

產品資訊驗證之區塊鏈技術應用

鄭錦楸¹、吳承浩²

¹ 南臺科技大學 資訊工程系、² 南臺科技大學 資訊工程系

¹chiou@stust.edu.tw、²mb1g0107@office.stust.edu.tw

摘要

為了保護商品資訊不被竄改，將商品資訊上傳至區塊鏈來達成目的，並且建立平台提供購買時的商品資訊驗證。若商品非具有時效性，則可以使用商品歸屬機制，也就是商品販售後，店家會替購買者將購買者自訂的 pincode 加上該商品的雜湊值重新上傳至區塊鏈，後續查看紀錄時，可以看到該商品為何人所擁有。

關鍵詞：區塊鏈、商品足跡、以太坊

Blockchain Technology Application for Product Information Validation

Jiin-Chiou Cheng¹, Cheng-Hao Wu²

^{1,2} Southern Taiwan University of Science and Technology, Computer Science and Information Engineering

¹chiou@stust.edu.tw, ²mb1g0107@office.stust.edu.tw

Abstract

To safeguard the integrity of product information, we upload it to the Blockchain and establish a platform for verifying the information at the point of purchase. If the product is not time-sensitive, we can utilize a product attribution mechanism. This means that after a sale, the store will re-upload the product onto the Blockchain for the purchaser, along with their customized PIN code and the product's hash value. This way, when checking the record later, the owner of the product can be identified.

Keywords : Blockchain 、 Product Footprint 、 Ethereum

壹、前言

現今社會商品製作技術越來越精進且純熟，例如有一項商品正在市場上發光發熱時，其他廠商的仿製品以及山寨品也隨之出現，導致光是看基本外觀很難辨別出真偽，但看商品背面的詳細資訊的真實性又有一定的質疑，因此利用區塊鏈技術的可追溯性及不可逆的特性來將商品資料牢牢記錄在鏈上，當消費者購買商品後，可透過掃描 QR Code 來查看商品從源頭到現在拿在手裡一條龍的經手資訊。

1.1、研究背景

人們在購買市面上眾多產品時，最怕挑選到有些乍看之下幾可亂真的仿製品，或是透過重新包裝偽裝成全新產品的二手貨。若產品為食用或親膚產品，更可能造成自身的危害。所以本系統希望透過區塊鏈的特性儲存商品的資訊，提供消費者在購買時多一份保障。

1.2、研究動機

為了達到保護資料的完整性又不讓資料被輕易竄改，除了將資料儲存於一般的資料庫以外，再將資料利用以太坊區塊鏈技術以 SHA-256 雜湊演算後，進行資料上鏈儲存，最終消費者購買產品後，可至區塊鏈上查詢商品的資料，因為區塊鏈的可回溯、不可逆性及分散式儲存的特性，讓消費者可以百分之百相信鏈上所查詢到的資料真實性，當某一節點的資訊不幸遭到修改時，其他未被駁的節點可以提供自己的資料來與已遭修改的資料進行比對，遵從少數服從多數的原則，若被修改的資料與多數未被修改的資料不一致，則該項被修改的資料會被其他節點的正確資訊所校正，有別於使用一般資料庫時，當資料庫被駭客進入並竄改內容時，整體資料的完整性就遭受破壞的風險，若要重新將資料校正回正確的資料，只能拿取先前資料庫備份的資料，若是資料來不及備份就遭到竄改，那麼該資料庫則會失去它的完整性難以復原正確的資料。

1.3、研究目的

統整以上描述內容，本研究主要目的是，透過響應式網頁建立一個平台 (DApp)。廠商在將商品上傳時，須透過電腦登入廠商編輯頁面，才能將商品資訊透過單次/批次上傳，給予任何有需要保護與儲存商品資訊的實體商品銷售廠商能藉由本系統將產品資訊上傳區塊鏈，替自己的產品資訊作一份保障；消費者則可以透過網址進到驗證平台，接著輸入序號進行商品資訊驗證，或透過手機掃描 QR Code，讓 QR Code 自動帶入序號，即可進行商品資訊驗證，購買後的消費者，還可使用商品結帳時所得到的 PIN 碼進行歸

屬的功能，讓所有希望消費品質與安全能得到保障的消費者安心。

貳、文獻探討

2.1、區塊鏈 (Blockchain)



