

出國報告（出國類別：其他）

參加 2018 年荷蘭央行

「內部稽核之現況與發展趨勢」

（Internal Audit: keeping pace with developments）

研討會心得報告

服務機關：中央銀行

姓名職稱：謝蕙如四等專員

派赴國家：荷蘭阿姆斯特丹

出國期間：107 年 6 月 2 日至 6 月 10 日

報告日期：107 年 8 月 31 日

摘要

近年來，創新科技高度發展引領全球掀起變革浪潮，諸如區塊鏈、大數據及人工智慧等新興技術不僅驅動產業型態轉變，也正一點一滴地滲透到我們的日常生活中，這對人類世界來說，無疑是一個嶄新又特別的體驗。

區塊鏈如同一本共享的分散式總帳，每個區塊鏈的參與者手上都會有這本總帳，帳本記錄著在區塊鏈上所有的交易紀錄，每次的交易若經大家確認屬實將會被記錄下來，並同步更新到這本總帳，而紀錄的方式係基於密碼學、演算法等技術，透過嚴謹的數學邏輯設計，確保記錄不可竄改。區塊鏈可運用的層面相當廣泛，舉凡金融、物流、醫療或娛樂等產業領域皆看重發展潛力，前景備受各界矚目，而其被視為新式的帳本技術，因此也成為會計界持續關注的重要議題。為使區塊鏈具體實踐到真實場景，不致流於空泛的想像，最佳的做法即是對該技術有基本的認識。本報告係以介紹區塊鏈運作原理為出發點，但避免使用艱澀的技術名詞，同時亦探討區塊鏈對會計領域的相關影響及探索未來的可能應用。

稽核人員須蒐集充分且適切的資訊據以支持稽核結論，因此大數據和機器學習等先進分析技術是促使稽核工作升級轉型的關鍵利器。當能夠融入更全面、多樣化的資料進行剖析和判讀，不僅更貼近組織運作真實樣貌，亦能擷取更具智慧深度的資訊內涵，供作決策輔助也將更趨精準。

在數位化時代下，科技應用的重要性與日俱增。為彰顯稽核人員的價值及達成所賦予的職責，除了持續精進專業知識與技能，也需要學會與高科技共處，利用新興技術增進稽查品質，提供組織創新洞見並協助優化營運效能，畢竟組織治理的良窳維繫於完善及健全的內部稽核制度。

目 錄

壹、前言.....	1
貳、區塊鏈相關技術及運作原理.....	2
一、區塊鏈的出現.....	2
二、解構區塊鏈.....	3
三、區塊鏈實際運作模式—以比特幣為例.....	13
四、區塊鏈特性.....	16
五、區塊鏈的本質—價值移轉.....	17
參、區塊鏈對會審領域帶來的變革.....	18
一、會計帳務處理.....	18
二、財務報告編製.....	18
三、查核工作內容.....	19
四、查核重點考量.....	20
五、查核人員新角色.....	22
肆、區塊鏈於會審實務可能應用場景.....	23
一、智慧合約與會計處理—以 IFRS15 客戶合約之收入為例.....	23
二、電子函證金融區塊鏈平台.....	26
三、自動化法規遵循.....	28
伍、資料科學領域與內部稽核相關議題.....	32
一、稽核本質在於分析資訊.....	32
二、大數據四項特質與內部稽核.....	32
三、人工智慧與內部稽核.....	33
陸、研習心得與建議.....	37
一、心得.....	37
二、建議.....	39
參考資料.....	41

表 目 錄

圖 1 區塊鏈示意圖.....	3
圖 2 區塊構造.....	5
圖 3 網路架構分類.....	6
圖 4 資料管理方式.....	7
圖 5 各節點遵循同一套共識規則.....	8
圖 6 雜湊函數特性.....	10
圖 7 字串經雜湊函數轉換示意圖.....	10
圖 8 公開金鑰加密驗證流程.....	11
圖 9 區塊鏈模型架構.....	12
圖 10 比特幣交易紀錄方式.....	13
圖 11 比特幣交易運作方式.....	14
圖 12 區塊鏈運作流程.....	15
圖 13 收入認列 5 步驟.....	23
圖 14 合約定義判斷邏輯.....	24
圖 15 履約義務判斷條件.....	24
圖 16 收入認列時點.....	25
圖 17 目前函證作業流程.....	26
圖 18 電子函證金融區塊鏈執行流程圖.....	27
圖 19 目前法遵流程.....	29
圖 20 目前法遵流程痛點.....	30
圖 21 未來法遵流程.....	30
圖 22 未來法遵流程優點.....	31
圖 23 內部稽核功能轉變.....	36

壹、前言

本次參加荷蘭央行（De Nederlandsche Bank，以下簡稱 DNB）於阿姆斯特丹舉辦「內部稽核之現況與發展趨勢」(Internal audit: keeping pace with developments)研討會，課程主題包含內部控制三道防線、作業風險管理與企業風險管理、區塊鏈及物聯網等，目的在於讓內稽人員深入瞭解新興科技進展以掌握內稽領域最新脈動，並聚焦在數位技術對內部稽核的影響、稽核人員的職責及回應措施。此外 DNB 設計個案分組競賽貫穿整個研討會，配合每天授課進度給予不同指令，促使團隊成員腦力激盪以完成任務，並引導學員進行反思及經驗分享，透過該個案活動更能貼近實務運用，有助啟發內控專業思維及洞察力。

數位科技浪潮席捲而來，顛覆各產業的運作型態，驅動經營模式的轉變。當組織引入新興技術時，內部稽核需協助企業重新檢視內部流程，辨識可能發生風險的環節，將其融入組織的管理體系。除此之外，內稽人員對技術本身的特質亦須有充分瞭解，方能評估為組織帶來的契機或可能遭遇的衝擊，適時提供優化營運的改善建議。

蓬勃發展的先進技術同樣地賦予會計相關領域嶄新的樣貌，伴隨而來的變革將如何影響會計、審計及內部稽核工作態樣？會計行業是否真的有可能被科技替代？會審人員如何運用創新技術以發揮槓桿效用進而為組織創造更大價值，將顯得無比重要。這些與數位科技攸關的議題是近年來會計界持續關注的焦點，也是本報告主要探討的核心重點。

本報告共分為五大部分，第一部分介紹區塊鏈相關技術及運作原理，第二部分說明區塊鏈對會計與稽核領域可能衍生的影響，第三部分闡述區塊鏈在會審實務可能的應用場景，第四部分探討與資料分析攸關之內部稽核議題，最後則為心得與建議。

貳、區塊鏈相關技術及運作原理

區塊鏈無疑是當今深受全球矚目的創新科技之一，為人熟知的加密貨幣交易或智能合約履行，皆屬於其應用範疇。區塊鏈技術已在許多產業引領變革，顛覆各領域以往既有的運作方式，正慢慢改變未來世界的社會樣貌。事實上，區塊鏈本身整合了各式技術，是多種技術的集合體，例如分散式帳冊技術、點對點網路、共識機制及加密金鑰等，也因為此複雜性，使得大眾較難以直觀淺顯的方式理解區塊鏈邏輯構成，遑論去想像區塊鏈技術如何於日常生活中實踐。但理解運作原理在區塊鏈的學習中是必要的，因為從中可得悉背後不同技術交互運用衍生出區塊鏈各種特徵，相關技術結合使用的可能性，從而根據現實狀況評估合適的應用場景，具體掌握其影響層面和未來前景，有助開啟我們對區塊鏈更廣泛的想像空間，更加活用區塊鏈技術。本章將對區塊鏈進行剖析，首先說明區塊鏈原理、所包含的核心技術及運作模式，並探討其具備的相關特性。

一、區塊鏈的出現

綜觀人類文明的進展歷程，信任在現代化社會中扮演著不可或缺的關鍵角色。在以物易物的原始社會中，是不需要藉各種信用中介即可完成交易。然而隨著交易活動增加，生產力提高，經濟不斷發展，以物易物的交換型態非常不具效率，於是發展出貨幣，作為交易的媒介並具備價值貯藏的功能。而信任即為貨幣系統的核心，一個國家的通貨能否促成價值實現，取決於民眾對該國信心及政府本身的信用，因此信任遂演變成維繫社會運行的基石，支撐經濟秩序的穩定。

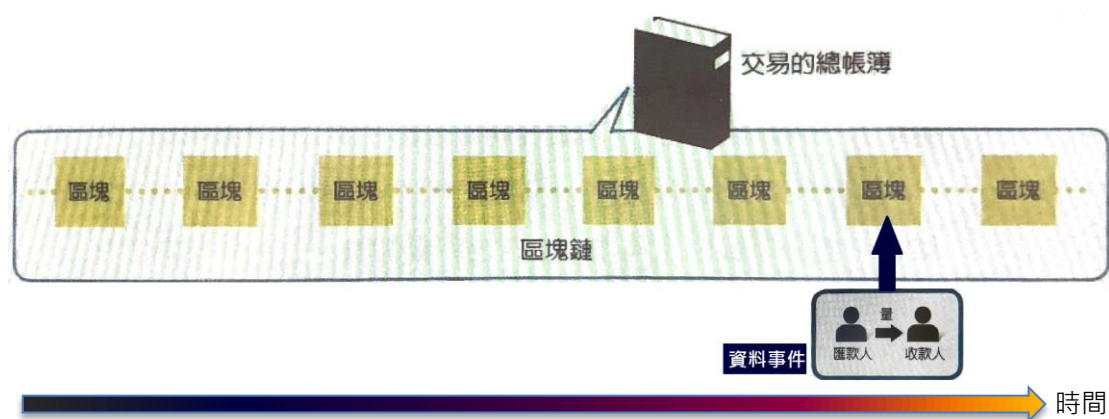
2008 年受到次貸危機衝擊，美國投資銀行雷曼兄弟破產所引發的金融海嘯席捲全球，各國政府為挽救潰堤的市場信心，輪番推行量化寬鬆政策，以緩解枯竭的流動性，卻也導致貨幣持續貶值，促使各界反思央行若無法遵守通貨紀律，傳統貨幣信任模式即遭受破壞。同年底，為信任提供另一種模式，標榜著去中心

化，利用區塊鏈技術作為底層應用的比特幣就此崛起。區塊鏈將信任託付給一種機制，該機制確保集體達成的共識才是真實可信，不需要相信交易對手或任何第三方擔保，而該共識係奠基於數學演算法的電腦系統程式。

二、解構區塊鏈

區塊鏈可以簡單的理解為儲存數據的方式，就像是一本共享的網路總帳本，記錄著每一筆交易信息，如圖 1 所示。在這本公共總帳上的交易內容是公開透明的，所有網絡使用者皆可查閱、驗證，而每次交易一旦被確認，即無法取消或變更，永遠地被寫入總帳。帳本由使用者共同維護更新，不受任何的中心機構管理。雖然區塊鏈可理解為一種分散式資料庫，但與傳統資料庫不同之處在於其所儲存的是交易而非單純的資料，其意謂著這些交易須通過驗證的程序才能被記錄下來，因此涉及與其他技術的配合。以下便依序解析區塊結構及相關的核心技術：

