二、研究計畫內容（以10頁為限）：

1. 摘要

目前流行病控管方式主要對象是高風險族群，例如:年紀、旅遊史…等方式去控管。但當管控對象是需要自主隔離或者居家檢疫時，如何有效讓管控對象確實依照疾管單位要求回報健康數據是個非常重要的問題。尤其部分人因為害怕而刻意隱匿疫情不通報，導致疫情的後續控制增添許多未知的變數，同時也可能導致其他原本未受感染威脅的人因此受到影響，讓流行病疫情更無法掌握。

自主隔離是以自身住宅進行隔離，並且有相關人員會以電話方式去做訪問，詢問該名可能感染者的健康狀況。本計畫將使用區塊鏈(Block Chain)以及智慧合約(Smart Contract)的方式，在藉由IOT的方式將病人的體溫、心跳、血壓等…，並且即時的將這些資料上傳至區塊鏈，讓這些資料無法被竄改。並且依靠手機APP，能夠即時通知該隔離者，定時定期去做健康資訊的上傳，並且不定時將其位置資訊上傳，以達成自主隔離的健康資訊控管，並且可以減少人力資源的使用。

1. 研究動機與研究問題

隨著交通科技的進步，人類流動的速度越來越快。從城與城之間，到國與國之間，人口遷移的速度與過去差上好幾倍。但也造成了疾病傳播速度過快的問題。當有一位具有感染力的四處旅遊，這位病人所接觸過的人，都有可能成為下一個感染者，並且在繼續傳染。如此一來，疾病擴散會非常的迅速。對此需要更多醫療上的資源，但如果能夠建立一套系統，能夠使未確診的高風險族群確實做好自我篩檢並且隔離。如此一來對人力精簡會有不少的壓力。一般來說，傳染病是由病原體依附著傳染源，再由傳播途徑去感染宿主。其中部分傳染病的傳染源是人類，經由空氣、飛沫、接觸等方式去感染下一個宿主。這導致在人口密集的城市，或是交通樞紐等地區，都可能大規模的傳染。此時有該疾病的各項特徵，或是曾與宿主有接觸者，皆被認為疑似個案，需要作後續追蹤。

近年來，智慧醫療是新的趨勢。使用人工智慧以及物聯網方式，將檢測裝置中所檢測的資料上傳。一方面可以將病歷上傳至雲端，供其他醫護人員去做檢調，另一方面使用人工智慧去診斷，可大幅度減省人力需求也可有效改善手工謄寫麻煩。再者，從IOT設備取得資料經過多手謄寫過程很有可能有錯誤，更有可能故意篡改資料內容，因此，透過IOT設備結合區塊鏈的機制讓資料一旦收集後即被簽署進區塊鏈的賬本中定能更精確掌握資訊的正確性。在建立區塊鏈結構中區塊標頭(表一)時，需先找出Nonce。由於不可得知輸入的值進行雜湊後結果為何，所以只能依靠暴力破解法去找出Nonce。這是十分大量的運算過程，通常要嘗試數十億至數兆個，直到找出Nonce為止，到此即被簽署至區塊鏈中的區塊。然而若要修改某區塊，須再找出Nonce，且因區塊中含有父區塊的雜湊值，所以若更改某個區塊的值，也必須將高度高於修改區塊的所有子區塊的Previous Block Hash。在區塊鏈的環境下隨時都有可能加入新的區塊，而且每個合法區塊的簽署都必須經過半數以上節點的認同，因此區塊內容被篡改的可能性極低。在乙太坊中有提供智慧合約(smart contract)的功能，可供使用者自行撰寫且可在私有網路下進行挖礦及測試。在實務應用上有如群眾募資、電子商務、抽獎等…。其中一項則是控制IOT的開關。

表一:區塊標頭結構

|  |  |
| --- | --- |
| 欄位 | 說明 |
| Version | 軟體/協定版本資訊 |
| Previous Block Hash | 父區塊的雜湊值 |
| Markle Root | 默克樹(Markle Tree)的跟雜湊值(Root Hash) |
| Timestamp | 區塊產出時間(Unixtime) |
| Difficulty Target | 區塊產出時的PoW難度，雜湊值需小於它 |
| Nonce | 計算雜湊使用的值 |

本計畫主要研究使用具備IOT功能的健康管理設備，例如耳溫槍、智慧手環等，利用該裝置在取得使用者的健康資訊後即時上傳至區塊鏈上，透過區塊鏈做資料控管，可以確保上傳後的資料無法被有心人士惡意竄改或人工繕謄造成的錯誤。另一方面可藉由設備所上的資料，再利用智能合約的判斷及早提供警示資訊給相關主管單位，進一步評估該使用者健康狀況，給予使用者適當的醫療照護作為。本計畫將不涉及醫療相關內容，僅就相關技術之建置與模擬進行研究。

