IPFS與智能合約在租屋上的應用 **Application of IPFS and Smart Contracts in House Rental**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **蔡芷晴** | **陳湧惠** | **楊雅雯** | **陳柏蓁** | **蘇民揚\*** |
| **Choi, Tsz-Ching** | **Chen, Young-Hui** | **Yang, Ya-Wen** | **Chen, Po-Chen** | **Su, Ming-Yang\*** |

銘傳大學資訊工程學系

Department of Computer Science and Information Engineering,

Ming Chuan University

08361021@me.mcu.edu.tw, 08360396@me.mcu.edu.tw, 08450936@me.mcu.edu.tw, 08361046@me.mcu.edu.tw,\*minysu@mail.mcu.edu.tw

**摘要**

以太坊整合了以太幣、支付和去中心化應用程式等技術，無論何時何地只要連上網路，就能夠便捷的使用這些功能，其中智能合約運行於區塊鏈上，人們透過去中心化應用程式和鏈上的合約做互動，合約便會自動執行其內容，但因智能合約的公開透明性會使房東及房客的個人資料透露，所以選用IPFS(星際檔案系統)，一個類似於區塊鏈協定的網路基礎設施，存放租屋契約，使用回傳的雜湊值進行加密得出密文並放入智能合約中，以保障房東及房客的隱私權。在本研究，我們藉由創建智能合約結合IPFS打造去中心化應用程式來探討其在租屋上的應用。

**關鍵字**：區塊鏈、智能合約、IPFS、租屋

**Abstract**

Ethereum has integrated technology which included Ether, payment, decentralized application etc. If connecting with internet, people can use the functions of these technology. Smart contract is one of the technology running in block chain, people can use decentralized application to interactive with smart contract and it implement its content automatically. However, the open characteristic of block chain and smart contract would show the personal information publicly, we take IPFS, a　 communications protocol similar to block chain, deposit the residential lease agreement, encrypt the hash return after upload and store in smart contract, to protect the privacy of landlords and tenants. In this research, we combined IPFS and smart contract to explore the technology application in rental housing by creating a decentralized application.

**Keywords**: Block Chain, Smart Contract, IPFS, House Rental

1. **簡介**

人們日常生活最重要的食衣住行，其中住的問題在租屋上往往產生許多租賃糾紛，例如水電瓦斯計價問題、房東剋扣押金任意漲租，或是房客未按時繳納租金、紙本契約容易變更等，以上的紛擾大多為彼此不遵守當初簽訂的租屋契約條款所導致的信任問題，隨著區塊鏈相關議題的盛行，它的特性恰巧適合用來解決此類問題。本研究將研發一個Dapp(去中心化應用程式)，讓房東能透過Dapp將租屋契約上傳至IPFS，再把IPFS回傳的檔案雜湊值進行加密放進智能合約，僅有房東及房客知曉密碼能夠解密，查看契約。由於IPFS根據內容尋址的特性，可以保證租屋契約的唯一性與無法竄改性，來保障雙方的權益，再藉由運行於區塊鏈上的智能合約來處理房客支付押金、房租，房東退還押金等交易流程，房客所支付的房租與押金會存放在智能合約中，而後房東再做提領，因此房東無法剋扣押金，這些交易紀錄會儲存於區塊鏈上，公開透明皆可追溯，我們將透過IPFS與智能合約來打造一個Dapp來解決租屋上的問題。

1. **相關文獻:**

**區塊鏈[1]:**

區塊鏈是一種類似資料庫的機制，它能夠將鏈上的資訊透明公開的給所有使用者查看。區塊鏈就是一種去中心化的技術，再沒有區塊鏈的世界就是有一個中央機構保存所有使用者的紀錄，每一個交易都須經由此中央機構來完成。而在區塊鏈的世界裡，區塊鏈將每筆資料透過雜湊演算法計算後變為一串雜湊值，經過許多礦工驗證後形成一個個的區塊，這些區塊裡會存放交易資料，每個區塊會指向前一個區塊有序的串接鏈結於一起。區塊由區塊頭和區塊主體所構成，區塊頭用來記錄區塊的主要資訊，區塊主體則用來紀錄區塊內的交易，每個區塊頭會包含前一個區塊的 Hash 值，以此來生成當前區塊的 Hash 值，因此可以根據當前的區塊不斷往前溯源至原先的創始區塊，具有可追溯性。