圖 1 區塊鏈示意圖



資料來源：Nikkei Computer(2016)。

(一) 區塊構造

區塊鏈由一個個區塊串接所構成，每次寫入數據時即創建一個區塊，並按照生成的時間排序。每個區塊係儲存交易的地方，內部構造可分為二部分：區塊表頭(block header)和一系列的交易資訊(transactions)。區塊表頭摘記與該區塊有關的特徵值；交易資訊則記載若干筆的交易紀錄。以下介紹表頭內主要的特徵值：

1. 前一個區塊雜湊值(Previous Block Hash)

上個區塊的區塊表頭經雜湊函數計算所得的雜湊值。目的在於使區塊間的資訊形成關聯，杜絕資料遭竄改風險，以保障數據正確性。

2. 時間戳(Timestamp)

代表區塊形成的時間標記。確保區塊依時間排列先後次序，亦可用來證實交易數據於某時間真實存在。

3. 難度值(Difficulty)

計算雜湊值的困難度。在比特幣區塊鏈中，為使區塊生成速度保持在 10 分鐘一個，故設立一個難度係數，該係數與生成時間成反比，每最新 2016 個區塊按統一公式自動調整難度值，若實際時長大於 10 分鐘，則降低難度，反之亦然。

4. 隨機數(Nonce)

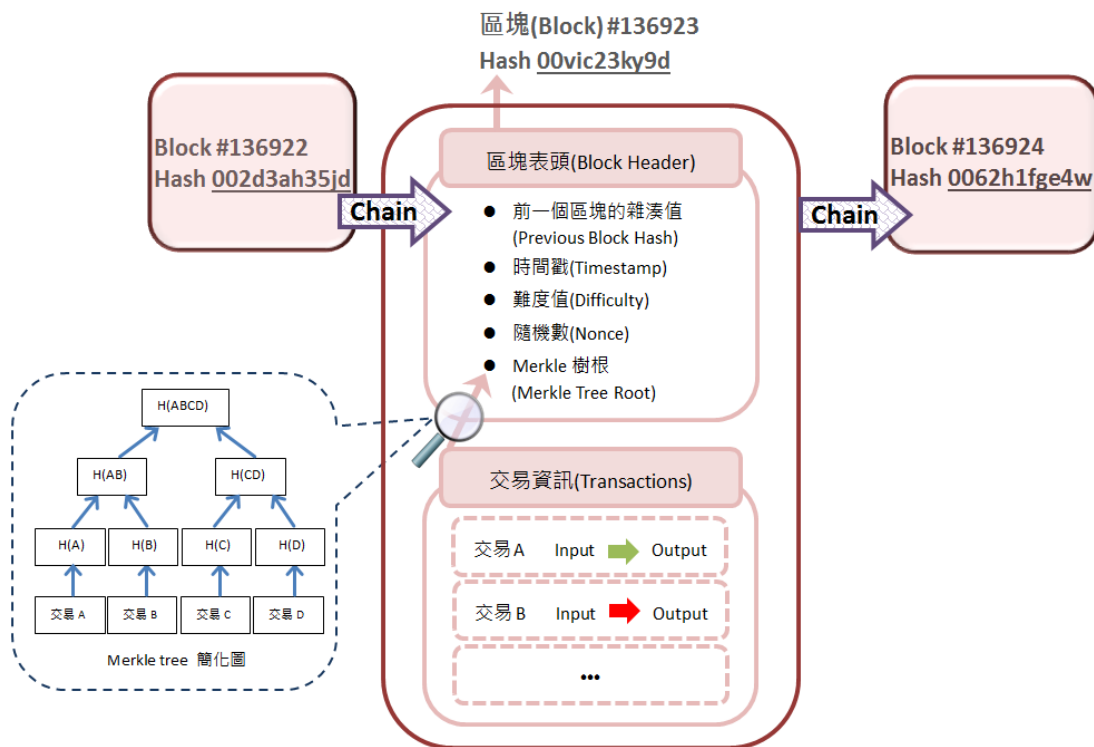
計算雜湊值所使用的參數。

5. Merkle 樹根(Merkle Tree Root)

由該區塊全部交易經過多次遞迴計算而產生的一個雜湊值。Merkle 樹(Merkle tree)是一種樹狀數據架構，依照雜湊(Hash)函數的運算結果所構建。先針對每筆交易本身進行 hash 運算，得出的雜湊值稱為葉子節點，節點每兩兩一組經過再次 hash 計算以建構其父節點，接著不斷重複該過程直到產生一個最終的

雜湊值。如圖 2，假設一個區塊有 A、B、C、D 四筆交易，經過 Hash 函數後產生四個雜湊值 $H(A)$ 、 $H(B)$ 、 $H(C)$ 、 $H(D)$ ，將雜湊值兩兩放入函數運算得出二個雜湊值 $H(AB)$ 、 $H(CD)$ ，再經相同計算得出一個雜湊值 $H(ABCD)$ ，即為 Merkle 樹根，該值便儲存於區塊表頭內。利用 Merkle 樹總結區塊中所有交易，因此可驗證某筆交易的存在，確保資料的完整性，若輸入數據有部分變動，計算出的雜湊值必然不同。另一方面，該架構可減少交易紀錄的資料量，如同對檔案進行壓縮，節省儲存空間。

圖 2 區塊構造



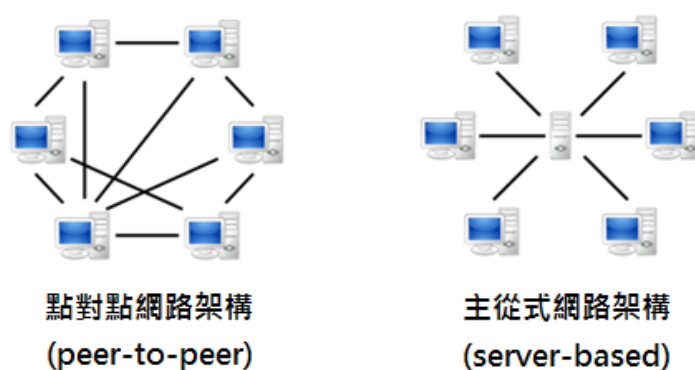
資料來源：自行整理。

(二) 點對點網路(Peer-to-Peer Network, P2P)

P2P 網路是一種沒有中央控制的網路技術或架構，透過用戶群(peers)之間傳輸型態實現資源分享及交換的網際網路體系，如圖 3。網路中的節點關係是對等的，不會有中心化節點存在，每個節點是服務端(server)，亦為客戶端(client)，可

自行決定成為運行所有功能的全節點(full node)，或選擇僅執行部分功能，可隨時加入或退出網絡。當節點越多，整個網絡系統越穩定，有助增強容錯性和抗攻擊能力，提升資料安全程度。

圖 3 網路架構分類

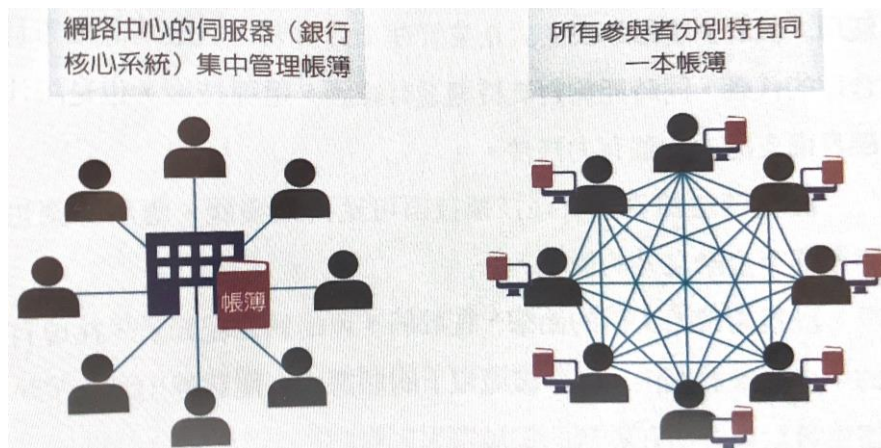


資料來源：作者整理。

(三) 分散式帳本(Distributed Ledger Technology, DLT)

不同於以往資料的儲存和交換透過中央式伺服器或機構負責管理，而是將維護的工作交由任何連接到該網路的電腦，稱為節點(nodes)共同分擔，如圖 4。參與運算的網路節點均擁有一份完整相同的帳本資訊，彼此互相連接，一旦新交易產生，各節點立即同步更新數據，實現分散式的儲存、紀錄和更新，整個網路系統所有資訊呈現公開透明。這種共享機制確保部分節點故障或退出，均不影響系統運作及帳本的完整性。

圖 4 資料管理方式



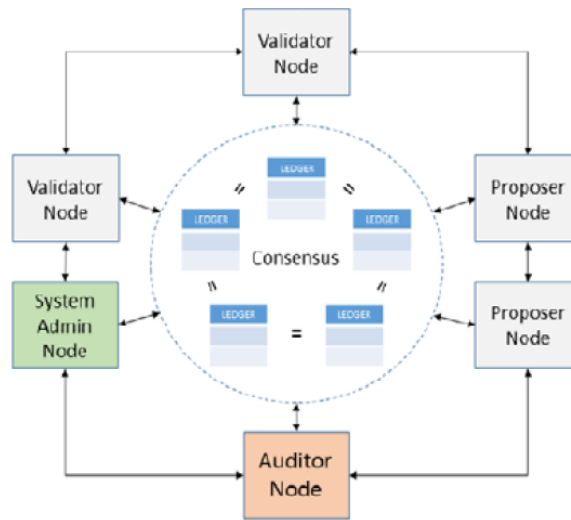
資料來源：Nikkei Computer(2016)。

(四) 共識機制(Consensus Protocol)

如前所述，區塊鏈提供一種機制保證所有人達成的共識是真實可信。那麼在分散式網絡架構的世界中，每個節點地位對等，在互不信任的前提下，要如何處理節點間達成相同共識的問題？要如何決定新生成區塊的先後以確保系統運行有序和公平？如何避免同一筆資金花費兩次造成的雙重花費(double-spent)？區塊鏈採用共識機制來解決此難題，就像是制訂一套供參與者遵循的交易制度和規則，其亦為構成區塊鏈中最核心的運作關鍵，如圖 5。目前，隨著共識技術的進展，演變出許多不同型態的共識機制，例如工作量證明(Proof of Work, POW)、權益證明¹(Proof of Stake, POS)和股份授權證明(Delegated Proof of Stake, DPOS)等。以下簡單介紹比特幣區塊鏈所使用的 POW 共識機制。

¹ 權益證明係指持有越多權益比例的節點越容易獲得記帳權；股份授權證明則類似於民主代議制度，先透過節點投票選出代理人，由代理人進行驗證和記帳。

圖 5 各節點遵循同一套共識規則



資料來源：整理自 Van Driel(2018)。

POW 機制基於電腦計算能力進行數學解題以獲取記帳權，該題目複雜難解卻容易驗證。所有參與運算的節點各自求解比特幣數學謎題，而謎題係以前個區塊資訊及當下的未確認交易(unconfirmed transaction)作為公式基礎，最快解題的節點將答案發布給其他節點套入公式中驗證，經集體證明無誤並接受後，即可將確認後的交易記錄打包為區塊並加到前一個區塊後面，接著系統即以此新區塊的值為依據產生下一道難題。換言之，前面區塊的資訊將以 hash 值的型態連結到下一個區塊，使區塊彼此相連。

