國立東華大學資訊工程學系

大學部畢業專題

指導教授：賴志宏 博士

區塊鏈交易系統－ShopP2P

A Trading System Based on Blockchain Technology: ShopP2P

組員： 洪廷鈞、徐培欽

中 華 民 國 一 一 〇 年 五 月

摘要

過去的交易模式存在成本及安全性的問題，在成本中包含了各式費用，如維護費用、人事費用、廣告費用及推銷費用等等，這些對於使用者來說都是不必要的交易成本，此外在購物平台的伺服器中儲存了大量的使用者個人資訊，使得資訊安全也產生疑慮。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，將以使用者目前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。透過當前的區塊鏈技術，本組打造出一個完整的交易系統，建立公平合理的交易成本，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、以太坊、智能合約、購物系統、點對點交易

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，「從電子商務使用情形方面來看，台灣網友電子商務使用率高於全球平均」(2020，財團法人台灣網路資訊中心)，更加突顯了國內網路購物市場的熱絡。當今市面上的知名電商平台都是以提供服務換取收入的經營模式為主體，讓使用者擁有便利交易資訊，由平台擔任交易過程的監督者，交易者在享受便利的服務時，必須支付一筆相當可觀的手續費，手續費的收取大部分都是為了滿足企業「營利」，而在達到營利之前，企業必定會花費大筆費用在於維護費用、人事費用、廣告費用、行銷費用等等，本組認為這樣的使用者收費方式不夠公平且合理。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，整個交易過程僅收取實現完成交易的最低「交易成本」，使用者的金錢只會用於最重要的核心上，不再是用於各種不必要的支出，令費用的收取更加公平合理。除了手續費問題外，我們也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。交易成本及資訊安全是現存交易平台還能改進的部分，我們期待能打造收費公平合理及保障使用者個人資料的交易模式，實現一個對交易更加友善的世界。

第二節 目的

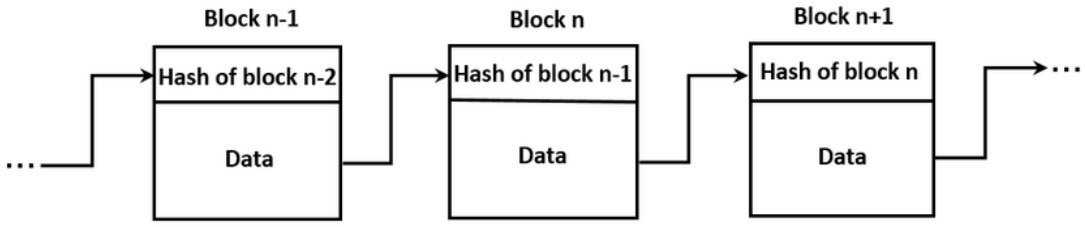
現今電商購物平台的交易成本中包含了各種額外費用，我們希望能將這些費用壓縮到最小，不讓維護費用、人事費用及廣告費用及行銷費用佔據使用者交易的一大部分，僅留下最核心的交易成本。本組透過區塊鏈技術發想出一種收費公平合理及保障個人資訊安全的交易模式，我們借重區塊鏈的各項優點，買賣雙方僅須負擔完成交易的「最低成本」，不必再被中介機構多收取一筆營業收入，同時交易僅會記錄錢包地址。本組規劃建立一套系統，是以區塊鏈作為核心，再加上一套本組發想出來的信用評比機制，期待能創造出對整個社會更棒的交易系統。

第二章 相關研究

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漲，人們對於安全問題也開始重視。近幾年，區塊鏈以去中心化、不可竄改及公開透明的特性，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出完整的程式邏輯。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，以此提升網路購物時的安全性與交易公平性。

