科技部 108 年度自行研究報告

區塊鏈技術所帶來的破壞式創新與政府的創新應用

研究單位：工程技術研究發展司

研究人員[1]：黃士育 助理研究員

研究期程：自 108 年 1 月 1 日至 108 年 12 月 31 日

---

[1]本文為研究人員自行完成之研究報告，不代表所屬單位之立場。

目　錄

圖 目 錄

-

摘　要

區塊鏈已經在過去幾年全球的貨幣狂熱及金融炒作下，從去年下半年開始熱度急速下降，整個數位貨幣市場開始進入熊市，各種數位貨幣的價格與交易量均大幅下跌，何時會再掀起一波浪潮不得而知，或者這只是浪尖上的一個小緩坡，就像 AI 一樣，正在累積更多的能量，才能往下一個高峰邁進。或許，隨著人們仰賴著數位化的過程中，這一切的改變皆在潛移默化地進行著，等待研發人員讓區塊鏈技術更加成熟、操作理解上更加友善，以及等待整個區塊鏈生態圈的發展更加趨於穩定完善。

而我們的政府或企業除了在推動數位轉型的過程，應該想想，哪些散落的、片斷的資料是可以運用區塊鏈的技術將其資訊數位化，從這個方面去著手，探索政府部會現有的需求面，或許跨部會的資訊交流會有更多的需求等待被挖掘，找到這些需求再結合國內的區塊鏈學者專家共同研發，勢必能發展出搶先布局全世界的區塊鏈應用技術。

本研究發現之主要發現為：

1. **中央銀行與區塊鏈**

中央銀行在今年 11 月的「財金公司 108 年金融資訊系統年會」簡報中有提出，由中央銀行來發行官方的數位新台幣，而實際的運行操作則由民間的電子貨幣公司負責使用，各個企業可以開發出不同的錢包，但裡面流通的金錢則是由央行所發行的數位新台幣，是將央行、金管會和電子貨幣的各自的責任義務進行一個分層負責的架構，兼顧各層級之間的利益，央行發行數位新台幣，除了原本流通的紙本新台幣，也可以掌握數位新台幣的流動，以順應未來數位的發展潮流。

2. **公務人員獎懲與區塊鏈**

人事行政總處在今年將公務人員獎懲令電子化(WebHR)上線，採用電子化方式發送，不再發送紙本文件，除了懲處與記 1 大功以上等重大獎勵採紙本外，這樣的電子化已涵蓋了 99%

的獎懲案。而除了電子化外，獎懲令更導入了區塊鏈的技術，透過區塊鏈的技術將紀錄在 WebHR 系統的數位證書，備份到國網中心所建立的聯盟鏈上，並透過區塊鏈的共識機制就可以確保不同節點所保存的數位檔案副本都是相同的，這樣的去中心化的儲存方式可省下備份的工作又達到驗證的效果，亦可避免駭客只要駭入 WebHR 系統就會被改寫資訊的資安問題。

3. 醫療病例與區塊鏈

衛福部將同意書數位化之後的資訊安全就顯得相當重要，為了避免兩造雙方的醫療糾紛，數位化同意書必須要導入區塊鏈的技術，先在數位同意書上，透過數位簽名或自然人憑證加入數位憑證，然後再把所有的資訊保存到區塊鏈上，讓民眾跟醫療機構能夠安心地使用數位同意書所帶來的便利。

本研究之主要建議為：

1. 科技部的區塊鏈應用

本部能夠設計一套系統讓各個機構以電子文件上傳到本部系統，並將資料加上區塊鏈，本部承辦人、校方研發處窗口，甚至是計畫主持人都可以上線了解送件的進度情況，這樣一來每年可以減少上萬張來自各機構的送件紙本，以及省去各機構郵寄紙本的成本耗費，同時也可以讓以往需耗費 3~5 天的郵寄時間，瞬間只要半天之內彼此就可以確認收送件的狀況，縮短了整個專題計畫送件的流程，同樣的系統也可以應用在本部在通知各機關及各計畫主持人時。

2. 區塊鏈應用在電子發票

電子發票或收據都能夠數位化並存放在手機的單一形式錢包中，政府只要制定好統一個規格，透過區塊鏈的技術建立一套電子發票的防偽機制，讓商家、公司行號及政府的任何單據都可以上區塊鏈，這樣大家就可以使用 app 來做報帳的動作。使用區塊鏈技術的電子發票就向在大家認可的文件上簽名或用印，具有共識且不可竄改的效力。

壹、 前言

一、研究緣起與目的

區塊鏈之所以被大家視為革命性的技術，世界上第一次只要靠網路的技術跟機制就能完成有價資產的交易及轉移，完全不需要透過中心化機構的轉手，這個手續就可以讓兩個彼此陌生且不信任的人在網路上進行交易。然而，區塊鏈已經在過去幾年全球的貨幣狂熱及金融炒作下，從去年下半年開始熱度急速下降，整個數位貨幣市場開始進入熊市，各種數位貨幣的價格與交易量均大幅下跌，何時會再掀起一波浪潮不得而知，或者這只是浪尖上的一個小緩坡，就像 AI 一樣，正在累積更多的能量，才能往下一個高峰邁進。或許，隨著人們仰賴著數位化的過程中，這一切的改變皆在潛移默化地進行著，等待研發人員讓區塊鏈技術更加成熟、操作理解上更加友善，以及等待整個區塊鏈生態圈的發展更加趨於穩定完善。

國內外金融科技的技術研究圈，對於區塊鏈的熱情並沒有隨著比特幣的幣值貶值而失去興趣，仍有一群技術愛好者持續的研究，及關注著整個數位貨幣及區塊鏈技術的發展。而這股熱情也蔓延到了文化領域，今年 10 月份台灣上映了全球首部以區塊鏈為題材的商業戰電影《聖人大盜》，一名台灣的年輕導演大膽且敏銳地仿照華爾街的商業戰爭形式，這也是台灣電影界算是首次嘗試了新穎性的金融電影題材，獲得了國內電影圈評審的青睞，此片入圍了今年度的金馬獎最佳新導演提名。這部電影點出了網路技術所帶來的機會與翻轉，以及區塊鏈的技術對傳統金融業帶來衝擊性的影響，就如同當初汽車的推出推翻了馬車、電子收費的便利使得收費員從行業的歷史上消逝，這些技術的演進都是跨時代的一種變革，我想值得推薦部內同仁來感受一下科技技術變革與電影文化的結合，而我們身為科技部的一員，就是在不斷地變革中，持續地與各領域的專家一起成長與學習，並協助所有的專家學者研發出更多創新的技術。

