邁向智慧政府與智慧學校之泛用型區塊鏈網路設計方法

夏肇毅(Chao-Yih Hsia)
晶智能中心 CubicPower.idv.tw
chaoyihhsia@gmail.com

摘要

區塊鏈的分散式帳本技術DLTs，可以應用到加密貨幣 Cryptocurrency 上並能進一步提供智能合約Smart Contract的功能 。它提供了分散式容錯性的架構與對資料不可篡改性的保護，相對的也付出了性能，運算力與資料量的代價。本文對分散式帳本技術的內涵與使用案例做了些簡單介紹，並針對應用到智慧政府與智慧學校的目標，提出了泛用型區塊鏈設計方法與簡單實作示範。讀者可以此文為出發點，對其技術與工具的應用再做深入研究，必能產生實際可用的智慧政府與智慧學校應用案例。

Abstract

The distributed ledger technologies (DLTs) based on blockchain technologies can be used on cryptocurrencies and also provide smart contract functionalities with a distributed architecture and the immutability of data. This article briefs the blockchain technologies and presents a general blockchain network design methodology for building smart government and smart school applications. A demo of building applications with Hyperledger Composer Playground is also included.

關鍵詞：區塊鏈, Blockchain, 分散式帳本技術, 加密貨幣, 智能合約, Hyperledger, 超級帳本, 金融科技, Fintech.

1. 前言

近年來金融科技風起雲湧，傳統金融業數位轉型蔚為風潮[1]。金融科技依照世界經濟論壇(World Economic Forum, WEF) 的金融服務業未來報告書所描述，包括有支付、保險、存放款、資本募集、投資管理以及市場資訊供應六個主要方向。政府、學界及業界不斷舉辦競賽來蒐集應用場景，慢慢地這些應用都已為金融業者所採納實現，因而就漸漸移出創新應用的焦點。到最近兩三年，隨著以比特幣為首的加密貨幣與ICO興起，接著也帶動起另一股區塊鏈熱潮。

本文的目的，是要提供一個如何針對泛用型(非單指加密貨幣)的應用，來設計區塊鏈網路的方法。報告的方式，是先簡介區塊鏈的前因後果，讓大家對區塊鏈技術有個基本的認識。同時也能了解區塊鏈技術的長處與限制，以便能針對其優點發展，而對其缺點有所因應。最後再以實例展示如何對智慧政府與智慧學校這種泛用型應用來設計一個區塊鏈網路。

自2009年比特幣Bitcoin發行開始[2]，加密貨幣Cryptocurrency就慢慢的發展起來。由2010年5月22日有人用1萬比特幣買到兩盒披薩起，逐漸加溫後爆熱。到2017年底達到歷史高點1比特幣近2萬美金，之後又曾崩跌七成。

比特幣使用的技術就是區塊鏈。所謂區塊鏈，就是把帳本資料紀錄在一塊塊的區塊中，然後再用特殊的方法將它連結成一個長長的鏈。在後面支撐這區塊鏈的，就是分散式帳本技術DLTs (Distributed Ledger Technologies)。有了區塊鏈後還要用Peer to Peer (P2P)網路把自己的帳本傳給他人分享。在裡面每個人都能修改帳本，但要聽誰的呢? 於是就發明了共識機制，在比特幣中用的是PoW(Proof of Work) 誰算得最快，做出最長的鏈，就聽他的，同時也給找出每個新區塊的人一定數量的比特幣做為獎勵。所以大家就投資硬體並結盟一起，搶當算力最高的人，以賺取比特幣酬勞。

在比特幣中定義，一個電子貨幣為一個簽章鏈。某個電子貨幣的擁有者將它轉移給下一個擁有者時，會對前次交易與下個擁有者的公鑰做hash再加以數位簽章，並加到電子貨幣底端，收款人對這數位簽章驗章來驗證該鏈的所有權。這過程表示如下:

付款人(*擁有者*):
擁有者簽名 = *簽章*(
(*交易*
+ *公鑰*(*擁有者* $_{+1}$)),
私鑰(*擁有*)
)

