國立東華大學資訊管理碩士學位學程

碩士論文

指導教授: 葉國暉 博士

適用於區塊鏈架構的輕量化區塊驗證流程：以智慧合約為例

A Lightweight Block Verification Process for Blockchain Architecture: A Case Study of Smart Contract

研究生：莊昀庭 撰

中華民國一零七年六月


國立東華大學
NATIONAL DONG HWA UNIVERSITY

學位考試委員會審定書

Certificate of Approval of Examination Committee

國立東華大學 資訊管理碩士學位學程碩士班

研究生 莊昀庭 君所提之 論文

National Dong Hwa University

The Thesis Graduate Student Proposed

(題目) 適用於區塊鏈架構的輕量化區塊驗證流程：以智慧合約為例

Title

經本委員會審查並舉行口試，認為符合 碩士 學位標準。

After evaluation and the oral examination by the committee members, the student complies with the master degree

學位考試委員會召集人 賴明豐 簽章

The Convener of Examination Committee

委 員 陳升忠 簽章

Committee Member

委 員 賴明豐 簽章

Committee Member

委 員 葉國暉 簽章

Committee Member

指導教授 葉國暉 簽章

Advising Professor

系主任 資訊管理碩士學位學程 主任 許芳銘 簽章

(所長)

The Director of Department

中華民國 107 年 6 月 11 日

ROC Year Month Date


國立東華大學
NATIONAL DONG HWA UNIVERSITY

致謝

一年很長也很短，現在回想起來這一年多的生活好像很充實但感覺過得太快，很感謝在這一段時間裡葉國暉老師給我很大幫助，包含論文指導和生活上的建議，並且都以鼓勵的方式讓我去做自己喜歡的事情，就算我放生論文出國溜達也沒責怪，只要我知道自己在做什麼，知道自己想要的是什麼就夠了，給予極大的自由讓我去控制時間，所以使我能在這不多不少的時間裡完成許多自己也從來沒預期過的事情。亦非常感謝系辦的佳芬姐和王大哥，不厭其煩的替我處理零碎瑣事，即使我常常拖沓或是不太靈光但也從不遷怒發脾氣，真的辛苦他們。還有一起窩在實驗的同學們，雖然大家都有各自的論文與生活，但是需要幫忙時都會伸出援手，然後一起把事情解決，工讀地方的老闆也常讓我在緊要關頭時放假回家趕報告，這真的是很大的幫助，最後還有感謝我的家人，在我煩躁暴躁的時候也容忍著，並常常關心我的身體狀況，該感謝的人真的太多了。

花蓮的天空很藍，綿延的山脈很青綠，東華的景致很美，還有學校裡很歡樂的人，原本以為碩士生活會枯燥沉乏，或是埋首故紙堆，但是出乎意料的有趣和豐富，在這裡遇見了陪我在家懶散的貓咪，指導我的老師們，處理生活大小事的助理，一起在實驗室趕論文的同學，還有意外認識的鄰居和老人家，一輩子同時有這麼多經驗的一年應該不多，我想會一直留著這份記憶，並且有機會就再回來花蓮敘敘舊。

最後再次感謝所有幫助過我的大家，希望每個人在未來的路上也能遇到這麼多友善包容的人，願每個人都能順遂平安，健康快樂。


國立東華大學
NATIONAL DONG HWA UNIVERSITY

適用於區塊鏈架構的輕量化區塊驗證流程：以智慧合約為例

國立東華大學資訊管理學系碩士學位學程

指導教授：葉國暉　博士

研究生：莊昀庭

摘要

近年來，隨著比特幣的出現與大量應用，加密貨幣成為熱門討論議題，而其核心之區塊鏈(Blockchain)技術也迅速被產業界所關注。區塊鏈技術具備去中心化、安全及公開透明等特性，現有應用大多為透過區塊鏈技術提升產業價值或是服務品質，其中以金融服務為目前區塊鏈技術最為頻繁的應用領域之一。現今區塊鏈應用大多透過以太坊(Ethereum)平台進行應用開發，然而，隨著使用者的大量增加，用戶端運算負擔將大量提升，進而影響系統營運效率。鑒於此，本研究提出一套輕量化區塊驗證流程，主要為在私有鏈的環境下，透過縮減區塊數量，並結合 RSA 環狀簽章和雜湊函數 SHA-256 等運算作為區塊鏈鏈結技術，讓使用戶端能降低運算負擔，提高系統營運效率。

關鍵詞：區塊鏈、智慧合約、驗證流程。


國立東華大學
NATIONAL DONG HWA UNIVERSITY

A Lightweight Block Verification Process for Blockchain Architecture: A Case Study of Smart Contract

Graduate Institute of Information Management,
National Dong Hwa University

Advisor: Kuo-Hui Yeh, PhD
Student: Yun-Ting Chuang

Abstract

The invention of Bitcoin and the booming application of Bitcoin in recent years, push cryptocurrency to its top. Blockchain, the core technology of Bitcoin, has picked up the attention of industry and rapidly adopted by firms. Nowadays, blockchain is adopted by most businesses for increasing their industry value and improving their service quality. Since blockchain has features of decentralization, secure and transparent, the technology mostly applied to financial firms. However, the increasing amount of users creates more blocks, which means the computing burden on clients. This issue can decrease performance and efficiency in firms or organization that adopted the technology or ran the system. Therefore, we proposed a lightweight block verification process in this research. By adopting private chain rather than public chain, the blocks can be reduced. With a private chain applied RSA ring signature and SHA-256 as linking technique, the computing burdens can be reduced and improve the operation efficiency.

Keyword: Blockchain, Smart Contract, Verify Process


國立東華大學
NATIONAL DONG HWA UNIVERSITY

目錄


國立東華大學
NATIONAL DONG HWA UNIVERSITY

圖目錄


國立東華大學
NATIONAL DONG HWA UNIVERSITY

表目錄


國立東華大學
NATIONAL DONG HWA UNIVERSITY

壹、 緒論

一、 研究背景與動機

處在資源豐富的時代下，網路服務與通訊技術的快速發展促使資訊應用更為創新進步並且連帶改變了社會的生活型態，其中金融科技也佔據重要的一環。在過往的金融交易中，銀行、證券、保險等許多類型的金融服務機構著實為關鍵位置，掌控著用戶的金流動向，但同時也代表多數人的交易必須被金融服務機構所控制，間接延伸出交易成本、交易風險或信任關係等問題，為解決此情況開始發展出許多新型態交易模式期望能改善傳統既定方法，而後也出現多種透過密碼學所產生的數位貨幣希望能部份取代現有貨幣，如第一個提出的去中心化機制的比特幣（bitcoin）便是其中最具革命性的代表。

比特幣起源於中本聰所發表的一篇論文，該篇論文提出以點對點（Peer-to-Peer）技術實現的電子現金系統。意即需要履行約定交易的雙方各自代表著一個端點，在交易過程中不經過第三方的處理，直接由端點和端點進行交易，如此便能省略交易成本以及和第三方的信任基礎，但是交易資料實屬隱私，其安全性至關重要，同時也必須證明交易的正當性，因此在此機制下的交易過程會被記錄在該篇論文所提出的關鍵技術「區塊鏈（blockchain）」上以作為交易證明亦可確保資料隱私與資料不被竄改。

區塊鏈(blockchain)在該篇論文所提出的概念為一個去中心化的分散式帳本，其中包含對等式網路（又稱點對點技術）、密碼學、數位簽章（Digital Signature）和時間戳伺服器（timestamp Server）等技術。在區塊鏈中會依據密碼學條件產生許多區塊（block），每一個區塊內會儲存許多交易資料，再利用雜湊函數（Hash Function）和時間戳記與上一個區塊形成鏈結，並在所有節點上儲存所有區塊使其形成分散式資料庫，同時因為所有節點皆擁有資料因此無法輕易竄改，進而使區塊鏈達到公開、分散且安全的目的。

公開、分散且安全的功能性引起許多產業的注意，希望能利用區塊鏈來節省維護成本或是提升工作效率亦或是創造更高的價值，首先嘗試採用的產業便是金融服務業，由於金融服務涉及重要的個人隱私資料與交易安全性，因此非常適合區塊鏈的特性，目前富邦金控、玉山銀行、中國信託...等等皆投入研究，國泰人壽也嘗試利用區塊鏈輔助理賠作業，更有新創公司 AMIS 成立了臺灣第一家商用區塊鏈平臺，當然不只有金融業看好前景，諸如：保險業、食品業、物流業以及醫療產業等等，各式各樣的行業都有業者決定投入研發，期望能透過新技術提升產業價值。

