區塊鏈存證與營業秘密保護之研究

郭彥呈

壹、緒論

貳、營業秘密合理保密措施之內涵

一、營業秘密合理保密措施之意義

二、我國實務對合理保密措施之認定

參、比較法上合理保密措施之認定

一、美國營業秘密法上合理保密措施之認定

二、美國法院對合理保密措施之實務見解

三、科技保護措施於營業秘密保護之運用

四、小結

肆、區塊鏈技術作為合理保密措施判斷因素之分析

一、區塊鏈存證與合理保密措施之關聯性

二、區塊鏈存證難以單獨構成合理保密措施

三、區塊鏈技術類型之分流：聯盟鏈與私有鏈之技術隔離功能

四、區塊鏈存證作為合理保密措施之輔助

伍、結論

作者現為臺北大學法律學系博士班學生。
本文相關論述僅為一般研究探討，不代表本局及任職單位之意見。

摘要

本文以區塊鏈存證技術與營業秘密法上「合理保密措施」之關係為核心。依我國營業秘密法第 2 條及美國統一營業秘密法、營業秘密防衛法等相關實務，合理保密措施並非要求絕對保密，而係著重資訊所有人是否係透過契約、管理或技術措施建立實質之接觸控制。區塊鏈係具有不可竄改、時間戳記，及可溯源等特性，惟其法律評價應依具體架構而定。

公開鏈主要具有資訊驗證及證據保存功能，通常欠缺限制未授權者接觸資訊之效果，原則上難以單獨構成合理保密措施，但得作為秘密管理之輔助證明。相較之下，聯盟鏈或私有鏈如結合准入管制、角色存取控制、身分驗證及金鑰管理，得限制未授權者接觸資訊，可能構成合理保密措施之一環。

本文主張，區塊鏈兼具事前防禦與事後證明功能，法院應依其架構、權限設計及接觸限制效果，納入企業整體保密制度而為綜合判斷。

關鍵字：營業秘密、合理保密措施、區塊鏈存證、聯盟鏈、私有鏈、接觸控制
Trade Secrets、Reasonable Measures to Maintain Secrecy、Blockchain-Based Evidence Preservation、Consortium Blockchain、Private Blockchain、Access Control

壹、緒論

當前進入科技與知識經濟之時代[1]，企業競爭的優勢已發生了典範轉移。在傳統工業經濟時期，企業主要係以土地、廠房、生產設備，以及金融資本等有形資產，作為累積財富與規模之核心；惟，隨著資訊技術的演化，無形資產已成為決定企業市場領導地位的關鍵因素。

舉例而言，根據智慧財產權及無形資產專業顧問機構 OCEAN TOMO 對於全球公開上市公司市場價值之長期追蹤，企業總市值中無形資產所占比例自 1970 年代的不到二成，已大幅成長至近年的九成左右[2]。

在此趨勢下，企業之經營核心已聚焦於無形資產，而其中之營業秘密，包含兩大類型，分別是商業性與技術性營業秘密，商業性如客戶名單、商品售價、交易底價，以及成本分析；技術性則如方法、技術、製程，或是配方[3]，營業秘密具有高度經濟價值[4]，並可能成為企業維持競爭優勢之關鍵，因而在企業資產中是占有重要地位[5]。對此可參我國立法，營業秘密法第 1 條，開宗明義指出：「為保障營業秘密，維護產業倫理與競爭秩序，調和社會公共利益，特制定本法。本法未規定者，適用其他法律之規定。」可見我國已透過專法建立了營業秘密保護制度[6]。

此外，根據我國營業秘密法第 2 條之規定：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合

---

1 天下雜誌，https://www.cw.com.tw/subchannel.action?idSubChannel=9（最後瀏覽日：2026/06/15）。

2 Intangible Asset Market Value Study, OCEAN TOMO, https://oceantomo.com/intangible-asset-market-value-study/ (last visited Aug. 4, 2026).

3 營業秘密保護實務教戰手冊 3.0，經濟部智慧財產局營業秘密主題網，https://www.tipo.gov.tw/tw/tradesecrets/872.html（最後瀏覽日：2026/08/04）。

4 最高法院 108 年度台上字第 2158 號民事判決。法院認為：「再依營業秘密法第 2 條規定，該法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合非一般涉及該類資訊之人所知、因其秘密性而具有實際或潛在之經濟價值、所有人已採取合理之保密措施等要件者而言。」

5 Threads 盜用推特商業機密？營業秘密是什麼？一文理解營業秘密對企業的重要性，台灣經濟新報，https://www.tejwin.com/insight/threads-%E7%9B%9C%E7%94%A8%E6%8E%A8%E7%89%B9%E5%95%86%E6%A5%AD%E6%A9%9F%E5%AF%86%E7%90%86%E8%A7%A3%E7%87%9F%E6%A5%AD%E7%A7%98%E5%AF%86%E5%B0%8D%E4%BC%81%E6%A5%AD%E7%9A%84%E9%87%8D%E8%A6%81/（最後瀏覽日：2026/08/04）。

6 我國營業秘密法條文。

左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」就營業秘密成立須具備三項要件，分別是秘密性[7]、經濟價值性[8]，以及第 2 條第 3 款之合理保密措施[9]。

相較其餘兩個要件，合理保密措施在法院認定上較具彈性[10]，法院通常綜合判斷企業是否已採取足以維持資訊秘密性之措施。就此，何謂合理保密措施[11]，以及採如何之手段方能達成合理保密措施之要求，成為了本文感興趣的重點。

隨著科技化浪潮[12]，企業管理資訊的方式朝向數位化[13]，近年區塊鏈技術，因其技術特徵具有不可竄改性[14]、可溯源性[15]，時間戳記[16]等特點，逐漸有研究探討區塊鏈技術能否運用於營業秘密保護，市場上亦出現區塊鏈存證服務。

