應用區塊鏈技術建構機車資產管理與交易平台
Constructing Motorcycle Asset Management and Trading Platform via Block chain

黃志泰	陳祈勳	林聖峯	曾宥翔
Chih-Tai Huang	Chi-Shiun Chen	Sheng-Feng Lin	Yu-Hsiang Tseng
德明財經科技大學	德明財經科技大學	德明財經科技大學	德明財經科技大學
資訊管理系	資訊管理系	資訊管理系	資訊管理系
副教授	學生	學生	學生
hgt@ takming.edu.tw	Chen850506@gmail.com	gamer99122@hotmail.com.tw	Sean850619@icloud.com

陳昱翰	李昀潔	蔡欣芸
Yu-Han Chen	Yun-Chieh Lee	Hsin-Yun Tsai
德明財經科技大學	德明財經科技大學	德明財經科技大學
資訊管理系	資訊管理系	資訊管理系
學生	學生	學生
hank4928@gmail.com	lala52540@gmail.com	cindyynu@gmail.com

摘　要

近期在金融界興起區塊鏈這個名詞，區塊鏈是在建構一個 “去中央控管”的營運模式或稱之為信任生態圈，而比特幣就是此一技術的實務應用典範，區塊鏈利用網路上的節點來交換訊息與保存資料，透過共識決來保持各節點資料的同步與一致性，而每個信任節點都儲存完整的資料，以達到去中心化的運作模式。因此，本研究嘗試運用 IBM 提出的超級帳本 Hyperledger 區塊鏈技術來解決機車資產管理與交易轉移問題，因為在台灣，機車是大學生主要的交通工具，但是機車交易市場不夠透明，資訊幾乎都被機車經銷商所掌控，若私自交易，也會因對機車資產來源或交易轉移過程不清楚，而受騙上當。但若運用區塊鏈去中心化、資料不可竄改與可追溯等特性，理應可解決上述之問題，並可行成一個機車交易信任生態圈。而為了驗證技術可行性，所以，本研究實作開發一套架構在 Hyperledger 區塊鏈技術上的機車資產管理與交易平台 App，以來驗證上述觀點，這套系統結合前台 App 與後台區塊鏈系統功能，提供給用戶做機車車籍資料資產建置、車輛資訊更新記錄(事故、保養、改車)、上下架銷售管理、交易紀錄管理及機車履歷資料追溯等功能。最後，本研究藉由實作機車資產管理與交易平台系統，得到充份的 Hyperledger 區塊鏈技術應用驗證。

關鍵詞：區塊鏈、共識決、Hyperledger、機車資產管理、機車交易 App。

Abstract

Blockchain this term is recently rose in the financial sector. The block chain is in the construction of a "central control" mode of operation or called the trust of the ecological circle, and Bitcoin is a practical application of this technology model. Block chain uses the nodes on the network to exchange messages and save data, through the consensus decision to keep the synchronization of data and consistency of each node, and each trusted node to store complete information to achieve the decentralized mode of operation. Therefore, this study attempts to use IBM's hyper-book Hyperledger block chain technology to solve the problem of locomotive asset management and transaction transfer, because in Taiwan, locomotives are the main transportation for college students, but the locomotive market is not transparent, information is always control by Locomotive dealers. If traded privately, because of the locomotive asset source or transaction transfer process is not clear, it will be deceived easily. However, if used the block chain to decentralize, the data can not be tampered with traceability and other characteristics, should be able to solve the above problems, and feasible into a locomotive transaction trust ecosphere. In order to verify the feasibility of the technology, this study has been developed to develop a set of architecture in the Hyperledger block chain technology on the locomotive asset management and trading platform App, to verify the above point of view. The system combined with the foreground App and backstage block chain system function, provided the user to do locomotive car information asset construction, vehicle information update records (accident, maintenance, change car), on the shelf sales management, transaction record management and locomotive history data traceability and other functions. Finally, this study is based on the realization of locomotive asset management and trading platform system, and fully validated by Hyperledger block chain technology.