要解開這道由比特幣網路所設計的工作量證明數學題具備三個組成要素：函數、區塊表頭及難度值，函數係指這道題目的計算方法，區塊表頭作為輸入數據，難度值則決定題目所需的計算量。比特幣網路採用 SHA256(Secure Hash Algorithm)函數算法，其數學公式可以簡易理解成，給定區塊資訊 X，須找到一個隨機值 N，使 X 和 N 代入函數 SHA256 中得出的雜湊值 H 小於目標值 Y。該過程可用下列公式表示：

$$H=SHA256(Block\ Header)<Y, Block\ Header=(X,N)$$

其中，H 為雜湊值 hash，X 為區塊資訊 block data，N 係隨機值 nonce，Y 代表目標值 target²。

由此可知，POW 機制即為找尋一個 nonce 值使該區塊的 hash 小於目標值。每個區塊除了本身的數據外，亦包含前個區塊的 hash 值，因此一旦前個區塊數據發生變化，原本所計算出符合規則的 hash 必然改變，藉著數學的方式，使區塊間產生無形的連結，彼此環環相扣，達成鏈(chain)的功能，確保資料安全且難竄改。

在分散式網路中，越多節點參與交易的檢驗，有助提高計算效率，促進系統運作越趨穩定。為吸引更多人加入，比特幣網路創造了誘因制度，讓節點間最先解出答案者，獲得寫入下一個區塊的記帳權以及比特幣作為報酬，而這個數學解題競賽的過程，稱為挖礦(mining)，參與爭奪獎勵的各節點，即為礦工(miner)。

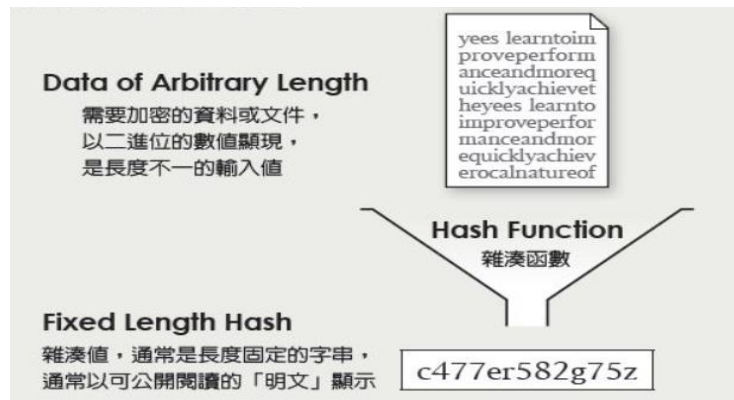
POW 為人所詬病之處在於解題所需的 nonce 為一隨機數，藉不斷的變換該值代入函數中，直到計算出符合要求的 hash 值，因此須投入相當多的資源，例如硬體設備及耗電量等，以完成大量的嘗試運算工作。

(五) 哈希函數(Hash Function)

哈希函數（又稱雜湊函數）係將任意長度的資料轉換成固定長度的一組字串，該字串即為 hash 值，如圖 6。

² 目標值的計算方式為目標值=最大目標值/難度值，其中，最大目標值為一恆定數，因此目標值的大小和難度值成反比，並隨著難度值變化做線性調整。

圖 6 雜湊函數特性



資料來源：陳君明(2017)。

哈希函數以數學公式表示為 $Y=Hash(X)$ ，具有下列特性：

1. 確定性：將相同的輸入代入哈希函數處理必會得到相同的輸出。即 $Hash(X)$ 必等於 Y 。
2. 易計算：給定輸入值 X ，要計算 $Hash(X)=Y$ 是容易的。
3. 不可逆：哈希函數為多對一映射函數，因此無法利用 hash 值反推訊息原文。已知 $Y=Hash(X)$ ，要透過輸出 Y 找出原訊息 X ，在計算上不可行，此特性又稱單向(one-way)運算。
4. 抗碰撞：對於任意兩個不同的輸入數，要輸出相同的 hash 值，即 $Hash(X)=Hash(Z)$ ，發生的機率極低。
5. 防竄改：對於任意的輸入值，即便是輕微的變動，就會徹底改變輸出的結果，如圖 7 所示。

圖 7 字串經雜湊函數轉換示意圖

$Hash(apple)=3A7BD3E2360A3D29EEA436FCFB7E44C735D117C42D1C1835420B6B9942DD4F1B$
 $Hash(apples)= F5903F51E341A783E69FFC2D9B335048716F5F040A782A2764CD4E728B0F74D9$

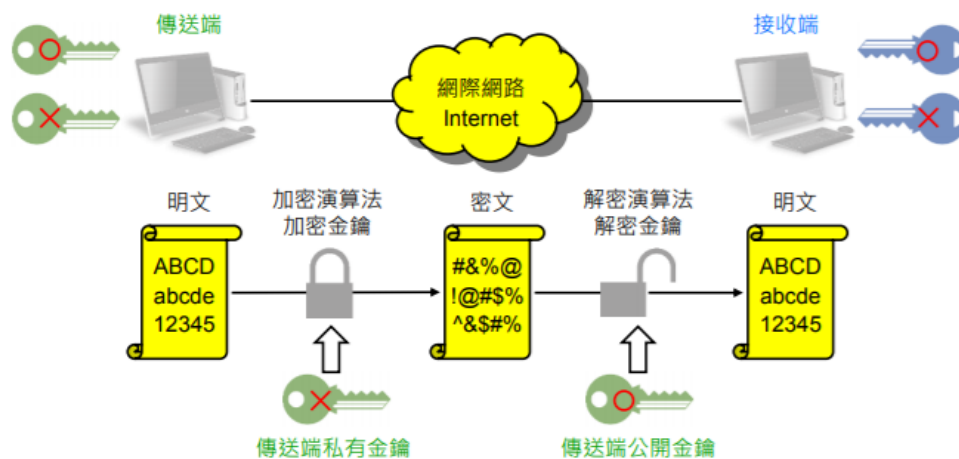
資料來源：王肇遷(2017)。

雜湊函數廣泛地被運用在區塊鏈中，例如交易時的數位簽章，建構區塊使用的工作量證明及彙總交易紀錄的 Merkle 樹等。

(六) 公開金鑰加密(Public Key Cryptography)

加密學係利用數學演算為原理對資料進行加解密，以避免傳送過程中發生資料外洩(data leak)及遭竄改風險，同時亦可驗證(verify)通訊雙方的身分。金鑰由一組字串組成，是加密演算法內的一個變數，如同密碼般，利用該金鑰可對明文(cipher text)產生相對的密文(plain text)，或將密文還原回明文。而公開金鑰加密，又稱為非對稱加密(Asymmetric Cryptography)，其於加解密過程中，分別使用兩組密碼—公鑰(public key)和私鑰(private key)，其特點有二：利用其中一對金鑰(公鑰或私鑰)加密資訊，唯有對應的金鑰得以解開；公鑰可對外公開，讓其他人用來加密傳送訊息，或可用於解密以認證身份，而私鑰則不可外洩。數位簽章(Digital Signature)即為此技術的應用實例，如圖 8，傳送端使用自己的私鑰對文件加密（或可稱為簽署），產生的密文連同公鑰發布至網路中，接收端若可使用傳送端的公鑰解密得到明文，即可驗證文件確實由傳送端發送，因為只有傳送端的公鑰可解開相對應的私鑰加密後的信息。

圖 8 公開金鑰加密驗證流程



資料來源：曲建仲(2017)。

(七) 區塊鏈模型架構

區塊鏈由多種技術堆疊而成的，而搭建區塊鏈所使用的模型架構可分成六個層次，如圖 9。

1. 資料層：最底層的數據區塊結構，如同設定記帳的格式。
2. 網路層：整個記帳體系的管理架構。
3. 共識層：各種共識機制採用，以決定由誰進行記帳。
4. 激勵層：將經濟因素導入區塊鏈中，決定了如何讓更多人自願參與記帳。
5. 合約層：可嵌入區塊鏈的電腦程式碼，達指定條件即可觸發系統自動執行。
6. 應用層：各類應用場景和案例。

其中的資料層、網路層及共識層是建構區塊鏈的基礎，而另外的三層則視使用情境而定，並不會出現在每個區塊鏈案例。

圖 9 區塊鏈模型架構



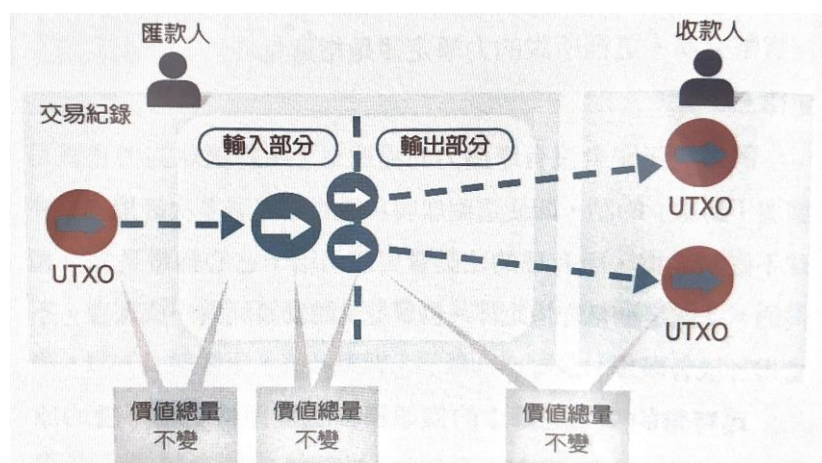
資料來源：自行整理。

三、區塊鏈實際運作模式—以比特幣為例

(一) 用戶間的交易流程

用戶雙方需要透過比特幣錢包(Bitcoin wallet)進行交易，比特幣錢包是一個應用程式，可安裝於電腦或手機。不同於傳統銀行帳戶以餘額呈現的管理方式，比特幣錢包將每筆交易分開列示，且分別記錄代表款項來源的輸入(input)和款項用途的輸出(output)，收到的比特幣在尚未花費前稱為未使用的交易輸出(Unspent Transaction Output, UTXO)，而未使用交易輸出將會是下一筆的輸入。以每筆交易為基礎的記帳方式有助追蹤軌跡，然而，若要得知帳戶餘額，則必須追溯整個交易歷史方能推算。

