國立臺灣大學工學院工業工程學研究所

碩士論文

Institute of Industrial Engineering
College of Engineering
National Taiwan University

Master Thesis

基於區塊鏈技術之智慧保險合約架構

Develop the Framework of Intelligent Insurance Contracts Using Blockchain Technology

黃禹
Yu Huang

指導教授：藍俊宏 博士
Advisor: Jakey Blue, Ph.D.

中華民國 111 年 6 月
June, 2022

doi:10.6342/NTU202201323

國立臺灣大學碩士學位論文
口試委員會審定書

論文中文題目：基於區塊鏈技術之智慧保險合約架構

論文英文題目：Develop the Framework of Intelligent Insurance Contracts Using Blockchain Technology

本論文係黃禹君（學號 P09546006）在國立臺灣大學工業工程學研究所完成之碩士學位論文，於民國 111 年 6 月 10 日承下列考試委員審查通過及口試及格，特此證明

口試委員：

藍俊宏 (指導教授) 藍俊宏

郭佳瑋 郭佳瑋

洪一薰 洪一薰

黃奎隆 黃奎隆

系主任、所長： 洪一薰 洪一薰

誌謝

首先感謝指導教授藍俊宏博士及工工所師長兩年的教導，回首兩年前參加洪一薰所長主持的招生說明會，當時滿心期盼著加入台灣最高學術殿堂，讓自己在多年工作後回到學校享受知識之旅，兩年後的今天在師長的指導下完成學業，達成自己一個階段性的學習。

另外感謝父母對自己的生育之恩及養育之情，以及內人對自己的支持。從入學的甄試到論文的撰寫，內人提供給我很多寶貴的意見，感謝她這段時間的陪伴讓我得以順利完成學業。

黃禹　謹識
于臺大工業工程研究所
民國 111 年 6 月

doi:10.6342/NTU202201323

中文摘要

歐美發展較早的保險公司多超過百年歷史，其中尤以人壽保險公司以提供長期的合約服務為經營目標。過去 20 年間由於經濟的發展及醫療費用支出的增長，人壽保險公司開發出各類型醫療保險商品及投資商品來滿足市場需求，同時間因為金融科技的衝擊，許多保險公司透過核心系統轉換達到數位化轉型及現代化，但是未來的金融環境不可預知，難以確保經過二十年後是否需要另一個現代化專案。

另一方面由於隱私意識抬頭，個人資料保護法規範客戶可以要求保險公司刪除其個人資料，但因為災難復原計畫保險公司需要定期備份資料，一旦契約終止，客戶要求刪除的部分資料已被移至備份資料中，公司需要將備份資料還原後，刪除資料後再備份，這在營運上會增加巨量的作業時間及成本。

鑑於區塊鏈與比特幣技術具有資料幾乎難以竄改，歷史資料可被完整記錄以及個人資料匿名化等特性，而後 Ethereum 及 Hyperledger Fabric 等技術發展出區塊鏈智能合約，可以在區塊鏈架構下自動執行合約杜絕人為介入，這些特徵具備被信任的基礎。經參考專業研究機構的報告，保險核心系統未來的主要功能是資料紀錄，這樣的定位與區塊鏈的特點相吻合，因此本論文將探討利用區塊鏈建立新的保險合約模型，並用不同的案例場景演示整體架構的可行性。之後可依照商品性質建立特定的保險區塊鏈，降低核心系統的複雜度，保留保險合約智能化最基本的結構，無論將來金融環境如何變化，合約都能被正確執行。

關鍵詞：保險合約、區塊鏈、智能合約

doi:10.6342/NTU202201323

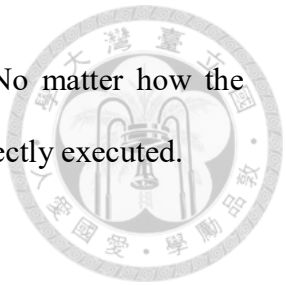
Abstract

It has been developed with a long history in most western insurance companies, in which life insurance companies particularly aim at offering long-term contracts. In addition, the surge in economic growth and medical cost has given rise to various health insurance products and investment-linked insurance policies to accommodate market demands in the past decades. Insurance companies have constantly transformed their core systems, facing the impact of the latest financial technology. However, the financial landscape is always unpredictable, and it is uncertain whether another modernization project will be necessary for the coming decades.

As privacy awareness rises, Personal Data Protection Act stipulates that insurance companies must delete customer data when requested. On the other hand, the Data Recovery Plan necessitates regular data backup in insurance companies. Once an insurance contract is terminated or a customer requests to delete his data, the insurance company has to recover the backup data, delete the data, and backup again. It is a time-consuming and costly procedure to go through.

Blockchain and bitcoin technology is characterized by their immutable data, complete records of transactions, and anonymity. Techniques such as Ethereum and Hyperledger Fabric lead to the creation of smart contracts, which can be self-executed under a blockchain structure without human intervention. Through referring to the reports from Gartner and TCS, which foresee the principal function of core systems will evolve toward data recording integrity in the future, which aligns exactly with the blockchain features. This paper will explore the use of blockchain technology to build a new insurance contract model and demonstrate the architectural feasibility with different scenarios. Finally, a specific insurance blockchain can be established according to the nature of the commodity, reducing the complexity of the core system and retaining the

doi:10.6342/NTU202201323



most essential and intelligent structure of the insurance contract. No matter how the economic environment evolves in the future, the contract can be correctly executed.

Keywords: Insurance Contract, Block Chain, Intelligent Contract

doi:10.6342/NTU202201323

目錄

doi:10.6342/NTU202201323

doi:10.6342/NTU202201323

圖目錄

doi:10.6342/NTU202201323

doi:10.6342/NTU202201323

表目錄

doi:10.6342/NTU202201323

第一章 緒論

金融商品與其他商品不同，金融機構在合約成立後，僅能以金融憑證的方式記載商品內容，不管是實體的紙張或電子檔案，雙方依照此憑證內容履行權利與義務。現行的憑證是由發行單位認證，歷史數據亦是由發行單位留存，資料的正確性及保留均是由發行單位負責，消費者有疑義時必須透過客服單位尋求解釋，如果購買的商品較為複雜，客戶很難獨自判斷是否正確。另一方面金融機構與客戶簽訂合約當下，必須收集及保存客戶個人資料以便識別客戶，一旦合約終止，客戶的資料還是存留在金融機構單位，這對於客戶是一個未知的風險。

保險商品與其他金融商品相較下，因為商品多元化及內含複雜的商品計算公式，保險合約維運需要更嚴謹的流程確保數據正確性。自從各國個人資料保護的意識抬頭，各國無不盡力完善個人資料保護的法令，由於保險公司業務特性需要收集到保戶個人隱私資料，對其影響極大。由於區塊鏈具有執行合約的能力，資料保留完整在歷史區塊，資產擁有者的身分可以被隱密，這幾項特性能夠揭露完整資訊並且保護當事人隱私，符合保戶的利益，目前已有在區塊鏈執行短期特定保險的合約應用如飛機延誤險，本論文將探討人壽保險合約在區塊鏈架構下實現的方法、可能遭遇的困難與優劣分析。

第一節 研究背景與動機

人壽保險業務隨著平均餘命的增加和鉅額的醫療費用，新類型商品不斷的推陳出新，換言之就是不斷地在保險合約資訊系統（保單管理系統或是核心系統) 增加新的規則，規則的數量可視為複雜的程度，考量保單合約最長的期間將一百年，不同年代的商品需要同時運行在一套保單管理系統，不同世代的商品規則參雜在一起，使得保單管理系統維運的困難度相當高。在這樣的結構下，軟體開發時間週期與成本都非常高，難以滿足市場快速變化的要求，以新冠肺炎的商品為例，台灣市場需求量約 2000 萬張保單，沒有在第一時間銷售的保險公司，相對的銷售量不會太高。如果要滿足商品上市時間，需要縮短系統開發時間或者部分採用人工的方

doi:10.6342/NTU202201323

式作業，這時品質相對會下降，工商時報 2020 年 9 月 9 號報導台銀人壽保險滿期金給付錯誤 (工商時報，2020)，單次溢付金額超過千萬元，其原因是給付金額由人工輸入。個人資料保護法實施後對保險產業是一個極為棘手的挑戰，保戶可以要求保險公司刪除個人資料包含保險公司的備份資料，其法規來源自個人資料保護法的第三條及第十一條規範個人資料保存的限制。第十一條第三項「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限」。基於上述的議題，如何利用新的模型解決以上的問題是本篇研究的動機。

doi:10.6342/NTU202201323

第二節 研究目的

區塊鏈具備了智能合約可以依據特定條件自動執行合約交易，杜絕了人工介入的情況，每項交易被記錄在區塊資料中且無法竄改的優點增加了資訊透明度及可依賴性，而區塊鏈去除實體記名的機制，可以符合個人資料保護法第三條及第十一條的法令要求。但區塊鏈也並非全然沒有局限，由於區塊鏈會在每個節點處存同樣的區塊資料，不適合儲存大量的資料，這意味著鏈上的合約功能不適合複雜的交易規則。當今已有產險公司將簡易的商品實施在區塊鏈智能合約，如飛機延誤險直接讀取機場的數據庫，超過合約上延誤的時間，區塊上的智能合約直接給付理賠金。台灣壽險業同樣也看到區塊鏈共享資料的特性，開發理賠聯盟鏈，2020 年 8 月 4 號 iThome 中的報導描述壽險公會落實區塊聯盟鏈的服務，保戶可在保險公司的理賠申請功能畫面填入理賠申請資時，可同時選擇要申請理賠的保險公司，申請資料會同時讓被選定的公司共享，提供保戶單一申請介面，取代過去需要對每家保險公司填寫申請書，簡化流程，提高理賠服務的客戶體驗。理賠聯盟鏈落實了資料共享的優點，但區塊鏈智能合約的優點尚未被開發，是以本篇研究如何善用區塊鏈智能合約的架構優點取代現有的保單合約管理系統。

doi:10.6342/NTU202201323

第三節 研究架構

接下來的章節會在第二章第一節介紹人壽保險公司商品分類以及核心系統的一直以來面臨的挑戰，第二節參考已發表的論文、專業機構報告及專家意見，闡述其意見及支持區塊鏈保險的觀點，第三節參考中本聰的所著之比特幣白皮書"A Peer-to-Peer Electronic Cash System"，說明支持去中心化區塊鏈的重要設計，另外介紹被理賠聯盟鏈採用的 Hyperledger Fabric 架構，其為本研究實現保險合約區塊鏈的推薦架構。

第三章介紹區塊鏈實架構下的保險合約及區塊資料內容。第一小節描述去除個人身分識別的鏈架構設計及資料內容，第二節描述保險合約鏈的區塊資料及區塊上註記程序的目的，第三節說明本研究的範例商品及變更交易的程序。

第四章以第三章的架構配合六個情境演示保險區塊鏈的區塊資料變化，並說明保險公司現行方案與保險區塊鏈的區別，第二節針對保險特有的回朔情境及資料錯誤提出解決方案。

第五章將總結第三章及第四章的演示結果，提出保險區塊鏈的優點及侷限性，另外提出保險聯盟鏈的架構下其它可以發揮的空間。

doi:10.6342/NTU202201323

第二章 文獻探討

文獻回顧第一節我們介紹人壽商品的種類及當前維運的挑戰；第二節參考兩家專業機構 Gartner 和 TCS 對於保險核心系統的報告，另外參考國內有關保險及區塊鏈的研究報告；第三節參考 Bitcoin 及 Hyperledger 的技術文件，描述區塊鏈的運作原理。最後將帶出本論文整合現代金融技術至保險合約制度上的突破點。

第一節 人壽保險商品種類及核心系統現代化的挑戰

一、人壽保險商品種類

保險是將不確定的損失藉由成立契約轉嫁給保險公司，如圖 2-1 所示來說明保險，保戶的義務就是繳交保險費。

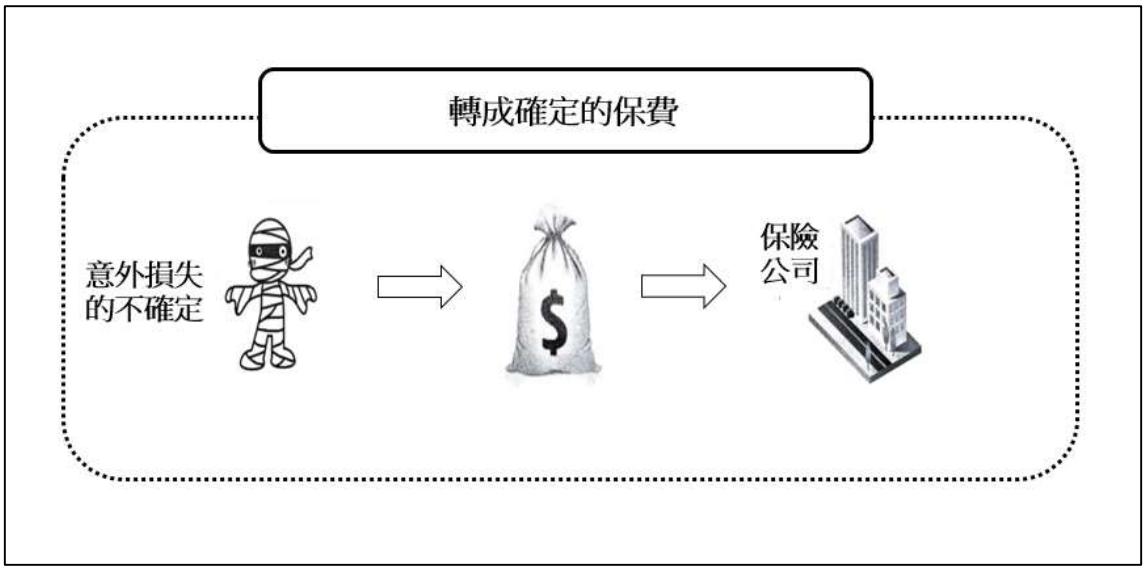


圖 2-1 保險契約 (資料來源：圖解保險學)

隨著人類的平均餘命增加以及巨大的醫療費用，人壽保險商品除了基本的保障型商品，保障死亡及生存給付外，還發展涵蓋特定疾病的給付，如癌症險及重大疾病等。如果以保費投資的角度而言，又可區分為傳統型商品和投資型商品。概括而言，可以以風險及投資方式來分類商品，表 2-1 以風險分類，表 2-2 以資金風險方式分類

(一) 以商品類型分類

doi:10.6342/NTU202201323

表 2-1 商品類型 (資料來源：圖解保險學)

商品名稱	敘述
死亡保險	保險人死亡生時，由保險公司依保險契約所約定的金額
生存保險	被保險人於保險期間屆滿仍然生存時，保險公司依照契約所約定的金額給付保險金
生死合險	保險契約約定以被保險人於保險期間內死亡或於保險期間屆滿仍生存時，保險公司依照契約所約定金額給付保險金者稱為生死合險，又稱為養老保險
重大疾病給付	主要是針對癌症，肌梗塞、冠狀動脈繞道手術、中風、慢性腎衰竭、重大器官移植、癱瘓等，保戶一旦罹患上重大疾病，依照保險契約之定範圍可領取一筆保作為醫療補助
生前給付	即被保險人在經醫師診斷因疾病或傷害致其生命經判斷不足六個月時，可以前申請領取保險金
健康保險	因疾病或傷害導致的下列經濟損失，由保險彌補其損失 (1)失去了工作能力所造成的收入損失 (2)由於藥物、住院、看護、手術及各項雜費的醫療、醫藥開銷
傷害保險	補償意外傷害所遭受之生命財產的損失
年金保險	對個人在特定期間或生存期間繼續提供定期性給付金額的保險

