新手指南丨什麼是零知識證明（ZKP）？

原文：
https://www.btcc.com/zh-TW/academy/crypto-basics/what-is-zero-knowledge-proof-zkp

區塊鏈領域最令人興奮的發展之一是零知識證明（ZKPs）的廣泛採用。這項技術提供了卓越的透明度、不變性和隱私性，並且已經成為確保區塊鏈上交換資訊隱私的三種可能的解決方案之一，其他兩種分別是安全多方計算（sMPC）和可信執行環境（TEE）。

零知識證明（ZKP）是什麼？

零知識證明 (zero knowledge proofs)，簡稱為 ZKP，它是密碼學中使用的一種方法，用於證明某些東西是已知的，而不直接揭示已知的資訊。它基本上允許在交換中對私人資訊保密。零知識證明是間接證明，允許您證明自己知道一個秘密，而無需向其他人透露該秘密。

在零知識證明中，基本角色是證明者和驗證者。證明者必須證明他們知道這個秘密。驗證者必須能夠驗證證明者是否說實話。

它之所以有效，是因為驗證者要求證明者做一些只有在證明者肯定知道秘密的情況下才能完成的事情。如果證明者正在猜測，他或她最終將被驗證者的測試證明是錯誤的。如果知道這個秘密，那麼證明者每次都會通過驗證者的測試，而不會出現問題。這就像銀行或機構要求您提供已知秘密單詞的信件以驗證您的身份一樣。你不是在告訴銀行你的銀行帳戶里有什麼，你只是在告訴他們你知道一個給定單詞的順序。

零知識證明的工作原理

零知識證明是一種加密協議，它允許一方（示證者）向另一方（驗證者）確認陳述的真實性，而無需透露有關該方的任何其他訊息（示證者了解到的內容和來源）。該定義最初是由麻省理工學院的研究人員 Shafi Goldwasser，Silvio Micali 和 Charles Rakoff 在科學文章《交互式証明系統的知識復雜性》（1985）中提出的。

零知識證明具有三個主要屬性：

1. 完整性－如果示證者知道陳述，那麼他可以說服驗證者。
2. 正確性－如果示證者不知道該陳述，那麼他只能以很小的機率欺騙驗證者。
3. 零知識－驗證者即使行為不誠實，也不會從示證者知道該陳述這一事實中得知任何其他訊息。

證明採用交互協議的形式。這意味著乙方向示證者提出一系列問題，示證者如果知道秘密，將正確回答所有問題。如果甲方的秘密未知，但他想說服對方的測試者，則他有一定的機率（例如 50%）正確地回答問題。

但是，經過一定數量的問題（10 - 20）後，審查員很有可能確定示證者不知道秘密。在這種情況下，所有答案都不會給出有關機密本身的任何訊息。

零知識協議有兩種類型：

1. 交互的（驗證者獨立地實時詢問示證者）；
2. 非交互式的（不需要驗證者和示證者之間的直接通訊；驗證者可以在事實之後驗證語句的真實性）。

零知識證明還可以根據是否有幾個驗證者確定斷言的真實性的階段而分為兩組－所謂的使用布爾函數的可信設置。

對於某些協議，例如 zk-SNARKs（簡明非交互零知識證明），這是前提條件。驗證程序生成一個特殊的秘密，該秘密在受信任的安裝後立即銷毀。如果秘密繼續存在，則可以偽造網路上的數據，從而平衡使用該協議的好處。

某些協議不需要受信任的安裝（例如 zk-STARK）。

zk-SNARKs

第一個利用零知識證明來做到交易匿蹤性的是ZEC，其中的演算法便是zk-SNARKs，但因為ZEC的新區塊獎勵會有大約20%進入基金會的口袋以支持運作，部分支持者不滿這種行為於是分岔出了ZCL，因此兩者的加密法與架構都是一致的。

zk-SNARKs是zero knowledge Succinct Non-interactive ARgument of Knowledge的縮寫，這幾個詞分別代表了：Succinct(簡潔，用很少的資料量可以完成整個溝通與驗證)、Non-interactive(只需要很少刺或不需要與原始發送者溝通即可驗證訊息)、ARgument(只在計算上是安全的，如果遇到一個計算能力極強的攻擊者會失效)。

零知識證明的應用和用例

1.ZKP 的應用

零知識的證明的應用主要有 5 個方面：

1. 區塊鏈：比特幣和以太坊等公共區塊鏈的透明度使交易的公開驗證成為可能。但是，這也意味著很少的隱私，並可能導致使用者的去匿名化。零知識證明可以為公共區塊鏈引入更多的隱私。例如，加密貨幣Zcash基於零知識簡潔的非互動式知識論證（Zk-SNAKR），這是一種零知識加密方法。
2. 財務：ING使用ZKP，允許客戶證明其秘密號碼位於已知範圍內。例如，抵押貸款申請人可以證明他們的收入在可接受的範圍內，而無需透露他們的確切工資。
3. 投票：如果公共區塊鏈記錄了投票，則不需要值得信賴的第三方來驗證結果。因此，ZKP可以使投票系統匿名，因為合格的選民可以在不透露身份的情況下證明他們投票的權利。
4. 認證：在身份驗證系統中，一方希望通過密碼等一些秘密資訊向第二方證明其身份，但不讓第二方學習任何東西。ZKP 可以幫助執行此類資訊交換。
5. 訊息傳遞：訊息的端到端加密是必要的，以便除了您要發送到的郵件之外，沒有人可以閱讀私人郵件。通過ZKP和區塊鏈，我們可以在消息傳遞世界中建立端到端的信任，而不會洩露任何額外的資訊。

2.ZKP 的具體用例

新創公司 QEDIT 開發了 SDK（軟體開發工具包），該工具包使您可以在現有的區塊鏈中實施零知識證明，以增加交易的隱私性，同時保持通過節點進行交易驗證的可能性。該項目已獲得歐盟委員會質量認證，其合作伙伴包括 VMWare，Ant Financial 和 Deloitte 等知名公司。

StarkWare 已經創建了基於 zk-STARKs 協議的解決方案，該協議也可以在現有網路上實現。該項目已經吸引了 Vitalik Buterin，Pantera Capital，Intel Capital，Sequoia Capital 和其他投資者的資金。

荷蘭銀行 ING 已發布零知識證明（ZKP）的修改版本–零知識範圍證明（ZKRP）。該協議可以證明客戶的工資在獲得抵押所必需的範圍內，而無需透露其本身的具體金額。