

國立東華大學資訊工程系

National Dong Hwa University

109 學年度大學部專題研究報告

109 CSIE Project Report

區塊鏈交易系統—ShopP2P

A Trading System Based on Blockchain Technology: ShopP2P



指導教授 Advisor： 賴志宏 博士

專題參與人員 Team Member： 洪廷鈞  
徐培欽

中 華 民 國 110 年 5 月 21 日

# 國立東華大學資訊工程學系

## 專題報告原創性聲明

### National Dong Hwa University

#### Department of Computer Science and Information Engineering

#### Statement of Originality

本人鄭重聲明：

所呈交的專題報告是在指導老師指導下進行的研究工作及取得的  
研究成果。除文中已經註明引用的內容外，本報告不包含任何其他  
個人或集體已經發表或撰寫過的研究成果。對本文的研究做出重要貢  
獻的個人與集體，均已在文中以明確方式標明。若有違上述聲明，願  
依校規處分及承擔法律責任。

I hereby affirm that the submitted project report is the result of research  
under the supervision of my advisor. Except where due references are  
made, the report contains no material previously published or written by  
another person or group. All significant facilitators to the project have  
been mentioned explicitly. Should any part of the statement were  
breached, I am subject to the punishment enforced by the University and  
any legal responsibility incurred.

學號 Student No.	學生姓名 Name	親筆簽名 Signature
410625023	洪廷鈞	
410636016	徐培欽	

日期 Date : \_\_\_\_\_

## 摘要

現今的資訊發展迅速，使人類擁有前所未有的便利生活，資訊帶來了便利，同時也帶來了隱憂。過去的交易模式存在個人資訊安全的問題，在購物平台的伺服器中儲存了大量的使用者個人資訊，使得資訊安全產生疑慮。隨著區塊鏈技術逐漸發展，本組構思一種以區塊鏈為核心的交易系統，解決過去交易平台所面臨的問題，透過以太坊及智能合約技術，建構一套點對點的交易系統。本系統部屬於以太坊虛擬機，並以智能合約為整體核心技術，在信用機制上，本系統先建立一個標準評價，若交易時遇到糾紛，將以使用者歷史評價分數與標準評價進行對比，透過對比就能產生相對應的懲罰效果，以實現能完全自行運作，不需要人為參與的去中心交易系統。面對使用者不熟悉以太坊環境操作，本組建置了一個網頁供使用者利用，以 API 方式與智能合約進行連接，讓使用者能從網頁進行整個購物流程，避免對初次使用者造成過大的使用障礙。區塊鏈無法儲存大量資料，故本組將系統所有檔案放置於星際檔案系統，以此實現持久的分散式檔案儲存。透過當前的智能合約及星際檔案系統等技術，本組打造出一個完整的交易系統，降低使用者資訊安全疑慮，讓社會擁有對使用者更加友善的購物環境。

**關鍵字：**區塊鏈、智能合約、星際檔案系統、去中心化、點對點交易

These days, people have a more convenient life because of the development of information technology. Information technology not only brings the convenient life but also brings the problem. The trading mode has some personal information issues now. The servers storage a lot of user's information on the shopping platform. With the growth of blockchain technology, we have come up with a trading system built by blockchain. This system will solve some problems in the old shopping mode. We build a peer-to-peer trading system with ethers and smart-contract. Our team will deploy the system in EVM. In the credit system, we use a standard rank. When users having some credit issue, the system will make judge by the historic rank and standard rank. We also build a website for beginners by API. Although blockchain can solve some security issue, it still exists some weak point, the storage space. Blockchain can not store a lot of information. We use the IPFS storage technology to overcome this problem. With these technologies, our team success build a complete trading system. We think society will have a more friendly shopping environment.

**Keyword:** Blockchain, Smart Contract, IPFS, Decentralization, Peer-to-peer Trade

# 目錄

摘要.....	I
目錄.....	II
圖目錄.....	III
第一章 前言.....	1
第一節 研究動機與背景.....	1
第二節 目的.....	1
第二章 相關研究.....	3
第一節 區塊鏈簡介.....	3
第二節 以太坊及智能合約簡介.....	4
第三節 交易機制.....	5
第四節 星際檔案系統(IPFS).....	6
第五節 資料串接.....	7
第三章 研究方法與步驟.....	9
第一節 系統開發.....	9
第二節 使用步驟.....	14
第四章 結果討論與建議.....	27
參考文獻.....	28

## 圖目錄

圖 2-1 區塊鏈示意圖 (Zhang, 2019).....	3
圖 2-2 區塊鏈 P2P 網路示意圖(Koteska, 2017).....	4
圖 2-3 買家給好評的情況.....	6
圖 2-4 買家給差評 賣家給好評的情況.....	6
圖 2-5 雙方給差評的情況.....	6
圖 2-6 星際檔案系統分散式網路節點示意圖.....	7
圖 3-1 交易系統設計架構.....	9
圖 3-2 Etherscan.io 查詢智能合約.....	10
圖 3-3 讀取合約.....	11
圖 3-4 寫入合約.....	12
圖 3-5 上傳 ShopP2P 到 IPFS.....	13
圖 3-6 成功於 IPFS 下載檔案到本機.....	13
圖 3-7 透過 ipfs.io 查看 ShopP2P.....	14
圖 3-8 檢查發現沒有釘選.....	14
圖 3-9 將檔案進行釘選.....	14
圖 3-10 交易流程圖.....	15
圖 3-11 網頁 ShopP2P 首頁.....	16
圖 3-12 註冊帳號頁面.....	16
圖 3-13 錢包與合約互動.....	16
圖 3-14 交易市場頁面.....	17
圖 3-15 商品資訊頁面.....	17
圖 3-16 輸入商品資訊.....	18
圖 3-17 錢包與合約互動.....	18
圖 3-18 網頁 ShopP2P 首頁.....	19
圖 3-19 註冊帳號頁面.....	19
圖 3-20 錢包與合約互動.....	19
圖 3-21 交易市場頁面.....	20
圖 3-22 交易市場中購買頁面.....	20
圖 3-23 購買時錢包與合約互動.....	21
圖 3-24 交易市場頁面.....	21
圖 3-25 我的物品頁面買入中.....	21
圖 3-26 我的物品賣出中頁面.....	22
圖 3-27 評價頁面.....	22
圖 3-28 評價時合約與錢包互動.....	23
圖 3-29 評價時合約與錢包互動.....	23

圖 3-30 買家給好評的情況.....	24
圖 3-31 買家給差評 賣家給好評的情況.....	24
圖 3-32 雙方給差評的情況.....	24
圖 3-33 代幣相關頁面.....	25
圖 3-34 信用儲值.....	25
圖 3-35 送出代幣.....	26
圖 3-36 挖礦設定.....	26
圖 3-37 信用儲值 1PGN.....	26
圖 3-38 信用餘額 0.1ETH.....	26

# 第一章 前言

## 第一節 研究動機與背景

在過去的日子中，人們的交易必須找到買賣雙方，通常會選擇到實體商店或市集等特定地點找尋交易對手，然而近幾年網路快速崛起，漸漸出現了網路這個新型態的交易媒介。網路的範圍十分廣闊，若沒有一個專門提供交易的平台，要找到交易對手也是件非常費時的事，於是專門提供 C2C 的電商服務平台就此發跡。隨著世界網路使用人數增加，電子商務使用率必定隨之增加，現今國內網路使用者在電子商務的使用率高於全球平均(財團法人台灣網路資訊中心，2020)，更加突顯了國內網路購物市場的熱絡。至今為止，我們幾乎都是透過一個交易平台進行交易，由所有交易流程都需要經過電商平台公司主導，才能順利完成交易。我們期待有一種不需要中介平台主導整個交易過程的模式，讓全體的用戶成為交易過程的監督者。我們發現當今購物平台會將使用者資料集中儲存於伺服器中，這些資料可能包括個人姓名、手機號碼、居住地址及付款資訊等等，此舉使得使用者資料安全產生疑慮。社會經常傳出大量個人資料外洩的案例，令使用者個人隱私權受到嚴重傷害，更使得不知情的民眾陷入詐騙的陷阱中(梁憶芳，2014)資訊安全是現存交易平台還能改進的部分，我們期待能打造一個保障使用者個人資料的交易系統，讓使用者擁有一個安全的交易系統。隨著區塊鏈技術日益發展，已經有越來越多領域開始著手區塊鏈的研究，本組認為區塊鏈所擁有的去中心化、匿名及不可竄改等特性十分適合作為去中心化交易系統的核心，故我們希望能透過區塊鏈技術打造一個理想的去中心化點對點交易系統，使整個系統不存在中心監督機構，避免所有將資訊儲存在一個伺服器中。透過分散式資訊儲存及匿名性增加使用者的個人資料安全，從而解決當今交易系統存在的資訊安全漏洞，以確保使用者的個人私密資訊安全。

