專題

COSO 觀點下區塊鏈應用於政府內部控制的效益與風險

應用區塊鏈的組織可以提升稽核或營運效率，然而採用區塊鏈可能會為組織帶來新的風險與新的控制需求，如資訊洩漏、難以識別應負責者等，因此 COSO 提出應用區塊鏈之內部控制指引。本文以 COSO 觀點，考量目前政府內部控制需求與目標，分析採用區塊鏈之可能情境，並進一步分析效益與風險，最後提出政府應用區塊鏈時，可採行的方案。

李長瑋、周濟群、蕭幸金（政治大學會計學系博士候選人、美國加州州立大學蒙特利灣校區教授、臺北商業大學會計資訊系教授兼副校長）

壹、前言

區塊鏈擁有「去中心化」、「可追蹤性」、「不可竄改性」及「匿名性」的特點，讓許多組織開始導入區塊鏈系統，以提升組織營運或稽核的效率。區塊鏈的特點有助於稽核的效率，或可協助組織進行內部控制，但導入區塊鏈時，除了面臨組織流程的改變及組織文化阻力的風險外，甚至採用的技術細節都可能讓組織面臨新風險。若導入的單位爲政府組織，一旦無法有效的因應新風險，可能使人民蒙受重大損失。因此在導入前，必須分析預期的效益與可能的風險，本文即針對政府部門應用區塊鏈於內部控制議題時，分析潛在的效益及可能的風險。

貳、區塊鏈的效益與問題

2008 年，區塊鏈（Blockchain）的概念誕生，是由中本聰（Satoshi Nakamoto）在網路上發表的一篇名爲《Bitcoin：A Peer-to-Peer Electronic Cash System》的論文而來。區塊鏈利用密碼學的概念將交易資料串連，再透過特定的證明方式來完成交易的紀錄。由組織內部控制的觀點，區塊鏈的特色將帶來幾個效益，包括「去中心化」可減少中間成本甚至提高效率；

「可追蹤性」因區塊鏈中之資訊是透明且公開，使交易紀錄更易於稽核；「不可竄改性」使交易紀錄難以在事後被其他人修改或隱瞞；「匿名性」的優點則是使交易雙方得以保有隱私。

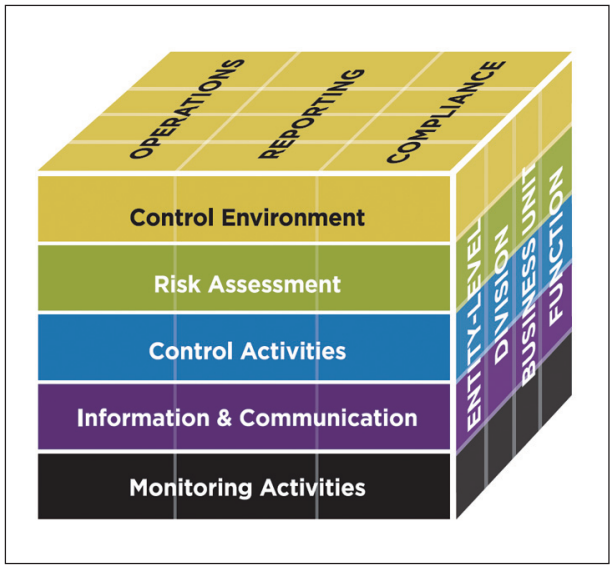
雖然區塊鏈的四個特色能爲組織內部控制帶來效益，但由政府部門的角度來看，可能需思考以下幾項問題：第一、政府各單位是具有層級關係的，「去中心化」後是否意味著將無人領導？或是水平化組織；第二、「可追蹤性」是緣於資訊公開，但政府的資訊是否能公開給所有人？第三、「不可竄改性」代表著一旦資訊有誤，將沒有可以修改的機會，是否將提高政府單位的事前檢查成本？最後是「匿名性」，若資訊相關人員皆採匿名，若發生問題又該由誰負責？

由文獻分析可知，採用區塊鏈面臨的風險其實是由流程或文化導致的管理問題而來，而區塊鏈帶來的效益與現況的衝突，也非無解之題，以前述四個問題來說，其實都可以透過技術解決，如採聯盟鏈（Consortium Blockchain）架構，並對部分資訊加密，再加上實名制的管理等，將詳述於後。