收款人(*擁有者* $_{+1}$):
驗章(
擁有者簽名 ,
公鑰(*擁有者*)
)

若要確認這個電子貨幣未被使用過，收款人就必須驗證過去的所有交易。有一種驗證方式是去建立驗證中心，讓它存著過去所有交易來確認某個電子貨幣是否被使用過。但為了達成去中心化目的，比特幣不用驗證中心的集中式驗證，而採用將所有交易紀錄傳給所有參與者自行驗證的方式。

比特幣在每個區塊內持續增加區塊中名為nonce的數值，直到這區塊的hash值是以一定數目的0起頭為止。這所需要的運算能力，與起頭為0的數目成指數級相關。因為這區塊的hash值會被帶到下一區塊，所以若有人想要竄改前面區塊的內容，則它必須花費大量計算能力來重新計算該點以後所有區塊的hash值。
因為是去中心化設計，最後要靠大家來決定要用誰計算出來的結果。其中的規則就是取用最長鏈，誰控制最多節點的算力，誰就能算出最長鏈。比特幣會控制系統讓當前算力在每10分鐘能產生一個區塊的程度。再加上傳輸驗證等因素，所以通常要六個循環，也就是一個鐘頭後才能確認交易已完成。

區塊鏈的另一個要角是乙太坊。它是個區塊鏈智能合約平台，應用程式在乙太坊虛擬機 EVM (Ethereum Virtual Machine) 中執行。乙太坊的區塊產生間隔降低到15秒左右，加上智能合約的出現，讓區塊鏈應用從單純的貨幣拓展到各行各業上。

比特幣中使用 UTXO (Unspent Transaction Outputs) Model，要把以前的交易加起來才知道各帳戶餘額。乙太坊所使用的 Account Model 就像銀行帳戶一樣，交易完會把帳戶餘額紀錄在區塊鏈當中，所以適合智能合約的發展。

比特幣是在公用網路上運作，所以需要用共識機制來確保不易被竄改，這種方式叫公有鏈 (Public blockchains)。相對有些完全在私人領域中運行的區塊鏈網路，就是私有鏈 (Private blockchain)。介於中間的就是聯盟鏈 (Consortium blockchains)。加入聯盟需申請，不對外開放，運作上有權限控管的機制。比特幣的PoW共識機制是最為人詬病的問題，因為它消耗了大量的能源。而性能問題又是公有鏈的共同弱點，比特幣最快每秒鐘只能處理7筆交易，乙太坊每秒20筆。而聯盟鏈性能較佳，可達每秒1000筆交易左右[8]。

2. 採用區塊鏈的業務實例

2018年3月，環球銀行金融電信協會SWIFT完成與34家銀行間，以分散式帳本提供國外同業帳戶 (Nostro Accounts) 即時可見性的概念驗證PoC［3］。它以 Hyperledger Fabric 1.0製作，提供了即時事件處理，交易狀態更新，完整監督紀錄，預期與可用結餘的可見性，即時簡易帳戶輸入確認，標示未完成輸入與相關問題與產生資料支援監管報表等功能。在PoC時，有28家銀行實際在沙箱中建立了528個Channels來測試。日後若要在生產環境中運作，則需建立達100,000個以上的 Channels。

國外一般在證券交易之後，紀錄就會傳送給清算單位。他們會比對買賣方紀錄，並確認雙方同意該條件。若有出入，清算單位會向交易單位報告以嘗試解決。清算流程結束後，就是結算。結算單位向買方收取現金，並向賣方收取證券。最後並交付證券給買方，以及現金給賣方。

歐洲央行在2016年提出了運用分散式帳本技術 (DLTs)在證券交易後業務的分析報告。報告中提到證券交易後功能(post-trading functions) 包括：保存帳戶(保管/登記)，檢查投資人控制資產的權利(KYC了解客戶與AML反洗錢)，交易結算前傳送及對帳(清算)，幫助結算及對沖結算風險，直到資金與證券轉移結束(風險管理)，執行參與交易者資金與證券轉移義務(結算)，確認發行完善並避免未授權的的證券產生(公證)，避免私人資訊被偷，惡意修改與阻斷服務(網路安全)，以及管理發行者事件及對投資人的影響(資產服務)。

