國網中心區塊鏈創新應用服務

葉羅堯　國家實驗研究院國家高速網路與計算中心副研究員

壹、前言

從 2009 年比特幣的第一個區塊被產出一直到 2015 年以太坊公鏈正式啟動，區塊鏈的各項應用正在快速發展中，不僅僅是虛擬貨幣的熱潮，更可預期區塊鏈技術在未來將在各種服務上（例如：身分認證、文件公證、電子投票等）都會與我們的生活息息相關，故國家實驗研究院國家高速網路與計算中心（簡稱國網中心）於 2016 年底設立區塊鏈技術團隊，由筆者帶領此團隊，其具有資訊安全與密碼學相關研究背景，目標是整合國網中心既有的計算資源與網路服務，協助國內政府、學術或民間單位發展區塊鏈各項應用。

國網中心於 1991 年成立，目前有新竹、臺中、臺南三大分部，擁有高速計算、大資料與 AI 分析主機，國家級高效能三地異地備援，並擁有最先進的學術網路 TWAREN，使用 100 Gbps 光纖網路骨幹連結臺北、新竹、臺中以及臺南四個主節點並有網路營運中心（NOC）24 小時值班人員可立即處理各項問題（如圖 1）。在資安方面已有資訊安全管理系統國際認證 ISO 27001:2013、雲端安全國際認證 CSA STAR Level 2 金牌，個資管理系統國際認證 BS 10012，且擁有全天候資訊安全維運中心（SOC），這些都是國網中心發展區塊鏈上擁有的獨特優勢。

圖 1　國網中心網路架構與資訊安全監控中心

資料來源：本研究整理

貳、區塊鏈簡介與特色

區塊鏈（Blockchain）是由比特幣所發展出來的一種技術，有不可竄改性、去中心化等特徵，也可其稱為分散式帳本，也就是大家共同維護同一份帳本，不過因為沒有一個中心化的管理者，為了確保帳本上的資料正確不被竄改，將每個區塊使用雜湊值串聯起來，後一個區塊須包含前面區塊的訊息，因此若要有人想竄改其中任一區塊的資料勢必破壞其中的關連性，如圖 2 所示，因此想要竄改資料變得極為困難。另一個問題是，由誰來添加新區塊，這個問題就牽涉到共識機制，常見共識機制大致如下：

一、PoW（Proof of Work）：也就是俗稱的挖礦，透過猜測隨機數（nonce）來搶得產生新塊的機會，是一種算力的比拚，去中心化最徹底的方式，可靠安全。不過較耗費能源，常見的比特幣、以太幣目前都是採用這種方法。

二、PoS（Proof of Stake）：類似於股權分紅制度，持有的貨幣越多就有越高的機率贏得添加新塊的機會，不必耗費大量算力，但容易造成分配不均，大者恆大。

三、DPoS（Delegated Proof-of-Stake）：類似 POS，只是持有大量貨幣者不自行出塊，而是透過類似董事會的方式投票選出出塊代表。

四、PoA（Proof of Authority）：直接決定誰有權添加新區塊，不必耗費大量算力，可縮短出塊時間，但容易使系統趨於中心化，為了避免出塊節點作惡，需有機制可以剃除作惡的出塊節點。

而區塊鏈依照開放程度可分為三大類型：

一、公有鏈（Public Blockchain）：完全開放，人人都可訪問、參與交易，比特幣與以太幣都是公有鏈。其優點是具公信力、去中心化程度高、安全性高；缺點則是鏈上資料完全公開、執行成本高、效率可能不佳、無法針對自己的需求做調整。

二、私有鏈（Private Blockchain）：個人或公司自己私有，不對外開放，如公司內部自行架設屬於內部的區塊鏈，只有公司員工可以加入。其優點是資料保密性佳、執行成本低、可控制程度高；缺點則是無法去中心化、安全性較差。