## 第二節 目的

全世界使用電子商務服務之人數逐年增長，交易金額亦是不斷增加，隨著電子交易平台的使用量上升，人們對於安全問題也開始重視。現今電商交易平台儲存了大量使用者個人資料，這些個人資料經常沒有受到良好的保護，使得這些重要的資料被流出到有心人士手上，常見的情況就是詐騙集團假借賣場客服人員，謊稱是工作人員操作錯誤，不小心設成分期付款，需要消費者到 ATM 解除分期付款這類詐騙手段。本組透過區塊鏈技術發想出一種保障個人資料安全的交易模式，區塊鏈以去中心化、不可竄改及公開透明等特性，讓使用者擁有更安全及值得信任的交易，除了單純的虛擬貨幣交易外，區塊鏈技術亦可透過智能合約建立起完整的程式邏輯，我們借重區塊鏈的各項優點，建立一個匿名的去中心化交易系統，整個交易僅會記錄錢包地址。本組規劃建立一套系統，是以區塊鏈作為核心，同

時加上本組發想出來的信用評比機制，再建立方便使用者瀏覽的平台網頁，再透過星際檔案系統儲存檔案。過去大部分會將檔案儲存於中心化的伺服器中，星際系統檔案可以有效分散儲存節點，建立一個點對點的大型檔案儲存網路，我們將所有系統檔案存放於星際系統檔案中，期待能創造出一個完整的去中心化交易系統。本組希望透過智能合約用以改善電子交易時遇到的困難，藉由區塊鏈特性，打造出一個值得使用者信任的交易平台，並將平台儲存於星際檔案系統中，以此提升網路購物時的安全性與交易公平性。



## 第二章 相關研究

本章共有五節，由於本系統是建立於區塊鏈基礎之上的交易系統，故將從區塊鏈開始進行介紹。介紹完區塊鏈後，將探討區塊鏈 2.0，以太坊及智能合約的出現使得區塊鏈得以寫入程式，設定好規則後就能自動執行，其方便的特性使其成為最知名的區塊鏈之一，同時造就現在眾多的智能合約出現。決定系統基礎後，需要研究相關交易機制，透過學習他人的區塊鏈交易平台研究成果，可以更快速瞭解如何建立一套完整的去中心化交易機制。有了系統及交易機制後，檔案如何儲存也是去中心化系統中非常重要的一環，為了避免傳統儲存在中心化伺服器的方式，需要透過星際檔案系統(IPFS)實現去中心化分散式網路節點儲存，以此建立一個安全且穩定的儲存空間。最後需要瞭解如何將所有系統串接於一起，我們須知道相關的串接模組，在網頁方面須瞭解 Ethers.js，在星際檔案系統方面須認識 JS-ipfs。

### 第一節 區塊鏈簡介

本系統的基礎建立於區塊鏈之上，區塊鏈的概念最早來自於 Nakamoto (2008) 發表的《Bitcoin: A Peer-to-Peer Electronic Cash System》，透過一種去中心化帳本技術，解決了以往需要第三方中心機構的信任機制，再加上密碼學技術，實現點對點的交易系統。區塊鏈是由多個分散的節點所組成，透過共識機制維持帳本運算及公平性，讓所有參與者可以在沒有第三方中心機構的方式下完成交易，所有人都會擁有相同的帳本。區塊鏈記錄了區塊鏈網路中發生的交易，使用了時間戳記、加密、經濟獎勵及分散式共識，藉此完成每一筆交易，如下圖(Data 中包含了 Timestamp、隨機值、礦工獎勵、資料內容等)。由於每塊區塊都包含前一個區塊的 Hash 值，使區塊串聯成區塊鏈，對於驗證區塊鏈區塊的方式稱作為挖礦，其執行挖礦之人即為礦工，礦工們以自身的運作資源提供整個區塊鏈網路交易的驗證服務，透過驗證計算每個區塊中的雜湊值，就能確保整個區塊鏈是正常運作，又基於共識機制由礦工們共同驗算計算過程，使區塊鏈變得不能從中竄改，只能繼續新增交易，避免有心人士刪除中間交易紀錄，以保障參與者的交易。

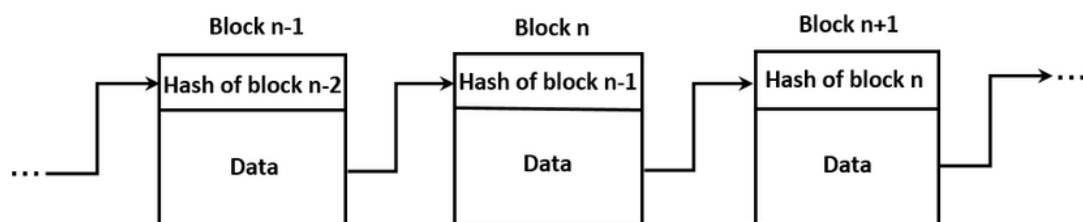


圖 二-1 區塊鏈示意圖 (Zhang, 2019)

在區塊鏈的交易是各節點之間的移動交易，因此不需要過往網路購物時的中介機構協助，參與者及參與者可以直接進行交易。

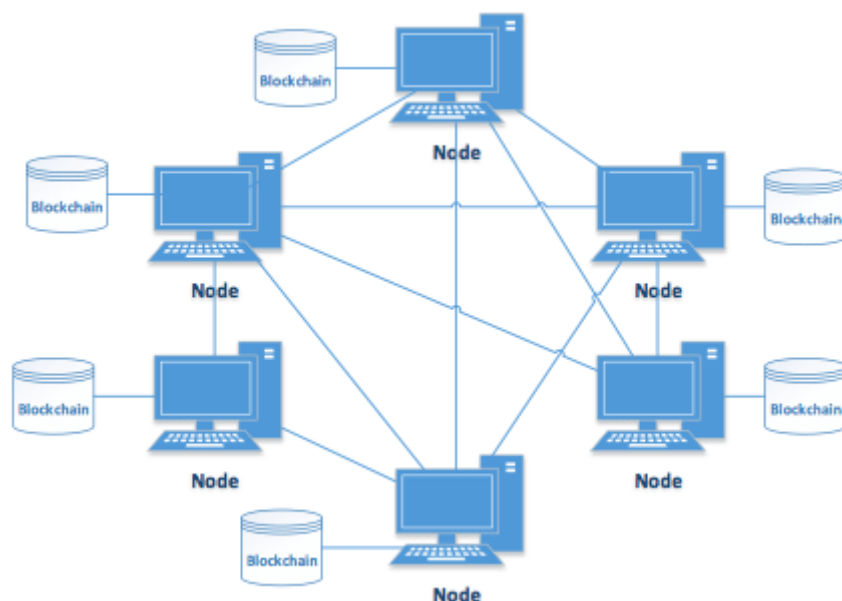


圖 二-2 區塊鏈 P2P 網路示意圖(Koteska, 2017)

## 第二節 以太坊及智能合約簡介

當有比特幣這個區塊鏈，只能實現將資料鏈在一起的功能，仍無法完成程式執行的效果，故出現了一套智能合約及去中心應用平台(Buterin, 2017)，本系統需要完成大量自動化執行，單運用比特幣是不夠的，故需要使用到以太坊及智能合約。以太坊是以區塊鏈為基礎而出現的開源平台，在以太坊交易的加密貨幣是以太幣，使用者可以在以太坊進行交易、撰寫與發佈程式(智能合約)來發展多元化的應用(陸毅軒, 2019)，具有圖靈完備的特色，可以編寫智能合約到區塊鏈中，建立在以太坊之上的特殊協議被稱為智能合約(Buterin, 2019)，讓使用者可以自行創建合約並於去中心化的世界中任意發想自己的規則，所有在區塊鏈中的智能合約只要達成條件就能自行運作，也因此很多事情都能夠讓智能合約來執行，不會受到外力干擾而中斷，因智能合約是存放於區塊鏈中，故智能合約不會被人竄改。

目前以太坊及智能合約已經在多個領域進行開發，像是選舉、後勤、管理、銀行系統、保險、房地產及物聯網等(加沛, 2018)。這是因為智能合約擁有區塊鏈的優點，其安全性高，所有的智能合約都儲存在區塊鏈上，沒有人能進行竄改，此外其具有自動執行的能力，透過自動化設計，不再需要人為干預，並且其具有高度自由，我們可以將各種程式設計藍圖置於智能合約中。

要使用智能合約，通常是利用 Solidity 的程式語言撰寫，若想順利執行智能合約，必須依靠以太坊虛擬機來完成，以太坊虛擬機是執行智能合約的環境，任何人都可以擔任驗證者，也就是礦工。當智能合約要執行時，需透過礦工將區塊打包寫入區塊鏈。以太坊為了避免參與者使礦工進行無意義的計算，因此會對每一次運算收取合乎工作量的手續費，而這手續費稱作為 Gas。