圖 10 比特幣交易紀錄方式

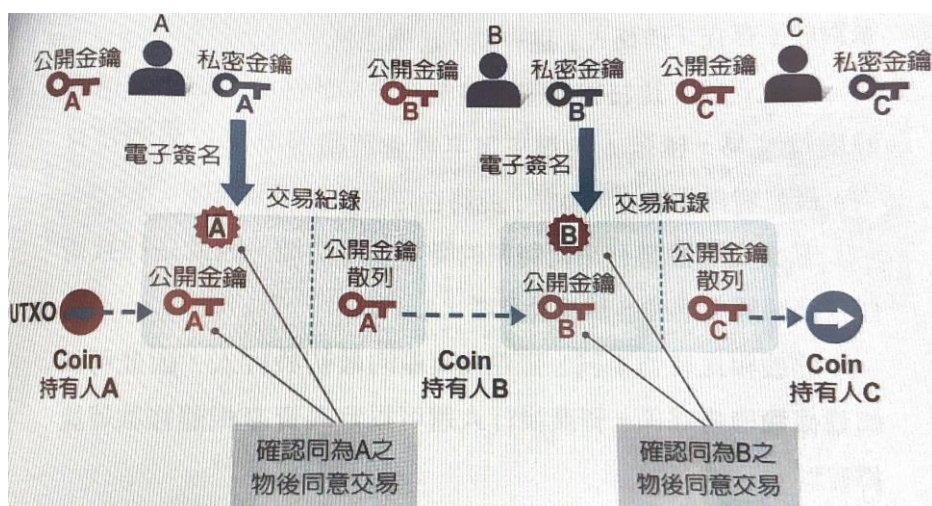


資料來源：Nikkei Computer(2016)。

每筆交易都有專屬的公鑰、私鑰以及比特幣位址(Bitcoin address)。公鑰為公開發布供驗證程序使用，私鑰則如同提款卡或銀行帳戶的密碼，用於證明對比特幣的所有權以發送款項，而位址的功能在於接收款項，實際運作方式如圖 11，當 A 進行轉帳給 B 時，需要 B 提供利用其公鑰經雜湊函數運算後（即公開金鑰散列）生成的比特幣位址，併同 A 使用自己的私鑰簽署所產生的電子簽名以及

當初收款使用的錢包位址，將資料經由網路傳送至各節點進行檢驗。若經節點確認並同意交易，將資料記錄到區塊鏈後，該款項即從 A 錢包地址轉移到 B 錢包地址。故從運作流程可知，任何人皆可透過區塊鏈上的公鑰和地址查詢每一筆交易，但必須擁有私鑰才能動用地址內的比特幣。

圖 11 比特幣交易運作方式



資料來源：修改自 Nikkei Computer(2016)。

(二) 區塊鏈的記錄

1. 產生新交易

接續前段，交易資料經網路傳遞，意即每當有新交易產生，系統會廣播 (broadcast) 至網路中的各節點。

2. 整合區塊的交易內容

各節點定期整合未確認的交易，查證其付款位址是否有足夠餘額支付轉帳款項並驗證簽章的正確性，接著將這些交易的 hash 值蒐集到區塊中，因此每個區塊包含多筆交易。

3. 決定負責驗證的節點

透過工作量證明及計算速度決定添加新區塊權利的節點。

4. 將區塊廣播給各節點

最先完成工作的節點將自己的區塊廣播給各節點。

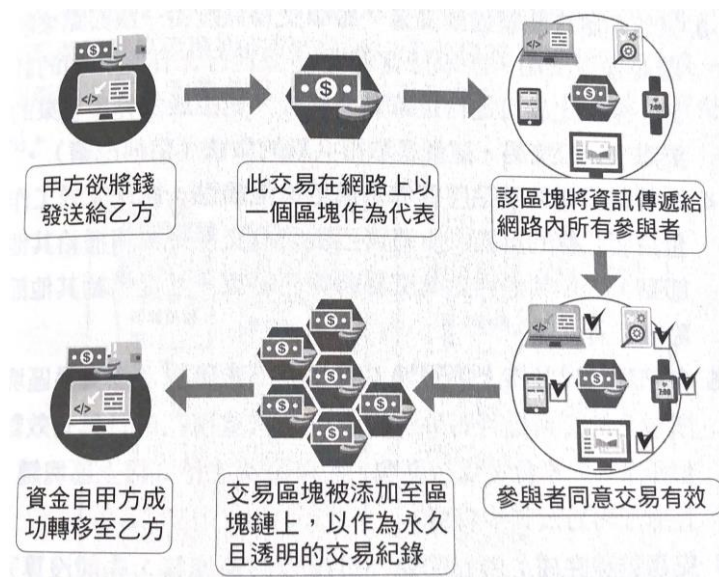
5. 各節點確認後接上區塊

其他節點確認該區塊內容的有效性，一旦接受(accept)該區塊，該區塊才正式連接上區塊鏈，無法再更動資料。

6. 再次進行創造區塊的流程

其他節點接受該區塊代表會利用該區塊的 hash 值計算下一個區塊的工作量證明，啟動創造接續新區塊的流程。

圖 12 區塊鏈運作流程



資料來源：王擎天(2018)。

四、區塊鏈特性

(一) 去中心化架構

交易的記錄係透過點對點軟體技術，不存在中心化的主機硬體或中央管理機構，整個網絡由所有用戶共同維護並同步更新訊息。

(二) 交易不可逆

一旦訊息經過驗證並添加至區塊鏈中，即永久儲存，無法撤銷或取消。

(三) 不可竄改

區塊鏈採用多次的單向性雜湊函數，區塊間均滿足嚴謹的數學計算條件鏈接在一起並按時間排序，前一個區塊的 hash 值已經包含在後一個區塊的 hash 值內，一旦更改某區塊中的資訊，將因不符規則變成無效。

(四) 資訊公開

區塊鏈開放給公眾參與，包括鏈上所記載的完整歷史資料、運行的協議和程式碼等對所有人都是公開的，系統呈現高度透明化，實現數據共享。

(五) 匿名性

用戶間遵循共同認可的機制，由寫入區塊鏈系統中的電腦程式自行判斷及運作，各節點或交易雙方無須信任彼此，因此不需公開自己的身份，每個用戶都是匿名的。

五、區塊鏈的本質—價值移轉

網際網路(Internet)的發展讓資訊的分享和流通變得便利，讓人們可以不受時空拘束，無時無刻和全球互動。而使用網路傳遞訊息時，實際上只是傳送複製的原有資訊，例如在傳輸電子郵件的過程中，無論是發送端和接收端，都保留著信件內容的副本，因此目前的網際網路僅能處理訊息交換。

在真實世界中，人們經常從事的是價值交換行為，如果想要透過網路上對有價值的資產—金錢、商品或產權等進行交換，這種資訊複製的邏輯便不可行，舉例來說，我跟 A 買一個物品，我在自己的電腦把 100 元轉給 A，我還是保留那 100 元的原檔，給 A 的僅是 100 元的複製檔而已，當付出的金額無法同時減少，如此的價值交換便無意義。真正的運作應該是「我把錢付出去，我手上即不應該有那筆錢」。

由於網路並無保護價值傳輸的機制，在交易雙方缺乏信任的情況下，從事價值交換活動時即須透過仲介系統協助，例如網路購物需要中間機構—銀行或第三方平台參與確認金錢和物件的交換。

而區塊鏈技術創建了一套以信用共識為基礎的機制，利用自動運行的網路運作模式來完成價值的傳遞，以比特幣的應用即證明在區塊鏈的架構下，可以安全的讓金錢在網路流動，過程不需中間人經手。在上段的例子中，我把 100 元轉給 A 時，區塊鏈就會確保我的帳本少 100 元，而 A 增加 100 元。

因此，區塊鏈被認為是新一代網際網路基礎建設，將現階段訊息型網路(Internet of Information)升級為價值型網路(Internet of Value)，人們得以隨時隨地在網路傳遞和儲存有價值的資產。而隨著相關技術不斷優化，由區塊鏈打造全球性的價值生態體系，勢必將重塑我們的生活、經濟和世界。

參、區塊鏈對會審領域帶來的變革

會計，是一連串過程的總稱，以有系統的方式詳實記錄特定個體相關經濟活動，實踐財務當責。這個過程從一筆筆交易發生開始逐步進行，先辨認每筆交易的經濟事項、衡量經濟後果，衡量完成後，接著記錄、分類、彙總這些經濟後果，並編製財務報表供利害關係人使用，從每筆交易著手，在會計帳冊上做成清楚的文書記錄。而審計的功能，則在於驗證這些會計帳冊的真偽，因此整個會計審計體系可說是圍繞著帳本展開的。區塊鏈被視為先進的數位化帳本技術，究竟將賦予會計行業怎樣的嶄新樣貌？以下探討區塊鏈在會計相關領域可能產生的影響。

一、會計帳務處理

複式簿記法(double-entry accounting) 是現代會計的核心，在十五世紀的義大利興起即普遍沿用至今。翻開複式簿記用的帳本，頁面以兩個欄位呈現，左邊的是借方(debit)，右邊則是貸方(credit)，每筆交易的金額記錄到一個帳戶的借項中，就一定要在另一個帳戶中記錄對應的貸項，接著予以加總，借方總額必然等於貸方總額。基於複式分錄所衍生的會計平衡原理，不僅有助檢查交易記錄的正確性，亦易於計算獲利和虧損，更能精準掌握財務狀況。

區塊鏈為記帳系統帶來新的變革稱為三式簿記法(triple-entry accounting)，係將傳統複式簿記的觀念加以擴展，除了將交易記入借方和貸方外，也記錄在區塊鏈網路中，因此交易雙方及區塊鏈均保留完整的交易資訊，利用三方共同記帳的方式確保交易的可靠和信賴度。

二、財務報告編製

透過區塊鏈技術建立統一格式的分布式帳本，增加企業內部和企業間的會計資訊透明度，可簡化進行試算和調整的流程，並藉同步結算實現資料串接整併，

更能即時掌握企業各項財務狀況，減少花費在對帳和合併的帳務處理時間，迅速完成財務報表編製作業。

三、查核工作內容

企業在區塊鏈上建立一個公開透明的財務系統，每筆交易都在區塊鏈上即時(real-time)進行，在這個能隨時擷取更新資料的環境下，非常有利於導入持續性稽核(continuous auditing)。

持續性稽核是一種以連續性為基礎且高度仰賴資訊科技所執行的稽核工作。運作原理奠基於電腦輔助查核工具與技術(Computer-Assisted Audit Tools and Techniques, CAATTs)，應用先進的分析工具和高效能設備，以自動化方式擷取特定時間的資料並進行分析，能夠即時從資料來源端取得關鍵資訊，後續的風險評估也能隨時並且持續地動態進行，提供迅速並精確反映所發生的事實和狀況的稽核報告。

查核人員作為企業區塊鏈上的一個節點，持續執行交易過程的各項查詢、監控和稽核分析作業，對於突然發生的異常項目和例外狀況，可立即採取回應，因此稽核流程中所包含的規劃及前置作業、決定查核程序之性質時間範圍、執行測試採用的方法等，皆將轉變為以即時風險為導向，針對風險較高項目投入稽核資源，更能彈性調整監控與稽核計畫，與過去每年定期辦理的傳統稽核不同，雖然傳統稽核可針對檢查結果對疑慮項目再次進行例外調查，原則上仍屬固定頻率的查核。此外，自動化作業減少人工稽核的負擔，降低耗費在彙總、調節和判讀實體帳目的處理成本。