(二) 以投資分類

表 2-2 資金風險分類 (資料來源：投資型保險最重要的大小事)

商品類型	資金風險
傳統型商品	保險公司承擔所有風險(投資風險、死亡風險、費用風險)
投資型商品	保戶承擔投資風險，保險公司承擔死亡風險和費用風險

doi:10.6342/NTU202201323

二、核心系統現代化的挑戰

數位化轉型一直是保險公司的重要戰略目標，而核心系統是數位化轉型的重要基石，因為保險合約各項的端到端(End to End)流程，核心系統都扮演不可或缺的角色，如銷售通路的酬庸、經營管理決策的數據分析及公司財務報告等都必須依賴核心系統的資料數據。

資訊系統現代化的目標之一是將業務流程及規則歸納後簡化，將之模組化，轉化成參數配置的方式取代程式代碼開發，目標是快速交付新商品，支持銷售通路及提升客戶服務效率。這幾項目標都有一個共通的議題就是簡化流程及歸納規則，人壽保險公司因為商品種類眾多及長期合約的性質，簡化流程及歸納規則一直是最大的挑戰，由以下的業務特性說明其原因。

(一) 商品種類多樣化

每個類型的保險商品會有不同的處理流程，不同的流程就會有不同的規則。例如分紅商品在週年日需要批次分紅作業計算紅利及給付作業，投資型商品的基金交易需要配合各類基金交易頻率的不同做特殊化處理，例如這段時間因俄烏戰爭，投資在俄國的基金需要下架或轉換。另外各種契約變更所需要的規則及公式均不相同，例如意外險的商品如果被保險人換了工作內容而調整職業等級，保費會因而調整。

(二) 長期合約的影響

人壽保險大多是長期合約，同類型的商品由於開發的年代不同，所用的經驗生命表或預定利率就有不同的版本，因此商品也會有世代的概念。如 1974 年販售的死亡險與 1989 年的死亡險所用的經驗生命表就不同，所以在 1974 年生效的保單在 1990 發生死亡理賠，除了給付保單上的理賠金外，還需要額外給付兩個版本經驗生命表的死差異，因為同一年齡在新的經驗生命表死亡率會較低。另一方面，因為新的法令要求，已經生效的保單同樣需要配合調整某些規則。這些都是短期合約可忽略。

doi:10.6342/NTU202201323

(三) 多個商品組合成一張保單的影響

業務員銷售保單時多數採用 Needs-Based Selling 的方式，收集客戶各類的需求後，儘量會在一張保單合約涵蓋各類型商品，例如剛進入職場的人會被推薦保障型的保單，包含一張死亡險外加醫療保障及意外保險。一張保單合約就包含了三個商品，不同種類的商品各有其規則，簽發在一張保單合約中，處理上需要考慮這三個商品的規則是否有相互依賴性因而增加整合性規則。例如死亡險是繳費 20 年期，醫療保障附約需要繳費到 75 歲，如果死亡險收費期滿後須要考慮醫療保障附約，保單合約需繼續維持效力。但是如果此張保單僅有一個商品，保險合約即終止。

doi:10.6342/NTU202201323

第二節 專業報告觀點

Gartner

2021 年十一月 Gartner 發佈了一份標題為 "Insurance business model evolution will reduce the role of core systems to record keepers by 2030" 的報告 (Gill & Harris-Ferrante, 2021)，在這份報告中，保險業務的演進呈現出一個趨勢 (如圖 2-2 所示)，隨著金融科技的發展，核心系統的對組織的價值會遞減，當到達 Intelligent 的階段時，核心系統的功能會導向成為資料記錄，負責資料輸出到智慧數據平台驅動業務流程及決策。

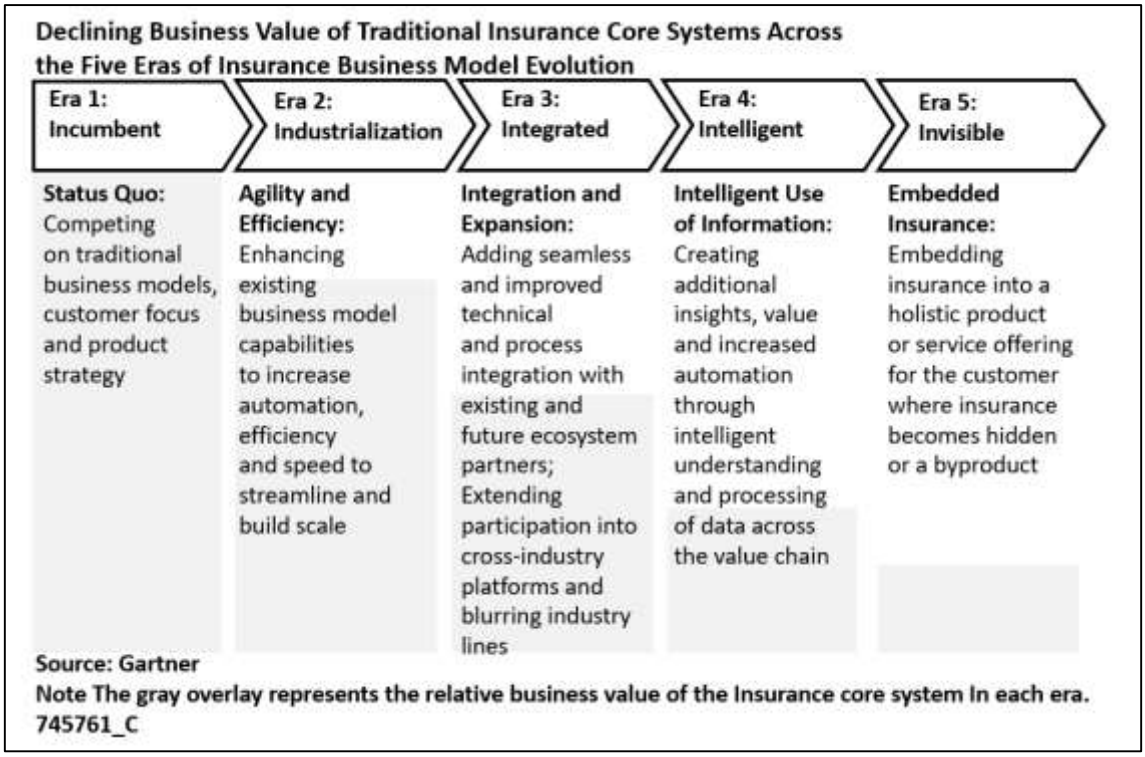


圖 2-2 Insurance Business Model Evolution Will Reduce the Role of Core Systems to Record Keepers by 2030 (資料來源：Gartner 報告)

報告中提出五個階段的表徵如下：

- Incumbent：保險商品及業務流程需要倚賴核心系統。
- Industrialized：在這個階段競爭的優勢著重在效率與降低營運成本，此階段保險公司為了彌補核心系統的不足，採用了機器流程自動化(robotic process automation)，流程管理(business process management)和人工智慧等工具。

doi:10.6342/NTU202201323

- Integrated：整合並加快與合作夥伴的作業流程，核心系統在這個階段扮演後台的營運系統，利用佈署開放式 API 及微服務(Microservices)與雲端服務提供者緊密連結，達到流程快速整合。
- Intelligent：著重在使用資料做為驅動決策及自動化，在這個階段核心系統轉向定位為資料的紀錄，與外部的智慧平台或自動化流程緊密結合。
- Invisible：著重在簡化用戶體驗，保險商品及服務會附加或在合作夥伴的商品，利用更獨立前後台架構服務，核心系統的功能僅有商品定義及法規報告，這個階段保險公司的核心策略將移到支援新契約及支援商品有關的服務。

該趨勢說明了隨著金融科技的發展，核心價值從倚賴核心系統功能支援的業務模式轉換成倚重其他科技廠商如雲端服務，接著到資料決策的智慧模式，到最後保險商品會結合合作夥伴商品，一併提供給消費者提供更友善的體驗。所以未來核心系統的功能僅在提供商品定義、保險合約紀錄及法規報告的平台。這個變化除了未來新科技公司快速的發展，另一方面 Gartner 從現有提供核心系統軟體的公司財報看到核心系統軟體服務廠商難以投入在新科技的發展。

TATA Consulting Service (TCS)

TCS 在 2020 年發布了這份標題為 "Insurance Product-Decode, Rationalize and Modernize" 的白皮書，對於保險公司不斷推出新商品所產生以下的問題羅列如下：

- 太多類似的產品使得業務流程複雜化。
- 類似商品但客戶得到不同的體驗。
- 法規遵從的要求需要重複性的修改相同的流程。
- 技術維護不具有成本效益，因為任何技術更改都將涉及重複的程式開發和測試。
- 公司需要為不再使用的產品保持專業知識。從長遠來看，傳統的技術人才只會增加公司的責任。
- 類似商品使得很難識別真正推動業務增長或是沒有競爭力的產品。換句話說，企業很難從數據中學習到有用的資訊。

這些問題即使透過核心系統現代化專案升級系統，還是會遺留在新系統，所以

doi:10.6342/NTU202201323

專案一開始就注定要失敗。

區塊鏈保險的相關文獻

2018 年交通大學研究生彭笙榕所著的”保險業應用區塊鏈技術之探討”中提到區塊鏈能保留資料的完整性，建立客戶對保險公司的信任度而且提升客戶體驗。另外透過智能合約可以簡化理賠流程，讓理賠資訊透明。這個觀點就是運用區塊鏈歷史資料完整性及不能竄改的特性，另一方面，保險公司意識到智能合約自動理賠改善了理賠流程及提升了客戶滿意度。

2021 年輔仁大學研究生李冠諭所著的”區塊鏈技術在外溢保單誘因回饋流程之設計”提出了利用穿戴式裝置回饋資料至區塊鏈保險合約，在區塊鏈設計自動化的機制回饋給客戶。這個研究延伸出區塊鏈保險合約與外部資料交換的機制，目前保險公司在保單生效與異動時需要與公會交換資料，在智能合約的架構下，在保險聯盟鏈生態下，與外部資料交換的效率勢必會獲得改善，錯誤率也會降低。

2021 年政治大學研究生林宛誼所著的”被遺忘權與資料留存的悖論—以區塊鏈技術為中心”。在這份研究提出了以主鏈及側鏈的架構，利用已發展出的跨鏈技術處理主鏈與側鏈資料交換，用主鏈與側鏈跨鏈可相互資料交換。隱私資料權限可在側鏈控管，將敏感資料的處理從主鏈抽離。

doi:10.6342/NTU202201323

第三節 區塊鏈技術平台

中本聰於 2008 年發表的比特幣白皮書”Bitcoin: A Peer-to-Peer Electric Cash System”後，比特幣在網際網路的環境下實現了數位化資產，這對世界是很大的變革。這也造成了一股趨勢，許多軟體開源團體基於區塊鏈的精神，發展出不同的技術及應用，本研究探討在區塊鏈上實現保險合約，此節介紹區塊鏈相關內容，包含比特幣及企業使用的聯盟鏈。以下說明目前區塊鏈的各類平台及種類以及比特幣區塊鏈上的特性，另外著重在聯盟鏈 Hyperledger Fabric 的技術架構。

Hyperledger 專案是由 Linux 基金會啟動的專案，由 IBM 參與開發，是一個許可制下的區塊鏈，適合企業在這個架構下實現智能合約的應用。

一、區塊鏈各類技術平台及種類

由現行區塊鏈的應用場景及相關投入發展的專案，可以從以下兩個角度來分類：

(一) 參與成員

表 2-3 區塊鏈類別 (資料來源：維基百科)

	公有鏈 Public chain	聯盟鏈 Consortium blockchain	私有鏈 Private chain
特性	公有鏈屬於 完全開放	聯盟鏈則採取會員制	私有鏈屬於特定 企業內部使用
參與者	所有人	聯盟成員	鏈的所有者

(二) 技術平台

表 2-4 區塊鏈技術平台 (資料來源：維基百科)

名稱	應用場景
Bitcoin	比特幣交易
Ethereum	乙太幣及智能合約

doi:10.6342/NTU202201323

名稱	應用場景
R3 Corda	應用在聯盟鏈 著重在金融業，目的把帳本從銀行「之內」，放到銀行「之間」，讓銀行共同維護一份帳本，並降低建立信任的成本。
Hyperledger Fabric	應用在聯盟鏈 在「許可制」的條件下，可以不需要讓所有節點都重複執行交易，只要在足以保證安全性的最低條件下讓「一部分」的節點執行即可，其他大多數節點不需重複執行，僅需進行少量驗證並更新自身狀態即可

二、比特幣應用的技術

中本聰所撰寫的比特幣白皮書中，我們可以瞭解到比特幣運作的要點。這幾項設計也成為後續各家區塊鏈技術平台著重的重點，以下描述幾項重要的特性。

(一) Proof-of-work

區塊鏈屬於分散式系統，而拜占庭將軍問題是分散式系統最難處理的問題之一。問題如後，分散式系統中的成員電腦可能出錯而傳送錯誤的資訊，用於傳遞資訊的通訊網路也可能導致資訊損壞，使得網路中不同的成員關於全體協同運作的策略得出不同結論，從而破壞系統一致性。而比特幣採用了工作量證明(Proof-of-Work)。說明 PoW 之前，我們先要提及雜湊函數(Hash Function)，雜湊函數有下列幾項特性，而比特幣採用了 SHA256 雜湊函數，輸出值為 256 個 byte。

- 相同輸入值就會產生相同的輸出值。
- 雜湊值具備不可逆的特性，由輸出值反推原始的輸入值十分困難。
- 不論輸入數值的長度為何，輸出值都是固定長度。

doi:10.6342/NTU202201323

- 不同輸入值不會產生相同輸出值的狀況。

比特幣利用區塊內的數據加上隨機產生的 Nouce(如圖 2-3 所示)做為 SHA256 的輸入值，經過 SHA256 函數產生輸出值，輸出值與比特幣的困難值(Difficult)比較，因為比特幣上的每個節點都在執行同樣的事，所以一旦某個節點的輸出值小於 Difficult，這個節點就會對外發布，其他節點可以根據發佈的資料經過 SHA256 驗證，驗證合格就可以在自己的節點加入這個區塊。由於 SHA256 的輸出值有 16 的 64 次方個變化，所以相當每個節點的計算量非常龐大，比特幣利用這樣的機制避免在分散式架構下出現資料性不一致的問題。