### 第三節 交易機制

我們發現有人透過區塊鏈技術研究出一套不動產交易系統，透過區塊鏈交易能使交易時程縮短並防止詐騙。傳統交易中買賣雙方基於信任找尋適合的第三方中介擔任保證單位，其中還是不可避免第三方的潛在中介風險(鍾斯羽，2017)，我們期待能透過區塊鏈技術解決中介機構的存在，雖鍾斯羽先生有提出一套交易系統，但須配合戶政區塊鏈、地政區塊鏈及銀行區塊鏈，這是目前台灣社會尚未存在的區塊鏈，故僅能以模擬的方式呈現，相較下本組並不存在此問題，我們的交易系統僅需要將合約部屬於以太坊鏈上即可運行，不用跟其他單位的區塊鏈互動，能提供十分完整的使用體驗。

本組目的之一就是要去除中介機構，讓區塊鏈分散式帳本去中心化的特性部份取代可信的第三方。交易時的交易效率亦是非常重要的一點，只要透過區塊鏈機制，就能夠實現點對點之間的交易，使之能精簡作業流程、提高營運效率以及降低交易成本(潘宜萱，2019)，本組期待能藉由區塊鏈技術，打造出更加有效率且低交易成本的點對點交易平台。

當使用者在一個有中央機構的交易環境中，需特別注意中央機構是否能始終保持正常運作，基於對中央式機構的信任，一旦中央式的機構故障或是被斷電可能不能再用這個系統。不過於此同時，分散式系統的交易速度比較容易變慢，因為帳本被分散式的紀錄在每個人的身上，所以每次的交易都必須經過一段時間的共識和同步(黃英睿，2019)，透過分散式系統，我們可以拜訪任何一個分散帳本，不用擔心中心機構出錯，不過仍然需要注意每次交易需要等待礦工驗證的過程。

在區塊鏈中，所有的交易資訊都是公開透明且不可竄改的，我們可以透過公開鏈去檢視每一筆交易紀錄，從而得出具有價值的數據資料。透過適當的統計，可提取出對產業有幫助的結果(蔡宛真，2019)。我們認為以區塊鏈為核心的交易平台能打破交易中心機構獨自把持數據的現況，為社會帶來更多的數據使用價值。

交易成本是影響買賣雙方是否使用服務的重要因素，透過智能合約交易，可以比其他交易平台擁有更高的效率及更低的交易手續費(歐日宋，2019)我們希望能透過智能合約技術，使整個交易成本更低，最終讓社會的總交易成本下降，讓人們享有更進步且友善的交易環境。

避免使用者惡意使用系統，本組發想一種信用評價對比系統，我們將整個交易分為三種情況(商品售價以 $X$ 表示)，買家好評、買家差評 賣家好評、買家差評 賣家差評。在買家好評機制中，代表買家如約收到心儀的商品，此時賣家不用給予回評，故發生在雙方交易順利的情況，此時智能合約會將 $X$ 給予買家， $3X$ 給予賣家。在買家差評 賣家好評機制中，代表賣家的商品有瑕疵或賣家未如約交貨，此時智能合約會將 $3X$ 給予買家， $X$ 給予賣家。在買家差評 賣家差評機制中，代表買賣雙方都認為對方有問題，此時會判斷雙方的歷史評價，歷史評價低於標準評價者，智能合約將沒收其押金 $2X$ ，相反地，歷史評價高於標準評價者，

智能合約將退還其押金 2X。整個信用機制整理如下圖。

假設商品售價為 10ETH，雙方交易前都給予合約 20ETH，合約內共有 40ETH：



圖 二-3 買家給好評的情況

若買家給好評，則 10ETH 轉到買家錢包，30ETH 轉到賣家錢包。

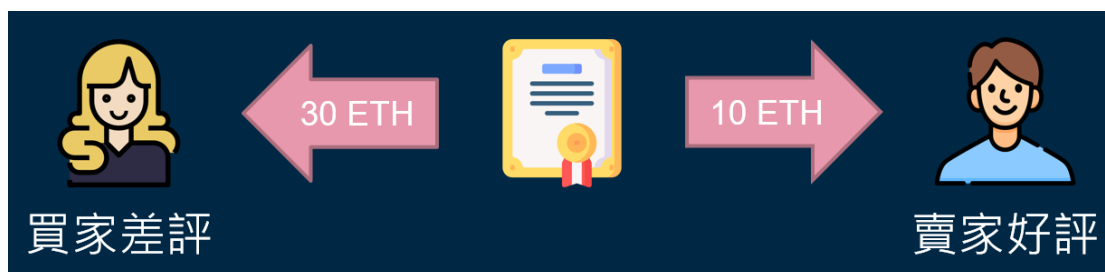


圖 二-4 買家給差評 賣家給好評的情況

若買家給差評 賣家給好評，則 30ETH 轉到買家錢包，10ETH 轉到賣家錢包。

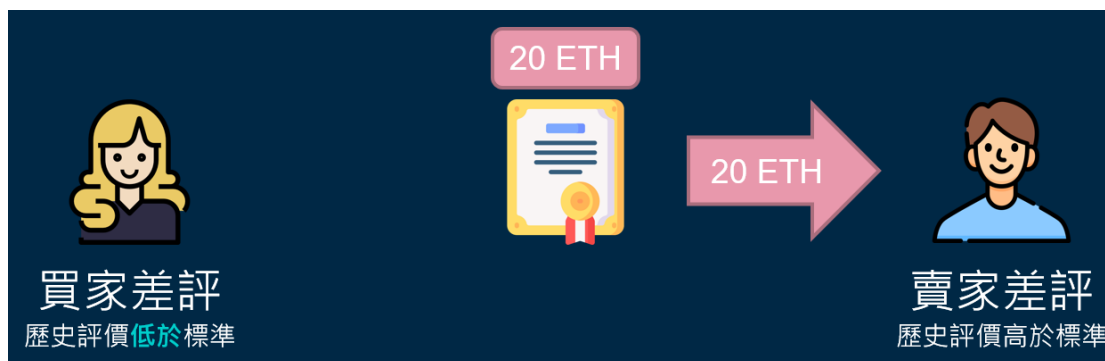


圖 二-5 雙方給差評的情況

若雙方給對方差評，歷史評價高於標準評價者將收到原先的押金，歷史評價低於標準評價者，則由平台沒收押金。當雙方給對方差評的情況發生時，系統將會調整雙方的標準評價，使之上升 10%。歷史評價計算方式：好評總價/(好評總價+差評總價)\*100%。

#### 第四節 星際檔案系統(IPFS)

區塊鏈是一個去中心化的網路，使用者能將所有資料放在鏈上，然而這個鏈

的空間並不是無上限，區塊鏈的儲存空間非常小，如果我們想放置一個很大的檔案可以透過拆成多個小檔案放在鏈上，若只有一個檔案還可以透過此方式運作，然而若所有人都將整個系統檔案放到鏈上，這樣會使得區塊鏈空間被大幅占用，同時影響整個鏈的驗證速度，為解決此問題，就必須將架設網頁的相關檔案放在傳統的中心化伺服器上，然而將檔案放在中心化的伺服器上就與去中心化的理念有所衝突。將資料放在中心化伺服器中，雖然可以讓使用者訪問到這個系統，並順利完成交易，但總有一天這個伺服器可能會受到攻擊，進而使資料被修改，使用者將無法再次拜訪網站。透過運用星際檔案系統，可以使整個系統去中心化更完整，星際檔案系統目的在於打造一個持久且分散式儲存與共用檔案的網路傳輸協議。所有上傳到 IPFS 網路的檔案，都會被系統分配到一個唯一且不可竄改的加密 Hash 值，若在 IPFS 網路中發現重複的資料，會被 IPFS 自動刪除，同時記錄歷史版本，以 P2P 的方式儲存檔案及其歷史版本紀錄。IPFS 具有高度安全性，不同於以往儲存在中心化伺服器，IPFS 會在網路中存有多個副本，並藉由 Hash 值進行驗證，避免檔案遭到惡意竄改。IPFS 將所有儲存資料放到網路上的多個節點中，組成一個巨大的儲存空間，同時將重複的檔案刪除，節省儲存空間。傳統的儲存方式若出現硬體故障，將使得檔案無法尋回，但透過 IPFS 能將風險分散到網路上的多個節點，除非所有節點同時故障，否則將持續提供穩定的檔案儲存。IPFS 亦能節省網路頻寬和成本，過去使用者需要向一個中心化伺服器取得資料，只要使用者過多，就會占滿整個網路頻寬，利用星際檔案系統會讀取最近的節點的特性，使網路資源效率提升。