區塊鏈採用分散式帳本技術[2]，透過分散式帳本就不再需要有中央機構來完成每一筆交易，而是讓所有使用者的電腦一起參與記帳，有交易發生時會同時發布給所有連接網路的電腦裡，同步更新每筆交易紀錄，且每個區塊的 Hash 值皆不相同，但凡有一個 byte 的改變，所產生的 Hash 值便會不同，這樣便可保障區塊無法被竄改，只要一經更動，便立即會被發現，如果有人想要擅改資料就需要同時修改超過半數電腦裡的紀錄，是一件十分困難的事情。

區塊鏈不會產生單點故障的問題，因鏈上有許多節點，即使其中一個節點失效，其他的節點仍能正常運作，具有分佈性。

**區塊鏈於畢業證書數位化的應用:**

近年來國內外有許多學校開始使用區塊鏈發放畢業證書[3]，像是美國的部分大學和公司已經不接受紙本畢業證書，只收數位畢業證書的情形出現。將證書放入區塊鏈內，可以減少偽造畢業證書的情形出現。且在像是求職或是升學等情況下也可以直接將畢業證書的Hash值傳送給學校或公司，不用寄送紙本而是直接透過Hash值檢驗證書真偽，可以加快審查的速度。

一張含有 文字, 螢幕擷取畫面 的圖片

自動產生的描述

圖 1-1 數位畢業證書示意圖

**智能合約[4]:**

智能合約(Smart contract)是由電腦科學與密碼學專家的學者Nick Szabo在1994年提出的，目的在於想讓傳統合約的交易成本降低和提升安全問題，然而當時代的技術尚未至臻成熟，因此沒有任何的平台能夠支持此概念，直到2015年以太坊(Ethereum)的出現，才真正有完備的平台來應用此發想。智能合約擁有和區塊鏈一樣地去中心化數據無法竄改[5]，資料公開透明，且只要一啟動合約，它就能照設計好的模式運行不需要有人去控制干涉，稱為去中心化應用程式(Decentralized App, Dapp)。

相較於傳統合約需要透過繁瑣的流程和各種花費來確保合約正常運行下，智能合約就簡潔許多。智能合約由創建者定義要實現的合約內容或商業邏輯並撰寫為程式碼，再發布至區塊鏈網路上，每一個合約都會被分配到一個專屬的合約地址，合約被部署後，想要調用此合約的使用者，只需花費交易手續費(Gas Fee)並指定此合約的地址，便能夠執行合約內的函式(Function)了，雙方只需要線上就能簽署合約，將合約送出後它就會儲存在公共的資料庫裡，不需要找公證人或是做其他防止對方反悔的條件，只要透過智能合約完成簽署動作就算有一方想反悔合約也會強制執行，沒有更改的餘地。

**區塊鏈於保險智能理賠的應用:**

在傳統的醫療保險運作方式中，要申請理賠必須要提供收據給保險公司後才會被受理，且需要有人來審核、執行程序，故無法及時給予理賠金，且保戶還需要先自行籌備所有的醫療費用。透過區塊鏈撰寫智能合約則可以將保險合約內容等資料上鏈[6]，透過分散式帳本將醫院、保戶、保險公司做連接，這樣在醫院內花費奪少保險公司也能夠提前知悉且做審核評估，在保戶出院時就不需要先付帳後向保險公司請款，而是可以由保險公司直接幫忙付清。或像是出國時飛機延遲起飛的狀況下，有投保旅遊不便險的保戶可以申請理賠，但可能會有部分的人會覺得申請理賠太花時間或步驟繁瑣而不申請理賠，但透過智能理賠系統則可以在符合旅遊不便險條件時理賠金就自動匯入帳戶內了。