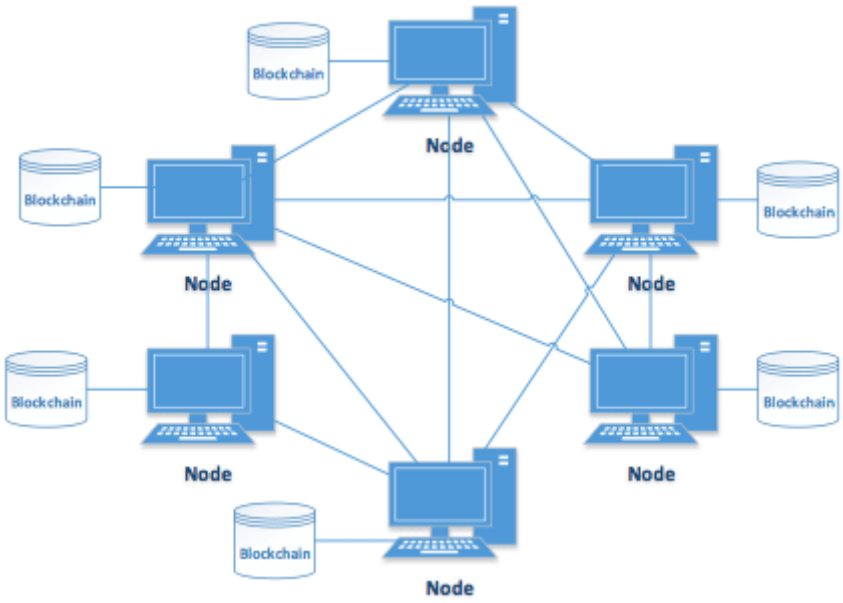
第一節 區塊鏈簡介

區塊鏈的概念最早來自於 Satoshi 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，如圖一(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。



圖一、區塊鏈示意圖 (2019，Kaiwen Zhang)

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、區塊鏈 P2P 網路示意圖(2017，Bojana Koteska)

第二節 以太坊及智能合約簡介

以太坊是以區塊鏈為基礎而出現的開源平台，「運行的加密貨幣為以太幣，使用者可以在上面進行交易、撰寫與發佈程式(智能合約)來發展多元化的應用」(2019，陸毅軒)，具有圖靈完備的特色，可以編寫智能合約到區塊中，「一個建立在以太坊之上的特殊協議被稱為智能合約」(2017，V Buterin)，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，而因智能合約是存放於區塊鏈中，因此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。」(2018，加沛)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。

若想使用智能合約，通常是利用 Solidity 的程式語言撰寫，若想要順利執行智能合約，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「使交易時程縮短並防止詐騙」(2017，鍾斯羽)的不動產交易系統，「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」(2017，鍾斯羽)，其想法與本組相近，皆是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。

本組的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」(2019，潘宜萱)，藉由區塊鏈即能達成此目標。交易時的交易效率亦是非常重要的一點，「透過區塊鏈機制的設計，實現點對點之間的清算，能夠簡化作業流程、提高營運效率以及降低交易成本」(2019，潘宜萱)，因此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 C2C 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，「基於對於中央式機構的信任，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」(2019，黃英睿)，相比之下，在分散式系統中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」(2019，黃英睿)。

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。」(2019，蔡宛眞)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。

交易手續費是影響買賣雙方是否使用服務的重要因素，「Books may be sold effectively and securely through smart contracts and are rewarded by having lower price fees than other platforms.」(2019，歐日宋)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四種情況(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、買家強制取回押金。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，若買方歷史評價低於標準評價，則智能合約會將 2X 給予賣家，2X 給予平台；若賣方歷史評價低於標準評價，則智能合約會將 2X 給與買家，2X 給予平台；若雙方歷史評價低於標準評價，則平台得到 4X。在買家強制取回押金機制中，代表買家給予差評後，賣家遲不給予回評，則買方得到 3X，賣方得到 X。整個信用機制整理如下表。