圖 1：區塊鏈五大特色

區塊鏈又稱分散式帳本。每筆交易都會被傳送到網路上提供給參與應用的節點，每個節點也會被永久保存任何產生的交易紀錄，因此不用擔心造假問題，實現所謂分散式記帳；也不必擔心惡意竄改問題，除非發生 51% 攻擊，也就是過半數節點原有資訊皆被竄改；而主流的區塊鏈應用案例為比特幣、以太坊，強調去中心化，不經由任何中央機構發行，僅遵守不可修改的程式運作，每個使用者皆是透過雜湊的公鑰及私鑰匿名執行任何操作；交易記錄會公開在查詢平台，俗稱區塊鏈瀏覽器，任何對象所發布的合約或是交易行為皆可被檢視。

基於以上原因，區塊鏈滿足下列特色：[1]

1. 去中心化
2. 可追蹤性

3. 不可竄改
4. 匿名公開
5. 加密安全



圖 2：以太坊

2.2、以太坊 (Ethereum)

Ethereum 是一個被廣泛使用的區塊鏈平台，使用者可以在其上撰寫並發佈程式，也就是所謂的智能合約，以發展各種去中心化的應用。在 Ethereum 中，智能合約透過去中心化的以太虛擬機 (Ethereum Virtual Machine) 來處理，給予使用者在區塊鏈上建立自己的去中心化應用，並達到更高程度的安全性和信任度。



圖 3：智能合約發佈及執行

2.2.1、以太坊-智能合約

使用 EVM (Ethereum Virtual Machine)，任何使用者都可以在平台上撰寫和發布智能合約。這些智能合約可以被儲存在 Ethereum 的某個區塊中，並在執行時被 EVM 處理。(圖 3) 說明智能合約 (Smart contract Source code) 撰寫、發布，及執行的過程，智能合

約需要先被編譯 (Compiler) 成 EVM bytecode，並在發布至區塊鏈網絡之後，才可在 EVM 上執行。[2]



```
contract SimpleStorage {
    uint storedData;

    function set(uint x) {
        storedData = x;
    }

    function get() constant returns (uint retVal) {
        return storedData;
    }
}
```

圖 4：Solidity 範例程式

2.2.2、Solidity

(圖 4) 是以 Solidity 語言撰寫之智能合約範例，智能合約可在 EVM 上執行。

(圖 3) Smart contract Source code 編譯後，變成可在 EVM 上執行的 Bytecode，當智能合約發布至區塊鏈網絡後，如同一般紙本合約簽署後的效用，合約參與者必須遵守合約內容規定，對智能合約而言，則是使用該合約的人，必續遵從合約內的程式碼邏輯，並且程式碼發布後，就被鎖住不可再變動。