**區塊鏈於線上募資平台[7]的應用:**

經2011年網路調查[8]有許多的捐款人都希望公開資金流向，有近半數的人因為擔心捐款沒有被用在正確的地方而不敢行動。但透過區塊鏈提供的完全透明公開的資料，讓有愛心的人可以放心地將金錢投入。各項專案計畫、用途、受眾、截止日、目標金額等等的資訊都會被詳細的紀錄起來，且如果超過預先設定的時間還沒有集到目標金額，則會透過寫入智能合約內的程式將捐款全數退回。

**IPFS :**

星際檔案系統簡稱IPFS(InterPlanetary File System)是一個分散式儲存系統，它屬於一種協議類似於HTTP，最初由 Juan Benet 設計，直到 2014 年在Protocol Labs 這個開源社群的幫助下蓬勃發展至今，其宗旨為建構一個開放共享、安全、高效率、持久化的網際網路協定讓全世界的人皆能對等的儲存和提取檔案。現今網站大多數是儲存在一個大型資料庫中，而這些資料庫則是由單一公司在控制管理，HTTP協議每次下載圖片、網站、視頻等，皆須從各個服務器下載文件是較為沒效率的方式，但IPFS可以一次從多個不同的節點找尋資料，相較HTTP協議來的更快速許多。

HTTP頁面平均壽命約100天[9]，就像是有時候有些儲存下來的網站有一天卻再也找不到了，IPFS提供文件回溯[10]，使數據可以一直保存在節點上。IPFS設計上也避免了一樣的文件重複上傳， IPFS 會根據檔案內容來產生一個專屬於此檔案的 Hash 值，與 HTTP 網路協定依據域名產生網址的方式有所不同，只要檔案內容有一個 byte 的改變，Hash 值便會完全不同，因此在IPFS 上，不會存在重複的檔案，由此來確保檔案的唯一性、真實性和不可竄改性，大大的節省了儲存空間。

在安全方面上更是優於HTTP，中心化服務難以抵擋DDoS攻擊，如有大量的訪問請求，服務器很容易就會癱瘓，但IPFS幾乎是不會發生這種情況，因為訪問IPFS的請求都會被分散到各個不同的節點，就不會產生服務器癱瘓等問題。

1. **研究方法:**

**智能合約：**

本研究使用了solidity語言撰寫智能合約及以太坊提供的線上版官方整合開發環境 Remix[11]作為智能合約的開發及測試環境，Remix提供對智能合約的撰寫﹑編譯及部置至虛構的本地區塊鏈上，模擬智能合約在區塊鏈上的運行狀態及觸發智能合約內函式時給予的回應，方便進行對智能合約調整及修改，如圖3-1，紅色框內的是該智能合約可觸發的函式，綠色框內是撰寫智能合約的地方，藍色框內是觸發函式後智能合約後區塊鏈給予的回應及該次互動的hash值。

本研究利用智能合約的特性，在租屋的應用上確保租屋契約不被篡改，透過與智能合約的互動收取租押金，履行租屋契約。在租屋出租﹑租客向智能合約支付押金後，房東不能再次更改租屋資料（押金﹑租金﹑租屋契約的hash值），直至租客退租﹑房東從智能合約中退還押金給租客為止。

一張含有 文字, 螢幕擷取畫面, 監視器, 黑色 的圖片

自動產生的描述

圖3-1 Remix的介面

**React:**

React是一個用來建構使用者介面的函式庫[12]，主要使用的程式語言為稱為JSX（JavaScript和XML）的HTML-in-JavaScript語法，能與其他的函式庫及套件配合使用[13]，建立一個符合使用者需求的前端介面。

本研究使用React開發網頁前端，加載了與智能合約﹑區塊鏈和加密貨幣錢包必需函式庫之一的ether.js函式庫[14]。如圖3-2，透過ether.js的函式，連上加密貨幣錢包與區塊鏈，使用撰寫好的智能合約的BYTECODE及API，部置智能合約到區塊鏈上(圖3-3)。