假設商品售價為 X 的情況，雙方交易前都給予合約 2X，合約內共有 4X：

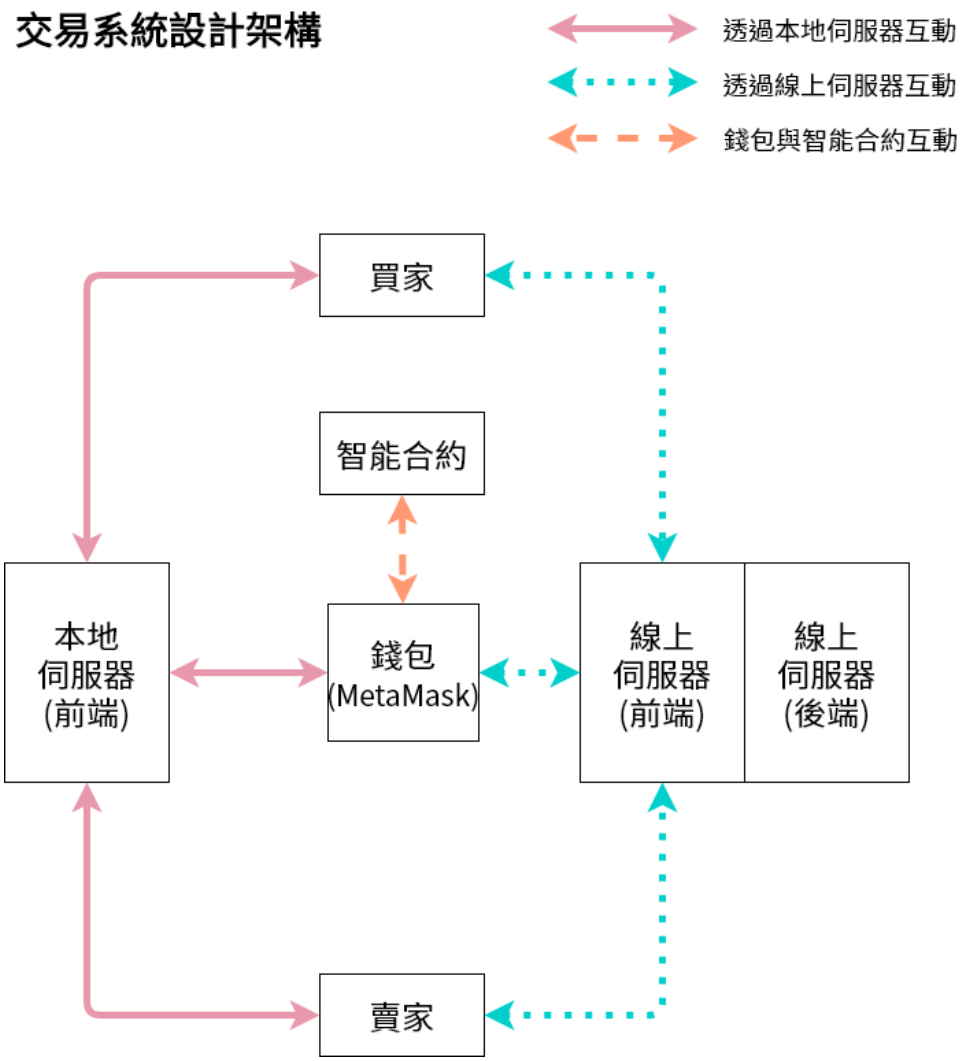
買家給評	賣家給評	發生時機	發生事件
好評		雙方交易順利	買方得到 X 賣方得到 3X 平台得到 0
差評	好評	賣家有問題	買方得到 3X 賣方得到 X 平台得到 0
差評	差評	雙方認為對方有問題	若買方歷史評價低於標準評價： 買方得到 0 賣方得到 2X 平台得到 2X
			若賣方歷史評價低於標準評價： 買方得到 2X 賣方得到 0 平台得到 2X
			若雙方歷史評價低於標準評價： 買方得到 0 賣方得到 0 平台得到 4X
強制取回押金		買方給予差評後，賣家不給回應評價	買方得到 3X 賣方得到 X 平台得到 0

表一、信用機制

第三章 系統介紹

第一節 環境

本組專案主要分成智能合約及網頁部分。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 0.8.0 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 及 Bootstrap5.0.0，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。