Keywords: Block chain, Consensus, Hyperledger, Motorcycle Asset Management, Motorcycle Trading App

1. 研究背景與動機

近期在金融界興起區塊鏈這個名詞，區塊鏈是在建構一個 “去中央控管” 的營運模式或稱之為信任生態圈(Trust Ecosystem)，而比特幣就是此一技術的實務應用典範，區塊鏈利用網路上的節點來交換訊息與保存資料，透過共識決來保持各節點資料的同步與一致性，而每個信任節點都儲存完整的資料，以達到去中心化的運作模式。

由於在區塊鏈上資料不再集中儲存與管理，資料與資訊將不再被少數企業、財團或政府所掌控，資料與資訊將更透明與正確，而且透過區塊與鏈結技術，更可做到資料不可竄改與追溯。

因此，本研究嘗試運用區塊鏈技術來解決機車資產管理與交易轉移問題，因為在台灣，機車是大學生主要的交通工具，但是機車交易市場不夠透明，資訊幾乎都被機車經銷商所掌控，若私自交易，也會因對機車資產來源或交易轉移過程不清楚，而受騙上當。但若運用區塊鏈去中心化、資料不可竄改與可追溯等特性，理應可解決上述之問題，並可行成一個機車交易信任生態圈。

不過，若要運用區塊鏈技術來解決機車資產管理與交易轉移問題，仍有下列問題待解決：

(1) 區塊鏈運作平台技術問題。
(2) 信任生態圈成員檢核認證問題。
(3) 信任生態圈機車資產檢核認證問題。
(4) 信任生態圈機車資產轉移認證問題。
(5) 信任生態圈機車資產履歷追溯問題。。

因此，可能需要設計獨特的運作架構，設備集及計算機程序來構建系統架構與運作程序，而這就是本文的研究動機。

2. 相關文獻與技術探討

區塊鏈技術是從比特幣(Bitcoin)開始，比特幣是一種新型態的數位資產及交易模式，強調去中心化及資料無法被竄改的特性，由日本人中本聰(Satoshi Nakamoto)在 2011 年 11 月 1 日密碼學討論群提出這個觀念[1]。

而今日比特幣這個去中心化及資料無法被竄改的特性正逐漸在顛覆集中式交易基礎，區塊鏈可視為一個公開的帳本，網路上的各節點都有完整的帳本備份，帳本裡面儲存所有的交易紀錄，而帳本本身以區塊紀錄，每個區塊包含一部分的交易，而每個區塊記著前面區塊的 id，形成一種鍊狀的資料結構，所以稱之為區塊鏈。

當某一個節點要發起交易時，會先將交易廣播給其他節點，此時所有節點都可以經由共識演算法來驗證這筆交易[2]。

不過，由於比特幣的區塊鏈技術是匿名的，在實務運作與管理上可能會有些問題，因此，IBM 提出一個超級帳本(Hyperledger)架構[3]，又稱為 fabric，fabric 是一個開放原始碼的區塊鏈運作平台，其核心服務是由 Membership、Blockchain 和 Chaincode 等三大服務所組成，如圖 1 所示。

Membership Services 這項服務用來管理節點身份、隱私、簽署 和 審查。Blockchain services 運用 HTTP 上的 P2P 協議來管理分布式帳本及設置共識協議。Chaincode services 提供一種安全且輕量級的沙盒運行模式，用來確認節點上執行如智能合約之 chaincode 邏輯[4]。

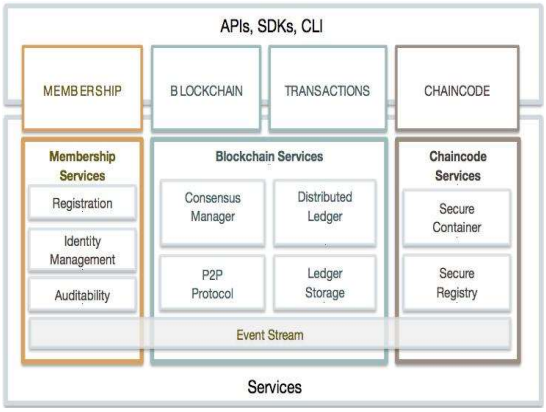

圖 1 IBM Hyperledger fabric 組成[3]

