什麼是工作量證明（POW）？

原文:
https://www.btcc.com/zh-TW/academy/crypto-basics/what-is-proof-of-work

提到區塊鏈，通常很多人會想到「挖礦」。而目前最基本的挖礦方式有兩種，分別是POW和POS。

本篇文章將會為你介紹工作量證明（POW）的相關知識，希望對你有所幫助。

什麼是工作量證明？

工作量證明是基於區塊鏈的演算法，可以保護許多加密貨幣，包括比特幣和以太坊。

大多數數字貨幣都有一個中央實體或領導者來跟蹤每個使用者以及他們擁有多少錢。但是沒有這樣的領導者負責像比特幣這樣的加密貨幣，需要工作量證明才能使在線貨幣在沒有公司或政府運行節目的情況下工作。

更具體地說，工作量證明解決了「雙重支出問題」，如果沒有領導者負責，這個問題更難解決。如果使用者可以雙花他們的硬幣，這會膨脹整體供應，貶低其他人的硬幣，使貨幣不可預測和毫無價值。

雙重支出是在線交易的一個問題，因為數位操作非常容易複製，這使得複製和粘貼檔或向多個人發送電子郵件變得微不足道。

工作量證明使數字貨幣翻倍變得非常非常困難。這聽起來很像：「證明」某人已經進行了大量的計算。

下載Android版　　下載iOS版
台灣用戶專享優惠活動（10,055 USDT 交易大禮包） <<<<

工作量證明是如何運作的?

比特幣是一個區塊鏈，它是一個共用分類賬，其中包含曾經發生過的每筆比特幣交易的歷史。顧名思義，這個區塊鏈是由區塊組成的。每個區塊都存儲了最新的交易。

工作量證明是向比特幣區塊鏈添加新區塊的必要部分。區塊被礦工召喚到生活中，礦工是生態系統中執行工作量證明的玩家。 每當礦工提出新的獲勝工作量證明時，網路都會接受一個新的區塊，這大約每10分鐘發生一次。

找到獲勝的工作量證明是如此困難，提供礦工贏得比特幣所需的工作的唯一方法是使用昂貴的專用計算機。如果礦工猜測匹配的計算，他們將賺取比特幣。他們產生的計算越多，他們可能賺到的比特幣就越多。

礦工們究竟在進行哪些計算？在比特幣中，礦工會吐出所謂的「哈希值」 ，它將輸入轉換為隨機的字母和數位字串。

礦工的目標是創建一個與比特幣當前「目標」相匹配的哈希值。他們必須創建一個前面有足夠的零的哈希值。連續獲得幾個零的概率非常低。但是世界各地的礦工每秒都在進行數萬億次這樣的計算，因此他們平均需要大約10分鐘才能達到這個目標。

誰先達到目標，誰就贏得了一批比特幣加密貨幣。然後，比特幣協議創造了一個新的價值，礦工必須對其進行哈希處理，礦工們開始重新尋找獲勝的工作量證明。