二、 研究目的與問題

區塊鏈在目前資訊技術領域裡還是一項尚未發展非常成熟完善的技術，仍有許多細節問題需待改善。以比特幣系統為例，現在的比特幣價值日益高升，使用者數目也快速成長，節點同時也會大幅增加，最明顯受其影響的便是驗證速度，即使在比特幣原先機制設定為當新區塊需要驗證時若總結點過多會省去舊有區塊並擷取部分最接近當前的區塊作驗證以節省驗證時間，但是還是必須有足夠的數量才能證明其安全性，也仍然以最完整或是最長的鏈作為判定標準，而最長或最完整的鏈也代表最多資料，需要耗費相對於單一主機過於大量的運算能力，因此導致在驗證過程中為了安全性犧牲區塊的驗證速度和儲存空間。

為解決上述所面臨的問題因此本研究提出了一個系統，此系統在同樣以區塊鏈技術為核心的以太坊（Ethereum）作為研究環境，但是由於以太鏈的主網路需要實際以太幣，考量經濟因素採用和以太鏈相仿機制的私有鏈做為研究環境並結合智慧合約（smart contract）和環狀簽章（ring signature）的技術使其他節點能在不降低系統安全性的條件下提高驗證效率。

因此本研究之目的為以下問題：在區塊鏈的環境下，如何透過結合智慧合約和環狀簽章等技術使其他節點在維持一定的安全標準下降低驗證所需的運算負擔，並提升其他節點的驗證速度？

三、 論文架構

本論文共分為五章。

第一章為緒論，主要說明研究背景、動機以及研究目的與問題，表達本研究所處的環境現況和引起研究之動機，並確立本篇論文接下來的研究目標。

第二章為文獻探討，介紹本研究中所需的背景知識和使用技術，了解研究中適合的方法，以利於接下來的研究過程順利執行。

第三章為研究架構，詳細闡述本篇論文的系統描述與目的、情境使用和研究方法，詳細解釋研究內容和研究過程。

第四章為效能分析，藉由圖表說明本研究之研究成果並且分析與原有系統與機制之間的效能差異。

第五章為結論，總結本研究的成果並且討論可能對該領域的影響和預期能貢獻的可能性。

貳、 文獻探討

一、 比特幣（Bitcoin）

2008 年中本聰（Satohi Nakamoto）所提出的論文《Bitcoin: A Peer-to-Peer Electronic Cash System》讓比特幣正式被公開。比特幣是一種點對點的電子現金系統[20]，作者提出一種去中心化的分散式分類帳本的技術稱為區塊鏈，比特幣本身則是基於密碼學原理產生的加密貨幣並且透過區塊鏈做交易，在區塊鏈中可以透過挖礦（Mining）獲得比特幣。挖礦的過程則是基於系統設定的條件，透過礦工（Miner）不斷的計算直到得出解答，此解答就是區塊鏈中的區塊，並且算出解答後必須發佈到公開網路告知其他所有的節點，通過工作量證明（proof-of-Work）後便會獲得獎勵，就是比特幣。

比特幣的總量約 2100 萬，因此挖礦難度會隨著礦產數量減少而提高，同時每大約 4 年挖礦的獎賞就會減半，在 2009 年發行貨幣後，開始每挖到一個礦能獲得 50 比特幣；在 2012 年 12 月 28 日第一次減半，之後每次的獎賞是 25 比特幣，最近一次的減半是在 2016 年 7 月 9 日，目前的獎賞金額是 12.5 比特幣，下一次的減半預計會在 2020 年，最終評估會在 2140 年將不再挖到礦。另外在比特幣系統中使用了工作量證明，在此機制下如果想要造成攻擊必須要擁有超過比特幣系統 51%的運算能力才有機會造成威脅，在目前的世界狀況還無法做到這一件事，因此比特幣還是一項安全的交易機制。

目前也出現許多和比特幣相關的探討，Ron 和 Shamir 曾提出關於比特幣的交易分析，作者透過大量的比特幣交易紀錄與統計分析解釋許多關於用戶行為的問題[3]，Reid 和 Harrigan 針對比特幣的匿名性分析，作者將拓樸結構與分析的額外資訊和技術結合調查盜竊比特幣的行為[4]，Barber 等人也深入分析關於比特幣成功的原因，確定問題和弱點並且提出適當的技術解決問題[12]，還有許多的學者分析比特幣的歷史資料作為研究目標。

比特幣的提出讓金融交易市場產生非常大的動盪，因為比特幣的核心概念是去中心化，去中化即交易帳本由所有的節點一起維護，因此不需要第三方或中介單位，這對於需要收手續費的單位來說必然影響很大，但是相對而言不收手續費的機制可以使許多小額交易更有機會達成，因此對於比特幣所帶來的衝擊不盡然是正面或是反面，也有許多的研究人員不僅關注比特幣，同時將眼光放得更遠，著手研究因應比特比同時出現的區塊鏈技術，或許會更具價值。

二、 區塊鏈（BlockChain）

區塊鏈是一項因應比特幣而被提出的一項技術，主要核心概念是去中心化、透明、安全的特性，在區塊鏈中是由許多區塊串連組成，每個區塊都儲存著資料和上一個區塊的雜湊值因此而串連起連形成一個鏈，以下是中本聰提出的論文基本概念流程描述，其變化過程以及演進可以由圖 1、圖 2、圖 3 和圖 4 和圖 5 解釋。

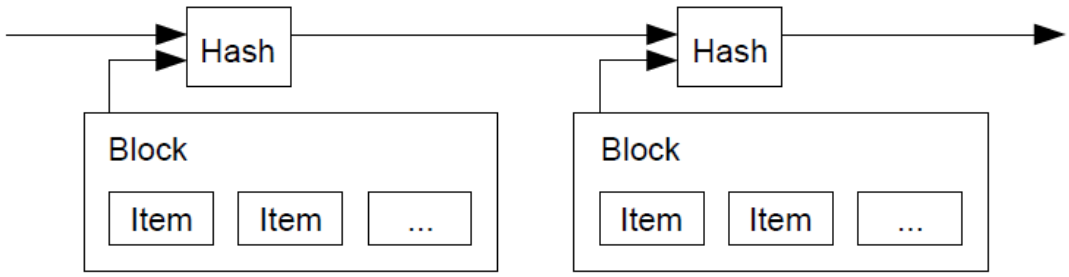

圖 1 區塊鏈第一步驟示意圖，本圖取自[18]

圖 1 說明了區塊鏈的第一步驟，先將許多交易資料放入區塊中並且作雜湊函數產生雜湊值。

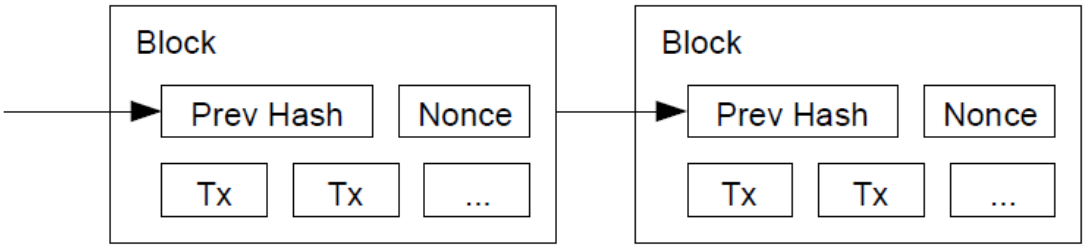

圖 2 區塊鏈第二步驟示意圖，本圖取自[18]

圖 2 說明每個區塊加入了前一個區塊的雜湊值，因此形成區塊鏈在一開始的概念，其中 Nonce 值是一個隨機數，用於計算雜湊值所使用的參數。

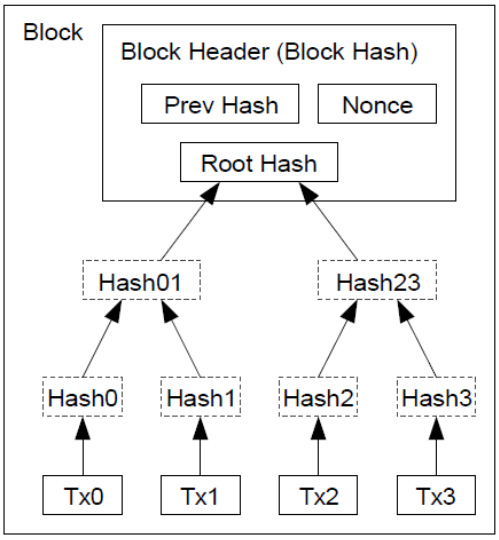

圖 3 縮減資料示意圖，本圖取自[18]