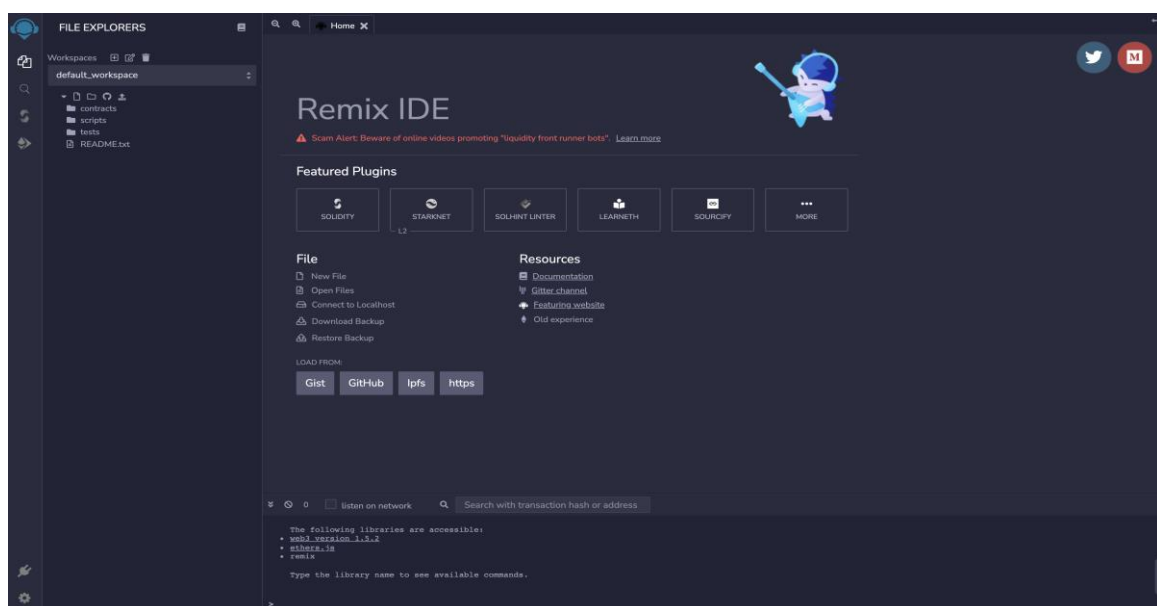


圖 5：Remix IDE 開發環境

2.2.3、Remix IDE

(圖 5) 開發智能合約的整合工具 Remix IDE，它是以太坊官方推薦的一個開發環境，專門為開發智能合約的提供了豐富的功能，其中包含完整的編譯器，可讓開發者編譯 Solidity 程式碼，並在 EVM 上執行智能合約。此外，Remix IDE 還提供環境建置的功能，讓開發者可以快速且方便地建立各種測試環境，便於進行測試和除錯並發布智能合約。

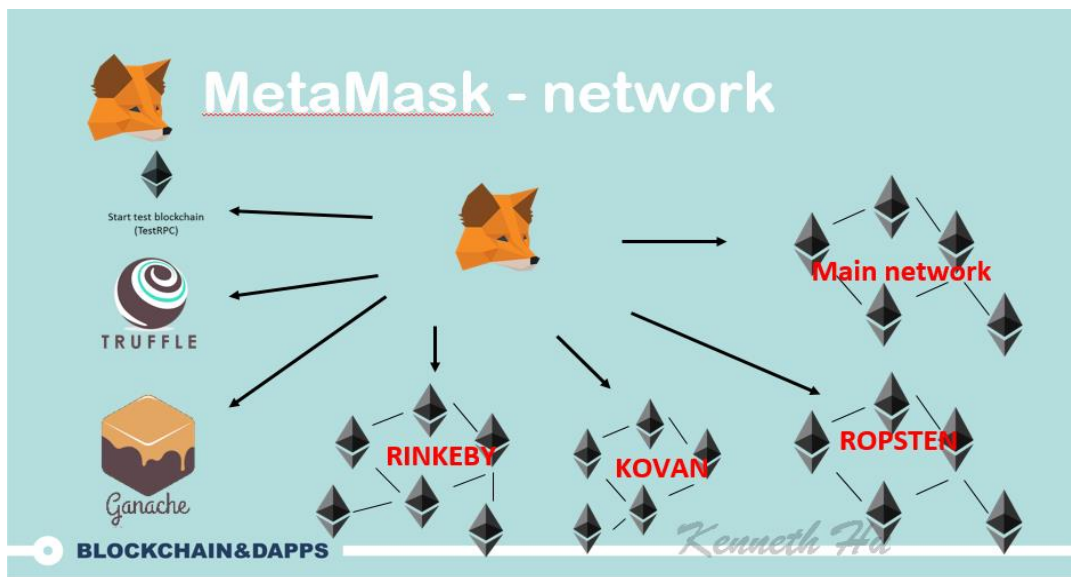


圖 6：MetaMask 網路圖

2.3、MetaMask

如 (圖 6) 架構，在公共測試網絡 (Ropsten, Rinkeby 等) 上測試 Dapp，然後啟動主網絡時，web3 provider 必須運行你佈署合約相同的網絡才能訪問合約，而能夠讓合約互動的管道可以用 Google Chrome 的擴充套件 MetaMask，這樣就可以連接到本地運行的 EVM 區塊鏈、公共測試鏈或以太坊公有鏈。[3]

2.4、Web3.js

```
var Web3 = require('web3');

if (typeof web3 !== 'undefined') {
  web3 = new Web3(web3.currentProvider);
} else {
  web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:8545"));
}
```

圖 7：引入 web3.js

web3.js 是一組用來和本地或遠程以太坊節點進行連接的 js 庫，以便讓 DApps 能夠訪問區塊鏈上的數據。依 (圖 7) 範例程式在底層的實現上，它是通過 RPC (遠端程序呼叫) 協議與節點通信，web3.js 可以與任何對外公開 RPC 介面的區塊鏈節點連接。[4]