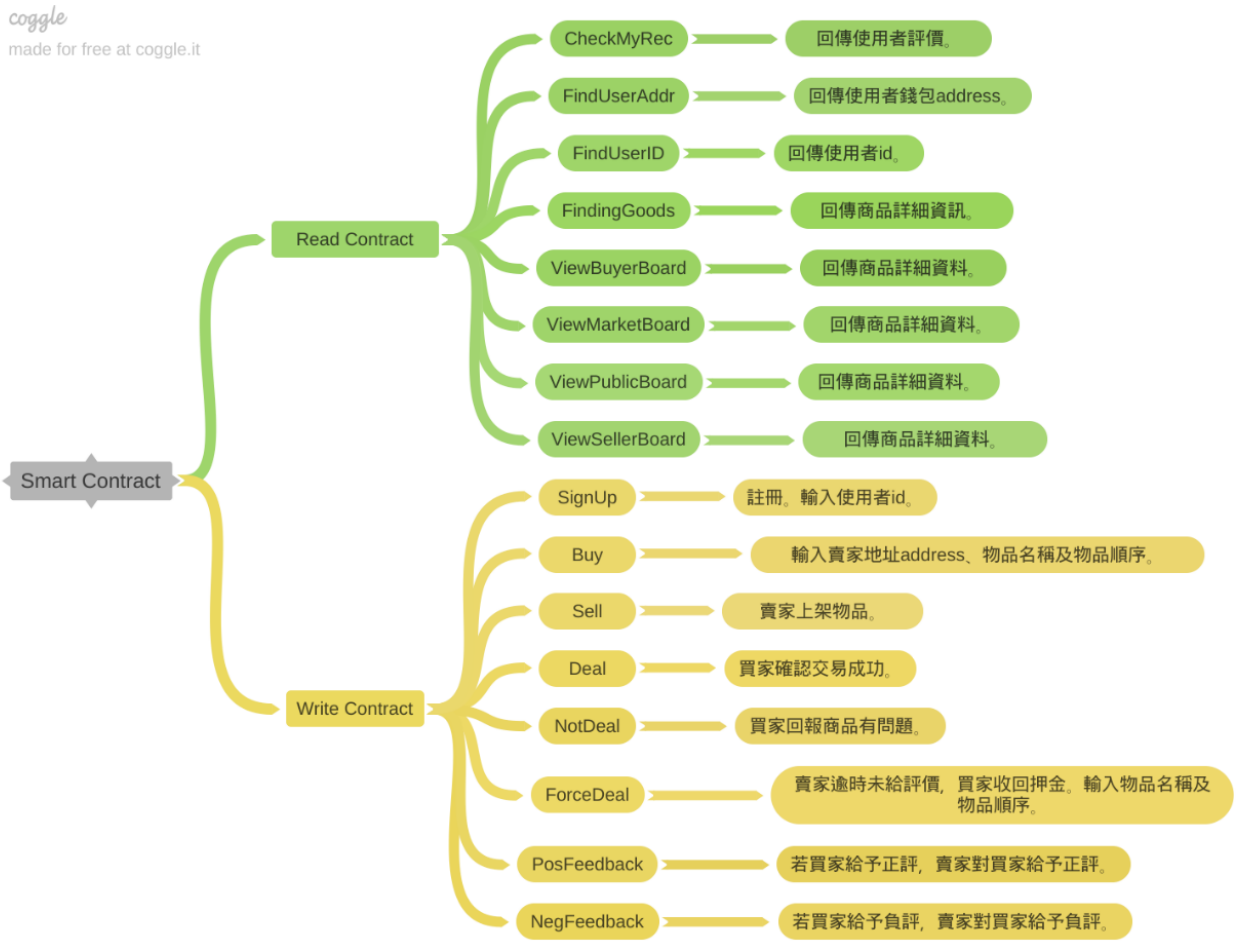


圖三、交易系統設計架構

本交易系統的買賣交易都是在智能合約上進行，使用者可以透用 MetaMask 這款錢包與合約進行所有交易互動，為讓所有使用者更方便使用，我們建立了一個網頁平台，使用者可以下載到自己電腦利用本地伺服器連上智能合約，或是直接連接我們架設的線上伺服器，我們透過 API 及 ethers.js 技術使合約內容可以呈現在網頁上，大幅降低了不熟悉以太坊及智能合約使用者的使用門檻。