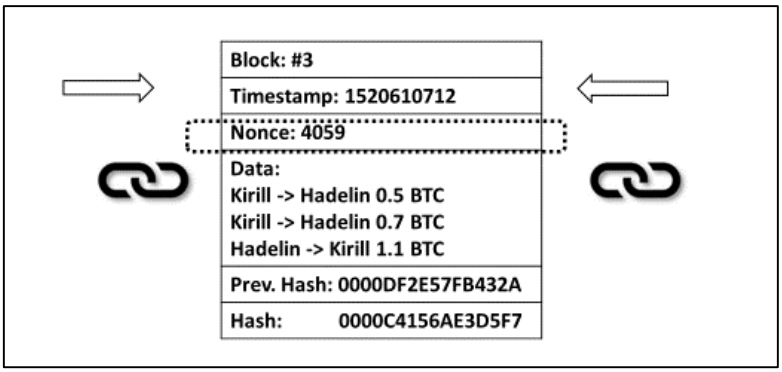


圖 2-3 比特幣區塊內容 (摘自 Eremenko, 2018)

(二) 使用非對稱式的密碼學確認交易的有效性

在比特幣的世界，個人註冊完帳號就可以使用這個帳號交易比特幣，不必以個人的真實身分交易。交易的有效性是透過公私鑰的機制，以目前資源還無法破解這個公私鑰的機制，這個機制可達到去身分識別化。

(三) 區塊鏈上的資料無法竄改

因為比特幣的每個區塊包含前一個區塊的 Hash 值，所以如要更改某一個區塊的內容，就必須要更改區塊鏈上所有區塊的資料，因為每個節點都保存一樣的區塊鏈資料，要竄更改資料，必須要同時更改所有節點上的區塊資料，這要全鏈上超過 51%的算力才可能達成。(如圖 2-4 所示)

doi:10.6342/NTU202201323

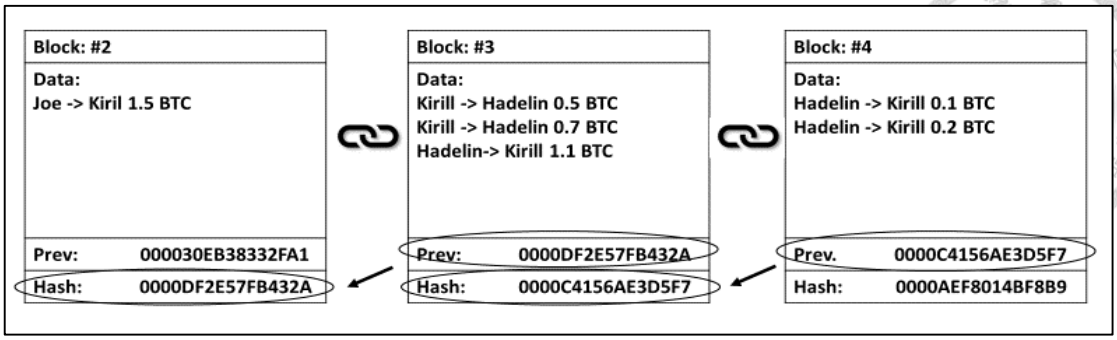


圖 2-4 比特幣前後區塊資料關聯 (摘自 Eremenko, 2018)

(四) 歷史數據完整的保存在區塊上

區塊上的資料無法串改，過去的所有交易及完整數據均可以完整的保留在區塊上，這種特性與現行多數的資訊系統不同，多數的資訊管理系統僅會保留當下的主數據，過去的異動的部分資料僅會保存在歷史數據。

三、聯盟鏈及 Hyperledger Fabric 架構

比特幣屬於公鏈的應用，任何人無須經過許可(Permissionless)即可加入，另外它為了達成一致的共識，必須讓每個節點都在做挖礦這同一件事。這種損耗效能及低效率的模型無法在企業實現。企業內或企業之間的網路需要考量安全性，所以事先獲得許可才能進入網路，權限是被事先核准給予適當的權限等級。IBM 的研究團隊發表的”Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”這篇文獻提出 Hyperledger Fabric 的架構，改善了比特幣執行效率的議題，做為區塊鏈在企業應用的模型。以下分幾點描述 Hyperledger Fabric 的特性：

(一) Hyperledger Fabric 與比特幣區塊模型比較

Order-Execute Model - 比特幣所使用的模型(如圖 2-5 所示)。比特幣上的每個節點需要對交易順序達成共識，也就是排序，確認順序後再交由每個節點驗證，每個節點驗證後再更新自己的區塊。

doi:10.6342/NTU202201323

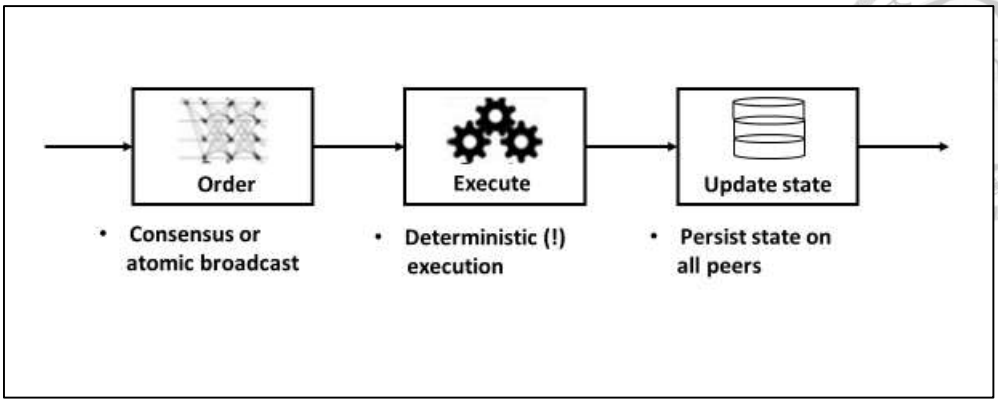


圖 2-5 比特幣的工作模型 (資料來源：IBM 報告)

Execute-Order-Validate Model – Hyperledger Fabric 架構(如圖 2-6 所示)交易會交由特定的節點(Peer)各自「執行」，如果執行結果一致就可以形成共識，未形成共識的交易會被捨棄。已形成共識的交易會經由一個特定服務(Order Service)進行「排序」並增加至區塊。接著這個特定服務再將新的區塊傳播給所有節點，收到區塊的節點僅需對交易進行少量「驗證」，若驗證結果無誤便可以更新自身狀態。

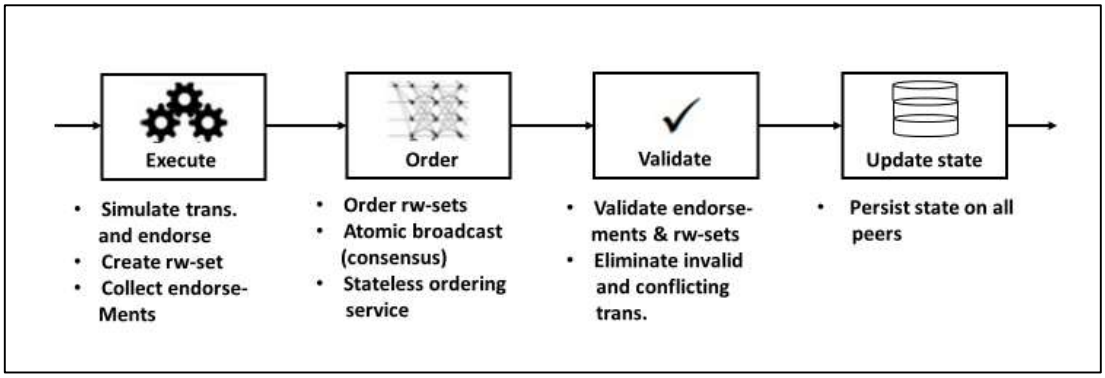


圖 2-6 Hyperledger Fabric 工作模型 (資料來源：IBM 報告)

在 Hyperledger Fabric 的節點會依照角色賦予不同的身分，分別為 Peer、Orderer 及 Client 三種身分，這些參與成員組合成一個 Channel 並共同維護一套帳本，而每一個 Channel 都是一個獨立的區塊鏈網路，擁有自己的帳本。這三種身分的說明如下：

- Client - 就是與 Hyperledger Fabric 互動的應用程式。
- Peer - 負責交易的執行和驗證，負責交易的節點稱為 Endorsing Peer，

doi:10.6342/NTU202201323

負責驗證的節點稱之為 Committing Peer。交易在被認可加入區塊帳本前需要得到 Endorsing Peer 的背書(Endorsement)，因為 Endorsing Peer 上具有能執行 Chaincode (Smart Contract)的能力，在背書之前模擬交易執行。Endorsing Peer 與 Committing Peer 的差異表示在圖 2-7。

- Orderer - 負責交易的排序及區塊的產生。

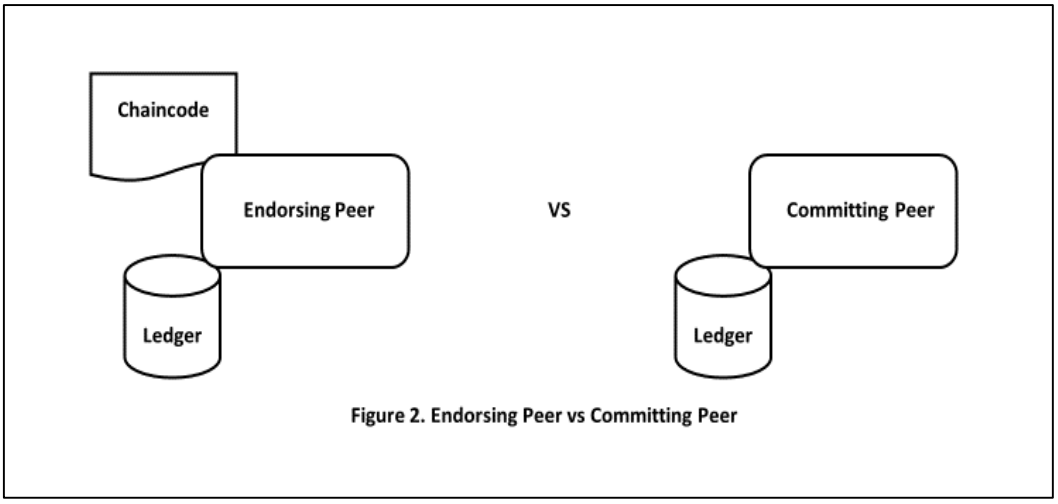


圖 2-7 Endorsing Peer vs Committing Peer (摘自 Thummavet, 2019)

(二) Hyperledger Fabric 身分認證及權限控管 Hyperledger Fabric 建置一個模組 MSP(Membership Service Provider)處理節點的身分認證及權限控管，Fabric 採用業界通用的 X.509 憑證來做身份識別，能夠相容於現有的身份管理體系。MSP 的功能只負責憑證的管理，不負責發布憑證。可以使用憑證機構（Certificate Authority, CA）頒發的憑證，但也可以使用 Hyperledger Fabric 提供的 Fabric-CA 發佈憑證。這樣的設計可以讓 Hyperledger Fabric 能夠與既存的公鑰基礎建設（Public-key Infrastructure, PKI）整合。

(三) Hyperledger Fabric 的網路架構

兩個不同的組織的節點 Org1-Peer 及 Org2-Peer 在同一個 Channel A，兩個節點上的 Chaincode 及 Ledger 因為同在一個 Channel A，所以相同。(如圖 2-8 所示)

doi:10.6342/NTU202201323

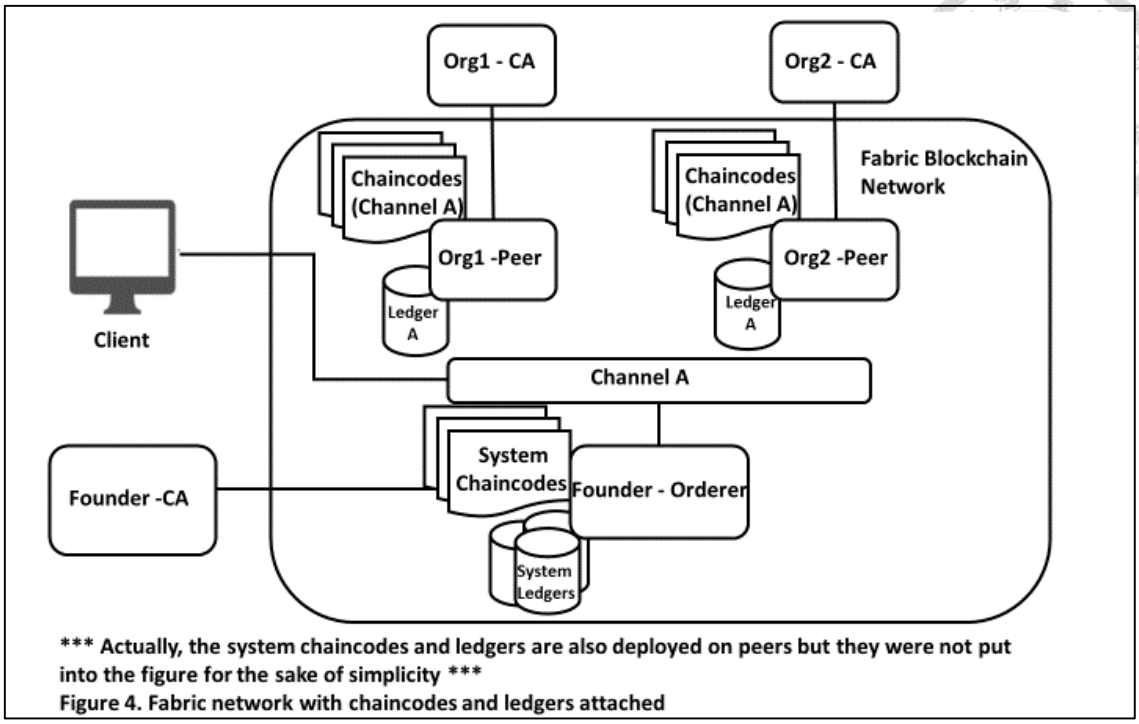


圖 2-8 兩個組織的簡易 Hyperledger Fabric 網路架構 (摘自 Thummavet, 2019)

(四) Hyperledger Fabric 多鏈的網路架構

存在兩個 Channel，Org2-Peer 同時存在 Channel A 及 Channel B，所以 Org2-Peer 具備兩個 Channel 的 Chaincode 及 Ledger。(如圖 2-9 所示)