一張含有 文字 的圖片

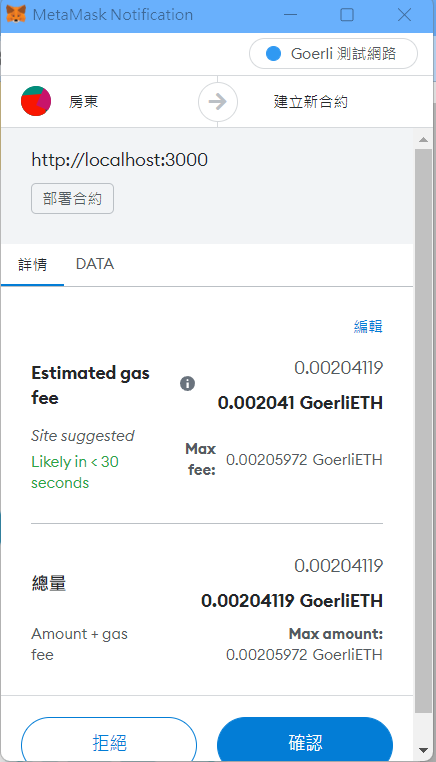
自動產生的描述

圖3-2 部置智能合約到區塊鏈上的程式碼 圖3-3 連接錢包部置合約到區塊鏈

React在前端網頁介面的開發上，使用XML作編寫語言，在js檔案建構一個網頁介面，如圖3-4，可以透過瀏覽器開啟的網頁介面。



圖3-4 前端網頁介面

1. **研究結果:**

**系統功能測試:**

圖4-1為房東新增租屋的運行結果，設定租屋名稱後連接MetaMask並部署一個專屬的智能合約，將會得到智能合約地址及交易Hash，到此新增租屋的流程便完成。



圖4-1 新增租屋之操作範例

從圖4-2中能看到房東上傳租屋契約到IPFS的操作結果，首先設定一組只有房東和房客才知曉的密碼，而後上傳已簽訂完畢的租屋契約，便會得到一串加密過的網址雜湊值，只有擁有這組密碼的使用者才能透過解密取得檔案存放的網址，如此便可保證租屋契約的隱密性，房東和房客也能方便地閱覽租屋契約。



圖4-2 上傳租屋契約之操作範例

如圖4-3所示，房東設定完房租及押金並填入契約網址密文後會得到交易Hash。若需確認、查閱租屋資料，可以跳轉至「查詢」頁面，如圖4-4，選取目標租屋，按下查詢後便能看到當初房東設定的房租、押金及契約網址密文，還有此租屋對應的智能合約餘額。

一張含有 文字 的圖片

自動產生的描述 一張含有 文字 的圖片

自動產生的描述

圖4-3 設定租屋資料之範例 圖4-4 查詢租屋資料之圖示

目的為租屋的使用者可以至「租屋」頁面，選擇要承租的房屋，按下決定租屋後，將來會由當時操作的使用者之錢包地址支付租金、押金。以圖4-6支付押金為例，輸入要支付的金額，連接MetaMask以完成支付程序。

一張含有 文字 的圖片

自動產生的描述 一張含有 文字 的圖片

自動產生的描述

圖4-5 租屋之範例 圖4-6 支付押金之圖示

圖4-7、圖4-8為房東至「管理」頁面選擇欲收取租、押金之房屋後連接MetaMask，利用智能合約中撰寫的收房租及退還押金的function，把存放在智能合約中的錢傳送給房東，並將房客先前支付的押金退還給其。

一張含有 文字 的圖片

自動產生的描述

圖4-7 房東收取租金之操作範例 圖4-8 退還押金之操作範例

利用圖4-2中設定的密碼及其對應之契約網址密文，可解密得到租屋契約在IPFS中存放的地址，前往下框中的契約網址便可閱覽當時上傳的租屋契約檔案。

一張含有 文字 的圖片

自動產生的描述

圖4-9 租屋契約存放之網址解密操作

**內容檢測:**

方利用Block Explorer這個網站，我們幾乎可以訪問與交易、錢包和區塊鏈相關的任何數據，包括交易金額、資金來源、目的地以及交易狀態，因此透過調閱交易紀錄，可以檢驗4.1的操作結果是否完善、確實。