而本研究由於要建立一個機車交易信任生態圈，讓每一個參與者都能獲得彼此間的信任，並能建立完整的資產與交易資訊，因此，資產所有權擁有者必須能被檢驗，所以不適宜採用比特幣的匿名性，較宜運用 IBM 提出的超級帳本(Hyperledger)架構，來做到成員身份證認，因此，本研究的區塊鏈運作平台，將建立在 IBM 提出的超級帳本 Hyperledger fabric 架構上。

3. 機車交易生態圈區塊鏈運作架構設計

本研究採用 IBM 提出的超級帳本 Hyperledger fabric 作為區塊鏈運作架構，係因為 Hyperledger fabric 並不是公有鏈，他是私有鏈或聯盟鏈，Hyperledger fabric 是需要經過用戶審查及認證才能加入區塊鏈交易的私有鏈; Hyperledger fabric 具備 CA（Certificate Authority）來進行公鑰、私鑰、數位簽章的發行，同時也能管理使用者的帳戶，確保實名制。

除了用戶認證外，Hyperledger fabric 在儲存交易記錄的區塊（Block）安全與隱私上，採用 PKI 加密機制的公、私鑰來執行數位簽章，進行區塊的加密。

另外其有嚴格的共識算法(consensus plugin)，Hyperledger fabric 實現 PBFT(Practical Byzantine Fault Tolerance；拜占庭容錯) 共識決演算法，PBFT 要求區塊鏈內的帳本參與節點，互相驗證區塊內的交易記錄，通過 3 分之 2 參與節點，共識決同意的交易記錄，就可以寫入帳本，來確保交易數據的不可竄改以及永久保存。

除此之外，Hyperledger fabric 提供 REST API，允許透過 API 來註冊用戶、查詢 blockchain 和發送 transactions。甚至一些針對 chaincode 的 API，可

以用來執行 transactions 和查詢交易結果。對於開發者來說提供了方便的介接介面。

另外區塊鏈分佈式網絡節點的拓撲結構，也是一個必須考慮的問題。因為在這個世界裡散佈著眾多參與者，每個參與者有不同角色或屬於不同的利益體，各種各樣的情況都會發生，如比特幣網絡節點是開放加入，只要您願意提供網路與計算，就可以成為比特幣區塊鏈網絡的節點，好處是可能以量來取得信任，但缺點是網絡節點的拓撲結構可能會過於發散。

但在 Hyperledger fabric 的區塊鏈網絡裡，就較單純，只有 Membership service，VP 節點，NVP 節點，如圖 2 所示。 VP 節點又稱為確認節點，確認節點儲存帳本，參與驗證區塊內的交易記錄，或發起交易，但 NVP 節點(非確認節點)，就不能儲存帳本，參與驗證區塊內的交易記錄，或發起交易，所以 Hyperledger fabric 的區塊鏈網絡節點的拓撲結構就較能掌握與不易發散，並較符合安全和操作需求。

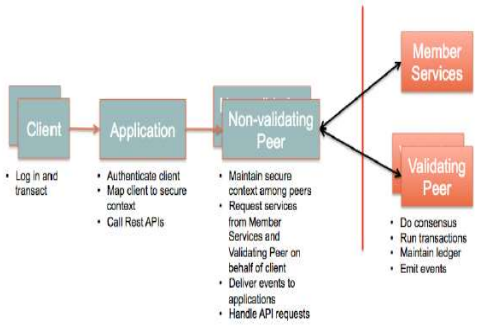

圖 2 IBM Hyperledger fabric 運作架構[3]