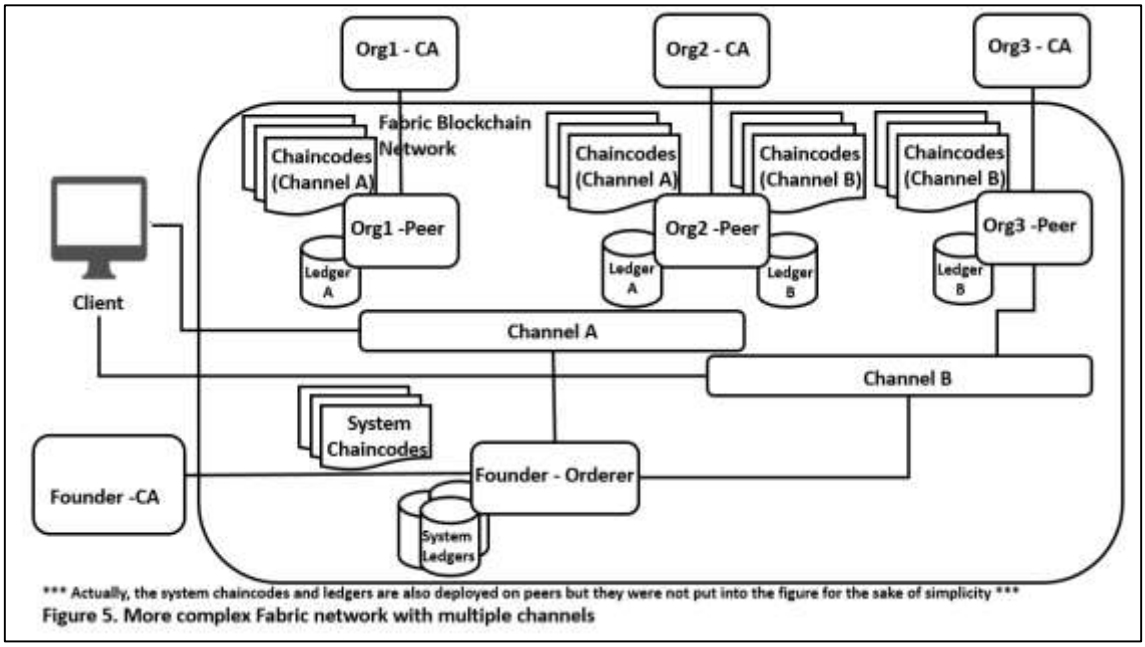


圖 2-9 多個組織和多個 Channel 的 Hyperledger Fabric 網路架構 (摘自 Thummavet, 2019)

doi:10.6342/NTU202201323

(五) 共識機制

Hyperledger Fabric 的節點是被事被許可加入，在這個前提下，節點可被信任的程度比一般未經過適當審核的機制來的高。透過 Endorsing Peer 的執行後的一致的背書(Endorsement)及 Committing Peer 的檢核，達到共識的機制。將區塊產生的 6 個步驟(如圖 2-10 所示)分為三個階段：

- Endorsement 階段（步驟 1-3）
- Ordering 階段（步驟 4-5）
- Validation and Commitment 階段（步驟 6）

步驟一、Client 遞送附上使用者簽屬的交易建議書給 Endorsing Peer。

步驟二、Endorsing Peer 確認交易的合法性後，模擬建議書的交易。

步驟三、當步驟二的結果正確，Endorsing Peer 發送具有背書的回應給 Client。

步驟四、Client 得到 Endorsing Peer 的背書回覆後，遞送交易給 Orderer Peer。

步驟五、Orderer Peer 產生新的區塊。

步驟六、Orderer Peer 發佈新的交易到鏈上的節點。

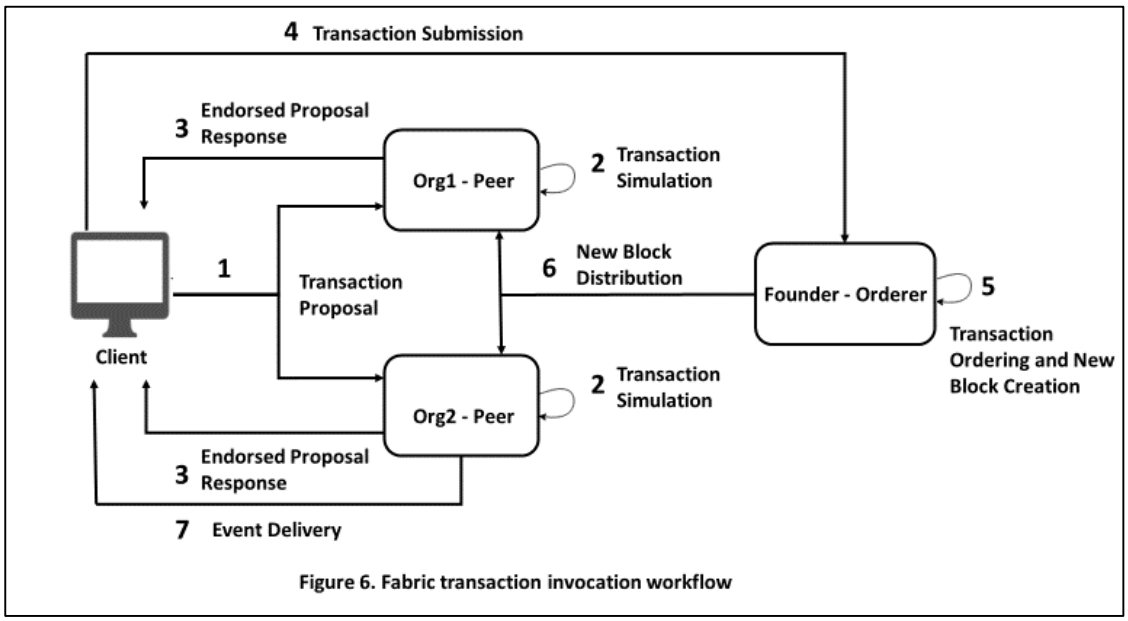


圖 2-10 Fabric 交易流程(摘自 Thummavet, 2019)

doi:10.6342/NTU202201323

第三章 智能保險合約架構

區塊鏈具有去個人化識別、資料不能竄改及歷史交易均在鏈上的設計。本章以第二章介紹的 Hyperledger Fabric 為基礎建構一個保險合約平台，平台僅銷售保障型的商品，讓智能合約的規則簡易化。由於保險交易的數據不是那麼直觀，交易完成後要追朔或複現其結果不易，所以在設計上，區塊除了儲存合約數據，同時也儲存產生這個數據的公式代碼及版本，一旦由於公式的錯誤導致某個數據不正確，可以回到產生這個數據區塊前的區塊數據，再利用更新後的公式版本再次產生正確的數據。

第一節 架構及去個人識別化

客戶購買人壽保險，需要提供個人資料識別實體的個人，並提供被保險人的健康資訊及財務說明做為風險評估的依據。由於保險公司有災難復原的機制，資料需要定期備份，一旦保險合約終止，客戶的資料的移除需要包含備份資料，現實實務上困難度及成本相當高。

可以仿效比特幣區塊鏈的設計，將帳戶的個人資訊去除，保戶所交付的資料可用數位簽章驗證。第一步先要透過認證程序，識別當事人，認證同時還需要審核被保險人與受益人是否有保險利益關係，這個步驟是排除道德風險，如被保人與受益人沒有保險利益，就不可以承保。受益人需要記載在保險合約，當有死亡理賠事故，由受益人送交死亡證明文件，才能啟動理賠。

設計單獨一個區塊鏈（鏈一）處理去除個人化的訊息，保戶確認身分後創建一個保戶代碼，接著填入承保需要衡量風險的生日、性別、職業及健康聲明書，可識別個人化的身分證號碼、電話號碼、聯絡地址等均不用提供。圖 3-1 所示，鏈一的輸出內容為需要成立契約的合約主數據及保費，鏈一的區塊資料(圖 3-2)主要為去除個人化的基本訊息及保費。

另一方面為了收取保費及支付理賠金的需求，保戶在鏈一創建身分時，保險公司需要提供一組虛擬帳號給要保人便於繳交保費，另外要保人及受益人須自行設

doi:10.6342/NTU202201323

定銀行帳號連結這個區塊鏈的身分帳號，如有保單貸款及理賠金給付時，付款金額會轉到這個身分帳號的帳戶，保戶須自行轉帳到此銀行帳戶。

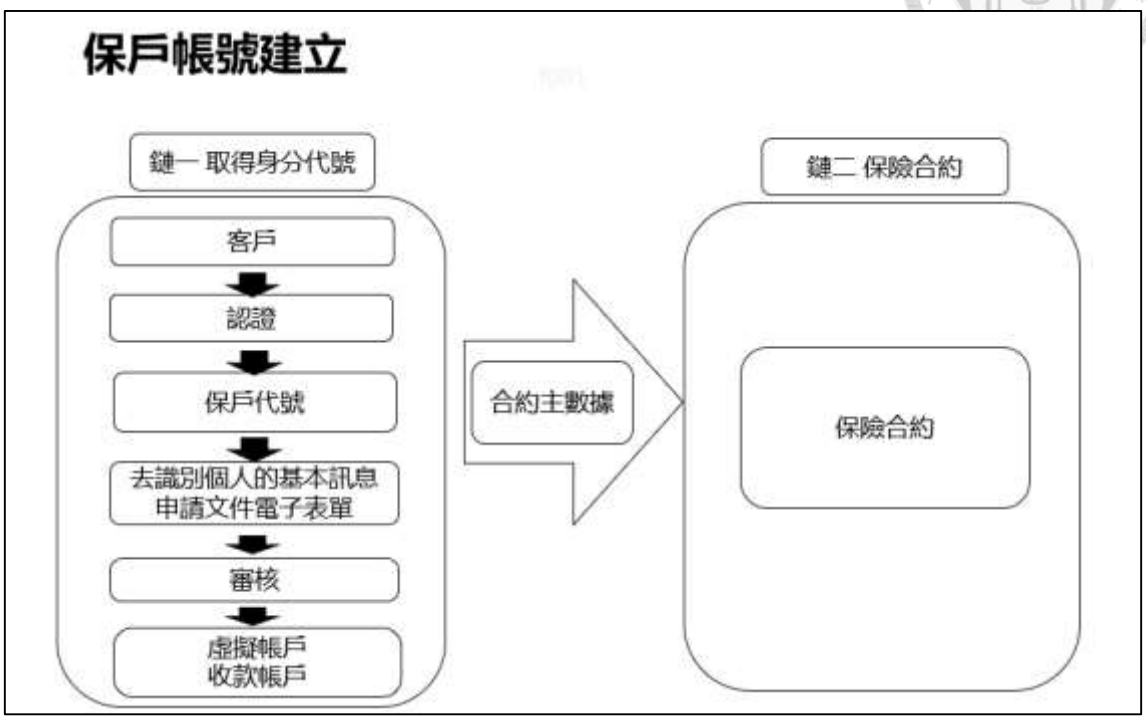


圖 3-1 創建帳號流程

圖 3-2 鏈一區塊資料

doi:10.6342/NTU202201323

基於以上的業務流程，將架構圖描述於圖 3-3。

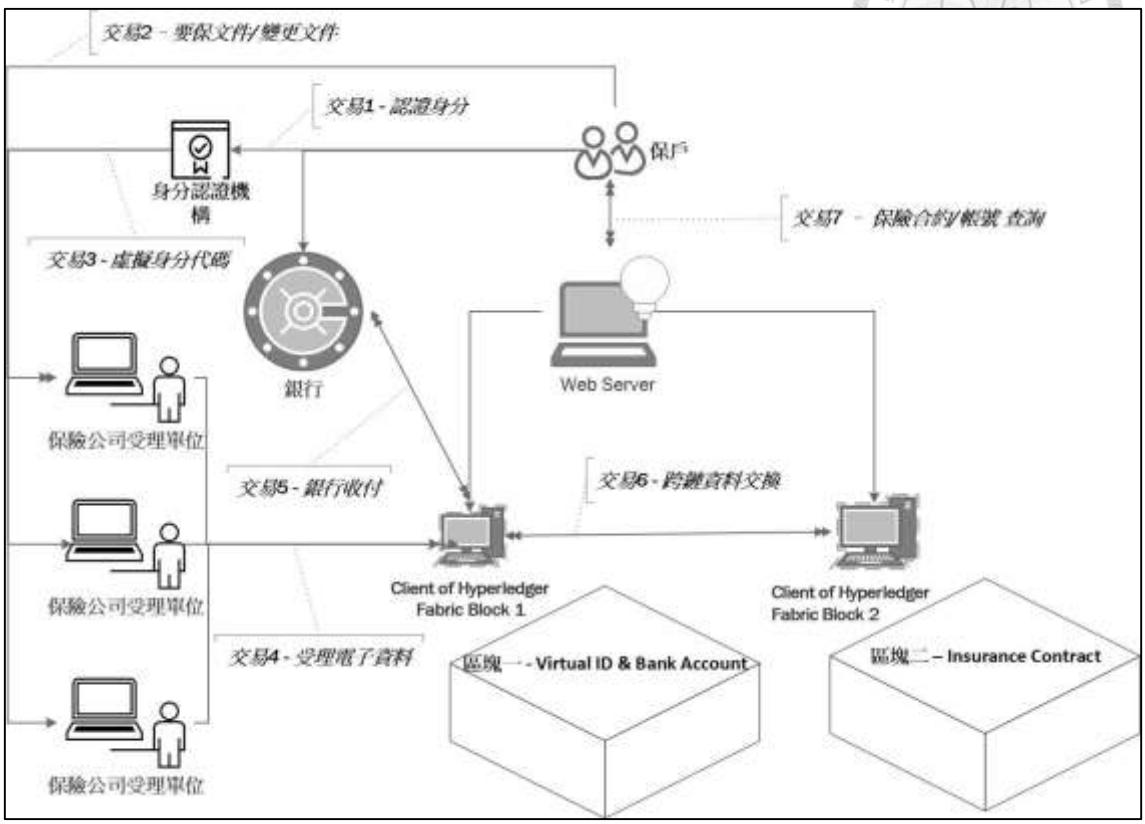


圖 3-3 區塊鏈保險合約架構圖

- 角色
  1. 保戶- 保險合約中的角色包含要保人、被保險人及受益人
  2. 身分認證機構 – 確認保戶身分及創建虛擬客戶代號
  3. 保險公司受理單位 – 受理新契約或是變更合約
  4. 銀行 – 保戶透過銀行繳付保費或領取保險給付
  5. Web Server – 保戶可透過 Web Server 上的 API 查詢鏈一/鏈二上的資料
  6. Client of Hyperledger Fabric Block1/Block2 – Hyperledger Fabric 架構的 Client
- 交易類型
  1. 認證身分 – 新保戶需要確認身分，確認保戶與投保身分一致
  2. 要保文件/變更文件 – 保戶遞送新契約要保文件或契約變更文件
  3. 虛擬身分代碼 – 身分認證確認後，產生虛擬身分代碼

doi:10.6342/NTU202201323

4. 受理電子資料 – 受理單位確認交易無誤將電子資料傳遞到鏈一
5. 銀行收付 – 客戶透過銀行給付保費或保險給付由鏈一傳輸到保戶指定的銀行帳號
6. 跨鏈資料交換 – 鏈一和鏈二的資料交換
7. 保險合約/帳號查詢 – 保戶透過 Web Server 上的應用程式查詢鏈一及鏈二的資料

doi:10.6342/NTU202201323

第二節 保險合約區塊結構

一、鏈二區塊資料(如圖 3-3 所示)

- 區塊主數據：區塊序號、區塊產生時間及保險公司代碼。
- 合約主數據：包含保單序號、客戶代碼、商品代碼、合約起訖日、繳費期限以及交易程式代碼。
- 數據表：運算所需要的數據表，如標準保費、次標加費費率及解約金表。
- 保單貸款：保單貸款數據。
- 繳費紀錄：歷次繳費金額及日期。
- 付款紀錄：保險給付或保單貸款記錄。
- 程式代碼：此區塊產生時所使用的程式代碼。

