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***



專題成員： 洪廷鈞、徐培欽

中華民國一一○年五月

**中文摘要**

關鍵字

**英文摘要**

關鍵字

**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到交易對手，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。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企業的「營利」，本組認為這樣的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，交易成本可從當前的按售價收取手續費，改變為按「交易成本」收取，讓費用的收取更加合理。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，這些資料可能包括姓名、手機號碼、居住地址及信用卡號碼等等，此舉使得使用者資料安全產生疑慮。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**

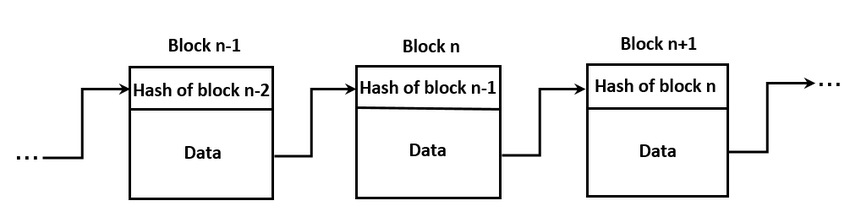
現有的電商平台對於手續費的收取不夠合理完善，目前交易機制會隨著交易價格的上升使手續費跟著上升，然而交易高單價的物品並不代表交易成本就會比較高。本組發想出一種收費公平合理及保障個人資訊安全的交易模式，買賣雙方僅須負擔完成交易的「最低成本」，不必再被中介機構多收取一筆營業收入，同時交易僅會記錄錢包地址。有了構思後，本組規劃建立一套系統，我們以區塊鏈為核心，實現發想的交易模式，期待能創造出更棒的交易平台。

**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。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，所有交易透過礦工的共識運算，讓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、區塊鏈示意圖 (2019，Kaiwen Zhang)

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。

**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，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。

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)。

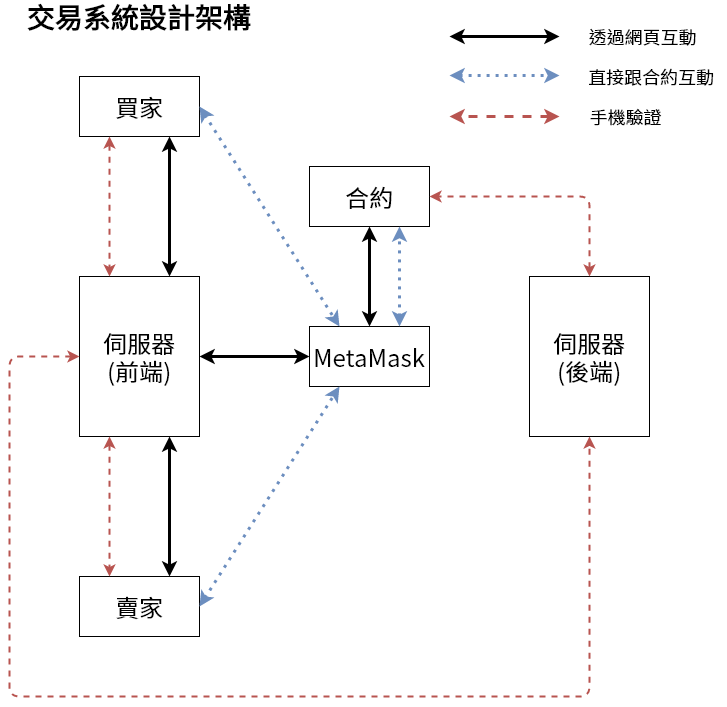
在區塊鏈中，所有的交易資訊都是公開透明且不可竄改的，我們可以透過公開鏈去檢視每一筆交易紀錄，從而得出具有價值的數據資料。「透過適當的統計，可提取出對產業有幫助的結果。」(2019，蔡宛眞)我們認為以區塊鏈為核心的交易平台能打破交易中心機構獨自把持數據的現況，為社會帶來更多的數據使用價值。