參、方法

3.1、系統規劃

本系統分為三個區域，一個是「廠商商品資料上傳」，另一個是「消費者驗證商品資訊」，第三個是「商品 QR Code 產生器」。

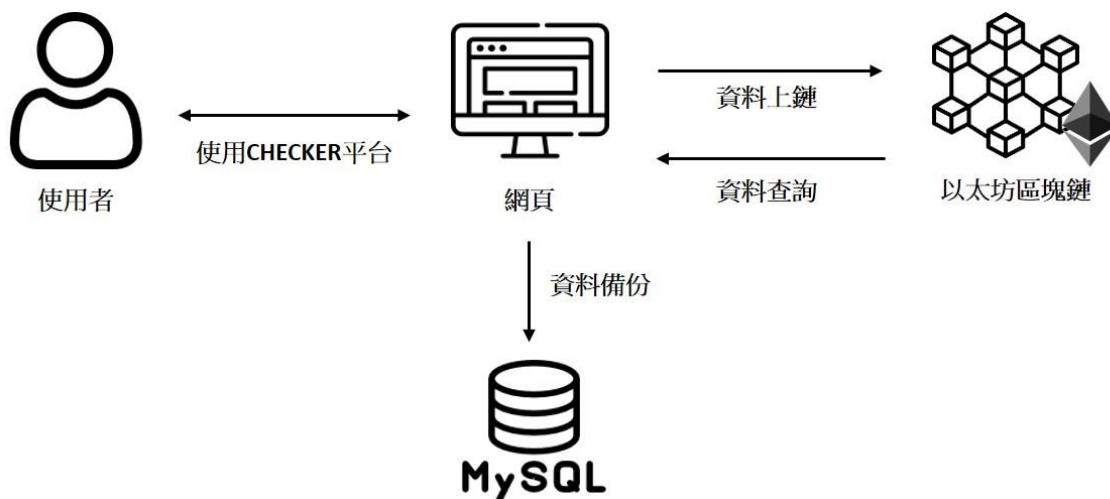


圖 8：系統流程介紹

首先，使用者分為合作廠商與消費者。如 (圖 8) 流程，合作廠商透過平台

(CHECKER) 登入，進行商品資訊上傳區塊鏈或從區塊鏈上查詢產品資訊；消費者僅能使用查詢產品資訊功能。

3.1.1、廠商商品資料上傳

廠商可在平台首頁點選”合作表單”，連結到表單填寫相關聯絡資料，平台會有專人跟廠商聯繫，確定合作之後將替廠商在資料庫建立平台帳號，讓廠商有平台帳號能進入自己的資料上傳頁面。而為了達到保存商品資料的完整性以及避免資料被輕易竄改，將資料儲存於區塊鏈，而因產品圖片與擁有者資訊儲存於資料庫，也順帶將已上傳至區塊鏈的資料儲存於一般的資料庫，讓商品資訊多一個管道儲存。在資料庫中，每個上傳後的商品資訊會給予專屬 PIN 碼提供修改產品擁有者。

3.1.2、消費者驗證商品資訊

消費者可透過網址進入驗證平台首頁，輸入商品序號，進行商品資料驗證；或是掃描商品上的 QR Code，系統直接帶入該商品的序號，即可進行商品資料驗證。最後，因查詢商品頁面有個商品擁有者欄位，若消費者已購買該產品，會在結帳時給予該商品專屬 PIN 碼，可透過 PIN 碼驗證，並更改該欄位擁有者名稱。

3.1.3、QR Code 產生器

由於考量 QR Code 要貼或印在產品上，因此獨立一個專門產生 QR Code 的應用程式，該應用程式僅限於合作廠商可使用。透過與平台相同的帳號登入後，介面會顯示該廠商已上傳至區塊鏈，也儲存於資料庫的產品資訊。

3.2、系統架構



圖 9：本系統架構圖

本系統前端介面使用 HTML、JavaScript、CSS 開發，後端處理使用 PHP、MySQL 開發，區塊鏈智慧合約撰寫使用 Solidity (以太坊的區塊鏈程式語言)，合約發佈使用 Remix IDE (智慧合約開發、測試與佈署等工具)，上傳與查詢資料使用 Web3.js (智慧合約與區塊鏈節點溝通的程式語言) 來與 Ethereum (以太坊區塊鏈) 進行溝通，目前處於測試階段，使用的是 Ganache (Ethereum 以太坊的測試用區塊鏈)，依上述形成 (圖 9) 之架構圖。