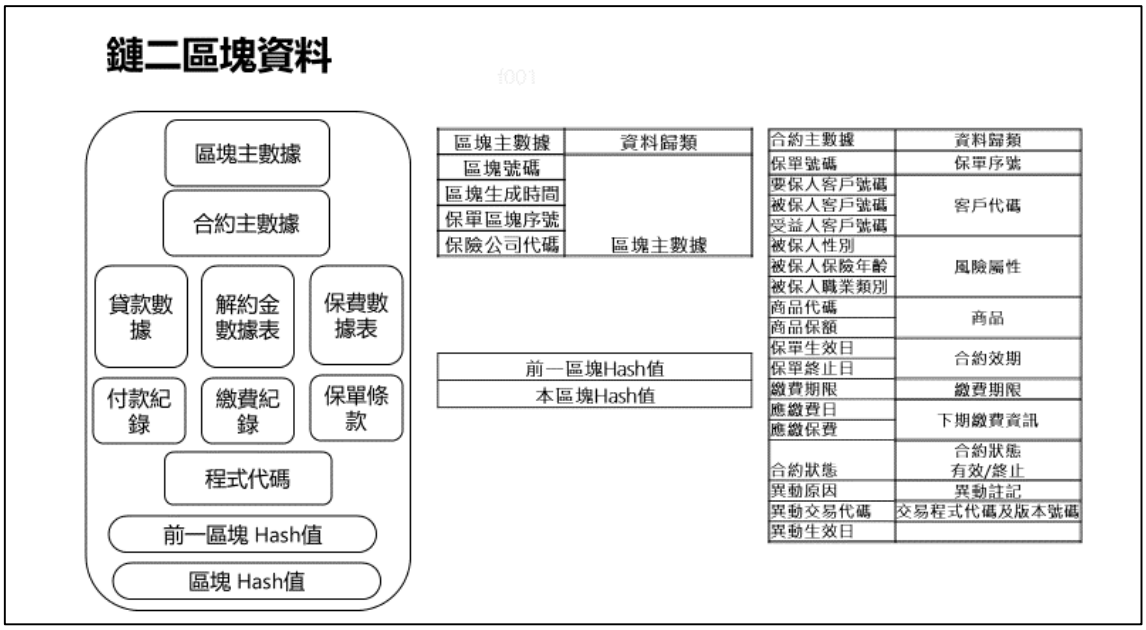


圖 3-4 鏈二區塊資料

二、鏈二區塊資料-程式代碼

資料處理就像是數學中的函數運算$f(x)=y$，f就是某個功能，x是資料處理的輸入值，y就是輸出值。一般資料處理記錄輸入及輸出，「處理」這個元件f，因為是一群代碼的組合，比較難像資料用較具體的方式紀錄。如果在正式環境 f 函數錯誤，導致y是錯誤，即使是修正了f這個功能，在機制上很難針對單筆或整批出錯的

doi:10.6342/NTU202201323

資料，重新用原始的輸入值x及修正後的f處理，得到修正後的數值y。如果要用這種方式處理，需要收集當時的x輸入值，另外需要開發特定的工具做單次處理，這樣還需要驗證這個工具，在時效考量下並非是最佳方案。在區塊鏈的結構下，上一個區塊就是本區塊的輸入值x，僅要修正f後，回朔到當時的區塊x，執行正確的f，後續的區塊會自然更新為正確的數值。可以設計在區塊鏈的結構下，記載著程式代號及版本，當需要修正資料時，可以依據程式代號索引到當時的程式代碼，修正後更新版本，再用前一個區塊正確的資料執行即可，此部分的案例在第四章詳細說明。表 3-1 是一個計算首期保費的範例，圖 3-5 演示程式代碼 A 在兩個區塊扮演的功能。

表 3-1 首期保費計算程序

程式代碼	交易內容-功能	函數代碼	函數
IS001	計算首期保費	CAL0001001	計算保險年齡
		CAL0002001	讀取費率表
		CAL0004001	計算標準體保費
		CAL0005001	計算次標準體加費
		CAL0006001	計算保費折扣
		CAL0007001	計算應繳保費

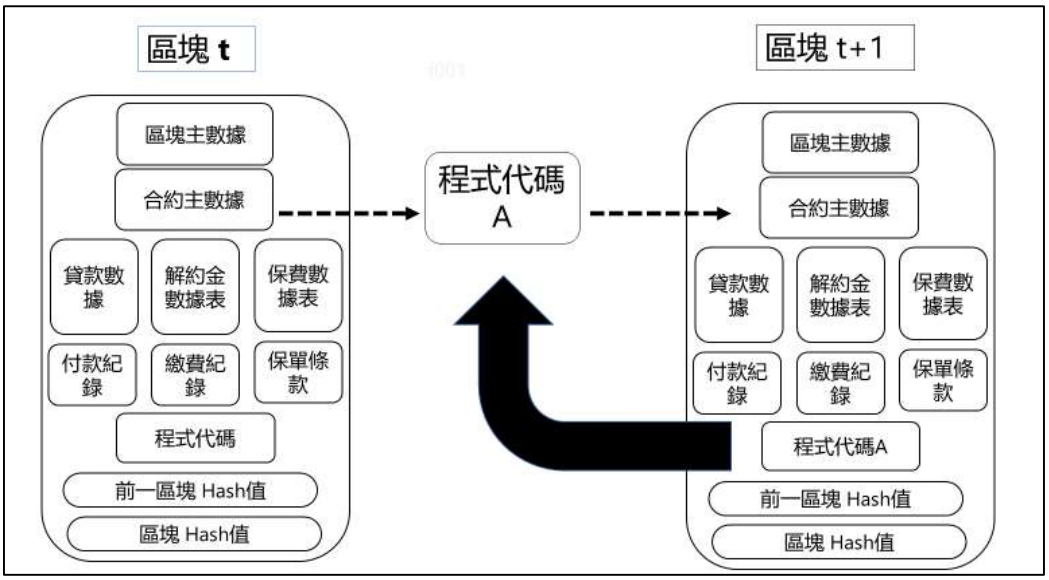


圖 3-5 程式代碼的作用

doi:10.6342/NTU202201323

第三節 商品說明

一、商品及相關數據

為了簡化模型平台僅銷售保障型單一商品，銷售商品為十年期分期繳費定期壽險。保費及相關數據表：

表 3-2 10 年期分期繳費定期險標準保費

10 年期分期繳費定期險 標準保費 男性 30 歲		
商品名稱	保險利益	每十萬元保額 單位:元
10 年期分期繳費定期險	疾病或意外身故	107

表 3-3 10 年期分期繳費長期加費費率表

10 年期分期繳費定期險 長期加費 男性 30 歲		
商品名稱	保險利益	每十萬元保額 單位:元
10 年期分期繳費定期險	疾病或意外身故	15

表 3-4 10 年期分期繳費解約金表

10 年期分期繳費定期險 解約金表	
年度	每十萬元保額 單位:元
0	0
1	0
2	13
3	24
4	31
5	35
6	37
7	35
8	29
9	17
10	0

doi:10.6342/NTU202201323

二、業務場景

(一) 新契約發單

保戶向保險公司購買人壽保險，需要提供個人資料確認實體的個人，再將被保險人的健康資訊及財務說明提供給保險公司作為風險評估的依據。

- 公式清單

表 3-5 首期保費計算程序

IS001	計算首期保費	CAL0001001	計算保險年齡
		CAL0002001	讀取費率表
		CAL0004001	計算標準體保費
		CAL0005001	計算次標準體加費
		CAL0006001	計算保費折扣
		CAL0007001	計算應繳保費

(二) 契約變更-降低保額

客戶將保額降低，例如發單時購買五百萬保額，經過三年後認為保障足夠，降低保額到三百萬，保險公司需要退兩百萬保額的未到期保費及解約金，並且重新計算保費。

- 公式清單

表 3-6 降低保額計算程序

程式代碼	交易內容-功能	函數代碼	函數
CF001	降低保額	CAL0008001	計算第t保單年度的t值 (變更日期-生效日期)
		CAL0009002	讀取第t年度及第t+1年度解約金
		CAL0010003	線性差值計算變更日期的解約金
		CAL0011004	計算變更日期到應繳費日的日數
		CAL0012005	計算應收保費或應退保費
		CAL0013006	加總應退(應收保費)及解約金

表 3-7 計算續期保費程序

程式代碼	交易內容-功能	函數代碼	函數
PC001	計算續期保費	CAL0002001	讀取費率表
		CAL0004001	計算標準體保費
		CAL0005001	計算次標準體加費
		CAL0006001	計算保費折扣
		CAL0007001	計算應繳保費

doi:10.6342/NTU202201323

(三) 續期保費收費

繳交續期保費(參考表 3-8)，超過期限未繳交保費會直接停效，並計算出解約金退給客戶。

- 公式清單

表 3-8 計算續期保費程序

程式代碼	交易內容-功能	函數代碼	函數
PC001	計算續期保費	CAL0002001	讀取費率表
		CAL0004001	計算標準體保費
		CAL0005001	計算次標準體加費
		CAL0006001	計算保費折扣
		CAL0007001	計算應繳保費

表 3-9 計算解約金程序

程式代碼	交易內容-功能	函數代碼	函數
ET001	停效日解約金	CAL0008001	計算第t保單年度的t值 (變更日期-生效日期)
		CAL0009001	讀取第t年度及第t+1年度解約金
		CAL0010001	線性差值計算應繳費日的解約金

(四) 契約終止

十年期到期，保險合約終止。

(五) 保單貸款

解約金屬於保戶，客戶可以解約金做抵押品貸款，但可貸金額為解約金的部分比例，另外由於定期壽險解約金超過一定年期後數值會遞減的特性，只允許在保單前六個年度貸款。

- 公式清單

表 3-10 計算保單貸款程序

程式代碼	交易內容-功能	函數代碼	函數
PL001	保單貸款	CAL0008001	計算第t保單年度的t值 (變更日期-生效日期)
		CAL0009001	讀取第t年度及第t+1年度解約金
		CAL0010001	線性差值計算貸款日期的解約金
		CAL0015001	計算解約成數比例

doi:10.6342/NTU202201323

(六) 死亡理賠

給付死亡保額扣除保單貸款本利和，保險契約終止。

- 公式清單

表 3-11 計算死亡理賠程序

程式代碼	交易內容-功能	函數代碼	函數
DS001	死亡理賠	CAL0016001	計算死亡保額
		CAL0017001	計算保單貸款本利和
		CAL0018001	死亡保額扣除保單貸款本利和

doi:10.6342/NTU202201323

第四章 案例研討

此章第一節呈現以區塊鏈的模型展示保險合約生命週期每個狀態的內容，第二節演示當某個交易因程式錯誤導致結果錯誤，在區塊鏈的模型上如何調整。

第一節 保單區塊演示

一、情境說明

- 要保人/被保險人 身分證字號 A123456789 男性，生日 1992/10/1
- 受益人　　身分證字號 A123456788 女性，與被保險人夫妻關係
- 購買 10 年期 保額 600 萬，生效日 2022/1/1，年繳保費
- 2023/1/1 繳交續年度保費
- 2024/2/1 繳交續年度保費
- 2024/3/1 解約 100 萬，保額變為 500 萬
- 2024/6/1 保單貸款 300
- 2024/7/30 死亡理賠，死亡時間為 2024/7/7

二、區塊鏈內容演示

(一) 區塊#1：創建保險契約(如圖 4-1 所示)

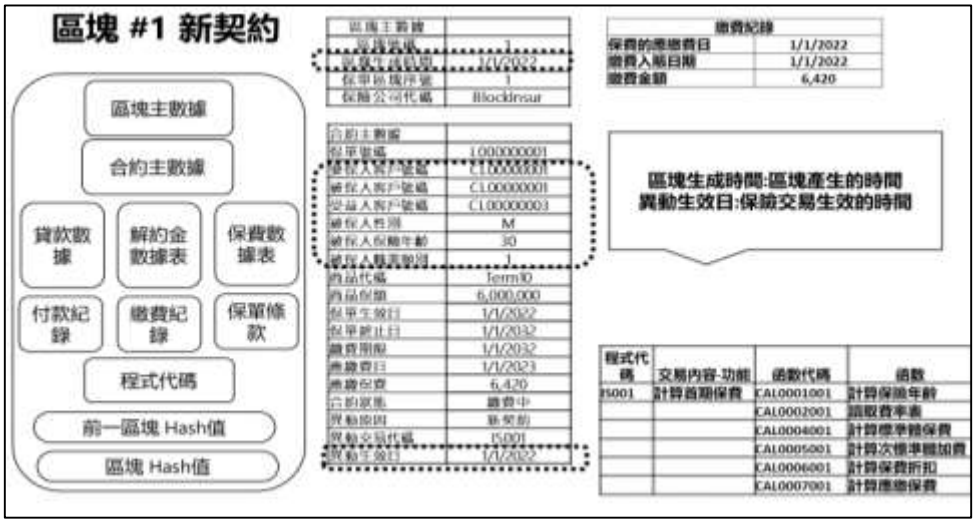


圖 4-1 創建保險契約

doi:10.6342/NTU202201323

(二) 區塊#2：繳續期保費

繳 2023/1/1 的續期保費，繳付完應繳費日變更為 2024/1/1，並新增繳費紀錄(如圖 4-2 所示)。

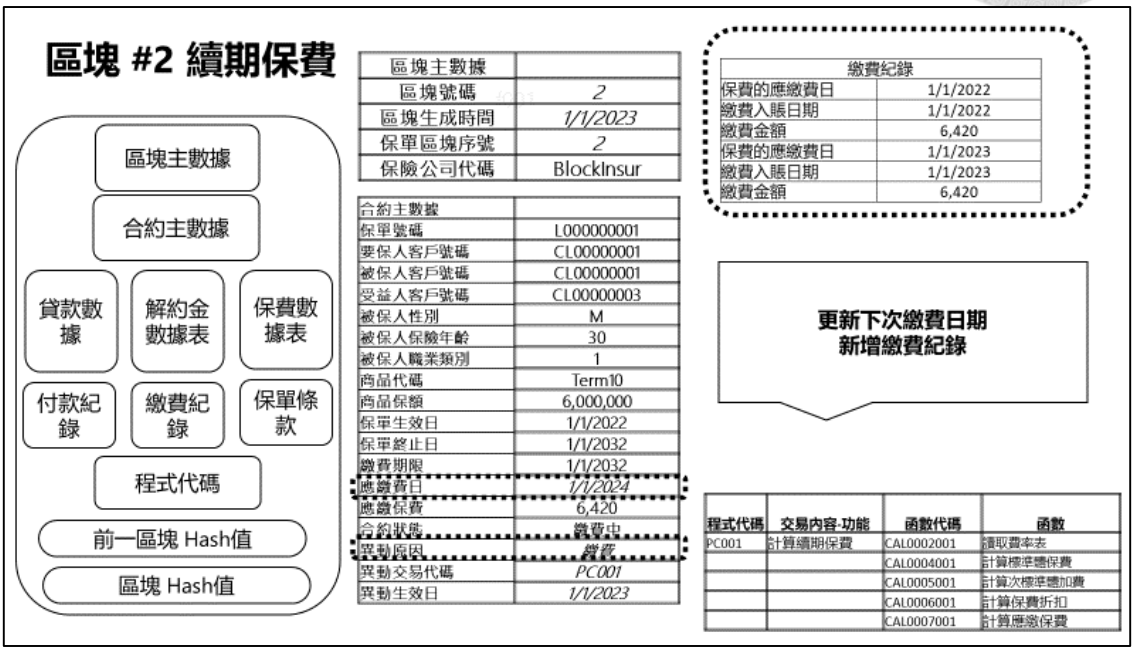


圖 4-2 繳 2023/1/1 續期保費

(三) 區塊#3：繳續期保費(如圖 4-3 所示)