區塊鏈的技術開發是為了解決網路上交易的資訊安全的問題，也就是「信任」的問題，因此技術上採取了軟體上的「共識」

（consensus）機制，但是現在把「共識」運用在區塊鏈上就很難理解它是如何運作，其實可以用一個簡單的案例來說明，就能簡單地理解共識機制是什麼。每戶住家大樓都有門牌地址，如果去查「台北市大安區和平東路二段 106 號」，就會發現這個地址屬於科技部，這就是共識，但是誰決定這個地址代表科技部呢？答案是政府。

所以說，共識是用來釐清爭端的好方法，而大家對地址的共識，就是由政府建立；同樣的，大家對金錢（或財富）的共識，是由銀行來建立基準制度；大家對法律（或犯罪）的共識，是由法院建立。這些都是交由權威機構來建立共識，也就是「中心化」的共識，這種現行運作方法比較有效率，但唯一要擔心的就是政府、銀行、法院被有心人士操縱。

為避免「中心化的共識」會受到人為的操控，於是乎就想到把權威機構去除，由所有的參與者共同建立共識，也就是「去中心化的共識」，其優點是不會因為駭客攻破集中式機房的電腦，就釀成政府或銀行的大災難。但缺點是共識由大家共同決定，所以運作效率通常比較差，因為彼此要先確認彼此手中的答案，才能達成共識。

因此，在區塊鏈的核心技術發展上，各方就是在找出使用軟體的技術來達成安全又高效率的「去中心化的共識」，這正是目前區塊鏈領域百家爭鳴的重要課題，若有一家業者或研究人員能找到一個最好的共識演算法就有一鳴驚人的機會。

二、研究方法與過程

(一)資料蒐集

1. 參加各個區塊鏈技術及應用的研討會。
2. 蒐集各個部會推動區塊鏈相關資訊。
3. 蒐集近年來學界區塊鏈技術研發計畫相關資料。

(二)意見交換

1. 與研討會與會人員或區塊鏈承辦業務同仁交流。
2. 徵詢亞太區塊鏈發展協會與學界區塊鏈專家意見。

(三)資料分析

1. 依據前述蒐集及意見交換獲得之資料，進行彙整及分析。

(四)報告撰寫

1. 完成本研究之成果報告。

貳、 認識區塊鏈

區塊鏈一詞最早是在 2008 年的時候，由一位名叫中本聰所寫的比特幣（Bitcoin）白皮書中所提出來的，是一種屬於對等式網路架構（Peer-to-Peer,P2P）的分散式帳本技術（Distributed Ledger Technology,DLT)，這個技術是由一連串的密碼學所組成，在每個區塊內都包含了區塊的容量大小、區塊的表頭(Header)、前一個區塊的加密雜湊值(Hash)、時間戳記、隨機數(Nonce)以及交易的資料內容，如下圖。

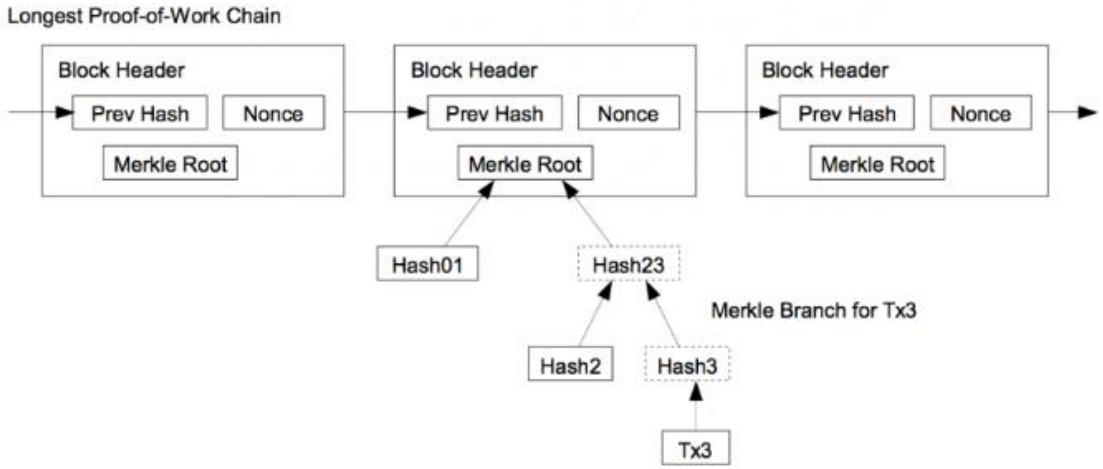

圖 1、區塊的格式

資料來源：比特幣白皮書(https://bitcoin.org/bitcoin.pdf)

區塊鏈中所用的技術並非全部都是近期新開發的技術，而是將在資訊領域過往幾個已純熟的技術(分散式技術、P2P 網路架構、雜湊函數、資料結構、共識演算法等)重新組合建構在一起。

區塊鏈網路中，在區塊鏈上的所有節點都有一套相同的「共同帳本」，可以把它想像是一個全民皆可參與的電子記帳本，而其中的資料以區塊(block)的形式為單位(可以視為記帳本的每一個分頁)來產生和儲存，並按照時間排序串成一條鏈（chain）的資料結構，所有

鏈上的有節點都可以共同參與網路上的資料驗證、儲存及維護。

一個新區塊的產生需要得到網路上多數節點(數量的多寡取決於使用不同的共識機制，如比特幣則須取得至少 51%的認可)的認可，並在認可後向網路內的各個節點進行廣播，以將所有節點上的資料同步更新，新的區塊產生後則不能更改或刪除，因此，所有完整節點中的帳本內容都是一致的。每個節點同時必須負責起交易確認和廣播的工作，透過網路內各節點的相連結，就可以獲得共同帳本的相關服務，