第二節 智能合約內容簡介

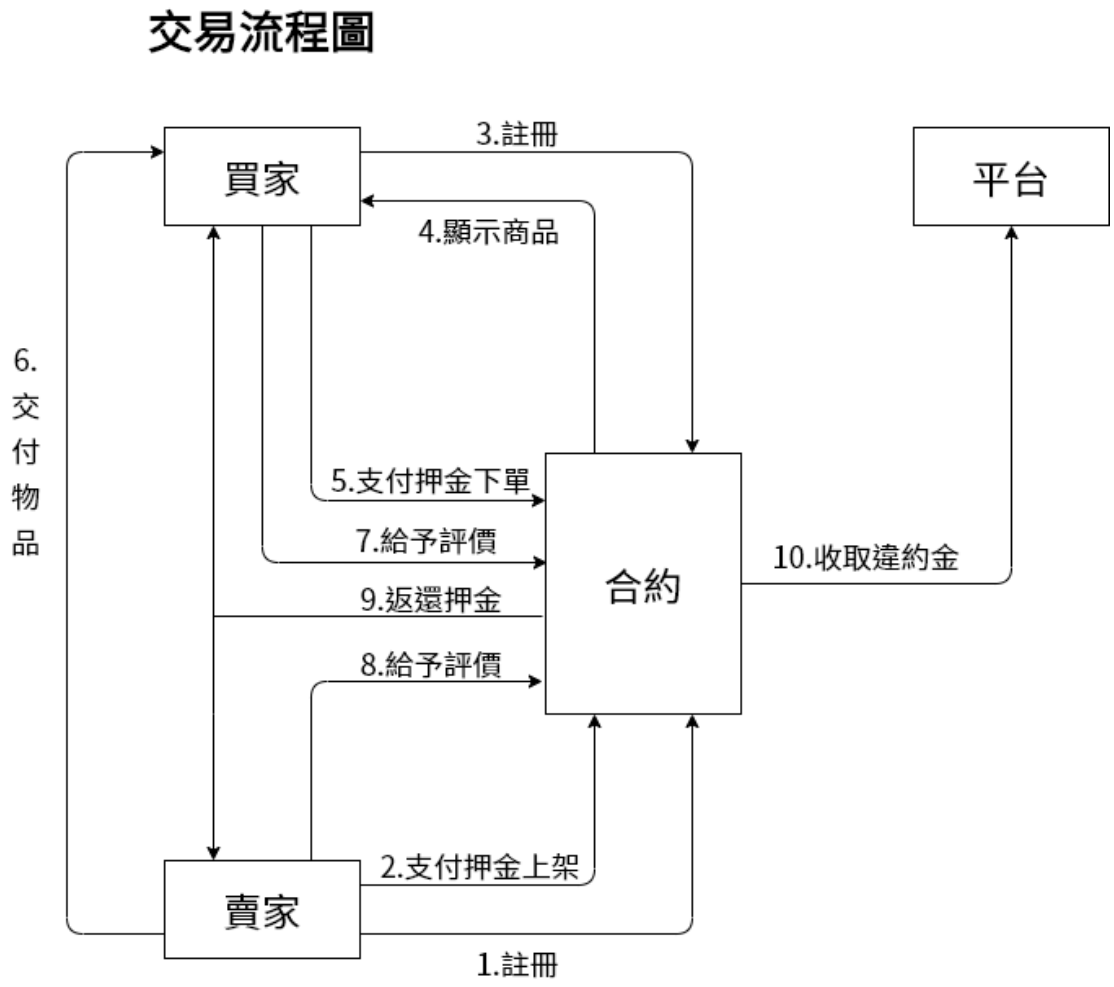
目前智能合約內有 Read Contract 及 Write Contract。在 Read Contract 中有 CheckMyRec、FindUserAddr、FindUserID、FindingGoods、ViewBuyerBoard、ViewMarketBoard、ViewPublicBoard 及 ViewSellerBoard 等功能。在 Write Contract 中有 SignUp、Buy、Sell、Deal、NotDeal、ForceDeal、PosFeedback 及 NegFeedback 等功能。在 Read Contract 的部分都是用於讀取區塊鏈內容，我們不需要花費任何的 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，詳細智能合約內容介紹如下圖，所有程式碼皆於附錄中。