參、COSO 與中央政府內部控制架構

內部控制架構最被廣泛應用爲美國 COSO 委員會所提出的架構，爲因應區塊鏈之應用發展，COSO 委員會已於 2020 年 7 月提出區塊鏈與內部控制指引（Blockchain and

圖 1　The COSO 2013 Framework



資料來源：Blockchain and internal control：The COSO perspective

圖 2　我國政府內部控制觀念架構

資料來源：行政院主計總處「政府內部控制之推動」電子書第三版。

internal control：The COSO perspective），該指引是採用 2013 年 COSO 提出的內部控制架構（上頁圖 1），共有五大要素及三大目標，五大要素分別爲控制環境、風險評估、控制作業、資訊與溝通、及監督作業；三大目標爲營運目標、報告目標、遵循目標。而我國行政院爲提升內部控制效率，亦參考 2013 年 COSO 的架構，發展政府內部控制觀念架構（上頁圖 2），有四大目標，分別是施政效率、可靠資訊、遵循法令及資產安全，內容可直接對應 COSO 架構的目標。不論是 COSO 或我國政府之內部控制架構，其目標皆是強化舞弊防治的風險管理，各項要素與目標必須做整體評估，不可單獨評估。

2013 年 COSO 內部控制架構的五大要素包含 17 項原則，控制環境之原則主要爲董事會或管理階層負責監督、設計與執行內部控制，且做適當授權及責任承擔；風險評估之原則主要爲辨識與分析相關風險，且要考量舞弊的狀況；控制活動之原則爲選擇與建立控制活動來達成內部控制目標，並透過資訊科技來達成目標；資訊與溝通之原則爲取得有效資訊及相關內外溝通；監督之原則則爲持續評估且進行檢討缺失。雖然 COSO 2013 內部控制架構提供可以遵循的內部控制原則，但內部控制仍要配合組織策略、績效與價值進行，故 COSO 委員會在 2017 年發布企業風險管理架構，連結風險與組織策略、績效與價值，且與內部控制架構互相配合，讓組織在評估風險時可以更加全面化。

肆、COSO 觀點下的區塊鏈效益與風險

前述提及區塊鏈風險主要是由組織管理而來，與 COSO 2013 內部控制架構極爲攸關，在區塊鏈與內部控制指引中，COSO 亦提出三項重要的管理議題，提供組織應用區塊鏈前進行評估。一是管理階層能否控制區塊鏈，若能控制，導入前後可能沒有差異；二是不同組織共用區塊鏈伴隨的共同承擔風險與控制；三是採用區塊鏈時，由於去中心化及匿名，可能會導致決策分散與責任無人承擔問題。

這三項議題也與區塊鏈的效益與風險相關，首先管理階層能否控制將影響區塊鏈是否能保持不可竄改及去中心化；再來是共用區塊鏈，雖然使資訊的分享更爲便捷，但可能會導致部分不該共享的資訊洩漏出去；最後則是去中心化與匿名，則組織成員將不受管理階層影響，但這可能使組織原有的管理結構崩壞，進一步影響組織運作。

從 COSO 的五大要素出發，可以進一步識別區塊鏈的效益與風險，由區塊鏈與內部控制指引中，五大要素下的效益與風險對應表（下頁表 1）的風險，可以對應到前述提及的區塊鏈之四大特點，也因此

這些風險，多數可以透過技術來降低發生的機率，眞正難以掌控的風險，反而存在於那些衍生於組織管理面的問題。

伍、區塊鏈應用於政府內部控制

不論企業組織或是政府單位，區塊鏈應用的效益與風險問題大同小異，若將區塊鏈應用於政府內部控制上，COSO提出的效益與風險，可作爲將區塊鏈應用於政府內部控制的基礎，包括：第一，政府單位有上下層級的關係，權力如無法全部下放，表示不可全部去中心化，仍有部分屬於管理單位監管；第二，資訊須公開，但不能公開之內容須加密或隱藏，只能讓有權限者瀏覽，表示可讓不同位階的人聚焦在他需要知道的資訊；第三，資訊不可修改，但要降低事前檢查成本，這表示需要採用更多的自動化與電子化，除了降低資訊不正確性之外，也可降低人員出錯造成之風險；最後，需要實名制，但不需讓鏈上所有參與者都知道，僅需在必要時可以識別，如發生問題須找出負責任者，而匿名與實名管理單位則由第一點所提之單位來監管。