這樣的機制可以讓區塊鏈具有資料不易被竄改的特性，並且在區塊鏈上的任一個節點都可以查證鏈上所有交易的正確性。因此，區塊鏈具有五大特色：

圖 2、區塊鏈的五大特色

至於上面所提到的節點，就是利用電腦硬體(windows、Linux)，花費一定的時間及電力等算力資源(就是大家說的「礦工」)，來計算出一組數學公式的結果，而最快計算出結果的節點，則具有為該區塊鏈記帳的權利(添加新區塊)，再來，該節點就必須向區塊鏈中的其他節點廣播計算的工作量證明 (Proof of Work, PoW)，這種使用算力來解決計算挑戰的過程稱之為挖礦(mining)，工作量證明是屬於「共識演算法」的一種。

區塊鏈系統上的節點根據不同的分工可分為，主節點(Full node)及輕節點 (Lightweight node)。主節點是區塊鏈網路的骨幹，可進行交易的確認和廣播，並存有所有區塊鏈上的交易紀錄，一個區塊鏈網路的主節點的數量越多也就越接近真正的去中心化，也代表著這個網路的安全程度。輕節點不像主節點那樣獨立運作，算是一般使用者的手機安裝的錢包軟體或是硬錢包，錢包內不需要有整個區塊鏈網路

的完整資料，只有交易時會將使用者錢包中的轉帳資料和區塊鏈網路進行核對。

以全球目前最龐大的比特幣為例，在比特幣節點觀測網站上可以查到 108/11/5 的節點數量大約是 9500 個上下，節點的數量會隨著每天會節點的上線數量有所不同，但經過一年的觀察，比特幣的節點數有隨著數位貨幣熱潮的退燒稍微遞減。

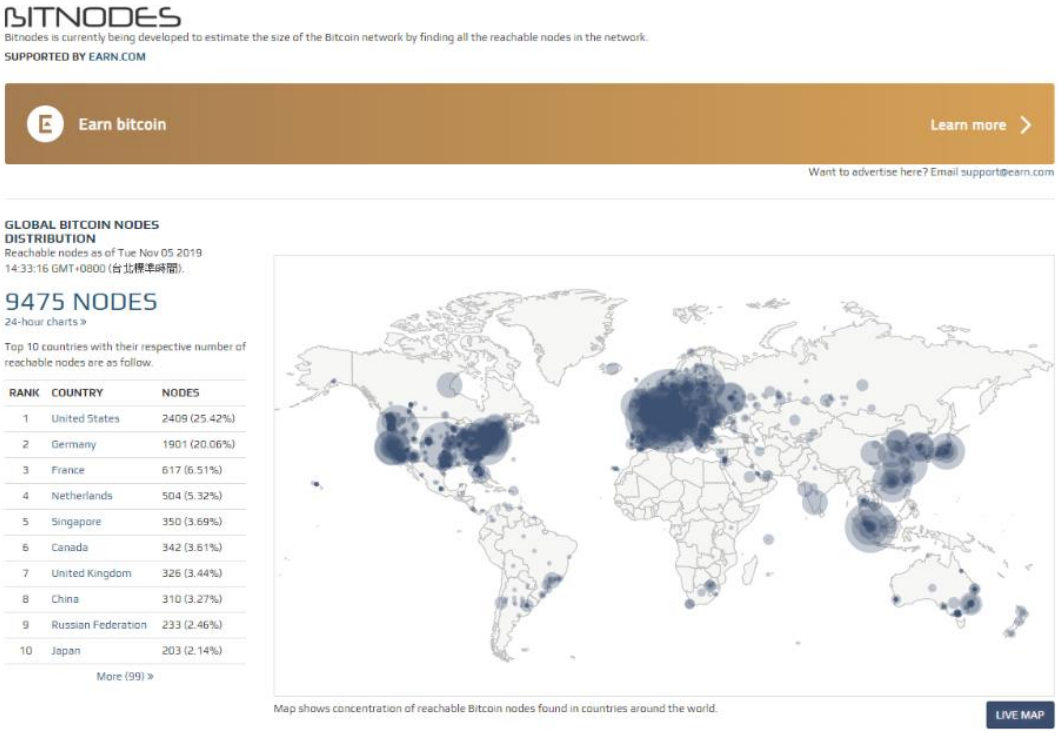

圖 3、比特幣 11/5 的節點數

資料來源：https://bitnodes.earn.com/

此外，區塊鏈可根據應用場景的不同，區分為兩類：1.公共鏈：任何人都可以加入區塊鏈網路進行資料存寫，如比特幣和以太坊（Ethereum）；2.私有(聯盟)鏈：屬於封閉型的區塊鏈，授權公司和組織才能加入網路。

一、 區塊鏈的核心技術

對於區塊鏈中的區塊、鏈是如何構成的，可以透過一個「Blockchain Demo」的網站，簡單的初步了解區塊鏈是如何運作的，也能知道區塊上記錄著哪些資訊、如何防止被惡意篡改、以及挖礦的電腦上都在計算哪些內容，下圖為該網站的區塊鏈的基本基本概念架