綜上所述，利用區塊鏈各節點資料同步的特點，實現將傳統事後查核模式提前至事前預防和即時偵測的預警模式，查核頻率將變得頻繁，方式也更為主動，聚焦在重要風險加強深度及廣度，更具效率和效果地執行查核，提升稽核品質。

四、查核重點考量

(一) 交易本質的驗證

區塊鏈分散式帳本與不可竄改的特點，讓查核人員不需投入過多時間核對與檢查資料正確及完整性，可省去確認文件真偽的紙本作業，而區塊鏈上的記錄皆經過交易雙方數位簽章的驗證，保證交易的真實性，也不再需要透過如函證等繁瑣的多方驗證程序。

然而，真實發生的交易及正確無誤的內容並不代表企業的營運活動係按照經營目標合乎規定地進行交易，換句話說，偽造、虛構、詐騙、未經授權及違法的交易仍有可能存在。而若涉及實體交換，單就區塊鏈的數據信息無法辨識和確認交易已經完成，例如物品是否已確實交給買方。此外，是否屬於關係人交易、是否正確歸屬至適當會計科目以及鏈外(off-chain)交易³，均為查核人員應關注的重要議題。

(二) 區塊鏈技術衍生的風險

區塊鏈重塑商業模式，優化現有的交易流程，但同樣存在前所未有的風險隱憂，查核人員必須研發新的風險管理技術和應變措施。在區塊鏈世界中，控管風險的體系主要著重在「鏈」本身的技術風險，分述如下：

1. 公開金鑰衍生的隱私和安全風險，例如私鑰保管、遺失、認證和暴露風險。
2. 區塊鏈各環節採用大量的演算法技術，高度複雜性衍生計算錯誤或設計缺陷產生系統漏洞的風險。
3. 共識協議的信度(reliability)，包含運作結果的一致性、穩定性和可靠性。查核人員需評估協議是否遭人為操縱，或被刻意攻擊。

³ 鏈外交易指在鏈外處理交易，每隔一段時間，再把結果寫入區塊鏈，以提升區塊鏈運作效率。

4. 區塊鏈可承載交易量的設定，取決於尋找滿足特定條件對數解的難度、節點的運算能力、參與節點的數量及交易廣播到各節點的速度等影響因素，因此需注意性能瓶頸(*scalability constraints*)可能導致業務運作遲滯或造成額外損失。
5. 符合區塊鏈相關法律規範及滿足監管要求的遵循風險。

(三) 新型態的網路安全(*Cyber Security*)風險和內部控制

即使在公司封閉的內部網路環境仍有可能遭受惡意攻擊，區塊鏈網路也可能成為駭客威脅的目標。由於區塊鏈分散式儲存資料的特性，部分節點遭攻擊癱瘓均無法影響其正常運作，具有充分的韌性(*resilience*)，然而只要在駭客眼中是有利可圖的攻擊對象，各節點仍無可避免地將成為鎖定目標。

在比特幣區塊鏈中，駭客主要攻擊的目標可分為兩種，一種是入侵交易所，因為大量集中資產和客戶資料吸引駭客目光，一旦攻陷即可獲得豐厚報酬；另一種是透過網路釣魚方式竊取節點電子錢包內的密碼，將私鑰詐騙得手後就可以把錢轉出。無論何種攻擊方式，駭客攻擊的目標都不在於區塊鏈本身的運作，而是在區塊鏈應用的端點找尋潛在的資安漏洞。查核人員對於任何可能遭受攻擊的管道，例如系統運作、網路協定、數位簽章及智慧合約等，都應該發展一套風險規範和防護標準，並持續強化實體和邏輯存取控制(*physical and logical access controls*)，以保護網路降低非法侵入或資料外洩的風險。

(四) 系統接口

考量企業現行的關連式資料庫或資訊系統，例如 ERP 系統等，皆已穩定運轉，長時間累積下來也貯藏豐厚的資料量，非區塊鏈技術短時間能取代，因此未來企業引進時傾向將區塊鏈與現有資訊系統介接，然而整合接口的介面也是最可能存在弱點，查核人員宜特別關注其相關風險。

五、查核人員新角色

(一) 智慧合約的驗證服務

智慧合約係將商業規則或合約交易條款程式碼化內嵌在區塊鏈系統，在特定條件被系統判斷為符合時，條款將自動執行，並依預定方式影響合約各方權利與義務。由於智能合約牽涉多方的權益，加上編寫技術本身的困難度且需將電腦程式語言轉化和人類意圖相對應，因而衍生出專業的智能合約認證需求，例如智能合約查核人員，負責驗證智能合約能否表達合約多方的真實意圖，是否存在未經辨認的錯誤和系統弱點，是否合乎企業正常營業活動和經營邏輯，評估管理階層是否對智能合約建立健全的內控制度以確保其運作的一致和穩定性。為了要扮演好這個重要角色，查核人員必須發展出一套專門針對智能合約的查核技能，包含熟悉程式編碼語言和增進智能合約相關知識等。

(二) 區塊鏈企業協議糾紛的仲裁人

企業面臨激烈競爭的經營環境，為創造優勢，公司間常見相互締結策略聯盟的關係並訂定合作協議。如同智慧合約的應用一樣，這類協議將被部署於企業間彼此串接的區塊鏈網路中執行。若衍生出法律糾紛或合約爭議，仍需透過訴訟或仲裁方式解決，舉凡律師或會計師等專業人士皆有可能擔任仲裁人。考量日後區塊鏈應用範圍擴大，對仲裁服務需求將日益殷切，查核人員應適時培養相關素質與能力以提供該類服務滿足社會期待。

肆、區塊鏈於會審實務可能應用場景

一、智慧合約與會計處理—以 IFRS15 客戶合約之收入為例

收入認列是衡量營運表現的起點，在財務報導上也是關鍵的財務數字，備受大眾重視。然而認列的時點和方式需仰賴許多判斷輔助，為增進財務報告的可比性，準則針對收入相關議題提供相當多的指引，惟目前實務上商業模式呈多樣性，在準則的適用上部分仍存有爭議。此外，遠距離銷售或市場通路分散往往導致企業難以掌控商品或服務實際售出情形，造成認列的落差。因此學術界開始思考是否能運用先進技術協助處理複雜的會計準則規定。舉例來說，智慧合約非常適合運用於處理具有複雜商業邏輯，附帶觸發條件的合約條款，若將該技術應用在自動化認列收入，即可減少會計人員不必要的主觀判斷，避免做出不一致的認列結果。而 IFRS 15 準則提供可逐步推行「收入認列五步驟」觀念性架構正好切合智慧合約應用邏輯的需求，會計人員先將認列的相關規定及考量因素編碼程式化，藉由電腦系統蒐集合約動態、更新資料，自動化判斷和執行相關會計處理。情境設想依序探討如下：

圖 13 收入認列 5 步驟

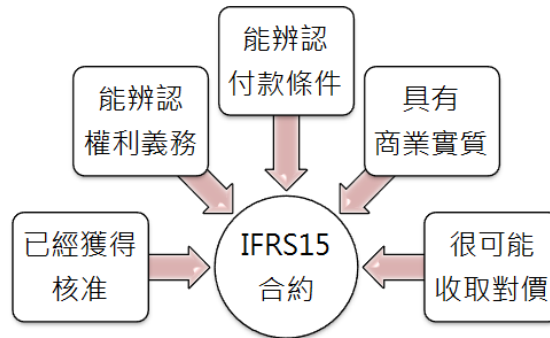


資料來源：自行整理。

流程①辨認與客戶間之合約

合約之定義必須符合所有條件，企業始能依 IFRS15 進行會計處理，因此需先將合約轉換成統一格式，經標準化後由系統依條件進行判斷，如圖 14。

圖 14 合約定義判斷邏輯

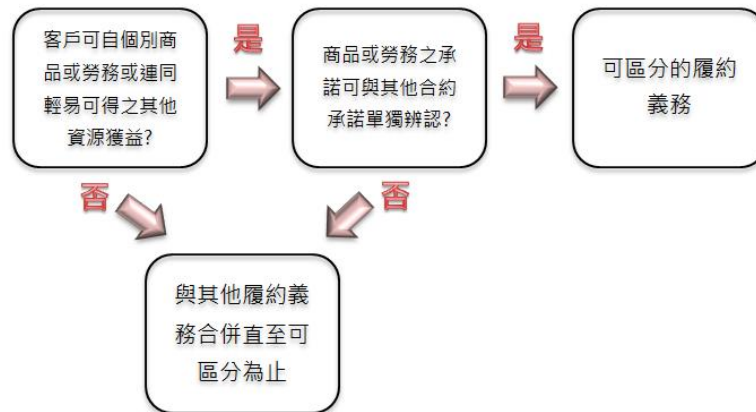


資料來源：自行整理。

流程②辨認合約中的履約義務

合約中的履約義務是否可區分的判斷條件如圖 15。

圖 15 履約義務判斷條件



資料來源：自行整理。

若之前即存在銷售個別履約義務的紀錄，則可連結至舊智能合約，以取得前次交易資料的內容。智能合約的資料是無法竄改的，可確保歷史紀錄的可信度。

流程③確定合約價格

交易的對價金額會列示於合約，若其中包含變動的對價，企業應使用期望值或最有可能金額估計，因此應於智能合約中提供變動對價發生的機率及對應金額等資訊。

流程④分攤合約價格

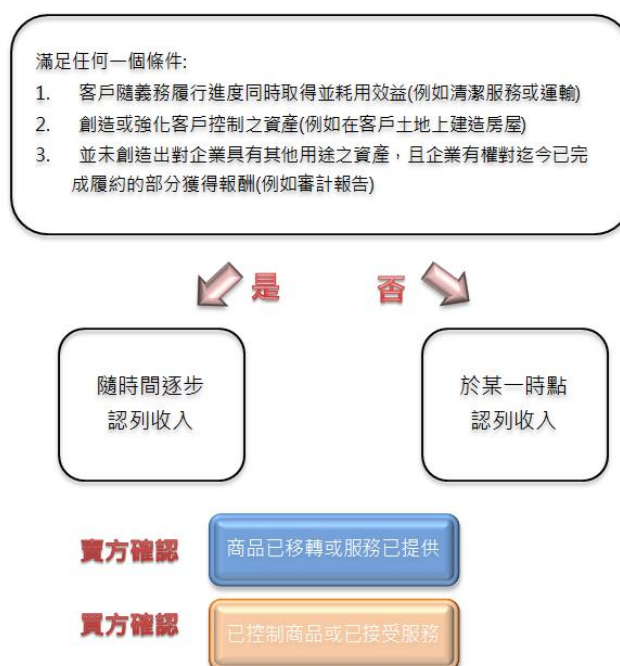
智能合約依各履約義務的相對單獨價格為基礎，自動分攤合約價格。

流程⑤在履約義務滿足時點認列收入

銷售時點的確認，可藉智能合約中條件設定於滿足履約義務的時點即認列收入。而滿足履約義務意味著企業將承諾之商品或勞務之控制移轉給客戶，因此需先評估商品或勞務之控制係於某一時點移轉或於一段期間移轉，據此區分為兩種收入認列模式，即某一時點認列或隨時間逐步認列，而辨認控制是否移轉於實務適用上多數仍需涉及會計人員的專業判斷。