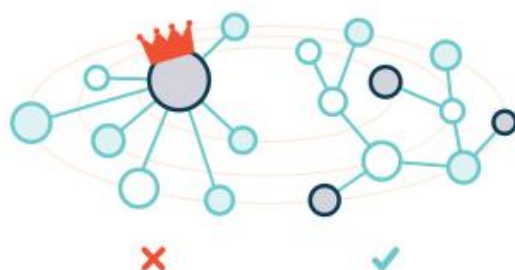


圖 二-6 星際檔案系統分散式網路節點示意圖

使用者存取檔案不再需要從一個主要伺服器存取，而是找尋離你最近的網路節點，藉此降低網路阻塞的風險，同時又能以最近的距離得到檔案，加快檔案的讀取速度。任何人都可以成為網路節點，同時檔案會有多份副本分布於各節點中，因此使整個網路的可靠性有所提升。

## 第五節 資料串接

有了系統架構及檔案儲存方式後，我們規劃以網頁的方式呈現給使用者使用，其優點是任何設備系統都可以使用，不會受限於設備作業系統。要如何將系統、檔案儲存及網頁串接變成了重要的議題，我們在區塊鏈方面預計利用 Ethers. js，

在星際檔案系統則是利用 JS-ipfs。起初我們規劃利用 Web3.js 使網頁與區塊鏈進行串接，但發現 Web3.js 無法與 MetaMask 錢包進行互動，於是我們改用 Ethers.js，這是一個以太坊的 JavaScript 模組，相較於 Web3.js，其擁有更簡潔的使用方式，在程式碼更少的同時，依然擁有完整的功能，透過這個模組，開發者可以與以太坊區塊鏈進行串接，實現與網頁互動的所有功能。

JS-ipfs 是透過 JavaScript 撰寫的 P2P 協議，可以在瀏覽器和 Node.js 中執行，實現所有 IPFS 功能，藉由 JS-ipfs 讓系統能與星際檔案系統串接，我們透過這個模組，實現讓使用者能把商品圖片及商品詳述從網頁上傳到星際檔案系統的功能，商品頁面的資料顯示也是如此，在使用者將資料傳到星際檔案系統後，我們會得到一串加密後的雜湊值(Hash)，我們將此 Hash 寫於區塊鏈上，以此方式保證使用者的資料都會完整被記錄於區塊鏈中，有了 Hash 值後，我們就可以到 IPFS 網路中找到對應的資料，因此不用擔心檔案遺失的問題發生。

### 第三章 研究方法與步驟

#### 第一節 系統開發

本組專案主要分成智能合約、網頁及星際檔案系統等部分。智能合約部分是以 Solidity 語言撰寫，這是一種靜態型及合約式導向的程式語言，主要用途即是撰寫智能合約。由於此種語言仍處於開發階段，故其版本變動十分快速，本組所使用的版本是以 0.8.4 為主，需特別注意各版本的語法使用差異。當 Solidity 撰寫完成後，經過編譯即可於 EVM 執行，EVM(Ethereum Virtual Machine)，是智能合約運行的環境。網頁的部分則是以 html 語法為主，外加使用 css。智能合約與網頁之間的溝通則是透過 API 用 Ethers.js 進行連接。使用區塊鏈須透過以太坊代幣錢包進行交易，本組推薦使用的是 MetaMask，這是一款相當簡單容易上手的錢包，能以 Google Chrome 套件的形式安裝，能輕鬆地與以太坊智能合約互動，對於測試智能合約來說十分便利。星際檔案系統提供去中心化儲存方式，可以將檔案儲存於多個網路節點中，並透過唯一的 Hash 值進行資料搜尋。

#### 交易系統設計架構

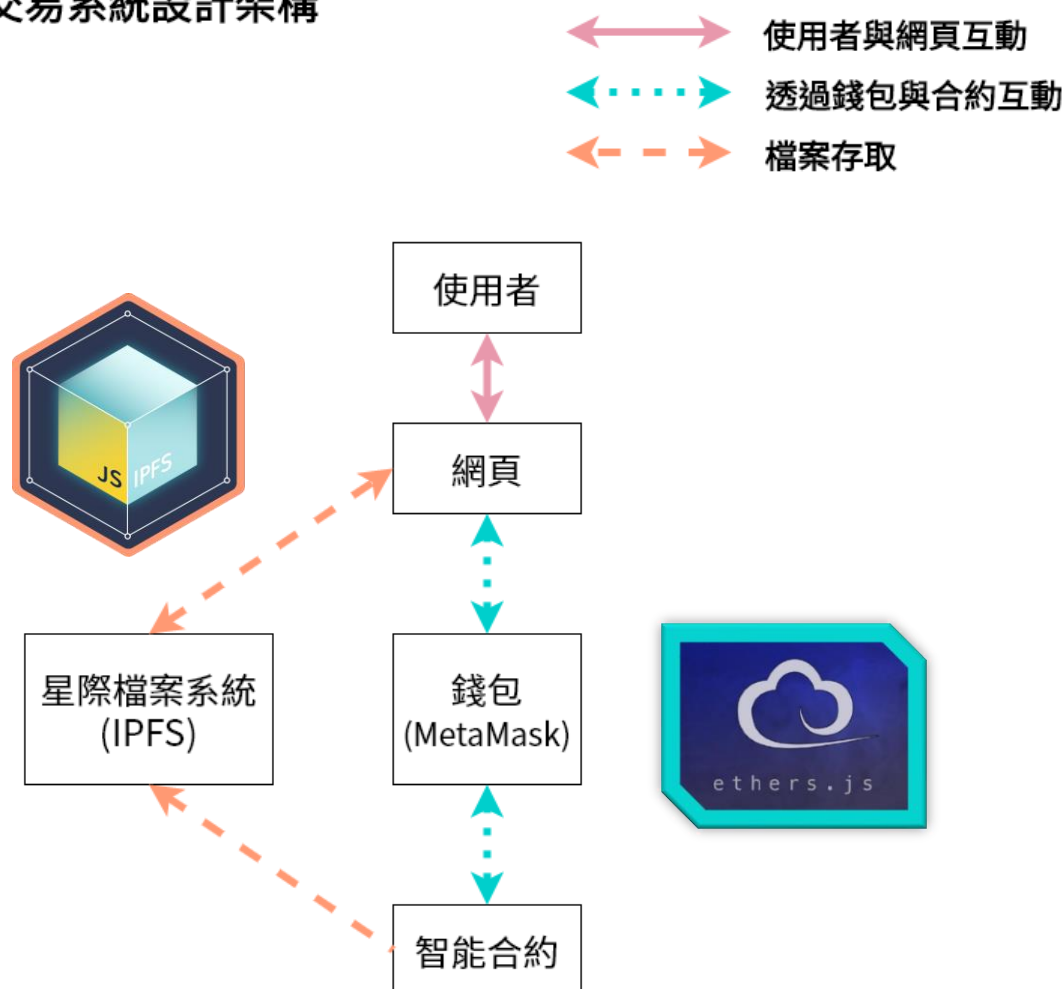
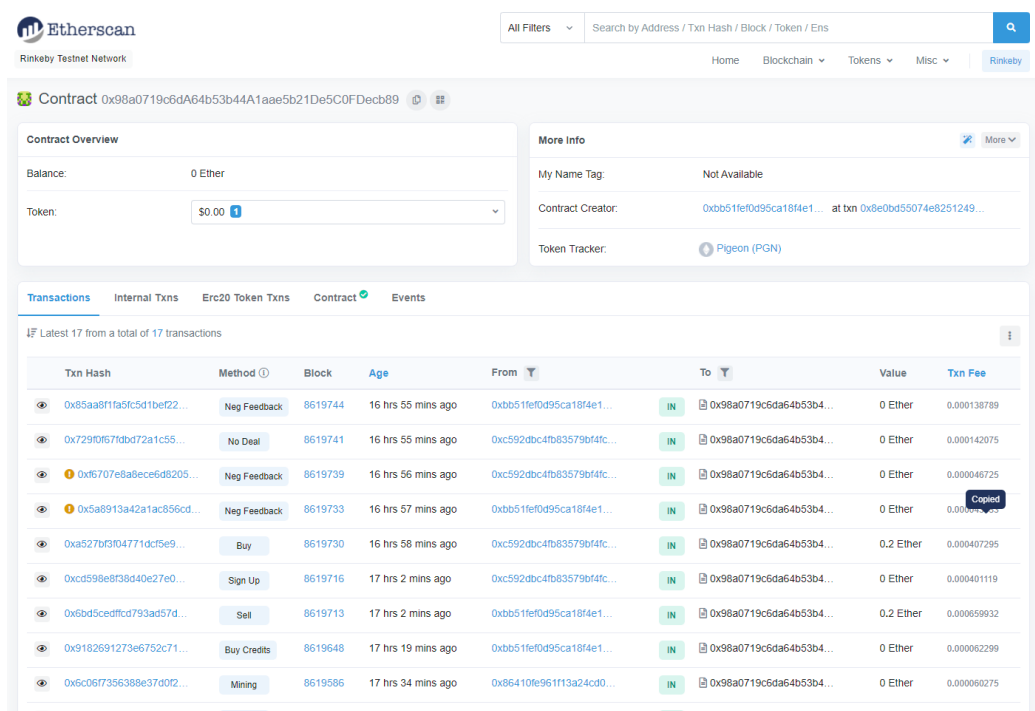