構圖。

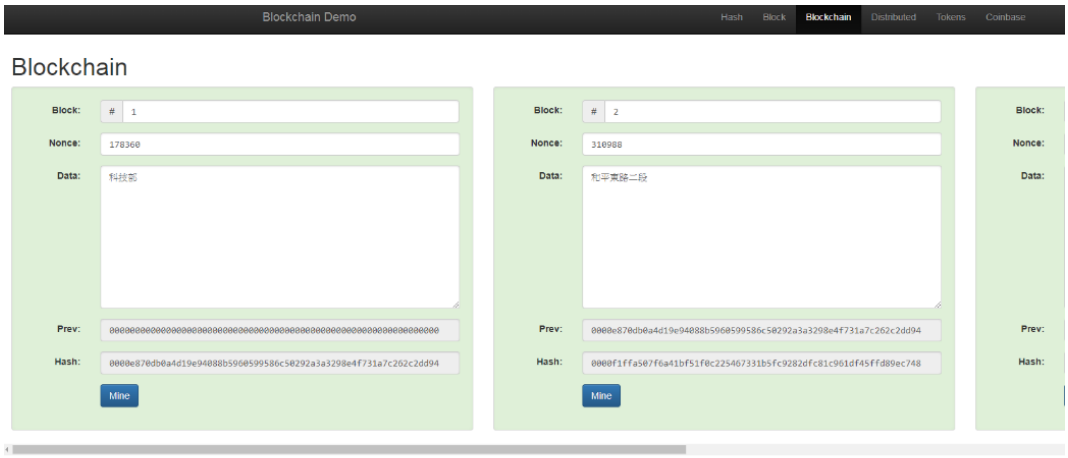

圖 4、區塊鏈的基本概念示意圖

從下圖中可以看到，「區塊」的結構包含了序號、隨機碼、內容以及雜湊值，並非是很複雜的結構，因為區塊鏈中使用的資訊技術，都是已經在資訊領域經歷很久考驗的成熟技術，只是在中本聰將他們組合起來，創造出區塊這樣具有安全性的結構。

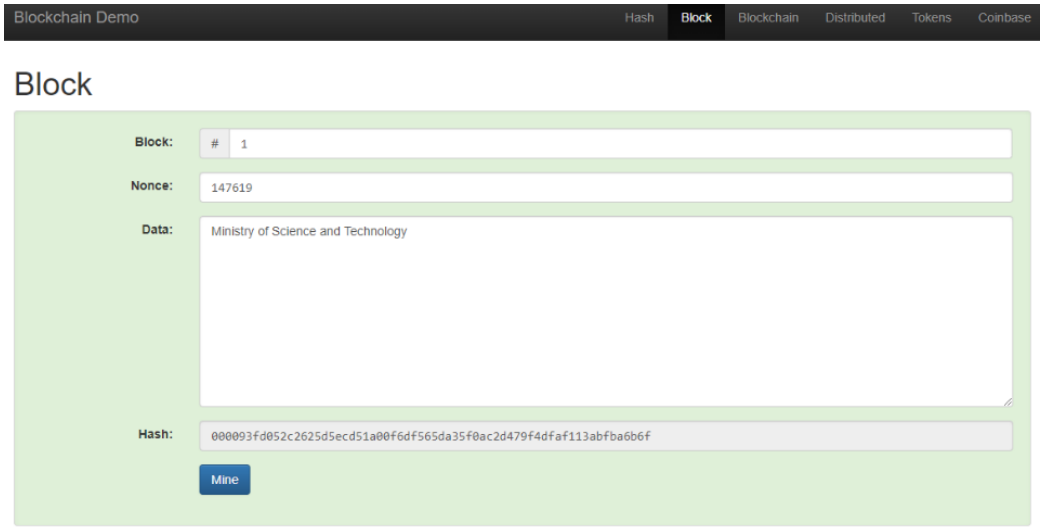

圖 5、一個區塊的架構

而其中「鏈」的呈現，則是將區塊彼此串接而成，每一個區塊的構成除了上述說的序號、隨機碼、內容及雜湊值之外，也必須包含前一個區塊的雜湊值，區塊「鏈」中的每個「區塊」代碼都與之前的區塊密不可分。每個新的區塊都包含前一個區塊的雜湊值（hash）」，而且每個區塊在添加之前都必須進行身份驗證，當區塊本身的內容或是前面區塊的內容有異動時，該區塊的雜湊值就必須重新計算，因此更

改區塊鏈是幾乎不可能的，如下圖。

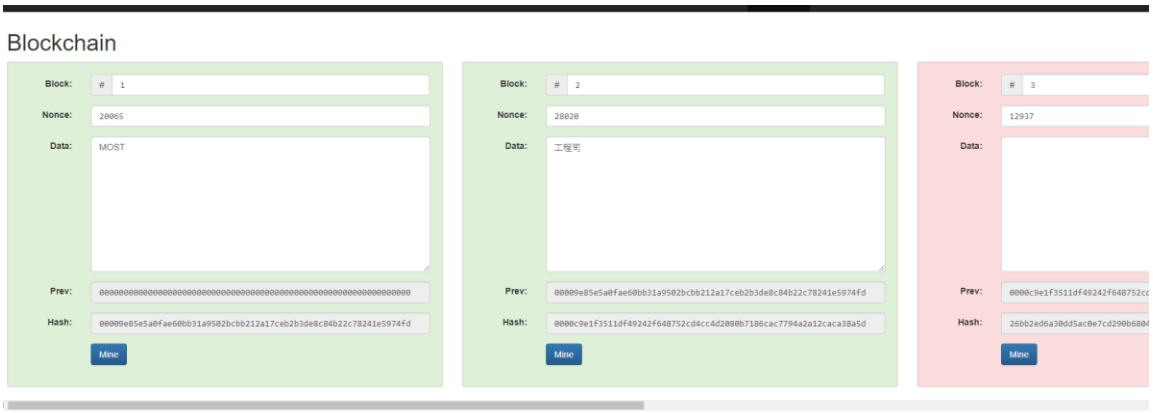

圖 6、區塊鏈的異動狀態

二、 區塊鏈 2.0

被稱作區塊鏈 2.0 的以太坊平台，允許開發者從頭到尾建構一個類似比特幣這樣的區塊鏈應用（通稱 DApp, Decentralized Application)，其最主要就是提供 DApp 開發者必要的模組化函式和工具，降低 DApp 的開發門檻和成本，除了讓開發者便利打造 DApp 之外，也可以讓各種 DApp 直接運行在以太坊平台上，並且根據使用量來收取以太幣的服務費。此外，智慧合約則是以太坊最重要的技術，主要是結合區塊鏈的防偽機制，合約的內容是開發者使用程式碼來撰寫，再由節點來執行的智慧合約的內容。以太坊使用較不浪費資源的 PoS 演算法，以免有心人士過於集中挖礦機，破壞了區塊鏈分散式架構的運作，並且改進了比特幣帳本同步時間過長的主要缺點，以太幣將帳本同步的時間縮短到 15 秒。