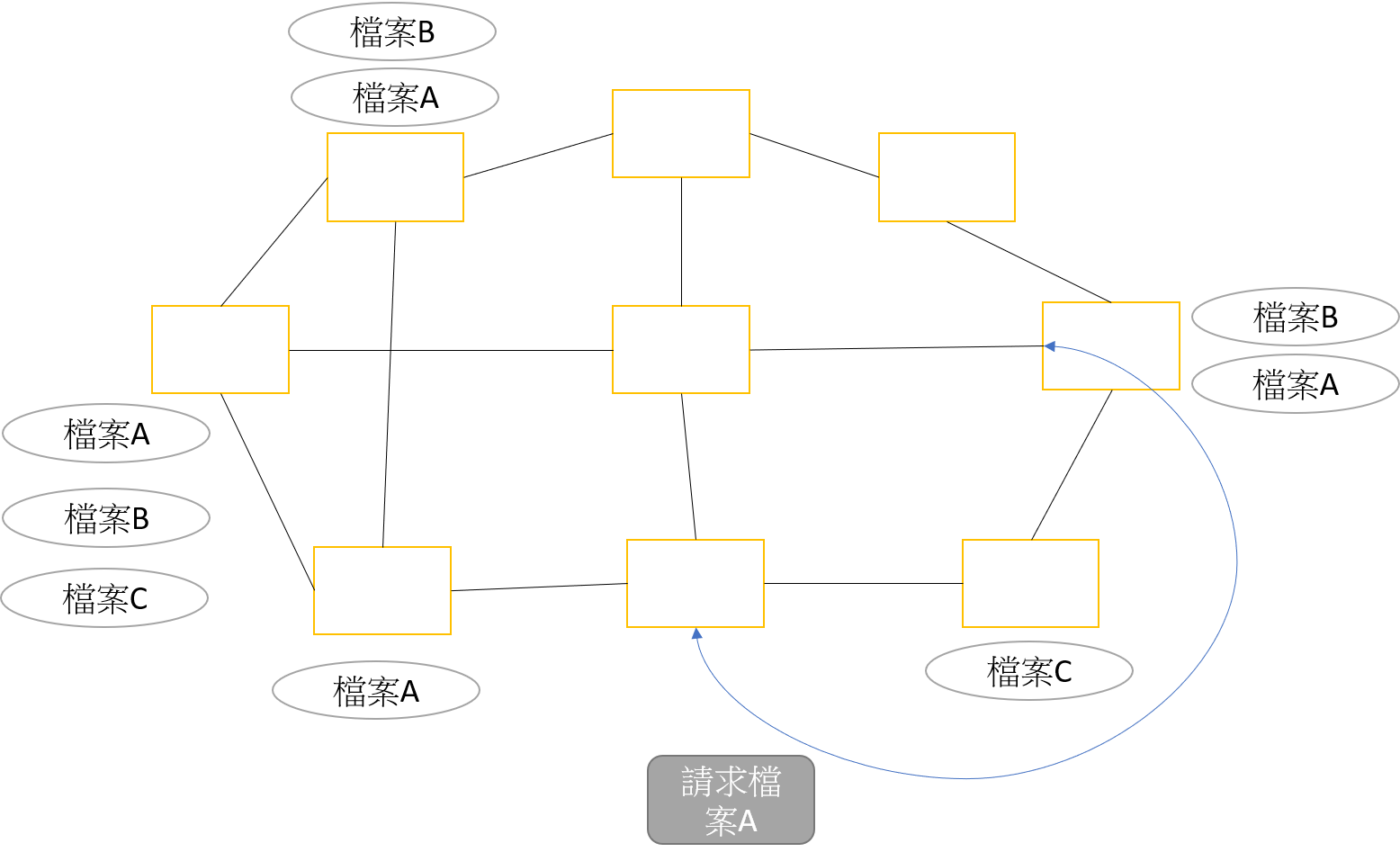
1. 文獻回顧與探討

* **區塊鏈(Block Chain)**

區塊鏈構成要素為P2P、區塊鏈網路參與者、交易、區塊、分散式帳本以及挖礦所組成。

1. P2P(peer to peer)

一種去中心化的網路技術，在其技術下，檔案將會存放至多個節點上(圖一)