圖 三-1 交易系統設計架構



本交易系統的買賣交易都是在智能合約上進行，為讓使用者方便使用，我們建立了一個網頁平台，使用者可以透過網頁用 MetaMask 這款錢包與合約進行所有交易互動，我們透過 API 及 Ethers.js 技術使智能合約可以呈現在網頁上，大幅降低了不熟悉以太坊及智能合約使用者的使用門檻。我們透過星際檔案系統儲存所有網頁及大型檔案(圖片及商品詳細情況)，避免存放於有風險的傳統中心化伺服器，同時良好地解決了區塊鏈儲存空間不足的問題。透過 JS-ipfs 使網頁能與 IPFS 串接，讓使用者能上傳大型檔案到星際檔案系統中，並將檔案 Hash 值透過錢包傳到區塊鏈中，使網頁能從區塊鏈中讀取到 Hash 值進而找到所需檔案，再將圖檔或文字檔於網頁中顯示給使用者閱讀。

目前智能合約我們利用 Remix 撰寫，規劃有 Read Contract 及 Write Contract 兩部份。在 Read Contract 的部分都是用於讀取區塊鏈內容，我們不需要花費任何的 Gas，相反地，若要使用 Write 部分的功能，就會需要與合約進行互動並且花費 Gas。



The screenshot displays the Etherscan.io interface for a smart contract. The top section shows the contract overview with a balance of 0 Ether and a token value of \$0.00. Below this, the 'Transactions' tab is active, showing a list of 17 transactions. The table includes columns for Txn Hash, Method, Block, Age, From, To, Value, and Txn Fee. The transactions are listed in descending order of age, with the most recent transaction at the top. The methods include 'Neg Feedback', 'No Deal', 'Buy', 'Sign Up', 'Sell', 'Buy Credits', and 'Mining'. The values are in Ether, and the fees are in Ether.

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x85aa811a5c5d1be22...	Neg Feedback	8619744	16 hrs 55 mins ago	0xb051fe0d95ca184e1...	0x98a0719c6da64b53b4...	0 Ether	0.000138789
0x729f0f671dbd72a1c55...	No Deal	8619741	16 hrs 55 mins ago	0xc592dbc4fb83579b4fc...	0x98a0719c6da64b53b4...	0 Ether	0.000142075
0xf6707e8a8ece6d8205...	Neg Feedback	8619739	16 hrs 56 mins ago	0xc592dbc4fb83579b4fc...	0x98a0719c6da64b53b4...	0 Ether	0.000046725
0x5a8913a42a1ac856cd...	Neg Feedback	8619733	16 hrs 57 mins ago	0xb051fe0d95ca184e1...	0x98a0719c6da64b53b4...	0 Ether	0.000046725
0xa527b9f04771dcf5e9...	Buy	8619730	16 hrs 58 mins ago	0xc592dbc4fb83579b4fc...	0x98a0719c6da64b53b4...	0.2 Ether	0.000407295
0xcd598e8f38d40e27e0...	Sign Up	8619716	17 hrs 2 mins ago	0xc592dbc4fb83579b4fc...	0x98a0719c6da64b53b4...	0 Ether	0.000401119
0x6bd5cedfcd793ad57d...	Sell	8619713	17 hrs 2 mins ago	0xb051fe0d95ca184e1...	0x98a0719c6da64b53b4...	0.2 Ether	0.000059932
0x9182691273e6752c71...	Buy Credits	8619648	17 hrs 19 mins ago	0xb051fe0d95ca184e1...	0x98a0719c6da64b53b4...	0 Ether	0.000082299
0x6c067356388e3700f2...	Mining	8619586	17 hrs 34 mins ago	0x86410fe961f13a24cd0...	0x98a0719c6da64b53b4...	0 Ether	0.000060275

圖 三-2 Etherscan.io 查詢智能合約

將智能合約部署完後，可以透過 Etherscan.io 去看到完整的智能合約內容，Etherscan.io 是提供使用者查詢智能合約詳細內容的地方，所有以太坊上的智能合約都能於此處查詢。

詳細智能合約內容介紹如下圖，所有程式碼皆於附錄中。



Code	Read Contract	Write Contract
Read Contract Information		
1. CheckUserCredits	查詢使用者信用餘額	
2. CheckUserRec	查詢使用者評價	
3. FindUserAddr	查詢使用者錢包地址	
4. FindUserID	查詢使用者的使用者名稱	
5. FindingGoods	查詢商品詳細資料	
6. ViewBuyerBoard	查詢買入中商品詳細資料	
7. ViewCount	查詢使用者買賣多少物品	
8. ViewMarketBoard	查詢商品詳細資料	
9. ViewPublicBoard	查詢賣場商品詳細資料	
10. ViewSellerBoard	查詢賣出中商品詳細資料	
11. balanceOf	查詢使用者 PGN 代幣餘額	
12. basicAmount	每次挖礦可以得到的獎勵數量	
13. basicTime	隨機未來時間	
14. decimals	發幣位數	
15. name	發幣名稱	
16. owner	發幣所有者	
17. symbol	發幣簡寫	
18. totalGoods	整個市場所有物品數量	
19. totalSupply	發幣總幣量	

圖 三-3 讀取合約

Code

Read Contract

Write Contract

Connect to Web3

1. Buy	購買，輸入賣家地址 address、物品名稱及物品順序
2. BuyCredits	購買信用額度
3. Deal	買家確認交易成功
4. ForceDeal	賣家逾時未給評價，買家收回押金，輸入物品名稱及物品順序
5. Mining	挖礦
6. NegFeedback	若買家給予負評，賣家對買家給予負評
7. NoDeal	買家回報商品有問題
8. PosFeedback	若買家給予正評，賣家對買家給予正評
9. Sell	賣家上架物品
10. SignUp	輸入使用者名稱，註冊
11. transfer	從自己轉幣給別人

圖 三-4 寫入合約

網頁頁面分為數個 html 及 css 檔案去進行開發。在網頁串接的部份，我們利用 Ethers.js 及 JS-ipfs 這兩個 JavaScript 模組，透過各平台的應用程式介面(API)，我們可以使其資料進行溝通。整個專案內容事先存放於星際檔案系統 (IPFS) 網路中，可以透過 IPFS 官方文件安裝相關應用程式於電腦中。在 IPFS 網路中上傳專案檔案，以此保證系統的去中心化特性。

```
Microsoft Windows [版本 10.0.19041.985]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\hpc06\Desktop\project>ipfs add -r ShopP2P
18 B / ? [-----]
added QmTiUdmPtrwxwnBbp8pdVRbEzBjC3kT6fCR9VXvnHS459 ShopP2P/README.md
73.97 KiB / ? [-----]
added QmQk2vAHd1mUnkHcXgJywKgDEpFyKE6xAYgasrqonKGxox ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.css
255.38 KiB / ? [-----]
added QmFTGdEqEBbjld8wHgdSDQzdDRC7E6ita9Z9wwmihyaRB ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.css.map
305.68 KiB / ? [-----]
added QmPmDiHJJPM91MermE3ujoITjZTWGB9LN293DmPHLvZwwM ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.min.css
418.69 KiB / ? [-----]
added QmdpF5jfSe6QALwfVmrglFu2tYzxrLAHmKbvjaANW7ni91 ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.min.css.map
492.71 KiB / ? [-----]
added QmdiYusRqWYd96pMsaygvBHYjPcGwoYmKd5w6sstlCRyCW ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.rtl.css
674.12 KiB / ? [-----]
added QmcpZsw7SvYfsAu8PZYXzDyFwpF4ms89YpNiTop7eAiYhZ ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.rtl.css.map
724.50 KiB / ? [-----]
added QmcvUP3DmnaWDGoC2EdQycNPxnS5mC4mkZNhJmWFhTHDzx ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.rtl.min.css
837.58 KiB / ? [-----]
added QmZJo2DnrSroCduhSeicoV2upWyaYtejPUVKLNZbURyJn9 ShopP2P/bootstrap-5.0.0-beta2-dist/css/bootstrap-grid.rtl.min.css.map
```

