中華民國第 59 屆中小學科學展覽會

作品說明書

高級中等學校組　工程學(一)科

第二名

052303

具有區塊鏈之 IOT 用電系統

學校名稱：新北市立淡水高級商工職業學校

作者：	指導老師：
職三 吳晨知 職二 張育丞	陳金雄

關鍵詞：區塊鏈、物聯網(IOT)、電能傳送與交易

壹、摘要

現代生活中電能扮演非常重要角色，由於使用者型態多而複雜，甚至因電能過度開發造成能源與環保問題，於是電能品質與資訊至為重要，結合新穎的科技技術改善目前電能管理，達成智慧化用電能系統成為現代電能管理顯學。

本研究概念來自物聯網(IoT)與區塊鏈技術，將二者結合並應用於電能管理系統上，使用戶端使用者與供電管理者皆有用電資訊平等權，進而達到更佳的用電資訊安全與節能效果。研究內容除了製作電力模組為物聯網電能系統之感知層，與無線傳輸模組及嵌入式樹莓派處理器前端伺服器組合而成網路層之外，更著重於應用層之後端區塊鏈伺服模組。目前研究已有電能資料、帳單與交易之工作量證明成果，所以具有公開不易篡改與交易節能功能。

貳、研究動機

電能是現代文明生活中重要的科技，但因過度開發與繁雜使用所造成能源枯竭與環保污染問題[1-3]，使得人類需面對這棘手問題，而有效的規劃電能與使用資訊透明化進而降低電能使用成為解決上述問題的重要方法[4-6]。

於是我們針對電能資訊透明化與電能資料傳送與交易進行了討論，討論過程中認知到迅速發展的網路通訊不僅局限於個人電腦之間聯繫，更擴展到雲端與物品之間的連結，而「物聯網」(IoT, Internet of Things)更是網路通訊進一步應用，於是思考到物聯網對現今人類生活的應用與改變[7-9]。進一步討論中，我們考慮將物聯網應用於電能規劃，智慧電錶便是物聯網應用於家庭用電的例子[10-12]，於是我們想設計屬於自己的「物聯網智慧電錶」，如何設計電力設備與電器進行監控與資料搜集，。

我們也想到物聯網電錶所收集電能資料是否可以正確保存？又或者是否可以降低被竄改機率?針對此問題加以討論後，想到現今熱門的區塊鏈技術[13-15]，利用公開金鑰與數位簽章演算法確認傳送者身份，加上雜湊值將前後資料連接起來驗證數據的連貫性與正確性，並利用分散式節點來達到去中心化之資料安全。於是我們針對區塊鏈應用於電能的案例進行搜集，發現各國都有公司開發擁有區塊鏈的電網，並利用區塊鏈達到節約能源與交易電能的案例[16-18]。

根據以上了思考與初步認知，讓我們再一次接受挑戰，決定努力研究物聯網與區塊鏈原理與架構，除了將課堂上的電子學、數位邏輯與專題製作學以致用外，並與指導老師討論研究方向與技術後，利用課餘時間研究物聯網架設與區塊鏈架構。

參、研究目的

經由上述研究動機描述，本論文研究目的是欲建立「具有區塊鏈之 IoT 電能系統」，而電能物聯網功能包含收集與儲存電能參數(電壓、電流、功率與消耗功率)，它是利用電力模組取樣資料後由無線模組傳送資料至物聯網網路層之前端伺服器樹莓派，達成資料擷取、計算與儲存為一體架構，這可使電能管理者建構長久電能大數據，並可提供用電使用者查詢電能資料。

應用層後端電能區塊鏈功能意指保護電能資料的公開性與安全性，所謂公開性是指某些時段電能參數資料加入區塊鏈後，我們可以公開查詢以利追蹤用電狀況，所以當發生電力管

理者提供電能不穩定，如異常電壓造成電器損失時，用戶端使用者可向電力管理者索賠;而安全性是指電能資訊經過傳送驗證後不易被篡改，這包含電能帳單的正確性。

將區塊鏈功能與物聯網(IOT)技術的結合可以應用於電能交易，使用戶達到節省電費與有效分配，也讓電力管理者能更有效管理電能，進而達到節能與環保功能。

綜合以上，我們想設計公開不易篡改性之電能使用資訊與電能交易，以利長期追蹤用電狀況並改善我們的電能管理效率，所以本研究的目的具有下列功能:

一、設計物聯網之電能負載遠端監控功能，來測量與建立電能參數數據。

二、發展具有公開性電能資料之區塊鏈，以達到資料真實性與公開性，若電能系統出現異常而傷害電器設備時，用電者不會被隱瞞並可向電能管理者請求賠償。

三、建立電能使用資訊之安全性區塊鏈，以達到定期取得定期電能帳單。

四、完成具有交易性之區塊鏈與計算交易電能累計功能，以達到節省電費與節能功能。

肆、研究設備與器材

為了製作此系統，我們需架設物聯網(IOT)之電能資料感知與網路傳輸，並需將電能資料計算與儲存於網路層之樹莓派處理器(Raspberry)前端伺服器，再由應用層後端區塊鏈伺服器做電能資料傳送與交易。由此可知，本研究需要硬體電力負載與電子電路、仞體的信號擷取及通訊協定設定與軟體的電能資料儲存和傳送/交易，因此所需的實驗設備與器材相當廣泛，其用途說明如下所示。

物聯網(IOT)之感知層需要實驗模組擷取電能參數並經由網路傳輸至網路層之前端伺服器，方能將收集電能參數存於資料庫(MySQ)，並做為後端應用層區塊鏈伺服器之挖礦依據，其研究設備及器材如表 1 所示，以下將介紹我們的實驗硬體及軟體。

表 1 研究設備與材料

編號	材料名稱	規格	數量	單位
1	樹莓派(RaspberryPi)	Raspberry Pi 3	2	組
2	電力模組(LT-114)	220V、10A	2	組
3	傳輸模組(YL-100T)	100mW、433MHz	2	組
4	筆記型電腦	4 核心、RAM8GB	3	臺
5	無線路由器	100MB	1	臺
6	插座	110V、15A	2	片
7	電機機械實驗設備	220V、10A	1	組
8	壓克力板	PP 塑膠	5	片
9	導線	0.75mm^2	1	捆
10	束帶	整線使用	1	包
11	無熔絲斷路器(NFB)	110V 10A 2P	1	組
12	PVC 管	16mm	1	支
13	電風扇	110V	1	臺
14	杜邦線	公轉母頭	20	條
15	Python+Flask	v3.6	3	套

(一)、硬體部分

硬體架設需簡易的電腦系統及電力控制系統表如 1 所示，在此我們將介紹「電力模組」(LT-114)、傳輸模組」(YL-100T)與「樹莓派模組」(Raspberry Pi)三項重要的模組所需設備與材料。

1.「電力模組」(LT-114)

「電力模組」(LT-114)能對線路中的電參數準確測量，提供電壓、電流、功率、功率因數、消耗功率等參數，它可以使用 RS485、TTL、433M 的方式進行通訊，方便遠距離收集數據，且內建繼電器，可以進行電源的遠端控制[19]

2.「傳輸模塊」(YL-100T)

低功率半雙工串列無線數據「傳輸模塊」(YL-100T)，其低傳送功率與工作頻率分別為 100mW 與 433MHz，並支援 TTL 信號，且具有體積小、低成本與穩定度高[20]。

。

3.「樹莓派」(Raspberry Pi)

由英國樹莓派基金會所開發，它的特點是低價硬體及自由軟體促進。我們將它架設成為前端伺服器，其功能包括電能參數收集、運算與儲存資料庫[21-22]。

(二)、軟體部分

1.作業系統(Linux)

Linux 為「樹莓派」(RaspberryPi)使用的作業系統，我們將樹莓派系統(RaspberryPi)設計成網路層之前端伺服器 Linux 系統，並配合 Python 與 MySQL 等軟體做為電能資料收集與儲存的基礎。

2.程式語言(Python)

Python 是一通用、直譯及物件導向的程式語言[23]，它具有簡潔與直覺式的語法、以及龐大的函示庫，所以適合本研究使用。在這我們使用 Python v3.6 除了達成前端伺服器收集與計算電能參數的功能之外，並能夠有效的控制電能負載。

3.資料庫(MySQL)

本研究將 MySQL[24]做電能資料大量記錄，提供用於電能管理者管理、檢查與最佳化操作的資料庫管理工具。將它 MySQL 與 Python 程式聯結，我們可將電能負載參數予以儲存並分析，且提供後端挖礦伺服器進行資料區塊化。

4. Python+Flask+Web 應用程式

本研究應用層之後端區塊鏈伺服器包含用戶端使用者與挖礦伺服器端之操作與電能傳送與交易，其所需軟體為 Python+Flask+Web 應用程式搭配 html、CSS 與 Javascript 等語言[25-26]。

伍、原理與研究規畫

一、原理

物聯網與區塊鏈是目前重要的生活應用與技術，若能將它們結合應用於電能資訊(帳單)與交易即是新的創新研究，這也是我們本次研究的重要想法。為了了解這兩者精神與應用，我們在此介紹其概念與原理。

(一)、物聯網(IoT)部分

物聯網(IoT)的英文全名為 Interent of Things，直譯意思就是「物」與「物」之間溝通透過網際網路聯結，也就是各獨立功能的普通物體能夠透過各種電信網路等資訊承載體實現互聯互通功能[7-8]，其基本概念如圖 1 所示。

圖 1 物聯網(IoT)能彼此將「物」與「物」溝通與資訊分享[7]

由圖 1 可知，各種生活與工業上系統可以互相聯絡，以致全有系統互相分享資料。另外，比爾蓋茲於 1995《未來之路》一書中提出物聯網(IoT)概念，但因當時各種硬體如感測器與無線網路尚未成熟，所以只限於概念提出。不過隨著硬體技術日以更新，物聯網(IoT)漸漸引起重視，並想藉著它應用於跨領域之「智慧生活」，物聯網(IoT)再次吸引人們的注意[9]。

物聯網(IoT)技術在感測器與無線網路技術發展快速進步後，加速了人類的生活應用，將它結合日常生活之食、衣、住、行、育與樂等各層面，「智慧生活」構想得以實現，使人們生活更具有可靠性與機動性，物聯網（IoT）的時代已經在改變我們的生活了。

物聯網(IoT)系統架構可分為感知層、網路層與應用層如圖 2 所示，以一般 IoT 智慧交通應用實例而言，室外的交通透過感知層之車流量感測器量測車輛數目，並經過網路層之 Wifi、藍芽或手機通訊系統將量測車流量資料傳送至應用層之使用者手機或電腦，使用者便可得知此資訊來決定出門的方式，所以經過各獨立功能的「車流量感測器」與「使用者手機或電腦」互聯互通，讓人們實現「智慧交通」。

圖 2 物聯網(IoT)三層架構圖[7]

同樣的，電能使用是現代生活品質幕後功臣，於是我們將利物聯網(IoT)技術來做智慧電能控制，它可經由感知層之感測器擷取出來的電能數據，並利用網路層之無線通信網路與網際網路等載體將獨立的物體「電能感測器」與「前端伺服器樹莓派處理器」互聯互通，達到電能參數自動收集與控制。

(二)、「區塊鏈」(Blockchain) 部分

區塊鏈定義是將各筆資料加上編碼(如流水號與雜湊值等)成為一單位「區塊」，再利用

前後區塊之雜湊值形成一條關係「鏈」，於是這條「鏈」將前後單位區塊串聯而成一「區塊鏈」[27]，其基本架構如圖 3 所示。其區塊內容包含交易資料與驗證資料，前者交易資料包括電能交易資料與交易者與被交易者名稱，而驗證資料包括區塊號碼、流水號與前後區塊之雜湊值。當一區塊鏈一旦形成後，前後單位區塊之傳送或交易資料便產生關係，若有其中「區塊」資料被改變，則會造往後關係「鏈」改變，所以就會發現某個區塊資料被篡改，如此就可降低資料被篡改及加強資料的還原性，進而達到資料更佳的公開性與安全性。

圖 3 區塊鏈架構圖

區塊鏈技術大致分為密碼學之「公私金鑰管理工具」(Public Key and Private Key Management Tools)與數位簽章(Digital signature)、「交易」(Transaction) 和「區塊」(Block)與「區塊鏈」(Blockchain)，其交易原理是指「挖礦」(Mining)行為，也是指「工作量證明」(Proof of Work)。

1.密碼學

密碼學當目的是為了將訊息隱藏不被破解，隨著技術演進加密訊息從「對稱金鑰加密」發展至「非對稱金鑰加密」，且若密碼學再加入「雜湊函數」方法則可加強驗證資料的真實性。因此結合「非對稱金鑰加密」與「雜湊函數」方法之「數位簽章演算法」技術可被廣泛地應用於驗證身分，而區塊鏈技術交易行為便需要如此加密機制[28]。

(1).非對稱加密(Asymmetric Cryptography)

非對稱加密(Asymmetric Cryptography)利用單向函式作為加解密基礎[27][29]，加密系統製作兩把不同但有相關性的金鑰，也就是私密金鑰-公開金鑰組合，公開金鑰是可公開於大眾而私密金鑰是需使用者私自存。由於非對稱加密之非對稱特性，所以解密速度相對於「對稱金鑰加密」(Symmetric Key Algorithm)較慢，安全性也隨之較高。非對稱加密製作順序是可先產生私密金鑰，再經由私密金鑰產生公開金鑰。一般而言，資料加密應用方式可分為二種。第一種是利用公開金鑰將資料加密但必須由私密鑰匙來解密;另外，也可由私密金鑰將資料加密但必須由公開金鑰驗證，本研究即採取此方式做身分確認。

(2).雜湊函數(Hash)

雜湊函數(Hash)是一種從任何一種輸入資料利用雜湊函數產立新的輸出數字「指紋」，雜湊值便是這新的指紋，而雜湊值通常用一個短的隨機字母和數字組成的字串來代表[27]。利用雜湊函數將欲加密資料輸出成與新的雜湊值，並利用此雜湊值對原本資料進行確認，以達到資驗證功能。一般而言，驗雜湊函數有以下特點:

A.相同輸入有相同輸出。

B.要利用雜湊值回推原始值是相當的困難。

C.少量變化就會輸出不同。

D.不管輸入多少輸出都是一樣長度。

E 原則上不會有不同輸入卻有相同輸出。

(3).數位簽章(Signature)

數位簽章(Signature)是將公私金鑰與雜湊函數結合起來的技術，主要是將透過私密金鑰對資料編密與加入雜湊函數，並利用公開金鑰確認編密資料之真實性與使用者，所以可避免中間人的資料更改與證明使用者身分 [27]。數位簽章基本概念如下，使用者 A 欲傳送交易資料給使用者 B，使用者 A 利用私密金鑰需分別產生公開金鑰與數位簽章再傳送至使用者 B，當使用者 B 收到公開金鑰與數位簽章後，可利用公開金鑰與數位簽章對照傳送資料是否為正確，亦可證明此交易資料是使用者 A 所為，以下為簡單例子說明。

區塊鏈於挖礦前之身分確認與交易證明如圖 4 所示，Alice 與 Bob 間之數位貨幣交易，其交易過程是 Alice 利用私密金鑰-公開金鑰組合與數位簽章進行數位貨幣的加密，待 Bob 收到公開金鑰、數位簽章與貨幣值後進行身分確認與交易證明[28]。接下來我們會針對上述的技術進行說明。

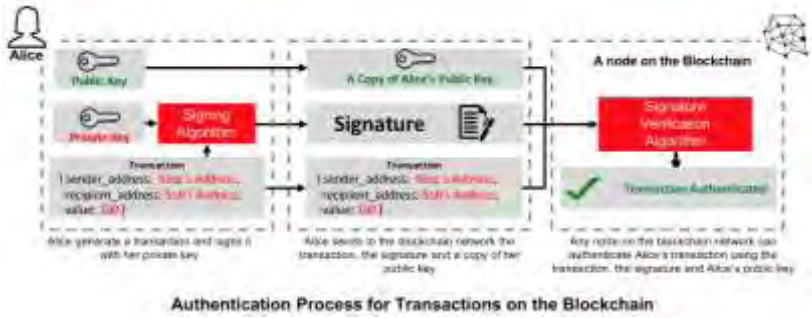


圖 4 區塊鏈交易身分確認與交易證明 [28]

2.區塊(Block)

區塊(Block)是封裝資料的一個協定，類似於網路協定的封包，裡面包含有「區塊驗證」與「交易資料」。其中「區塊驗證」記錄了交易完成的區塊驗證碼，其內容包含「區塊號碼」(Block Number)、「前區塊雜湊值」(Previous Block Hash)與「目前區塊雜湊值」(Current Block Hash)、「流水號」(Nonce) 與「時間戳」(Timestamp)。

(1).交易(Transaction)提交

當有筆交易資料欲行使交易而建立區塊時，其流程如圖 5 所示。其過程包含用戶端使用者署名、建立交易資料、輸入私密金鑰，並建立提交資料，提交資料包含交易資料、公開金鑰、數位簽章與礦池 IP，而後提交至區塊鏈伺服器礦池後等待礦工挖礦。

圖 5 交易提交之示意圖

(2).「挖礦」(Mining)

「挖礦」(Mining)目的是為了讓一個區塊與下一個區塊上鏈以形成區塊鏈，但隨著電腦的運算速度越來越快，計算雜湊值能力也加快，因此竄改區塊鏈的雜湊值時間變知，為了避免這樣的事情發生，所以會利用「工作量證明」(PoW,Proof-of-Work)的方式來延長製作區塊速度，讓竄改者不容易竄改，利用「工作量證明」(PoW,Proof-of-Work)計算雜湊值所產生的「流水號」(Nonce)來觀察驗證資速度。

工作量證明是指執行「雜湊值」時需滿足「目標雜湊值」限制條件，也就是說「目標雜湊值」代表「工作難度」難易度，所以設定「目標雜湊值」之限制位元數就是改變「工作難度」級數。

綜合以上所描述得知，聯網(IoT)與區塊鏈原理與概念可提供本研究參考，其二者整合構想如圖 6 所示。圖 6 顯示 IoT 系統感知層擷取電能參數後，由網路層傳輸電能參數至前端伺服器，並顯示電能資料與控制電能系統。再者，此物聯網(IoT)之應用層可結合後端伺服器進行區塊鏈之交易(Transaction)機制，進而達成電能資料不易被篡改。

圖 6 具有區塊鏈之 IoT 電能系統的原理圖

二、實驗規劃

本研究的 IoT 用電能系統實驗規劃分為六部分，如圖 7 所示，其順序為感知層之實驗設備架設與擷取電能參數，網路層之傳輸電能參數與建立電能參數資料庫，與應用層之用電者提出電能參數傳送與交易及區塊鏈工作量證明，工作量證明後之後可公開傳送/交易資料，若是屬性為交易資料則計算累計交易電能。

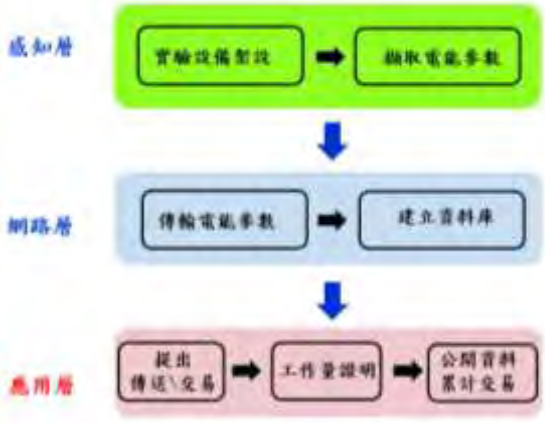


圖 7 IoT 與區塊鏈用電能系統規劃

根據實驗規劃後，我們的實驗架構依序可分成三部分如圖 8 所示。第一部分為感知層之電力模組(LT-100)從電力負載擷取電壓、電流與功率之電能參數;第二部分為網路層將電力模組(LT-100)所擷取電能參數，利用 RF 傳輸模組(YL-100T)之傳送端(Tx)與接收端(Rx)傳輸至前端伺服器(Raspberry)，並將電能參數儲存於資料庫(MySQL)以利於電能管理者分析電能數據。第三部分為當電能數據資料庫建立後，應用層之用戶端使用者便可獲得欲傳送與交易

電能資料進而向後端區塊鏈伺服器進行提交，當工作量證明後用戶端使用者可以得到區塊鏈化能資料，以下是我們的實驗規劃。

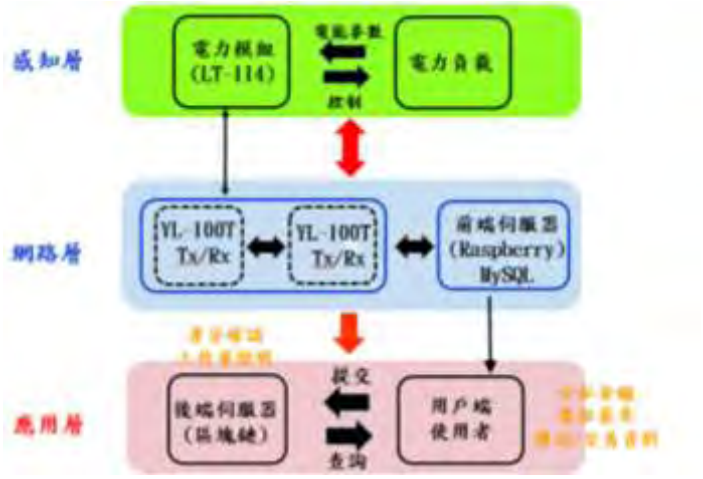


圖 8 IoT 與區塊鏈用電能系統實驗架構

(一)、感知層與網路層建置

1. 感知層與網路層連接

感知層與網路層連接包含「電力模組」(LT-114)與「傳輸模塊」(YL-100T)等所組合而成來收集電能參數如圖 8 所示，「電力模組」(LT-114)與插座串聯，並將電能參數經由「電力模組」(LT-114)插槽上的傳輸模組(YL-110T)傳輸給樹莓派，所以感知層與網路層結合功能包含下列功能:

a. 電能資料取樣:電能資料之電壓、電流與功率可由電力模組(LT-114)取樣得之。

b. 電能資料傳輸:電能資料之電壓、電流與功率可由傳輸模組(YL-110T)傳送至「樹莓派」(Raspberry Pi)伺服模組。

c. 負載控制:若發生異常負載時，我們可以控制負載啟動與停止。

2..「樹莓派」(Raspberry Pi)前端伺服器模組

「樹莓派」(Raspberry Pi)伺服器模組是將「樹莓派」(Raspberry Pi)與「傳輸模塊」(YL-100T)組合，利用「傳輸模塊」(YL-100T)連接至「樹莓派」(Raspberry Pi)的 UART（通用非同步收發傳輸器，Universal Asynchronous Receiver/Transmitter），利用「傳輸模塊」(YL-100T)接收電能負載模組之電能參數存入到樹莓派之 MySQL 資料庫中，所以「「樹莓派」(Raspberry Pi)伺服器模組包含以下功能:

a. 電能資料收集:利用輪詢(Polling)方式輪流收集不同負載之電能資料，所以我們可以分時段收集多負載電能資料。

b. 電能資料計算:將收集電能資料之電壓、電流與功率資料後，加以計算為 10 進制資料，並進一步計算消耗電能。

c. 電能資料儲存:將以上之電能資料之電壓、電流、功率與消耗電能資料儲存於 MySQL，做為區塊鏈系統傳輸與交易用。

(二)、應用層之區塊鏈伺服器模組

網路層內部前端伺服器模組的資料庫可將電能參數傳送給應用層之後端區塊鏈電能系統，後端區塊鏈電能系統包括用戶端及區塊鏈挖礦伺服端。用戶端主要功能有公私金鑰產生、數位簽章之形成及傳送 (Transmission)與交易(Transaction)，而區塊鏈挖礦伺服端包

含身分確認與工作量證明(POW,Proof of work),其規劃內容如下:

1.公私金鑰產生

使用 RSA 加密演算法來產生私密金鑰與公開金鑰，函數式如下:

$$private\_key = f_r(random) \quad (a.1)$$

$$public\_key = f_{RSA}(private\_key) \quad (a.2)$$

式(a.1)是利用函數 $f_r(random)$產生私密金鑰 private_key，而式(a.2)是使用函數 $f_{RSA}(private_key)$產生公開金鑰 private_key。

2.數位簽章之形成

產生了公開金鑰與私密金鑰後，接下來可以利用私密金鑰與傳送/交易資料 Data 來產生數位簽章 Signature，函數式如下:

$$Hash = f_{SHA}(Data) \quad (b.1)$$

$$Signature = f_{Sig}(private\_key, Hash) \quad (b.2)$$

式(b.1)是利用函數 $f_{SHA}(Data)$產生雜湊值 Hash，而式(b.2)是使用函數 $f_{Sig}(private_key, Hash)$產生數位簽章 Signature。

3.傳送 (Transmission)與交易(Transaction)

在電能資料、交易、帳單的寫入時會提出交易，在寫入區塊鏈資料庫前交易必須要有公開金鑰與私密金鑰來進行電能傳送與交易，在電能傳送與交易之前需要使用加密技術先產生私密金鑰再產生公開金鑰，私密金鑰用戶端使用者自行保存並產生數位簽章，而公開金鑰與數位簽章區塊鏈伺服端於驗證時使用。而傳送與交易類型如下:

傳送與交易中可分成三種交易類型，分別為電能參數資料類型、帳單類型與交易類型，用戶端使用者與電力管理者之傳送/交易行為，根據需要可以重複選擇一種類型以上，其說明如下:

(1).電能參數資料類型

我們使用此類型作為電能資料傳送方式如圖 9(a)所示，以利電能管理者建立資料透明化，並使用電者正確了解電能使用狀況，如此當電能系統出現異常時而傷害電器設備時，用電者便可知電壓值於區塊鏈時不可更改性而得此資訊，如電壓突然由 110 V 升至 130 V 時用電者不會被隱瞞而可以請求賠償。

(a)

(b)

(c)

圖 9 電能參數傳送/交易提交類型。(a)電壓、電流與功率傳送類型，(b)電能(帳單)傳送類型，(c)電能交易類型。

(2).帳單類型

用戶端使用者透過區塊鏈產生區塊帳單，所以每個月可以自行產生電能帳單，如用戶端使用者本月及上個月使用 150 度電能，而本月使用 120 度電能，都經區塊鏈將此前後二個月中的每個月電能帳單當作每個區塊後並成鏈如圖 9(b)所示。

(3).交易類型

使用於雙方在每筆交易串聯而成區塊鏈的狀況，交易行為包括用戶端使用者與電能管理者和用戶使用者之間交易如圖 9 所示(c)，以讓三方都得到好處，在此我們以用戶端使用者 A 與用戶端使用者 B 為例，其說如下:

交易過程中用戶端使用者 A 與電能管理者的電能契約為 200 度，因用戶端使用者 A 在該月發現不需要滿載契約容量，而是僅需 90 度電能，於是將過多的電能剩餘量 110 度轉賣給其他使用者。而此時若用戶端使用者 B 於本月用電是突然激增而超過契約容量，此時將提高電費成品，於是若有其他用電者可以以較便宜電費賣給用戶端使用者 B。所以在這個機制之下，用戶端使用者 A 與用戶端使用者 B 都可得到經濟上利益，且電能管理者也有亦可獲得交易管理電能成本，如此便可控制總電能的使用，降低發電與維護成本，進而減少環境污染。

4.挖礦

礦工在挖礦時會先將寄件者傳送到礦池的交易進行驗證，需透過數位簽章與公開金鑰、進行電能資料與身分驗證，再進行工作量證明，方可產生新區塊，其過程如下所示。

(1).身分確認

當有筆傳送或交易資料至區塊鏈伺服器，系統會透過公金鑰、雜湊值與數位簽章進行確認電能資料與寄件者的身分，函數式如下:

$$\text{Hash} = f_{SHA}(\text{Data}) \quad (c.1)$$

$$\text{Verifier} = f_{Ver}(\text{private\_key}, \text{Hash}, \text{signature}) \quad (c.2)$$

