[PDF Database Document] - BTCC Cryptocurrency Exchange

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

工作量證明（POW）是什麼？POW工作原理、代幣及優缺點分析

去中心化是加密貨幣最初願景的關鍵部分。為了實現這一目標，需要有一種無需金融機構參與即可確認交易的方法，這就是工作量證明（POW）和權益證明（POS）等共識機製誕生的原因。

工作量證明 (PoW) 是一種向加密貨幣區塊鏈添加新交易區塊的形式。在這種情況下，工作是產生與目前區塊的目標雜湊相符的雜湊（一長串字元）。執行此操作的加密貨幣礦工將贏得將該區塊添加到區塊鏈並獲得獎勵的權利。

加密貨幣始於工作量證明，因為它是第一個加密貨幣比特幣（BTC）使用的就是 POW 機制，它以其安全性而聞名，但也因其效率低下和對環境的嚴重影響而聞名。這也足以看出工作量證明機制的重要之處。

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。

內容目錄

- 工作量證明的歷史
- 工作量證明是什麼？
- 工作量證明是如何運作的
- 工作量證明與挖礦
- 為什麼工作量證明很重要？
- 工作量證明與權益證明的差異
- 工作量證明的優點與缺點
- 工作量證明代幣有哪些？
- 工作量證明的未來如何？
- 總結

工作量證明的歷史

在詳細介紹工作量證明前，我們可以先看看其歷史起源。

工作量證明（PoW）的起源可以追溯到 1993 年，當時 Cynthia Dwork 和 Moni Naor 正在尋找一種解決方案來阻止垃圾郵件和 DoS 攻擊。他們關於透過處理定價的論文概述了工作量證明的基礎知識。

1997 年，Adam Black 將他們的想法整合到了 Hashcash 中。他的演算法要求寄件者在電子郵件中包含計算成本較高的字串，從而使垃圾郵件發送者難以發送大量電子郵件。

垃圾郵件的解決方案本質上是增加發送單封電子郵件的成本。這個實驗證明你可以使用計算難度來表示線上事物的價值。這啟發了其他人，看看他們是否可以使用相同的想法來製作現金的數位表示。

這個想法再次出現在尼克・薩博所謂的「收藏品理論」和論文「掏錢：金錢的起源」中。

2004 年，這些想法啟發 Hal Finney 創建了一個版本，稱為可重複使用工作量證明。 2009 年，中本聰為

比特幣創建了著名的工作量證明共識機制。這是第一個去中心化的實施，解決了雙重支出問題，並使比特幣成為第一個成功的數位現金形式。

工作量證明是什麼？

工作量證明（POW）是基於區塊鏈的演算法，是一種用於確認和記錄加密貨幣交易的共識機制。

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。但是為了實現去中心化，像比特幣這樣的加密貨幣並沒有這樣的領導者負責，因此，需要工作量證明等共識機制來確認和記錄交易。

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。

而之所以稱之為「工作量證明」，是因為網路需要大量的處理能力。工作量證明區塊鏈由世界各地競相成為第一個解決數學難題的虛擬礦工來保護和驗證。獲勝者可以使用最新的經過驗證的交易更新區塊鏈，並獲得網路獎勵預定數量的加密貨幣。

接下來我們將對此進行詳細說明。

工作量證明是如何運作的？

每種加密貨幣都有一個區塊鏈，它是由交易區塊組成的公共分類帳。對於工作量證明加密貨幣，每個交易區塊都有一個特定的雜湊。為了確認該區塊，加密貨幣礦工必須產生小於或等於該區塊的目標哈希值。

為了實現這一目標，礦工使用快速產生計算的挖礦設備。

加密貨幣中的工作量證明之所以運作良好，是因為找到目標哈希很困難，但要驗證它並不困難。這個過程非常困難，足以防止交易記錄被操縱。同時，一旦找到目標哈希，其他礦工就很容易檢查它。

以比特幣為例，我們可以看看該加密貨幣是如何使用工作量證明來維護其區塊鏈完整性的：

當比特幣交易發生時，它們會經過安全驗證並被分組到一個區塊中進行開採。然後，比特幣的工作量證明演算法會產生該區塊的哈希值。比特幣使用的演算法稱為 SHA-256，它總是產生 64 個字元的哈希值。

礦工們競相成為第一個產生低於區塊哈希值的目標哈希值的人。獲勝者可以將最新的交易區塊添加到比特幣的區塊鏈中。他們還以新鑄造的硬幣和交易費的形式獲得比特幣獎勵。比特幣的固定最大供應量為 2,100 萬枚，但在此之後，礦工將繼續為其服務收取交易費用。

比特幣使用的工作量證明演算法旨在每 10 分鐘添加一個新區塊。為此，它根據礦工添加區塊的速度來調整挖掘比特幣的難度。如果挖掘發生得太快，哈希計算就會變得更加困難。如果進展太慢，他們就會變得更容易。