在歐洲央行報告中分析，如果利用分散式帳本技術，因為每一節點都保存一份資料，而使得資訊重複最大化。同時因為必須在多方中達成共識，所以比起集中式資料庫技術，這限制了它的結算的速度。但就算是使用現成的中央式資料庫技術，如果各單位的資料庫間缺乏互用性，依舊讓交易後流程緩慢。

2018年1月，IBM與全球最大貨櫃運輸公司馬士基航運公司宣布合資意願，將以區塊鏈技術來提供安全且有效率的貿易系統[5]。原本的流程是由很多單位間，以點對點的方式溝通。新系統要將所有單位連在一起，做資訊整合。這中間所帶來的好處，與傳統的SOA(service-oriented architecture)解決方案類似，人為審批程序仍為效能最大障礙。只有做到end-to-end自動化的STP (Straight-through processing) 讓流程自動跑完，才有機會達到最大效益。

3. Hyperledger超級帳本區塊鏈平台

Linux基金會在2016年開始Hyperledger開源專案社群，用來建立區塊鏈框架與平台。希望以區塊鏈技術建立分享帳簿資料庫(Shared Ledger Database)應用在金融，健康與供應鏈上。主要的框架專案有由Digital Asset, Blockstream 與 IBM 所提供的 Hyperledger Fabric 與 Intel 提供的 Hyperledger Sawtooth。育成中的開發工具有 HyperLedger Composer 與 HyperLedger Explorer 等專案。

其中Hyperledger Composer是一個快速建立區塊鏈應用模型的工具[6]。它讓使用者能很快地把使用情境中的業務邏輯建立使用範例，用來測試這解決方案的可行性與潛在問題。最後它會產生一個網頁服務器來和 Hyperledger Fabric 溝通，讓整個區塊鏈網路運作起來。 Hyperledger Fabric 是一個模組式框架，可加入共識及會員服務，並執行智能合約程式。

在Hyperledger Composer的一般業務情境中，都會有供交易的資產 (Assets) 。這可能是貨物，財產或服務。然後還有讓資產轉換擁有者的交易(Transactions)過程，以及交易的參與者 (Participants) 。舉例來說，在拍賣網站裡，Assets就是拍賣品，Participants 就是買家與賣家，而Transactions 就是成交紀錄。使用者就是利用這模式來建立區塊鏈應用。

4. 智慧政府與智慧學校區塊鏈應用設計探討

要推展區塊鏈分散式帳本技術DLTs到智慧政府與智慧學校的應用時，首先要了解現有不同性質的資料庫架構，包括：

-獨立分散資料庫

各自為政，無互操作性。如現行各單位的電腦中心，應付本身業務需求即可，各自獨立運作。針對單位資料交換的需要，會有通訊閘道的設立。

-集中式資料庫

所有資料全都匯集到中央資料庫。

-中央控管分散式資料庫

集中式資料控管，分區資料儲藏，由中央控制修正權。主要是處於不同地理區的單位，中間連線會有頻寬限制。所以平時就近存取資料，利用Replication Server 複製技術，將重要變動資料傳向他處。

如果原來是各自為政，無互操作性的獨立分散資料庫，那麼建立區塊鏈DLTs網路所帶來的好處，主要還是資訊整合的效益，也許改用中央控管分散式資料庫架構會性能更好。當要追求的是不易竄改的安全性時，那麼建立區塊鏈DLTs才有價值。所以貴重，有價值，有所有權的項目才是我們尋找的目標。譬如資產的轉移，學位的授予，資格的擁有，分數的評斷等。我們把這些值得妥善保管的標的先統稱為資產Assets。

有了值得保存的目標後，通常他們的所有權會轉移。資產的轉移要經過交換的過程，看要一手交錢一手交貨，還是要先享受後付款。通常都是要拿等值的資產來交換，我們把這過程稱為交易(Transactions)，而參與交易的人為參與者(Participants) 。

