性。**

**2：与其它硬件钱包使用蓝牙进行软硬件钱包之间信息交互不同，我们设计的全新硬件钱包同时满足usb 与蓝牙两种信息传输方式，在支持多种信息传输方式的基础下，我们又增加了信息传输的安全性。**

**3：我们此款硬件钱包同时支持nfc 功能，使得我们可以同时支持双离线虚拟货币支付场景。**

**4：与其它硬件钱包与手机完全是两个独立的产品不同，我们手机壳的硬件钱包设计，将硬件钱包与软件钱包的安装设备（手机）两个独立的产品，“合为一体“，既大大增加了硬件钱包的便携性，同时使得硬件钱包更不易丢失。**

**5：与其它硬件钱包千篇一律的外观设计不同，我们的硬件钱包设计，同时注重美观性，使得硬件钱包即实用，又美观。**