建議在某一時點的認列模式下由賣方啟動「商品已移轉或服務已提供」的提議，並提示買方於智能合約上相對確認「已控制商品或以接受服務」；而依完成程度認列模式則仰賴買方逐次認定其「已逐步」控制商品或接受服務。兩種認列模式均可能碰到延遲確認的買方，最好能在智能合約附加條件，若經數次通知後買方仍未確認，則視為已確認，避免因買方疏忽而延誤認列收入。收入認列的判斷條件如圖 16。

圖 16 收入認列時點



資料來源：自行整理。

二、電子函證金融區塊鏈平台

財金公司為順應國內銀行加速佈局區塊鏈的趨勢，於 2016 年 9 月 20 日由國內外金融機構及周邊單位等 48 位會員機構共組「金融區塊鏈研究暨應用發展委員會」，以達資源整合發揮綜效。其中，與 20 家國銀合作推動的「金融區塊鏈電子函證平台」，目前已和四大會計師事務所簽約，預計自 2018 年半年財務報告開始試行，會計師進行查核簽證時，即可透過該區塊鏈平台實施函證之審計程序。利用區塊鏈不可竄改、保障隱私、可追蹤紀錄等特性有助提升函證之效率和品質。

(一) 現行函證作業之流程

圖 17 目前函證作業流程



資料來源：黃宣蓉等(2018)。

流程①查核人員填寫詢證函，發函給廠商、客戶及有往來之金融機構。

流程②查核人員請求客戶用印授權。

流程③受查客戶核對資料無誤。

流程④受查客戶確認用印授權。

流程⑤查核人員郵寄詢證函，須針對已發函之詢證事項、函證結果及相關索引編號等設置控制程序，以掌握回函進度。

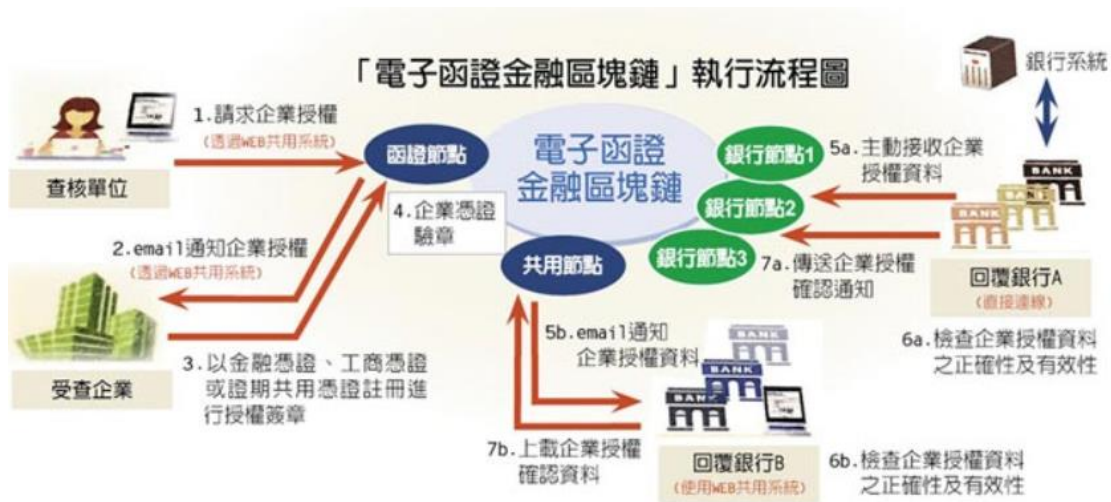
流程⑥受函證者填寫回函。

流程⑦受函證者郵寄回覆結果。

(二) 現行函證作業之痛點

傳統函證作業耗費大量的人力、物力及時間，包含查核人員及受查者人工紙本謄寫查填回覆、郵寄往來時間等，且過程中又容易發生錯誤、疏漏、偽造、舞弊與遺失等風險。而改以電子郵件形式雖可節省遞送的時間和成本，卻亦涉及回函者身分和權限難以驗證、流程中被攔截或變造等可靠及安全風險。

圖 18 電子函證金融區塊鏈執行流程圖



資料來源：朱漢崙(2018)。

(三) 電子函證區塊鏈架構

為了維持整體網路傳輸速度及成本，區塊鏈內各節點可分為下列三類：

1. 函證節點：審計方共用節點。於該節點架設 WEB 共用系統供查核單位參與。
2. 共用節點：回覆方共用節點。考量國銀規模及硬體設備等因素，對於數位化程度不高的參與銀行，於該節點架設 WEB 共用系統供非直連銀行使用。
3. 直連銀行節點：回覆方直連結點。針對高數位化的參與銀行，設置直連結點，可直接與銀行內部系統連線。

(四) 電子函證區塊鏈流程

流程①查核人員登入 WEB 共用系統進行函證申請。

流程②透過 WEB 共用系統向受查客戶發出授權請求。

流程③受查客戶以憑證註冊進行授權簽章。

流程④WEB 共用系統確認雙方之關係並根據所設定的權限以驗證授權。

流程⑤、⑥授權之函證發函至回覆方。直連銀行節點主動接收函證請求，並直接與銀行內部資料庫核對及填覆；非直連銀行則利用 WEB 共用系統接收函證，以人工方式查填並於系統上回函。

流程⑦回覆的函證直接回傳於函證節點，WEB 共用系統將提供載點下載。該電子函證經數位加密，必須具有權限的查核人員才得以其私鑰解密函證。

(五) 電子函證區塊鏈之亮點

藉由區塊鏈平台，可大幅減輕函證程序的兩個重要關鍵—身分和權限驗證所產生的風險，回覆方的身分可經由數位憑證確定身分，在系統上預先設定對應回函的權限可幫助確認授權，詢證函以電子簽章加密，僅查核單位和回覆銀行可取得並解密，過程中不會產生舞弊、資料外洩及竄改等風險，又可提供稽核軌跡，節省人力成本，縮短函證作業時間，增進查核效能。

三、自動化法規遵循

近年來，為防範金融風險再次發生並促進市場穩定，各國政府相繼加大對金融業的監管力度，日益繁重的法令規定迫使金融機構法遵成本遽增。金融機構在強化法令遵循所投入的成本除了內控內稽和風管制度、委託會計師辦理查核財報外，針對不同監理要求，例如稅務、資本適足率(Capital Adequacy Ratio, CAR)、防洗錢(Anti Money Laundry, AML)、打擊資恐(Combating the Financing of Terrorism, CFT)等，產生額外的因應措施又進一步導致經營成本向上攀升。

2016年8月世界經濟論壇(World Economic Forum, WEF)發表的區塊鏈技術將如何改造金融服務研究報告揭示未來金融機構導入區塊鏈以達成自動化法令遵循(Automated Compliance)的可能性。

(一) 現行法令遵循之流程

圖 19 目前法遵流程



資料來源：World Economic Forum(2016)。

流程①金融機構每年委任會計師辦理財務報表查核簽證，並對相關事宜進行安排與協調。

流程②查核團隊實地執行查核工作，確認所需資源並視風險評估結果決定查核程序之性質、時間和範圍。

流程③受查機構提供大量紙本財務資料，並在查核期間允許團隊成員連結至公司資訊系統直接讀取資料進行查核分析。

流程④查核團隊執行測試驗證資訊的完整和正確性。

流程⑤查核團隊在整個查核期間持續與管理階層、治理單位討論重大缺失或適時發現。

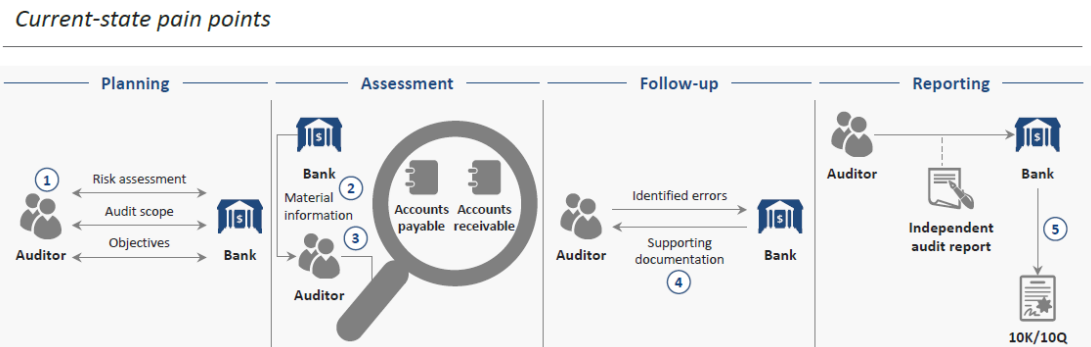
流程⑥查核團隊若對機構之經營有疑慮，可要求額外補充資訊以加強查核深度。

流程⑦查核工作完成階段，團隊成員根據查核結果，對整體財務報表是否允當表達表示意見，出具獨立查核報告(independent audit report)。

流程⑧受查機構將查核完成的財報送交不同的監理單位，例如證交所、金管會或稅務單位，提交相關的申報資料。

(二) 現行法令遵循流程之痛點

圖 20 目前法遵流程痛點



資料來源：World Economic Forum(2016)。

痛點①查核團隊進行實地查核時，需要受檢人員配合調閱資料並詳實答覆，雖盡量避免不必要的檢查或詢問，然或多或少影響其業務運作。

痛點②由於查核報告須於規定期限內提交，查核工作往往投注龐大的人力、物力與時間進行記錄核查，且因成本有限，僅能實施抽查。

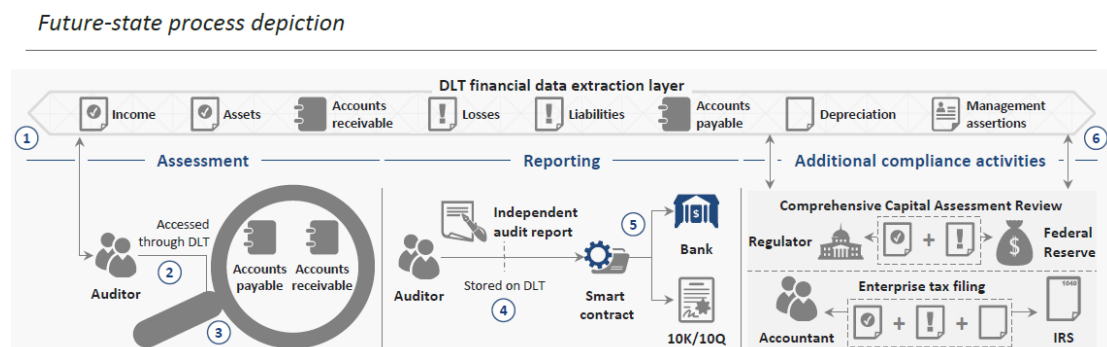
痛點③查核團隊若未獲准進入受查機構之資料庫系統，相關資料以人工複製摘取，增加錯誤的可能性。