就好比一輛汽車，在今天由甲賣給乙N元。這其中Asset 是汽車，Participants 有甲和乙。而
在這 Transaction 裡記錄著:

- 資產 = 汽車
- 賣方 = 甲
- 買方 = 乙
- 總額 = N元
- 日期 = 今天

這就是一筆交易紀錄。

用這個資產轉移交易模式，我們可以設想一些智慧政府中能應用區塊鏈的例子。如債券發行網路，基金結算網路，信用狀網路，房地交易網路，拍賣市場網路，貨品交易網路，寶石交易網路，身分資料展示網路，就診資料網路和汽車履歷網路等。在交易的內容上，除了做權利的轉移外，還可以做發行，廢止，開放或撤銷等不同動作。比如說證券，公司可以發行股票，交易所可以讓股票上市。投資人可以買賣股票，交易所可以讓股票下市，公司可將股票買回。各種不同交易都可以設計在Transactions裡設計。

而當發展智慧學校應用時，可以先構想一些可以轉移的資產，如學號，學分，學位。學校每年發行一定數量的學號，讓新生來取得。同時也發行不同學分讓學生來取得，同時記錄成績。最後累積一定學分後，就取得學位。之後這學號就註銷，不再作用，僅供查詢之用。

到這裡應該就能略略體會區塊鏈與一般資料庫不一樣的應用實現方式了。

5. 泛用型區塊鏈應用開發步驟

在區塊鏈發展的過程中，一般稱區塊鏈1.0是加密貨幣應用，區塊鏈2.0是智能合約在金融及產權上的應用。而到了區塊鏈3.0，就是將區塊鏈應用到各行各業上。本文的泛用型區塊鏈網路，指的就是在區塊鏈3.0上的應用。它的設計目標，就是把一般應用的資料庫層轉換成一個DLT區塊鏈網路層。所以開發的方法還是承襲傳統的方式，只是把資料庫建模過程改成區塊鏈智能合約建模。所以針對一個泛用型的區塊鏈網路開發，應該有以下步驟:

-必要性與可行性分析:

- 篩選目標專案群，挑出值得使用DLTs保存重要資料的專案。之後按規模大小，必要性與急迫性排出優先次序。

-架構規劃

- 了解 HyperLedger Fabric 架構與性能
- 根據專案規模，容量，速度，需求來規劃適合的架構
- 利用 HyperLedger Composer 練習區塊鏈建模概念

-系統分析(SA)

- 篩選能交易所有權且值得轉換到區塊鏈保存的資產項目
- 挑選可完全轉換到區塊鏈的原有的應用網頁
- 確認所篩選的資產資料完備，能滿足功能需求
- 利用智能合約當資產資料載體

-系統設計(SD)

- 訂定智能合約規格
- 將原有SQL資料表對應定義到智能合約內
- 設計滿足應用需求的操作API規格
- 將此區塊鏈 API 視為資料介面層與 DB2, Oracle, MSSQL, MySQL, NoSQL 對等相對應
- 上層的Web應用可選擇任何一種資料介面層
- 開發時再一步步的將原有SQL API 轉到區塊鏈API 上
- 利用原有的應用網頁做功能測試

-開發(Implemantation)

用Hyperledger Composer來產生解決方案的步驟為:

- 建立業務網路結構: 定義資料模型，業務邏輯以及存取控制規則。
- 定義業務網路: 一個業務網路包括資產，交易，參與者，存取控制規則，事件與查詢。
- 產生業務網路檔
- 部署業務網路
- 產生業務網路服務器
- 產生應用程式

-測試(Test)

-部署(Deployment)

6. 應用Hyperledger Composer建模範例

利用Hyperledger Composer所提供的Playground［7］，我們可以隨手驗證一下區塊鏈網路的業務模型。

進入Hyperledger Composer 所提供的Playground。修改 Model File，在SampleAsset內新增Address 與Type。