式(c.1)是利用函數 $f_{SHA}(\text{Data})$產生雜湊值 Hash，而式(c.2)是使用函數 f $f_{Ver}(\text{private_key}, \text{Hash}, \text{signature})$確認身分。

(2).工作量證明

工作量證明是指執行傳送/交易電能參數之雜湊值猜測，當雜湊值符合預設「工作難度」/「目標雜湊值」時，工作量證明便宣告完成，採取流水號累計方式可觀察猜測雜湊值的次數。「工作難度」設定方法可由「目標雜湊值」之’0’位元數來表示，在此我們將「工作難度」分為 5 級，其所對應「目標雜湊值」之限制位元數如表 2 所示。

表 2 「工作難度」級數

工作難度	目標雜湊值限制位元數
1	1
2	2
3	3
4	4
5	5

工作量證明時需要傳送或交易資料 Data、前區塊雜湊值 Previous_Hash 與流水號 Nonce 做為本區塊雜湊值猜測之依據，函數式如下:

Guess_Hash $=f_{POW}$(Data, Previous_Hash, Nonce) **satisfy** work_diffculty (d.1)

式(d.1)是利用函數 f_{POW}(Data, Previous_Hash, Nonce)滿足限制條件「工作難度」work_diffculty 而產生工作量證明之雜湊值 Guess_Hash, 。

礦工挖礦結束因而產生新區塊(Block)附加於區塊鏈(Chain)中，所以前後區塊具有鏈結性。新區塊內容包含傳送/交易資料與計算結果之區塊驗證資料;其傳送/交易資料有傳送者、接件者與電能資料(Transactions)，而區塊驗證資料有區塊號碼(Block_number)、流水號(Nonce) 、時間戳 (Timestamp) 、前區塊雜湊值(Previous_Hash)與本區塊雜湊值(Hash) ，其電能區塊內容架構如圖 10 所示。

圖 10 電能資料區塊內容架構

5. 公開傳送/交易完成資料

公開工作量證明完成後之傳送/交易資料，本研究架設區塊鏈伺服端公開區塊鏈資料網頁，並製作用戶端使用者操作界面網頁提使用者查詢。

6. 累計交易

區塊鏈伺服端提供累計電能交易功能，其電能交易包含用戶端使用者與電力管理者之電

能交易及用戶端使用者間電能交易，其累計電能交易式如下:

$$E_{h,\text{Tran}} = \sum_{i=1}^{M} E_{h,g,i} + \sum_{j=1}^{N} E_{h,k,j} + \sum_{j=1}^{N} E_{h,s,gain} \quad \text{(e1)}$$

$$E_{h,Remain} = E_{h,con} + E_{Tran} - E_{h,Dis} \quad (e2)$$

以下不同代號對應的意思:

$E_{h,Tran}$：用戶端使用者 h 累計電能交易。

$E_{h,g,i}$：用戶端使用者 h 與電能管理者 g 之第 i 次電能交易。

$E_{h,k,j}$：用戶端使用者 h 與其他用戶者 k 之第 j 次電能交易。

$E_{h,s,gain}$：用戶端使用者 h 向其他用戶者 s 購買電能，稱為「交易獲得電能」。

e. 計算剩餘電能，合計契約容量與交易獲得電能後扣除損失電能與交易電能總合如式(9)所示。

$E_{h,Regain}$：每個月契約容量扣除累計交易量及損失電能並加上得到電能，稱為「剩餘電能」。

$E_{h,Dis}$：用戶端使用者 h 經交易或電能耗損後剩餘電能，稱為「損失電能」。

$E_{h,con}$：用戶端使用 h 者向電能管理者 g 每月購買電能值，稱為「契約容量」。

7. 工作難度與流水號之關係圖表

由於工作量證明的工作難度可以控制區塊的產生時間，因此我們針對了工作難度與流水號之關係進行研究，希望可以找出交易提交最佳化的方法。

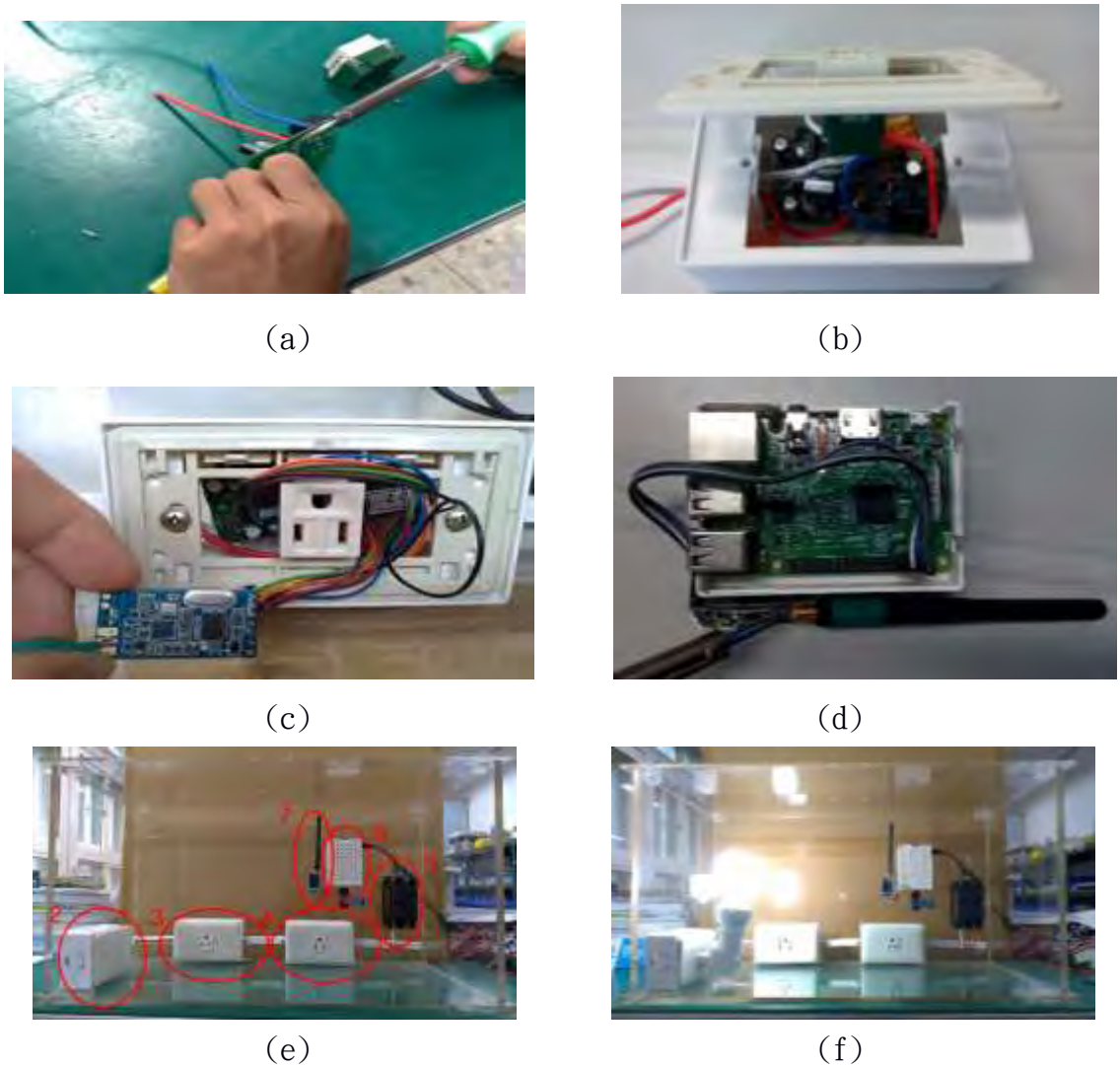
此實驗方法先在提出傳送/交易時輸入相同私密金鑰，並讓其他資料保持空值，包括傳送/交易的時間參數，讓傳送/交易的變化保持一致。再來會有變化的是傳送/交易後經過挖礦後所產生的區塊驗證資料，我們會依照工作難度的五級並紀錄每一級做五十次挖礦後的工作難度對應流水號，統計出每一次提交交易中所需要的猜測次數。

陸、研究過程與結果

經過我們的實驗設備架設測試後，無論在物聯網(IoT)感知層、網路層之前端伺服器與應用層之後端伺服器區塊鏈電能資料傳送/交易設設置，其系統硬體與軟體我們都得到初步研究結果，其研究過程與結果將予以說明。

一、感知層與網路層建置

製作完成感知層之電力模組(LT-114)擷取電能參數與前端伺服器網路層之前端伺服器(Raspberry)，皆建構在一個小型空間模型上，如圖 11 所示。其圖 11(a)為電力模組(LT-114)電路焊接圖;圖 11(b)為「電力模組」(LT-114)焊接於負載媒介(插座)以利負載連接於系統內;圖 11(c)為「電力模組」(LT-114)、「傳輸模組」(YL-100T)與負載媒介(插座)整合於插座盒內。



(a) (b)

(c) (d)

(e) (f)

圖 11 物聯網(IoT)之感知層與網路層架設圖。(a)電力模組(LT-114)電路焊接圖，(b)電力模組(LT-114)組裝圖，(c)電力模組(LT-114)與傳輸模組(YL-100T)組合圖，(d)樹莓派前端伺服器模組，(e)架設完成圖，(f)電能負載測試圖。

圖 11(d)為前端伺服器模組，主要是「樹莓派」(Raspberry Pi)與「傳輸模塊」(YL-100T)組合成。綜合以上，其感知層與網路層系統整體架設完成圖完成如圖 11(e)所示，圖中顯示器具編號如下:

1. 編號 2-4 為「電力模組」(LT-114)、「傳輸模組」(YL-100T)與負載媒介(插座)整合模組。
2. 編號 5 為電源無熔絲開關。
3. 編號 6 為樹莓派伺服器。
4. 編號 7 為樹莓派伺服器專用之「傳輸模組」(YL-100T)。

圖 11(f)電能負載通電測試圖，將量測 1000 筆以上電壓、電流、功率與消耗電能之電性參數皆儲存於前端伺服器 MySQL 資料庫如圖 12 所示，資料表亦記載量測電能管理者與用電端使用者。除了可以收集資料，還可以針對負載操作

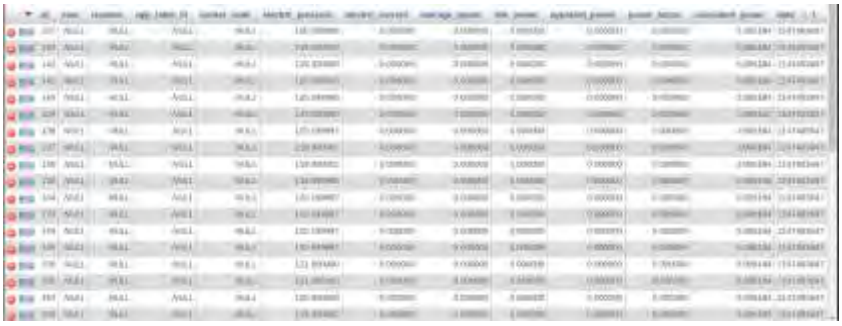


圖 12 前端伺服器 MySQL 資料庫之負載量測電能參數

二、應用層之後端伺服器區塊鏈系統

本研究之 IOT 應用層之後端伺服器區塊鏈系統包含了用戶端使用者(User terminal)及區塊鏈伺服端(Blockchain Master)部分;前者是指用電使用者將電能資料傳送給區塊鏈伺服端進行挖礦並查詢挖礦後區塊鏈資料，而者是不但具有用電使用者與電能管理者之電能資料(含電能帳單)傳送與交易功能，且也有用電使用者之間的電能交易功能。

(一).用戶端使用者(User terminal)之傳送與易部分

為讓戶端使用者可以進行電能資料查詢與傳送與交易，本研究設計了區塊鏈使用者操作平台，而區塊鏈使用者操作界面(User Interface,UI)之網頁界面如圖 13 所示，其中包含了傳送\交易前之準備與交易後之區塊鏈資料查詢功能，其功能如下所示:

1.產生公私金鑰(Key Generator)。

2.提出電能資料(含電能帳單)傳送與交易(Transmission\Transaction)。

3.用戶端使用者查詢區塊鏈資料(View Results)。

圖 13 使用者(User)網頁操作界面

(二).區塊鏈伺服端(Blockchain Master)部分

本研究之之區塊鏈伺服端提供電能與交易資料成區塊鏈化功能，主要是由礦工將電能傳送與交易資料進行挖礦動作，也就是指進行工作量證明(POW)演算，其操作界面之網頁如圖 14 所示，其中包含了挖礦前之準備及傳送與交易成功後之區塊鏈資料管理功能，其功能如下所示:

1.伺服端接收資料與確認身分。

2.具有挖礦功能(Mining)。

3.查看區塊鏈資料架構(Diagram)。

圖 14 區塊鏈伺服端(Blockchain Master)之網頁操作界面

(三).電能資料傳送與交易之區塊鏈化步驟

從用戶端使用者(User terminal) 產生公私金鑰至傳送\交易電能資料至區塊鏈伺服端(Blockchain Master)進行挖礦成資料區塊鏈化，並顯示區塊鏈資料架構，其架構包括區塊碼(Block)、流水號(Nonce)、前區塊雜湊值(Pre-Hash)與本區塊雜湊值(Hash)。而資料區塊鏈化後提供用戶端使用者查詢區塊鏈資料，目前完成電能資料傳送與交易之區塊鏈步驟如下:

1.產生公私金鑰

本研究之區塊鏈使用者之產生公私金鑰網頁界面下如圖 15 所示，按下產生金鑰的按鈕，這時會產生一組「公開金鑰」(Public Key)與「私密金鑰」(Private Key)，而公開金鑰為 16 進制之 324 位元碼:

30819f300d06092a864886f70d010101050003818d0030818902818100fc5fb2962417556af00dab82f334169ea48157c89358b42edd223195bc39c94d02741be99d3226ddb14ece898ca9df7d2d9a3cb8560007aaf746edfad90e609a19b7bf246c81a2f0b4ebd62eaf0ad4df35f2ccbd5c92788f953dc89bb54c1fafaa18809b11278cf025af59624807e17b4d4900871a5e0b6b53aea599f44db9bf0203010001