因此，本研究將 Hyperledger fabric 的區塊鏈網絡架構，套用到機車交易信任生態圈運作架構設計，發展出如下圖 3 之運作模式。

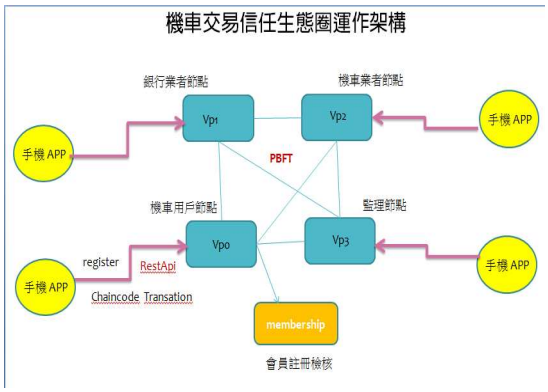

圖 3 機車交易信任生態圈運作架構

我們取消了 NVP 節點，在這個機車交易生態圈運作的都是 VP 節點，而 VP 節點 主要由 銀行保險業者、機車製造銷售與維修業者、監理單位及機車用戶所組成，這個機車交易生態圈的帳本就儲存在這四大類族群的網路節點設備上，而且也只有這些節點可以參與驗證區塊內的交易記錄，或發起交易。

在這個機車交易信任生態圈的所有運作，都是透過我們所發展的手機 App 來完成，使用者可依其所好，連線到任意的某一 VP 節點，來登錄進入這個區塊鏈網絡，然後透過 Rest Api 及 PBFT 共識演算法，在這個生態圈區塊鏈上完成各種交易處理，如圖 4 所示。

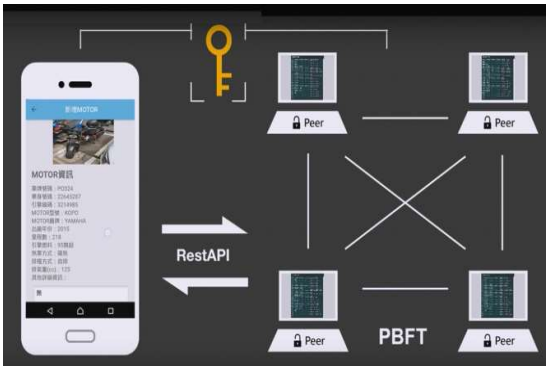

圖 4 機車交易 APP 與生態圈運作架構

4. 機車資產管理與交易平台系統功能設計

本研究主要是要發展一架構在 Hyperledger 區塊鏈技術上的機車資產管理與交易平台 App，因此，在研究方法上是採取實作與雛型系統開發模式，並按照技術探討與分析、功能設計及實作開發驗證等程序來進行。

由於本研究是透過區塊鏈技術來建置機車資產管理與交易生態圈，所以在系統功能設計上，是從機車資產建置開始就寫入區塊鏈，而且包含所有的保修紀錄、機車資產交易與轉移紀錄、甚至異常紀錄都會完整保留寫入區塊鏈內，甚至衍生出機車資產履歷追溯的功能。

因此，在這個生態圈的用戶，可以在任何時候、任何地點知道生態圈內機車資產的變動狀況，可大大降低買到問題車輛的風險，使得交易獲得更高的品質及保障。

總結本研究所發展的機車資產管理與交易平台 App，具有以下幾項功能特色:

(1) 去中心化

因為使用分散式計算和帳本存儲技術，不存在中心化的硬體或管理機構，在生態圈任意節點的權利和義務都是均等的，生態圈中的資料由整個生態圈中的節點來共同維護。而各端點的資料，不會只儲存在某個特定機構上，可消除特定廠商，掌握市場獨大的情況。

(2) 難以竄改資料，具有不可竄改性

機車資產或相關交易資料建立後，因資料儲存到各個節點上，如要更改資料，會因無法在全部節

點上偽造及竄改紀錄，使得資料無法任意更改。

(3) 自治性與共識決

端點採用基於共識決的協商機制來取得共識與一致的協議，使得整個生態圈中的所有節點能夠在此共識決協議的環境下自由且安全的交換數據，然後逐漸形成自治性，不易受到特定或少數異常節點干擾。

(4) 安全性與可追溯性

因資料都經過數位簽章加密才寫入區塊鏈，而且一旦蓋好時間戳，這個區塊裡的資料 就沒有辦法任意竄改。另因每一筆交易資料都會完整保留，讓使用者能追溯查詢如：交易紀錄、保養紀錄及資產轉移記錄等。