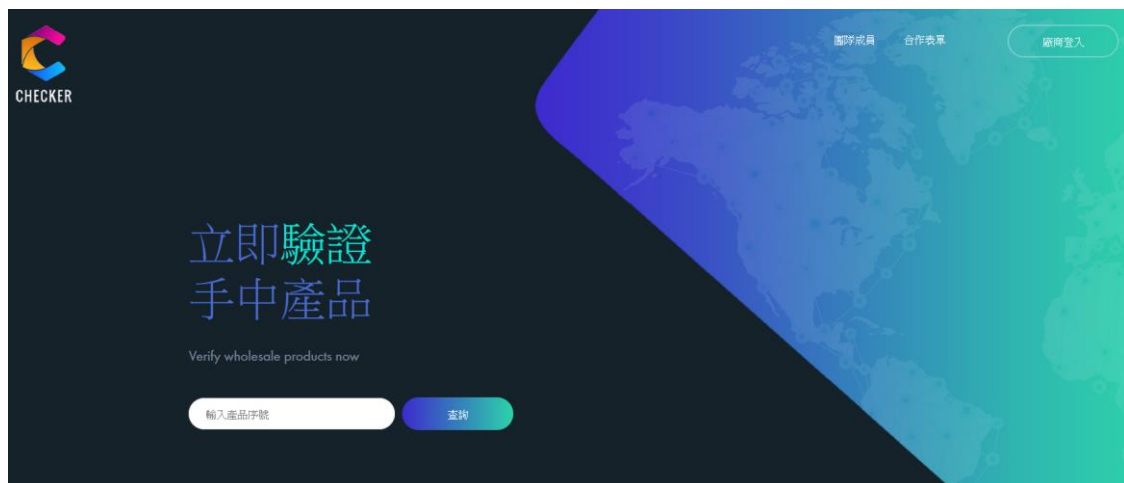


圖 10：本系統首頁

3.3、研究結果

(圖 10) 是本系統首頁，可在輸入框輸入欲查詢的產品序號。若是廠商進入首頁，可選擇右上角的合作表單，並填寫資訊與我們平台合作；而已經合作廠商，則可透過廠商登入進行產品資料上鏈。



The image shows a web form titled "CHECKER 廠商合作" (CHECKER Factory Cooperation). At the top, there is a header with the CHECKER logo and a colorful abstract background. Below the header, the form is divided into several sections. The first section displays the email address "4a7g0061@stust.edu.tw" with a link to "切換帳戶" (Switch Account) and a red asterisk indicating a required field. The subsequent sections are input fields for "電子郵件 *" (Email), "廠商名稱 *" (Factory Name), "廠商型態" (Factory Type), and "聯絡電話 *" (Contact Phone), each with a placeholder text "您的回答" (Your Answer).

CHECKER 廠商合作

4a7g0061@stust.edu.tw [切換帳戶](#)

