



新手指南 | 什麼是區塊鏈預言機？

原文：

<https://www.btcc.com/zh-TW/academy/crypto-basics/what-is-a-blockchain-oracle>

預言機（Oracle）是**區塊鏈**中非常重要的功能。由於區塊鏈不可竄改與永久保存的特性，許多產業開始藉此發展區塊鏈相關技術。然而，為了保持資訊安全性，基本上區塊鏈網路的建構是封閉的，無法接收區塊鏈以外的資訊。因此，在不同區塊鏈上運行的專案需要借助預言機服務的幫忙，來協助我們將資料輸入區塊鏈中。

本文將為您詳細介紹什麼是區塊鏈預言機？以及它的主要應用場景，讓我們一起往下看吧！

什麼是預言機？

在計算機領域，預言機是一種抽象電腦，又稱諭示機。預言機具備圖靈機的一切功能，並額外擁有一種能力：可以不通過計算直接得到某些問題的答案，這個過程叫做 Oracle（神諭）。也就是說，預言機可以解決圖靈機通過計算也無法解決的問題，比如從外界獲取問題的答案。

為什麼區塊鏈需要預言機？

由於區塊鏈是一個封閉的系統環境，目前區塊鏈只能獲取到鏈內的數據，而無法獲取鏈外真實世界的數據。

本質上來說，**智能合約**即寫好了條件和結果的程式碼，當特定條件被給予或滿足時即能夠觸發。而若智能合約執行需要的觸發條件是區塊鏈外部的訊息時，就必須要依靠 Oracle 提供數據，透過 Oracle 將現實世界的數據輸入到智能合約中。

因為智能合約只能被動接收數據，無法主動去獲取鏈外的數據，這就是區塊鏈需要 Oracle 的原因。

為什麼區塊鏈預言機如此重要？

預言機為去中心化的 **Web3** 生態系統提供了一條路徑，其中去中心化和數位化是核心底層特徵。它們是一個專用實體，將區塊鏈平台連結到現有的外部數據源，以促進基於真實世界資訊的智能合約的執行。

Oracles 被公認為分散式 Oracle 網路或 DON，可說明 Web3.0 集群無縫訪問數據交匯點、傳統通道和高級計算，而不會有任何麻煩。它們幫助開發人員構建混合智能合約，其中存在鏈上代碼和鏈下基礎設施的組合，以支持創新的 [DApp](#) 專案。當鏈上數據存在於區塊鏈網路中時，鏈下數據在生態系統之外產生共鳴。

使用區塊鏈技術的公司和實體與 Chainlink 等知名 Oracle 網路攜手合作，以擴大其能力。

預言機在擴大智能合約的可操作性範圍方面發揮著重要作用。同時，缺乏區塊鏈預言機將限制智能合約的使用。值得注意的是，預言機不僅僅是區塊鏈和外部世界之間的紐帶，它們也是提高核心網路效率的基礎設施層。oracle 在將外部數據資源連結到請求方之前，先對其進行查詢、驗證和身份驗證。一些強大的預言機解決方案可以輕鬆地將數據轉發到智能合約，同時將其恢復到外部來源。

區塊鏈預言機如何工作？

所有 oracle 網路都執行三個重要功能，包括：從可靠的外部來源收集數據；使用簽名消息在鏈上發送資訊；通過以智能合約的形式安全地存儲數據源，使最終使用者可以訪問數據源。

一旦數據存儲在智能合約中，其他自動協議就可以通過引用「檢索」功能的訊息調用輕鬆訪問它。數據還可以由以太坊節點或網路參與者通過訪問 Oracle 生態系統的存儲部分直接使用。

區塊鏈預言機的主要應用場景

1. 去中心化金融

去中心化金融（DeFi）已成為過去幾年中最熱門的趨勢之一。預言機在支援 DeFi 集群方面發揮著重要作用，因為它們可以呈現出用戶輕鬆訪問與資產和市場相關的財務數據。

例如，處理虛擬資產的貨幣市場使用價格預言機來確定投資者的借貸能力。這些預言機有助於檢查投資者的頭寸是否抵押不足，是否與清算有關。此外，自動化做市商使用價格預言機將流動性集中在現行市場價格，以說明提高效率。

2. NFT和區塊鏈遊戲

在預言機的說明下，智能合約在非金融領域找到了自己的位置，比如 NFT 和區塊鏈遊戲。NFT 是高度動態的，並且容易隨著外部事件的波動而變化。而計算預言機有助於創建可驗證的隨機性，從而為 NFT 分配隨機特徵。這些預言機在選擇遊戲中的隨機贏家或 NFT 掉落方面也起著重要作用。電子遊戲使用可驗證的隨機性來增強其生態系統的參與度和不可預測性。

3. 去中心化衍生品

衍生品是兩方或多方之間的金融合約，其價值基於相關資產。衍生品允許人們對標的資產提出不同的視角（長期或短期），從實質上促進金融穩定。公共智能合約平台可以創建和交易金融衍生品，包括基於區塊鏈的資產。預言機可以通過提供價格饋送，結算價值和合約到期來確定參與方的收益或損失，從而在去中心化衍生品中發揮重要作用。

4. 智能合約保險

在免信任且可靠的信任源加持下，保險產品可以通過智能合約的形式實現。當前的商業案例比如 **Etherisc** 的去中心化的保險應用（如航班延誤保險和作物保險）平台，**FlyingCarpet** 的人工智能和地理數據的新型可編程保險等。

5. 去中心化預測市場

像 **Augur** 和 **Gnosis** 這樣的去中心化預測市場利用人群的智慧來預測現實世界的結果，如總統選舉和體育博彩結果。如果投票結果受到用戶的質疑，預言機可用於快速和安全的解決方案。