圖 3 說明了區塊鏈使用 Merkle Tree 將交易資料以樹狀方式產生出一個根，之後將根使用雜湊函數產生出 Root Hash，此時在區塊中會有一個稱為 Block Header 的區塊，每一個 Block Header 的資料長度為 80 Byte，裡面包含上一個區塊的雜湊值、Nonce 和一個 Root Hash。下一步圖 4 接著解釋區塊中如何將資料縮減減少空間。

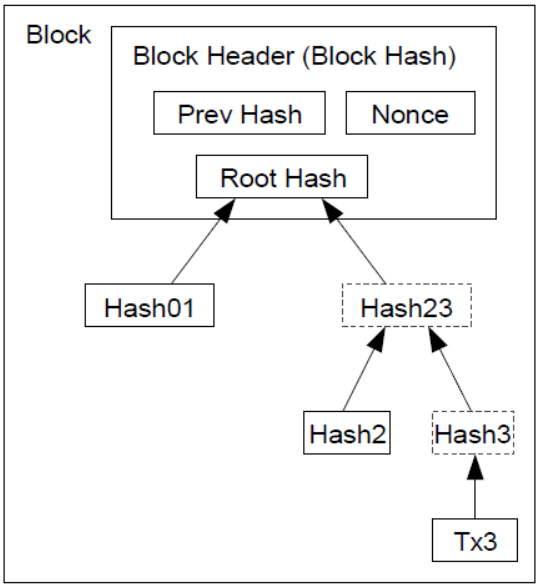

圖 4 區塊中刪除資料示意圖，本圖取自[18]

圖 4 說明了使用 Merkle Tree 將資料壓縮之後可以刪去部分資料，因此可以使每個區塊的資料量不要太大，因為所有節點都會儲存該資料，隨著時間累積的容量將會使資源負擔過大。最後區塊鏈的型態會呈現如圖 5 的架構。

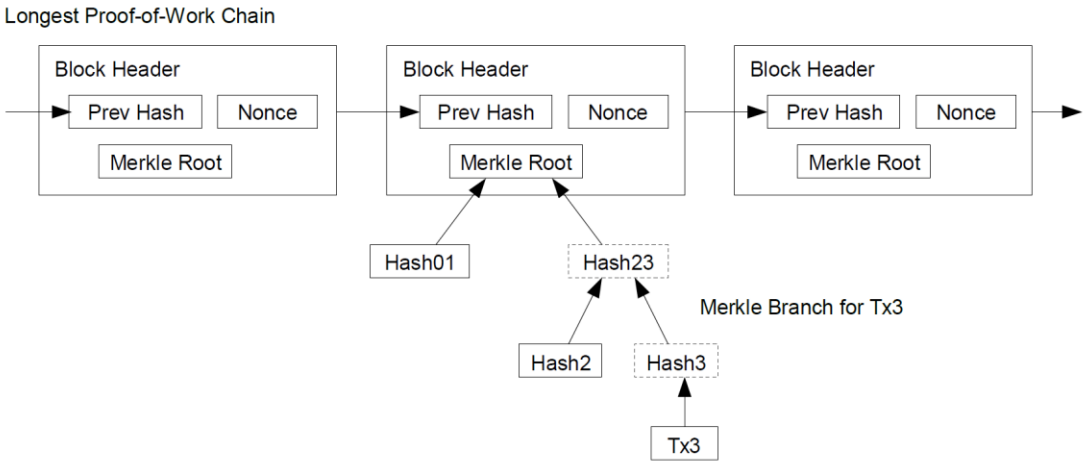

圖 5 區塊鏈架構，本圖取自[18]

雖然在區塊鏈的系統中已經縮減了資料量，但是比特幣累積至今已經有142GB，以太幣也有 45GB，都是個龐大的數字，因此本研究認為本系統可以著手改善此問題。

經由以上五個圖便可瞭解區塊鏈如何建立並且延續下去，且在區塊鏈中大量使用雜湊函數，雜湊函數是一種單向加密方式，非常容易驗證但是非常不容易透過碰撞產生相同答案，目前有許多的雜湊函數，在區塊鏈中使用的是 SHA-256，而驗證方法只需要將待驗證的資料同樣做一次加密得到一組雜湊值，之後只需比對兩個雜湊值，只要相同就能驗證成功，因此在區塊鏈也採用這樣的簡易卻有效的方法。

三、 以太坊（Ethereum）

比特幣是目前最大的區塊鏈平台之一，另一個就是以太坊。

以太坊最初由 Vitalik Buterin 在 2013 年提出，並寫下《以太坊白皮書》確立以太坊的概念，以太坊和比特幣最大的差別為，比特幣的所設計的智慧合約概念只適用於比特幣，但是 Buterin 認為應該要更具有靈活性並且能讓其他人自由開發，因此在以太坊有差別性的就是具有可自由開發的智慧合約（Smart Contract），智慧合約可以被解釋成一段程式碼，並且儲存在以太鏈上，透過付費機制創造交易的情況使智慧合約啟動運作，在合約中一切都是自動化，因此可以應用在許多方面，而本系統最後採用類似於以太坊機制的私鏈便是取其原因，能夠在區塊鏈中執行，使系統能更容易與區塊鏈整合。

雖然以太坊和比特幣有一部分不相似，但是同樣都有加密貨幣，以太幣（Ether）目前是市值第二高的加密貨幣，僅次於比特幣，兩者的相似之處還有同樣使用工作量證明，工作量證明雖然簡易並且能使所有節點都能參與，但是所有的節點都在做一樣的事情會造成大量資源被浪費，因此又發展出另一種共識機制稱為權益證明（Proof-of-Stake），相較於工作量證明，權益證明採用偽隨機的方式挑選驗證者，因此省略所有人同時挖礦的資源，能更節省運算資源，目前以太坊的開發人員正在積極研究如何將權益證明放在以太坊使用。

除此之外，研究以太坊的學者 Sovbetov 也對最常見的五種數位貨幣：比特幣、以太坊、達世幣（DASH）、萊特幣（Litcoin）和門羅幣（Monero）做分析比較，包含市場價格分析和交易量的起伏[16]；Hirai 則透過測試驗證智慧合約在以太坊虛擬機（EVM）執行的安全性，能夠作為以太坊和智慧合約的分析基礎[15]；Yuan 等人亦提出關於關於以太坊和智慧合約的應用「ShadowEth」，作者們設計了一套系統使私人智慧合約能夠在公開的區塊鏈中運行，並且確保使用者的隱私與安全性[11]，以太坊的發展日趨成熟完善，同時開發與應用也將會越來越多。

四、 智慧合約（Smart Contract）

智慧合約目前最為廣泛被應用的就是在區塊鏈上執行的程式，對於程式語言亦有多種可以使用與選擇，如：solidity、Javascript 等等。近年由於區塊鏈的發展因此智慧合約的應用也隨之而生，且不僅限於原始用於比特幣和以太坊等虛擬貨幣，更有許多方向的研究與探討，如以下舉出幾項例子說明。

2016 年 Yasin 與 Liu 的論文研究提出了一個關於網路身分和智慧合約的管理系統，他透過區塊鏈技術與智慧合約管理個人在網路上的身分[2]；2016 年由 Bogner 等人提出一個分散式應用程式(Decentralized Applications, DAPP)，透過基於以太坊的智慧合約的方式實行共享日常用品的共享經濟模式[1]；2017 年 McCorry 等人發表的論文中提到他們首次實現使用區塊鏈匿名但公開的特性進行投票，是第一個不需依賴第三方並且透過智慧合約的方式自動計算票數，同時能最大保護投票人的投票隱私[9]；2017 年由 Cha 等人發表的論文主要涉及物聯網(IoT)設備的安全性問題，因此作者等人提出了區塊鏈連接閘道器（BC 閘道器）的設計，能夠有效保護使用者資料的存取，其中依然透過智慧合約的方式在區塊鏈上執行[13]。

從上述幾個論文案例可知現今區塊鏈的發展應用在各個領域，智慧合約同時也有許多新的方向與應用。

五、 環狀簽章（Ring Signature）

數位簽章（Digital Signature）是一種透過密碼學技術來驗證身分的技術。而環狀簽章是利用數位簽章所產生的應用。

Ronald L. Rivest、Adi Shamir 和 Yael Tauman 在 2001 年提出一篇論文《How to Leak a Secret》當中提出了環狀簽章的概念並且實作 [10]，作者在論文中表示環狀簽章的簽署使當中任何一個成員不被揭示，但是和團體簽章不同，環狀簽章沒有管理者也不需要經過協調，任何人也都可以使用自己的私鑰一起簽屬而不會被發現，因此若有重要公共文件需要簽屬，簽屬人可以放心地使用環狀簽章而不必擔心被識別。