痛點④查核團隊和管理階層、治理單位的溝通討論亦多少影響其日常業務。

痛點⑤向不同監理單位申報資料時，所受理的報導格式往往不一致，增加轉換之作業成本。

(三) 未來區塊鏈法令遵循之流程

圖 21 未來法遵流程



資料來源：World Economic Forum(2016)。

流程①查核團隊透過節點連結至受查機構區塊鏈平台萃取即時財務資訊。

流程②由於查核團隊可於平台獲取查核所需資料，避免打擾經辦人員日常工作。

流程③查核團隊可於平台上直接進行資料分析，避免手動複製發生之錯誤。

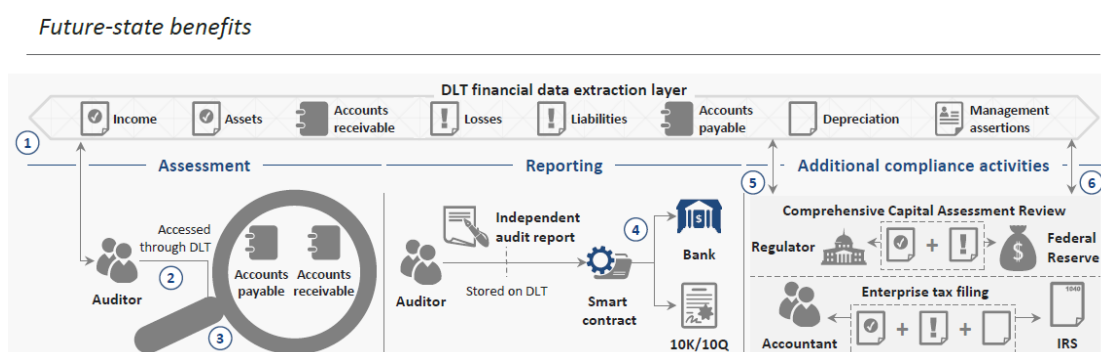
流程④查核進度和查核報告結果亦能於平台分享，保留完整審計軌跡，供受查機構或監理單位即時查閱。

流程⑤透過智能合約的部署，定期將財報資訊轉換成多種面向的分析報告，以滿足不同財報使用者需求。

流程⑥區塊鏈平台可持續地自動執行相關遵循的業務活動。

(四) 未來區塊鏈法令遵循之亮點

圖 22 未來法遵流程優點



資料來源：World Economic Forum(2016)。

亮點①透明性：在區塊鏈中，每項交易資料均獲得驗證和記錄，且一經確認後即不得修改，並供即時公開查閱。

亮點②自動化審計：查核人員可於節點嵌入審計軟體執行即時查核工作，得以驗證每筆交易，實現全範圍審計，大幅節省投入人力和時間等資源，加快稽核進度。

亮點③減少錯誤：利用科技的輔助可消除人工處理程序下的人為錯誤。

亮點④整合系統：所有資訊皆儲存於區塊鏈上，將財務報告及其他須申報的內容加以整合，利用標準化模組將資料直接進行轉換。未來公司要準備各式報表時，可重複使用區塊鏈的資訊並將其用於不同目的之上。

亮點⑤、⑥擴大法遵需求：自動化大幅減少耗費的遵循成本並減輕行政負擔，在法遵得以有效落實下促使受查者可進一步滿足監理機關更為精確的監管需求。

伍、資料科學領域與內部稽核相關議題

一、稽核本質在於分析資訊

內部稽核職能係協助機構檢查其營運活動及管控措施等實施狀況，並適時提供改善建議。內稽人員必須獲取充分且適切的證據，據以支持稽核意見和結論，而蒐集查核事項相關資料，並進行辨識、分析、評估及記錄等過程也成為內稽主要工作程序。因此稽核本質上與資料運用存有密不可分的關係。而資料科學(Data Science)的快速進展，是促成內稽升級轉型的關鍵利器，透過大數據或人工智慧等技術從龐雜的資料量解讀資訊意涵，更能深入瞭解組織運作的實際樣貌，洞察風險所在與掌控情況，並藉由數據趨勢預測可能衝擊，及早發現與因應，提升稽核效能與價值。

二、大數據四項特質與內部稽核

(一) 資料量(Volume)

內稽人員稽查對象遍及組織各部門及所屬單位，手中握有相當廣泛的資料和文件，這些資訊一直都存在著，但傳統稽核受限於資源配置，通常僅能以抽查方式實施，難免產生抽樣風險，導致解讀證據的偏差；大數據的應用可檢視所有交易資訊，透過全面且完整的檢視母體數據，得出的分析結果貼近事實而不再僅只是推論，提高信賴程度。

(二) 資料類型(Variety)

數位化時代的來臨，數據的來源和種類呈多樣性，其中以非結構化資料(unstructured data)占絕大多數，這些數據包含許多不同的格式，例如文字、圖片、音檔、影片等。利用大數據探勘技術可處理結構化、非結構化、傳統財務資訊或

非財務資訊等多元類型資料，並能將組織內部或外部等多種來源數據整合成既定格式，便於內稽人員提取彙整後的資料進行加值分析。

(三) 資料速度(Velocity)

資料的產生及更新速度越來越快，大數據技術具備即時且高速處理資料的能力，讓講究時效的持續性稽核得以落實，能夠以連續性、立即回應為基礎進行稽查活動。

(四) 真實性(Veracity)

真實性攸關資料品質與可信度，是影響決策精準度的關鍵要素，也是資訊分析的根基。對內稽人員而言，運用分析技術前必須充分了解數據的定義、來源、係於何種情況下產生、確保數據安全的相關措施等，並將偏差、偽造、異常等資料過濾去除，避免使用品質不佳或不完整的數據進行分析，使結果偏離事實，得到錯誤資料解讀，造成決策失當。

三、人工智慧(Artificial Intelligence, AI)與內部稽核(Internal Audit, IA)

人工智慧可定義為讓機器展現人類智慧的科技⁴，而機器學習(Machine Learning)則是實現 AI 的一種方式，奠基在強大的運算效能和海量數據，讓電腦自行學習從資料中摸索運行規律進而創造演算規則，且持續精進改善，達到像人類一樣具有辨識或預測能力，是時下資料科學領域備受關注的技術之一。傳統的機器程式需要透過人工編寫一步步的指令以完成特定任務，那麼當人類不知道問題的解答時，機器同樣無法回答問題，然而透過機器自主學習可以協助探索未知領域，激勵人類智慧發展。

⁴ Artificial intelligence is a broad term that refers to technologies that make machines smart.

(一) 機器學習的方式

1. 監督式學習(Supervised Learning)

在訓練的過程中明確告訴機器答案，意即所有資料均含有人工標記(label)。

2. 非監督式學習(Unsupervised Learning)

訓練的資料沒有標準答案，不需要事先輸入標記，而是讓機器自行解析關連結構，找出擁有相同特徵的資料群或潛在規則。

3. 強化式學習(Reinforcement Learning)

直接讓機器根據不同的狀況嘗試各種行動，每進行一個動作，外部環境都將隨之改變，但訓練時並不會告訴它所採取的哪一步驟是正確、哪一步驟錯誤，而是給予正負回饋，若環境的變化離目標更近，則給予正向回饋(positive reward)；若離目標更遠，則給予負向回饋(negative reward)，機器再將執行結果的回饋內化吸收，逐步修正行動以達到最佳目標。原則上無須考慮過去的狀態，每一個事件只受到前一個事件的影響，適合運用在需要進行一連串動態決策的情況下，圍棋程式 Alpha Go 便是強化式機器學習的一種應用。

(二) AI 與內稽工作

1. 稽核程序自動化

將重複、大量、具規則性及程序繁瑣的庶務交由電腦進行，例如對例行業務活動可實施即時監測，自動過濾不合理交易以縮小稽查範圍，針對篩選出可能舞弊或異常事項，立即採取行動。另一方面，可持續蒐集查核證據，進行勾稽、比對並將分析結果產生稽核所需報表，加速稽查時程。

2. 協助探索全新觀點

利用 AI 先進的認知智能技術，有助挖掘隱藏的洞察，捕捉從前未能解讀的資訊涵義，並研判趨勢及動向，對未來可能發展做出預測，讓內稽人員得以嶄新、周詳的思維展現內稽的核心價值。

(三) 針對人工智慧的稽核重點

1. AI 治理(AI Governance)

組織為達成目標導入 AI，進而針對 AI 活動所進行指導、管理和監督的程序，其強調以課責性為基礎以確保 AI 活動能反映組織價值。

2. 資料架構與基礎設施(Data Architecture and Infrastructure)

有關資料存取的管控、隱私和安全性、資訊使用者和擁有者的職責。

3. 資料品質(Data Quality)

如同人類的學習一樣，AI 演算法需要運用資料進行訓練以萃取出特徵，因此如何選擇正確和合適的資料至關重要。組織必須確保資料的正確、完整和可靠性，避免將偏差或錯誤值作為輸入的訓練資料。

4. 對 AI 進行績效評估(Measuring Performance of AI)

組織必須訂定績效指標衡量 AI 活動有效支持組織目標的達成。

5. 人為因素(The Human Factor)

AI 係由人類開發製造，難免內含人為錯誤或偏差進而影響演算法的效能，組織應清楚辨識並管理該等偏誤風險，確保 AI 的產出成果使用符合法律、道德，並對使用行為負責。儘管 AI 技術的複雜性，組織應保持 AI 相關資訊公開透明以取得大眾信任。

6. 黑盒效應(The Black Box Factor)

深度學習(Deep Learning)是進階版的機器學習方式，模擬人類神經網絡的運作方式，讓電腦處理更多信息的關聯性，做出更精準的判斷，更能呈現人類智力的特徵。在這樣高度複雜演算法中並不存在明確的規則，無法確切理解 AI 的思考模式，因此稱為黑盒效應。內稽人員須協助組織理解並關注 AI 內部運作過程不具透明度所構成的風險。

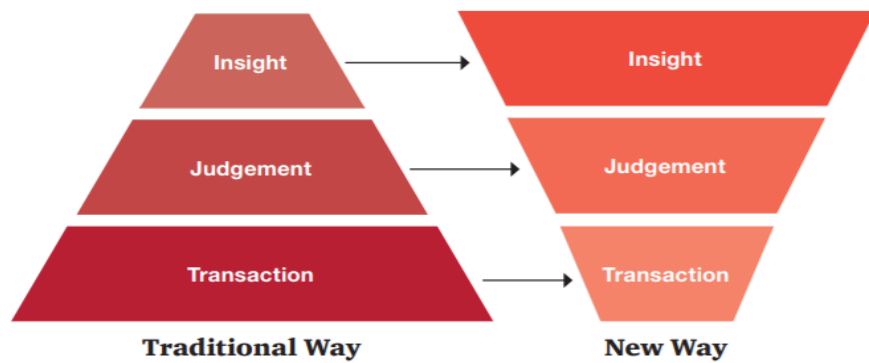
(四) 未來稽核樣貌

可以預見未來的稽核業務型態，將由傳統仰賴人工大量紙本審閱和檢視日常流程缺失轉型為將定義明確且龐雜繁複的例行性查核程序交由電腦、機器人擔任，內稽人員則針對其所辨識出的異常訊息執行更深入地調查。由於 AI 思路缺乏人類生活的常識，容易產生無意義或偏差的判讀結果，因此內稽需進行其後端的覆核工作，並針對 AI 潛藏風險或漏洞發展更完整的程式檢核邏輯，根據不可預見突發事件制訂應對措施，持續精進控制活動。