圖4-10中可以看到圖4-1裡的智能合約有順利地部屬，圖4-11為設定租屋資料的紀錄，圖4-12房客成功地支付押金，金額為房東當初設定的1 wei，圖4-13智能合約中存放的房租傳送給房東，圖4-14智能合約中存放的押金退還給房客。

一張含有 文字 的圖片

自動產生的描述

圖4-10 部署合約之Transaction Details

一張含有 文字 的圖片

自動產生的描述

圖4-11 Set Data之Transaction Details

一張含有 文字 的圖片

自動產生的描述

圖4-12 房客支付押金之Transaction Details

一張含有 文字 的圖片

自動產生的描述

圖4-13 房東收取房租之Transaction Details

一張含有 文字 的圖片

自動產生的描述

圖4-14 退還押金之Transaction Details

1. 結論

本研究中主要探討的利用IPFS與智能合約等區塊鏈相關技術來進行租屋上的應用，雖然區塊鏈算是新興的技術，沒有悠久的歷史沿革，但是利用它的特性應用在租屋方面上使所有租賃功能與交易流程自動化，解決了信任問題，交易記錄公開透明，所有資料皆被永久的儲存於區塊鏈上，任何人皆無法對其進行竄改、刪除，透過了這個去中心化應用程式，整合了區塊鏈技術，維護了房東和房客彼此間的權益，有效的解決許多過去會發生的租賃糾紛，並把租屋契約電子化的保存於IPFS上，也符合環保永續發展的方向，也不會發生遺失紙本契約或任意竄改租屋契約內容的可能，且隨時隨地只要有網路，便能使用這個去中心化應用程式，相當便利。

區塊鏈當然也有一些缺點，便是每組房東房客建立專屬智能合約與支付房租、押金與提領房租和退還押金等交易流程，此過程每次皆會對使用者扣除一些手續費，用來當作礦工獎勵或維護區塊鏈網路，這樣會造成交易多次花費過多手續費的交易成本高昂的問題，對使用者而言不太友善。以太坊之前進行改版從最初的PoW挖礦機制，轉型成PoS權責驗證機制，導致之前我們使用的測試鏈被全面廢除，所以轉向了新的測試鏈進行部署，有了一些小波折。

本研究讓我們學習到了IPFS和智能合約等區塊鏈技術的功能與背後運作原理，在開發智能合約的過程中，學習了Solidity的程式語言，並運用React和Bulma等前端框架搭建使用者介面，和Firebase資料庫和網站的連接，與一些API的串接等，還學習了許多加密演算法，在未來我們可以利用所學實作出Web3的Dapp應用。

**參考文獻**

1. Blockchain Facts：What Is It, How It Works, and How It can Be Used

https://www.investopedia.com/terms/b/blockchain.asp

1. 關於區塊鏈你至少要知道什麼?

https://rich01.com/what-is-blockchain/

1. 把畢業證書存進區塊鏈！清大創全台首例推加密證書，校友也能申請

https://www.bnext.com.tw/article/63554/nft-diplom

1. What Is Ethereum and How Does It Work?

https://www.investopedia.com/terms/e/ethereum.asp

1. What Are Smart Contracts?

https://www.cryptoninjas.net/what-are-smart-contracts/

1. 保險科技-區塊鏈應用於保險業

https://www.youtube.com/watch?v=eqa5LNj-Pro

1. 度度客線上募資平台

https://dodoker.com/

1. 台灣第一個區塊鏈群眾募資平台「度度客」：改善捐款透明度問題，位公益募款領域寫下新篇章

https://www.seinsights.asia/article/3290/3270/5957

1. https://ipfs.tech/
2. 【IPFS 技術佈道人】入門淺談：什麼是 IPFS？

https://blockcast.it/2019/10/16/let-me-tell-you-what-is-ipfs/

1. https://remix.ethereum.org/
2. https://zh-hant.reactjs.org
3. React新手入門

https://developer.mozilla.org/zh-TW/docs/Learn/Tools\_and\_testing/Client-side\_JavaScript\_frameworks/React\_getting\_started

1. Web3 Tutorial: build DApp with Hardhat, React and Ethers.js

https://dev.to/yakult/a-tutorial-build-dapp-with-hardhat-react-and-ethersjs-1gmi