*必填

電子郵件 *

你的電子郵件

廠商名稱 *

您的回答

廠商型態

您的回答

聯絡電話 *

您的回答

圖 11：廠商合作表單

廠商可透過填寫 (圖 11) 合作表單，平台會替合作廠商開通平台帳號，供廠商後續能登入平台進行產品資訊上鏈。

圖 12：廠商資料上鏈 – 單筆

廠商登入平台後，可選擇單筆/多筆資料上鏈，(圖 12) 為選擇使用單筆資料上鏈的介面，僅能輸入單一產品資訊及圖片上傳。

請確認資料筆數及內容是否正確，筆數：8

限.csv檔 瀏覽... test.csv

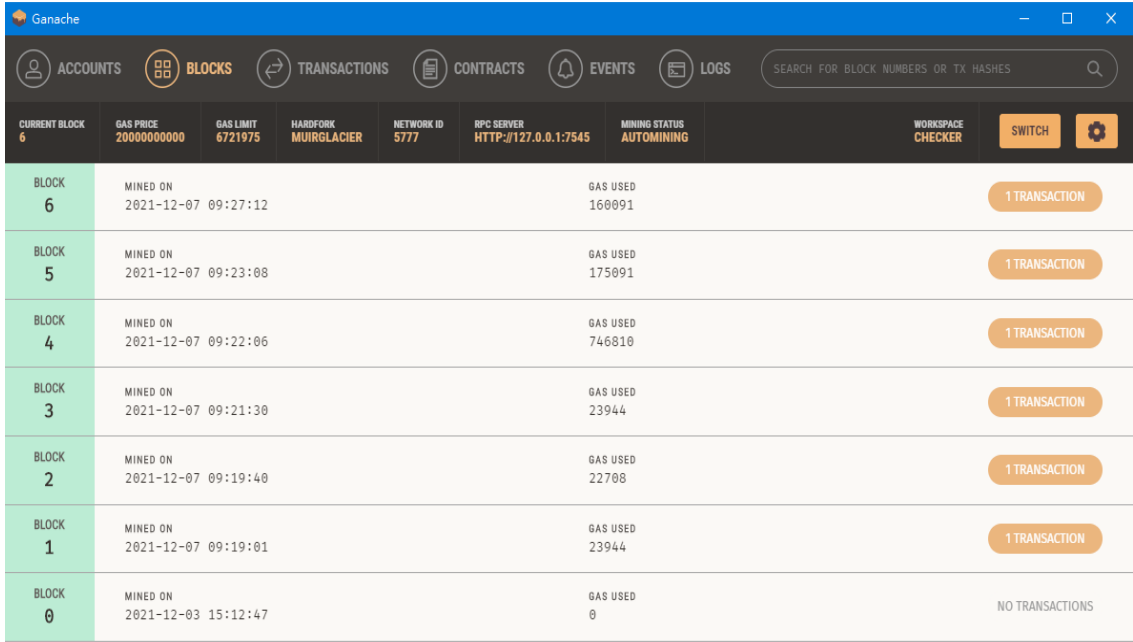
限.jpg檔 瀏覽... smile.jpg

產品編號	產品序號	品名	產地	製造商	製造日期
3	test-a03	test3	tw	test	2021/9/2
4	test-a04	test4	tw	test	2021/9/3
5	test-a05	test5	tw	test	2021/9/4
6	test-a06	test6	tw	test	2021/9/5
7	test-a07	test7	tw	test	2021/9/6
8	test-a08	test8	tw	test	2021/9/7
9	test-a09	test9	tw	test	2021/9/8
10	test-a10	test10	tw	test	2021/9/9

確認上鏈 關閉

圖 13：多筆資料上鏈

若選擇多筆資料上鏈，則會跳出 (圖 13) 處理視窗，廠商可使用 csv 檔將多筆產品資訊上傳，平台也會在上傳前預覽產品資訊，讓廠商能確定要上傳的資料是否有正確。



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE CHECKER	SWITCH	SETTINGS
6	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING			

BLOCK	MINED ON	GAS USED	TRANSACTIONS
6	2021-12-07 09:27:12	160091	1 TRANSACTION
5	2021-12-07 09:23:08	175091	1 TRANSACTION
4	2021-12-07 09:22:06	746810	1 TRANSACTION
3	2021-12-07 09:21:30	23944	1 TRANSACTION
2	2021-12-07 09:19:40	22708	1 TRANSACTION
1	2021-12-07 09:19:01	23944	1 TRANSACTION
0	2021-12-03 15:12:47	0	NO TRANSACTIONS

圖 14：Ganache 區塊鏈狀態

產品序號：test-a02

綁定擁有者 修改PIN碼

產品編號	2
產品序號	test-a02
品名	test02
產地	TW
製造商	test02
製造日期	2021-12-04
擁有者	'無'