圖 三-5 上傳 ShopP2P 到 IPFS

我們透過 `ipfs add -r` 就可以將整個資料夾傳送到 IPFS 網路中，同時使本機成為網路節點。我們也可以發現所有的檔案都有個別的 Hash 值，這個值可以確保該檔案的唯一性，當有他人竄改時，其 Hash 值就會改變，改變任一資料夾內的檔案也將使資料夾 Hash 被改動，故可以透過檢查 Hash 值得知該檔案是否有被竄改。

```
Microsoft Windows [版本 10.0.19041.985]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\hpc06\Desktop\project>ipfs get QmYxsQ6yPWUinGkdQnovfpPz3gfBphNiH8SFhqcigZAMqS
Saving file(s) to QmYxsQ6yPWUinGkdQnovfpPz3gfBphNiH8SFhqcigZAMqS
85.52 MiB / 85.52 MiB [-----] 100.00% 13s

C:\Users\hpc06\Desktop\project>
```

圖 三-6 成功於 IPFS 下載檔案到本機

有了檔案 Hash 值後，就可以到 IPFS 網路中查找此檔案是否可以被其他使用者存取，我們可以透過 `ipfs cat` 抓取檔案，也可以利用 `ipfs get` 下載檔案到本機節點，只要這兩個指令能成功執行，代表其他使用者可以在 IPFS 網路中得到這份專案的檔案。

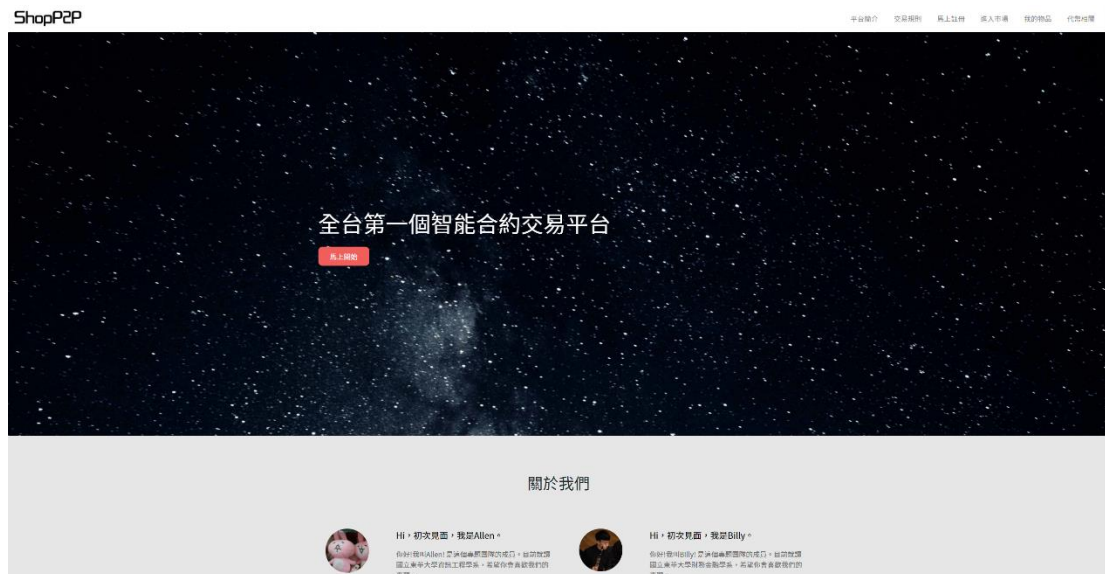


圖 三-7 透過 ipfs.io 查看 ShopP2P

確認 IPFS 網路中有 ShopP2P 專案檔案後，使用者也可以透過網頁的方式存取檔案，只需要利用 ipfs.io 就可以實現，這是由 IPFS 提供的一種網頁讀取檔案的途徑。雖檔案已經可以供使用者瀏覽使用，但 IPFS 網路具有定期清理垃圾檔案的設定，因此這個檔案沒有被本機釘選的話，很快就無法在 IPFS 網路中找到檔案。

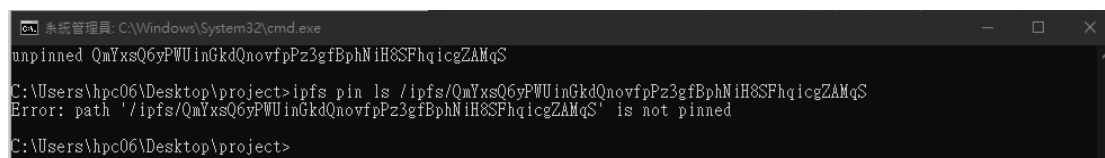


圖 三-8 檢查發現沒有釘選

ipfs pin ls 是查詢這個 Hash 值的檔案有沒有被釘選於本機節點，當檔案被釘選的話，本機電腦就成為儲存這個檔案的節點，就不會被 IPFS 主網路給刪除。



圖 三-9 將檔案進行釘選

利用 ipfs pin add，可以將這個 Hash 值的檔案釘選在本機中，確保檔案存於 IPFS 網路的節點中，使用者就可以持續地得到檔案。

## 第二節使用步驟

本節將詳細介紹交易平台的使用方式，分成交易及信用代幣兩部份，交易部

份一共有十個步驟，賣家註冊、支付押金上架、買家註冊、顯示商品、支付押金下單、交付物品、買家給予評價、賣家給予評價、返還押金及收取懲罰金。以交易流程圖建構使用者整個交易流程的概念，再透過步驟式圖文介紹，讓使用者能快速上手，在進到平台前，需事先準備好 MetaMask 錢包，使用者可以在習慣的瀏覽器進行安裝，通常可以在擴充功能中找到。由於本系統目前是使用 Rinkeby 測試鏈，故使用者的錢包須先切換至 Rinkeby 測試網路。在信用代幣方面，有信用儲值、送出代幣及挖礦設定，在這個頁面主要是希望能解決使用者重複註冊的問題，透過隨機固定一小段可以跟合約互動的時間，確保每個人在那個時間只能用一個帳號跟合約進行互動，以此避免使用者重複註冊，同時我們給予停留在網頁上的使用者獎勵，因為越多人使用網頁將使 IPFS 網路更加穩定，故我們會給予信用代幣，這個代幣可以強化對他人的評價權重。

