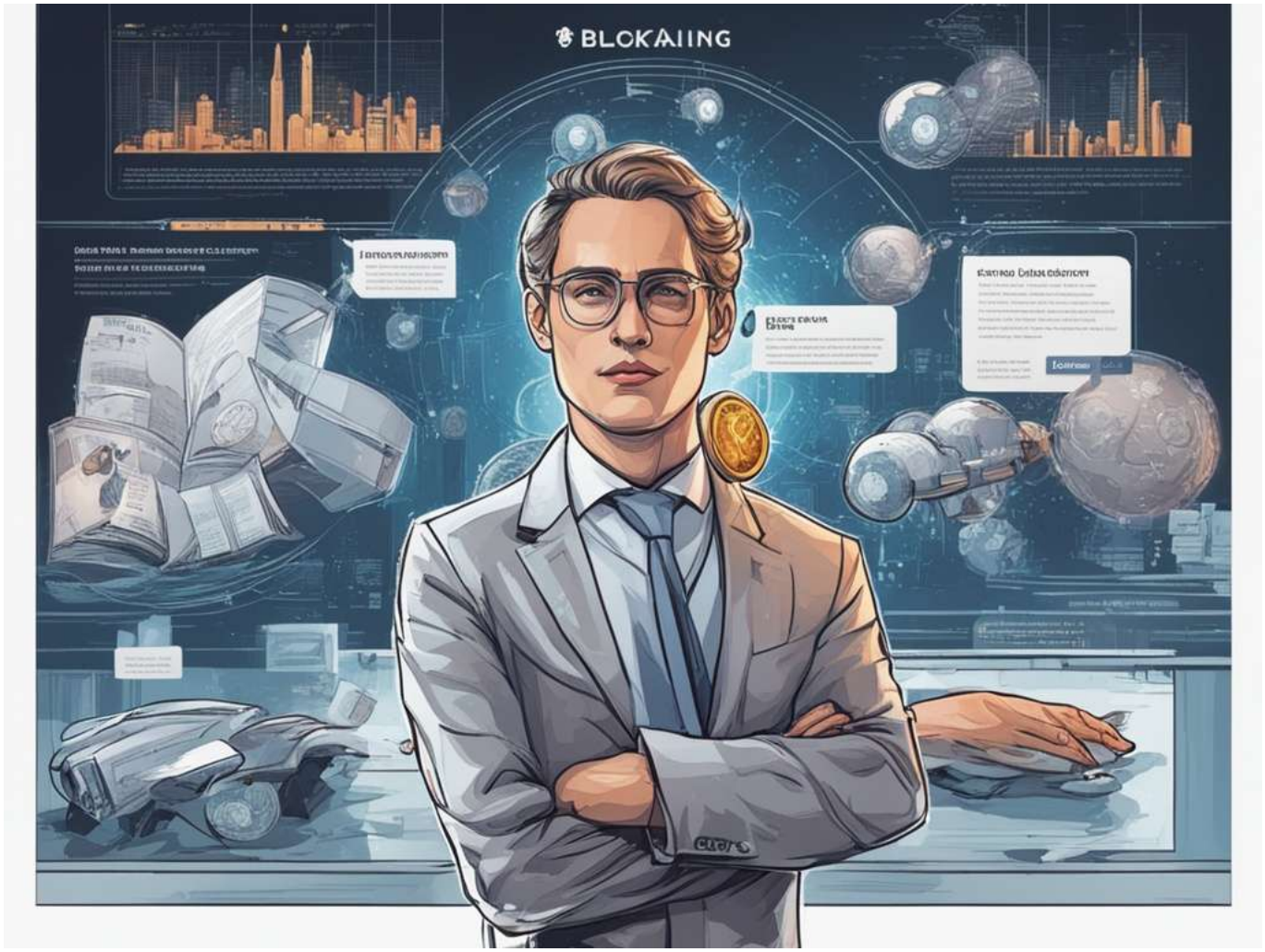
[PDF Database Document] - BTCC Cryptocurrency Exchange

原文:
https://www.btcc.com/zh-TW/academy/crypto-basics/bitcoin-smart-contracts-explained-and-how-they-work

比特幣智能合約：解釋及其運作原理



與人們普遍認為的相反，比特幣的區塊鏈具有高度可編程性，能夠執行智能合約。事實上，比特幣區塊鏈上的幾乎每一筆交易都可以看作是智能合約在發揮作用。從確保交易安全到達成複雜的金融協議，這種功能允許廣泛的可能性。

比特幣與以太坊等以智慧合約為核心的平台的主要區別在於它們支援的可程式類型。以太坊擁有圖靈完整的腳本語言，為智慧合約提供了更多的靈活性和複雜性。然而，比特幣的腳本語言更簡單但更強大，可以執行重要的智能合約，使其本身成為一個強大的工具。