本研究所發展的機車資產管理與交易平台，分前台 App 系統功能與後台區塊鏈系統功能，後台區塊鏈系統功能主要有用戶管理、資產管理、車輛資訊更新(事故、保養、改車)管理、賣場資訊管理及交易管理，如圖 5 所示。

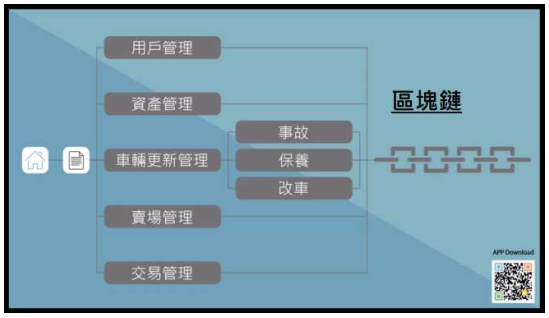

圖 5 機車資產管理與交易平台區塊鏈功能架構

而後台區塊鏈系統功能，主要是接收前台 App 系統的操作要求，然後利用 Hyperledger fabric Chaincode 功能來發起交易(transactions)，並將相關資訊寫入區塊鏈中。

至於前台 App 系統功能，主要是提供給用戶做機車車籍資料資產建置、車輛資訊更新記錄(事故、保養、改車)、上下架銷售管理、交易紀錄管理及機車履歷資料追溯，如圖 6 所示。

圖 6 機車資產管理與交易平台 APP 功能架構

5. 機車資產管理與交易 App 系統功能說明

本章節開始說明本研究所開發的機車資產管理與交易平台 App 的幾個主要功能，首先是 App 主畫面，如圖 7 所示。用戶從 App 主畫面登入註冊後，點選我的 MOTOR 選項，可進行機車資產建置、車輛資訊更新記錄(事故、保養、改車) 、上下架銷售管理；點選尋找 MOTOR 選項，可進行機車訂購與交易處理；點選交易紀錄，可進行特定機車交易紀錄及履歷追溯查詢。

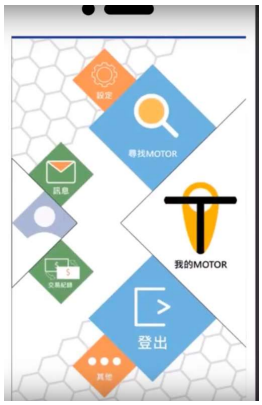

圖 7 機車資產管理與交易平台 APP 主畫面

底下因篇幅問題，我們僅說明幾項主要功能，所有圖示畫面均是實機錄製，若是單機畫面圖示，則圖示左側是機車資產管理與交易平台 APP 的實機操作畫面；而圖示右側則是後台區塊鏈系統運作截錄畫面。若是雙機畫面圖示，則圖示左右兩側是截錄機車資產管理與交易平台 APP 在雙方機器上的相關交易處理實機操作畫面；中間則是後台區塊鏈系統 PBFT 共識演算法運作示意畫面。

(1) 機車車籍資料資產建置-新增車輛

透過新增車輛功能，能建置用戶所擁有的機車車籍資料資產，如圖 8 所示。

圖 8 機車資產管理與交易平台 APP 新增車輛功能

當使用者輸入完車籍資料，按下 下一步及登錄後，機車資產管理與交易平台 APP 就會透過

fabric chaincode REST API 發起交易，然後在這個生態圈區塊鏈上，經由 PBFT 共識決演算法來取得共識，若最後獲得共識，就會將此筆新增的機車車籍資料寫入區塊鏈內，如圖 9 所示，圖 9 右側顯示的是寫入區塊鏈的加密機車車籍資料。