值得關注者，區塊鏈存證服務之運作是將資訊的雜湊值（Hash Value）[17]入鏈保存，此舉可使該資料其生成時間、內容，歷史紀錄等可被檢證，亦即將資訊上

7 林洲富，營業秘密與競業禁止，頁 13，五南圖書出版股份有限公司，2018 年 8 月 3 版。

8 同前註，頁 19。

9 李志強，淺談營業秘密合理保密措施之可行作法，清流雙月刊 54 期，頁 46-51，2024 年 11 月。

10 智慧財產及商業法院 114 年度民秘聲字第 37 號民事裁定。法院認為：「又聲請人對於系爭資料設有雲端系統、簽署保密協議之合理保密措施，非任何人可輕易接觸，堪認聲請人業已釋明該等訴訟資料具有秘密性、經濟性，且已採取合理之保密措施，而為其不欲為他人所悉之營業秘密。」

11 林洲富，同註 7，頁 21。

12 數位轉型浪潮下的臺灣科技新創，行政院，https://www.ey.gov.tw/Page/448DE008087A1971/01c022f4-dd6f-4698-9886-1b182b7f827d（最後瀏覽日：2026/06/15）。

13 關於數位化相關計畫，數位管理共好加值計畫，產業競爭力發展中心，https://assist.nat.gov.tw/wSite/ct?xItem=289617&ctNode=150&mp=2（最後瀏覽日：2026/06/15）。

14 關於不可竄改性，請參郭彥呈、范建得，區塊鏈與營業秘密保護困難之突破，頁 85，元華文創股份有限公司，2021 年 8 月初版。

15 郭彥呈、范建得，同前註，頁 86-89。

16 關於時間戳記其實並不複雜，其概念可由這則實例理解，智慧財產法院 101 年度民專訴字第 119 號民事判決：「被證 3-3 為 Kinetic Case 於 2010 年 12 月 6 日上傳於 Youtube 標題 How to install the Kinetic Case 之影片，上傳完成後由 YouTube 網站自動加註上傳的時間戳記為 2010 年 12 月 6 日，應可推定該上傳時間點為真正，另於 YouTube 網站以 How to install the Kinetic Case 檢索亦可顯示標題為 How to install the Kinetic Case 之影片並觀看等情，業經本院於 102 年 1 月 8 日當庭勘驗屬實，並作成勘驗光碟可證」。

17 關於哈希算法之相關討論，可參郭彥呈、范建得，同註 14，頁 97-98。

鏈保存，而透過零知識證明系統[18]，可推知資料為真，於此區塊鏈存證被學者認為具有提高可信度，以及降低資料遭他人竄改之風險[19]。

所以，本文所欲探討者，在於區塊鏈存證能否成為營業秘密保護工具？是否符合合理保密措施之要求？抑或僅具輔助性資訊管理與證據保存功能？其是否具有與保密協議（Non-Disclosure Agreement, NDA）、門禁制度，或權限管理相類似之接觸限制效果？

目前區塊鏈存證雖可協助證明資訊之存在時點及內容完整性，但能否限制第三人接觸該資訊，仍有進一步分析之必要。

我國目前對於區塊鏈的研究主要分成兩大類，其一是對於虛擬資產[20]，其二則是對於區塊鏈證據的研究，然而對於區塊鏈與營業秘密保護，研究相對有限[21]。

綜上，本研究以區塊鏈存證與營業秘密合理保密措施為研究核心，探討區塊鏈存證之功能與效果，以及對於營業秘密保護之作用。

18 什麼是零知識證明？，ethereum.org，https://ethereum.org/zh-tw/zero-knowledge-proofs/（最後瀏覽日：2026/06/16）。

19 蘇凱平副教授演講「數位證據」與「區塊鏈」的證據法則，司法院，https://www.judicial.gov.tw/tw/cp-1429-883117-604b3-1.html（最後瀏覽日：2026/06/15）。

20 政院通過「虛擬資產服務法」草案 健全虛擬資產業務經營與發展、保障交易人權益，行政院，https://www.ey.gov.tw/Page/9277F759E41CCD91/bfd446a7-ce23-4308-9347-9ce6e6c44196（最後瀏覽日：2026/06/15）。

21 我國多數學者研究興趣如，余啟民，電子簽章法與區塊鏈應用，當代法律 52 卷，頁 69-87，2026 年 4 月。鄭婷嫻，國際監理架構下穩定幣與真實世界資產代幣化（RWA）——區塊鏈金融之法制與貨幣政策風險，當代法律 48 卷，頁 24-37，2025 年 12 月。徐素圓，區塊鏈與代幣化發展，集保雙月刊 278 卷，2025 年 2 月。蘇凱平，司法聯盟鏈與數位證據——寫給法律實務工作者的簡介，月旦律評 30 期，頁 55-62，2024 年 9 月。葉奇鑫、高慶仁，論司法聯盟鏈應如何解決數位證據驗真問題，月旦律評 31 期，頁 55-62，2024 年 10 月。

貳、營業秘密合理保密措施之內涵

一、營業秘密合理保密措施之意義

如果企業對於自己重要資訊完全未採取保護措施，即便該資訊具有高度商業價值[22]，法院仍可能認定其不具備營業秘密之地位[23]。值得關注的是，我國營業秘密法，並未明文道何種措施方屬合理保密措施[24]，其主要交由法院依個案判斷[25]。

