第一章

人類文明的發展和貨幣息息相關，先有了貨幣的種子，在這基礎上數位貨幣得到成長的條件，所以這一切都從**第一節 貨幣的起源**說起。中國，歐洲的希臘都是最古老的使用貨幣者，他們在貨幣的

改進上有著什麼樣的貢獻，而每當國家的國力失去優勢時，貨幣文化也跟隨著轉移了，貨幣的功能開始變化。**第二節 貨幣的價值與功能**，人類對於開始簡單的貨幣僅有的交換價值到賦予更多的使命，

使得貨幣不再單純化。什麼權力讓貨幣屬於國家的象徵？**第三節 鑄幣權，金本位，美元，不列敦森林協定**，這一連串的歷史改進，既然造就了人類空前的文明，也埋下了隱憂和災難，貨幣怎麼會失去了信任？ **第四節 失去信任的貨幣時代**，告訴我們貪婪的後果，人類濫用貨幣給自己造成的傷害。不過，人類依然不斷前進，所謂塞翁失馬焉知非福，沒有公權力的任意糟蹋貨幣，就不會有**第五節**

數位貨幣的興起。從短短的不到十年數位貨幣興起帶來的狂瀾，使得許多銀行家開始警覺，而各國監管機構也展開研究參與討論數位貨幣的屬性，到底數位貨幣是否是可以代表真實的貨幣呢？**第六節數位貨幣到底是不是真實貨幣**，從各種討論和觀點中，我們更可以肯定數位貨幣，就是人類最希望的貨幣，它將席捲金融，最終代替紙幣，塑膠貨幣，就像紙幣取代黃金，歷史告訴我們，這是不可能阻擋的洪流。

第二章

第一章討論了數位貨幣的來世與今生，很少述及它的核心技術－區塊鏈(Blockchain)，一個被2016世界經濟論壇譽為第四次工業革命的代表。數位貨幣的啟蒙者比特幣可能會最終被其他數位貨幣取代而消失，但是區塊鏈不會，它將是繼網際網路發明後另一個閃耀的明星，會照亮到下一個世紀。什麼是區塊鏈？我們從**第一節 區塊鏈的技術基礎**，了解區塊鏈，從純粹的技術角度來審視它，並用一個實際在數位貨幣上應用的例子來說明，區塊鏈不僅能夠為數位貨幣服務，它還有更多的功能，我們用了高盛與金融時報合作的研討會上的案例，說明他在其他金融解決方案的做法。不過，除了區塊鏈的技術創新，它的運作中有一些特殊性，是和其他系統不一樣的地方，它是一種創新的融合，融合運用了其他的科技，但究竟是如何集合運作，只是了解區塊鏈簡單運作原理，對於想進而參與區塊鏈的開發建制者而言是不足的。所以，我們接下來的五節分別對區塊鏈的主要特性一一說明，這五個章節代表未來區塊鏈發展的不同領域。在**第二節 分散式帳本**，說明區塊鏈的儲藏特性。一個和傳統資料處理大相逕庭，是區塊鏈的構建核心。**第三節 去中心化的網路結構**，我們習慣了中心化的思考去建立系統，去控制流程，去處理交易，排除障礙。而沒有中心的區塊鏈它是如何做到的呢？在區塊鏈的集體運作中密碼運用是讓一般非科技人士卻步的，我們盡量的簡單，**第四節 密碼學的基礎運用**。因為在後面一章還有更深的討論。區塊鏈沒有中心，為了形成一個能自治的管理機制，必須要引進智能，早期的區塊鏈已經有了智能合約的雛形，請看**第五節 智能化的管理**。**第六節 開放程式，共識的動力，平等精神**。會讓讀者感受到區塊鏈最偉大的地方，一個眾志成城，平等開放透明，幾乎讓人不敢相信世界仍存在一個烏托邦。最後，每一個

技術都有它的問題和缺陷，我們也發現區塊鏈運行了將近九年，它有很優秀的地方，難免也有不足，**第七節 不完美的區塊鏈**，指出區塊鏈在處理效率上的低落，耗費大量能源，以及版本更新都存在一些問題，這也正是給我們的機會讓我們能改進創新。

第三章

區塊鏈的關鍵核心技術，包括採用雜湊現金（Hashcash）演算法來進行工作量證明，讓區塊鏈中的各網點有機會參與驗證，達到公正性，且交易過程採用橢圓曲線數位簽章演算法來確保交易安全，並在每筆交易與每個區塊中使用多次Hash函數以及默克爾樹（Merkle Tree），不只是為了節省儲存空間，更重要的是藉由將前一個區塊的Hash值加入新區塊中，讓每個區塊環環相扣，也因此做到所謂的可追蹤且不可竄改的特性，同時也使用時間戳來確保唯一區塊序列的安全，以下便依序解釋這些關鍵技術及密碼學，共識機制簡介。

第四章

源於比特幣的區塊鏈技術，不僅為金融機構所重視，也逐漸為世界主要經濟體及重要國際組織所關注，在歡呼和質疑聲中，漸成聲勢。我們在第二章中不止說明瞭區塊鏈騰空的優勢，也敘述了區塊鏈的隱憂。區塊鏈畢竟成為顯學，許許多多的科技精英和天才不斷的努力改進之下，他們 除了基於新理論創造新的區塊鏈系統，如何最大化挖掘現有區塊鏈系統的潛力同樣重要。為解決比特幣擴展性問題，“側鏈”形成了除擴容外，最理想的解決方式。為解決比特幣性能瓶頸問題，“閃電網路”是一個可能的發展方向。“閃電網路”將大量的微小支付移到主鏈之外，形成多個支付處理中心。此外，更多的群集效果（grouping effects），這是目前最流行的現象，當一個耀眼的網路新明星吸引了目光，參加的開始區隔，展示了公有，私有，聯盟鏈，不同的區塊鏈模式也跟著蜂擁而至。甚至於為了一次解決所有對區塊鏈不滿意的技術方式，而希望一個圖靈完備的重新技術解決方案，以太坊是最重要的發展，它繼承了區塊鏈的基因，卻也完美的結合了其他集中化系統的基因，也是支持智能合約的極好平台，它對速率的提升和完整的系統框架，為圖靈完備做了最好的詮釋。