由於環狀簽章具有不可否認性並同時達到安全與匿名性的目的，許多研究開始延伸應用環狀簽章做為身分認證的基礎。Zhang 和 Kim 認為盲簽章與環狀簽章對於使用者的匿名與隱私非常有用，因此作者們首先提出基於環狀簽章與盲簽章的 ID 辨識方法，並且分析其效率與安全性[5]；亦有學者提出基於環狀簽章的新架構 ID 鑑別系統，且可證明不可偽造，適用於一般存取結構[14]；Herranz 和 Sáez 使用雙線性設計基於環狀簽章的身分辨別模型，並應用於不同的存取機制[6]；Au 等人提出一套系統稱為 CBRS（Certificate Based Ring Signature）遵循 Gentry 在 EuroCrypt 2003 中提出的 CBE（Certificate Based Encryption）思想，保留了 CBE 的優點，也繼承環狀簽章的匿名性特性，另外他們還提出 CBLRS（Certificate Based Linkable Ring Signature）為 CBRS 的變體，具有可鏈結性，可證明兩個簽章為同一人所簽屬但仍然保留該使用者的匿名性[8]。

環狀簽章的匿名特性與不可否認性促使許多關於身分鑑別的應用與深入研究，在此本研究也參考環狀簽章的特性作為研究核心，透過環狀簽章與其他技術的結合已達成研究目的。


國立東華大學
NATIONAL DONG HWA UNIVERSITY

參、 系統研究架構

一、 前言

此章節將詳細介紹本研究之系統描述、系統目的、情境設定和執行方式。

系統描述會說明此系統所使用的背景環境以及所需要的初始設定狀態，接下來會個別詳細說明本研究如何達到系統目的，並且利用情境設定來說明使用情況以及適用於何種狀況，最後會說明本系統的執行方式以達成系統目的。

二、 系統描述

由於目前廣泛使用的區塊鏈系統皆非常關注安全性問題，所以會透過謹慎的驗證來證明其正確性，謹慎的驗證即導致犧牲驗證速度，本研究將透過我們所提出的系統嘗試改善這項問題。目前在區塊鏈中實際執行的驗證方式是採用工作量證明（Proof-of-Work），此驗證方式會採用最長或是散播最廣的鏈作為標準，而最長的鏈也會包含最多的資料量，延伸出的問題便是區塊的儲存，所以我們也會在系統中同時解決此問題。

在本系統中的初始狀態會有一個被鎖定為目標的區塊鏈，以比特幣舉例而言：在區塊鏈中的每個 Block 會存有 Block Header 和交易資料，Block Header 內則分成三個部份，分別是上一個區塊的雜湊值、Nonce 值和 Root Hash，Root 的值為交易資料經過 Merkle Tree 的樹狀結構後所產生的根（Root），之後將 Root 放入雜湊函數算出一個雜湊值就稱之為 Root Hash，可以代表為所有交易資料的總結。而在比特幣系統中為了能較快速驗證所以只會驗證 Block Header；在以太坊目前也使用同樣方法，即只使用 Block Header 做驗證。透過上述解釋瞭解了每個區塊內儲存的資料，本系統亦延續只採用該區塊鏈的所有的 Block Header 作為系統初始狀態的設定並包含未來會產生的 Block Header，當系統皆收到設定值後接下來會使用環狀簽章技術，在環狀簽章中我們使用 RSA 演算法，因為在環狀簽章依據原始特定條件下 RSA 的使用上會更加有效率，系統將所得到的 Block Header

透過規則設定做環狀簽章，最後，系統會使接收到環狀簽章成為新區塊鏈中區塊所儲存資料，生成一個新的區塊鏈。

在此將先歸納系統中本研究設定的系統初始狀態設定項目，共有三項：

1. 鎖定為目標的區塊鏈。
2. 使用該區塊鏈中的區塊編號與所有 Block Header。
3. 使用環狀簽章：採取 RSA 數位簽章演算法。

三、 系統目的

此章節會提及系統如何達成前些章節敘述的研究目的：透過本系統能使其他節點在維持一定的安全標準下降低驗證所需的運算負擔，並提升其他節點的驗證速度。

在系統中，本研究選擇透過智慧合約執行系統，智慧合約為特定用於區塊鏈的一段「程式碼」是以太坊最核心的概念之一，以太坊使程式碼能被放在以太鏈上，透過付費機制啟動合約以執行合約內容，即執行區塊鏈上的程式碼。另外佈署在區塊鏈上的程式碼依然維持區塊鏈的特性因此無法竄改，並且維持去中心化的運作方式，而本系統採用智慧合約之原因為智慧合約和區塊鏈有密切關係，並且能將此系統發佈到各節點上，以本研究之觀點能將本系統讓各節點皆可自由使用。接下來系統中會使用環狀簽章，利用環狀簽章的概念將區塊鏈以固定區塊數量分段做數位簽章，最後再用與以太坊機制相似的測試用私有鏈來產生區塊，以此大幅減少區塊鏈數量。

於本論文的目的中，第一部分著重於驗證效能的提升，由於透過本系統在不降低安全性的條件下大量的減少了區塊數量，因此在驗證速度便能夠可加快，且系統內部機制使用 RSA 數位簽章也使資料具有不可否認性，亦可使用在回溯時驗證，驗證後資料依然為原始區塊鏈的資料，保持一定安全性，因此而達成本論文所提出的第一個目的。

第二部分的研究目的為希望能節省節點的儲存空間，原始區塊鏈在本系統中透過系統的處理將會大幅減少區塊數量，各節點透過本系統將可以儲存更少的區塊但是依然可驗證各個區塊，因此能使節點有效的減少儲存空間亦可降低節點的運算負擔，使資源更能創造新的價值。

四、 系統執行方式

系統執行方式在此章節主要區分為總體概念性的介紹和個別細節介紹。

以下說明的是系統的建立過程，圖 6 說明的是以私有鏈為初始設定狀態所建立的方式。

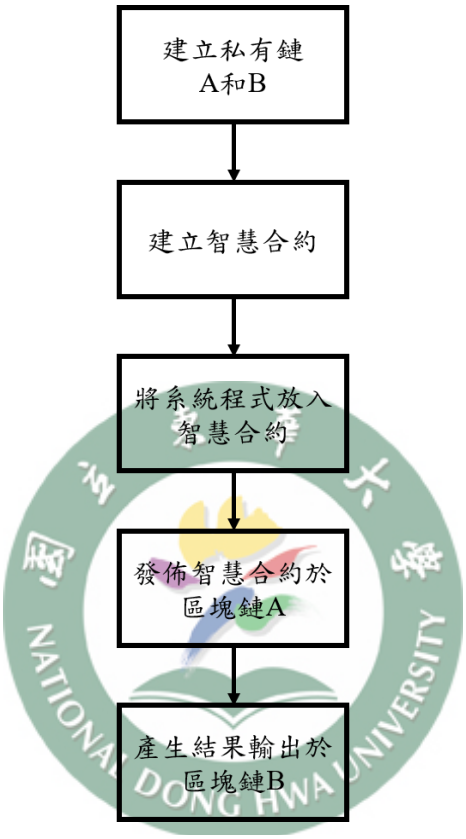

圖 6 系統建立流程圖

圖 6 第一步驟是透過建立兩個和以太坊相似機制的私有鏈來作為實驗對象，A 是目標區塊鏈，即會被系統獲取 Block header 的鏈，B 則是區塊鏈 A 透過系統處理後會儲存資料的區塊鏈。

第二步驟是建立智慧合約，智慧合約必須先創建出來之後才能發佈到區塊鏈上，因此在第二步驟先創建。

第三步驟是將系統程式碼放入區塊鏈中並且測試，此時智慧合約尚未發佈於區塊鏈，因為智慧合約一旦發佈後便不可更動，待測試系統完畢確認無狀況後會進入到第四步驟，將智慧合約發佈到區塊鏈 A，透過區塊鏈 A 的貨幣（在以太鏈