工作量證明和挖礦

工作量證明與挖礦緊密相連。 PoW 定義了礦工透過產生與區塊目標匹配的哈希值向同行顯示他們已執行所需計算的確切過程。另一方面，挖礦的重點是向區塊鏈添加新的區塊並獲得相關的硬幣獎勵。

比特幣交易的處理方式可以讓我們清楚地了解 PoW 和挖礦之間的關係。比特幣網路上的所有用戶交易最終都會進入記憶體池（mempool），礦工從中選擇交易以添加到下一個比特幣區塊。每個礦工都參加為比特幣區塊鏈創建新區塊的競賽，從記憶體池中挑選幾筆交易並將它們捆綁到候選區塊中。

然而，在候選區塊被接受為有效之前，礦工必須執行計算，產生低於比特幣工作量證明演算法設定的目標的哈希值。第一個為其候選區塊生成匹配哈希的礦工將其廣播給其他礦工，其他礦工可以輕鬆驗證和驗證其對區塊鏈記錄的添加。

成功的礦工在區塊鏈中添加了一個新的有效區塊後，將獲得區塊獎勵和相關的交易費用。因此，當挖掘下一個區塊的競賽開始時，比特幣區塊鏈的高度就會成長。

＼開戶送 10 USDT！ ／

點擊此處開設 BTCC 帳戶

為什麼工作量證明很重要？

出於多種原因，工作量證明演算法至關重要。最引人注目的是，它為網路參與者提供了一種安全且去中心化的機制，以維護區塊鏈帳本的完整性。 PoW 激勵世界各地的礦工花費運算能力來驗證區塊，從而填補了通常由銀行等中央實體扮演的角色。

PoW 的另一個主要好處是它可以規範新貨幣的創建。就比特幣而言，演算法包括挖礦難度調整，以穩定礦工產生新區塊的速率。比特幣的程式碼指定了每個區塊 10 分鐘的目標，該演算法旨在如果哈希率增長到礦工生產區塊的速度快於平均水平的程度，則增加找到新區塊哈希的難度。

如果沒有與 PoW 相關的挖礦難度調整，礦工耗盡 BTC 供應的速度可能會快於永續經濟所需的速度。此外，隨著 PoW 鏈上網路算力的成長，不良行為者攻擊系統變得不切實際。

Braiins 的一項研究顯示，透過實體算力攻擊比特幣網路的保守成本為 55 億美元。然而，這樣的操作在現實世界中執行是不切實際的，因為成本攻擊超過了任何感知到的好處。除此之外，潛在的攻擊者可以立即因為誠實行事並為比特幣貢獻算力而獲得獎勵。

工作量證明與權益證明的差異

工作量證明是第一個加密貨幣共識機制。 2012 年，隨著 Peercoin (PPC) 的推出，另一個替代方案——權益證明 (PoS) 出現了。它根據交易驗證器在網路中質押或鎖定的代幣數量來選擇交易驗證器。

比特幣的最大競爭對手以太坊一直在其區塊鏈上使用工作量證明，直到 2022 年 9 月才實現了備受期待的向權益證明的過渡。透過下表，我們可以更清楚這兩者的一些主要差異：

工作量證明

- 驗證是由礦工網路完成的
- 比特幣作為獎勵和交易費用支付
- 競爭性需要消耗大量的能量和運算能力

權益證明

- 驗證由提供以太幣作為抵押品的參與者完成
- 以太幣僅用於支付交易費用
- 使用更少的運算能力和能源
- 因為沒有困難，所以更快達成共識

由於權益證明不需要與工作證明一樣多的運算能力，因此它更具可擴展性。它可以以更低的費用和更少的能源消耗更快地處理交易，使權益證明加密貨幣更環保。由於不需要昂貴的硬件，因此開始抵押加密貨幣也比挖礦容易得多。

然而，從安全角度來看，工作量證明更加安全可靠。權益證明的一個潛在問題是，擁有大量加密貨幣的各方可能擁有過多的權力，而這是工作量證明所不存在的問題。

工作量證明的優點和缺點

了解了兩大共識機制的差異後，接下來，讓我們來看看工作量證明的最大優點和缺點：

優點
- 高水準的安全性和去中心化
- 抗審查
- 從經濟上激勵礦工保護網路
- 促進再生能源的採用

缺點
- 交易速度較慢且費用較高
- 與較新的共識模式相比，挖礦需要較高的資本和營運支出
- 能源使用量高

作為區塊鏈最早的共識模型，工作量證明系統的優缺點只有隨著產業的成熟才變得明顯。儘管出現了新的創新，但 PoW 仍然是在公共區塊鏈上達成共識的最成熟、最經過時間考驗的方法。