根據前面問題與須改善之處，政府內部控制應用區塊鏈有以下幾點目標：第一是要建立具備上下階層的區塊鏈架構，而且中央監督單位需要獨立，以行使監督之權；第二是根據不同層級的參與者要有不同的資訊瀏覽權限；第三是要配合採用其他的自動化工具，且資料可能需要電子化；最後則是可將匿名轉爲實名的機制，須配合中央監督單位。就以上條件，政府內部控制應用區塊鏈模式，較佳方案是使用

表 1　區塊鏈效益與風險對應表

要素	效益	風險
控制環境	● 提供自動化紀錄避免人為錯誤且降低舞弊機會 ● 透明度高可以即時報告且易於追蹤	● 權力下放導致監督者要求各單位都要負責 ● 操作者可能不受管理階層控制
風險評估	● 提供內外部利害關係人即時的報告，更快的評估運作目標	● 難以辨識誰負責承擔風險 ● 區塊鏈與其他系統的整合風險
控制活動	● 降低資料被修改的風險 ● 降低資料遺失風險	● 區塊鏈的管理問題（註 1） ● 是否有人可以掌握區塊鏈（註 2）
資訊與溝通	● 資訊的遺失機會較低 ● 跨部門分享，即時整合資料	● 資訊可能不正確
監督	● 更快且有效的發現問題 ● 配合工具可聚焦高風險領域	● 資訊變得更複雜 ● 可能缺少中央監督單位

註 1：有以下三項 (1) 私鑰相當於區塊鏈中的身分證明；(2) 共識演算法是確認交易是否有效的機制；(3) 智能合約是在區塊鏈上運作的程式。
註 2：掌握區塊鏈是指控制區塊鏈中 51%以上的節點。
資料來源：Blockchain and internal control：The COSO perspective。

聯盟鏈，而且要加上身分管理單位及中央監督單位。此外，爲了避免上級長官掌握區塊鏈，可能還要有一定數量的參與者才能降低發生的機會。

陸、可採行之參考方案

效益與風險的改善方案雖可解決應用區塊鏈於政府內部控制的問題，但仍必須透過 COSO 內部控制架構的檢視，確認是否可以確實降低風險，須對應效益與風險對應表（上頁表 1），分析聯盟鏈、建立身分管理單位、賦予不同職級的權限、及自動化技術配合等方案，在 COSO 內部控制架構五大要素的效益與風險。

COSO 觀點下的改善方案檢視表（表 2），彙整前述的各項觀點，其中使用聯盟鏈，將可以適度地進行身分管理，且提供不同身分的權限，因此使用聯盟鏈可以改善原有區塊鏈應用在政府內部控制的問題。聯盟鏈的效益不僅於此，在聯盟鏈中，可讓各部會成爲單獨之區塊鏈，而各部會的區塊鏈則可再成爲部會聯盟鏈。

以行政院的部分部會爲例，聯盟鏈架構如下頁圖 3，各部會以部會聯盟鏈作爲連結，形成最大的聯盟鏈架構，而各部會則以各自的員工爲子節點發展各部會的區塊鏈。採用聯盟鏈架構可避免單一部會取得資訊過於複雜，同時聚焦在自己部會的資訊，若有取得他部會資訊之需求，再透過部會聯盟鏈去取得其他部會的資訊即可。而主管單位則可透過聯盟鏈取得跨部資料，快速整合不同部門的資訊，提升行政決策的效率，若是在各部會間搭配自動化技術，還可提升處