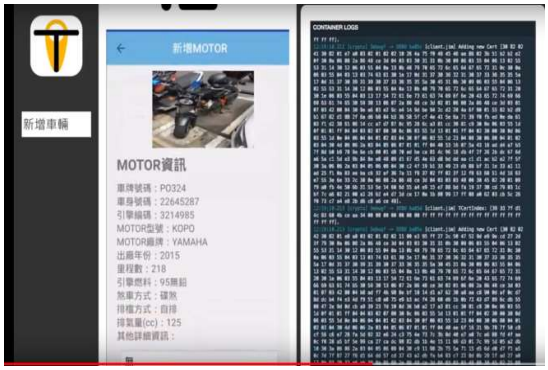

圖 9 透過 APP 新增車輛資產並儲存至區塊鏈

(2) 車輛資訊更新(事故、保養、改車)-狀態更新

透過狀態更新功能，能記錄用戶機車相關的事故、保養、改車等資料，如圖 10 所示。

當使用者輸入完相關記錄資料，按下確認鍵後，機車資產管理與交易平台 APP 就會透過 fabric chaincode REST API 發起交易，然後在這個生態圈區塊鏈上，經由 PBFT 共識決演算法來取得共識，若最後獲得共識，就會將此筆狀態更新資料寫入區塊鏈內，如圖 11 所示。

圖 10 機車資產管理與交易 APP 狀態更新功能

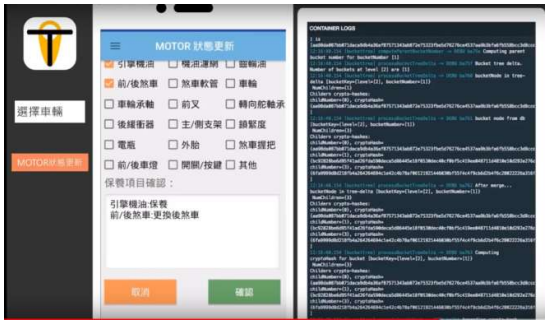

圖 11 透過 APP 記錄車輛狀態並儲存至區塊鏈

(3) 交易紀錄管理及機車履歷資料追溯-履歷追溯

透過追溯功能，用戶能經由區塊鏈追溯機車相關的資產擁有者及相關事故、保養、改車等記錄資料，如圖 12、13 所示。

圖 12 透過 APP 經由區塊鏈追溯資產擁有者記錄

圖 13 透過 APP 經由區塊鏈追溯機車保養記錄

(4) 上下架銷售管理-上架銷售

透過上架功能，用戶能將所擁有的機車資產上架銷售，如圖 14 所示。

圖 14 機車資產管理與交易 APP 上架銷售功能

當使用者輸入完相關上架銷售資料，按下確認鍵後，機車資產管理與交易平台 APP 就會透過 fabric chaincode REST API 發起交易，然後在這個生態圈區塊鏈上，經由 PBFT 共識決演算法來取得可上架銷售共識，若最後獲得可上架銷售共識，就會將此筆上架銷售資料寫入區塊鏈內，如圖 15 所示。

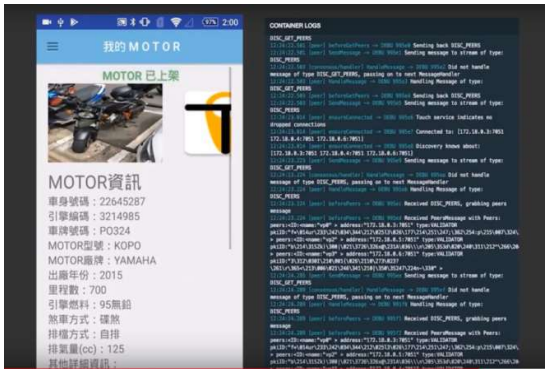

圖 15 透過 APP 上架銷售並儲存至區塊鏈

(5) 機車訂購與交易處理

機車上架銷售後，可透過尋找 MOTOR 選項，進行機車訂購與交易處理，在處理程序上依序為確認交易與金額、確認付款及交車機車資產轉移，如圖 16、17、18 所示。

所有程序都是透過機車資產管理與交易平台 APP 經由 fabric chaincode REST API 發起交易，然後在這個生態圈區塊鏈上，經由 PBFT 共識決演算法來取得確認交易與交易金額共識、確認付款共識及機車資產轉移共識，若獲得共識，就會將相關資料寫入區塊鏈內。