智能合約：定義與基礎知識

例如，可以對智能合約進行編程，使其在預定的時間延遲後自動將比特幣從一個用戶轉移到另一個用戶，從而確保交易的迅速和安全。然而，智能合約的複雜性並不局限於這種簡單的應用。它們可以包含複雜的條件標準，以滿足各種應用的特定需求。或者，它們也可以像要求數位簽名以促進貨幣交換一樣簡單明了。

要充分理解智能合約的複雜性，就必須了解它們作為記錄在區塊鏈數位分類帳上的程序的基本性質。許多區塊鏈都採用腳本語言來支援這些程序，使它們能夠按預期運行。在某些情況下，在區塊鏈上進行的交易包含了決定其處理的邏輯，而在其他情況下，專用程式被部署在區塊鏈上，允許用戶與之互動以執行特定功能。

這兩種表現形式都是智慧合約的代表，體現了智慧合約的多功能性和適應性。智能合約的實用性在於其源自於區塊鏈數位分類帳的固有優勢。智能合約在去中心化的基礎設施上運行，具有很強的彈性，可抵禦各類攻擊，確保交易的完整性和安全性。此外，它們被記錄在不可更改的數位分類帳上，使其對所有參與者透明且可存取。

圖靈完備性淺釋

在智慧合約領域，圖靈完備性是一個至關重要的概念。圖靈完備性是為了紀念傑出的艾倫-圖靈而命名的，它概括了程式語言及其執行環境的基本能力。圖靈完備性的核心是指程式語言在時間和記憶體等資源充足的情況下執行任何演算法或解決任何計算問題的能力。

這一深刻特徵是大多數現代程式語言的標誌。圖靈完備性的精髓在於它的通用性和普遍性；用一種圖靈完備性語言編寫的任何程式都有可能被複製到另一種語言中。然而，在智能合約方面，圍繞圖靈完備性的爭論愈演愈烈。

問題來了：智能合約語言需要圖靈完備性嗎？支持者認為，以太坊及其同類產品作為著名的智慧合約平台，其強大之處在於其圖靈完備性。相較之下，比特幣雖然可編程，卻缺乏這項決定性屬性。這種分歧源自於比特幣交易雖然可以客製化，但不具備圖靈完備語言的運算能力與彈性。

比特幣與智能合約：強大的協同作用詳解

在比特幣生態系統中，每一筆交易本質上都是一個智慧合約。決定比特幣支出的標準稱為腳本金鑰（scriptPubKey）或鎖定腳本（locking script）。相反，滿足這些標準的資料和腳本稱為 ScriptSig 或 ScriptWitness，這取決於輸入是否利用了 SegWit 技術。這種靈活性和可編程性對比特幣交易的高度客製化和安全性至關重要。

各種機制進一步增強了比特幣的智慧合約功能。其內建的腳本語言為創建複雜的交易邏輯奠定了堅實的基礎。閃電網路（lightning network）是一種鏈外擴展解決方案，可以更快、更便宜地執行智慧合約。日誌合約（Discreet Log Contracts）提供了隱私增強功能，而側鏈（sidechains）則實現了與其他區塊鏈的互通性。

比特幣智能合約：演進與歷史

比特幣最初是一種點對點電子現金系統，現在已轉變為一個能夠創建和執行複雜智能合約的平台。雖然比特幣的腳本功能最初被認為只是一種附加功能，但社群很快就意識到了比特幣腳本語言的巨大潛力。這促使人們探索和開發各種類型的智能合約，徹底改變了在區塊鏈上進行交易的方式。

比特幣智能合約的發展歷程始於多重簽名設定的出現。這些設定允許交易由多方簽署，確保了更高的安全性和信任度。然而，2012 年推出的 “按腳本哈希付費”（Pay-to-Script-Hash，P2SH）才是比特幣智能合約發展的一個重要里程碑。 P2SH 允許向腳本進行交易，而腳本的條件只有在贖回交易時才會顯示，這大大提高了比特幣網路上智能合約的靈活性和複雜性。

此後，比特幣社群不斷推動智慧合約功能的發展。 2021 年 11 月啟動的 Taproot 升級引入了 Schnorr 簽名和默克爾化抽象語法樹（MAST），進一步提高了比特幣智能合約的隱私、效率和複雜性。這些進步使得交易更加複雜和安全，從而能夠在比特幣區塊鏈上建立新的用例和應用程式。

比特幣智能合約的歷史證明了比特幣協議的適應性和社區探索創新、安全和可擴展性之間平衡的奉獻精神。隨著比特幣網路的不斷發展，我們期待看到智慧合約技術取得更大進步，推動去中心化經濟的創新和價值創造達到新水準。