三、 比特幣使用的 PoW 演算法

工作量證明的技術原理是檢查雜湊函數(hash function)的一套規則，區塊的寫入規則是檢查「所產生的函數值的開頭是否有 4 個 0」，只有符合規則的函數值，才算是在這個鏈上合法運作的區塊。在區塊鏈的每個區塊都可以記錄多筆交易，只要區塊上的某個欄位有變動，都會引響到產生出來的函數的改變，導致函數不符合規則而造成區塊失效，進而造成整個區塊鏈上的資料失效。

區塊鏈在紀錄每筆交易時，還必須確認每個人在付錢的時候，錢

包裡是真的有錢，因為區塊鏈上並不會記錄每個人有多少錢，而是區塊鏈會藉由區塊彼此串連的特性，往前追溯歷史交易紀錄，去查證某個人過去的交易紀錄，來推算某個人所擁有的代幣數量。

之前很流行的挖礦，事實上就是在執行工作量證明（PoW）的運算，決定誰挖到礦、誰是在做白工的機制，挖到礦的人取得記帳權，因此有部份「礦工」為了提高挖礦效率，而客製出專門挖比特幣的硬體，造成挖礦機大賣的情形。擁有挖礦機器的礦工，因為運算能力比其他電腦強太多，反而破壞了區塊鏈假設「每台電腦運算能力皆差不多」的分散式系統概念設計，使得駭客只要攻破少數幾個運算能力強大的礦場，就會讓比特幣系統變得不安全。

當理解工作量證明是如何增加駭客攻擊的難度後，那就可以用同樣的認知去理解更多不同區塊鏈的防偽機制，例如以太坊的權益證明（Proof of Stake, PoS），若要取得新增區塊的權利，就必須持有越多的加密貨幣機會越高，在這個機制裡，使用了一個 coin-age(幣齡)的概念，當你持久的貨幣越多，或者是持久的時間越長，你取得新增區塊的機率就相對越高，當你一但新增區塊之後，你所擁有的幣齡就會歸零，避免持有貨幣越久的人壟斷整個鏈，也不會像 PoW 是在比較看誰的算力比強。

參、 研究發現與部會推動區塊鏈的案例

一、 區塊鏈的重要性

比特幣這套轉帳系統在 2008 年被提出時，中本聰的文章裡面只有提到區塊（block）、鏈（chain），但是沒有區塊鏈。區塊鏈是在比特幣出現幾年之後，大家才從比特幣這個應用中，歸納出來的概念。直到 2015 年問世的以太坊（Ethereum），就是把區塊鏈這項概念，變成大家都可以共用的基礎建設。想要在區塊鏈上建立應用的開發者，如今不用從頭打造一套專屬的區塊鏈，只要在以太坊上撰寫相對簡單的智慧合約，就能快速創造出類似比特幣的轉帳系統。

從歷史的角度來看，越來越多人想要在區塊鏈上建立應用，以太

坊這項技術就因應人們的需求而被開發出來，人們常說的區塊鏈領域變化很快，或是「幣圈一日，人間一年」，正確來說應該是「應用與基礎建設的循環」可能都是幾週或幾個月就循環一次，如同摩爾定律一般區塊鏈技術隨時都在不斷地更迭，所以才會讓人覺得永遠有新的應用出現，而這些應用又同時促使了區塊鏈的基礎技術發展。

區塊鏈的主要目的是將散落在各地的資訊(紙本資料)數位化，過去 20 年的全球化浪潮，讓各領域的分工更加細緻，但同時也增加了資訊的複雜度，所以，我們的政府或企業除了在推動數位轉型的過程，應該想想，哪些散落的、片斷的資料是可以運用區塊鏈的技術將其資訊數位化，或許從這個方面去著手。例如，明年要推動的數位身分證，區塊鏈能扮演的腳色就是數位的鋼印，能避免數位檔案被偽造，未來各部會或機關有越來越多紙本文件數位化，區塊鏈這套防偽技術也將越來越重要。

因此，探索政府部會現有的需求面，或許跨部會的資訊交流會有更多的需求等待被挖掘，找到這些需求再結合國內的區塊鏈學者專家共同研發，勢必能發展出搶先布局全世界的區塊鏈應用技術。以下，就提供近年來政府在施政上與區塊鏈結合的案例。

二、 中央銀行與區塊鏈

區塊鏈是目前全球最熱門的數位資產防偽技術之一，不同的區塊鏈就有不同的防偽技術，就好像新台幣、美金和日幣的鈔票上可能或多或少有使用浮水印這種防偽技術，但技術上會有些許差異，其安全性及成本也就會有所不同。因此，就可以理解為什麼全球會有這麼多種不同的區塊鏈，全球市面上 2,000 多種密碼貨幣有些是採用完全不同的區塊鏈技術來防偽，例如比特幣和以太坊，以及和台北市合作的 IOTA 基金會的 tangle 技術，以沒有區塊、沒有鏈的創新防偽技術，目前所有的區塊鏈技術也都還在調整修正，試圖找到最完整的狀態，以成為最後世界通用的國際標準。

而中央銀行在今年11月的「財金公司108年金融資訊系統年會」簡報中有提出，希望官方及民間聯手推動數位新台幣的架構(如下圖)，由中央銀行來發行官方的數位新台幣，而實際的運行操作則由民間的電子貨幣公司負責使用，各個企業可以開發出不同的錢包，但裡面流通的金錢則是由央行所發行的數位新台幣。