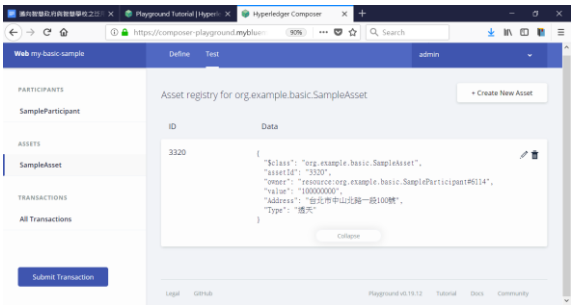
```
asset SampleAsset identified by assetId {
        o String assetId
        --> SampleParticipant owner
        o String value
        o String Address
        o String Type
}
```

在SampleTransaction 內新增buyer 與seller。

```
transaction SampleTransaction {
        --> SampleAsset asset
        o String newValue
        --> SampleParticipant buyer
        --> SampleParticipant seller
}
```

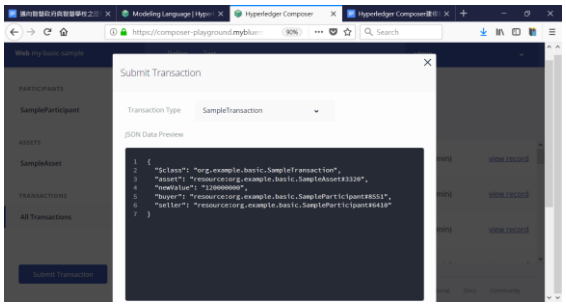
其中符號"o"表示資料欄位，而"-->"表示物件連結指標，與資料庫中的外鍵類似。

點選Test tab後，再點Create New Participant。
點選Create New Asset 後輸入資料，可見完成資產輸入後的畫面(圖一)。



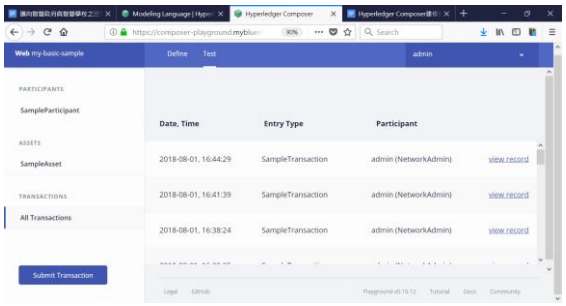
圖一：完成資產輸入

點選Submit Transaction 來做交易(圖二)。



圖二：新增交易

之後便可見所有交易(圖三)。



圖三：交易後結果

這這過程中，我們可以看到如同資料庫欄位的定義，也能看到像資料庫正規化後的外鍵連結。多練習一下，應該很快就能得到如何將資料庫轉到智能合約的概念了。

7. 結論

本文中討論了在智慧政府與智慧學校可應用區塊鏈技術來保存資料的標的，提出了以在Hyperledge平台上使用Hyperledger Composer建模的方式來驗證泛用型區塊鏈網路想法的可行性。之後再一路由系統分析，系統設計，開發，測試到部署的步驟，來設計泛用型區塊鏈應用。並提供了操作實例以供依循。同時也討論了區塊鏈網路的DLTs分散式帳本技術並非百利無一害的選項，採用之前需要深入了解該解決方案的長處與限制。先慎重篩選出必須妥善保存的資料後，再執行本文的泛用型區塊鏈網路設計步驟，將能收事半功倍的成效。

參考文獻

[1] 夏肇毅,”推動Fintech金融科技發展風潮的科技動力探索”, NCS 2017全國計算機

會議論文集, DOI: 10.29428/9789860544169.201801.0100
[2] Nakamoto, Satoshi ,"Bitcoin: A Peer-to-Peer Electronic Cash System",2008
[3] SWIFT,"SWIFT completes landmark DLT proof of concept",2018
[4] European Central Bank,"Distributed ledger technologies in securities post-trading",2016
[5] IBM,"A global trade platform using blockchain technology aimed at improving the cost of transportation, lack of visibility and inefficiencies with paper-based processes", 2018
[6] The Linux Foundation,"Hyperledger Composer"
[7] The Linux Foundation,"Hyperledger Composer Playground"
[8] Forbes,"The Problems With Bitcoin And The Future Of Blockchain",2018