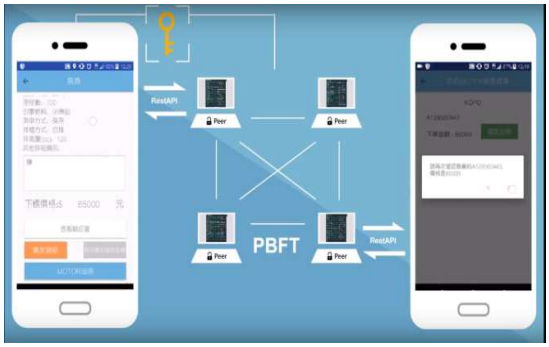

圖 16 透過 APP 確認交易金額並儲存至區塊鏈

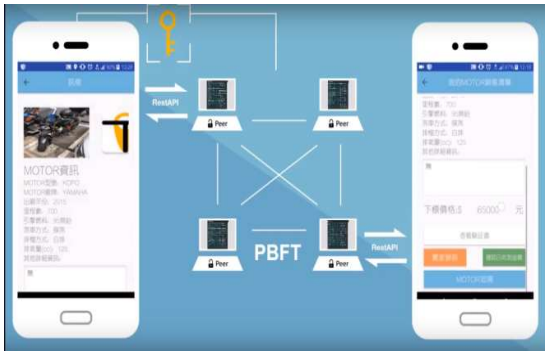

圖 17 透過 APP 確認交易付款並儲存至區塊鏈

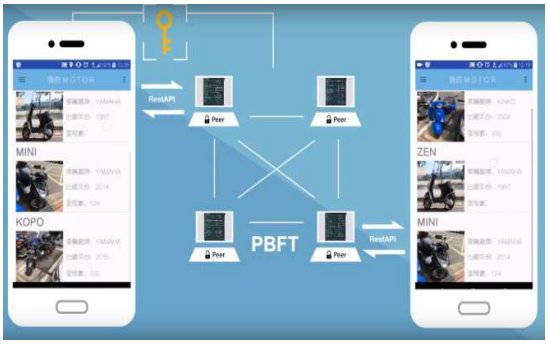

圖 18 透過 APP 完成資產轉移並儲存至區塊鏈

6. 結論與建議

本研究提出以 Hyperledger 區塊鏈技術來架構機車資產管理與交易平台；其理由在於：資產所有權擁有者必須能被檢驗，所以不適宜採用比特幣的匿名性，較宜運用 IBM 提出的超級帳本(Hyperledger)架構，來做到成員身份證認。

其次，區塊鏈網絡節點的拓撲結構，也是一個必須考慮的問題，比特幣網絡節點是開放加入，缺點是網絡節點的拓撲結構可能會過於發散。

但Hyperledger fabric的區塊鏈網絡就較單純，只有 Membership service，VP 節點，NVP 節點，且只有 VP 節點能儲存帳本，參與驗證區塊內的交易記錄，或發起交易，因此 Hyperledger fabric 的區塊鏈網絡節點的拓撲結構就較能掌握與不易發散，較符合安全和操作需求。。

因此，本研究採實作開發方式，在 Hyperledger 區塊鏈技術上發展一套機車資產管理與交易平台 App，以來驗證上述觀點，這套系統結合前台 App 與後台區塊鏈系統功能，提供給用戶做機車車籍資料資產建置、車輛資訊更新記錄(事故、保養、改車)、上下架銷售管理、交易紀錄管理及機車履歷資料追溯等功能。

最後，本研究藉由實作機車資產管理與交易平台系統，得到充份的 Hyperledger 區塊鏈技術應用驗證。

參考文獻

[1] Satoshi Nakamoto,” Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/en/bitcoin-paper.

[2] LightBlue,” 五個問答讓你秒懂區塊鏈原理及應用”, http://www.lightblue.asia/q-n-a-for-blockchain.

[3] ” Hyperledger Whitepaper”, https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/edit#heading=h.m6iml6hqrnm2.

[4] ” Blockchian區塊鏈：IBM HyperLedger fabric 簡述”, https://read01.com/RRB5PM.html.