繳 2024/1/1 續期保費，繳付完應繳費日變更為 2025/1/1，新增繳費紀錄。

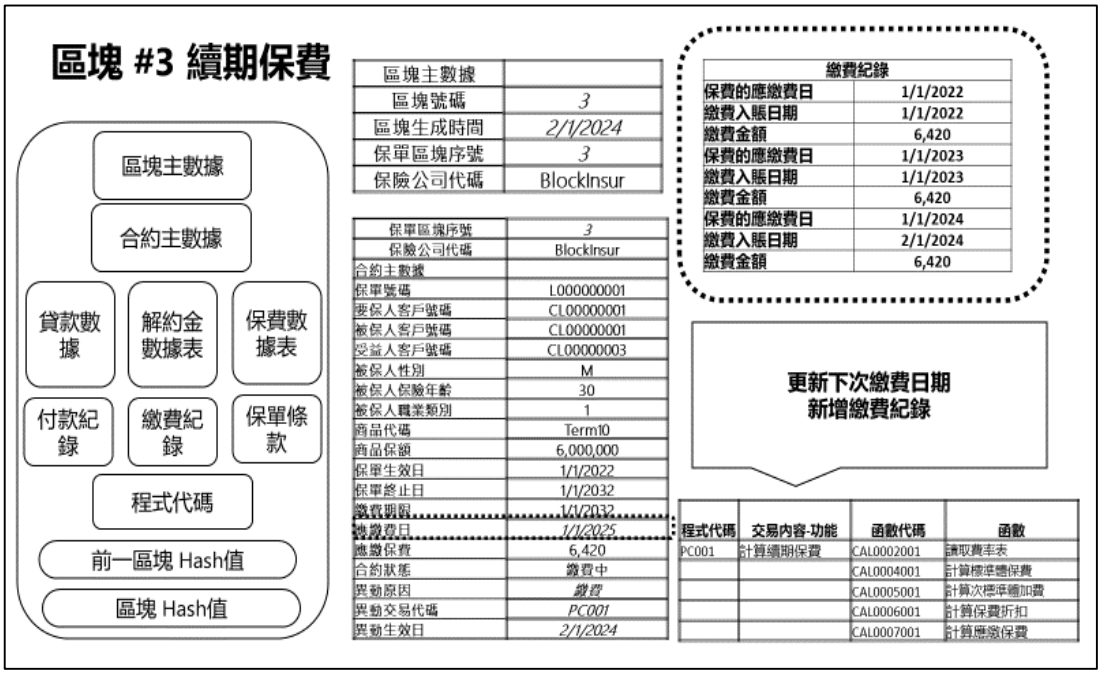


圖 4-3 繳 2024/1/1 續期保費

doi:10.6342/NTU202201323

(四) 區塊#4-降低保額 (如圖 4-4 所示)

降低保額由 600 萬降低為 500 萬，需要退回 100 萬元保額的解約金及未到期保費，保費亦需要變更為 500 萬元保額的保費。

在這個案例中，演示計算步驟說明保險商品規則的複雜，呼應第二章所提到的保險的規則非直觀。第一步需要計算保單年度，交易發生日在 2024/3/1 與生效日 2022/1/1 的時間為兩年兩個月，所以保單年度為 2，第二步索引解約金表，找出第二年度及第三年度 100 萬元保額的解約金，分別為 130 和 240，第三步用線性差值計算出 100 萬保額在 2024/3/17 的解約金為 148，第四步判斷客戶已經繳費到未來，所以需要退未到期的比例保費，先計算應繳費日到交易日這段期間的日數為 306，第五步計算 100 萬元的比例保費為 895，第六步加總解約金及未到期保費，退客戶金額為 1043(表 4-1 所示)並更新付款數據(如圖 4-5 所示)。

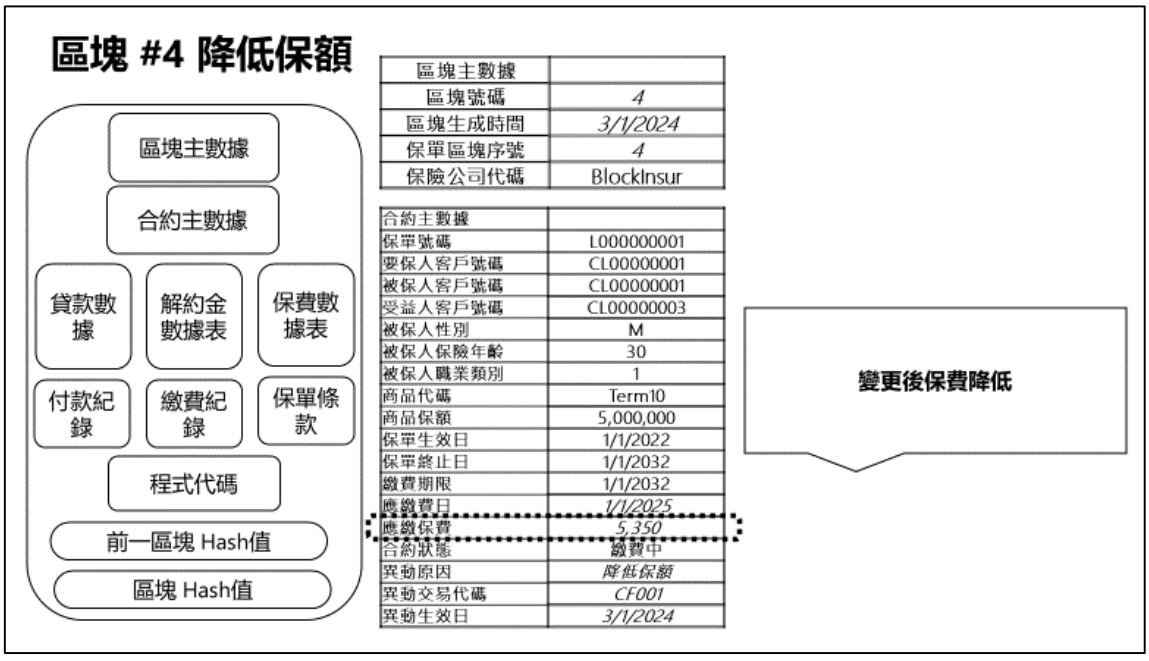


圖 4-4 降低保額主數據

doi:10.6342/NTU202201323

表 4-1 降低保額步驟說明

程式代碼	交易內容-功能	函數代碼	函數	計算過程
CF001	降低保額	CAL0008001	計算第t保單年度的t值 (變更日期-生效日期)	t= 2 2024/3/1 - 2022/1/1
		CAL0009001	讀取第t年度及第t+1年度解約金	1000000/100000=10 t年度:10*13=130 t+1年度:10*24 = 240
		CAL0010001	線性差值計算變更日期的解約金	(306/366)*130+(60/366)*240 = 148
		CAL0011001	計算變更日期到應繳費日的日數	d=306 2025/1/1 - 2024/3/1
		CAL0012001	計算應收保費或應退保費	6420/600*100 * (306/366) = 895
		CAL0013001	加總應退(應收保費)及解約金	148+895 = 1043

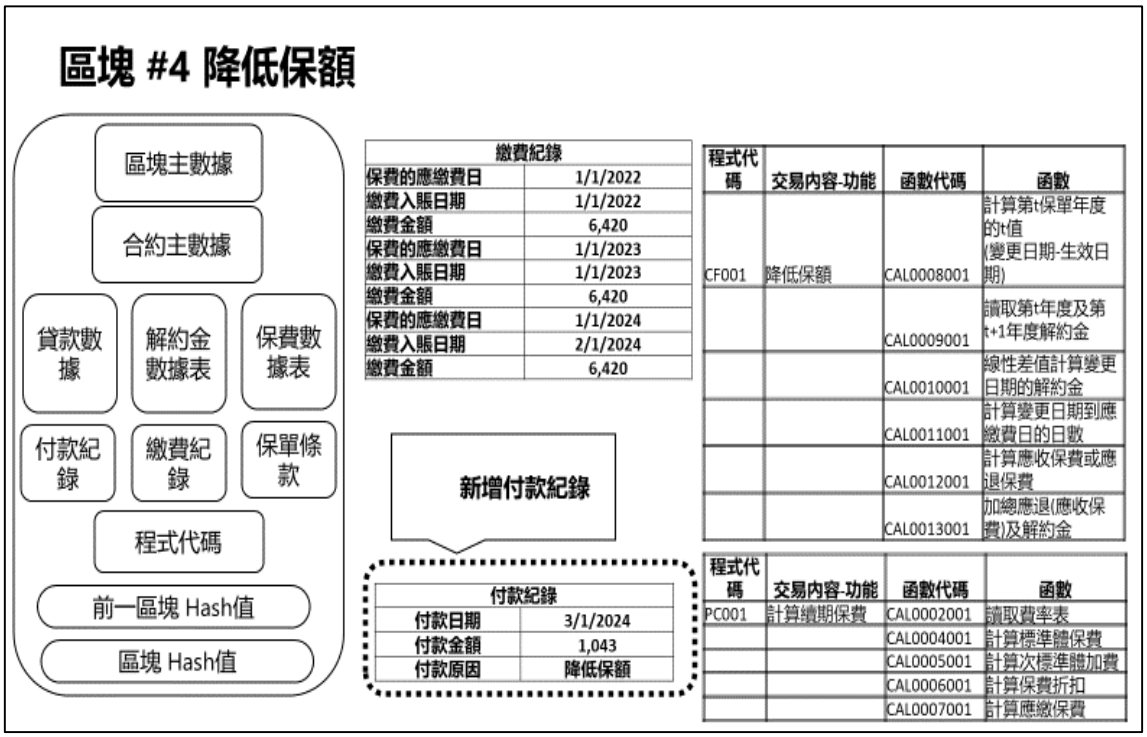


圖 4-5 降低保額付款資訊

(五) 區塊#5：保單貸款(如圖 4-6 及圖 4-7 所示)

保單具有解約金，可作為擔保品質押貸款。保險合約會記載貸款本金、貸款日及貸款利率。

doi:10.6342/NTU202201323

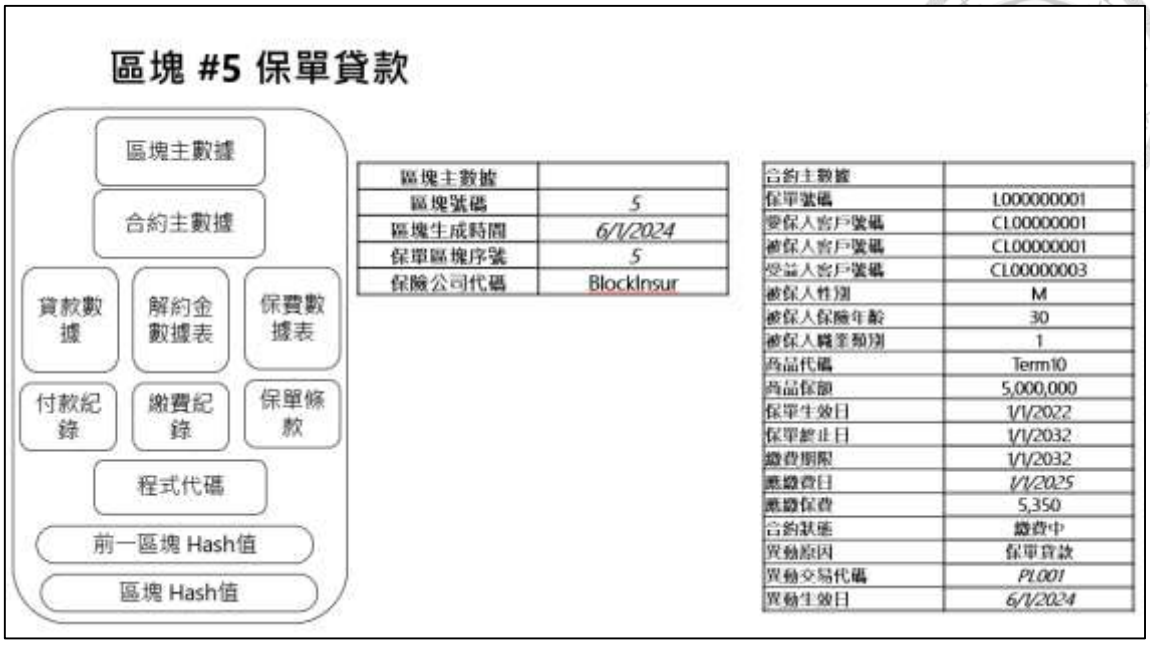


圖 4-6 保單貸款主數據

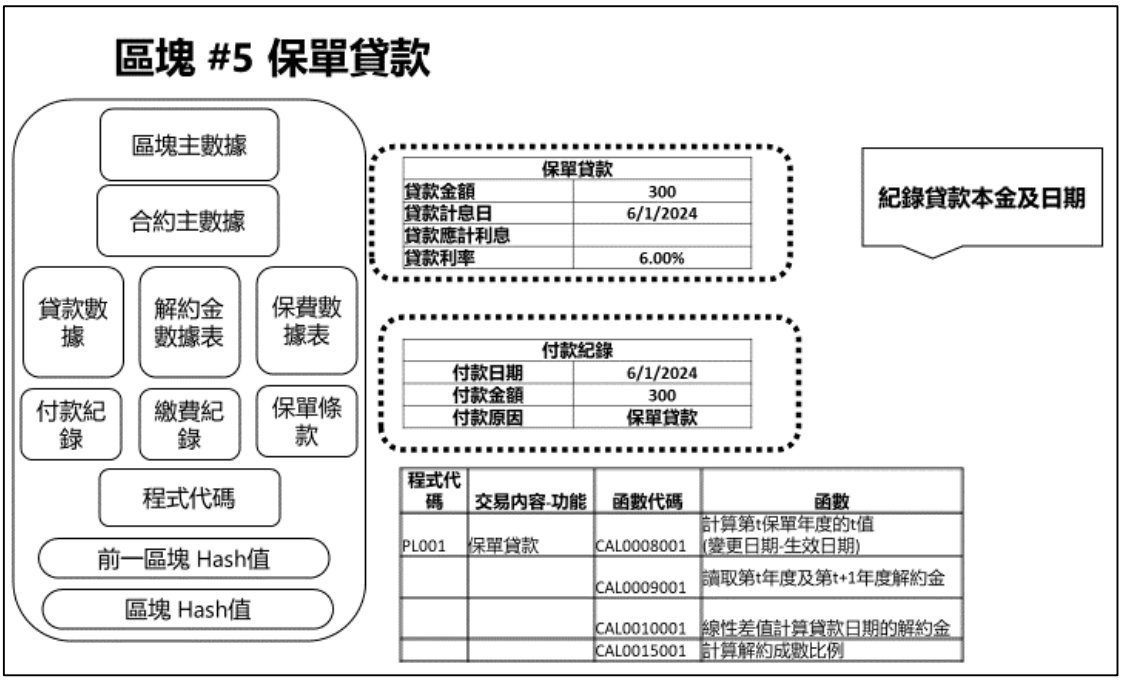


圖 4-7 保單貸款貸款數據

(六) 區塊#6：死亡理賠(如圖 4-8 及圖 4-9 所示)