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。

**第三章 系統介紹**

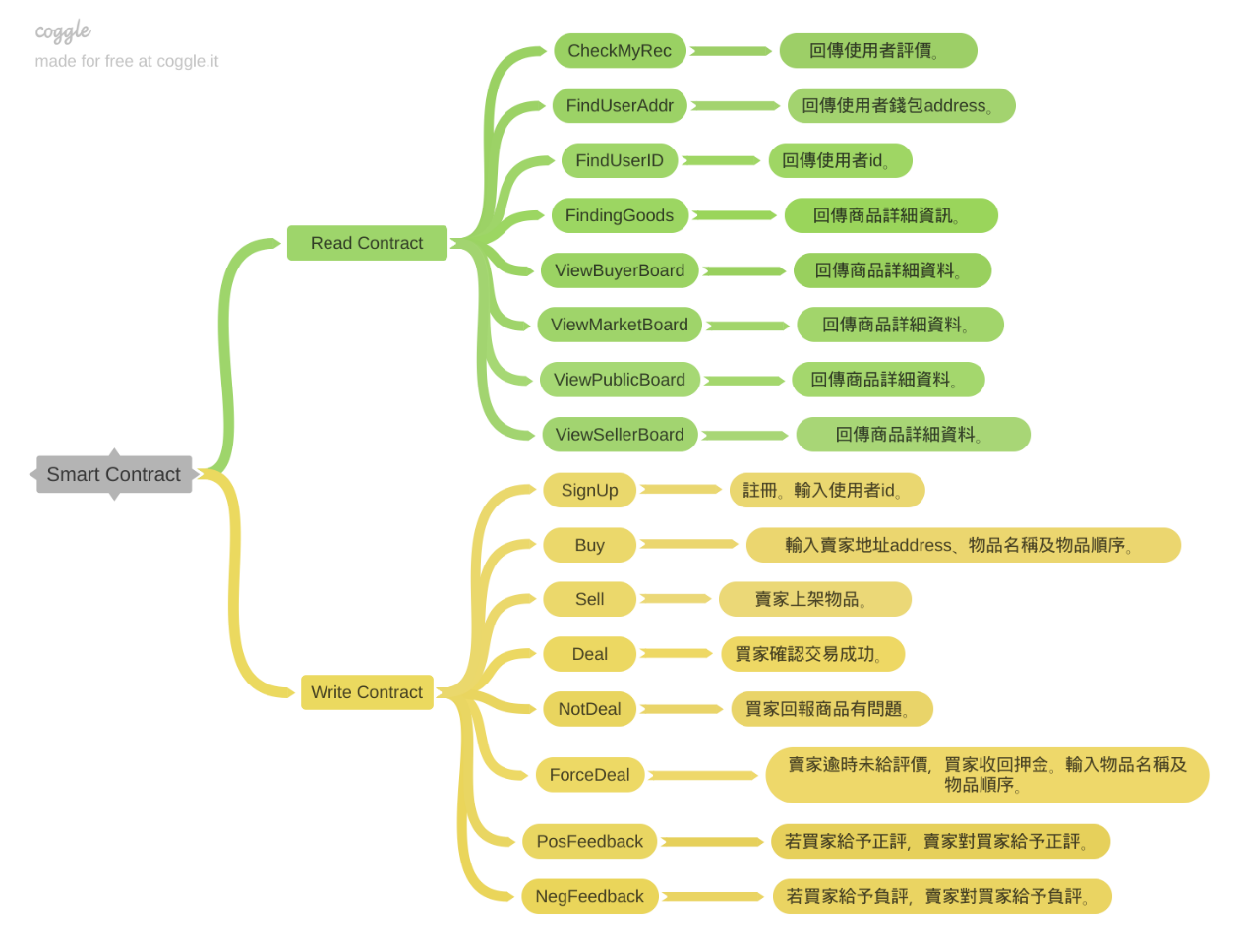
**第一節 環境**

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、交易系統設計架構(介紹此圖)

