新手指南丨什麼是權益證明（POS）？如何區分POS和POW?

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

權益證明（POS）是一種加密貨幣共識機制，用於處理交易並在區塊鏈中創建新區塊。共識機制是一種驗證分散式資料庫中的條目並保持資料庫安全的方法。在加密貨幣的情況下，資料庫被稱為區塊鏈 ， 因此共識機制保護區塊鏈。

本文將為您詳細介紹什麼是權益證明？它和工作量證明（POW）又有什麼區別？讓我們一起往下看吧！

什麼是權益證明？

引入權益證明是為了克服工作量證明系統的缺點，它允許硬幣持有者抵押硬幣（質押），以便有機會驗證交易並獲得交易費用。 雖然PoS 協議通過隨機選擇過程選擇驗證者，但擁有更多硬幣的人會自動擁有更多的挖掘能力，即擁有更多股份百分比的人更多投資於貨幣並分配了更多事務。它可以保護使用者，因為它降低了硬幣價值快速下降的風險。所選的驗證者檢查並添加區塊以賺取獎勵，如果他們提供的資訊不準確，他們可能會失去部分賭注。

由於加密採礦中的交易分佈在點對點網路中，因此個人計算機或網路擁有者可以將大量的計算能力用於採礦，並在此過程中賺取可觀的錢。因此，許多個人和公司將整個網路專用於加密採礦，旨在增加收入。

權益證明的特點

權益證明演算法具有三個基本特點，無論它們在生態系統中如何採用：

1. 固定數量的硬幣：

在任何給定時間，只有有限數量的硬幣通過網路流通。創建新硬幣的可能性並不存在（例如在比特幣和其他基於PoW的系統的情況下進行挖掘）。網路要麼從有限數量的硬幣開始，要麼從工作量證明開始，將硬幣帶入網路，然後切換到權益證明。

2. 交易費用作為偽造者的獎勵：

每筆交易都附帶費用，這將被收集並提供給將創建新塊的實體。如果偽造的區塊被證明是欺詐性的，則該實體將失去交易費及其股份，這稱為斜切。

3. 51%攻擊的不切實際性：

51%的攻擊是不切實際的，因為它要求攻擊者擁有網路中總硬幣的51%，這是昂貴的。因此，執行攻擊太耗時，成本高昂且無利可圖。積累如此大比例的加密貨幣將會出現困難，因為可能沒有足夠的貨幣來購買，或者購買更多的硬幣變得昂貴。驗證不正確的交易也會導致驗證者失去他們的賭注，使他們的獎勵為負數。

POS vs POW

工作量證明和權益證明都是所謂的「共識機制」，即區塊鏈保持其完整性的方法，共識可以解決數字貨幣「雙重支出」問題。如果加密貨幣的使用者可以通過多種方式多次花費他們的硬幣，那將破壞整個系統，貨幣將毫無價值。

簡而言之，這些「X證明方案」有助於驗證通過區塊將哪些交易添加到區塊鏈中，這些交易為最新的交易，而贏家將獲得獎勵。

工作量證明和權益證明各自以不同的方式選擇一個「贏家」，將創建下一個區塊的實體。

通過工作量證明，礦工是參與者。如果他們有更多的計算能力，他們更有可能向區塊鏈添加額外的區塊，這是由電力驅動的。而在權益證明中，如果礦工有更多的錢，他們更有可能贏得額外的區塊 。換句話說，權益證明依賴於用戶擁有多少「權益」的「證明」。

權益證明的目標

權益證明旨在減少圍繞工作量證明 （PoW） 協定的可擴充性和環境可持續性問題。工作量證明是一種驗證交易的競爭性方法，它自然會鼓勵人們尋找獲得優勢的方法，特別是因為涉及貨幣價值。

比特幣礦工通過驗證交易和區塊來賺取比特幣，但是他們用法定貨幣支付電費和租金等運營費用。當前，礦工們正在用能量換取加密貨幣，而挖掘工作量證明加密貨幣所需的能量會深刻影響定價和盈利能力的市場動態。同時人們還需要考慮一些環境的問題，因為 POW 挖礦所耗費的能源幾乎和一個小國一樣多。

PoS 機制試圖通過有效地用質押代替計算能力來解決這些問題，從而個人的挖掘能力被網路隨機化。這意味著應該大幅降低能耗，因為礦工不能再依靠大型單一用途硬體農場來獲得優勢。

權益證明是否比工作量證明更好？

不一定。雖然權益證明是為了克服工作量證明的缺點而建立起來的，但是它仍有有許多令人詬病的點。因此，權益證明吸引了不止一些批評者。其中一個原因是以太坊開發人員已經迅速吹捧權益證明的優勢，但它尚未被證明有效，因為它尚不存在。

Blockstream 研究總監 Andrew Poelstra 在2015年寫了一篇數學論文，稱權益證明「從根本上無法在比特幣的信任模型中產生分散式共識」。但是，如果權益證明確實有效，那麼它很可能是一種更環保的替代方案，可以實現與工作量證明相同的目標，但效率更高。