二、我國實務對合理保密措施之認定

（一）合理保密措施之判斷標準

關於合理保密措施之認定，我國判決實務上可參最高法院 108 年度台上字第 36 號民事判決：「又營業秘密所有人採取之保密措施是否達合理之程度，應衡酌該營業秘密之種類、事業實際經營情形及社會共識或通念，依具體個案之情形為判斷，如客觀上足使一般人以正當方法無法輕易探知，即難謂非合理之保密措施。」

最高法院 102 年度台上字第 235 號民事判決指出：「按營業秘密法第 2 條第 3 款規定『所有人已採取合理之保密措施』，應係指所有人按其人力、財力，依社會通常所可能之方法或技術，將不被公眾知悉之情報資訊，依業務需要分類、分級由不同之授權職務等級者知悉而言；此於電腦資訊之保護，就使用者每設有授權帳號、密碼等管制措施，尤屬常見。」此一見解已成為了司法實務上常為引用之判准。依此見解，合理保密措

22 關於商業價值相關討論，商業模式圖，經濟部中小及新創企業署，https://www.sme.gov.tw/expdesign/files/13622/5F86D268-4673-4851-89BA-382CE31F27AB（最後瀏覽日：2026/06/15）。

23 張志朋、林佳瑩，營業秘密訴訟贏的策略，頁 1-210，元照出版有限公司，2022 年 9 月 3 版。

24 財團法人資訊工業策進會科技法律研究所，從產業秘辛和實務數據探索營業秘密管理，頁 1-383，元照出版有限公司，2019 年 11 月初版。

25 智慧財產法院 109 年度民營訴字第 9 號民事裁定。法院認為：「而原告等已制訂並執行合理保密措施，包括與員工簽訂含保密條款之聘雇契約、員工守則明載對所有機密資訊均以嚴格權限控管、對機密資訊紙本採取門禁管理、規定檔案銷毀流程、制訂『保全管理作業指導書』，明定智慧財產權保護措施，並訂有資訊保安管理程式，對所有管控檔之存取均有限制，並不得擅自帶出生產區或複印，且與設備供應商均簽有保密契約，並舉辦多場資訊安全及秘密保護教育訓練、行為準則。」

施的核心精神在於，企業有主觀上保密意思、客觀上已採取保密行動、接觸範圍受到一定限制，一般人足以知悉該資訊具有保密性質[26]。

（二）法院實務常見之保密措施

依我國法院實務觀察，企業常見之合理保密措施可分為三類，分別是契約、管理，以及技術。在契約措施上，常見的如 NDA[27]、員工保密切結書，以及離職保密條款等，此部分的手段係透過契約方式，讓員工明瞭資訊具有保密性質。

管理措施面上，企業通常是採取檔案資訊分級授權管理[28]，並且限制特定人員接觸，應用門禁系統，以及文件標示借閱紀錄追蹤等。技術措施上，包含如帳密管理、防火牆、加密系統，以及存取紀錄等資安措施。

對此，智慧財產及商業法院 108 年度民營上易字第 1 號民事判決明確指出：「本院審酌被上訴人為資本額 500 萬元之中小型企業（被上證 1），員工人數僅十數人，被上訴人對於報價單之內容已限制僅有少數人可以接觸、知悉，對於被上訴人公司電子信箱，亦透過限制使用人員及設定密碼之方式加以保護，並與員工簽訂到職切結書及離職切結書，課予員工保密之契約義務，使員工明確知悉被上訴人有將營業秘密資訊加以保護之主觀上意思及客觀上作為，整體觀之，應認被上訴人對報價單之營業秘密，已採取合理之保密措施。」

由此可見我國法院並不要求企業採取單一特定措施，而是重視企業是否建立整體性的保密制度。

---

26 同前註。

27 NDA 保密協議什麼時候簽？新創募資與 DD 的分層揭露原則，台大創創中心網站，https://tec.ntu.edu.tw/blog/startup-nda-guide（最後瀏覽日：2026/06/15）。

28 章忠信，台積電洩密案之營業秘密保護討論，著作權筆記，https://www.copyrightnote.org/paper/pa00172.pdf（最後瀏覽日：2026/06/15）。

（三）實務判決評析

由上述判決觀察，我國實務上對於合理保密措施之認定，逐漸形成以接觸控制為核心判斷之趨勢，無論是保密契約、分層授權或帳密管理，其共同功能均在限制未授權者接觸資訊。

反面觀察之，若某項技術僅能證明資訊存在，內容未遭修改，然而欠缺實質接觸限制的可能，按我國實務觀察，是否構成合理保密措施，仍有疑義。

參、比較法上合理保密措施之認定

一、美國營業秘密法上合理保密措施之認定

我國營業秘密制度起源於英美法體系[29]，由此美國法對於合理保密措施的發展具有重要的參考價值。我國營業秘密法第 2 條有關合理保密措施之規定，亦受到美國營業秘密法理論的影響[30]。因此，探討美國法上合理保密措施之標準如何認定，有助於我們理解營業秘密。

美國多數州於 1980 年代陸續採納統一營業秘密法（Uniform Trade Secrets Act, UTSA）[31]，作為州營業秘密法之主要依據。按 UTSA 規定，營業秘密必須符合兩

---

29 章忠信，我國營業秘密保護之法制發展歷程，著作權筆記，https://www.copyrightnote.org/ArticleContent.aspx?ID=3&aid=3236（最後瀏覽日：2026/06/15）。

30 營業秘密法概述與實務問題，法務部調查局網站，https://www.mjib.gov.tw/userfiles/files/25-%E7%B6%93%E6%BF%9F%E7%8A%AF%E7%BD%AA%E9%98%B2%E5%88%B6%E8%99%95/%E7%87%9F%E6%A5%AD%E7%A7%98%E5%AF%86/04%E7%87%9F%E6%A5%AD%E7%A7%98%E5%AF%86%E6%B3%95%E6%A6%82%E8%BF%B0%E8%88%87%E5%AF%A6%E5%8B%99%E5%95%8F%E9%A1%8C.pdf（最後瀏覽日：2026/06/15）。