圖四、智能合約內容

第三節 使用流程

本節將詳細介紹交易平台的使用方式，我們一共分為十個步驟，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、返還押金及收取違約金。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。



圖五、交易流程圖

1. 賣家註冊

圖六、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」。

圖七、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。

圖八、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。

2. 支付押金上架

圖九、交易市場頁面

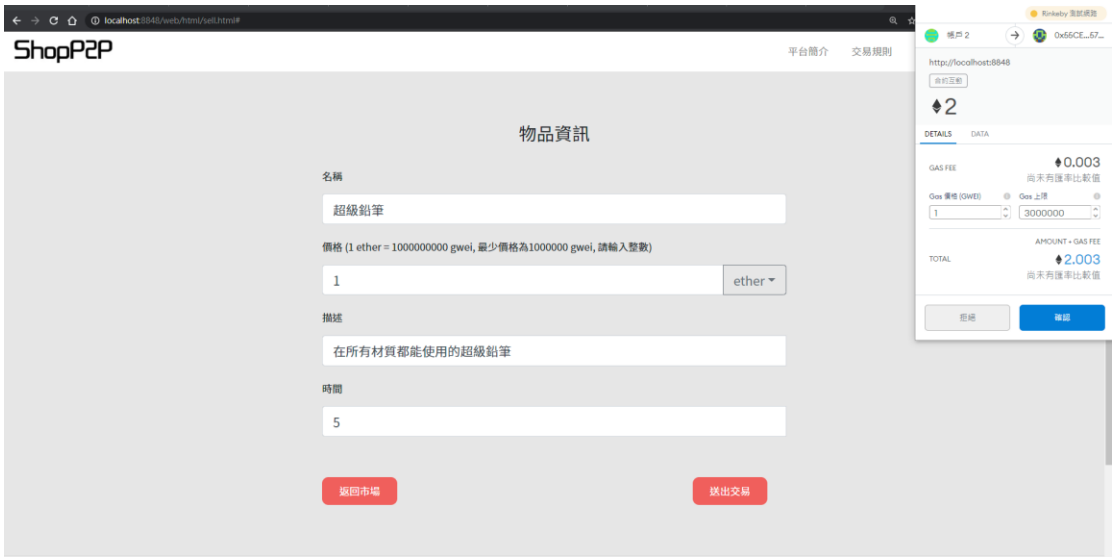
註冊完成後，可以點擊「進入市場」到交易市場，這邊會顯示目前販售中的物品。若使用者想要販售物品，此時可以點擊「我要賣東西」。