內實行則為以太幣）和智慧合約做交易促使智慧合約執行，最後便會將產生結果儲存在區塊鏈 B 的區塊上。

以上圖 6 主要解釋了本系統的主要流程，接下來由圖 7 解釋系統內部的處理流程。

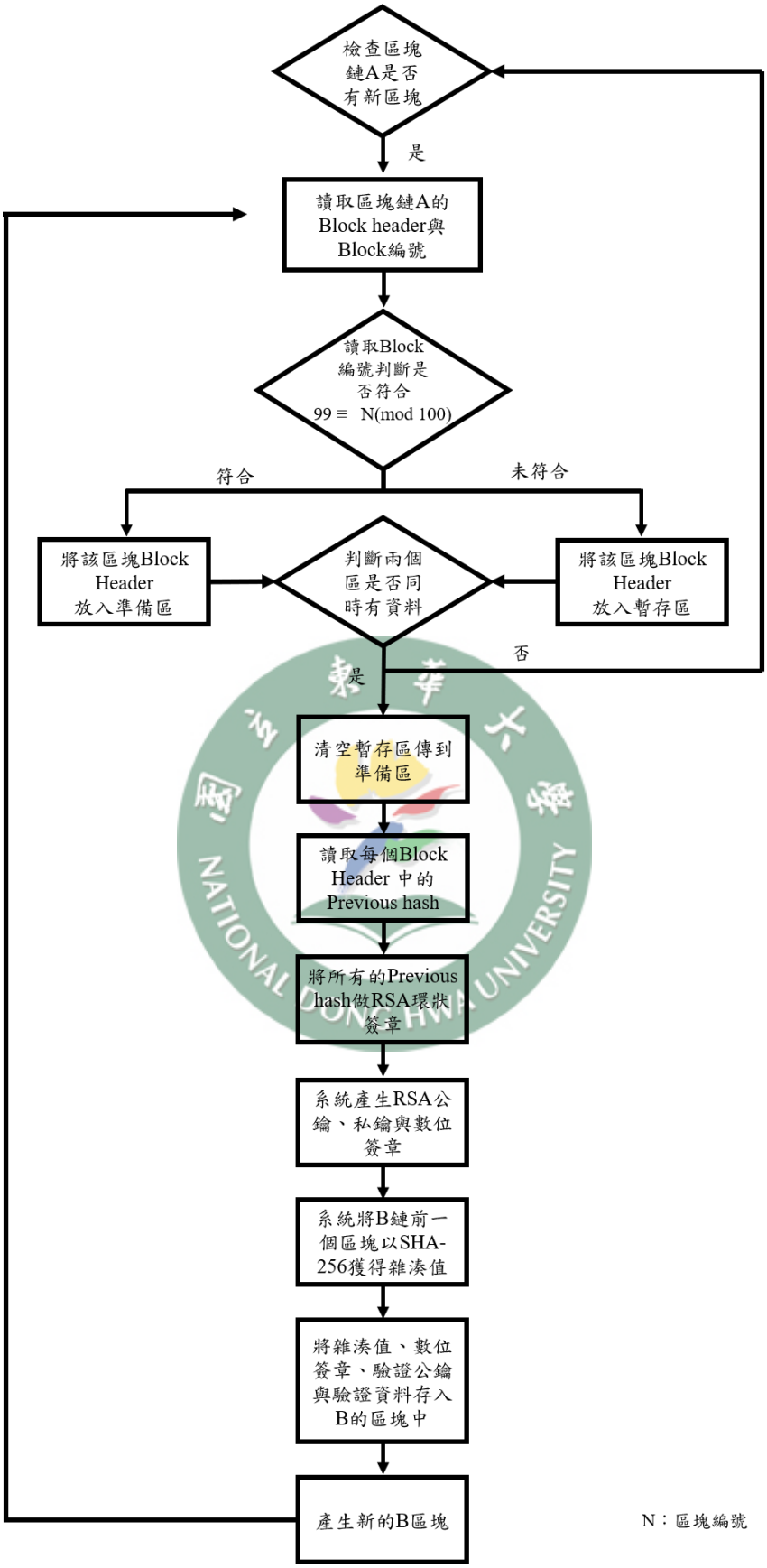
檢查區塊
鏈A是否
有新區塊
是
讀取區塊鏈A的
Block header與
Block編號
讀取Block
編號判斷是
否符合
99 ≡ N(mod 100)
符合
未符合
將該區塊Block
Header
放入準備區
判斷兩個
區是否同
時有資料
將該區塊Block
Header
放入暫存區
否
是
清空暫存區傳到
準備區
讀取每個Block
Header 中的
Previous hash
將所有的Previous
hash做RSA環狀
簽章
系統產生RSA公
鑰、私鑰與數位
簽章
系統將B鏈前一
個區塊以SHA-
256獲得雜湊值
將雜湊值、數位
簽章、驗證公鑰
與驗證資料存入
B的區塊中
產生新的B區塊
N：區塊編號

圖 7 系統流程圖

於系統中，第一步驟會先檢查並讀取區塊鏈 A 中的區塊編號 N 與 Block Header，由於需要藉由區塊編號確認區塊數量，確認讀取資料後系統會依據每 100 個區塊縮減一次，在本研究中，我們透過計算發現每 100 個區塊依次是最有效的縮減數量，因此在系統中藉由區塊編號判定該區塊是否為每 100 個區塊中的最後一個，若不符合即把該區塊的 Block Header 資料放入暫存區，若符合條件則將區塊資料放入準備區，如圖 8 所示。

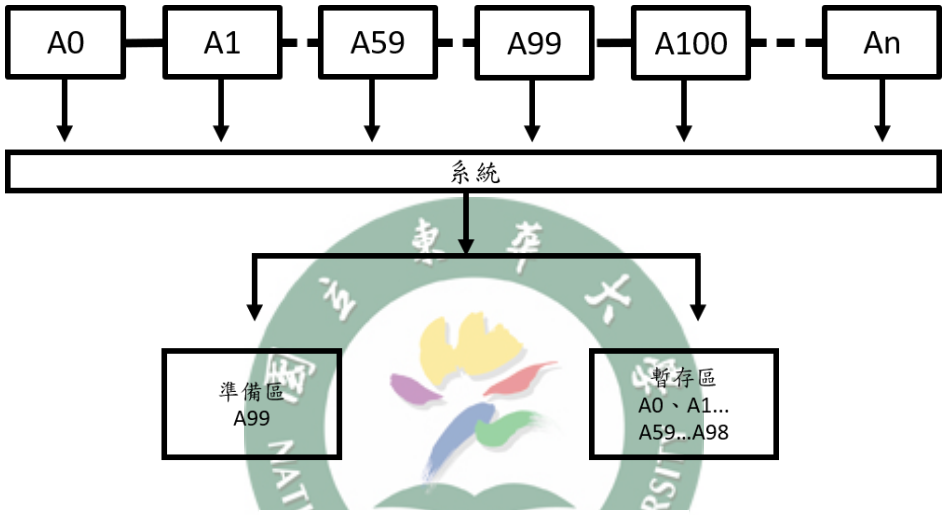

圖 8 系統分類範例

在系統中，每一次存取完一區塊即會檢查兩個區域是否同時存有資料，若同時存有資料表示已存有 100 個區塊的資料，系統會自動將暫存區的資料匯入準備區，並且進入後續流程，如圖 9 與圖 10 所示。

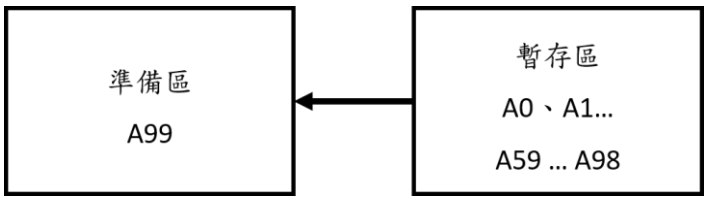

圖 9 區塊流程範例

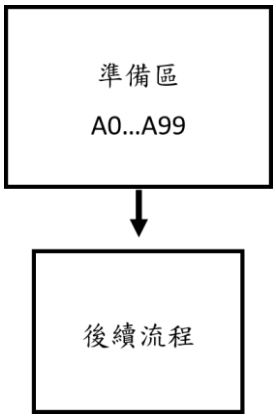

圖 10 區塊傳輸範例

當系統中暫存區的資料皆匯入準備區之後，系統會依序讀取每一區塊資料中的 Previous hash，此處 Previous hash 為區塊鏈 A 的區塊資料，在系統中將會讀取到 100 個 Previous hash 資料，並且透過環狀簽章產生出公鑰、私鑰與數位簽章，最後，在區塊驗證的流程中，可透過公鑰與原始資料判斷是否被竄改。於本系統中，私鑰由系統保管不對外公開，公鑰則與數位簽章以及原始資料儲存於區塊鏈 B 的區塊中，如圖 11 所示。