31 卡內基美隆大學，https://euro.ecom.cmu.edu//program/law/08-732/TradeSecrets/utsa.pdf（最後瀏覽日：2026/06/15）。相關討論亦可參見，葉雲卿，美國營業秘密訴訟之程序要件—營業秘密之特定與證據調查，北美智權報，https://naipnews.naipo.com/12279/（最後瀏覽日：2026/06/15）。UTSA 第 1 條第（4）款（UTSA § 1(4)）法條原文為：「(4)“Trade secret” means information, including a formula, pattern,compilation, program, device, method, technique, or process, that:(i) derives independent economic value, actual or potential, from notbeing generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and(ii) is the subject of efforts that are reasonable under the circumstancesto maintain its secrecy.」

項要件，其一為資訊具有經濟價值，而其二係資訊所有人已採取在該情況下屬於合理的保密努力[32]。

美國法並未要求資訊所有人採取絕對保密措施，而是採取合理努力（Reasonable Efforts）標準。換言之，只要企業已依據資訊性質、產業特性，以及自身資源採取適當保護措施，即有可能符合營業秘密保護要件。

2016 年美國制定營業秘密防衛法（Defend Trade Secrets Act, DTSA）[33]，建立聯邦層級營業秘密保護制度，DTSA 延續 UTSA 之基本架構，同樣強調合理保密措施的重要性。根據聯邦法院見解，合理保密措施通常包括 NDA、資訊分級管理，以及資訊安全管理制度等。

二、美國法院對合理保密措施之實務見解

除法律規定外，美國法院透過大量的判決進一步建構合理保密措施之判斷標準，在 Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.[34] 一案中，法院指出，營業秘密所有人並無義務採取極端或絕對之保密措施，法律所要求者僅是在具體情況下採取合理努力維護資訊秘密性。即使部分資訊曾於有限範圍內流通，若企業整體上仍持續透過契約、管理或技術手段維護資訊之秘密狀態，仍不因此喪失營業秘密保護資格。本案顯示美國法院所採取者並非結果導向之判斷模式，而是行為導向之觀察模式。法院重視者並非資訊是否完全未曾外流，而是企業是否持續展現維護秘密性之努力。

---

32 UTSA，同前註。

33 王偉霖，2016 年美國聯邦保護營業秘密法（DTSA）於我國營業秘密法制之借鏡，萬國法律 209 期，頁 87-108，2016 年 10 月。亦可參北美智權報，同註 31。法條原文係為：「18 U.S.C. § 1839(3) (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information... if—(A) the owner thereof has taken reasonable measures to keep such information secret; and(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;」

34 Rockwell Graphic Systems, Inc. v. DEV Industries, Inc., 925 F.2d 174 (7th Cir. 1991). 法院認為「"The requirement of reasonable efforts has both evidential and remedial significance. But the query is what is reasonable under the circumstances, and this is another way of asking whether the owner of the trade secret has encountered the optimal cost-benefit trade-off.""The higher the fence, the more guards, the more secure the secret—and the higher the cost of security to the owner. ... Perfect security is not required."」

此外，在 Learning Curve Toys, Inc. v. PlayWood Toys, Inc.[35] 一案中，法院認為企業透過 NDA、限制接觸人員範圍以及控制產品開發資訊流通等措施，足以構成合理保密措施。該案特別強調資訊接觸範圍之控制（control of access），並認為企業應使資訊僅限於具有業務需要之人員知悉。本案進一步揭示合理保密措施之核心在於接觸控制（Access Control）。無論企業採取契約措施、管理措施或技術措施，其目的均在於限制未授權者取得資訊，非單純保存資訊內容。

另外，在 Religious Technology Center v. Netcom On-Line Communication Services, Inc.[36] 一案中，法院指出，即使資訊曾於有限範圍內流通，只要資訊所有人仍持續透過保密義務或技術措施限制第三人接觸，其秘密性仍可能受到維持。據此，美國法院對於合理保密措施之認定，並不要求資訊處於絕對封閉狀態，而要求企業持續維持資訊之秘密管理狀態。

在 E.I. duPont deNemours & Co. v. Christopher[37] 一案中，原告公司正在興建化學工廠，被告透過租用飛機自空中拍攝工廠內部設施，藉此蒐集原告之製程資訊。被告主張，原告既未以屋頂覆蓋工廠，即表示其未充分保護相關資訊。然法院認為，法律並不要求資訊所有人必須採取不合理或過度昂貴之保密措施，僅須依具體情況採取合理努力維持資訊秘密性即可。據此，即使原告未能完全杜絕第三人以特殊方式取得資訊，仍不影響其營業秘密之成立。

---

35 Learning Curve Toys, Incorporated, Plaintiff-counter-defendant-appellee, v. Playwood Toys, Incorporated, Defendant-counter-plaintiff-appellant, v. Roy Wilson, Harry Abraham, and John Lee, Counter-defendants-appellees, 342 F.3d 714 (7th Cir. 2003). 法院認為：「...the text of the Act does not require a trade secret owner to maintain absolute secrecy; it requires 'efforts that are reasonable under the circumstances.' Control of access is a primary indicator of such reasonableness.」「...the concept was strictly closely held within PlayWood. Only PlayWood's key personnel... were aware of the concept. It was not revealed to any other employees, let alone anyone outside of the company.」

36 Religious Tech. Center v. Netcom On-Line Comm., 907 F. Supp. 1361 (N.D. Cal. 1995). 法院認為：「The secrecy of the information need not be total.」「A trade secret is not destroyed if it is multiplexed or revealed to a few outsiders under an express or implied duty of confidentiality. Moreover, where the disclosure was unauthorized, the court must look to whether the owner took swift action to maintain the secrecy of the information or to control further dissemination.」