表 2　COSO 觀點下的改善方案檢視表

要素	改善方案
控制環境	採用聯盟區塊鏈，並以政府各部門作為單位節點，而部門相關員工則各為子節點，參與者應保持適當之數量，針對不同職級的人給予不同的權限
風險評估	需要身分管理單位，僅有此單位可以將匿名身分識別，且提供各個參與者不同的身分權限，可以瀏覽各不同等級的資訊，同時可以識別責任承擔者。 可配合獨立監督單位，讓非參與者（如人民）進行監督，降低利害關係的影響。
控制活動	身分管理單位獨立於參與單位之外，可一個或分散多個管理，降低參與者被識別出之風險，同時也可以降低上級單位掌控下級單位，減少掌握區塊鏈之機會。
資訊與溝通	透過自動化技術協助，進行多方校驗，同時配合智能合約進行資訊的傳遞。自動化技術可以快速整合各部門資料，讓管理者更快做出決策。
監督	建立身分管理單位與獨立監督單位，配合自動化技術與智能合約監測，在降低資訊複雜度的同時，可以更快發現問題，也避免沒有中央監督單位。

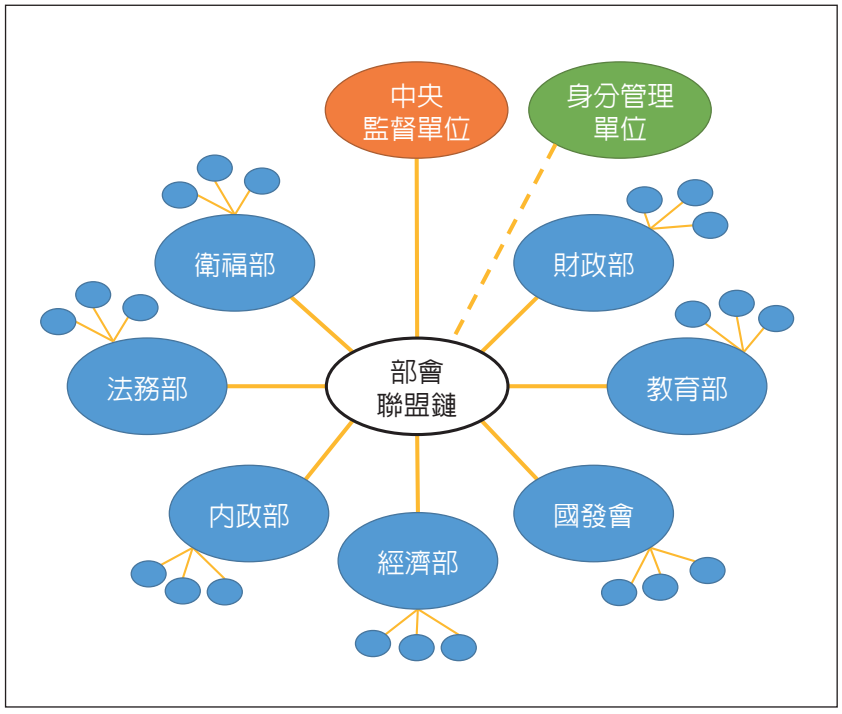
資料來源：作者自行整理。

理速度，降低資料整合之成本。而透過各部會職員成爲子節點，加上身分管理單位進行匿名實名的管理，也可降低主管單位試圖影響下級單位，減少區塊鏈被掌握的機會，更能充分的發揮其眞正效益。

柒、結語

政府應用區塊鏈於內部控制，其需求與原始區塊鏈之特點有所不同，但理解區塊鏈的運作並做充分的風險分析，最後調整應用至合適政府單位，可以更有效的協助政府單位，除了讓內部控制效率提升，也能讓各部會的運作更佳。誠如 COSO 在區塊鏈與內部控制指引中提到，「雖然區塊鏈有潛力可以提供更好的解決方案，但管理階層仍要理解區塊鏈，並評估相關風險，讓區塊鏈的應用更有效」。本文提供可採行之參考方案，建議政府單位在導入區塊鏈協助進行內部控制之前，能審愼評估應用區塊鏈可能產生的風險，並分析可能的解決方案，確認其效益確實超過成本，且風險能夠被掌控，才能眞正有效發揮區塊鏈織功能。❖

圖 3　以行政院為例的部會聯盟鏈架構（僅列部分部會為例）



資料來源：作者自行繪製。