圖十、物品資訊頁面

選擇我要賣東西後，需要輸入商品資訊，包含商品名稱、價格、描述及時間（幾日內可以完成物品交付）。

圖十一、輸入物品資訊

輸入完商品內容後，點擊「送出交易」。



圖十二、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

圖十三、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」。

圖十四、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。

圖十五、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。

4. 顯示商品

圖十六、交易市場頁面

從交易市場中可以看到上架的物品已經在交易市場中等待購買，此時可以看到販售物品、販售價格、賣家名稱、交易概述及到貨時間。

5. 支付押金下單

圖十七、交易市場中購買頁面

如果想要買東西的話，點選商品後會跳出「我要購買」按鈕。

圖十八、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

圖十九、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。

圖二十、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。

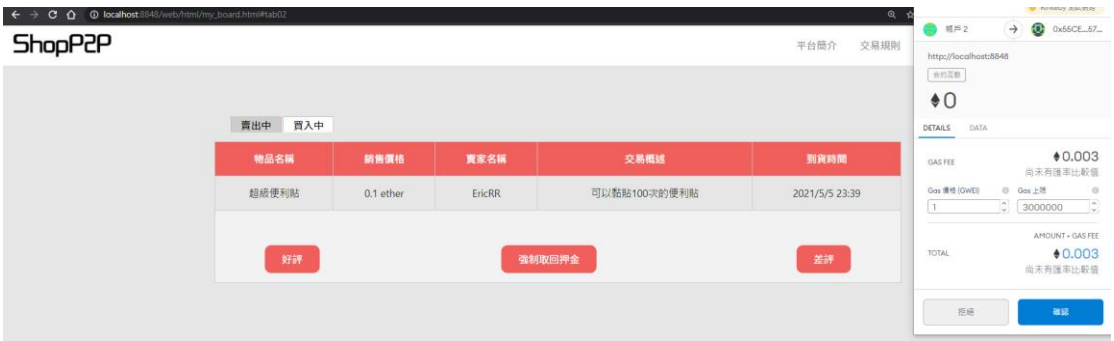
圖二一、我的物品賣出中頁面

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

圖二二、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。



圖二三、平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)

圖二四、平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

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

買家給評	賣家給評	發生時機	發生事件
好評		雙方交易順利	買方得到 10 ETH 賣方得到 30 ETH 平台得到 00 ETH
差評	好評	賣家有問題	買方得到 30 ETH 賣方得到 10 ETH 平台得到 00 ETH
差評	差評	雙方認為對方有問題	若買方歷史評價低於標準評價： 買方得到 00 ETH 賣方得到 20 ETH 平台得到 20 ETH
			若賣方歷史評價低於標準評價： 買方得到 20 ETH 賣方得到 00 ETH 平台得到 20 ETH
			若雙方歷史評價低於標準評價：

			買方得到 00 ETH 賣方得到 00 ETH 平台得到 40 ETH
強制取回押金		買方給予差評後， 賣家不給回應評價	買方得到 30 ETH 賣方得到 10 ETH 平台得到 00 ETH

表二、返還押金情況說明

10. 收取違約金

發生於買賣家都給予對方差評，如上表，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違約金。

第四章 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，實作一套去中心化且公平合理收取手續費的交易系統，讓買賣雙方擁有一個不同的交易選項，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，讓整個服務不再需要中心機構的監督，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，在個人資訊保護也十分具有優勢，因為其具有匿名性的特性。以太坊中的智能合約則是本系統的核心技術，我們透過各種事前建立的交易機制，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，因此讓整個系統能夠獨立運作，免除了需要與他人交互驗證的情況。透過本組提出的系統，使用者可以讓總成本的組成僅剩下交易成本，不再是傳統以維護費用、人事費用及廣告行銷費用堆疊而成一個肥大的交易成本。本系統運用區塊鏈的特性，大幅增加了使用者資訊的安全。本平台每次交易時需等待錢包與合約互動，故無法做到即時交易，未來有機會可以研究如何減少互動時間，此外可以嘗試以太坊之外的選擇，或許會擁有更低的交易成本，以增加在費用方面的競爭力。

參考文獻

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

Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.www.bitcoin.org*

Yahya Shahsavari, Kaiwen Zhang, Chamseddine Talhi (2019). Performance Modeling and Analysis of the Bitcoin Inventory Protocol. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON 2019) At: San Francisco, California, USA. Retrieved from www.researchgate.net/publication/331639364

Bojana Koteska, Elena Karafiloski, Anastas Mishev (2017). Blockchain Implementation Quality Challenges: A Literature Review. Sixth Workshop on Software Quality Analysis, Monitoring, Improvement, and Applications At: Belgrade, Serbia. Retrieved from https://www.researchgate.net/publication/320127088

V Buterin (2017). A next generation smart contract & decentralized application platform. Retrieved from https://blockchainlab.com/

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。

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/。

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。

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。

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。

蔡宛眞 (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。