交易流程圖

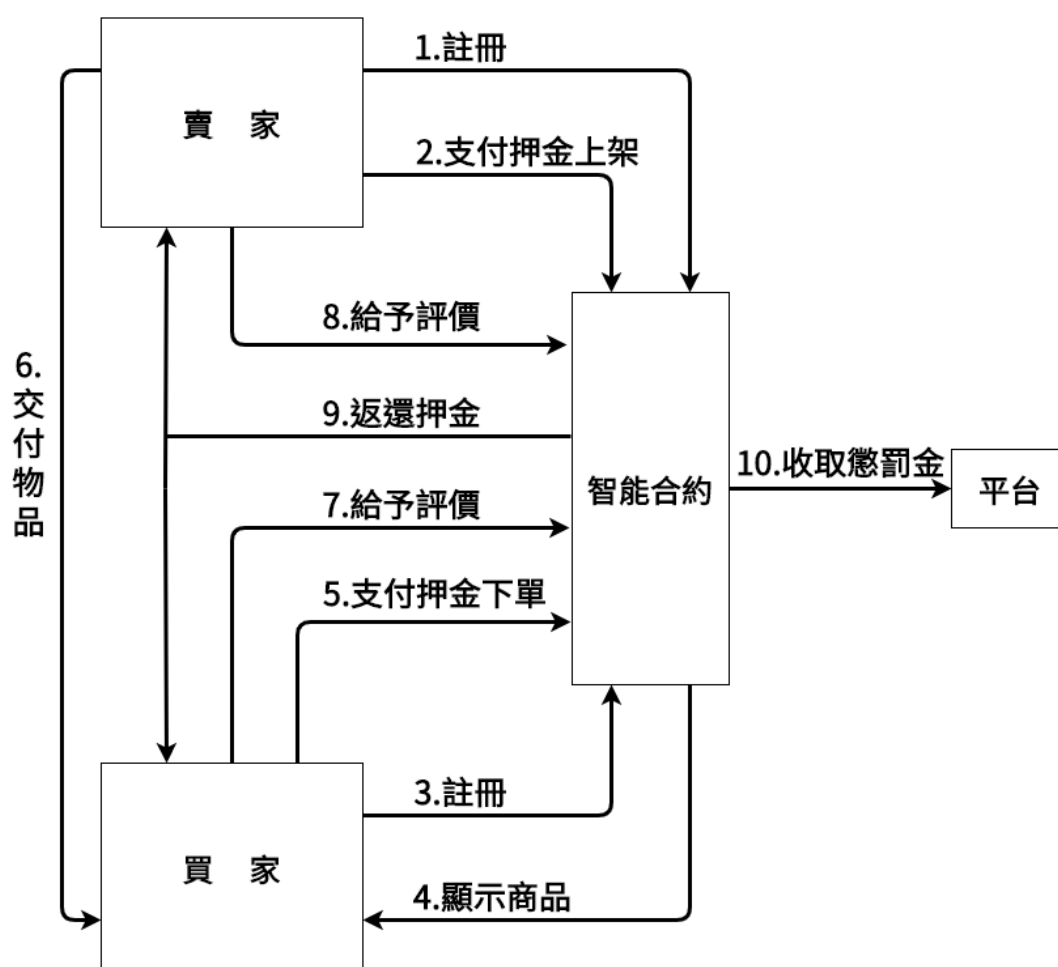


圖 三-10 交易流程圖





## 2. 支付押金上架

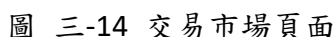


圖 三-15 商品資訊頁面

17

ShopP2P

平台簡介 交易規則 馬上註冊 進入市場 我的熱點 代幣初探

### 物品資訊

名稱  
木桌

價格 (1 ether = 1000000000 gwei)  
1000000000 gwei

描述  
一張結實的木桌

數量 (大數)  
6

圖片  
上傳檔案 tabia.png 修改圖片  
hash: QmB8EhQ7Ww2V3QgNf55x5vH989vnlK8N2w5Hn2

詳情  
這是一張純手工打造的原木木桌，非常適合餐廳使用！  
hash: QmAT3GwN88TtK7yB8u8M9u8W59qELWGrNheV

送出交易 送出支付

圖 三-16 輸入商品資訊

圖片及詳述會儲存在 IPFS，故會得到一筆經過加密的 Hash 值，其他資料則存放於區塊鏈中。輸入完商品資訊後，點擊「送出交易」。

ShopP2P

平台簡介 交易規則 馬上註冊

### 物品資訊

名稱  
木桌

價格 (1 ether = 1000000000 gwei)  
1000000000 gwei

描述  
一張結實的木桌

數量 (大數)  
6

圖片  
上傳檔案 tabia.png 修改圖片  
hash: QmB8EhQ7Ww2V3QgNf55x5vH989vnlK8N2w5Hn2

詳情  
這是一張純手工打造的原木木桌，非常適合餐廳使用！  
hash: QmAT3GwN88TtK7yB8u8M9u8W59qELWGrNheV

送出交易 送出支付

ETH 0.2

DETAILS DATA

0.001 ETH 商人未清還上 0.001 ETH

Gas 價格 (Gwei) 0 Gas 上送 0

1 10000000

AMOUNT + GAS FEE 0.201 ETH 此筆交易平均要 0.201 ETH

忽略 確認

圖 三-17 錢包與合約互動

此時 MetaMask 會跳出合約互動的交易確認，賣家需支付售價之兩倍押金給予智能合約，點擊「確認」即可上架物品。跳出交易完成通知後，點擊「進入市場」到交易市場看上架之商品。



### 3. 買家註冊



圖 三-18 網頁 ShopP2P 首頁

到網站首頁後，點選「馬上開始」按鈕或右上角「馬上註冊」就可以進到「註冊帳號」。



圖 三-19 註冊帳號頁面

輸入你想要使用的暱稱，並按下「送出交易」，這邊的交易是合約進行 0 ETH 的交易，目的是將這個錢包地址記錄至合約中，需特別注意一個錢包地址僅能註冊一次。



圖 三-20 錢包與合約互動

我們以 MetaMask 作為錢包示範，此時 MetaMask 會跳出合約互動的交易確認，按下「確認」等待合約互動，跳出完成交易通知即完成註冊。



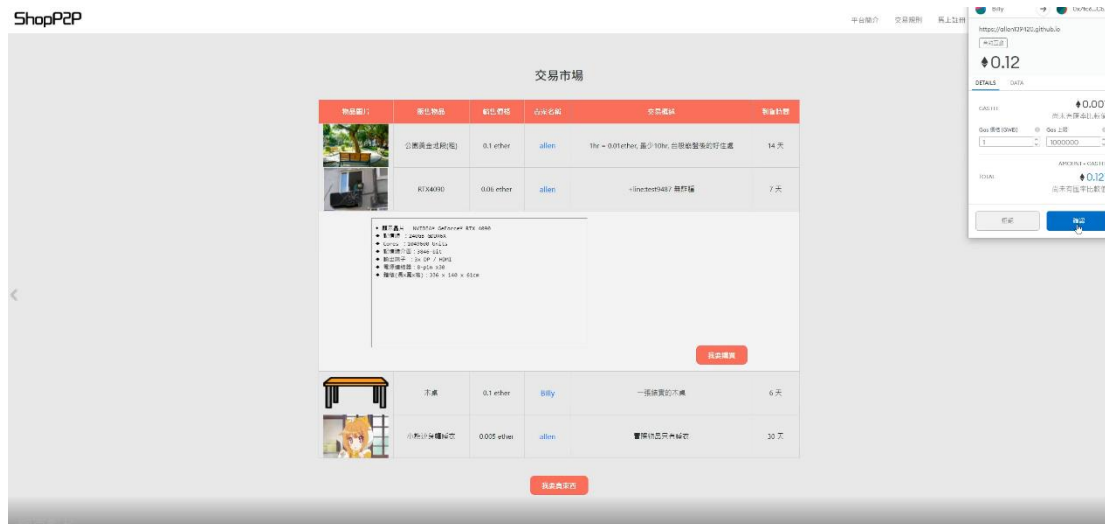


圖 三-23 購買時錢包與合約互動

點擊「我要購買」後，MetaMask 會跳出合約互動的交易確認，需要支付售價兩倍之押金給予合約，點擊「確認」等待交易。等待跳出完成交易通知，就代表下單成功。

## 6. 交付物品



圖 三-24 交易市場頁面

交易市場中的商品被買家下單，此時就不會顯示在交易市場中。

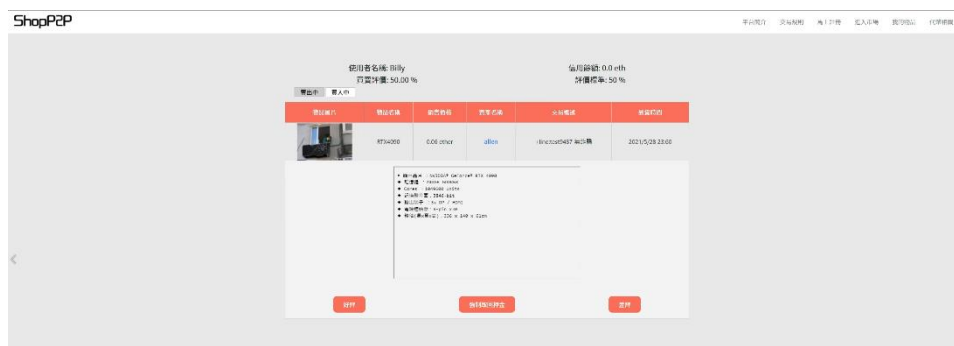


圖 三-25 我的物品頁面買入中

在買家視角中，商品改出現在「我的物品」的買入中，此時就可以跟賣家約交付物品。



圖 三-26 我的物品賣出中頁面

在賣家視角中，交易市場中的商品被下架，商品出現在「我的物品」的賣出中，此時就可以跟買家約交付物品。

## 7. 給予評價



圖 三-27 評價頁面

買家完成商品取貨後，可以選擇給予「好評」、「差評」。「強制取回押金」是在買家給予負評後，賣家遲遲不給回應評價時使用。



圖 三-28 評價時合約與錢包互動

選擇對應的評價按鈕後，需要跟合約互動，按下確認後等待執行交易及評價。等待跳出完成合約互動通知，就代表交易完成。

## 8. 賣家給予評價(僅發生於買家給予差評時)



圖 三-29 評價時合約與錢包互動

若買家給予差評，賣家可以選擇「好評」或「差評」，若買家給予好評則不會有此環節。

## 9. 返還押金

詳細情形如下圖：

假設商品售價為 10ETH，雙方交易前都給予合約 20ETH，合約內共有 40ETH：



圖 三-30 買家給好評的情況

若買家給好評，則 10ETH 轉到買家錢包，30ETH 轉到賣家錢包。



圖 三-31 買家給差評 賣家給好評的情況

若買家給差評 賣家給好評，則 30ETH 轉到買家錢包，10ETH 轉到賣家錢包。



圖 三-32 雙方給差評的情況

若雙方給對方差評，歷史評價高於標準評價者將收到原先的押金，歷史評價低於標準評價者，則由平台沒收押金。當雙方給對方差評的情況發生時，系統將會調整雙方的標準評價，使之上升 10%。歷史評價計算方式：好評總價/(好評總價+差評總價)\*100%。