圖 15 產生公私金鑰之公開金鑰

為提醒使用者之私密金鑰被竊看，我們設計隱藏式私金密鑰模式，需要按下產生私密金鑰按鈕才會顯示私密金鑰如圖 16 所示，由於私密金鑰由使用者自己保存，所以不能在提出電能資料傳送與交易送出。私密金鑰(Private Key)為 16 進制之 1216 位元碼:

3082025c0201002818100fc5fb2962417556af00dab82f334169ea48157c89358b42edd223195bc39c94d02741be99d3226ddb14ece898ca9df7d2d9a3cb8560007aaf746edfad90e609a19b7bf246c81a2f0b4ebd62eaf0ad4df35f2ccbd5c92788f953dc89bb54c1fafaa18809b11278cf025af59624807e17b4d4900871a5e0b6b53aea599f44db9bf0203010001028180245a247f3bf3a07a26d9d13aab8d7534a4bd7cc78771df826097ec4c85304daeaa0bcf79770b224e0c9c2d63e2bf1552129f84df8883b89707c74fc03243bfe62954325dc201068c2b391492b59805b742c4b0451ec9a4b0287ebd7c02

3daf48b6305e142f7670531d7f1ab5a1ed1d8504693393b3ab21fef6848e8a8cb5b701024100fd14
63ed53231c44f03175c5bc9d39e3288db2ec453ba1d9be4a337d7d6d89cfa56d61e7c763668d55e9
e80ee7eacb1ff4dcc566d773b7b31ff998563937c9a5024100ff4938e25ed3725a94db5bc0519841
2fe3d9bcb24f587ae457d962eda10b3c518d19a5f40173735c5cba5f684b3644b9e2045009808f7d
199924dc421fbe3093024100deee913fc3565056a1c6cfd9c9562e61dd9d4499403b514d3f84996a
d78c20335ba3c8f4a4fcf89f53a8e2140f53126f2a01379a69fbb33c04d496ce8d4489490240383f
81f11ec3a8269d35d7f98000f41c0130308b79401d93c2677b8cb037318b2673c845032cd4f63cd8
33bd5f150dff86f53c4d5bae41fa29ec1d3bd492ab5102403bd5e7abe86be0968d32389341bd04ae
5c4e993cc21644fa868833fb3d8f1ff76b78bbcf49aa3a17d20c574de2b3618e347d4e9f11d79480
62e2ce048ea525fe

圖 16 顯示私密金鑰

2.顯示使用者用電及交易資料

為將 IoT 之 MySQL 資料庫與區塊鏈系統連結，我們先用戶端使用者(User terminal)建立電能使用資料，並由網頁界面顯示電能資料以利使用者選用而提出電能資料傳送與交易，電能資料顯示如圖 17 所示，圖 17(a)是用戶端使用最新電能使用資料，而圖 17(b)目前用戶端使用者全部電能使用資料。

(a)

(b)

圖 17 (a)用戶端使用最新電能使用資料，(b)目前用戶端使用者全部電能使用資料。

3.輸入電能資料

我們可以用填寫或點選方式輸入電能資料。其內容包括用電使用者、管理者/交易者、

電壓、電流、功率與消耗功率等資料。在此，我們可分三種情形提出傳送與交易，分別為
(1).使用者僅傳送電能資料給電能管理者。
(2).使用者傳送電能與交易資料給電能管理者。
(3).使用者間傳交易資料。

我們先實驗使用者僅傳送電能資料給電能管理者之事件，使用者與電能管理之選用電能參數區塊鏈如圖 18 所示。圖中顯示使用者(Chen)為傳送者(Transmitter)將電能參數資料傳至區塊鏈伺服端系統，其指定電能管理者(Manager)為接收者(Receiver)。傳送電能參數資料電壓 V=121.400002 V、電流 I=0.084 A、功率 P=10 W 之 電能 W=2.7 Kw-hr。待輸入電能資料與輸入私密金鑰(Private Key)後開始準備傳送電能資料。

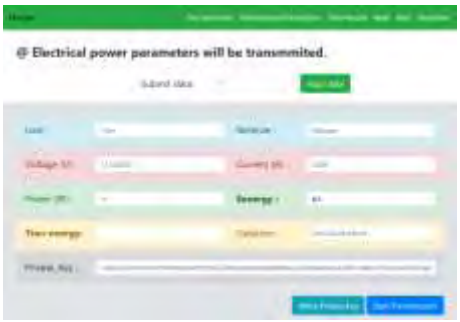


圖 18 輸入電能使用與傳送資料

4.提出傳送/交易

用戶端使用者提出提出傳送/交易請求時，系統產生數位簽章(Signature)如圖 19 所示，圖 19 亦顯示之前輸入的使用者(Chen)、電能管理者(Manager)、電能資料與公開金鑰(Public Key)，待使用者確認輸入資料無誤後即可按下「確認鈕」將資料傳送至區塊鏈伺服端。

圖 19 提出傳送/交易請求

其數位簽章(Signature)碼為 16 進制之 256 位元碼:
7ae53fdfe70ac5b2c9ac069979a41dbfcb2928c80cc4f98a07715ed5f4109e5715ef3f4214fd21
29bdaf928ae9ea756b36419f0aea534062596749988d96e173b798e389949388545ecc7315b0d1
54aa264883e204d65f92f542afb4084de1844588fc8b71e875b976c413ef9642a76b72ac55d29f
ae6296f9d7a801ef7ceedf

5.區塊鏈伺服端接收資料

區塊鏈伺服端(Blockchain Master)接收電能資料也就是指礦池之電能資料，其內容如圖 20 所示。由於礦池之電能資料是由用戶端使用者(User terminal)所傳送而來的，所以需將做身分驗證，也就是區塊鏈伺服端根據所收到的數位簽章(Signature)與對應的公開金鑰(Public Key)來確認用戶端使用者，待確認資料無誤後，再將這些礦材(電能資料)提供給礦工挖礦而成為區塊鏈其中的新區塊。在此，根據之前所做的操作，其欲挖礦的電能資料如圖 20 所示，電能資料之電壓 V=121.400002 V、電流 I=0.084 A、功率 P=10 W、電能 Energy E= Kw-hr，這正是使用者(Chen)所傳送來的資料吻合。

圖 20 礦池之待挖礦電能資料

5.工作量證明(POW)

工作量證明(POW)即是挖礦的重要工作，礦工(電腦)會將礦池內的交易清單之電能資料逐一進行交易，「工作難度」決定交易速度，本次實驗是設定「工作難度」為 2。工作量證明之順序則是由時間最早資料的開始處理，所以需注意欲傳送或交易資料是正確性。當按下 Mine 按鈕時即開始會進行交易的驗證，也就是將礦池的資料經過工作量證明(POW)後產生新的區塊鏈驗證資料，其驗證後每個區塊會區塊會產生區塊驗證特徵參數時間戳（Timestamp）、區塊碼(Block number)、流水號(Nonce)、前區塊雜湊值(Previous Hash)與本區塊雜湊值(Hash)。

於是我們可呈現完成工作量證明後之區塊 2 (Block=2)部份資料，其內容如圖 21 所示。在此可看出當礦工挖完礦後，會將礦池清單清空，並形成區塊(Block_2)資料。區塊資料除了使用者(Chen)傳送來的資電能資料電壓 V=110.7 V、電流 I=20.5 A、功率 P=1820.5 W、 消耗電能(意指電能帳單)Energy E=0.5 Kw-hr 外，並顯示其時間戳（Timestamp）與區塊碼(Block number)。工作量證明資料皆公開於網頁，並提供用戶端使用者查詢(於後文說明之)，所以可達到電能公開不易篡改性。

圖 21 工作量證明完成後電能資料

6.區塊鏈架構

我們先假說目前有三個區塊鏈伺服端工作，也就是有三位礦工進行挖礦，挖礦完成後，其三個區塊鏈伺服端圖 22 表示。一個完整區塊表示可由圖 22(a)表示，Master1 之區塊包含區塊碼(Block)、流水號(Nonce)、使用者(User)、接收者(Rec)、電能資料(電壓 V、電流 I、功率 P、電能 E.E)與交易電能 T.E.E、前區塊雜湊值(Pre-Hash)與本區塊雜湊值(Hash)，而前區塊是指 Block=1(初始區塊)。在此，區塊資料包含使用者(Chen)傳送來的資電能資料電壓 V=121.400002 V、電流 I=0.084 A、功率 P=10 W、消耗電能(意指電能帳單)Energy E=0.0005 Kw-hr，且其他區塊驗證資料為:

Block_1

Nonce: None

Pre-Hash:0

Hash: 0000000016b52afffb5860b5e3a076b0513c0c4970d1c6a549afe151cdacabc

(a)

(b)

(c)

圖 22 區塊鏈之區塊 2 架構 (a)伺服端 1，(b)伺服端 2，(c)伺服端 3。

由於目前我們假設有三位礦工挖礦並進行協商後的結果，圖 22(b)與(c)所顯示的伺服端 Master2 與伺服端 Master3 之區塊參數均與伺服端 Master1 一樣，其區塊碼(Block)、流水號(Nonce)、使用者(User)、接收者(Rec)、電能資料(電壓 V、電流 I、功率 P、電能 E.E)與交易電能 T.E.E、前區塊雜湊值(Pre-Hash)與本區塊雜湊值(Hash)都與伺服端 Master1 相同。

7.用戶端使用者之資料查詢部分

當伺服端完成交易流程與建立區塊鏈之新區塊後，用戶端使用者便可查詢傳送/交易的內容，而查詢需先輸入伺服端 Master 主機網址(IP)與埠(port)，而後按下查看「傳送/交易鈕」，用戶端於是可以得到從伺服端傳來之電能(帳單)與交易資料，其傳送/交易資料與伺服端挖礦資料一致，所以於此亦包含寄件者、接收者、電能參數、時間戳與區塊號碼，其內容如圖 23 所示。

圖 23 使用者查詢已傳送/交易資料

以上區塊鏈之區塊 2(Block_2)僅進行電能資料與電能帳單傳送之過程，所以沒有進行電能交易。於是我們將測試第二種例子，也就是增加使用者與電力管理者電能交易，所以在「Tran_engergy」選項輸入欲交易電能值如圖 24 所示。其輸入電能資料電壓 V=110.1 V、電流 I=18.3 A、功率 P=1601.1 W、 消耗電能(意指電能帳單) Energy E=1.2 Kw-hr 外，且增加交易電能 Tran_engergy=50 Kw-hr，也就是使用者 Chen 將轉讓電能 50 kW-hr 給電能管理者，而後並重複之前操作步驟進行電能傳送與交易。

圖 24 用戶端使用者與電能管理者之電能交易

在此，我們看到新的挖礦後區塊鏈資料如圖 25 所示，除了之前區塊鏈之區塊 2(Block=2)資料外，我們增加新的區塊 3(Block=3)，其區塊內容除了有使用者(Chen)傳送來的資電能資料電壓 V=121.400002V、電流 I=0.084A、功率 P=10 W、 消耗電能(意指電能帳單) Energy E=0.0005 Kw-hr 外，增加交易電能 Tran_engergy=50 Kw-hr，並顯示其工作量證明後之時間戳（Timestamp）與區塊碼(Block number)。

圖 25 具有與電能理者之挖礦完成後電能資料

以上為區塊鏈之區塊 2(Block_2)與區塊 3(Block_3)都是用戶端使用者與電力管理者進行電能資料傳送(含帳單)與電能交易，接下來我們將測試用戶端使用者間電能交易。同樣地，用戶端使用者 Chen 將與使用者 Lee 進行電能交易，也就是使用者 Chen 將轉讓電能 200 kW-hr 給使用者 Lee，所以在「Tran_engergy」選項輸入 200 kW-hr，如圖 26 所示，並重複之前的操作步驟進行電能傳送與交易。

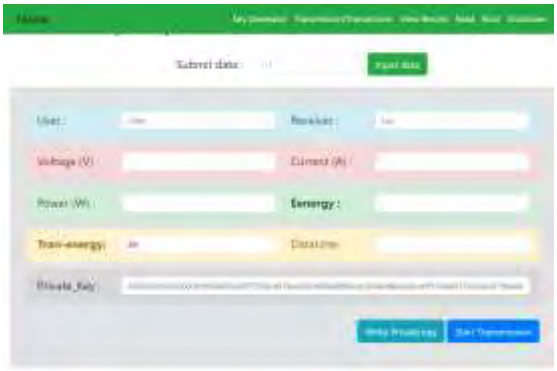


圖 26 用戶端使用者間電能交易傳送

同樣地，我們看到新的挖礦後區塊鏈資料如圖 27 所示，除了之前區塊鏈之區塊 1(Block=1)與區塊 2 (Block=2)資料外，我們增加新區塊 3(Block=3)，其區塊內容除了用戶端使用者 Chen 將與使用者 Lee 間交易電能 Tran_engergy=20 Kw-hr，並顯示其工作量證明後之時間戳（Timestamp）與區塊碼(Block number)。工作量證明資料除了公開於網頁外，也可計算累計的交易電能值，所以目前累計電能交易值為 70Kw-hr。

圖 27 用戶端使用者間電能交易之挖礦完成後電能資料

8.多重區塊

根據以上的測試，我們可得每個區塊鏈伺服端之三個區塊如圖 28 表示。同樣地，圖 28(a)表示每個區塊區塊碼(Block)、流水號(Nonce)、使用者(User)、接收者(Rec)、電能資料(電壓 V、電流 I、功率 P、電能 E.E)與交易電能 T.E.E、前區塊雜湊值(Pre_Hash)與本區塊值(Hash)。而三個區塊之區塊碼(Block)、流水號(Nonce)、前區塊雜湊值(Pre_Hash)與本區塊雜湊值(Hash)分別如下:

Block_2

Nonce_2: 5381

Pre_Hash_2: 0000000016b52afffb5860b5e3a076b0513c0d2d4489a9c4675c98e7e4a48a0d
Hash_2: 00017a85dfc827c980839e5e5912dbda48e1e970d1c67c264a549af9bcdccabb
Block_3
Nonce_3: 2863
Pre_Hash_3: 00017a85dfc827c980839e5e5912dbda48e1e970d1c67c264a549af9bcdccabb
Hash_3: 0008353ca03c0bb35e6dacb4cb354573a192c7660652abdbc34adbdc1920c2c2
Block_4
Nonce_4: 6280
Pre_Hash_4: 0008353ca03c0bb35e6dacb4cb354573a192c7660652abdbc34adbdc1920c2c2
Hash_4: 000440b184175ef377ee3f3bc5e9a34b2d85437acb3530bb192c9809ecaadbab