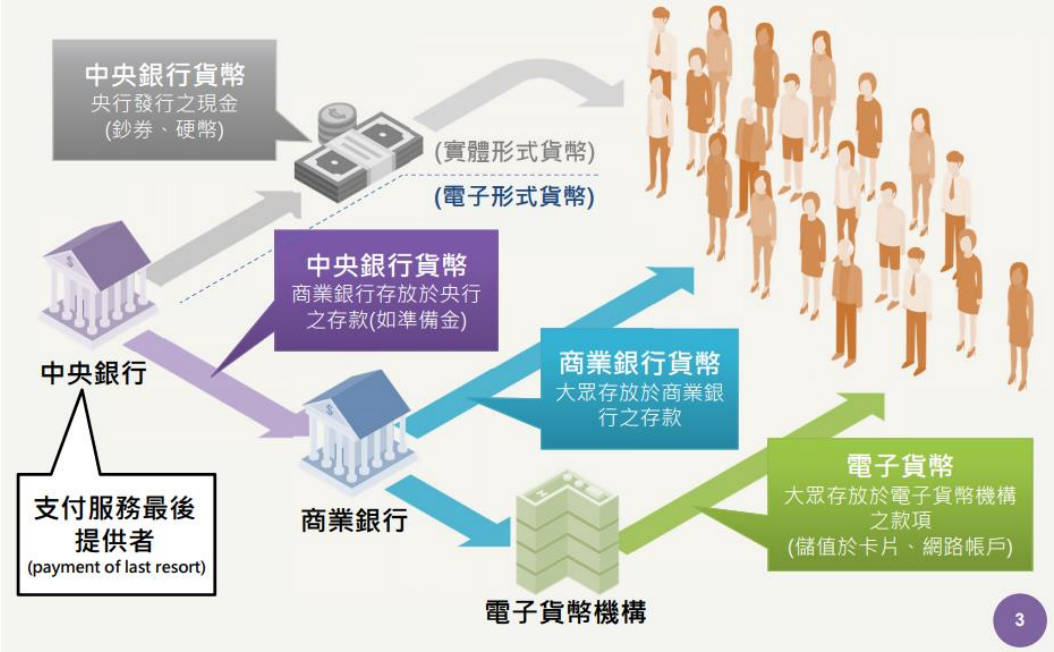

圖 7、中央銀行所構思的數位新台幣架構

資料來源：中央銀行(https://www.cbc.gov.tw/public/Attachment/91171155471.pptx)

這樣數位新台幣的架構，是將央行、金管會和電子貨幣的各自的責任義務進行一個分層負責的架構，兼顧各層級之間的利益，央行發行數位新台幣，除了原本流通的紙本新台幣，也可以掌握數位新台幣的流動，以順應未來數位的發展潮流；對於金管會來說，由於央行及金管會可以對數位新台幣制定統一個規格，解決了電子支付會面臨到各機構彼此不相通的窘境，但金管會也不用背負著如何推動數位新台幣的重責，則是由民間的電子貨幣公司來協助發展。而區塊鏈在數位新台幣則應該扮演重要的腳色，提供一個去中心化的科技來協助數位新台幣的流通、轉帳等金融帳務的資訊安全。

三、 公務人員獎懲與區塊鏈

今年在由科技會報舉辦的第四屆臺灣區塊鏈愛好者年會上，行政院人事行政總處舉了一個他們應用區塊鏈技術在實際公務上的例子。

從過去的統計數據來看，人事行政總處的公務人員獎懲令是他們最大宗的紙本資料，因為公務人員記功懲罰的案件，包含了嘉獎(1 次、2 次均有紙本)，小功 1 次、2 次等，一年平均發出 370 萬件的紙本獎懲令，此份紙本除給當事人必須簽收外，同時也必須副知所屬單位，因此，光在獎懲令上政府一年就平均需要發出 1 千多萬份的紙本資料，當然這份資料不會是只有薄薄的一張，通常都是厚厚的一疊，可想而知，每年必須要砍掉多少樹木來做這件事情。

有幸的是人事行政總處在今年將公務人員獎懲令電子化(WebHR)上線，採用電子化方式發送，不再發送紙本文件，除了懲處與記 1 大功以上等重大獎勵採紙本外，這樣的電子化已涵蓋了 99%的獎懲案。而除了電子化外，獎懲令更導入了區塊鏈的技術，然而紙本資料的數位化，不就是使用圖檔或是 PDF 電子檔，為什麼有需要使用區塊鏈呢？

我們都知道，紙本資料可以蓋上鋼印或是機關用印來增加偽造的難度，以確保紙本的有效性。但是數位資料就目前的技術則是難以防偽，只要是具有基本數位能力的人都可以使用修圖軟體製作出一張數位證書或是修改它，但也不能說目前完全都沒有防衛機制，只要將數位資料交由核發證書的主管保管，只要主管的權限沒有被盜，就可以確保這份數位證書的有效性。然後，大部分的數位證書的發行者與查驗者往往都是不同的單位，就像部內的同仁要拿數位證書去別的機構申請資料，該機構就無法驗證它的有效性，彼此的確認還是必須將資料印出來再機關用印。

因此人事行政總處與本部的國網中心合作，透過區塊鏈的技術將紀錄在 WebHR 系統的數位證書，備份到國網中心所建立的聯盟鏈上，分別將證書寫到國網中心以及各個相關機關的各個節點上，畢竟區塊鏈的運作方式就是製作數位檔案的副本，並將副本備份到各自獨立的節點(機關)上，並透過區塊鏈的共識機制就可以確保不同節點所保存的數位檔案副本都是相同的，這樣的去中心化的儲存方式可省下備份的工作又達到驗證的效果，亦可避免駭客只要駭入 WebHR 系統就會被改寫資訊的資安問題。

至於承辦人員及資訊人員是否需要學習區塊鏈的技術嗎?其實一點都不用，前端的使用者介面跟其他一般的公務應用系統相同，區塊鏈的技術只會在系統的後端去串聯及進行備份的運作。這個區塊鏈應用改變了政府過往習慣以中心化系統作業方式，但以目前的狀況是解決了紙本浪費這個大問題，但是仍還未解決跨機關協作的問題，若同仁要使用數位證書向民間機關申請任何許可時，這樣的數位證書可能還是得回到原始的紙本狀態，使用正式的官方用印才能夠。若是要透過區塊鏈來進行驗證也是可以，就是民間機關把公務人員所提供的數位證書檔案中的 Hash 值，與國網中心所建立的聯盟鏈中該證書的 hash 值進行驗證即可知道真偽。