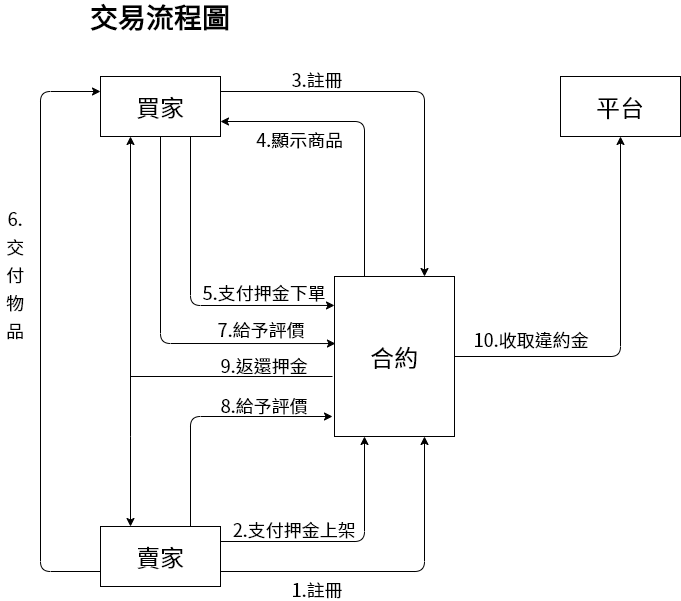
**第二節 智能合約內容簡介**

 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。

圖、智能合約內容簡介

**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，並切換至Rinkeby測試網路。



圖、交易流程圖

1. 賣家註冊



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」。



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。



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。

1. 支付押金上架



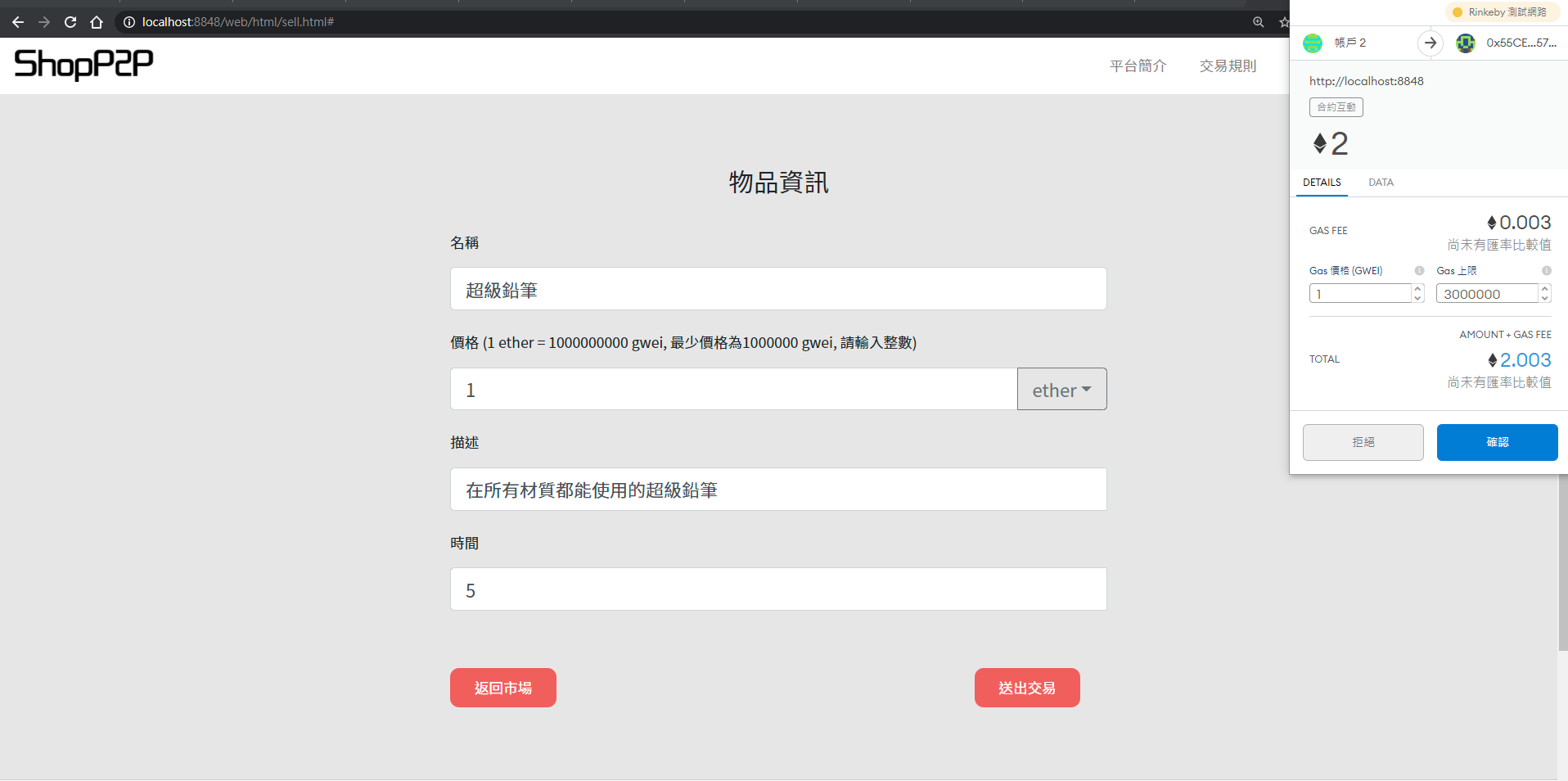
註冊完成後，可以點擊「進入市場」到交易市場，這邊會顯示目前販售中的物品。若使用者想要販售物品，此時可以點擊「我要賣東西」。