37 E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970). 法院認為：「To require DuPont to put a roof over the unfinished plant to guard its secret would impose an unjustifiable burden.」「Our technology has carried us beyond the stage where the robber baron must need use a crowbar or the hissing fuse to steal a corporation's treasures. ... We cannot allow a competitor to breach the wall of secrecy by a means which is so far removed from fair play.」

在 Electro-Craft Corp. v. Controlled Motion, Inc.[38] 一案中，法院認為，雖然原告所主張之技術資料具有一定經濟價值，然其未要求員工簽署 NDA，亦未建立明確之資訊分級制度或限制員工接觸相關資料，因此欠缺合理保密措施，不得主張營業秘密保護。法院強調，資訊所有人應採取積極措施限制資訊流通範圍，非僅於事後主張資訊具有重要性。即使資訊本身具有高度經濟價值，若企業未建立足以限制未授權者接觸資訊之制度，法院仍可能否認其營業秘密之地位。由此可見，資訊價值與合理保密措施乃屬不同判斷層次，二者不得混為一談。

綜合前述判決，美國法院對合理保密措施之理解，可歸納為兩項核心原則。其一，合理保密措施並不等同於絕對保密，企業僅須依其具體情況採取合理努力即可；其二，合理保密措施之本質在於建立資訊接觸控制機制，以限制未授權者取得資訊。此二項原則亦構成本文後續分析區塊鏈技術法律定位之重要基礎。

三、科技保護措施於營業秘密保護之運用

隨著資訊科技發展，企業保護營業秘密之方式已逐漸由傳統紙本管理，轉向數位管理[39]，當代企業除透過保密契約與內部管理制度之外，亦大量運用資訊科技作為營業秘密保護的手段[40]。

例如，企業可以透過權限分級制度，使不同職位員工僅能接觸到其業務所需之資訊，亦可透過加密技術避免資料於傳輸或儲存過程中遭第三人取得，此類措施均已被美國以及我國法院視為合理保密措施之一環。

但是，並非所有科技措施當然構成合理保密措施，倘若某項技術僅能記錄資訊之產生、修改，或流轉過程，無法實際限制資訊接觸，其功能可能較偏向資訊管理或證據保存，非傳統意義上之保密措施。

---

38 Electro-Craft Corp. v. Controlled Motion (1983). 法院認為：「The owner of a trade secret cannot merely intend that the information remain secret. The law requires more than a subjective intent; it requires an objective manifestation of that intent through reasonable efforts under the circumstances.」「ECC's physical security measures were lax. ... Drawings were not kept in a central or locked location... [and] none of the ECC drawings were stamped 'confidential' or 'secret.'」

39 數位轉型是什麼？八分鐘了解七大好處、轉型三階段與產業案例，國泰金控，https://www.cathayholdings.com/holdings/brand/fintech/ctc/trends/digital_transformation（最後瀏覽日：2026/06/15）。

40 營業秘密之保護與管理，經濟部智慧財產局營業秘密主題網，https://www.tipo.gov.tw/tw/tradesecrets/885.html（最後瀏覽日：2026/06/15）。

四、小結

綜合上述比較法觀察，美國法無論 UTSA、DTSA 或相關法院判決，均採取合理努力標準作為判斷合理保密措施之依據，法院所重視者並非企業是否達到絕對保密，而是其是否已建立足以維護資訊秘密性之制度。

此外，隨著資訊科技發展[41]，科技之措施已逐漸成為營業秘密保護之重要工具，然而法院對於科技措施之評價仍以其是否具有限制資訊接觸功能為核心判斷標準，換言之，若僅具記錄、驗證，或證據保存功能，欠缺實質保密效果，是否得直接構成合理保密措施，仍須討論之[42]。

此一問題在區塊鏈存證機制上尤其具有爭議，區塊鏈存證雖然具有不可竄改、時間戳記，以及可溯源性等優勢，但其是否具備前述合理保密措施所要求之保密功能，仍有待進一步分析。然而若是未區分區塊鏈之底層架構，即一概地否定其限制接觸之可能，似乎失之武斷。下文將進一步討論區塊鏈技術之特性及其於營業秘密保護制度中之定位。

肆、區塊鏈技術作為合理保密措施判斷因素之分析

一、區塊鏈存證與合理保密措施之關聯性

如上一節所述，無論我國法院實務或美國法上之合理努力標準，均強調合理保密措施之核心功能在於維持資訊之秘密性，並限制未授權者接觸營業秘密[43]。因此，判斷某項措施是否構成合理保密措施時，應觀察其是否具備保密功能，非僅著眼於其資訊管理或證據保存效果。

據此，區塊鏈存證與傳統保密措施雖同樣具有保護資訊之目的，但其法律上之評價並不完全相同。

41 關於資訊科技之相關資訊，技術報告，中央研究院資訊科技創新研究中心，https://www.citi.sinica.edu.tw/main/research-tech-reports（最後瀏覽日：2026/06/15）。

42 公開鏈可能無法單獨認為是合理保密措施。

43 關於營業秘密之保護，記住 3321，守住營業秘密，臺灣高等檢察署網站，https://www.tph.moj.gov.tw/4421/4475/632364/861322/post（最後瀏覽日：2026/06/15）。

二、區塊鏈存證難以單獨構成合理保密措施

區塊鏈存證之主要功能，在於利用區塊鏈技術記錄特定資訊之雜湊值、建立時間及歷史紀錄，以確保資訊之完整性以及不可竄改性，亦即，其證明某項資訊曾於某特定時點存在，以及資訊未遭事後修改。