在此我們可觀察每個區塊流水號(Nonce)，其代表意思是指工作量證明(POW)之驗證次數，也就是每個區塊之挖礦速度不一樣，這是由於挖礦時是採用隨機雜湊函數方式。另外，我們可發現前後區塊之雜湊值且有一致連貫性，也就是指本區塊雜湊值(Hash)之前區塊雜湊值(Pre_Hash)會等於前區塊之雜湊值(Hash)，所以 Pre_Hash_3= Hash_2 及 Pre_Hash_4= Hash_3，此關係造成區塊間之「鏈」，所以每個區塊能以此關係建立聯結形成「區塊鏈」。同樣地，圖 28(b)與(c)所顯示的伺服端 Master2 與伺服端 Master3 之區塊參數均與伺服端 Master1 一樣，所以其區塊碼(Block)、流水號(Nonce)、使用者(User)、接收者(Rec)、電能資料(電壓 V、電流 I、功率 P、電能 E.E)、交易電能 T.E.E、前區塊雜湊值(Pre-Hash)與本區塊雜湊值(Hash)都與伺服端 Master1 相同。

(a)

(b)

(c)

圖 28 區塊鏈之區塊號碼 2-4 內容架構。 (a)伺服端 1，(b)伺服端 2，(c)伺服端 3。

根據以上不斷測試用戶端使用者與電力管理者及用戶端使用者間之電能資料傳送(含帳單)與電能交易，伺服端均可完成交易與建立區塊鏈之新區塊，所以用戶端使用者便可查詢目前所有電能資料傳送(含帳單)與電能交易的內容。用戶端於是可以得到從伺服端傳來之電能(帳單)與交易資料，其交易資料與伺服端挖礦資料一致，所以用戶端使用者(Chen)可收到使用者(Chen)與電能管理者與另一使用者(Lee)曾經傳送(含帳單)與電能交易資料，也就是指所有挖礦後之寄件者、接收者、電能參數、時間戳與區塊號碼，其內容如圖 29 所示。

圖 29 使用者查詢所有電能傳送/交易資料

除了可以看所有的電能資料(帳單)與交易，還可以看到使用者使用電能的累計交易，從圖 30 可以看到此表中所使用的欄位，有「契約容量」、「損失電能」、「交易電能」、「交易獲得電能」與「剩餘電能」，其中損失電能會自動從用戶端使用者扣除 MySQL 中的消耗功率，當電能無法扣除時會拒絕執行傳送/交易，達到限額並提醒使用者電能消耗完畢。

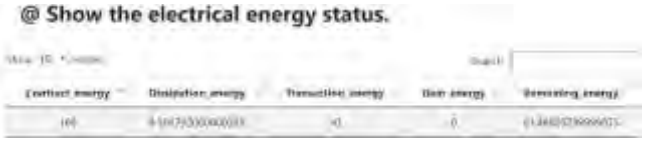


圖 30 累計交易之用戶端使用者電能花費計算

四、工作難度與流水號之關係

由於我們需要找出提交交易中的最佳化，因此我們針對工作難度、流水號之間做實驗，會重複的上述的實驗過程中的提交交易流程但依照實驗規劃進行實驗。可以看到表三中不同等級的平均值，如果要詳細數據可以從附錄 1 去查看，從附錄 1 可以看到即使難度有提高，但流水號仍有猜測次數很少的時候。

可以看到隨著難度提升流水號的時間也會上升，並可以從圖 31 中看到級數與流水號平均值折線圖，橫軸為級數，縱軸為 50 次流水號的平均值，從此圖表可以看到在級數 2~4 有急速的上升，前後都是平穩的成長。

表 3 工作難度與流水號平均值對應表

工作難度	1	2	3	4	5
平均值	26.56	216.46	10794.2	29172.66	30431.58

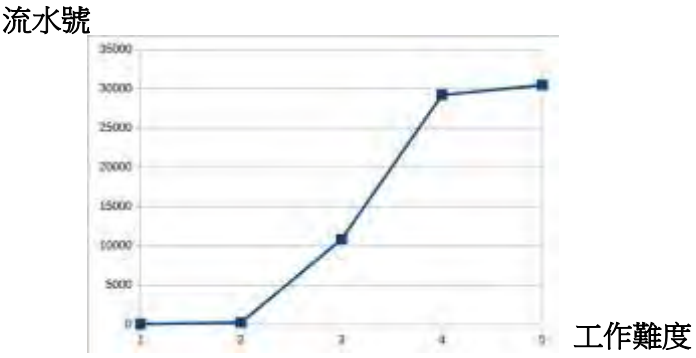


圖 31 級數與流水號平均折線圖

柒、問題與討論

此研究結合了硬體系統、韌體程式撰寫與軟體設計，其硬體部分包括了感知層電力配線與電子電路;韌體撰寫部分包含了感知層之電力模組(LT-114)之電能參數擷取設定與網路層之 RF 通訊模組(YL-100T)模式預置;軟體設計部分則是以網路層之前端伺服器 Raspberry 之電能資料過濾、解碼、計算與儲存，與應用層之區塊鏈伺服器之工作量證明演算法與網頁設計程式為主，研究過程我們發生了下列問題:

問題一:電能參數傳輸錯誤。

解決方法:電能參數傳輸錯誤是由於 RF 通訊模組(YL-100T)傳送鮑率錯誤，所以需設定 RF 通發射端與接收端一致的傳送鮑率。

問題二: 電能參數收集錯誤。

解決方法:前端樹莓派伺服器所收到的電能參數需再經過加權位式計算，方能得到正確的電能參數。

問題三:多負載電能參數取得錯誤。

解決方法:前端樹莓派伺服器可以用輪迴方式擷取多負載電能參數，以達到多使用者或多重負載之電能資料擷取。

問題四:伺服端挖礦資料之重複性錯誤。

解決方法:這是由用戶端使用者傳送重複資料至區塊鏈伺服端，我們先在用戶端增加「確認」功能，但仍然無法有效解決此問題。於是在區塊鏈伺服端加強資料確認，將重複資料予以刪除，避免工作量證明時重複證明。

問題五:伺服端使用者身分確認失敗。

解決方法: 用戶端使用者傳送資料需要公開金鑰(Public Key)至區塊鏈伺服端挖礦，卻在伺服端驗證使用者身分時發生失敗驗證。我們發現伺服端確認使用者身分時，公開金鑰

(Public Key)與數位簽章 (Signature)無法一致性，於是我們在驗證時需使兩者資料編碼型態一致，才可正確確認使用者身分。

問題六:工作量證明(Proof-of-Work)速度與區塊鏈資料安全性之矛盾性。

解決方法:工作量證明之工作難度級數決定挖礦速度，而流水號(Nonce)是挖礦次數，所以流水號(Nonce)可觀察挖礦的速度;工作難度級數愈高則挖礦速度愈久，流水號相對的也較大如表 3 所示，表 3 為實驗規劃的條件下所得結果。工作難度級數為 1 之流水號平均值(Nonce)為 26.56，而工作難度級數為 5 平均值為 30431.58，所以工作難度級數平均值之最高級數 5 為最低級數 1 達 1145.76732 倍。工作難度提高工作難度雖可增加資料的安全性，但也減少電能資料傳送與交易的速度，所以設定適當的工作難度是重要的，同時搭配時間的測量也可以作為適當設定工作難度的依據。因此如何設定工作難度級數與搭配時間做為調整依據是另一項重要議題，是往後可以繼續研究的。

問題七:區塊鏈間之前後區塊雜湊值無法連貫性問題。

解決方法:這是由於我們剛開始無法在前後區塊產生有效的資料鏈結，於是我們先設定啟始區塊之雜湊值，所以第一筆傳送/交易資料於工作量證明時方可銜接啟始區塊之雜湊值，並在往後區塊工作量證明時正確設定前後區塊之雜湊值連貫性。

問題八:不同區塊鏈伺服端之協商問題。

解決方法:不同區塊鏈伺服端之挖礦時機與速度不一樣，所以會產生不同的區塊鏈長度，此時系統需要做不同區塊鏈伺服端間協商以求最大區塊鏈長度，但由於我們單機挖礦實驗無法有效測試，於是先假設各個區塊鏈伺服端工作量證明大小，並取其最大長度之區塊鏈伺服端之區塊鏈為協商後之區塊鏈。

問題九:區塊鏈伺服端資料之竄改問題。

解決方法:如果區塊鏈伺服端資料遇到竄改，如電能資料之電壓值、消耗能量與交易能量，及流水號(Nonce)與雜湊值(Hash)，此時需要做各區塊鏈伺服端間之協商得到最可能正確值，目前我們正在討論如何選擇協商機制以達到此目的。

問題十:區塊鏈伺服器之網頁操作界面(UI)之整合性問題。

解決方法:本系統由於使用 Python+Flask+Web 應用程式作為網頁開發設計整合，如用戶端使用者與區塊鏈伺服端之網頁操作界面(UI)操作沒做好整體規畫，不但易混肴出錯且會浪費許多時間檢查。

問題十一:區塊鏈伺服器之電能交易的最佳化問題。

解決方法:本系統可進行用戶端使用者與電能管理者與用戶端使用者間之電能交易，其最大目的是希望電能交易而降低總電能量使用，所以如何設定交易契約以達到最佳效果是另外一個重要議題。

捌、結論

依據上述研究結果，證明將區塊鏈結合物聯網(IOT)電能遠端量測以達到電能資料安全性、電能交易與節能想法的可行性，雖然只是初步完成簡易「具有區塊鏈之 IOT 用電系統」，但已看出本研究具有公開不易篡改性之電能參數、帳單與交易之區塊鏈能力，其系統功能包含如下:

一、研製感知層之電力模組(LT-114)與網路層之「傳輸模組」(YL-100T)為主的 IoT 遠端多使用者之量測與監控功能，使得電能系統更加自動化。

二、完成網路層之前端伺服器「樹莓派」(Raspberry Pi)電能數據收集與 MySQL 資料庫儲存系統，不但可方便用戶端使用者查詢，也可讓電能管理者掌握電能使用狀況，並成為電能資料區塊鏈化的基礎，達到強化電能參數之真實性。

三、以 Python、Flask 與網頁設計等方法設計電能區塊鏈傳送與交易資料平台，並鼓勵用戶端使用者加入此系統參與挖礦工作，進而達到更多的電能交易。

四、本研究之區塊鏈部分利用了密碼學、數位簽章、雜湊函數與工作量證明(Proof-of-Work)等方法建立傳送與交易電能資料(含帳單)之正確性、可靠性與安全性。

五、設計一套具有僅有電能資料(含帳單)、用戶端使用者與電能管理者與用戶端使用者間之電能交易與累計系統。

六、紀錄工作量證明之工作難度與流水號關係，使我們可以知道影響傳送/交易速度的原因。

綜合以上，此研究結合物聯網(IoT)與區塊鏈技術應用於電能智慧型控制，我們透過電力模組(LT-114)取得各組負載之電氣特性參數，並以「傳輸模組」(YL-100T)傳送至「樹莓派」(RaspberryPi)前端伺服器，而前端伺服器以輸流模式輸流取得多組負載之電氣特性參數並建立電能資料於 MySQL 資料庫。後端的區塊鏈伺服器主要為 Python+Flask+Web 應用程式做為網頁開發設計界面(UI)與區塊鏈之傳送/交易系統。所以此研究可將電氣特性參數(含帳單)及交易建立區塊並成鏈，達到電能與交易資料公開透明化，進而防止資料篡改。如此一來，「具有區塊鏈之 IOT 用電系統」可以讓用電使用者能節省電費，電能管理者能有效調配電能並降低電能使用之日將不遠矣。

由於這是初步的研究結果，尚有許多功能需改進與增加，未來會努力改善與加強的研究，包括更多人使用的物聯網(IoT)遠端量測、更多電能數據收集、更方便與自動化的區塊鏈傳送與交易資料平台、更完整工作量證明之選舉協商機制、工作量證明之適當難度設定與區塊鏈去中心化功能。

拾、參考資料

[1] 劉承揚，全球科技革命 全球環境及能源之衝擊，http://mail.tku.edu.tw/cyliu/，淡江大學。

[2] 能源的使用對環境的影響， 教育部環保小組發行台師大技職中心。

[3] 駱尚廉，環境與能源 共創「低碳節能、安全永續」的環境，遠東 60 週年白皮書。

[4] 曾羣倫，居家環境之智慧節能控制系統設，東海大學電機工程學系碩士論文，2012 年。

[5] 凌拯民，家用負載之電氣特徵量測及辨識南，台科技大學電機工程系, 2014 年。，

[6] 電能管理與需量控制 Q&A 節能技術手冊，經濟部能源局，2016 年。

[7] 金乃傑，http://www.csie.ntpu.edu.tw/~yschen/course/2012-1/…/ch14.pdf，國立台北大學。

[8] 曹睿華智慧城市物聯網應用從創新到實踐，工研院資通所，2018 年 9 月。

[9] 張志勇，物物相聯的龐大網路—物聯網，534 期科學月刊。
[10] 蔡孟伸，智慧電網應用與節能減碳，國立台北科技大學。
[11] 陳佐民，互動式電力管理系統，實踐大學資訊科技與通訊學系。
[12] Beth Hartman, Bill LeBlanc , “In Pursuit of the Perfect Portal: Smart Meters, Big Data, and Customer Engagemen”, An E Source White Paper, 2015.
[13] 許孟祥，區塊鏈商務應用概論：實例與分析，新陸書局，2018 年 2 月。
[14] 區塊鏈技術演進史，iThome，http://www.ithome.com.tw/news/105370 2016/4/23。
[15] 徐明星，圖解區塊鏈，碁峰出版社，2017 年 8 月。
[16] 沈煒翔，全球應用區塊鏈技術建構分散式能源交易之實例與效益探討，工研院綠能與環境研究所。
[17] Transactive Grid:Blockchain Technology Powers Microgrid In Brooklyn, Blockchain News,2016/7/15.
[18] Blockchain holds key to reinventing energy grid,The Huffington Post,2016/7/29.
[19] 電力模組 LT-114，https://world.taobao.com.
[20] 傳輸模組 YL-100T，https://world.taobao.com.
[21] 樹莓派(RaspberryPi)官網，https://www.raspberrypi.org/。
[22] 江志良，打造 IoT 與嵌入式系統，碁峰出版社，2016 年 12 月。
[23] 鄧文淵 , Python 零基礎入門班，碁峰出版社，2018 年 7 月。
[24] 施威銘研究室，最新 PHP+MySQL+Ajax 網頁程式設計旗標，2014 年 5 月。
[25] 賴屹民，Flask 網頁開發 第二版,，2018 年 7 月。
[26] 陳惠貞，一步到位！RWD 網頁程式設計：用 HTML5、CSS3、Bootstrap 打造響應式網頁，旗標 出版社，2017 年 12 月。
[27] 王毅丞，實戰區塊鏈技術：加密貨幣與密碼學，碁峰出版社，2018 年 5 月。
[28] A Practical Introduction to Blockchain with Python,http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python.
[29] 黃明祥，資訊安全與網路安全概論，東華出版社，2016 年 7 月。

