[PDF Database Document] - BTCC Cryptocurrency Exchange

原文:
https://www.btcc.com/zh-TW/academy/crypto-basics/a-guide-to-preventing-cryptocurrency-hacks

加密安全丨預防加密貨幣所被駭指南

目前，加密資產已經成為熱門的投資方式，但在安全方面，加密貨幣仍然面臨著重大的挑戰。加密貨幣市場每天都在遭受著駭客的攻擊，而有關加密駭客事件的消息傳出使得許多想要嘗試加密貨幣的投資新人開始變得猶豫不決。

加密貨幣被駭大多數情況下是加密貨幣交易所被駭客攻擊了，那麼這種情況下，我們還能找回自己的資產嗎？讓我們一起往下看吧！

加密貨幣並不會被駭

首先，我們需要先清楚一個概念，就是加密貨幣本身並不會被駭客入侵。因為區塊鏈技術使用一種稱為散列的密碼學原語來安全地將正確的塊添加到鏈中。

哈希是一長串字母數字字符，從存儲在塊中的數據隨機生成。每個散列對於每個塊都是唯一的，對數據的任何微小更改都會導致不同的散列。因此，如果有人試圖更改單個交易，不僅需要重新計算當前塊的哈希，而且這適用於所有後續塊的哈希。

礦工驗證每一筆交易，以確保准確計算每個區塊。要做出改變，你需要說服超過 50% 的礦工同意你，這當然不是一件容易的事。

由於其去中心化的性質，比特幣和所有其他加密貨幣，尤其是那些擁有許多不同礦工的加密貨幣，更難被攻擊，因為沒有單點故障。

加密貨幣交易所被駭

加密貨幣交易所偶爾會被黑客入侵，截止目前，已經有不少加密貨幣交易所被駭客入侵。比較知名的交易所有 Bitmart、Binance 和 Bitfinex。2021 年 12 月，Bitmart 就因為遭到駭客攻擊而損失了約 150 美元到 2 億美元。Bitfinex 以治理代幣 BFX 的形式將所有損失的資金返還給用戶，這是為了匹配被盜資金的等值美元。幣安則向投資者保證，他們將獲得全額退款。

在過去的大規模黑客攻擊事件中，有些交易所無法償還用戶並破產。這就是為什麼盡可能避免這種情況很重要的原因。

如何選擇安全的加密貨幣交易所

作為一名投資者，想要避免因為交易所被駭造成的資產損失，首先我們應該選擇安全的加密貨幣交易所來進行交易。

我們主要可以從四個方面進行選擇：

1.交易所是否有名。知名的交易所一般會有強大的技術支撐，可以避免大多數的駭客攻擊。

2.交易所是否遭受過駭客的攻擊。如果一個交易所之前遭受過駭客的攻擊，那麼你需要加以注意，因為這證明該交易所存在一些漏洞，並且你無法知道該漏洞是否完全修復，以及交易所中是否有其他漏洞的存在。

3.交易所如何處理被駭的情況。如上述所說，許多加密貨幣交易所都遭受過被駭的情況，那麼這些交易所的處理方式對你的選擇尤其重要，因為這意味著，如果交易所再次被駭官方將會採取什麼樣的方式來處理你的資產損失。

4.交易所的基礎。交易所是否有良好的基礎也是一個需要重點考量的因素。一些交易所可能會受到司法機關的監管，因此會有更高的網絡安全標準，或者為客戶提供資金保險。簡單來說，他們會更加注重客戶的資金安全。

交易所被駭後可以找回自己的加密貨幣嗎？

上文我們告訴了您如何預防加密貨幣交易所被駭後造成的損失，但是如果你使用的加密貨幣交易所已經被駭了，還可以找回自己的加密貨幣嗎？

實話說，想要自己追回被駭的加密資產是一件很難的事情，一般加密交易所被駭後，你只能等待交易所提供好的賠償措施，因為你並不能看到駭客攻擊的幕後細節。

如果駭客要將你被盜的資金轉移到交易所，只要你能證明這些資金是你的，那麼交易所獲取可以幫你攔截這筆被盜的資金。但通常來說，這種方法並不太可能實現。

你能做的最好的事情就是吸取教訓，教育自己如何更好地保護自己的資產，並專注於接下來的交易中。