第五章

區塊鏈最初是應用在金融業上，而數位貨幣係建構在區塊鏈的底層技術平台上應運而生，本章非常適合從事金融業務行銷企劃暨管理人員的讀者來品味，筆者也試著儘量從業務發展的角度來整體通盤的闡釋科技，以期讀者能將其應用在實際的業務上。首先讀者須認知到金融科技創新（如數位貨幣與區塊鏈等）已是趨勢，誰先取得先機，誰即先取得優勢，另也針對一些重要名詞再重點的做了下說明，如數位貨幣、區塊鏈、比特幣、來特幣、瑞波幣及以太幣等；接下來介紹比特幣交易有那些參與者所組成來運作，包括礦工、用戶及交易所等；同時也對區塊鏈的連結與延伸做了應用說明，包括智能合約、側鏈與閃電網路等，以期區塊鏈之金融交易更能自動化處理、更廣泛運用及更適合數量大金額小的快速作業；再者，區塊鏈從公有區塊鏈演進到私有區塊鏈，而私有區塊鏈又可

再區分為公司私有區塊鏈與聯盟（合作伙伴）區塊鏈，另也特別介紹了與金融業有關連的R3CEV國際公司之聯盟（合作伙伴）區塊鏈應用；也許讀者會認為上述說明或與前述之章節內容有所重複，但筆者係從業務應用面所關切的角度來彙總簡要說明，以期與本章最後的金融應用做連結呼應，亦即數位貨幣與區塊鏈在國際上金融業的應用暨台灣金融業上的選擇應用，範圍包括了銀行業、證券業與保險業等三方面，其中又以銀行業著墨較深，實因銀行業是最先被提出來應用的。筆者也期望經由如此循序漸進的鋪陳，能給讀者在業務面上，勾勒出一個整體性的概念與思維，並以此為藍本，進而激盪出改良式的創新與應用。

第六章

在所有的產業當中，金融業應是屬於被各國主管機關所高度監理的行業，而金融業之內部組織亦設有獨立的稽核與遵法單位，負責來監理金融業務，以期符合法令規章與內部控制制度，並保護消費者之權益。在面對數位貨幣與區塊鏈的破壞式創新，如何適當與有效的監理，俾利科技及業務兩者與時俱進，並滿足消費者各項需求與體驗，其將對未來金融科技創新的發展影響深遠，亦考驗著主管監理當局的智慧，不可不慎。本章主要適合從事金融業之稽核與遵法人員的讀者來品味，首先介紹破壞式金融創新（數位貨幣與區塊鏈）來勢洶洶，監理主管機關應儘速迎頭趕上建立規範機制；接下來說明各國政府（包括美國、中國、俄國、德國、英國、日本、加拿大、韓國、泰國、台灣等）對數位貨幣與區塊鏈所持的態度與因應；再者，談到本章的重點，即各國的金融監理沙盒機制，監理沙盒為在金融軟體開發的過程中，建構一個與外界環境隔絕的測試環境，讓參與者可在其內盡情的測試各項軟體功能並受主管機關監理之，其規範的嚴謹與寬鬆各有不同，唯皆鼓勵創新，另金融監理沙盒首創於英國，各國適用的對象或有差異，包括英國、新加坡及台灣適用於金融及非金融業，澳大利亞限非金融業，香港限銀行業等，亦皆分別做了說明；最後，對開放與監理之間的取捨，提出些許建議，以期科技創新、業務發展與監督管理等三方面均能有所取捨與均衡，俾利取得一致
的共識，共謀多贏的前景。

第七章

前面幾章對數位貨幣的發展與區塊鏈技術有完整的說明，對金融產業的應用也有詳細的闡述，本章將介紹數位貨幣與區塊鏈技術對經濟生態的影響，希望讀者能夠對數位貨幣與區塊鏈技術的應用，有更進一步的認識與了解。本章首先介紹數位貨幣與區塊鏈的發展概況，接者說明數位貨幣與區塊鏈創新主要發展方向與應用案例，政府如何善用區塊鏈技術提升服務品質，以及未來數位貨幣與區塊鏈技術的發展，相信在技術、成本、利益、法規、安全、便利等諸多因素的考量下，數位貨幣與區塊鏈將逐漸實際應用在各個領域。

第八章

在2017年已經很清楚的看到數位貨幣與區塊鏈技術將帶給許多產業更安全、更有效率、

更低成本的交易方式，當然也包括政府服務。全世界都關注數位貨幣與區塊鏈的發展，許多國家也都投入資金及人力在這一個領域，台灣在這一輪新科技的競爭中，當然也不會缺席。這一章說明台灣在數位貨幣與區塊鏈做了甚麼？其他國家或企業有沒有一些值得我們學習效仿的發展歷程？我們如何掌握這次的機會與克服挑戰？希望這些分析能夠給有興趣的讀者帶來一些想法與回響。