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)。



輸入完商品內容後，點擊「送出交易」。



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。

1. 買家註冊



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」。



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。



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。

1. 顯示商品



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。

1. 支付押金下單



如果想要買東西的話，點選商品後會跳出「我要購買」按鈕。



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。

1. 交付物品



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。

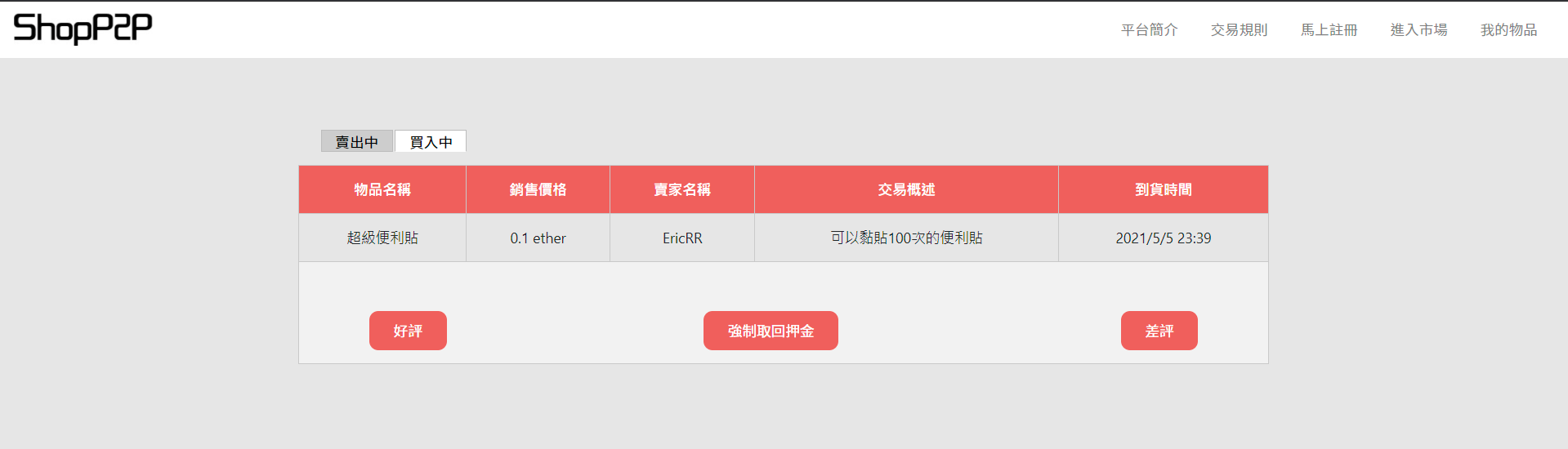


在買家視角中，商品改出現在「我的物品」的買入中，此時就可以跟賣家約交付物品。

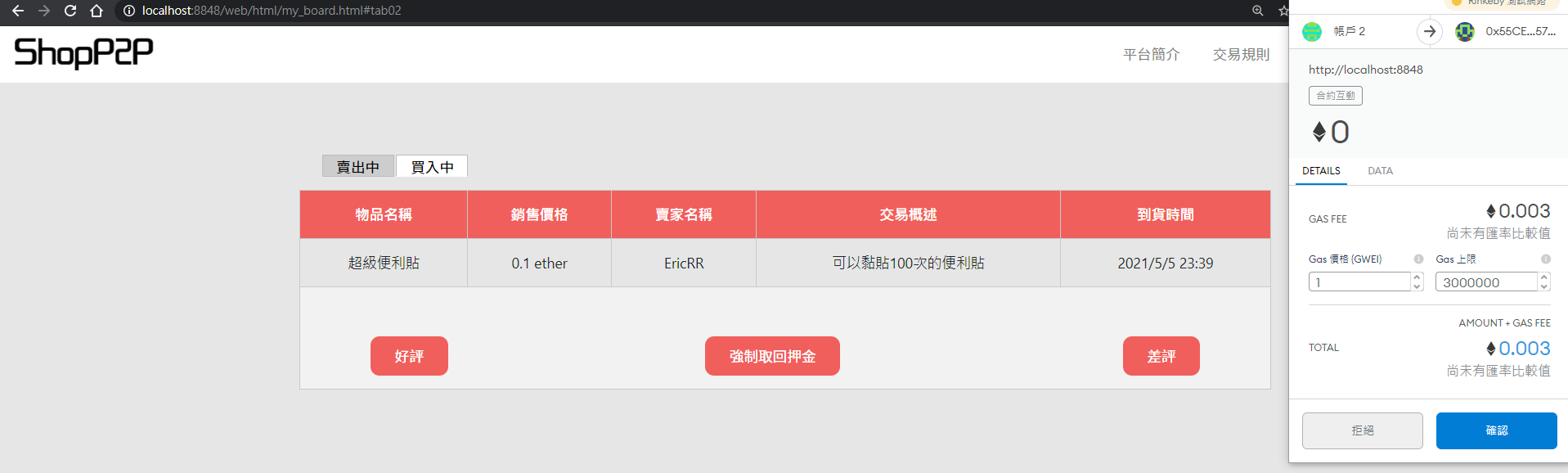


在賣家視角中，交易市場中的商品被下架，商品出現在「我的物品」的賣出中，此時就可以跟買家約交付物品。

1. 給予評價



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。



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。

1. 賣家給予評價(僅發生於買家給予差評時)



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。

1. 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 | 賣家商品有瑕疵 | 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 |

1. 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平台，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。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。(虛擬貨幣的優點、自己的跟別人的差異&解決的甚麼問題)

**參考文獻(期刊>研討會>學位論文)**

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

Kaiwen Zhang (2019). Performance Modeling and Analysis of the Bitcoin Inventory Protocol. *www.researchgate.net/publication/331639364*

V Buterin (2017). A next generation smart contract & decentralized application platform. *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。

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。