被保險人死亡送件的時間一般會晚於真正死亡的時間，所以區塊創建的時間會晚於交易生效的日期(死亡日期)。

doi:10.6342/NTU202201323

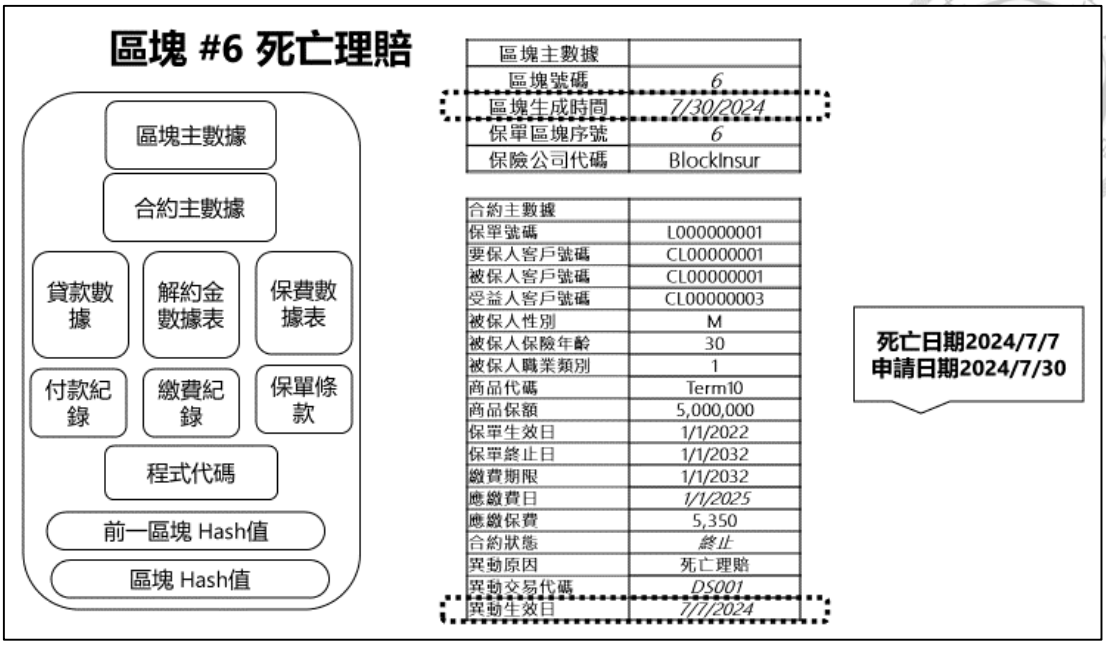


圖 4-8 死亡理賠主數據

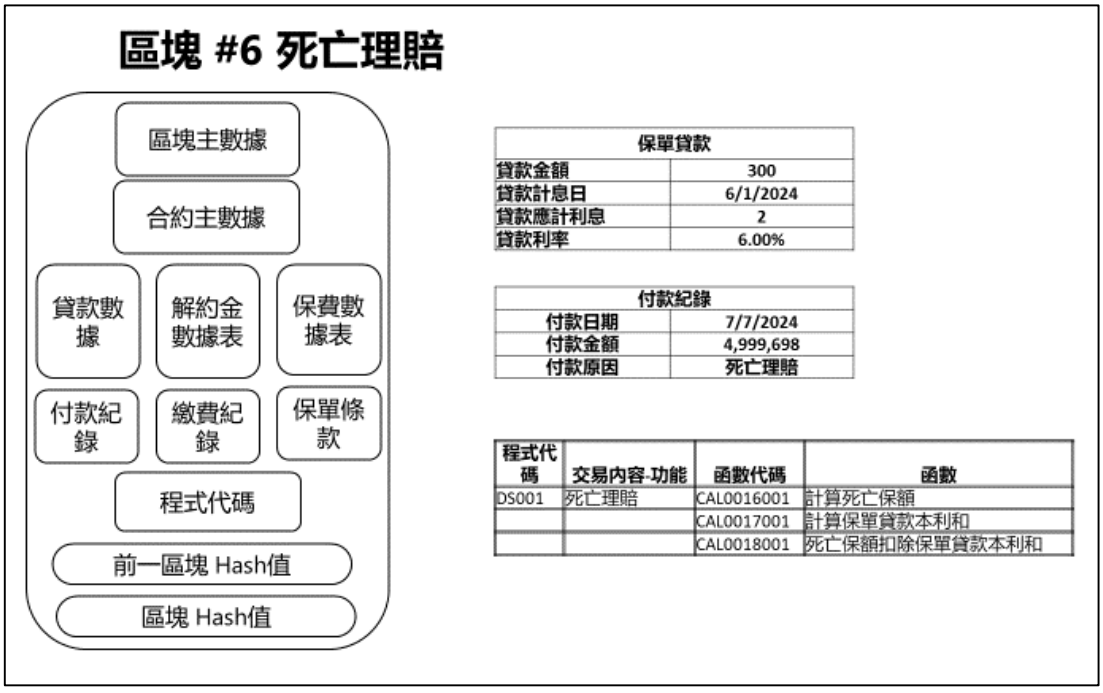


圖 4-9 死亡理賠付款數據

doi:10.6342/NTU202201323

三、差異比較

區塊鏈實現保險合約與現行方式較大的差異就是數據資料的保存方式的不同，現行的方式都是保留主數據就是保險合約的最新狀態，過去的資料變化會採用變更的歷史紀錄保存，如要推演完整的數據需要從最初的數據加上變更紀錄一條條數據推演，才會得到某個時間點的完整數據內容。而以區塊鏈的方式，每個區塊都是主數據，觀察數據會較直觀(如圖 4-10 所示)。另一方面用原始數據組合變更紀錄的方式推演每一個時間點合約的狀態，必須要由程式代碼加工，比較有機會產生錯誤。

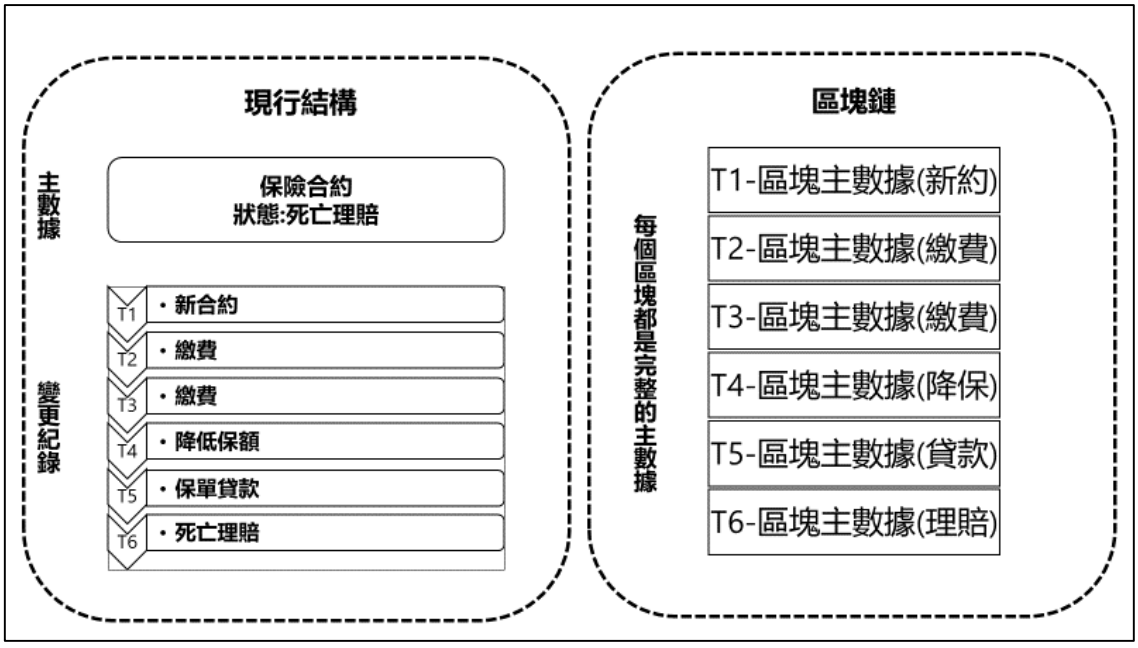


圖 4-10 現行模式與區塊鏈保險合約資料結構比較

doi:10.6342/NTU202201323

第二節 資料修正

在第二章介紹將程式代碼記載在區塊中，做為資料修正的方式，此小節演示步驟，另一部分保險公司經常會出現一種追朔交易的情境，例如客戶在 5/1 用銀行扣款繳交保費成功，可是客戶已經在 4/29 發生意外死亡，一般死亡申請會過一段時間才遞交到保險公司，情境是遞交到保險公司的申請日是 5/10，因為死亡的實際日期 4/29 在繳交保費之前，所以保費入帳這件交易需要被取消，其他些交易類似追朔時間承認某個交易亦可用套用在此模型，例如職業變更導致保費調整，後面保費入帳的需要取消，待職業變更完成後再重新按照新的保費入帳。在保險區塊上以主數據的異動生效日做為事件發生的先後順序 (如圖 4-11 所示)。

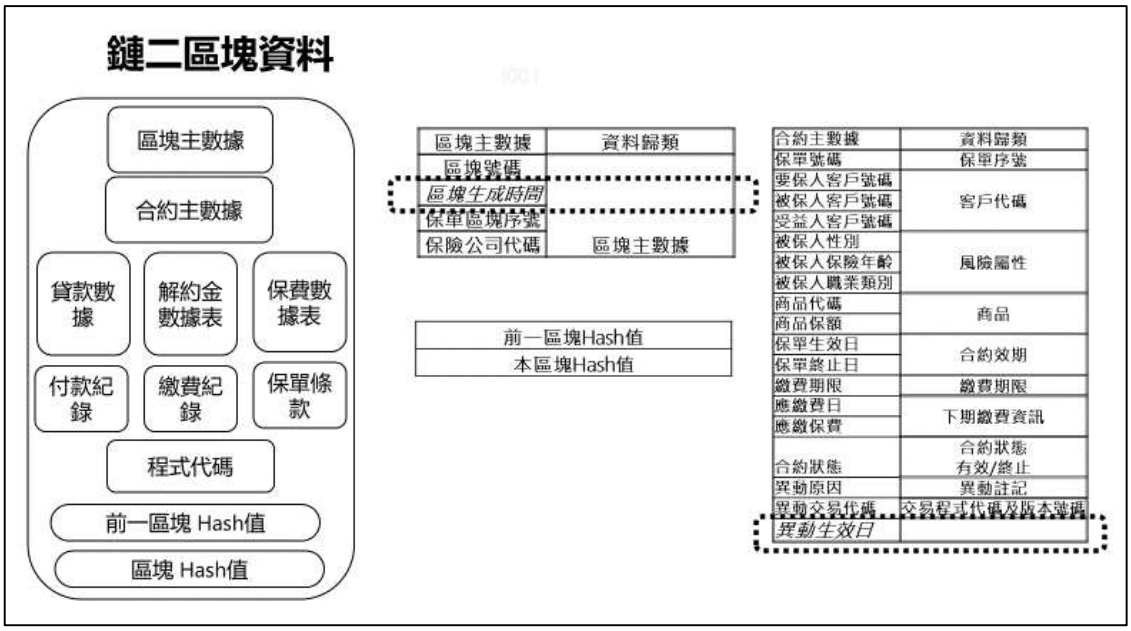


圖 4-11 異動生效日與區塊生成時間差異說明

一、新增過去的交易

新增一個異動交易日在過去的交易，並且已有區塊產生在此異動日之後(如圖 4-12 所示)。因為此交易異動日之後的區塊需要重新執行，方法是增加新的區塊按照順序返回到此新增加交易之前的區塊，區塊四是回到區塊二的狀態，區塊五是回到區塊一的狀態，再從區塊一依異動時間序產生交易 D、B、C 的區塊(如圖 4-13 所示)。