然而，合理保密措施所要求者，乃係資訊所有人對於資訊接觸範圍的控制，此可參常見之保密措施如 NDA、文件分級，以及門禁管理等，均具有直接限制第三人取得資訊之功能。

相較之下，區塊鏈存證並不當然具有阻止第三人接觸資訊之效果。即使企業已將重要文件進行區塊鏈存證，倘若該文件本身仍可以被任意下載、複製或傳送，資訊外洩風險並不因此降低。

例如，公司將其研發之技術文件進行區塊鏈存證，並取得時間戳記紀錄，然若公司並未建立權限管理制度，所有員工均可以自由存取該文件，該區塊鏈存證僅能證明文件存在時間，惟無法防止文件遭未授權人員取得。據此，企業仍難以主張已採取合理保密措施。

因此，區塊鏈存證雖能提升資訊可信度及完整性，惟其本質仍屬資訊管理及證據保存工具，非資訊隔離工具，倘若欠缺其他保密措施之配合，原則上不宜單獨認定其已符合營業秘密法上合理保密措施之要求。

三、區塊鏈技術類型之分流：聯盟鏈與私有鏈之技術隔離功能

前述「區塊鏈存證難以單獨構成合理保密措施」之結論，本質上建立於「公開鏈（Public Blockchain）」[44]之技術架構。於公開鏈架構下，任何人均得任意檢視鏈上之交易軌跡，縱使上鏈者僅為資訊之雜湊值，然就該區塊鏈技術本身而言，確實欠缺限制他人接觸或隔離資訊之功能。惟探討區塊鏈技術於營業秘密法上之適用時，不應對不同區塊鏈架構作相同評價，而是應重點區辨不同區塊鏈架構於技術控制層面本質上之差異點[45]。

---

44 公鏈、私有鏈、聯盟鏈是什麼？區塊鏈的三大分類介紹，CHAINEE，https://chainee.io/what-is-public-blockchain-private-blockchain-consortium-blockchain（最後瀏覽日：2026/06/15）。

45 同前註。

區塊鏈技術依其開放程度與權限管理機制，尚得區分為「聯盟鏈（Consortium Blockchain）」與「私有鏈（Private Blockchain）」。相比於前揭公開鏈的完全去中心化與數據公開性，聯盟鏈與私有鏈具備高度的「准入管制（Permissioned）」[46]特徵。在此類架構下，企業得透過「角色存取控制（Role-Based Access Control, RBAC）[47]」與加密金鑰（Cryptographic Keys）[48]管理機制，嚴格限制僅有通過身分驗證之特定節點或特定權限之員工，始得存取、解密並讀取鏈上之資產與機密數據。

當企業採取具備權限控管之聯盟鏈或私有鏈進行內部資訊管理時，該技術已超越純粹事後證據保存之範疇，而兼具事前接觸限制之實質功能。

至於聯盟鏈或私有鏈於實際運作上如何維持營業秘密之秘密性，應進一步區分「營業秘密資料本身」與「用以驗證該資料之鏈上資訊」。企業運用區塊鏈保護營業秘密，並非必須將營業秘密之原始文件或明文內容直接上傳至區塊鏈。

較為適當之作法，係採取「鏈上存證、鏈下保存」[49]之架構，將技術圖紙、配方、原始碼，以及客戶資料等營業秘密原始文件，保存於企業內部之伺服器、加密資料庫，或其他具有存取控制之儲存環境，而僅將該文件經雜湊運算所得之雜湊值、時間戳記、權限異動，或係存取紀錄等資訊寫入區塊鏈。

---

46 補充言之，關於數位證據監管鏈之研究，區塊鏈智能合約與跨境數位證據監管鏈之應用，李昌鈺博士物證科學教育基金會，https://www.hclf.org.tw/uploads/magazine/attachment/136/%E5%8D%80%E5%A1%8A%E9%8F%88%E6%99%BA%E8%83%BD%E5%90%88%E7%B4%84%E8%88%87%E8%B7%A8%E5%A2%83%E6%95%B8%E4%BD%8D%E8%AD%89%E6%93%9A%E7%9B%A3%E7%AE%A1%E9%8F%88%E4%B9%8B%E6%87%89%E7%94%A8.pdf（最後瀏覽日：2026/06/15）。

47 什麼是基於角色的存取控制（RBAC）？基於角色的存取控制僅根據使用者在組織中的角色允許或限制使用者對資料的存取，CLOUDFLARE，https://www.cloudflare.com/zh-tw/learning/access-management/role-based-access-control-rbac/（最後瀏覽日：2026/06/15）。

48 什麼是密碼編譯金鑰？金鑰是一組按特定順序排列的隨機字元。加密通訊協定使用金鑰來更改資料，對資料進行加擾，這樣任何沒有金鑰的人都無法解碼資訊，CLOUDFLARE 網站，https://www.cloudflare.com/zh-tw/learning/ssl/what-is-a-cryptographic-key/（最後瀏覽日：2026/06/15）。

49 Ajay Kumar Shrestha, Julita Vassileva & Ralph Deters, *A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives*, 3 Frontiers in Blockchain, art. 497985, at 7 (2020). “Therefore, we have a general architecture of the user data sharing system based on blockchain and off-chain data storage as shown in Figure 1. The general architecture ensures that the actual user data is never exposed to the blockchain. The user data is first hashed and encrypted before uploading it into the off-chain storage. The data owners from their client applications can directly store them on the off-chain storage. The terms and conditions regarding the access to user data are encoded in smart contracts along with the metadata and hash of the data and published on a blockchain platform (Ethereum).”