未來，人事總處有提到會將電子化及區塊鏈技術逐步拓展應用到公務人員的在職證明、離職證明等文件上，依照數量來依序導入。而我想，我會更期待未來能再各個民生上面看到更多的區塊鏈應用導入，例如交通、醫療等，並透過區塊鏈技術的導入並非只是解決數位化的問題，而是透過區塊鏈的技術，能夠進行跨領域、跨機關、跨國界的資訊交流、分享及使用，讓資訊的交流是能夠彼此流通且更有安全保障的。

四、 醫療病例與區塊鏈

假如你現在到醫院，大概已經不會看到醫師在使用紙本紀錄病歷，因為現在應該有 99%的醫師應該都是使用電腦來輸入電子病歷，除了少數沒有參與健保的醫院，否則只要是健保的醫院都必須使用電子病歷。

衛服部過去十幾年來已經積極地推動電子病歷交換中心的建置，讓跨院、跨診所之間的電子病歷能夠交換，打破了醫療機構之間的資訊傳遞障礙，其實這樣的情況與銀行體系相當雷同，銀行也是存在著跨行業務運作的問題，跨行轉帳相當要求即時性及精準性，所以由財政部邀集業者成立了財金公司，因此目前銀行及民眾才能如此便利的相互轉帳及帳務結算系統。

但是，醫院雖然電子病歷可以相互調閱，但是並非每位醫師都需

要調閱病歷才能進行診斷，再加上醫師對於其他的醫師診斷也不見得會參考，所以對於目前現行的電子病歷交換發展，也沒有在積極關注推動。

現在其實存在著一個醫療資源浪費的問題，我想衛服部及民眾都清楚這個問題的存在，但是要解決就必須靠衛服部積極地推動數位化及區塊鏈技術的導入，以及相關醫療法規的調整，例如一直有個問題困擾著我，就是之前為了植牙跟矯正的問題，我想多聽看看幾間牙醫師的建議，但是每到一間新的牙醫診所，我就必須重複照 X 光，若是有其他疾病，甚至需要重複抽血，而會有這樣的資源浪費，是因為現在有全民健保，民眾不用花費做 X 光及抽血，醫師或許也覺得這樣做法可以對醫院來說增加一定的收入，所以也就不會有反對的意見。但是對於民眾來說，重複照 X 光會對身體有一定的傷害，若是未來能將在醫院所做的電子病歷資料(包含血液檢查資訊、X 光檢查影像)，授權不同的醫療機關使用，就可以避免掉醫療資源的浪費。

為此，衛服部目前正在推動跨機構的「照護資訊整合平台」，這個平台架構了一個私有區塊鏈的分散式儲存架構，在每個醫療機構都架構一個 Gateway 用來存取機構內外的醫療資訊，每個 Gateway 在區塊鏈系統中都扮演著網路節點的角色。由於是屬於私有區塊鏈的架構，所以要加入鏈必須有著會員資格上的限制，以確保整個私有鏈的運作及資料安全，更採用共識速度較快的權益證明(Proof-of-Authority, PoA)，讓節點中的各個節點輪流定時產生區塊。

而這個平台為何一定要使用區塊鏈技術呢？主要是因為線上授權的機制設計，讓民眾在這個平台可以進行實名制註冊，透過平台中的區塊鏈所設計的智慧合約，讓民眾可以不受到地域、時間的限制，可以授權給醫療機構和醫護人員調閱醫療資訊，同樣的也可以在智慧合約中修改條約內容及設定終止條件。

另外一個重要的因素是常常在醫療機構的使用的紙本同意書也希望能夠數位化，但以往的同意書都是紙本，也必須要家人親屬才能簽署，若家人需要時間才能趕至醫療機構，往往就會錯過最佳的治療

時間，因此，同意書數位化之後的資訊安全就顯得相當重要，為了避免兩造雙方的醫療糾紛，數位化同意書必須要導入區塊鏈的技術，先在數位同意書上，透過數位簽名或自然人憑證加入數位憑證，然後再把所有的資訊保存到區塊鏈上，讓民眾跟醫療機構能夠安心地使用數位同意書所帶來的便利。

肆、 研究建議

一、 民生區塊鏈應用的落地

基於科技來自於人性這句話，過去大家都使用紙本進行任何的行政商業作業，而在這個作業最大的問題來自於地域上的限制，一封信件、一份公文從台灣寄送到美國必須飄洋過海數日才會到達，然後在目前任何東西都數位化後，克服了這樣的地理限制，因此各國無不推動數位化、智慧化政府。但在數位化的普遍後，仍存在著一個問題，就是跨機構、跨單位、甚至是跨國的協作問題，單位機構之間彼此數位資料的格式並不一致，對於數位資料信任度的定義不同，造成雖然已經數位化，但仍必須有許多紙本或人工的作業程序，以及各機構反覆身分認證、資安認證的複雜程序。直到區塊鏈的技術出現後，這樣的問題才有被解決的機會，而區塊鏈的專家們也朝著去中心化的目標在持續研發技術。

我想在不久的將來有個區塊鏈的應用就會被實現，而且是最貼近我們生活周遭的一個例子，就是現在大家手機裡面的各個 app，每個銀行、商店、政府單位等應用都有屬於各自的 app 應用程式，而這些 app 裡面的資料彼此並不能流通，各家的交通票(飛機、高鐵、台鐵)、會員卡以及各場活動、景點的門票都存在各自的 app 裡面，而且每個 app 也都需要各自的身分認證，要記一堆的帳號密碼，這些問題困擾著你我，因此也就是區塊鏈技術的切入點，倘若所有的資料都能集中到同一個空白 app，讓有需要的應用 plug in 進來，這樣是不是就會比較方便了，也可以達到去中心化的目標。而這個想法其實國際各大廠商都已經嗅到並且著手在布局，為的就是搶食這塊大餅，如 Facebook、阿里巴巴等大廠，都在建構屬於自己的區塊鏈貨幣，並拉

