[PDF Database Document] - BTCC Cryptocurrency Exchange

原文:
https://www.btcc.com/zh-TW/academy/crypto-basics/blockchain-consensus-mechanism

新手指南丨區塊鏈的靈魂是什麼？一文帶你了解三大主流共識機制

區塊鏈是一個去中心化帳本，它用於記錄許多計算機上的交易，以便記錄不能被後續塊更改或更改，而不會在網路內串通。區塊鏈利益相關者看到的每個塊都會創建一個分散式寄存器，這是一個正式的交易記錄，可確保數據自創建以來可見且未更改。

分類帳的狀態不會改變，並且由於公共區塊鏈作為分散的自動化系統運行，因此必須有一個高效、公平、即時、有效、可靠和安全的機制，以確保區塊鏈上的每筆交易都是真實的，並且所有參與者都同意分類帳的共識狀態。可以說，共識機制是區塊鏈的靈魂。

區塊鏈的靈魂——共識機制

共識演算法，也稱為共識機制，它是用於即時實現關於區塊鏈真實狀態的共同協議的系統。

簡而言之，這樣的系統確保了區塊鏈網路的所有節點都是同步的，並且交易是經過身份驗證和保護的。一旦節點同意交易的合法性，它就會獲得批准，然後記錄在區塊鏈上。在那之後，這個街區永遠留在那裡。

除了保證整個區塊鏈的安全性外，共識演算法還有助於在去中心化網路中的陌生人之間建立信任。之所以能夠實現這一點，是因為演算法決定了要信任哪些節點以驗證和啟用事務。

三大主流共識機制

PoW、PoS、DPoS 是區塊鏈的三種主流共識機制，它們分別代表區塊鏈網路的三種主要記帳規則。

1. 工作量證明機制（PoW）

工作量證明是最古老的演算法，與中本聰（Satoshi Nakamoto）創建的第一個區塊鏈一起出現。這種共識機制完全依賴於充當節點的礦工。他們競相解決複雜的加密難題，首先完成這項工作的人將獲得挖掘下一個區塊的權利。此外，「贏家」將獲得新鑄造的加密貨幣獎勵。

（1）優點

PoW主要的優點是防止駭客攻擊。由於這種共識模型需要大量的計算能力和精力，因此駭客很難改變系統。即使他們試圖這樣做，設備，電力和努力的成本也將超過獲得的利潤。且由於區塊幾乎不可能改變，因此用戶可以確保它保持每筆交易的真實性和可追溯性。

（2）缺點

隨著區塊鏈技術變得越來越先進，解決哈希變得越來越困難，整個過程需要越來越多的計算能力。因此，礦工必須使用昂貴的專用硬體，並消耗大量能源。另一方面，這種共識機制與緩慢的交易速度有關。驗證一個區塊和批准一筆交易可能需要十多分鐘。同時，交易費用也相當高。

（3）案例

除了比特幣和以太坊，萊特幣、門羅幣等區塊鏈也依賴於 PoW 演算法。

2. 權益證明機制（PoS）

權益證明是第二大流行的共識機制，它需要的不是計算能力，而是需要抵押能力來驗證區塊。節點必須抵押區塊鏈的本地令牌才能參與共識過程。

網路通常需要最少數量的令牌才能成為驗證器，如果驗證者離線太長時間，或者如果驗證者進行欺詐行為，則質押的令牌可能會部分丟失。

PoS 驗證器接收交易費用作為獎勵。交易的驗證器是隨機選擇的，然而，被選中的可能性與抵押代幣的數量相關。權益證明被認為比工作量證明更具成本效益，因為它需要流動的加密貨幣而不是物理硬體，並且幾乎不需要用電。

（1）優點

在權益證明中，驗證者不需要購買昂貴的硬體，只需使用他們的普通PC即可。因此，更多的人可以負擔得起成為節點。節點越多，去中心化程度就越強。此外，共識過程更加節能，並且提供了更快的交易速度。

（2）缺點

儘管每個 PoS 驅動的區塊鏈協議都有不同的規則和條件，但大多數協議都要求驗證者在一段時間內鎖定最少量的加密貨幣。在此期間，無論加密貨幣下跌或飆升，你都無法「取消」並交易它。

並且，擁有較大抵押資金的驗證者在網路上的權重更大，因此它們可能對交易驗證產生過大的影響，這也會導致加密貨幣囤積。

（3）舉例

Flow、Cardano、Avalanche、Polygon 和 Tezos 是使用權益證明共識協議的區塊鏈之一。這些平台在加密社區中非常受歡迎，因為它們被設計為可擴展和可持續的。

值得注意的是，以太坊目前正在從工作量證明轉向權益證明共識模型，以使區塊鏈更快、更便宜、更環保。

3. 委託權益證明機制（DPoS）

委託權益證明是權益證明的增強版本。驗證特定區塊的委託人將由使用者投票，而不是隨機選擇驗證者，而擁有最多抵押代幣的委託人將被選擇。

如果選擇了委託人，則抵押人將獲得總質押池的份額。每個區塊的委託人數量是有限和隨機的，使每個人都可以更公平地參與。此外，數量有限的委託人使共識機制能夠更順暢地運作。

（1）優點

DPoS 主要的優點是即時投票允許持續監控網路安全。一旦抵押人檢測到惡意活動，他們就會立即投票選出可疑的代表，而這可疑的代表可以隨時被逐出網路。在能耗上，DPoS甚至比PoS更節能、更實惠。

委託權益證明機制的使用也對交易確認和執行的速度產生了積極影響。基於 DPoS 的區塊鏈每秒可以進行 2,000 到 8,000 筆交易。

（2）缺點

雖然 DPoS 系統因其分散的功能和民主方法而受到讚譽，但仍有可能使網路更加集中。如果委託人決定透過建立所謂的卡特爾來聯合努力，那麼交易驗證將依賴於一小群人，這將使網路有偏見並容易受到惡意行為的影響。

另一個問題與網路安全有關。很明顯，一個好的區塊鏈網路需要大量的使用者。負責維護網路的人越少，組織 51% 攻擊就越容易 – 當一個人或一群人獲得對超過 50% 的區塊鏈哈希算力的控制權時，這種攻擊是可能的。

（3）舉例

Tron、Steem、EOS 和 WAX 等區塊鏈在 DPoS 共識機制之上運行，所以這些區塊鏈在交易速度方面都是高度可持續和高性能的。