由於雜湊函數（Hash Function）係具有單向性，原則上無法僅由雜湊值反推出原始文件內容[50]，因此得在不直接揭露營業秘密內容之前提下，利用區塊鏈之不可竄改性與可追溯性，作為證明特定資料於特定時間已存在及其內容完整性之技術性依據。

另一方面，如企業因特定業務需求而有將相關資料置於聯盟鏈或私有鏈之必要，亦不宜將營業秘密以明文方式直接供所有節點讀取，而應結合資料加密、身分驗證、金鑰管理、角色權限控制，以及節點准入等技術，使僅有經授權之特定成員得以存取或解密相關資訊。

亦即，聯盟鏈或私有鏈之保密效果，並非當然源自其「非公開鏈」之性質，亦非單純依賴區塊鏈之不可竄改特性，而係取決於其具體架構是否能夠實質限制未經授權者接觸資訊。

倘企業僅將營業秘密以明文方式記錄於區塊鏈，而未採取適當之加密、權限管理，或接觸控制措施，即使採用私有鏈或聯盟鏈，亦難僅憑其鏈型即認為已具備合理保密措施。

反之，如其透過鏈下保存、資料加密、准入控制，以及權限管理等制度，使營業秘密僅能由特定授權者接觸，並利用區塊鏈記錄相關存取及權限異動軌跡，則此種技術架構即具有事前限制接觸，與事後追蹤驗證之雙重功能，並得納入企業整體保密制度之一環，作為判斷其是否已採取合理保密措施之重要因素。

此時，區塊鏈技術於營業秘密法第 2 條第 3 款之定位，應視其具體架構而可能成為兼具雙重功能之「技術保護措施」：其一，透過鏈下保存、資料加密、身分驗證、權限管理及節點准入等機制，使未經授權之第三人或一般員工原則上無法接觸營業秘密內容，進而達成限制資訊流轉範圍之效果；其二，結合區塊鏈之時間戳記、不可竄改性及分散式帳本特性，記錄相關授權、存取或修改之歷史軌跡。

[50] Urs Wagner & Thomas Lugrin, *Hash Functions*, *in* Trends in Data Protection and Encryption Technologies 21, 21 (Valentin Mulder et al. eds., 2023). “Hash functions are one-way functions that map arbitrary-length input to fixed length output. Cryptographic hash functions enjoy additional properties, making them suitable for many cryptographic applications. Established hash functions are considered secure, and no significant development is expected in this area. Insecure hash functions should be discarded, and existing secure hash functions should be promoted and adequately used.”

綜上，倘若企業所採取者為准入型聯盟鏈或私有鏈，且該系統在架構設計上已實質限制未授權者之接觸可能，此類區塊鏈架構即可能具備合理保密措施所要求之接觸控制功能。此時，法院於個案判斷時，即不應將其視為單純的輔助性證據工具，則該區塊鏈系統本身即可能構成合理保密措施之一環，並得作為法院認定企業已採取合理保密措施之重要判斷因素。

四、區塊鏈存證作為合理保密措施之輔助

雖然，區塊鏈存證（公開鏈）難以單獨構成合理保密措施，然此並不代表其對於營業秘密保護毫無貢獻。法院判斷合理保密措施時，往往採取整體觀察模式[51]，並非要求企業必須採取特定形式之保密措施，若企業已建立 NDA、權限管理，帳號控制，以及資訊安全制度[52]，並進一步利用區塊鏈存證記錄營業秘密之建立、存取及流轉過程，則該區塊鏈存證仍可能成為法院認定該企業已積極保護資訊之佐證資料。

舉例來說，如果企業除了要求員工簽署保密契約外，亦將研發文件之建立時間、修改紀錄，以及存取紀錄透過區塊鏈保存，當未來發生營業秘密侵害爭議時，企業即可藉由區塊鏈紀錄證明其長期將相關資訊視為機密資訊管理，並持續維持其保密狀態。

---

51 智慧財產及商業法院 112 年度民營訴字第 15 號民事判決。法院認為：「按營業秘密法第 2 條第 3 款所稱所有人已採取合理之保密措施，係指所有人按其人力、財力，依社會通常所可能之方法或技術，將不被公眾知悉之情報資訊，依業務需要分類、分級而由不同之授權職務等級者知悉而言；此於電腦資訊之保護，就使用者每設有授權帳號、密碼等管制措施。而就營業秘密之秘密管理性要件，包含主觀及客觀要件，所有人主觀上應有管理秘密之意思，亦即主觀將某項資料、資訊認屬秘密而為管理，且客觀上有管理秘密之狀態，即客觀上亦係作為秘密而為一定之行為，使員工或外部人員瞭解其將該資料、資訊當成秘密加以保守之意思。查：系爭資料雖儲存於原告公司之正航系統中，並設有授權使用帳號密碼，業據原告陳述在卷（本院卷二第 151 頁營業秘密內容分類整理表），而足認原告主觀上有保護該等資訊之意願，惟就其資訊安全防護手段而言，原告雖主張僅有負責業務之人員有權限登入正航系統取得系爭資料等語，然原告業已自承：被告黃明仁任職期間，原告公司含法定代理人共 13 人，除了財會是專人外，其餘員工均身兼數職，故多數員工均負責業務等語（本院卷二第 101 頁），足認原告公司內多數員工均可取得系爭資料，顯見系爭資料之共享型態，客觀上並無明確之分類分級管制，亦難認原告已採取管制檔案傳輸及存取資訊之追蹤管理等整體防護措施，難認合於合理保密措施之要件。」

52 關於資訊安全制度之相關資訊，共通規範，國家資通安全研究院，https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/（最後瀏覽日：2026/06/15）。