三、聯盟鏈（Consortium Blockchain）：對特定族群開放，跨組織形成聯盟，如數家銀行可形成自有的聯盟鏈（如：R3 Corda），在鏈上共享資訊或執行交易，其優點是有一定去中心化程度、適合跨組織、成本低；缺點則是可能存在惡意成員，節點數量不足容易影響安全性。

以上簡單介紹共識機制並比較開放程度，服務開發者可以根據應用的需求選擇開放條件與共識機制，然而任何選擇都有其優缺點，主要還是依照使用的情境去決定。在一般開發上，若

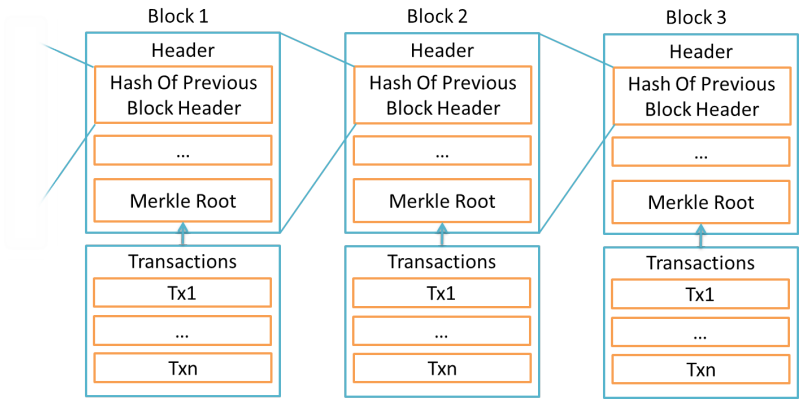

圖 2 區塊（Block）與鏈（Chain）概念圖

資料來源：本研究整理

是直接在公有鏈上佈署和執行智能合約（Smart contract）通常需要支付高額成本，另外也不能自行決定區塊鏈共識機制、出塊時間、無法控制成員等缺點，因此大部分應用主要還是以聯盟鏈為主，故節點的數量與安全性變得重要許多，且若負責出塊的節點（Miner）被入侵或決定作惡，需有其他具有出塊權限的節點剝除作惡節點的出塊權限，因此維持一定數量的公正出塊節點是必須的。針對此議題，國網中心將區塊鏈出塊節點建置於北、中、南三地，提高可用性與安全性，並且將其節點納入「NOC、SOC」中，享有即時流量監控、定期弱點掃描等防護。

近來區塊鏈的應用已經從單純加密貨幣進展到去中心化應用程式 DApp（Decentralized Application），主因在於智能合約的引入，程式設計師可以撰寫所需的智能合約部署到鏈上來實現自己的 DApp。DApp 具有區塊鏈的特性，如資料不可竄改性、去中心化、為雙方提供可信任的機制等，是一種突破性發展，尤其是在跨組織間需要建立信任機制時，區塊鏈就能提供非常好的工具，此時不須信任人或任何組織，僅需信任此機制，且可完全公開透明以供檢視，在各行業領域幾乎都能派上用場。比如雙方將打賭球賽這件事寫成智能合約佈署到區塊鏈上，並各自把自己的押注寫入鏈上，智能合約可自動根據球賽結果判定雙方的獎金。然而當球賽結果出來時，仍需要可信任的第三方將球賽結果寫入智能合約，智能合約才能得知比賽結果。也就是說智能合約是獨立存在於區塊鏈環境中，並無法自由地與真實世界溝通，需有公正可信任的第三方來將結果寫入智能合約，這個公正可信任的第三方一般稱為 Oracle，可以透過智能合約向 Oracle 下 Query 來取得所需資訊，可取得的資訊包含 URL、隨機數、數學運算等，也可在智能合約間溝通。當區塊鏈的應用越來越普遍時，需經常與外界取得資訊，屆時 Oracle 服務會變得非常重要。