圖一: P2P示意圖

架構下所有設備皆為對等，也被稱為對等式網路。在P2P的所有端點同時為請求檔案的客戶端，也是回傳檔案的伺服器端。

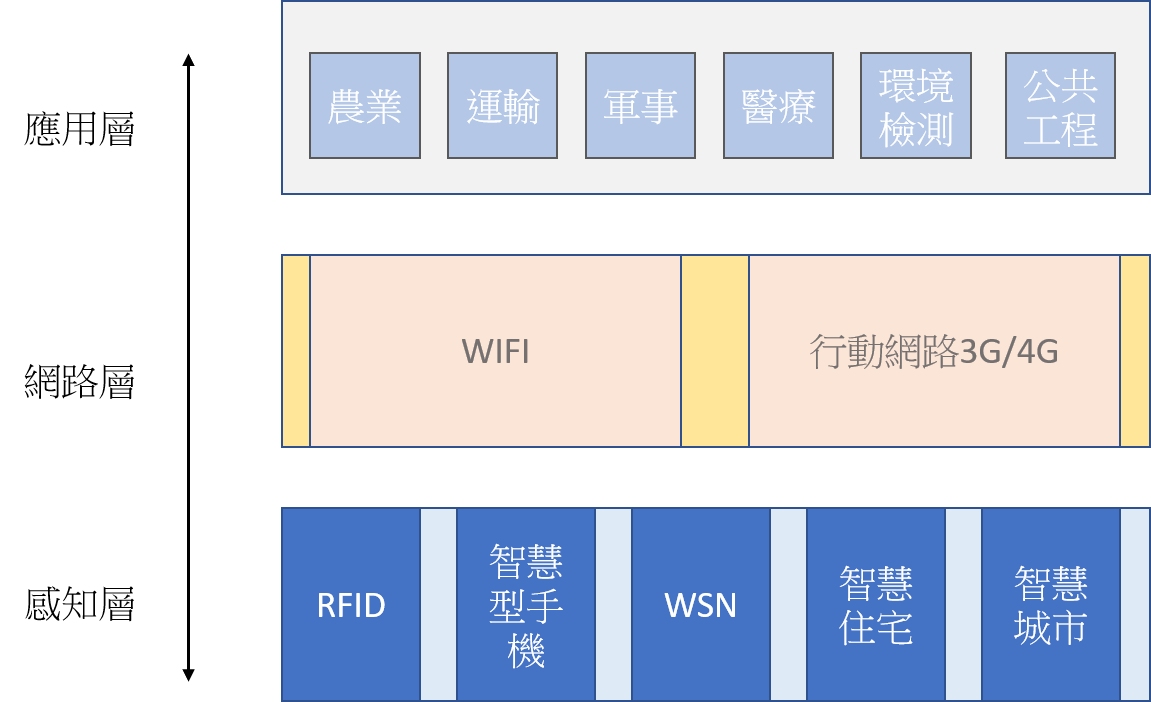
* 區塊鏈網路參與者

以比特幣為例子，分為使用者與礦工

使用者:進行比特幣交易。本計畫為進行監測健康狀況的IOT設備。

礦工:進行大量數學運算，搶先產出區塊者，可獲得比特幣為報酬。

* 交易:進行比特幣匯款時所發出的命令， 其中包含了匯款者，收款者、金額等資訊。
* 區塊:儲存多筆的交易，並在比特幣網路中流通。
* 分散式帳本:一種不具備中心的資料庫，在區塊鏈下，所有的區塊會儲存在節點中的帳本(資料庫)。在同個網路下，所有節點的帳本都是一模一樣的，所以就算有個節點故障，也可以依靠其他節點的資料進行交易。
* 挖礦:產出區塊的行為即為挖礦，若成功挖礦則可以獲得比特幣，而能夠獲得比特幣的人只有成功產出區塊的那一位，所以礦工之間競爭產出區塊。產出區塊需要大量的運算能力，所以在社會上中是不乏聽說有惡意軟體會偷偷進行挖礦。
* **物聯網(IOT)**:Kevin Ashton 在1998首次提出，並在近幾年備受關注。其中架構為感知層、網路層、應用層，感知層為感測器，網路層為WIFI、或3G、4G有線網路，應用層則是以感測裝置連接網路，形成一套系統並對各行業進行應用。

****

圖二: IOT示意圖[1]

結合上述物聯網所開發的硬體設備，改善了舊時檢查只能定點測量，現今部

分身體健康檢查並不受限於地點，能夠隨時隨地的進行。

表二[2]:生理資訊量測裝置類型

|  |  |  |  |
| --- | --- | --- | --- |
| 類型 | 體內植入式 | 體外配戴式 | 體外量測式 |
| 裝置 | 植入式心電量測器 | 體液量測器  平衡量測器  體溫量測器 | 傳統血壓計  耳溫槍 |

生理感測網路由感測器、匝道器、以及生理資料庫。感測器是負責偵測生理資訊，如上表所示。匝道器則為具有通訊功能的裝置，如智慧型手機，將感測器中所取得資料透廣網路上傳至生理資料庫。生理資料庫則是記錄個人生理資料，將有效資料篩選出來。