＼開戶送 10 USDT！ /

點擊此處開設 BTCC 帳戶

工作量證明代幣有哪些？

工作量證明（PoW）不僅僅是第一個共識機製，也是采用率最高的共識機制。目前，超過 60% 的加密貨幣使用工作量證明演算法。然而，實施共識模型的最有價值的網路如下：

- **比特幣（BTC）**：該網路是世界上最安全和去中心化的 PoW 系統。比特幣的成功主要歸功於中本聰巧妙的 PoW 工程，它不僅安全，還為網路參與者提供了永續的經濟。
- **萊特幣（LTC）**：萊特幣於 2011 年作為比特幣分叉推出，複製了傳統網路的各個方面，例如其 PoW 共識模型。萊特幣通常被稱為比特幣黃金中的白銀，並且仍然是市值最高的加密資產之一。
- **狗狗幣（DOGE）**：受 Meme 啟發的加密貨幣狗狗幣於 2013 年推出，採用 PoW 技術，其根源可追溯到萊特幣。狗狗幣和萊特幣可以實現更快的交易，但通常不如比特幣安全。
- **門羅幣（XMR）**：門羅幣是一種注重隱私的加密貨幣，它實現了工作量證明演算法。其獨特的功能，包括環簽名和隱形位址，使得追蹤區塊鏈上的交易變得困難。門羅幣的工作量證明演算法被設計為抗 ASIC，這意味著它更適合個人礦工而不是大型採礦作業。
- **比特幣現金（BCH）**：比特幣現金是一種加密貨幣，是由於比特幣區塊鏈硬分叉而於 2017 年創建的。它採用工作量證明共識演算法，類似比特幣。比特幣現金旨在透過將區塊大小限制增加至 32 MB 來提高比特幣的可擴展性和交易速度。然而，由於其網路中少數礦池佔據主導地位，它面臨中心化的批評。

BTCC 提供 300+ 種 POW 代幣交易對，包括比特幣、狗狗幣、萊特幣等，槓桿最高可達 500，如果您對此感興趣，可註冊 BTCC 進行購買。

工作量證明的未來如何？

工作量證明將區塊鏈引入了世界。礦工們在一場永無止境的競賽中競爭以生產新區塊並收集相關獎勵，從而使不良行為者越來越難以危害網路。這種新穎的共識機制透過激勵運算能力的使用來保護底層帳本的完整性，從而提供了無與倫比的安全性。

PoW 共識演算法旨在透過使用難度調整實現來調節代幣的發行，從而提供穩定的經濟。由於礦工無法透過累積更多代幣來自動增加其在網路上的持有量或股份，因此代幣的供應分配更加有效。

傳統共識模型繼續佔據公共區塊鏈最大的市場份額，並且可能始終是在去中心化網路之間建立共識的最安全的選擇。

＼開戶送 10 USDT！ /

點擊此處開設 BTCC 帳戶

總結

工作量證明是許多加密貨幣用來驗證區塊鏈上的交易並獎勵參與網路的代幣的共識機制。這是一個競爭過程，使用公開的交易資訊來嘗試產生小於該挖掘週期的網路目標的十六進位數字。

儘管更多新的共識機制出現，但 POW 機制仍是去中心化網路之間建立共識的最安全的選擇。

想了解更多有關區塊鏈和金融的資訊，可以進入 BTCC 學院 及 資訊 頁面進行查看。

BTCC 提供超 300 種虛擬貨幣合約，包含各種熱門加密貨幣（如比特幣、以太幣、狗狗幣、SOL 幣等），且合約槓桿高達 500，您可以在該交易所以最低的成本開始交易。

對於新手來說，**建議可以先透過 BTCC 交易所提供的模擬交易功能（免費提供100,000U贈金）先練手，等逐漸熟悉虛擬貨幣槓桿交易的玩法和特性後，再正式進場操作。**

BTCC 也提供現貨交易，現貨交易將不提供任何槓桿，您將以當前價格進行買賣。如果您對此感興趣，可註冊 BTCC 開始您的投資之旅。

BTCC 註冊優惠活動

註冊後即可獲得 10 USDT 贈金，再加入官方 LINE 參加活動可獲得額外 10 USDT 贈金。新用戶註冊後 7 天內入金，贈金最高 10,055 USDT！趕快開始註冊吧！

更多優惠內容：關注 BTCC 活動中心

註冊 BTCC 贏10,055U豐厚贈金（入金活動）

關於 BTCC

- 安全性高，已獲得美國、歐洲、加拿大等地監管牌照
- 無資金費率
- 300 種虛擬貨幣合約
- 10到500倍靈活槓桿
- 交易費低至 0.01%
- 行業領先的市場流動性，交易深度大
- 提供通證化代幣（貴金屬、美股、台股）
- 24 小時線上真人客服
- 每月提供大量福利活動

立即註冊 BTCC 帳戶