#### 10. 收取懲罰金

發生於買賣家都給予對方差評，如上圖，合約會自動執行歷史評價對比，信用評價低者會被收取押金視為懲罰金。

為了解決多重帳號的問題，本組發想一種驗證機制，希望能夠把使用者與帳號進行某種綁定。我們透過發行代幣，讓使用者於設定的一小段時間內與合約進行互動，互動過後就可以獲得代幣。我們認為在同一時間內，使用者只能夠手動以一個錢包地址與合約進行互動，以此避免使用者擁有多個帳號。此外，透過這個機制，可以鼓勵使用者停留於本系統中，藉此增加 IPFS 網路節點。當使用者進入網站的時候，系統就會開啟一個計數器，這個計數器會跟合約上生成隨機數字的函數做比對，若兩數字相同，這一分鐘內透過 MetaMask 與合約互動者，就可以得到代幣，超過時間進行互動的話，會讓合約重新生成隨機數字，使之成為未來新的一個時間點。使用者擁有代幣，可以跟合約換取信用額度，以此得到比一般使用者高 1000 倍的對他人評價權重，未來交易給對手評價時，就會有放大評價的效果，目前設定一枚代幣可以換取 0.1ETH 額度內擁有 1000 倍的評價權重。

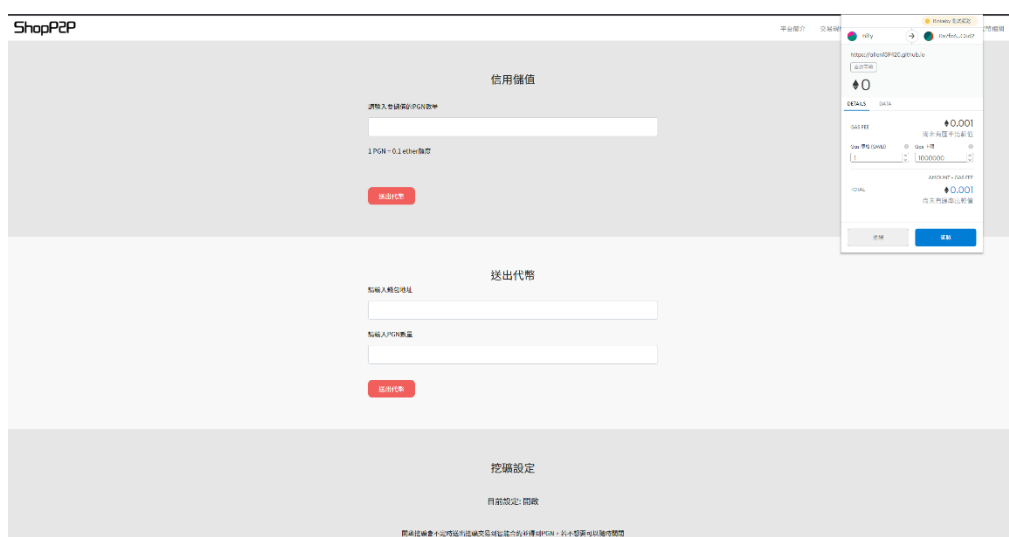


圖 三-33 代幣相關頁面

開啟挖礦設定後，時間到 MetaMask 就會跳出合約互動確認，一分鐘內完成確認者即可獲得代幣。



圖 三-34 信用儲值

信用儲值可以將 1PNG 代幣轉換成 0.1ETH 額度內擁有 1000 倍的評價權重。



圖 三-35 送出代幣

送出代幣可以實現將 PNG 代幣轉到指定錢包的功能。



圖 三-36 挖礦設定

使用者可以自行選擇是否參加挖礦，若選擇挖礦的話，當計數器跟合約上生成隨機數字的函數做比對相同時，MetaMask 將會跳出交易確認，這一分鐘內與合約互動者，就可以得到代幣。



圖 三-37 信用儲值 1PGN



圖 三-38 信用餘額 0.1ETH

完成交易後，即可發現自己的信用餘額有所提升。在 0.1ETH 額度內得到比一般使用者高 1000 倍的對他人評價權重，未來交易給對手評價時，就會有放大評價的效果。



## 第四章 結果討論與建議

本研究基於預先規劃之交易構思，提出研究架構，及探討相關文獻，實作一套保護使用者個人資訊的去中心化交易系統，讓買賣雙方擁有一個與傳統平台不同的交易選項，其設計架構與理念也可以供其他相關研究者參考。區塊鏈具有去中心化的特性，透過這個核心特性，使整個服務不再需要中心機構的監督，使用者之間的交易成為點對點交易，不可竄改性更是保護區塊鏈的重要機制，讓個別惡意使用者無法竄改整個交易過程，此外所有資訊都可以在網路上被查看，因此具有高度透明的特性，對於數據分析也能做出貢獻。本系統在個人資訊保護十分具有優勢，因為其具有匿名性的特性，整個交易僅會記錄使用者的錢包地址，而非如傳統購物平台紀錄多筆重要個人資訊。以太坊中的智能合約則是本系統的核心技術，我們在事前於智能合約建立一套完整的交易機制，透過智能合約的程式設計，每當條件成立時就會自動執行，此外我們也不用跟其他機構的區塊鏈合作，整個系統能夠自行獨立運作，免除了需要與他人交互驗證的情況。本系統運用區塊鏈的特性，大幅增加了使用者資訊的安全，使個人資料外洩的風險降至最低。本組將所有大型檔案放置於星際檔案系統中，透過這個方式，使本專案的檔案能持續且安全地分散於多個網路節點中，藉此去除以往中心化伺服器儲存的缺點，同時巧妙地解決區塊鏈本身儲存空間不足的問題。本系統仍然存在可以改進的部分，區塊鏈每次交易時需等待錢包與合約互動，這個動作是目前區塊鏈技術所必經之事，也因此使其存在一定的等待時間，未來有機會可以朝研究如何減少互動時間前進。此外，本組建議可以嘗試以太坊之外的選擇，或許會擁有更低的礦工驗證手續費，以增加本系統的市場競爭力。星際檔案系統這個去中心化儲存網路會定期清理檔案以節省網路空間，要如何維持本專案的檔案不會被清掉也是一個值得探討的議題。

## 參考文獻

- 加沛 (2018)。不可不知 何謂「智能合約」？。區塊客，  
<https://blockcast.it/2018/03/11/what-is-a-smart-contract/>。
- 陸毅軒 (2019)。實現在每秒交易數量有限之公有區塊鏈下可稽核的彩票系統  
(未出版之碩士論文)。國立臺灣師範大學，台北市。
- 梁憶芳 (2014)。基於個人資料保護法的個人資料檔案風險管理資訊系統(未出  
版之碩士論文)。國立中興大學，台中市。
- 黃英睿 (2019)。tp-Merkle tree 提高公有區塊鏈交易速度之研究(未出版之碩  
士論文)。國立臺灣師範大學，台北市。
- 蔡宛真 (2019)。區塊鏈技術於商務車聯網交易紀錄之實作與研究(未出版之碩士  
論文)。國立聯合大學，苗栗縣。
- 歐日宋 (2019)。基於區塊鏈技術之二手書交易市場(未出版之碩士論文)。國立  
清華大學，新竹市。
- 潘宜萱 (2019)。區塊鏈為基礎的信用卡交易清算架構之設計 -以台灣信用卡交  
易為例(未出版之碩士論文)。輔仁大學，新北市。
- 鍾斯羽 (2017)。應用區塊鏈技術之不動產交易系統設計(未出版之碩士論文)。  
國立臺北科技大學，台北市。
- 財團法人台灣網路資訊中心 (2020)。2020 台灣網路報告書。  
<https://report.twnic.tw/2020/index.html>
- Benet, J (2014). *IPFS - Content Addressed, Versioned, P2P File System*.  
Retrieved from <https://arxiv.org/abs/1407.3561>
- Buterin, V. (2017). *A next generation smart contract & decentralized  
application platform*. Retrieved from <https://blockchainlab.com>
- Koteska, B., Karafiloski, E., Mishev, A. (2017). *Blockchain  
Implementation Quality Challenges: A Literature Review*. Sixth  
Workshop on Software Quality Analysis, Monitoring, Improvement,  
and Applications, Belgrade, Serbia. Retrieved from  
<https://www.researchgate.net/publication/320127088>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.  
Retrieved from [www.bitcoin.org](http://www.bitcoin.org)
- Shahsavari, Y., Zhang, K., Talhi, C. (2019). *Performance Modeling and  
Analysis of the Bitcoin Inventory Protocol*. IEEE International  
Conference on Decentralized Applications and Infrastructures  
(DAPPCON 2019), San Francisco, California, USA. Retrieved from  
[www.researchgate.net/publication/331639364](https://www.researchgate.net/publication/331639364)