(五) 內部稽核功能的轉變

在高科技的輔助下，內稽人員的角色將由交易的檢查者轉型為洞見的提供者，利用數據分析技術以精準剖析所掌握資料，擷取更具智慧深度的資訊內涵，提出更多元的問題類型，據以進行有影響力的溝通，如圖 23。面對複雜且不斷演進的外在環境，內稽人員亦須持續關注與組織相關的發展趨勢，預測可能風險，以前瞻的視野協助組織回應科技變革帶來的挑戰與契機。

圖 23 內部稽核功能轉變



資料來源：PWC(2018)。

陸、研習心得與建議

一、心得

(一) 會審人員不會被科技取代，但工作型態必然轉型

面對來勢洶洶的科技變革浪潮，無論是會計和稽核人員不禁憂心自己的工作是否將會被電腦或機器人取代？當企業導入區塊鏈後，每一筆進貨、銷售交易或與銀行、投資者等利害關係人的往來資訊都記錄在一個不可竄改的共享帳本上，並能對多個來源的交易信息進行驗證，財務記錄的真實性、完整性、正確性均獲得保障。這些交易事件的會計過程，包含分錄、過帳、試算、調整、結帳和編製財務報表都透過區塊鏈帳本由電腦自動生成，人工的會計記帳工作將逐漸減少，企業不再需要審計人員或內部稽核人員覆核這些交易情況是否正常；更有人預言，區塊鏈所創建的信任機制，將會讓許多中介的角色消失，例如稽核人員或審計機構，因為鏈上的資料不需再由第三方提供認證，換言之，認證服務的關鍵在於信用問題，一旦信任可被取代，將大幅削減對審計資源的需求。在先進科技的衝擊下，會審行業真的即將瀕臨滅絕嗎？其實是不會的。理由有三，分述如下：

第一，會計涉及許多的估計。相較於過去準則以歷史成本為主的會計模式，國際財務報導準則(International Financial Reporting Standards,以下簡稱 IFRS)更強調財務報表能夠反映資產負債的真實價值，因此著重以公允價值為衡量基礎，而當市場公開報價無法取得時，則需對相關評價參數進行適當的估計。加上經營活動隱含許多未來事項不確定性，部分會計項目無法精確衡量僅能仰賴估計，若估計時所依據的情況發生變動，或由於新資訊或更多經驗，估計則須修正。在區塊鏈中，假設會計記錄一經確認便不得修改，即使會計系統的擁有者亦不能踰越該限制，這樣的運作方式並不切合會計實務需求。

第二，會審領域需要專業判斷。不同於以複雜、細節描述的規則基礎(ruled-based)報導準則，近年改採用的IFRS係以原則基礎(principle-based)訂定會計準則，對交易如何處理和分類需要較多的專業判斷，增加企業與會計師判斷的運用空間，而稽核人員執行的查核過程及針對稽核結果提出的意見均涉及專業判斷。專業判斷反映的是人的能力、想法、偏好或經驗等，即使對於相同的訊息，每個人做出的主觀判斷往往也不一樣。因此在會審領域中，對於大多數的問題並不是運用非黑即白的對立思維即可解決，而是存在灰色地帶的討論空間，透過不斷地對話與溝通以達成共識。這種牽涉到專業判斷和討論的過程並非系統或機器人可輕而易舉取代的。

第三，信任需要長時間互動累積。區塊鏈將共識寫進算法中，盡可能在彼此沒有信任的情況下產生最大程度的共識，但這個共識僅保證記錄的真實性，而資料的真實性也僅只是信任的基本要求，換言之，區塊鏈所實現的信任僅是最低程度的共識。事實上，信任是一種多層次的概念，是逐漸累積的動態過程，舉例來說，你相信一個人所提供的資料都是真實的，到你相信他會為你盡心負責，是需要經過時間歷程逐漸加深。而稽核人員和高階管理階層間的信任關係，也是建立在長時間累積的厚實基礎之上。稽核人員熟諳企業經營業務及規章制度等，能協助企業有效控管風險，對於企業外部環境的變動趨勢伴隨而來的潛在機會和挑戰亦可適時給予建議。具備這種相當程度瞭解與熟悉感所維繫的互信才是高層次信任的體現。

總結上述，先進技術並不會取代會審人員的工作，但工作型態無疑地將隨之改變。在數位科技時代下，會審人員應學會如何與高科技共處，利用新興技術輔助決策，充分發揮職能效用。畢竟這些技術都只是一種客體，能夠讓它們產生作用的主體是身為人類的我們，因此要保持開放心態，並非一味抗拒科技帶來的變化，而是主動瞭解並善用科技的力量以創造更高的價值。

（二）瞭解資料科學分析的重要性，以獲取決策資訊

諸如機器學習、大數據等技術，皆須經過長時間累積巨量資料，進而從中萃取高品質決策資訊。為避免因為數據不足導致演算法表現不佳，宜及早佈局資料科學領域，儘速投入相關場景實際運用，俾發掘更多潛藏知識。

二、建議

（一）因應數位科技時代，內稽人員應致力提升稽核附加價值

物聯網及區塊鏈等新興科技顛覆許多產業運作生態，對內稽領域而言不應僅將新技術視為挑戰，亦應以機會看待。當數位科技改變營運流程的同時可能衍生新的風險，內部稽核功能即可適時發揮，找出風險潛藏之處進行評估及規劃，幫助組織回應風險；創新技術也是促使內稽升級的關鍵利器，協助優化決策能力，增進稽核效能。

稽核人員雖然不需過於鑽研艱澀的技術理論，但對新科技的概念仍應具備一定程度的瞭解並熟悉基本的應用能力。除持續進修及訓練外，針對不同稽核案件需求可向外外部電腦專家尋求協助或諮詢，藉由相關的科技知識發揮槓桿效用，快速適應急遽變遷的數位時代。

為因應數位科技時代，建議本行內稽人員增進下列專業素養及能力以提升稽核之附加價值：

1. 面對快速變革時代，保持開放心態
2. 跟上科技發展進程，提升適應科技能力
3. 主動汲取新知，提升風險意識，培養洞察力及創造性思考
4. 持續強化溝通技巧、人際關係與領導能力

(二) 持續關注電腦輔助稽核技術之發展趨勢

隨著先進科技不斷演變，越來越多新穎的方法和應用工具蓬勃發展，若能從中找尋合適電腦技術，並且實踐於稽核領域，將可降低稽核成本，進一步提升效率及效能。舉例來說，目前在數據分析領域非常熱門的兩個應用工具—R 語言和 Python 語言，和其他程式語言相比，相對容易入門，網路上亦提供許多的開放式學習資料。Python 語言有著直觀、易於理解的編寫程式碼方法，R 語言則擅長處理純文字資料。兩者皆有豐富套件可使用，分析的結果亦有多種樣版、模組供選擇呈現，便於將資料視覺化(visualizing data)，讓使用者以看圖說故事的方式清楚了解資料意義，有助互相溝通與理解。

目前本行會計流程已採電子化作業，相關會計報表、帳簿皆上傳至報表管理系統儲存，不再列印紙本，相信未來必然有更多的線上作業應運而生。在這樣的數位化環境下，其實創造一個相當有利於稽核人員活用資料的空間。建議可深入瞭解及研究各種應用程式，關注電腦輔助稽核技術新發展，適時加以運用，拓展資料分析深度與廣度，據以提供多面向洞察與見解，持續強化本行風險控管能力。

參考資料

Lynn(2017),「監督式學習?增強學習?聽不懂的話,一定要看這篇入門的機器學習名詞解釋!」,取自

<https://www.inside.com.tw/2017/07/19/machine-learning>

Nikkei Computer (2016),「FinTech 革命—金融科技完全解析(汪平、金恬然、皇甫彥帝譯)」,臺北市:遠見雜誌。

王肇遷(2017),「區塊鏈應用:台灣股票結算交割系統」,國立政治大學金融學系研究所碩士論文。

王擎天(2018),「區塊鏈」,新北市:創見文化。

曲建仲(2017),「顛覆金融業的區塊鏈」,《科學月刊》,第575期,頁42-47。

朱漢崙(2018年6月22日),「會計師簽查財報,年底啟用區塊鏈」,取自

<http://www.chinatimes.com/newspapers/20170622000133-260205>

周濟群(2018),「新科技與財會之碰撞:智能合約與收入認列」,《會計研究月刊》,第389期,頁100-103。

黃宣蓉、湯明勳、陳伊瑩(2018),「電子銀行函證」,《月旦會計實務研究》,第5期,頁133-143。

陳君明(2017),「理解區塊鏈,不能不知道的密碼學」,取自

https://www.hbrtaiwan.com/article_content_AR0007296.html

陳建文(2014),「2013亞洲區內部稽核研討會(ACIIA Conference)專題分享—淺談持續性稽核與持續性監督」,《財金資訊季刊》,第78期,頁41-47。

Braun, G., Struthers-Kennedy, A. and Wishna, G. (2017), "Building a Data Analytics Program," *Internal Auditor*, August, 41-45.

- CPA Canada, the AICPA and the UWCISA (2017), "Blockchain Technology and Its Potential Impact on the Audit Assurance Profession." Retrieved from <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf>
- Hoelscher, J. (2018), "Taking The Lead on Blockchain," *Internal Auditor*, February, 19-21.
- Lee, L. (2016), "Big Data and Internal Auditors," *Internal Auditor*, October, 20-21.
- McCollum, T. (2017), "Audit in an Age of Intelligent Machines," *Internal Auditor*, December, 24-29.
- PwC(2018), "Transforming Internal Audit through Data Analytics. Retrieved from <https://www.pwccn.com/en/risk-assurance/publications/transforming-ia-through-data-analytics.pdf>
- Piper, A. (2016), "A Matter of Trust," *Internal Auditor*, April, 26-31.
- Van Driel, K. (2018), "DLT arrangements and Cryptos," *De Nederland Bank seminar on Internal Audit: Keeping Pace with Development*, June.
- The Institute of Internal Auditors (2017), "Artificial Intelligence - Considerations for the Profession of Internal Auditing," *Global Perspectives and Insights, Special Edition*.
- World Economic Forum(2016), "The Future of Financial Infrastructure: An Ambitious Look at How Blockchain can Reshape Financial Services," *The World Economic Forum*, August.
- Willemsen, P. (2018), "Internet of Things: Data Science and Auditing," *De Nederland Bank seminar on Internal Audit: Keeping Pace with Development*, June.