此時，區塊鏈存證雖非保密措施之核心內容，然其仍有助於證明企業具備保密意思以及保密行為，因此區塊鏈存證可以視為合理保密措施之補強機制，而非替代。

對於本文先前所述之聯盟鏈與私有鏈系統，本身即可能構成合理保密措施之一環，並得作為法院認定企業已採取合理保密措施之重要判斷因素，可能會有反對意見認為，聯盟鏈或私有鏈所採行之角色存取控制、帳號密碼驗證，以及加密金鑰管理等機制，其本質上與現行企業資訊系統所使用之權限管理制度並無二致[53]。因此，即使企業將資訊建置於聯盟鏈架構中，其真正發揮保密效果者仍為權限管理機制，非區塊鏈技術本身。據此，區塊鏈僅屬資訊系統之載體，並不應被賦予合理保密措施地位。

此項見解固非無據，蓋營業秘密法所重視者，確實並非技術名稱本身，而係該技術是否具有維持資訊秘密性及限制未授權者接觸之效果。若企業僅將既有資料庫更名為區塊鏈系統，而其權限管理方式與一般伺服器無異，確有重複評價之疑慮。

但是，聯盟鏈與私有鏈之法律意義並不僅止於權限控管。相較於傳統集中式資料庫，聯盟鏈尚兼具分散式帳本[54]、共識機制[55]、不可竄改性，以及完整軌跡保存等特徵。其除具有事前限制資訊接觸之功能外，亦能完整記錄資訊之存取、修改及授權歷程。此種兼具接觸控制與軌跡留存之雙功能，已超越一般資訊管理系統所能提供之保護程度。

傳統見解固然認為聯盟鏈之角色存取控制與傳統集中式資料庫之權限控管在邏輯上並無異[56]，惟兩者在資安防禦深度與內部信任機制上存在本質之差別。

53 反對見解可能認為區塊鏈系統與傳統上之保密措施差異不大。

54 最高法院 114 年度台上字第 6733 號刑事判決。法院指出：「現今使用區塊鏈技術之加密虛擬貨幣，透過分散式帳本技術進行記帳驗證，具有去中心化、高度匿名之特性。」

55 臺灣雲林地方法院 113 年度重訴字第 2 號刑事判決。法院指出：「由於虛擬貨幣當中的加密貨幣，具有去中心化【利用區塊鏈技術驅動的貨幣，並不由任何中心化機構（如政府或銀行）發行和控制；而是基於一套共識機制，通常在創立初階已經把發行規則嵌於程式碼中（code is law），確定代幣總供應量及挖礦難度、獎勵減半週期等，這些規則無法被竄改。」

56 傳統見解可能忽略聯盟鏈以及私有鏈保護機制周密於一般傳統手段。

在傳統集中式資料庫架構下，資料庫管理員（Database Administrator, DBA）[57]或掌握後台核心權限之內部人，客觀上皆有能力任意竄改存取權限、偽造讀取紀錄，甚至於事後抹除入侵與洩密之軌跡。反之，聯盟鏈基於分散式共識機制與區塊鏈不可竄改性，縱使是系統管理節點亦無法單方悄悄為惡或事後消滅證據。

此項技術差異，方為聯盟鏈超越傳統資安系統，而更符合營業秘密法「合理保密措施」要求之關鍵技術內涵。

倘若企業所建構之聯盟鏈系統已透過身分驗證、權限分級，及加密金鑰機制，實質限制未授權者接觸資訊，自功能觀察言之，其與法院所肯認之帳號密碼管理或權限控管措施並無本質差異，理論上亦應受到相同評價。

伍、結論

綜上所述，本文認為區塊鏈技術與營業秘密法上的合理保密措施，應採取前述技術架構分流之動態觀察模式，並完整認識到區塊鏈於營業秘密保護上係兼具「事前防禦（保密措施）」與「事後證明（證據保存）」之雙重功能價值。

首先，就「事後證據保存」之工具價值而言，無論企業是採用公開鏈、聯盟鏈，或私有鏈架構，區塊鏈技術所具備之不可竄改性與時間戳記特徵，均能協助證明特定資訊係於一定時間點存在，並驗證其內容是否有遭事後變更，進以大幅降低企業於訴訟中之舉證負擔。即使公開鏈存證欠缺實質之接觸隔離機制，其仍得作為輔助性工具，用以佐證企業主觀上，是具有保密意思及將資訊納入秘密管理制度之客觀事實。

其次，針對具備准入管制之聯盟鏈或私有鏈系統，因其在技術層面已結合「角色存取控制」與「加密金鑰管理」，客觀上已能實質限制未授權第三人之接觸，實質具備事前資訊隔離之效果。惟依我國司法實務，法院對於合理保密措施之認

[57] 關於 DBA 之相關討論，控制資料庫管理者（DBA）的存取權，IBM，https://www.ibm.com/docs/zh-tw/db2/11.5.x?topic=ownership-controlling-access-database-administrators-dbas（最後瀏覽日：2026/06/15）。

定，乃採取「綜合衡酌多項因素」之整體判斷模式，非僅憑單一技術措施即可逕行認定。

據此，企業若建構具備權限控管之聯盟鏈或私有鏈系統，則該區塊鏈系統本身即可能構成合理保密措施之一環，並得作為法院認定企業已採取合理保密措施之重要判斷因素，其資安防禦深度亦因分散式架構而優於傳統集中式資料庫。

本文主張，司法實務於審理新興科技應用之營業秘密案件時，應捨棄區塊鏈僅具單純存證功能之印象。若企業建構具備權限控管之聯盟鏈或私有鏈系統，法院應重視該技術對於資訊隔離之貢獻，並將其納入整體保密作為的綜合評價因素，如此方能兼顧營業秘密法維護資訊秘密性之制度目的，以及數位治理時代之科技趨勢。