doi:10.6342/NTU202201323

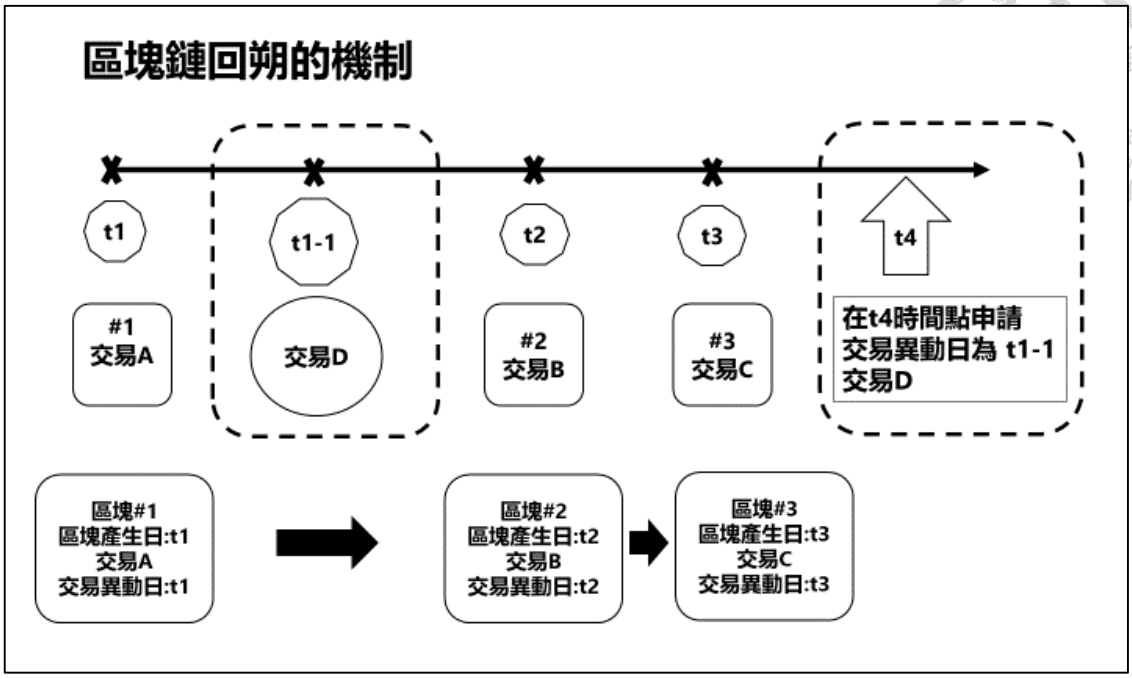


圖 4-12 資料回朔機制-1

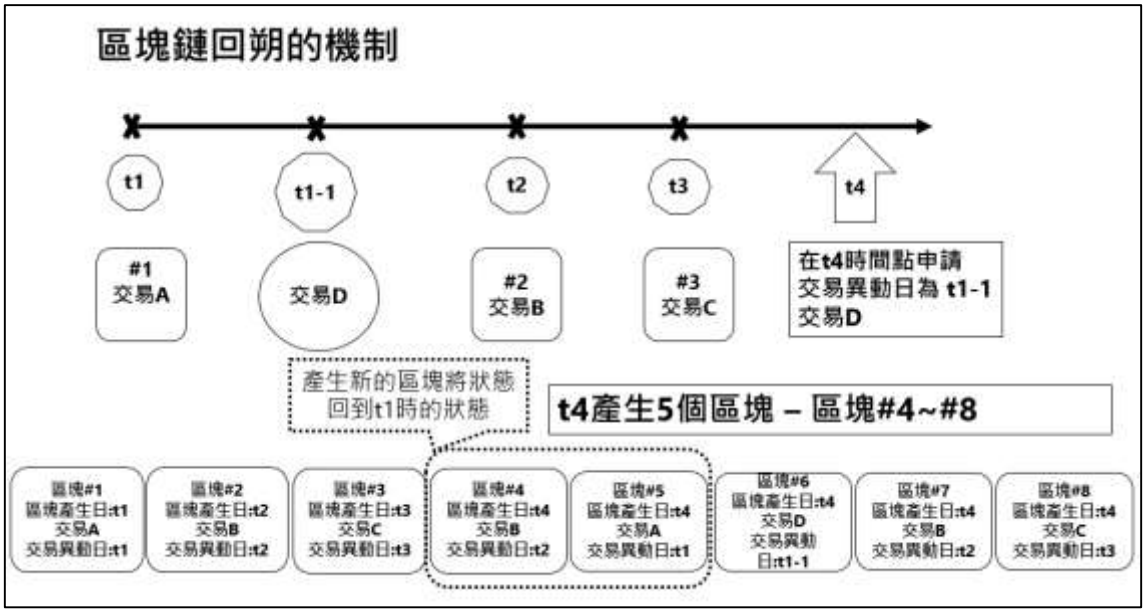


圖 4-13 資料回朔機制-2

二、修正程式錯誤的方式

依序在 t1，t2，t3 產生區塊，時間到了 t4 時，發現 t2 區塊的程式有錯，導致區塊二的數值 bx 和區塊三的數值 cx 不正確，在 t4 時間修正區塊二的程式版本由 G001 修正為 G002，依照前一節回朔的方式，產生新的區塊將狀態回到 t1 區塊的狀態，此時區塊二可使用正確的程式版本 G002 運行產生正確的數值 b，而區塊三

doi:10.6342/NTU202201323

依照用正確的程式版本執行會得到新的數值 c (如圖 4-14 所示)。

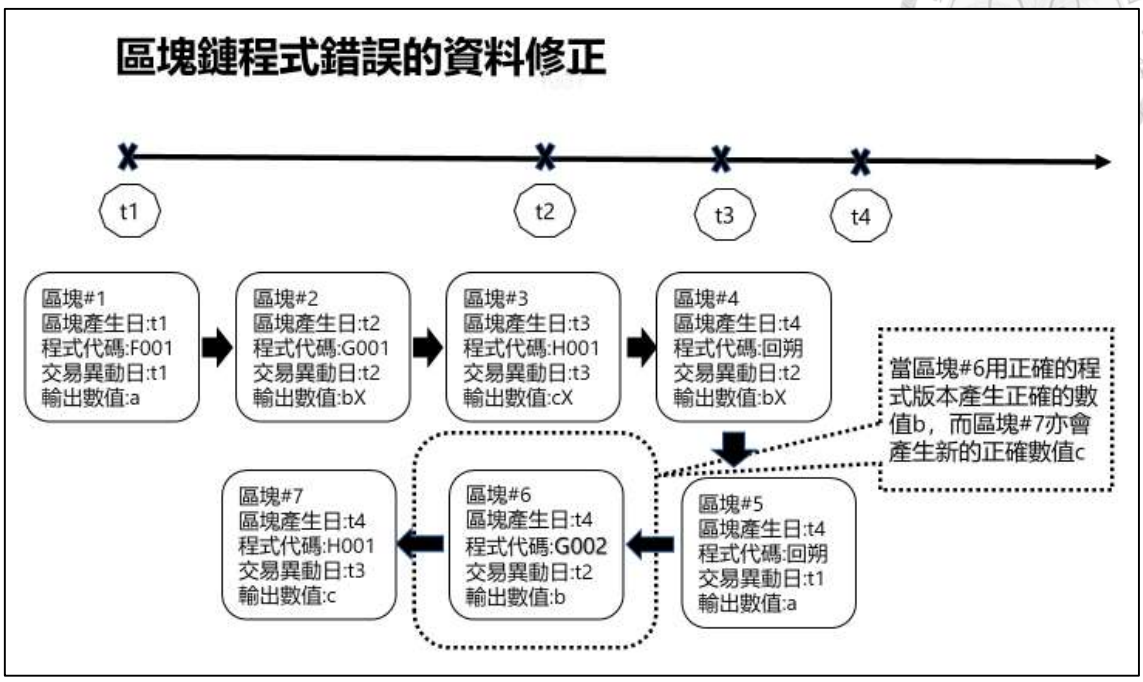


圖 4-14 資料修正機制

doi:10.6342/NTU202201323

第五章 結論與建議

第一節 研究結果

從第三章的架構及第四章的案例演練驗證可得到以下目標：

一、去個人識別化

利用兩個區塊鏈結構可以將保戶個人資料不在儲存在主鏈上，第一個區塊鏈也僅是保留無法識別個人資訊的碎片化資料，符合個人資料保護法的法令要求。

二、歷史資料保留完整且無法竄改

每個區塊保留上一個區塊的 HASH 值，歷史數據完整且不能竄改，具有透明度，提供良好的用戶體驗。

三、區塊完整記錄智能合約及交易結果

每個區塊記載此區塊的智能合約及結果，事後可以有效追蹤每個交易過程，讓複雜的保險合約不僅能夠記載每一個時間點的狀態，還能夠利用追朔的機制修正錯誤，修正的過程也一併被清晰的紀錄在每個區塊。

四、區塊的交易均由錄智能合約執行，杜絕人為介入可能的錯誤

區塊鏈上的每個交易均由智能合約或由 client 端的程序執行，杜絕人為介入可能發生的錯誤。

五、方向與 Gartner 及 TCS 專業報告相吻合

Gartner 研究報告提到到了 2030 年由於保險業務的經營模式及金融科技的發展，保險核心系統將會轉變為資料紀錄的功能，從這個角度區塊鏈是一個適當的選項，區塊鏈就是一個資料紀錄的平台，且具備隱蔽個人資料的功能。但是區塊鏈的智能合約也並不適合處理大量資料和太複雜的規則，必須簡化商品，呼應了 TATA 白皮書對於核心系統現代化應該簡化商品的論點。但這並非否定保險公司創新商品的策略。保險公司可以依商品屬性來配置到不同的鏈，例如年金合約鏈和意外險

doi:10.6342/NTU202201323

合約鏈，而客戶對於保險商品的體驗及需求可以在前台做功能分類及分流，保障型的商品是保險的基本需求，相對規則單純，可以以單一鏈的結構處理保險合約，而一些較特殊的商品如理財投資相關的商品，相對要客製一些服務或用多個鏈處理，將特殊處理或複雜的基金交易由特定的側鏈處理，主鏈與側鏈分工，但是這樣的架構設計需要做詳細的效能評估。對於不同種類商品整合的功能可以在前台處理，這樣的解決方案可以符合對不同的需求的客戶群達到效率與客製的服務。

從保險公司營運的角度，一旦保險合約在區塊鏈上運行，保險智能合約會自動執行，保險公司可以降低歷史保單維運的技術人員，將資源轉移到提升未來競爭力的金融科技。

doi:10.6342/NTU202201323

第二節 保險區塊鏈的潛力與未來發展

區塊鏈應用在保險合約除了可以達到上述的效果，還衍生了一些其他的可能性，但這需要異業結合或法令的配合，這些應當是保險智能合約其他的發展及優勢，以下是幾點是其他可發展性的優點。

一、各類應用服務容易整合

如 Gartner 報告中所提到，保險公司的營運需要與其他應用服務整合，如防詐欺、客戶理賠調查，這些需要核心系統提供資料，因為區塊鏈有現成開源的 API 可以快速佈署這些應用，需求單位只需要確認業務的規則或是需要調整規則，都能夠快速的佈署。

二、合作夥伴的整合會更有效率

保險公司在不同的業務流程需要與其他合作組織資料交換，如公會所需的統計報告、銀行通路的業績及佣金紀錄等，因為區塊鏈保留過去完整資料的特性，再授售予適當的權限，這些組織可以自行透過 API 由各自的資訊單位取得所需要的資料，取代以往雙方使用者單位各自與資訊單位溝通需求，再由兩邊的資訊單位互相溝通。

三、保險公司退場機制

超過百年經營人壽保險公司在國外比比皆是，但同樣的也有保險公司因為某些原因退場，將保單或公司出售給其他公司，台灣過去有幸福、國華、安泰等保險公司出售業務或被其他公司合併，合併前要估算被併購公司的資產負債，包含了保單的準備提存和未來的利差損，合併後要資料轉換到買方的核心系統，如以每個鏈處理同類型商品的機制，這兩個工程相對都相當容易，例如資料轉換每張保單僅需要產生新的區塊，將公司代碼轉換成新的公司即可，對客戶的溝通亦相對容易。

doi:10.6342/NTU202201323

四、保險平台的雛型

這項是第三點的延伸，保戶如果對原公司服務不滿意，想要將合約轉換到另一家公司，保戶可以跟其他公司商議，是否願意承接保單，如果願意，客戶可以在原公司解約，將解約金轉到新公司，如同行動電話攜碼到另一家電信公司，當然這其中還有是否因為詐欺行為被原保險公司主動解約的道德風險需要事先審查。

五、保單貸款不侷限於原保險公司

因為長期壽險多具有現金價值，保戶可以向保險公司質押貸款，貸款利率會參考保單預定利率及市場利率，在聯盟鏈的結構下，如果資料是共享，客戶可質押保單向其他保險公司或銀行貸款，取得較優惠的貸款利率。

六、保戶的自主性服務提高

在區塊鏈的架構下，保戶會更容易透過手持式設備檢視自己的保單，保險公司也可以省略信函的通知，保戶可以利用手持式裝置的行事曆同步保險公司需要告知的事項及日期，如繳費通知等，降低成本及提升整個服務的品質。

doi:10.6342/NTU202201323

第三節 結論

總結以上的論點，區塊鏈的架構是實現保險合約的一個很好的方向。根據以往的經驗中，保險公司會採用各類技術架構及科技應用來實現現代化或數位化的目標，這類的專案完成後在一定的時間內可以維持高效能的營運，但人壽保險公司經營可能長達一個世紀，未來商品的需求及外部經濟環境的變化往往都非當下可以預測，經歷了十年或二十年核心系統可能又將再面臨現代化的議題。在區塊鏈的結構下，保險合約的生命週期被完整的紀錄，同時同一個鏈上的節點都會保留一份同樣資料，客戶介面及智慧決策由其他平台整合，所有的功能類似積木的組裝，未來有新類型的商品可以容易設計不同的鏈並加入此架構，客戶的權益資訊可以很清晰的獲取，達到保險公司與客戶雙贏的局面。

doi:10.6342/NTU202201323

參考文獻

[1] 維基百科 (2022, May 9)。區塊鏈。https://zh.wikipedia.org/zhtw/%E5%8C%BA%E5%9D%97%E9%93%BE

[2] 維基百科 (2022, May 9)。超級帳本。https://zh.wikipedia.org/wiki/%E8%B6%85%E7%BA%A7%E8%B4%A6%E6%9C%AC

[3] 工商時報 (2020, September 9)。保險金給付出錯，台銀人壽挨罰 120 萬。https://ctee.com.tw/news/insurance/332826.html

[4] 彭笙榕 (2018)。*保險業應用區塊鏈技術之探討*。國立交通大學科技管理研究所碩士論文。

[5] 李冠諭 (2021)。*區塊鏈技術在外溢保單誘因回饋流程之設計*。輔仁大學資訊管理學系碩士班碩士論文.

[6] 林婉誼 (2021)。*被遺忘權與資料留存的悖論—以區塊鏈技術為中心*.國立政治大學科技管理與智慧財產研究所碩士論文.

[7] 立法院 (2015)。個人資料保護法。https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

[8] 田篦照博 (2018)。區塊鏈智慧合約開發與安全防護實作(朱浚賢譯)。旗標。

[9] 吳家揚 (2022)。投資型保險最重要的大小事。財經傳訊。

[10] 宋明哲 (2019)。圖解保險學。五南。

[11] Antonopoulos, Andreas M. (2017). Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media

[12] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. (2017). 區塊鏈：金融科技與創新 (蔡凱龍，王立恆譯)。財團法人台灣金融研訓院。

[13] Elli Androulaki et al. (2018, Apr 17). Hyperledger Fabric: *A Distributed Operating System for Permissioned Blockchains.* IBM. https://arxiv.org/pdf/1801.10228v1.pdf

[14] Eremenko, K. (2018, May 4). *How does Bitcoin/Blockchain Mining work?* https://medium.com/swlh/how-does-bitcoin-blockchain-mining-work-36db1c5cb55d

[15] Gill, S., & Harris-Ferrante, K. (2021, November 23). *Insurance business model evolution will reduce the role of core systems to record keepers by 2030*. Gartner

[16] Hyperledger Fabric official web site. https://hyperledger-fabric.readthedocs.io/en/release-2.4/whatis.html

[17] iThome (2020, August 4)。【雲端測試平臺將成未來創新試驗場】壽險公會如何打造區塊鏈聯盟鏈服務？https://www.ithome.com.tw/news/139141

[18] Juin Chiu (2020, Jul 6). *Hyperledger Fabric 獨特架構背後的設計哲學*。https://medium.com/bsos-taiwan/deep-dive-on-hyperledger-fabric-ed0c8578da2e

doi:10.6342/NTU202201323

[19] Phuwanai Thummavet (2019, May 2). *Demystifying Hyperledger Fabric (1/3): Fabric Architecture.* https://www.serial-coder.com/post/demystifying-hyperledger-fabric-fabric-architecture/#hyperledger-fabric-architecture

[20] Raghupathy, N P (2020). *Insurance products -decode, rationalize, and modernize* [White paper]. TATA Consulting Service. https://www.tcs.com/content/dam/tcs/pdf/Platform/bfsi-platforms/insurance-policy-administration-system.pdf

[21] Satoshi Nakamoto (2008) Bitcoin: *A Peer-to-Peer Electronic Cash System*.

doi:10.6342/NTU202201323