攏整個生態系的產業鏈，讓以他們所開發出來的 app 錢包，可以串聯整個龐大的商業物流。

二、 科技部的區塊鏈應用

有了其他部會機關推動區塊鏈的經驗及成效，本部可以效仿其他部會以此為借鏡，對於區塊鏈導入到部內的業務推動應可更加積極。其實，部內大多數的業務其實都已經屬於線上申辦業務，且本部並不像其他部會業務需要與民眾直接面對面接觸，設有臨櫃服務的機制，大部分業務都是採用無紙的作業方式進行，但本研究仍有兩個方向的業務建議希望藉由導入區塊鏈技術來推動無紙化的作業方式。

1. 本部每年年底在大批專題計畫申請時，全國大專院校的研發處都必須要造冊將申請計畫的主持人資料，及學校用印資訊印出紙本造冊通知本部進行收件，每年本部大批專題計畫的申請件數約 2 萬件，每件計畫至少必須印 2~3 張的紙本，所以每年的大批專題計畫就必須耗費 4~6 萬張的紙本，若再算上各執行機構郵寄到本部的郵寄費用，所耗費的資源就相當可觀。倘若本部能夠設計一套系統讓各個機構以電子文件上傳到本部系統，並將資料加上區塊鏈，本部承辦人、校方研發處窗口，甚至是計畫主持人都可以上線了解送件的進度情況，這樣一來每年可以減少上萬張來自各機構的送件紙本，以及省去各機構郵寄紙本的成本耗費，同時也可以讓以往需耗費 3~5 天的郵寄時間，瞬間只要半天之內彼此就可以確認收送件的狀況，縮短了整個專題計畫送件的流程，可以為計畫主持人爭取多一些的計畫撰寫時間，也可以讓部內縮短專題計畫的處理時程，達到多方共贏的優勢，可以每年為國家省下 2~3 百萬的業務成本。

2. 每年大批專題計畫的結果發函通知，都是科技部紙本寄送最大宗的時候，若採用上述同樣的技術，本部在通知各機關及各計畫主持人時，只要發 email 通知各機關研發處窗口及計畫主持人審查結果，設計一套系統可以讓機關窗口進行該機關的計畫審查核定查詢，而其中的函文資料都存放在科技部，但機關窗

口可以進行下載;同樣的,計畫主持人在收到電子通知信件後,可以到個人研究人才網上進行計畫的核定通知,在申請計畫的系統頁面,就可以知道計畫的通過與否,並可以下載本部的函文資料及核定清單資訊,如此一來,就可以大大的減少紙本的耗費及傳遞訊息所消耗的時間,以過去的經驗來看,從核定通過到計畫主持人收到核定結果,往往都需要 1~2 週的時間,畢竟部內綜規司的每個承辦人要負責的學校業務也是相當龐大。但是,這樣線上化的資料為了資安上的考量,都必須導入區塊鏈的技術,避免遭到有心人士的篡改及變造。

3. 若未來系統化及區塊鏈的技術能夠導入本部的各項申辦業務系統,將能擴展到相關的其他系統,例如國合系統、科發基金系統、產學業務系統等等。

三、 區塊鏈應用在電子發票

我們公務人員在出差時,總必須將交通、住宿的紙本收據謹慎收好,這樣回來的時候才能有收據可以報銷,雖然現在的報帳機制已經開放線上訂房網站所開立的訂房憑證也可以做為報銷的依據,明年更放寬規定,出差時的交通收據,只要是當日往返或使用經費結報系統報支者,就可以不用檢據票根,包含搭乘高鐵、飛機。

但是現在市面上正在流通的電子發票仍有很大的比例是使用紙本,雖然財政部所推動的電子發票整合平台可以將發票儲存在雲端或載具,但是不論是商家、公司行號、政府機構還是民眾必須先到系統上註冊,操作相當複雜,導致公司行號還是習慣將紙本印出來作業。如果說,未來不論是電子發票或收據都能夠數位化並存放在手機的單一形式錢包中,政府只要制定好統一個規格,透過區塊鏈的技術建立一套電子發票的防偽機制,讓商家、公司行號及政府的任何單據都可以上區塊鏈,這樣大家就可以使用 app 來做報帳的動作。

使用區塊鏈技術的電子發票就向在大家認可的文件上簽名或用印,具有共識且不可竄改的效力。同時,每個與發票相關的關係人,都可以藉由系統去追溯發票的來源、狀況等資訊,這樣的資訊透明化、

可交流性及跨單位跨時間便利性，可降低整個電子發票的耗費成本，並在發票轉遞過程中簡化流程，且資料完整保存，及遏制浮報虛報、一票多報等問題。最後，所收集到的大數據資料，也可以作為商業分析之使用。

目前推動區塊鏈化電子發票最積極的是中國，由於幾乎所有的中國人或去到中國的外國人都使用微信支付，甚至可以說只要中國人到的地方，都可以找到微信支付的影子，所以中國為了掌握整個金流的方向，早在去年就已經在深圳推動了區塊鏈電子發票，光一個省份一年內就開出 600 萬張的區塊鏈電子發票，未來更將試辦的經驗拓展至全國，以達到發票全國無紙化，並且同時也對於稅務的準確性大大的提高。區塊鏈電子發票的技術並非困難，只是各部會需配合做業務的調整及法規的修正，希望未來能夠看到部會推動上能再多一點力道。

四、 未來展望

本研究過程中，區塊鏈的技術仍然在不斷地進展，老實說，以目前區塊鏈的技術發展階段，仍有很大的發展空間，技術成熟度仍然不足，本人未來將持續對此業務技術進行研究與應用探討，對於技術的發展、各部會的應用狀況及本部可以導入區塊鏈的業務空間等進行分析，提出相關行政研究計畫，期望亦可供各科技機關作為區塊鏈技術應用及對區塊鏈有熱情的人士之參考。

伍、 參考資料

〔1〕https://bitcoin.org/bitcoin.pdf

〔2〕https://zh.wikipedia.org/zh-tw/%E5%8C%BA%E5%9D%97%E9%93%BE

〔3〕https://www.mile.cloud/zh-hant/what-is-blockchain/

〔4〕https://www.bnext.com.tw/article/49047/blockchain-tech

〔5〕https://anders.com/blockchain/

〔6〕https://bitnodes.earn.com/

〔7〕https://www.cbc.gov.tw/public/Attachment/91171155471.pdf