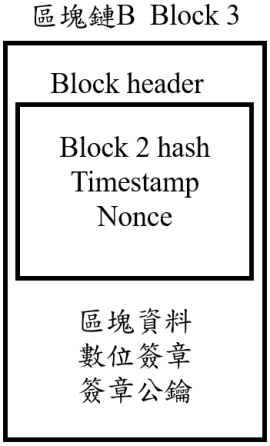

圖 11 新區塊示意圖

五、 應用情境：智慧保單

本節將會透過情境說明來帶入系統應用，藉此說明本研究之系統適用於哪種情境運作。本研究之情境主要參考自 2017 年 10 月份的 IEEE Special Report : Blockchain World 中的《How Are Smart Contracts Really Going to Work ?》[7]。

該篇文章所探討的是如何應用智慧合約於現實生活，內容選定的是機票的保單處理，並透過智慧合約技術去確認旅客搭乘的航班是否有延誤，若是航班延誤合約便會將理賠費用直接匯入旅客帳戶，若航班準時，合約將會把保險金額匯給公司。簡言之，在智慧合約的輔助下，保險公司將可不須要透過大量人工處理，即省去查找資料與驗證資料等繁複流程。

若該保險公司有非常多的客戶，每位客戶可能有不只一份保單，且每份保單的理賠方式亦都不相同。因此保險公司將需要足夠數量之人力來審查理賠資料和證據。而若該公司使用智慧合約技術，每一位客戶的每一份不同類型保單將可透過智慧合約技術自動處理，節省許多保險專員的人力耗置。且智慧合約將會自動審查資料，只要符合條件就會執行合約內的設定，每一次的審查保單都會產生一筆交易資料，最後交易資料都將儲存在區塊鏈中。隨著時間的增長，區塊鏈系統內的交易紀錄將大幅增加，將帶來巨量資料儲存與分析效率問題，而本研究所設計的輕量化區塊鏈驗證流程即可改善此一狀況。

底下將說明本研究所設計之區塊鏈驗證流程如何應用於智慧保單應用之中。首先，保單內容會以智慧合約方式呈現，並發佈在一個區塊鏈 A 中，系統將會把智慧保單寫入 A 的某個區塊中，並以智慧合約的形式執行系統程式，同時間，系統將建立另外一個專屬於公司內部驗證用的區塊鏈 B。系統執行後便會讀取所有區塊鏈 A 的 Block header，透過系統簡化將結果輸出存在區塊鏈 B 的區塊中，而公司內部需要驗證則只需要透過區塊鏈 B 做驗證，讓公司內部的其他節點可更快速驗證並節省大量儲存空間，使資源能更為活用。

以下將以圖解的方式說明在保險公司內此系統是如何運作。首先，使用者選定需要的機票保險，如圖 12。

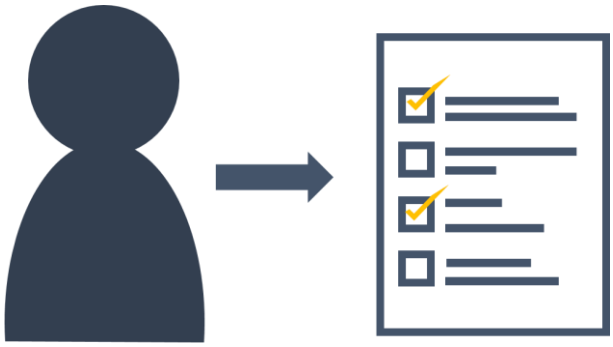

圖 12 使用者選擇需要的保險方案

接下來，如圖 13，使用者會將航班資訊與金額付給智慧合約。

圖 13 使用者將資料與費用付給合約

智慧合約收到資料與費用後會先與外部系統「Oracle」要求航班資訊確認是否正確，如圖 14。

圖 14 合約與外部系統確認資料

若確認資料無誤，智慧合約便會開始確認使用者支付的金額是否足夠負擔保險費用，如圖 15。若是足夠，智慧合約就會要求外部系統提供此航班的狀態，如圖 16，最後經由外部系統回傳的狀態判斷是否需要賠償保險費用，如圖 17。

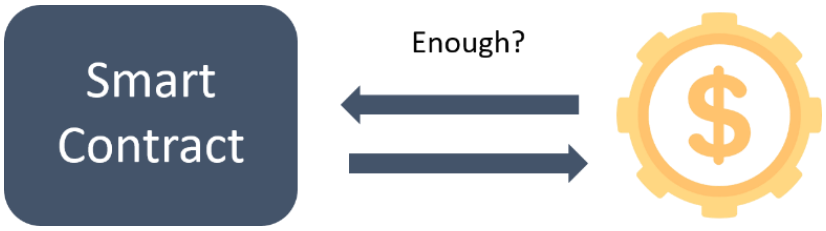

圖 15 合約確認金額是否足夠

圖 16 合約查詢班機狀態

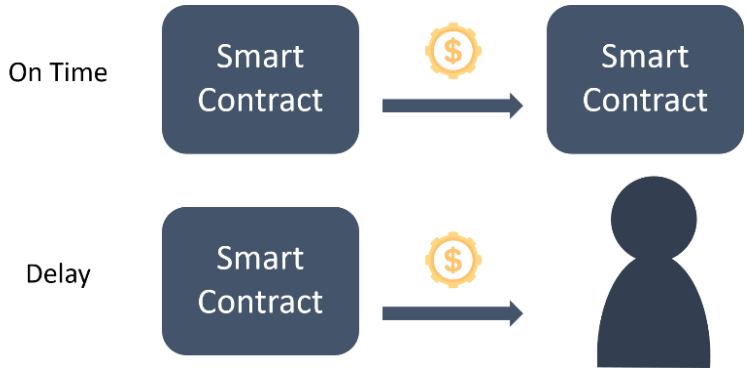

圖 17 合約支付費用

接下來，每張保單執行完成後便產生一筆交易紀錄，許多的交易紀錄會被儲存在該公司原有的區塊鏈 A 中，如下圖 18，每個區塊中都會有非常多數量不一的資料。

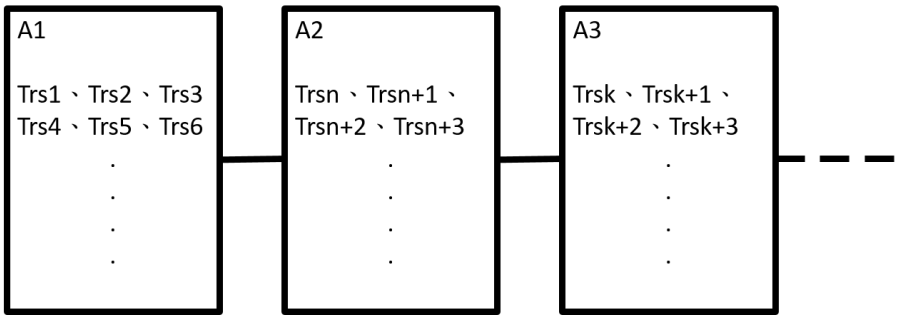

圖 18 區塊鏈 A 示意圖

隨著保單交易數量的增加，許多業務便希望透過區塊鏈輔助公司系統節省成本並且搭配智慧合約提升效能，而本研究所提出之系統會將區塊鏈 A 中每 100 個區塊透過環狀簽章與加密技術形成一個區塊鏈 B 的新區塊，藉此大量縮減區塊數量並且提高驗證效能，如圖 19 與圖 20。

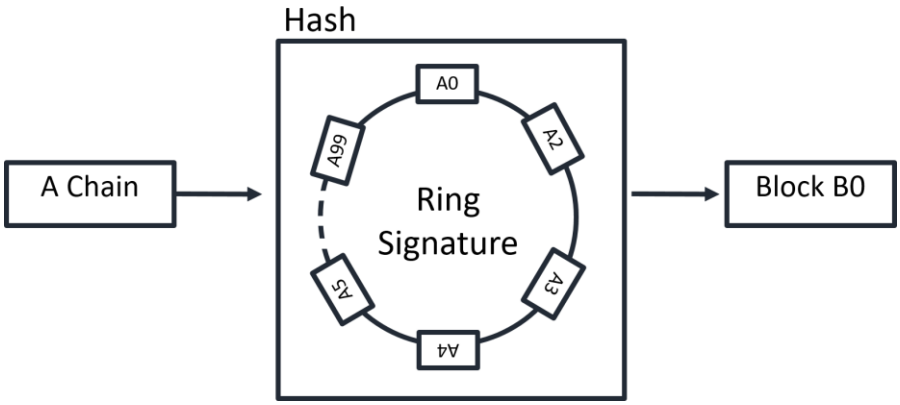

圖 19 區塊鏈 B 產生示意圖 1

於上圖 19 為示意在系統中會將 A 區塊鏈的區塊透過環狀簽章將每 100 個 A 區塊鏈的區塊縮減並輸出為區塊鏈 B，圖中舉例為 A0 至 A99 共 100 個區塊縮減為 B0 一個區塊。下圖 20 則為區塊鏈 A 與區塊鏈 B 的縮減過程。