另外區塊鏈也不適合儲存檔案，像早期比特

幣限制了每個區塊大小為 1MB，並且為了增加其區塊交易數則利用「隔離見證」（Segregated Witness）來擴充；以太坊雖沒有明顯的限制，但 Gas Limit 間接的限制了區塊大小，因此若要在區塊上儲存檔案，勢必需要仰賴其他資源，常見可用的資源有以太坊 swarm 和 IPFS，兩者皆是分散式檔案儲存系統，由於社群目前以 IPFS 為主流，故這邊將針對 IPFS 做介紹，IPFS 全稱 InterPlanetary File System，目的是為了解決目前網際網路中心化的問題，它是一個 P2P 的分佈式檔案系統，將檔案上傳到 IPFS 上可得到一個根據內容所計算出的雜湊值，這個雜湊值就是這個檔案的 Address，因此同樣內容的檔案上傳會得到同樣的 Address，在此系統上的任何節點都可以透過 Address 讀取此檔案，其去中心化的理念與區塊鏈精神相符，IPFS 應用在 DApp 上是非常合適的，不過因為存放 IPFS 上的檔案，任何人都可以訪問，敏感檔案在上傳到 IPFS 之前應都做防護才可。

參、國網中心區塊鏈服務項目規劃

目前國網規劃出四大服務項目，如圖 3 所示，分別為：智慧合約應用服務、節點建置維運服務、雲端儲存加密服務、資料介接安全服務。

一、智慧合約應用服務

本團隊已有區塊鏈證書查核系統正式開發的經驗，因此在系統建構、流程規劃已算熟悉，也了解到系統安全為必要考量，故往往會提供創新安全設計，不論是智能合約客製化或是區塊鏈系統建置都能提供具有質量的服務。目前不僅限於以太坊智能合約，其他常見的如 Hyperledger Fabric、Indy 也已經有相關應用正在建置中，在未來國網中心也會持續提供各式 DApp 客製化服務，目前主要以政府、學研單位 PoC 系統為主要業務核心，期待協助國家推動區塊鏈各式便民應用。

二、節點建置維運服務

節點數量是區塊鏈安全基礎之一，若節點的數量不足或安全性不佳都會對整個區塊鏈平臺帶來風險，而國網中心除了具有北、中、南分部可以建置若干節點外，節點間更有 100 Gbps 光網路骨幹聯繫，保證整個分散式系統的溝通與同步，資安方面亦取得各項認證，並有 SOC 與 NOC 運作來保障節點的安全性。由於國網本身的網路、資安監控設備早已建置非常完善，在建置節點與安全維運在國內具有無法取代的優勢，故非常適合協助各產業節點維運，提高第三方節點數量達到去中心化。

三、雲端儲存加密服務

通常 DApp 運作需要有一個分散式儲存系統，並且需有加密服務，國網中心在證書驗證系統已經有整合 IPFS 的經驗，並且考量到安全性，所有上傳的檔案都先經過 AES 加密，即使有人取得檔案也無法得知檔案的內容。IPFS 的運作同樣需要多個節點運作來維持穩定與效率，並且國網中心區塊鏈團隊也依業務需求獨創研發出可具監控功能之可撤銷式 IPFS，目前正申

請專利中，並且國網中心維運國家級 AI 運算設備，因此儲存空間優勢，也是國內首屈一指的。

四、資料介接安全服務

最後一塊拼圖也就是 Oracle 服務，隨著區塊鏈應用越來越普遍，Oracle 服務的需求會持續增加，這項服務是國網中心區塊鏈實驗室正在建構中的服務之一，將以「Intel SGX」此類硬體安全模組設備為基礎核心進行建置。未來可應用許多重要場域，例如人事局公告、司法公證資料、保險理賠、公益彩券等，都需要有公正單位將真實世界的資料添加到區塊鏈裡，不過目前國內並無這類相關服務，且一般民間單位也不一定適合扮演這樣的角色，由於是國網中心屬於政府單位的財團法人，不以營利為目標，因此非常適合扮演這樣的第三方公正者角色。