圖 15：消費者查詢

每上傳一筆資料，會在鏈上形成一個區塊，本系統以 (圖 14) Ganache 本地端測試鏈，來模擬區塊生成。

消費者查詢介面，若序號輸入正確，則會進入 (圖 15) 查詢頁面，提供消費者查看產品資訊，以及附帶一張該產品的圖片。

圖 16：pincode 商品歸屬

購買產品得到 pincode 後，可以透過 (圖 16)「綁定擁有者」選項，將產品歸屬於購買的消費者。

廠商編號	產品編號	產品序號	品名	產地	製造商	製造日期	產品圖片	擁有者	pin	上傳時間
1	1	test-a01	泰山純水	台灣	泰山企業股份有限...	2021-12-24	b'\xff\xd8\xff\xe...	chenghao	testtest	2021-12-21 ...
1	2	test-a02	maker	tw	test02	2021-12-02	b'\xff\xd8\xff\xe...	'無'	82963054	2021-12-23 ...
1	3	test-a03	test3	tw	test	2021/9/2	b'\xff\xd8\xff\xe...	'無'	96078119	2021-12-23 ...
1	4	test-a04	test4	tw	test	2021/9/3	b'\xff\xd8\xff\xe...	'無'	59972195	2021-12-23 ...
1	5	test-a05	test5	tw	test	2021/9/4	b'\xff\xd8\xff\xe...	'無'	11526621	2021-12-23 ...
1	6	test-a06	test6	tw	test	2021/9/5	b'\xff\xd8\xff\xe...	'無'	77416520	2021-12-23 ...
1	7	test-a07	test7	tw	test	2021/9/6	b'\xff\xd8\xff\xe...	'無'	52702741	2021-12-23 ...
1	8	test-a08	test8	tw	test	2021/9/7	b'\xff\xd8\xff\xe...	'無'	31164150	2021-12-23 ...
1	9	test-a09	test9	tw	test	2021/9/8	b'\xff\xd8\xff\xe...	'無'	97512529	2021-12-23 ...
1	10	test-a10	test10	tw	test	2021/9/9	b'\xff\xd8\xff\xe...	'無'	94270199	2021-12-23 ...

圖 17：QR Code 產生介面



圖 18：QR Code 產生結果

(圖 17) 廠商操作時：

1. 選擇要產生 QR Code 的項目
2. 選擇 QR Code 存放路徑

系統透過包取自動帶入平台驗證的序號，產生出如 (圖 18) 的結果，QR Code 中也會顯示所對應的產品序號，防止 QR Code 被其他產品盜貼或廠商自行貼錯的情形發生。

肆、結論

本系統實現利用區塊鏈技術對商品資料進行完整的保護，讓消費者能夠對自己購買的商品進行查詢驗證，確保購買到的是真貨而非贗品，以達到讓消費者能夠安心購買的目的。並且購買當下能以本系統產生的 QR Code 作為真品辨識的首要依據，萬一有仿冒品出現時，以本系統區塊鏈上的資訊作為次要且更加無誤的辨識依據。

4.1、未來展望

在利用 PIN 碼驗證並進行商品歸屬以及產品圖片的部分，依然使用中心化資料庫的方式來儲存，容易被竄改之風險；還有以太坊的交易速度和高昂手續費也是需要解決的難題。

4.1.1、圖片儲存

由於圖片所佔用的檔案大小較純文字大，因此先將圖片使用 IPFS (星際檔案系統) 進行分散式儲存，並將上傳圖片後所得到的 hash 存至區塊鏈，(圖 19) 的左邊是 HTTP 右邊是 IPFS，用 IPFS 方法相較比放在單一資料庫 (HTTP) 中，更具有安全性可靠性且

不易被竄改。[5]