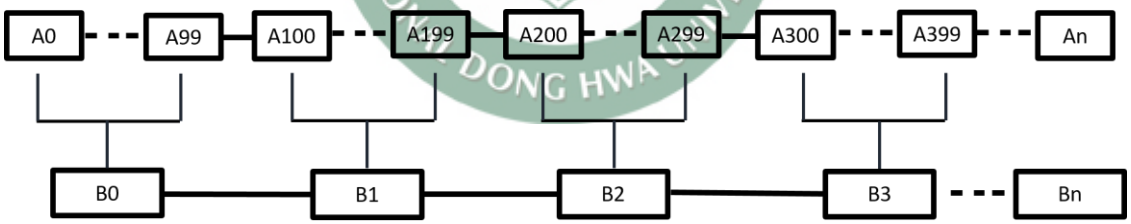

圖 20 區塊鏈 B 產生示意圖 2


國立東華大學
NATIONAL DONG HWA UNIVERSITY

肆、　系統效能分析

藉由第三章完整的論述本研究之系統架構，說明系統流程與執行方式，以下本章節將解釋系統之效能分析，證明本研究能有效改善原有系統並達成前述章節所提及的，在區塊鏈的環境下，如何透過結合智慧合約和環狀簽章等技術使其他節點在維持一定的安全標準下降低驗證所需的運算負擔，並提升其他節點之驗證速度的目的。

首先，本章節會以簡單幾項項目說明比特幣與以太坊之差異，包含挖礦時間與單一區塊的容量，並比較不同機制系統所需的區塊確認次數，如表 1。

表 1 比特幣與以太坊簡易比較表

	Bitcoin	Ethereum
挖礦時間	約10分鐘	約15秒
單一區塊容量	< 1MB	< 40KB
區塊確認次數	6 ~ 120	12~ (依需求而定)
一日區塊數量	144	5760

由表 1 可知，比特幣的挖礦時間為每 10 分鐘產生一個區塊，以太坊則為每 15 秒產生一個區塊；比特幣的單一區塊最高容量不會多於 1MB，以太坊在區塊容量方面則大幅減少為 40KB 以下；在區塊驗證數量方面，比特幣為 6 至 120 個，相關文獻中的說明為，6 個區塊驗證是最基本要求，若最安全驗證則需要 120 個，在以太坊機制下最基本區塊驗證數量為 12 個，可依安全性需求增加至所需數量；

最後是依據時間計算，比特幣一日會產生的區塊數量為 144 個，以太坊一日產生的區塊數量約為 5760 個。

在此章節本研究以區塊鏈 A 的第 A963 區塊的產生與驗證程序為例，舉出該區塊在區塊鏈 A 與區塊鏈 B 間的驗證差異。

在圖 21 中，區塊鏈 A 經過系統縮減後會產生出區塊鏈 B。兩者之間的完整區塊鏈的區塊數量分別為 962 個與 8 個，在數量明顯有極大的差異。

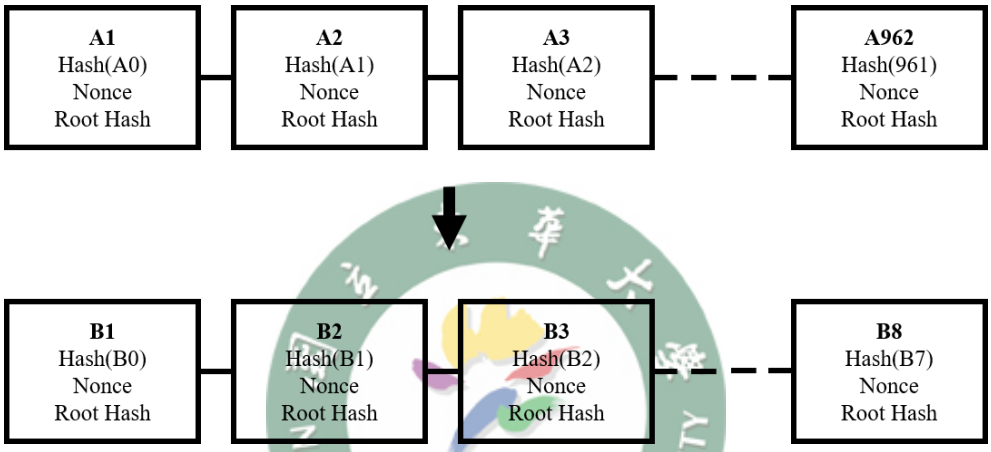

圖 21 區塊縮減示意圖

接下來在驗證的過程中，在本研究中由於採用的研究環境是模仿以太坊，故以以太坊所提出的 12 個確認為基準。

以下本研究假設 k 為 A 區塊鏈已有的區塊數量，在系統中所設定的驗證流程所需區塊數量則依據表 2 所示。

表 2 系統之區塊驗證數量

區塊數量	驗證之區塊次數	
k < 100	A : 12次	
100 ≤ k < 200	A : 11次	B : 1次
200 ≤ k < 300	A : 10次	B : 2次
300 ≤ k	A : 5次	B : 3次

如表 2 所見，若 A 區塊鏈的區塊數量少於 100，即 k < 100 則無法產生 B 區塊鏈，故只採用 A 區塊鏈的最後 12 個區塊做驗證。

接下來是當 A 區塊鏈的區塊數量介於 100 與 200 之間，即 100 ≤ k < 200 則只會有 1 個 B 的區塊，因此驗證時採用驗證 B 區塊的一個區塊與 A 區塊鏈的 11 個區塊。

當 200 ≤ k < 300 會改成驗證 2 個 B 的區塊與 10 個 A 區塊。

最後是當 300 ≤ k 能產生三個以上的 B 區塊時會存在至少三個有效的 B 區塊，達到本研究所需的驗證基本數量，此時驗證數量為 A 區塊 5 個與 B 區塊 3 個，當兩者同時驗證成功才能證明新區塊合法。

由上述所提出之驗證流程，本系統在驗證過程中相較於以太坊需要驗證 12 次以上只需要驗證 8 次。以太坊新區塊驗證 12 次所需的時間約為 3 分鐘，本系統則大約只需要 1 分 16 秒左右的時間，其中時間分析由下方圖示解釋。

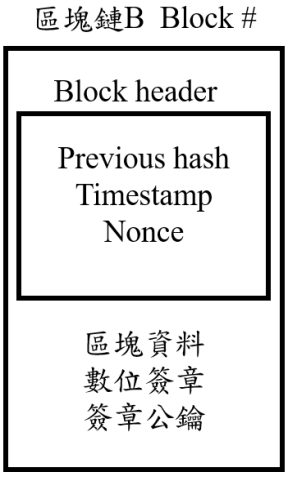

圖 22 區塊 B 之資料

本研究所提出的 8 次驗證分別為 5 個 A 區塊驗證與 3 個 B 區塊驗證，A 區塊為舊有區塊鏈故 5 次的驗證時間約為 1 分鐘 15 秒，B 區塊的 3 次驗證驗證時間為 0.18 毫秒，不足 1 秒以 1 秒計算，因此總驗證時間約為 1 分中 16 秒，其中 B 區塊的驗證是透過驗證 RSA 環狀數位簽章，由圖 22 所示，圖中的「區塊資料」為需要被加密的資料，資料內容為區塊鏈 A 所縮減的 100 個區塊的區塊雜湊值，每一雜湊值為 256 bit = 32 Byte，因此在 RSA 環狀簽章的加密的過程中實驗資料的長度為 32Byte，實驗結果如圖 23。

