



[PDF Database Document] - BTCC Cryptocurrency Exchange

原文：

<https://www.btcc.com/zh-TW/academy/crypto-basics/what-is-a-bitcoin-wallet>

BTC教學 | 什麼是比特幣錢包？冷熱錢包有什麼區別？

在加密貨幣交易中，我們必然會說到的一個詞就是「錢包」。那麼你知道我們常說的加密貨幣錢包和比特幣錢包到底是什麼嗎？

這裡我們將為您介紹比特幣錢包，並區分我們常說的冷錢包和熱錢包分別指的是什麼？

什麼是比特幣錢包？

比特幣（BTC）與傳統貨幣完全不同，它具有抗審查和點對點電子現金系統的特點，因此存儲比特幣的錢包也與我們日常所說的「錢包」大不相同。

比特幣錢包是用戶用來交易比特幣和其他基於區塊鏈的加密貨幣的關鍵基礎設施，它沒有實體，使用公鑰加密技術對數字資產進行保護，並且不需要中介來處理交易，但開發人員仍然使用我們與現金相關聯的術語「錢包」來稱呼它，是為了幫助用戶駕馭加密貨幣的新世界。

實際上，比特幣錢包是一種設備、程序或服務，可生成和存儲包含用戶透過區塊鏈交易訪問、發送和接收加密貨幣所需的數字「憑證」的主文件。

比特幣錢包中的公鑰與私鑰

用戶與公共比特幣區塊鏈交互所需的最低「憑證」是一對公共和私人加密密鑰以及一個公共比特幣錢包地址。這些憑證用於對公共區塊鏈上的有效比特幣交易進行數字簽名和驗證。顧名思義，這些憑證中最敏感的私有密鑰必須絕對保密，就像銀行帳戶的 PIN 或安全碼一樣。它由唯一的字母數字字符串組成，是用戶訪問、消費或轉移其加密貨幣所必需的。

公鑰是從私鑰派生出來的，它使用戶能夠從其他人那裡接收加密貨幣。與私鑰一樣，它也由很長（256 位）的字母數字字符串組成。

比特幣錢包用於生成相應的公共錢包地址，作為交易的公共標識符。該地址是公鑰（160 位）的「散列」版（縮短版），便於與他人共享。要注意的是，比特幣錢包可用於生成無限數量的公共地址，但所有公共地址都連結回同一個用戶錢包。

用戶不要忘記或放錯其私鑰的記錄，這一點至關重要。由於比特幣是一個非中介的點對點系統，用戶無法

求助於第三方來幫助他們找回丟失的公鑰，這意味著他們有可能永遠無法獲得資金。

冷錢包與熱錢包的區別

比特幣錢包主要分為三種類型，分別是軟體、硬體和紙質錢包，它們的特性和安全級別各不相同。根據比特幣錢包是否連結到互聯網，它還被進一步分類為「熱」或「冷」錢包。

正如硬體和軟體指的是物理和非物理計算機部件一樣，加密世界中的錢包的冷熱指的是你存儲加密貨幣的方式。

1. 冷錢包

硬體錢包或冷錢包將您的助記詞和私鑰存儲在安全的物理設備中，並透過將您的私鑰與互聯網隔離開來保護您免受網絡攻擊。

雖然冷錢包的軟體相當於生活中的保險箱，但它仍然允許您的比特幣存在於區塊鏈上並被質押，但您的物理設備充當此保險箱的鑰匙。每筆交易都需要您的密鑰（物理設備）來響應交易，並且您的設備有一個 pin 以提供額外的安全層。

冷錢包幾乎總是抵禦安全威脅的最安全解決方案。

2. 熱錢包

熱錢包是指在線的虛擬錢包，便於將加密貨幣發送給其他用戶或交易所。虛擬化意味著你的助記詞和私鑰存儲在網上、錢包的瀏覽器或應用程序中，這使得它們更容易受到網絡安全威脅，不像冷錢包使用安全元件等物理硬件來保護這些信息。

熱錢包之所以「熱」，是因為它們始終連結到互聯網。因為無需處理任何硬件來進行集成，使得熱錢包更靈活、更方便地支持更廣泛的資產。

加密貨幣錢包

比特幣只是世界上成千上萬種加密貨幣中的一種，每天加密世界都在開發新的貨幣類型。

除了比特幣專用錢包外，還有許多加密錢包應用程式可用於保護和持有您的加密資產。有些錢包可能只支持一種貨幣，而有些錢包則兼容多種加密貨幣和山寨幣，這種兼容多種數字貨幣的錢包被稱為多加密貨幣錢包。

每個加密錢包都有一個唯一的錢包地址，而加密錢包的地址會根據您交易的加密貨幣決定是否改變。

如，如果你交易的是比特幣，你的錢包地址將在每次交易後更改；而如果你交易的是以太坊，則錢包地址保持不變。

加密錢包使用小技巧

如果您希望擴大您的投資組合併購買多種貨幣，建議您將資產分配給多個加密錢包，這樣也可以更好地保護您的資產安全。

隨著加密市場熱潮的興起，許多犯罪分子盯上了加密資產。因此，如果你的加密錢包中放有過多的數字資

產，很可能就會引起駭客或其他網路不法分子的注意，一旦發生意外就會損失慘重。

此外，使用多個錢包可以避免出現因忘記私鑰而無法訪問所有加密貨幣的情況。