附錄 1 每一種級數 50 次的流水號關係表

工作難度		1	2	3	4	5
流水號	POW_1	8	18	43411	43411	171521
	POW_2	1	142	37238	37238	92789
	POW_3	1	55	104297	104297	33
	POW_4	1	353	27737	27737	28530
	POW_5	12	44	88747	88747	414849
	POW_6	14	748	22522	22522	589
	POW_7	38	137	19764	85615	42
	POW_8	22	374	476	1516	51662
	POW_9	47	55	3983	6151	48315
	POW_10	66	621	4775	15651	27737
	POW_11	52	431	6265	4568	3515
	POW_12	1	424	5165	21551	5464
	POW_13	10	311	1561	16515	11632
	POW_14	8	521	8444	3515	45151
	POW_15	12	464	2131	51165	15111
	POW_16	5	542	8446	358	23165
	POW_17	12	314	5116	6264	15165
	POW_18	71	44	525	5464	6516
	POW_19	121	55	252	12313	51231
	POW_20	13	161	5165	11516	6511
	POW_21	12	185	3736	15151	5151
	POW_22	12	49	8447	548	51242
	POW_23	18	154	2352	451	4516
	POW_24	21	245	845	5151	8602
	POW_25	14	247	6521	56165	15156
	POW_26	15	626	3871	516	15616
	POW_27	22	483	2387	111	5821
	POW_28	35	151	5615	5613	4987
	POW_29	48	626	12155	11632	5623

	POW_30	5	489	1553	1612	9456
	POW_31	1	542	7844	4382	4644
	POW_32	9	12	3546	1515	4884
	POW_33	5	28	8465	15156	44654
	POW_34	5	32	1534	58920	8956
	POW_35	5	5	6131	4283	16561
	POW_36	121	60	5115	15163	45151
	POW_37	64	41	595	235131	6511
	POW_38	4	38	1516	1131	51242
	POW_39	8	36	2113	51623	5623
	POW_40	27	53	1565	46651	8956
	POW_41	38	12	4846	48467	3515
	POW_42	55	15	5162	95955	15165
	POW_43	61	482	5161	5454	15156
	POW_44	40	151	9815	15556	4644
	POW_45	25	62	6468	51445	16561
	POW_46	1	57	4467	4645	516
	POW_47	6	37	8652	13131	15156
	POW_48	72	31	5584	15623	51623
	POW_49	13	48	1513	51531	51531
	POW_50	51	12	6116	59807	4832
	平均	26.56	216.46	10794.2	29172.66	30431.58

【評語】052303

本作品配合環保議題之智慧用電能系統，利用樹莓派進行區塊鏈結合物聯網(IOT)電能遠端量測以達到自製機電系統製作原型中電能資料安全性、電能交易與節能等功能，作品已具有初步「具有區塊鏈之 IOT 用電系統」的雛形。該作品探討物聯網、區塊鏈、以及電能的傳送和交易所需相關工程技術相當完整，對於節能環保的觀念，在系統規劃上相當詳盡，面對的技術或實務問題，亦能提出適切的工程解決方案，具有創意性，實在值得鼓勵。由於電網電力的分配與調度屬國家戰略資源，對於如何將作品的技術擴大推廣，建議和相關單位了解，進而在質化與量化的效益上，評估此作品的技術在各個應用層面的實用性。

作品海報

壹、研究動機

人類的大量開發與使用能源，造成環境污染與能源枯竭問題，因此智慧化電能管理系統成為解決方案之一，而政府也修正電業法來嘗試解決上述問題，讓國人也能參與發電與售電，可信任的交易平台成為重點之一，因此研究針對了智慧化電能管理系統與可信任的交易平台兩項技術融合進行研究。

貳、研究目的

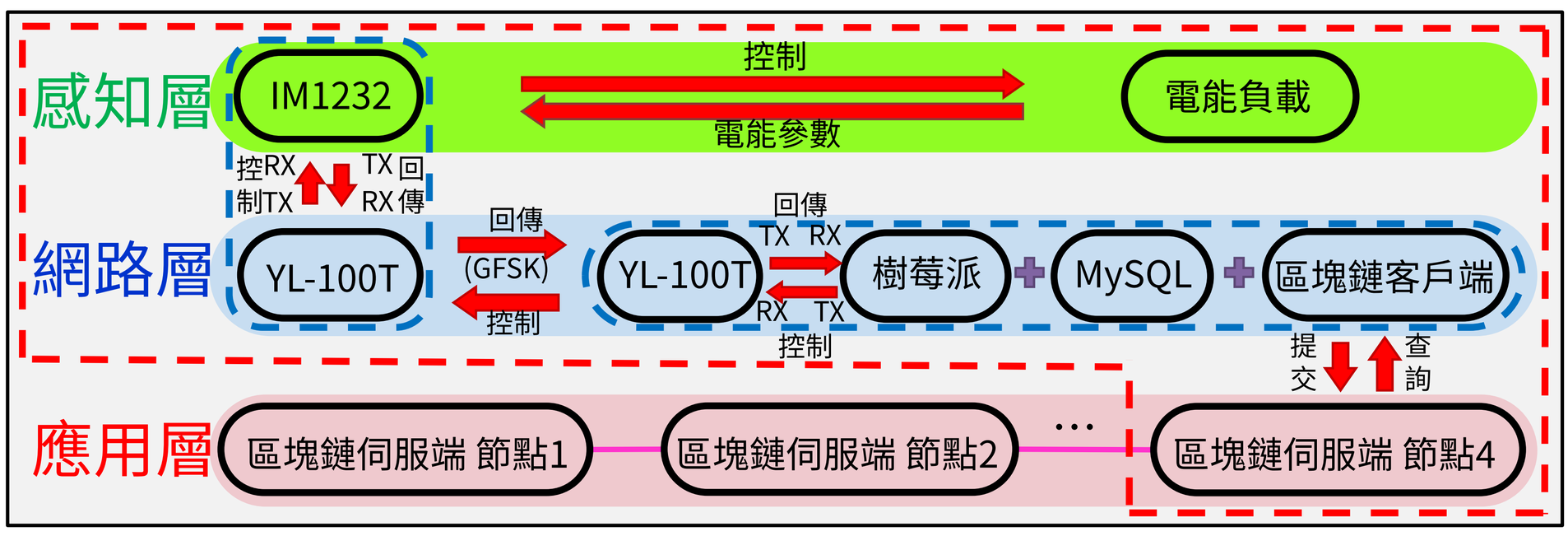
一、設計負載遠端監控之功能，進行電能量測、計算與建立電能資料庫，以達到智慧化電能管理系統。
二、保護電能資料、電能交易與電能帳單的區塊鏈交易平台，以建立自動化、穩定運作、可擴充性之系統。
三、融合上述兩者，讓整體運作降低電費、調配電能負載與整體節能，並發展匿名開放性電能資料庫。

參、原理與實驗規劃

一、原理

(一).電能物聯網技術

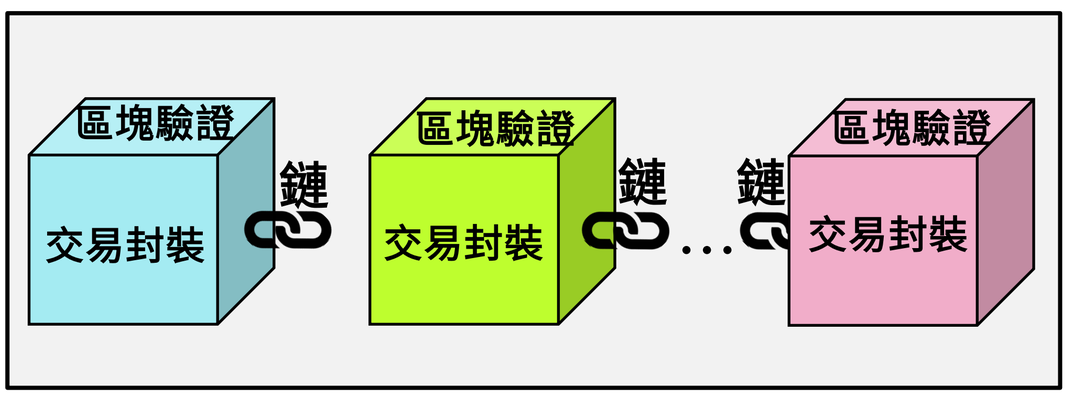
經由網際網路將所有電能感知器、網路傳輸器與應用端伺服器連結在一起形成三大架構如下：
1.感知層：利用電能擷取模組感知電能負載信號，並採取輪詢(Polling)方式收集多重負載。
2.網路層：以無線傳輸模組做為電能資料網路傳輸，並予以計算與建立電能資料庫。
3.應用層：將電能資料、帳單與交易傳送至礦池後，伺服器做工作量證明驗證與建立區塊鏈。



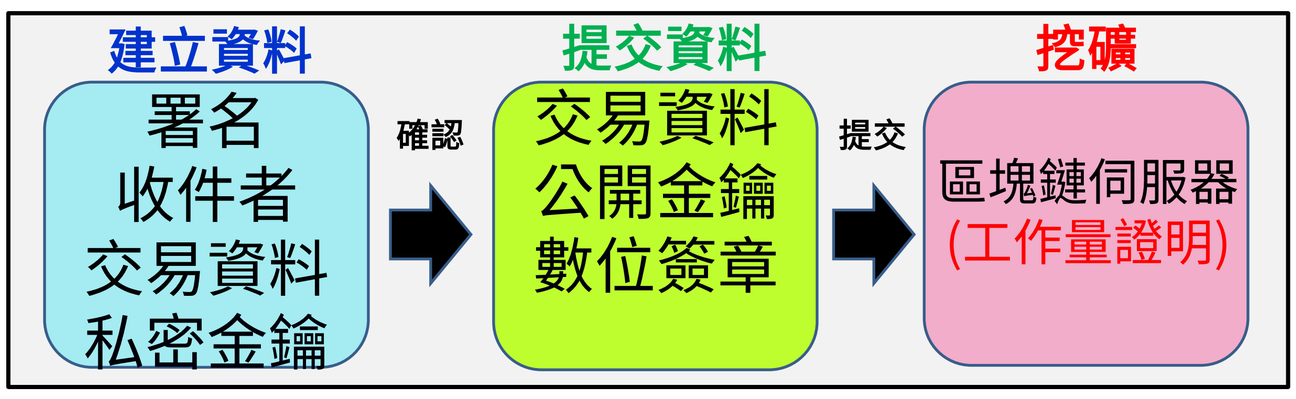
具有區塊鏈之IoT用電系統架構與物聯網之關聯圖

(二).電能區塊鏈技術

經由雜湊值使前後「區塊」(Block)間產生「鏈」(Chain)關係，串聯形成「區塊鏈」(Blockchain)。



區塊鏈架構圖



提交交易流程圖

1.提交交易

使用者將「交易資料」執行「提交交易」製成「區塊」的流程如下:
(1).建立資料：建立欲上鏈的交易資料，如電能資料類型、電能交易類型或電能帳單類型。
(2).提交資料：提交至礦池的交易封裝，若交易封裝內交易資料為電能交易類型則需確認剩餘電能值。
(3).挖礦：經由工作量證明產生雜湊值將前後區塊成鏈。

2.挖礦

區塊經由「工作量證明」(PoW,Proof of Work)產生驗證區塊與雜湊值並與前區塊形成區塊鏈，工作量證明工作如下：
(1).交易封裝之雜湊值(Hash)猜測。
(2).流水號(Nonce)為計算挖礦次數與速度。
(3).猜測雜湊值滿足目標雜湊值時完成驗證。
(4).目標雜湊值之工作難度為高位元組0數值。
(5).記錄礦工與挖礦獎勵額度。