比特幣智能合約：類型與優化

在技術層面上，P2PKH 腳本提出了一個嚴格的要求：要使用透過該腳本發送的比特幣，用戶必須提供一個 ECDSA 簽名，該簽名必須與腳本中嵌入的公共金鑰的雜湊值精確匹配。該簽名是所有權的最終證明，可驗證交易並保護資金安全。

P2PKH 的核心優勢在於它將比特幣的所有權直接與私鑰持有者綁定。由於只有私鑰所有者才能產生與公鑰哈希值相符的有效簽名，因此比特幣仍由其安全控制。這使得 P2PKH 成為比特幣安全交易的絕佳選擇，

確保只有預定收款人才能獲得資金。

比特幣腳本：語言與重點

比特幣協議擁有一種內建的腳本語言（通常稱為腳本），它是定義比特幣生態系統中金幣消費規則的支柱。這種語言是比特幣用戶創建智能合約的重要組成部分，智能合約規定了價值轉移的條件。腳本使用戶能夠設定比特幣輸出必須滿足的特定條件。例如，一筆交易可能需要來自不同錢包的多個簽名，或資金釋放前的時間鎖定到期。這些條件提供了靈活性和安全性，確保只有在滿足約定條款的情況下才能轉移資金。Script 的一個重要方面是其功能有限。雖然它是一個功能強大的工具，但它不是圖靈完備的，這意味著它不支援某些複雜的程式結構，如循環。這項限制有助於保護比特幣網路免受拒絕服務（DoS）攻擊，因為它可以防止執行可能會消耗過多運算資源的潛在惡意腳本。儘管有其局限性，腳本仍支援比特幣系統不可或缺的一系列智能合約功能。比特幣支援的一些主要智能合約類型包括

- 支付到公共金鑰哈希（P2PKH）：這可以確保只有交易的預期收款人才能使用其中的比特幣，提供了一種安全、可驗證的轉帳方式。
- 多重簽名腳本：這些腳本需要多個錢包的簽名才能釋放資金，從而實現對比特幣消費的協同控制。
- 時間鎖定比特幣交易：這種機制可防止交易中的比特幣在特定時間結束前被使用，提供了一種延遲釋放資金的機制。
- 支付到腳本哈希值（P2SH）：透過向腳本的哈希值發送比特幣，這種交易方式提高了效率和隱私性，因為實際腳本不會在區塊鏈上顯示。

比特幣閃電網路終極指南

閃電網路（Lightning Network）就是這樣一個改變遊戲規則的協議，它是將比特幣功能提升到新高度的第二層解決方案。閃電網路允許比特幣區塊鏈上的節點建立直接通訊管道，使它們能夠在主鏈之外進行數量不限的交易。這種創新方法大大降低了交易費用，提高了交易速度，為比特幣用戶開闢了一個充滿可能性的世界。

閃電網路成功的關鍵在於它能夠處理鏈外交易，同時仍保持比特幣區塊鏈的安全性和不變性。當節點打開閃電通道時，它們之間會建立一條安全的支付路徑，從而實現快速且有效率的價值交換。這些交易保持在鏈外，減少了比特幣區塊鏈的擁堵，並提高了整體可擴展性。

此外，閃電網路與智慧合約的整合進一步擴展了其功能。具體來說，透過閃電通道轉發支付需要使用哈希時間鎖定合約（HTLC）。這種智慧合約可確保資金從一個節點安全地轉移到另一個節點，同時保持支付路徑的完整性。透過運用智慧合約的力量，閃電網路不僅能實現更快、更便宜的交易，還能為去中心化應用程式和服務帶來新的機會。

側鏈技術

比特幣區塊鏈曾經是唯一的先驅，但隨著許多側鏈的出現，比特幣區塊鏈也不斷發展。這些額外的區塊鏈提供了整合機會，利用去中心化技術的力量帶來了前所未有的好處，增強了區塊鏈生態系統的可擴展性、互通性和整體功能，推動了創新和應用。

在比特幣網路上創建安全智能合約

用複雜的智慧合約功能釋放比特幣的力量。在比特幣網路上，每筆交易本質上都是一個智慧合約，透過腳本確保比特幣的安全，該腳本限制只有目標收件人才能存取。然而，比特幣的智能合約潛力遠不止這些基本功能。雖然腳本語言不是圖靈完備的，但它無需循環就能實現非凡的功能。透過利用閃電網路（Lightning Network）和其他第二層協議，比特幣協議得到了增強，成倍地拓寬了智慧合約的可能性。探索比特幣智慧合約的前沿世界，了解它們如何徹底改變你的交易和業務運作。