肆、智慧合約應用服務案例

今年 6 月與臺中市政府合作的區塊鏈畢業證書系統正式運作，是國內第一批採用區塊鏈正式發行官方試行版畢業證書的單位，如圖 4、圖 5 所示，本系統以太坊配合 IPFS 建構，可使用 QRCode 供驗證者快速驗證。第二版更加入具獨創性之限時驗證和撤銷功能，限時驗證讓驗證單位必須拿到臨時性密碼並在限定時間內完成驗證；而撤銷功能是保證使用者的檔案可以從系統上被刪除，這兩項功能都是為了保護使用者的隱私性。

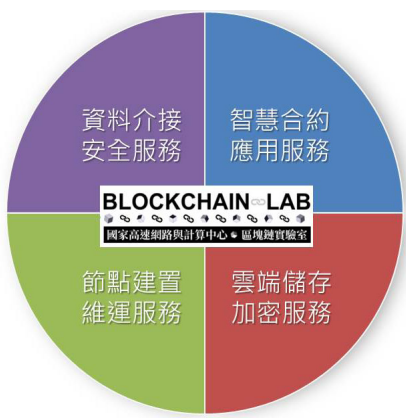

圖 3　國網中心區塊鏈實驗室服務項目

資料來源：本研究整理

伍、未來願景

由於區塊鏈技術目前能在快速發展中，許多機制與協議不斷更新，未來的區塊鏈究竟是以怎樣的方式與我們的生活結合仍然存在許多可能性，可以確定的是區塊鏈提供了一個突破性的技術讓以往中心化且須建構在信任之上的互動多了一種選擇。而國網中心基於既有的完善建設上發展這個跨時代的應用與服務，目標是協助國內的區塊鏈應用能更快的普及化，不論是政府、學研單位、甚至民間企業都是我們國網中心服務對象，期待能將國網優勢充分發揮讓社會大眾、中小企業了解，擁抱這個創世紀、革命性的新科技。

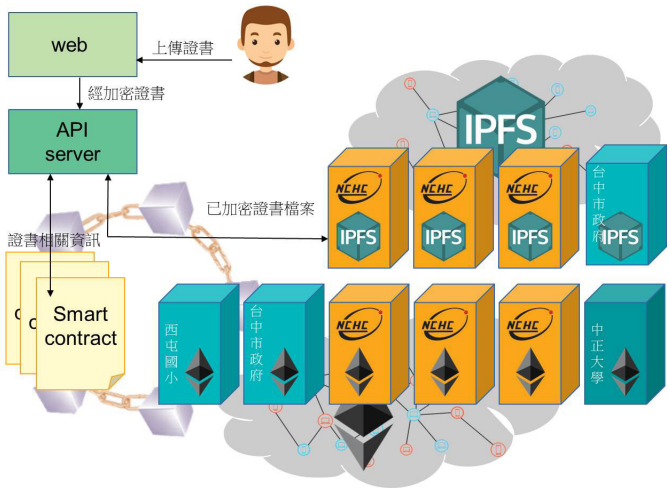

圖 4 臺中市國小畢業證書區塊鏈查核系統架構

資料來源：本研究整理

圖 5 臺中市國小畢業證書查核系統介面

資料來源：本研究整理

參考文獻

1. Bitcoin Wiki <https://en.bitcoin.it/wiki/Genesis_block> (accessed 2 Oct. 2018)
2. Ethereum Documentation <http://www.ethdocs.org/en/latest/introduction/the-homestead-release.html#milestones-of-the-ethereum-development-roadmap> (accessed 2 Oct. 2018)
3. Oraclize Documentation <http://docs.oraclize.it/#data-sources> (accessed 2 Oct. 2018)
4. IPFS Documentation <https://docs.ipfs.io/guides/concepts/hashes> (accessed 2 Oct. 2018)