工作難度表

工作難度	位元數	獎勵額度
1	1	2
2	2	4
3	3	6
4	4	8
5	5	10

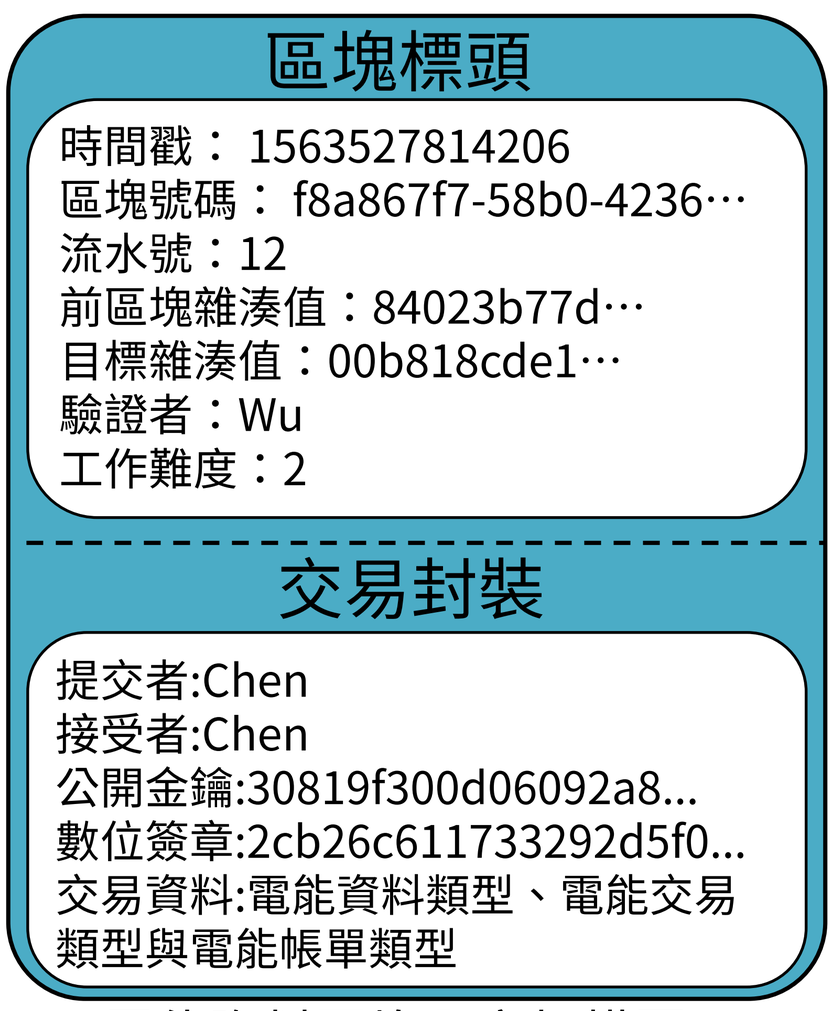
二、研究規劃

(一).系統架構

1.感知層：電力模組(IM1232)收集電能負載的電能資料。
2.網路層：傳輸模組(YL-100T)收集電力模組的電能資料，並存入樹莓派伺服器(Raspberry Pi)，製作交易資料後進行提交 。
3.應用層：接受提交後，經挖礦儲存至區塊鏈伺服器。

(二).區塊鏈(Blockchain)

1.區塊資料：由「區塊標頭」與「交易封裝」組成。
(1).區塊標頭：時間戳、區塊號碼、流水號、前區塊雜湊值、目標雜湊值、驗證者、工作難度等。
(2).交易封裝：提交資料、交易資料。
a.提交資料:提交者、接受者、公開金鑰與數位簽章。
b.交易資料:依照需求輸入所需要的資料，有電能資料類型、電能交易類型與電能帳單類型。



電能資料區塊內容架構圖

2.交易提交

(1).建立資料

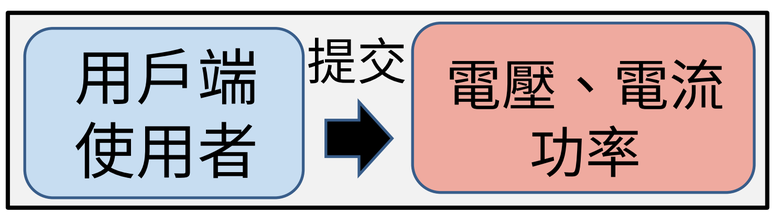
a.私密金鑰函數如式(1)代入亂數產生私密金鑰。
b.公開金鑰如式(2)代入私密金鑰產生公開金鑰。
c.雜湊函數如式(3)代入交易資料產生交易資料雜湊值。
d.數位簽章函數如式(4)代入私密金鑰與交易資料雜湊值產生數位簽章。

$$private\_key = f_r(random) \quad (1)$$
$$public\_key = f_{RSA}(private\_key) \quad (2)$$

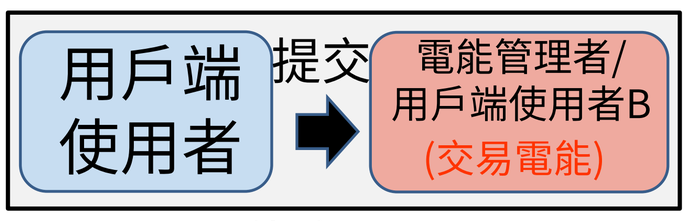
$$Hash = SHA(Data) \quad (3)$$
$$Signature = Sig(private\_key, Hash) \quad (4)$$

(2).提交資料

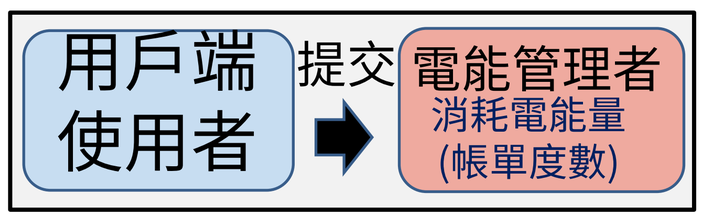
a.交易資料、公開金鑰與數位簽章會產生交易封裝提交於礦池。
b.交易資料分成三類型：
(a).電能資料類型：紀錄開放性電能資料，詳知電能系統狀況，異常時可請求賠償。
(b).電能帳單類型：彙整每月份交易紀錄，經由每個提交者自行產生。
(c).電能交易類型：讓電能可進行買賣功能，其中會有提交者、接受者與驗證者(礦工)。



電能資料圖



電能交易圖



電能帳單圖

(3).挖礦

a.接收交易封裝，並解析出交易資料、公開金鑰與數位簽章，以雜湊函數如式(5)將代入交易資料產生猜測雜湊值。
b.驗證交易資料函數如式(6)代入公開金鑰、交易資料雜湊值與數位簽章驗證交易資料。
c.工作量證明函數如式(7)代入交易資料、前區塊雜湊值與流水號以滿足目標雜湊值。
d.計算累計電能交易，也就是帳單之功能如式(8)所示 。

$$Hash = SHA(Data) \quad (5)$$
$$Verifier = fver(public\_key, Hash, signature) \quad (6)$$

$$PoW = PoW(Data, Previous\_Hash, Nonce)$$
$$Difficulty = work\_difficulty$$
$$Guess\_Hash = PoW\ satisfy\ Difficulty \quad (7)$$

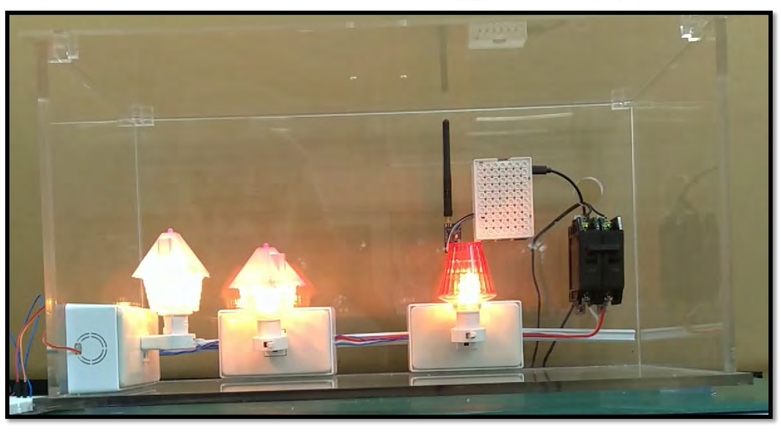
(a).電能交易累積計算

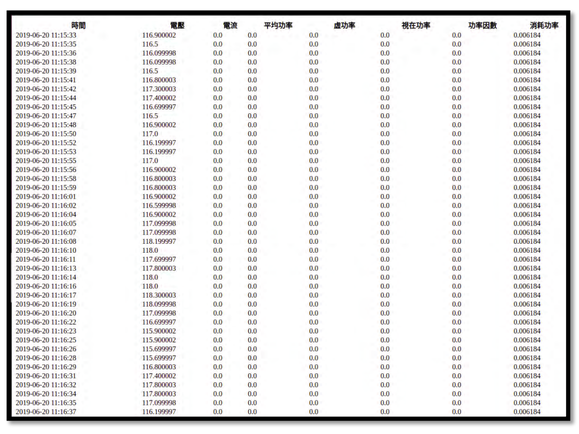
將每個月所有的電能交易做累計計算，產生電能交易列表與總結電能的電能帳單，其公式如(8)所示。

$$契約容量 + 產生電能 + 得到電能 - 消耗電能 - 交易電能 - 手續費 + 獎勵 = 剩餘電能 \quad (8)$$

肆、實驗過程與結果

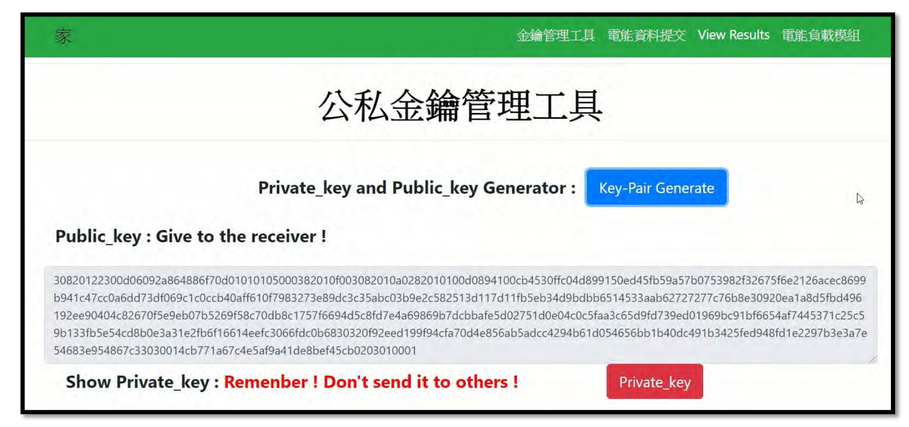
依據上述規劃，我們完成以下實驗過程，並且得出以下實驗過程與結果，經由以下15個步驟完成本系統，並進行討論。


步驟1、實驗設備完成

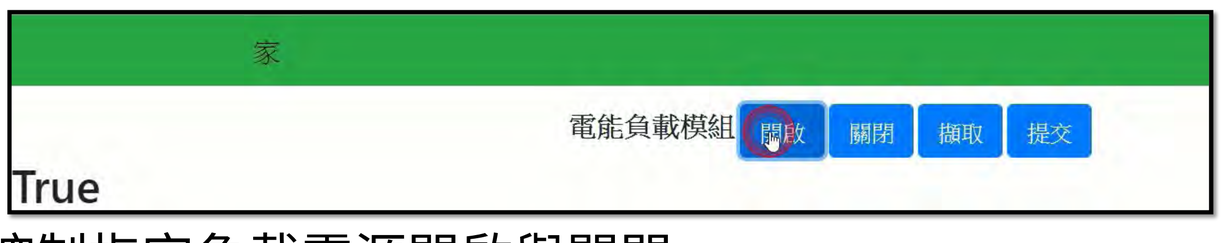


時間	電壓	電流	平均功率	虛功率	視在功率	功率因數	消耗功率
2019-06-20 11:15:33	116.900002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:35	116.5	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:36	116.099998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:38	116.099998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:39	116.5	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:41	116.800003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:42	117.300003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:44	117.400002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:45	116.699997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:47	116.5	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:48	116.900002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:50	117.0	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:52	116.199997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:53	116.199997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:55	117.0	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:56	116.900002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:58	116.800003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:15:59	116.800003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:01	116.900002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:02	116.599998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:04	116.900002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:05	117.099998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:07	117.099998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:08	118.199997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:10	118.0	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:11	117.699997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:13	117.800003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:14	118.0	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:16	118.0	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:17	118.300003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:19	118.099998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:20	117.099998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:22	116.699997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:23	115.900002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:25	115.900002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:26	115.699997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:28	115.699997	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:29	116.800003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:31	117.400002	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:32	117.800003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:34	117.800003	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:35	117.099998	0.0	0.0	0.0	0.0	0.0	0.006184
2019-06-20 11:16:37	116.199997	0.0	0.0	0.0	0.0	0.0	0.006184