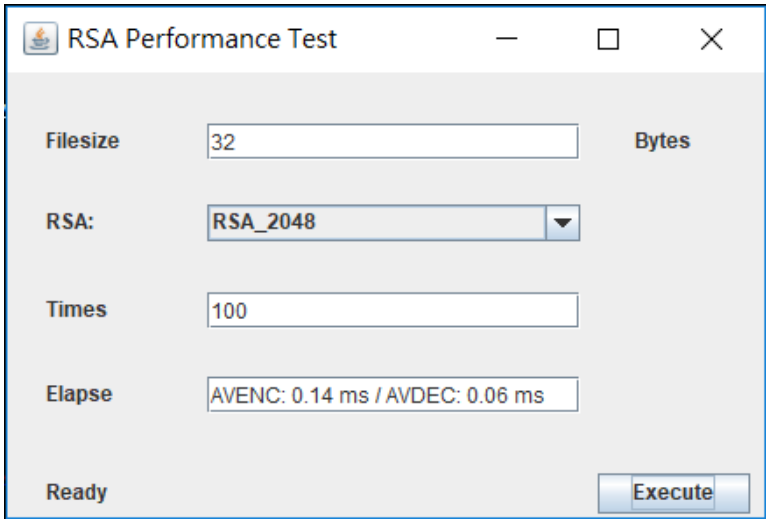

圖 23 簽章實驗測試結果

圖 23 為實驗測試結果，圖中的 AVENC (Average Encryption Time)代表測試 N 次中平均加密一次的時間；AVDEC (Average Decryption Time)代表測試 N 次中平均解密一次的時間。

實驗中使用長度 32Byte 的資料測試作為 RSA 環狀數位簽章所需的加解密時間，實驗次數為 100 次，由圖 22 中可知平均加密一次的時間為 0.14 毫秒，平均解密一次的時間是 0.06 毫秒，由此可推斷出來當有 100 筆資料使用環狀簽章進行加密時所需時間為 14 毫秒，解密時間為 6 毫秒。簽章時間 14 毫秒相較於 15 秒的挖礦時間非常短暫因此不影響區塊鏈 B 的產生，解密時間只需要 6 毫秒，亦不影響驗證流程，並且相較於 15 秒的驗證時間更為省時。

原先以太坊的區塊驗證時間大約為 3 分鐘，本研究提出的輕量化驗證流程所需大約 1 分鐘 16 秒，在驗證過程中兩者總體時間相比之下，每一個區塊的驗證時間差距為 1 分鐘 45 秒，能節省 57.8% 的時間，在效能方面具有明顯提升。此外，本研究提出之系統對於節點儲存的設備需求也可降低，如表 3，本研究所提出的輕量化系統在資料儲存的硬體設備需求可大幅降低，可節省約 99% 的容量。

表 3 比特幣與以太坊及研究系統之比較

	Bitcoin	Ethereum	系統
單一區塊容量	< 1MB	< 40KB	< 7KB
一日區塊數量	144	5760	57~58
一日產生資料	約144MB	約230.4MB	約400KB
驗證時間	60分鐘	15秒	1分16秒

第四章主要說明了本研究提出的輕量化驗證流程與原有的系統之效能分析，說明在驗證速度能夠有明顯提升，且能夠節省各節點的設備需求降低成本，對於資料龐大的區塊鏈應用可有效地簡化驗證流程，十分適用於需要效率且具有大量數據的單位或機構，可用於提升驗證速度，並藉此節省設備對於資料儲存與運算的負擔。

伍、 結論

本研究提出了一套架構適用於區塊鏈架構的輕量化區塊驗證流程，方法中主要利用了環狀簽章與雜湊函數來所縮減區塊鏈中的區塊驗證運算時間，且該機制將可搭配智慧合約技術來開發出新的應用。再者，透過智慧保單使用案例，本研究進一步說明如何利用所提出之輕量化區塊驗證流程來提升驗證速度與降低資料儲存需求。


國立東華大學
NATIONAL DONG HWA UNIVERSITY

參考文獻

[1] A. Bogner, M. Chanson, A. Meeuw, “A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain” In IoT'16 Proceedings of the 6th International Conference on the Internet of Things, Nov. 07-09, pp.177-178, Stuttgart, Germany, 2016.

[2] A. Yasin, L. Liu, “An Online Identity and Smart Contract Management System” IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, June 10-14, 2016.

[3] D. Ron, A. Shamir, “Quantitative Analysis of the Full Bitcoin Transaction Graph.” In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg, 2013

[4] F. Reid, M. Harrigan “An Analysis of Anonymity in the Bitcoin System.” In: Altshuler Y., Elovici Y., Cremers A., Aharony N., Pentland A. (eds) Security and Privacy in Social Networks. Springer, New York, NY, 2013.

[5] F. Zhang, K. Kim, “ID-Based Blind Signature and Ring Signature from Pairings.” In: Zheng Y. (eds) Advances in Cryptology - ASIACRYPT 2002. ASIACRYPT 2002. Lecture Notes in Computer Science, vol 2501. Springer, Berlin, Heidelberg, 2002.

[6] J. Herranz, G. Sáez, “New Identity-Based Ring Signature Schemes.” In: Lopez J., Qing S., Okamoto E. (eds) Information and Communications Security. ICICS 2004. Lecture Notes in Computer Science, vol 3269. Springer, Berlin, Heidelberg, 2004.

[7] M. E. Peck, “Special Report: Blockchain World: How Are Smart Contracts Really Going to Work?” IEEE SPECTRUM OCT 2017, pp. 30-31.

[8] M. H. Au, J. K. Liu, W. Susilo, T. H. Yuen, “Certificate Based (Linkable) Ring Signature”. In: Dawson E., Wong D.S. (eds) Information Security Practice and Experience. ISPEC 2007. Lecture Notes in Computer Science, vol 4464. Springer, Berlin, Heidelberg, 2007.

[9] P. McCorry, S. F. Shahandashti, F. Hao, “A Smart Contract for Boardroom Voting with Maximum Voter Privacy” Financial Cryptography and Data Security, Vol. 10322, pp. 357-375, 2017.

[10] R. L. Rivest, A. Shamir, Y. Tauman, “How to Leak a Secret” ASIACRYPT, LNCS, Vol. 2248, pp. 552–565, Springer, Berlin Heidelberg, 2001.

[11] R. Yuan, YB. Xia, HB. Chen et al, “ShadowEth: Private smart contract on public blockchain”, JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 33(3): 542-556 May 2018.

[12] S. Barber, X. Boyen, E. Shi, E. Uzun, “Bitter to Better — How to Make Bitcoin a Better Currency.” In: Keromytis A.D. (eds) Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science, vol 7397. Springer, Berlin, Heidelberg, 2012.

[13] S. C. Cha, J. F. Chen, C. Su, K. H. Yeh, “A Blockchain Connected Gateway for BLE-based Devices in the Internet of Things” *IEEE Access*, Vol. 6, pp. 24639-24649.

[14] S. S. M. Chow, SM. Yiu, L. C. K. Hui, “Efficient Identity Based Ring Signature.” In: Ioannidis J., Keromytis A., Yung M. (eds) Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science, vol 3531. Springer, Berlin, Heidelberg, 2005.

[15] Y. Hirai, “Defining the Ethereum Virtual Machine for Interactive Theorem Provers.” In: Brenner M. et al. (eds) Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science, vol 10323. Springer, Cham,2017.

[16] Y. Sovbetov, “Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero”, Journal of Economics and Financial Analysis, 2(2), 1-27., 2018.

[17] BitInfoCharts,
https://bitinfocharts.com/ (accessed on 16th March 2018)

[18] Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf. (accessed on 16th March 2018)

[19] Blockchain,
https://www.blockchain.com/ (accessed on 25th May 2018)

[20] Ethereum,
https://www.ethereum.org/ (accessed on 12th April 2018)

[21] Etherscan,
https://etherscan.io/chart/blocktime(accessed on 12th April 2018)

[22] Ethereum White Paper
https://github.com/ethereum/wiki/wiki/White-Paper. (accessed on 12th April 2018)

[23] Ethereum Yellow Paper,
https://ethereum.github.io/yellowpaper/paper.pdf. (accessed on 12th April 2018)

[24] Pro’s and Con’s on Bitcoin Block Pruning
https://news.bitcoin.com/pros-and-cons-on-bitcoin-block-pruning/
(accessed on 12th May 2018)

[25] Satoshi Nakamoto,
http://satoshinakamoto.me/ (accessed on 12th May 2018)

[26] Taipei Ethereum Meetup 台北以太坊社群專欄
https://medium.com/taipei-ethereum-meetup (accessed on 15th April 2018)

[27] 以太坊白皮書

https://github.com/ethereum/wiki/wiki/以太坊白皮書

(accessed on 22th April 2018)

[28] 維基百科-比特幣

https://zh.wikipedia.org/wiki/比特幣 (accessed on 11th May 2018)

[29] 維基百科-以太坊

https://zh.wikipedia.org/wiki/以太坊 (accessed on 11th May 2018)

[30] 維基百科-區塊鏈

https://zh.wikipedia.org/wiki/區塊鏈 (accessed on 11th May 2018)