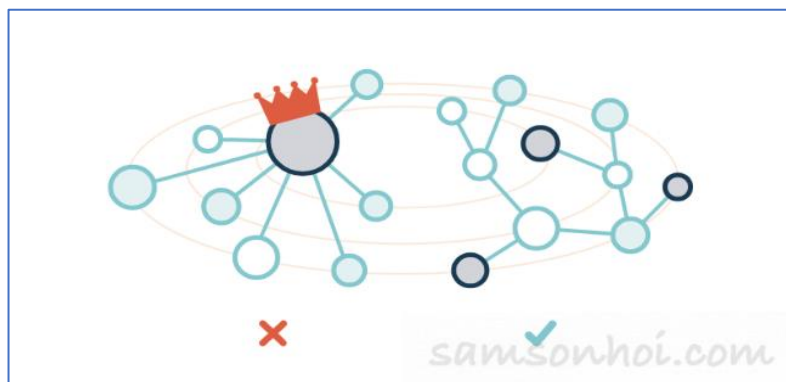


圖 19：HTTP 與 IPFS 比較圖

4.1.2、以太坊交易速度

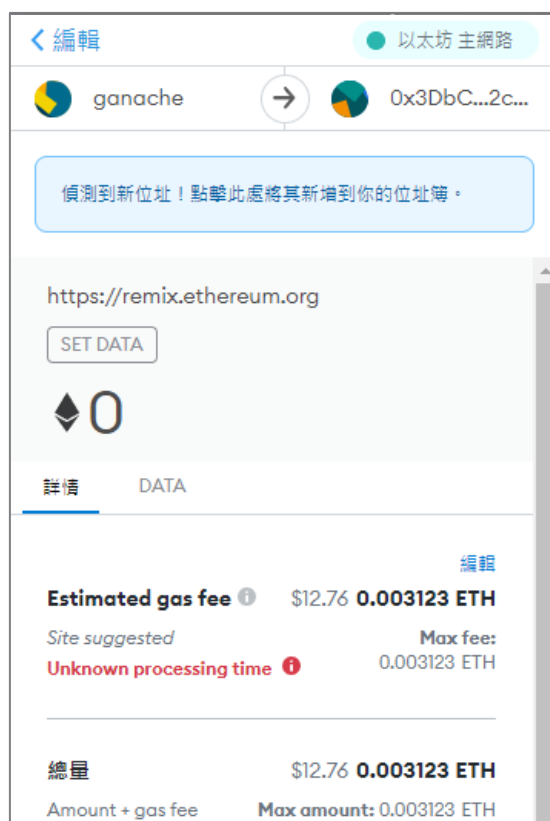


圖 20：以太坊單筆資料上鏈消耗參考圖

產品上鏈時的手續費有可能發生 (圖 20) 中，比產品販售單價高的情形，甚至礦工驗證時間較長也會消磨耐心，未來可改用其他區塊鏈運行本平台，如：MATIC、FLOW

等，藉此解決高昂手續費和交易速度問題。

	同質化代幣 (Fungible Token)	非同質化代幣 (NFT, Non-Fungible Token)
代表	法幣, 石油, 比特幣 (BTC)、以太幣 (ETH)	NFT (機票, 房屋產權, 加密貓)
特性	可替代性, 可分割性, 一致性	不可替代性, 不可分割性, 唯一性

首先, 我們經常聽到的比特幣 (BTC)、以太幣 (ETH), 屬於同質化代幣, NFT屬於非同質化代幣, 來看看到底這兩個名詞有什麼特性呢?

圖 21：ERC-20 與 ERC-721 比較

4.1.3、商品歸屬

以 ERC-721 標準, 如 (圖 21) 的特性, 將不同的產品資訊儲存在各個具有 ID 證明的代幣, 當消費者購買產品時, 能夠記錄購買者做以商品持有者歸屬, 也能同時得到標記該產品資訊的代幣, 這樣不僅讓產品資訊紀錄在區塊鏈上, 也可做為產品歸屬之依據。

參考文獻

- [1] <https://vocus.cc/article/5ee927f9fd89780001092042> (2020/06/26)
- [2] <https://medium.com/@daniel.mars622/%E4%BB%A5%E5%A4%AA%E5%9D%8A%E5%8D%80%E5%A1%8A%E9%8F%88%E6%99%BA%E8%83%BD%E5%90%88%E7%B4%84%E5%9F%BA%E7%A4%8E%E4%BB%8B%E7%B4%B9-b7317347a612> (2018/6/1)
- [3] https://www.slideshare.net/Kenneth_hu/20180711-metamask (2018/07/11)
- [4] <https://ithelp.ithome.com.tw/articles/10203545> (2018/10/20)
- [5] <https://ithelp.ithome.com.tw/articles/10293967> (2022/09/22)
- [6] R. Aroul Canessane, N. Srinivasan, Abinash Beuria, Ashwini Singh and B. Muthu Kumar, Decentralised Applications Using Ethereum Blockchain, 10.1109/ICONSTEM.2019.8918887 (2019/03/15)
- [7] W. Wu, Weighted Evaluation Technologies For Blockchain Suitability, <https://hdl.handle.net/11296/mda79m> (2020/07/14)
- [8] G. Pierro and H. Rocha, The Influence Factors on Ethereum Transaction Fees, 10.1109/WETSEB.2019.00010 (2019/05/27)
- [9] J. Sun, M. Li and J. Ma, Research and application of data sharing platform integrating Ethereum and IPFs Technology, 10.1109/DCABES50732.2020.00079 (2020/10/19)