步驟2、收集電能資料



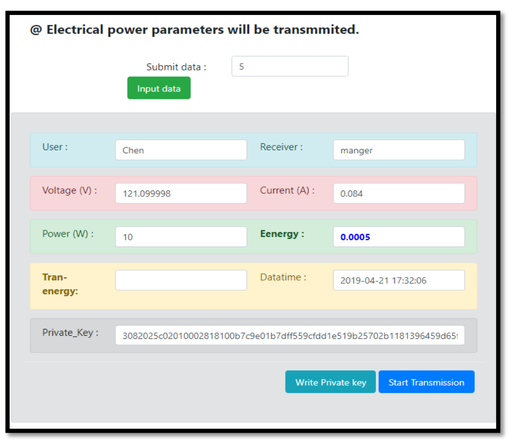
步驟3、產生私密金鑰與公開金鑰

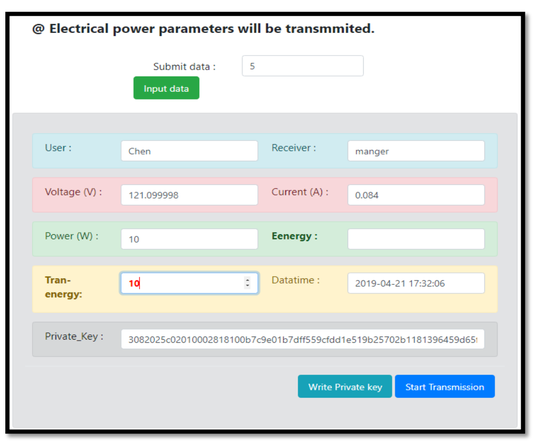


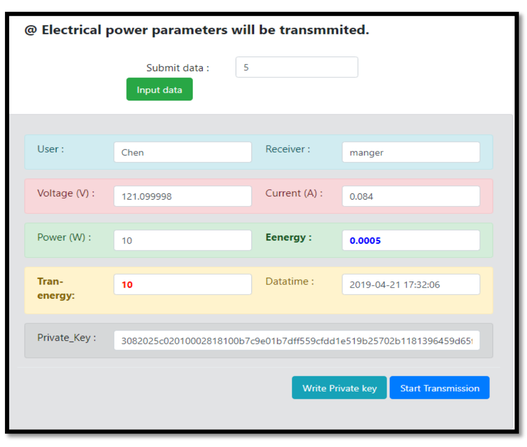
步驟4、電能負載模組控制指定負載電源開啟與關閉

步驟5、電能資料擷取

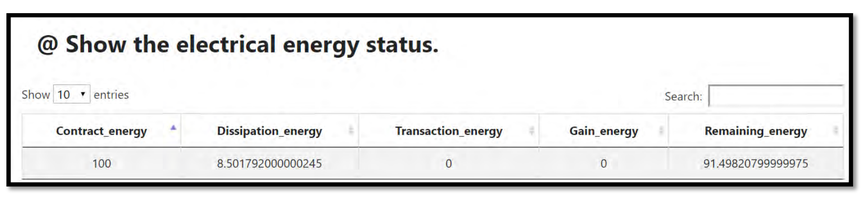
步驟6、電能資料提交交易







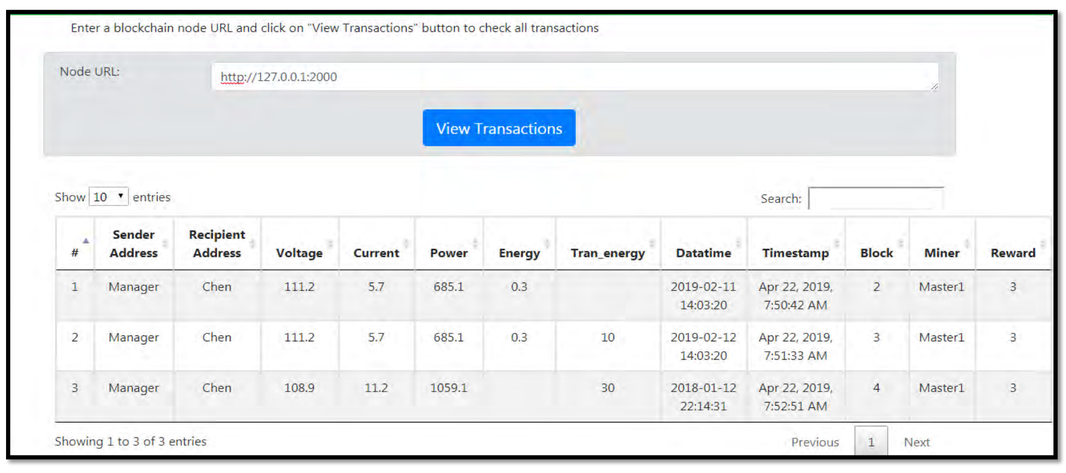
步驟7、 輸入帳單資料 步驟8、 輸入交易資料 步驟9、 輸入帳單與交易資料 步驟10、 交易提交與數位簽章



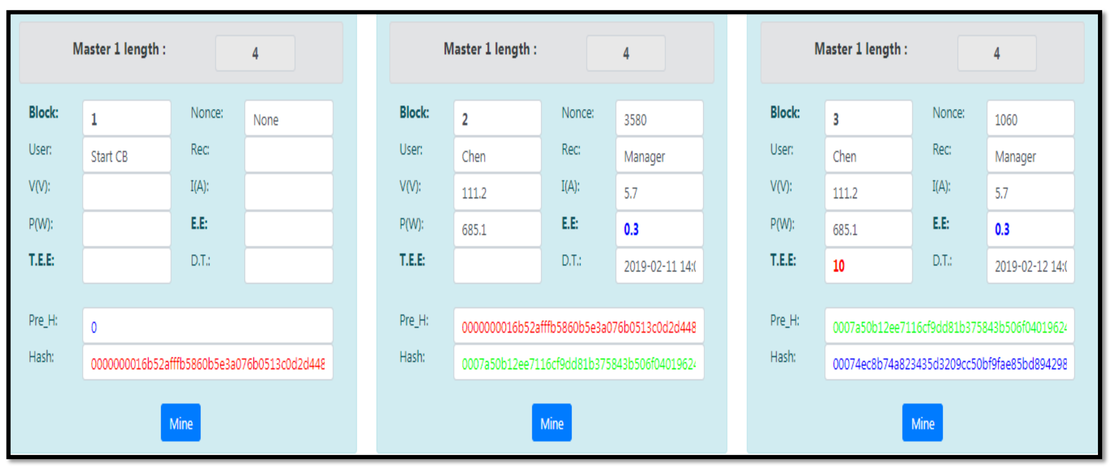
步驟11、顯示電能狀態

步驟12 、手動更新礦池

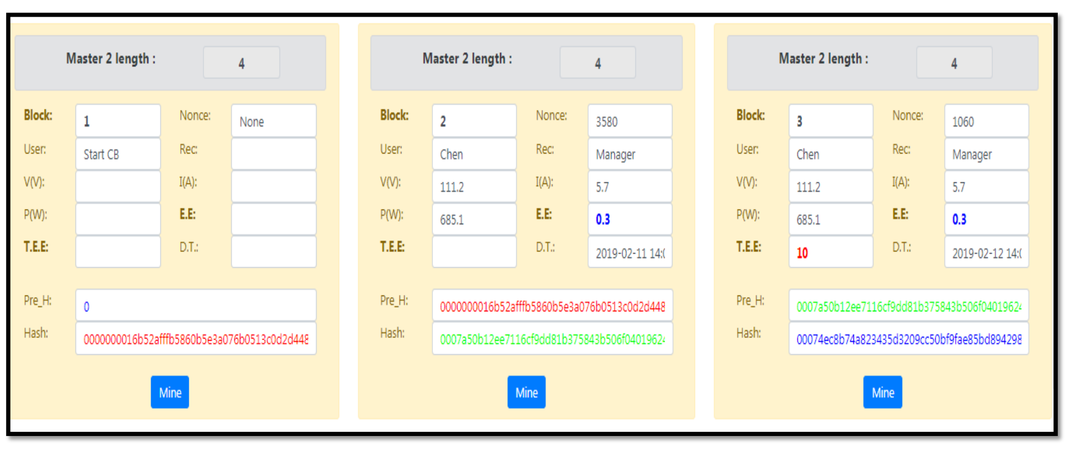
步驟13、手動執行挖礦



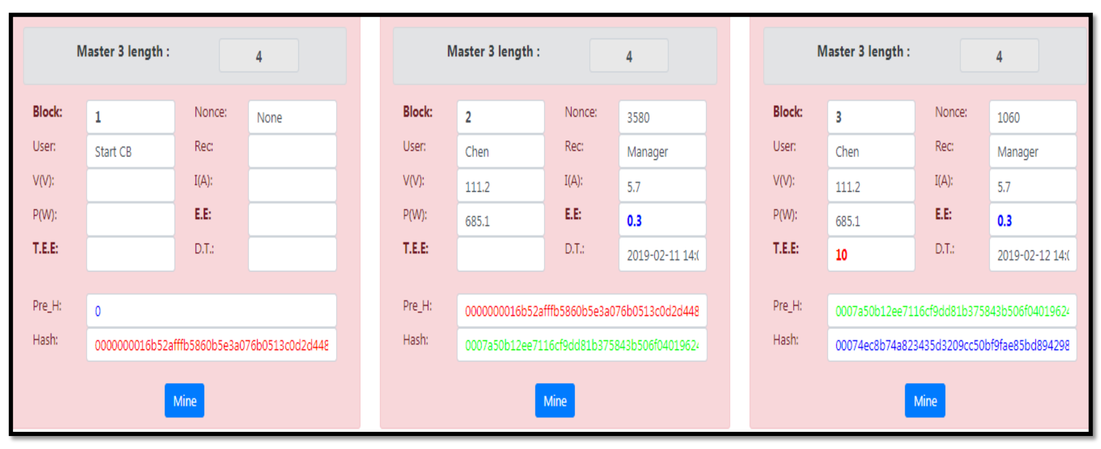
步驟14、查詢區塊鏈紀錄



步驟15.a、伺服端1區塊鏈



步驟15.b、伺服端2區塊鏈



步驟15.c、伺服端3區塊鏈

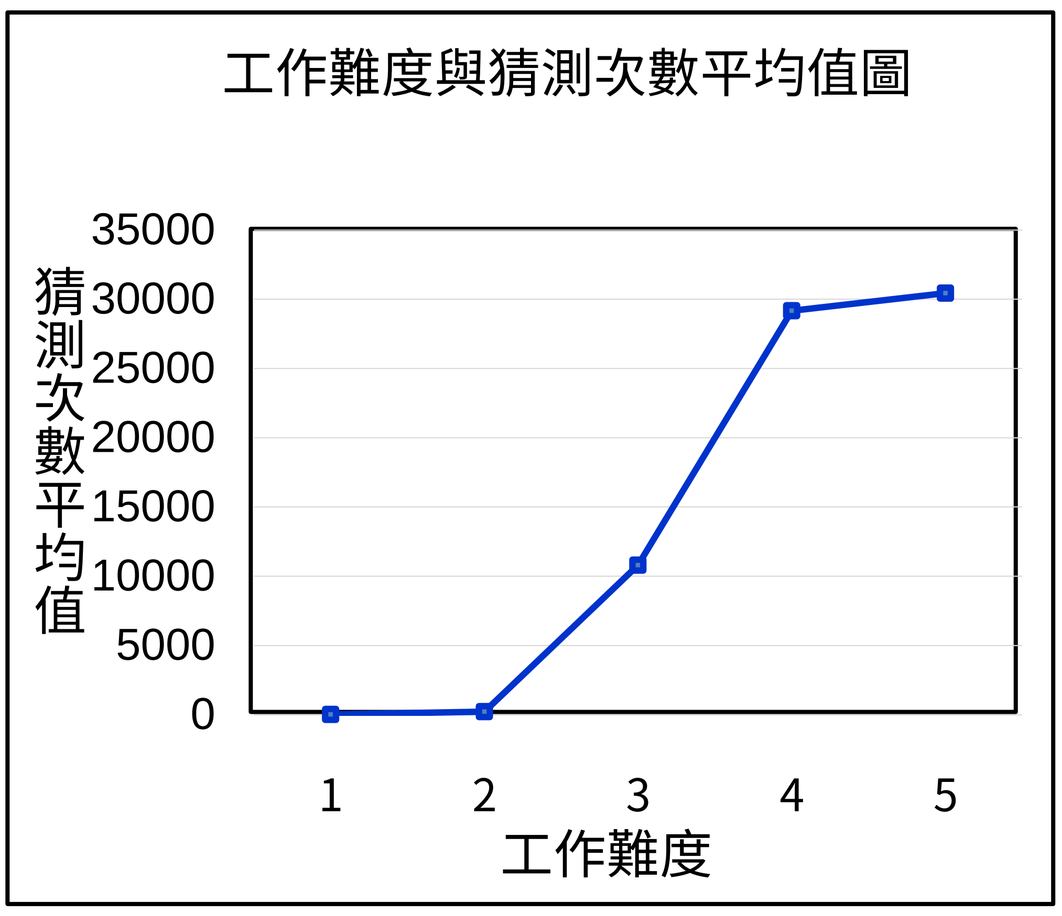
伍、問題與討論

問題一：安全性與區塊製作速度之矛盾性。

討論：增加工作難度的難度可以增加區塊與區塊鏈的安全性，但在實驗的過程中發現到增加難度會讓樹莓派超出能承擔的運算量，因此針對每次提交交易的產生出來的流水號進行研究，發現增加難度會讓計算工作量證明所計算的次數增加，因此在工作證明這方面在運算能力較強的電腦中是可以，但在物聯網方面會受處理器的計算能力而無法快速運作。

工作難度與猜測次數平均值對應表

實驗次數/工作難度	1	2	3	4	5
第一次	8	18	43411	43411	171521
第二次	1	142	37238	37238	92789
第三次	1	55	104297	104297	33
第四次	1	353	27737	27737	28530
第五次	12	44	88747	88747	414849
第六次	14	748	22522	22522	589
第七次	38	137	19764	85615	42
第八次	22	374	476	1516	51662
第九次	47	55	3983	6151	48315
第十次	66	621	4775	15651	27737
平均值	21	254.7	35295	43288.5	83606.7



工作難度與猜測次數平均值圖

問題二：傳播者模式下使用簡單方法達成共識遇到的問題。

討論：在兩個節點之間達成共識的條件下必須確認兩個節點的礦池已經無交易封裝的情形下同步，否則會出現雙重支付問題(Double Spending)，未來會加入確認礦池與區塊鏈中是否有相同的交易封裝。

問題三：具有區塊鏈之IOT用電系統如何在未來達到研究目的的目標。

討論：由於目前還在實驗階段，許多部份還未完成，會先針對電能資料轉換電能交易自動化、週期內自動產生電能帳單與去中心化等項目進行研究，讓我們可以朝著前進開源節流目標前進。

陸、結論

一、系統功能

以Python、Flask與網頁設計等製作具有區塊鏈之IoT用電系統，功能如下：

(一).感知層與網路層設計具有遠端監控、遠端量測與建立電能資料庫，設計出智慧化電能管理系統。

(二).應用層設計可以保護各節點產生的電能資料、電能交易與電能帳單之區塊鏈交易平台。

(三).融合物聯網技術與區塊鏈技術，完成電能資料提交交易自動化、驗證者挖礦自動化與解決兩個節點之間區塊鏈不一致問題，並發展匿名的開放性電能資料庫，完成具有區塊鏈之IOT用電系統。

二、未來展望

此系統在未來的發展與對人類的貢獻：

(一).持續更新系統各類核心模組，使系統擁有自動化、穩定運作、可擴充性。

(二).改進目前的「共識演算法」(Consensus Algorithm)，讓系統在去中心化、安全性與擴展性皆達到。

(三).未來系統增加分散式儲能設備分擔電網供電容量，達到削峰填谷的用電系統。

(四).增加參與者的運作，讓整體運作降低電費、調配電能負載與整體節能。

柒、參考文獻

[1]Beth Hartman, Bill LeBlanc ,“In Pursuit of the Perfect Portal: Smart Meters ,Big Data, and Customer Engagemen”, An E Source White Paper, 2015.

[2] Blockchain holds key to reinventing energy grid,The Huffington Post,2016/7/29.

[3] A Practical Introduction to Blockchain with Python, http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python.

[4] Transactive Grid:Blockchain Technology Powers Microgrid In Brooklyn, Blockchain News, 2016/7/15.