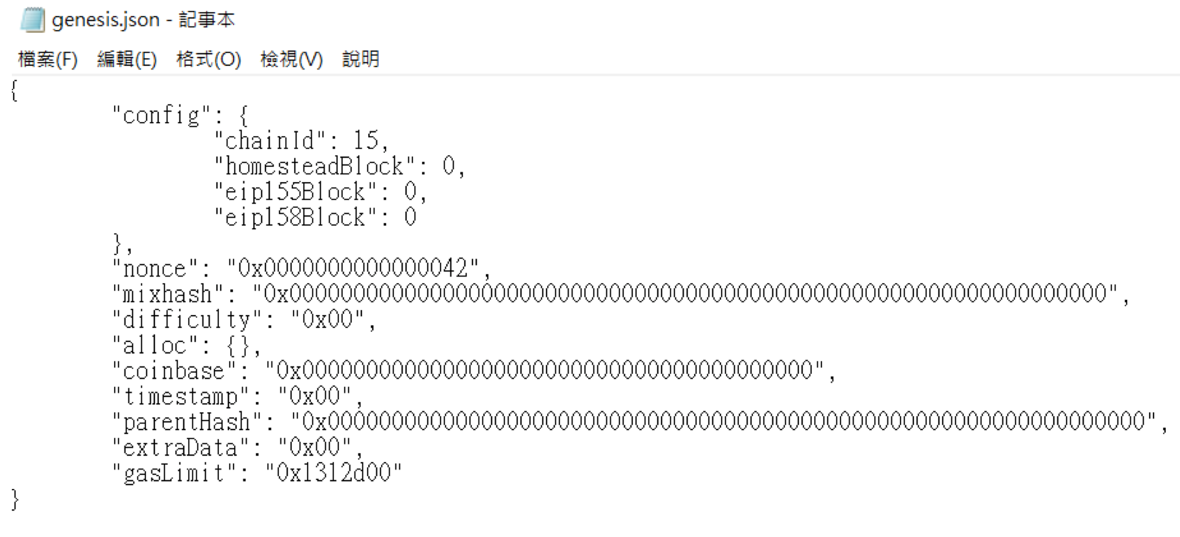
1. 研究方法及步驟

為了能夠使研究環境能夠順利進行，需要事前準備

1. **智慧合約撰寫**: 首先要先知道如何寫出一個能夠進行物聯網的一套合約，並且針對各種可能去做設定參數，並且能夠達到監測數據傳遞的正確性。
2. **設備準備**: 完成了基本的合約設定後，需要有能夠使用的設備，例如耳溫槍。當人體溫度超過標準時，基本就代表人體的狀況異常，可能是感冒、中暑，甚至是流行性感冒的特徵，對此使用溫度作為判斷標準。
3. **手機APP設計:** 需要進行健康評估以及提醒自我檢測的裝置，由於現在幾乎人人都有手機，能夠使用手機作為傳遞資訊的依據。近期的智慧手環便有可以像手機連線的功能。若將檢測設備與手機連線，在自我檢測時，數據辨識機器所測量而並非由人進行輸入，進而減少測量數值被惡意更改的可能。
4. **資料庫建構:**當用戶完成檢測並且擁有數據後，需要上傳至資料庫，並且交由系統去判斷該數據是否正常，當資料異常時，系統需要發出警示。
5. **實驗**: 當上述皆準備完成後，就會進行實驗的步驟，去實際操作現實中所有狀況的可能性。

基於以上步驟，首先需要熟悉智慧合約的編寫，所使用的是以太坊的Geth進行區塊鏈架構。Geth具備智慧合約的建立、執行，乙太幣的匯款、建立帳戶、挖礦等…功能，並且能夠建立私有鏈，在私有鏈下挖礦可以獲得乙太幣，且相較具有流通性的主網更容易成功挖礦，所以在測試情況都是以自行架構的私網進行。

在建構私網時，需要先建立創始區塊



圖三: 創始區塊內容

以上為創始區塊中所需要的數值，期包含意義如下表:

表三: 創始區塊內容意義[6]

|  |  |
| --- | --- |
| nonce | 用於挖礦的一個64位隨機數 |
| mixhash | 與nonce配合用於挖礦，由父區塊的一部份產生的hash |
| diffculty | 當前區塊難度，設定過大會造成挖礦困難 |
| alloc | 預設帳號以及乙太幣數量，由於在私鏈挖礦較為容易，所以不進行設定。 |
| coinbase | 礦工帳號，可日後設定。 |
| timestamp | 創世區塊的時間戳記 |
| parentHash | 父區塊的hash值，由於是創始區塊，所以設定為0 |
| extraData | 額外訊息 |
| gasLimit | 設定gas的消耗，限制區塊包含交易的總合，設定為最大 |

使用Geth將此json檔進行初始化，就完成了私有鏈架構，完成私有鏈後，即可在command line底下進行創建帳號、挖礦、交易...等功能。

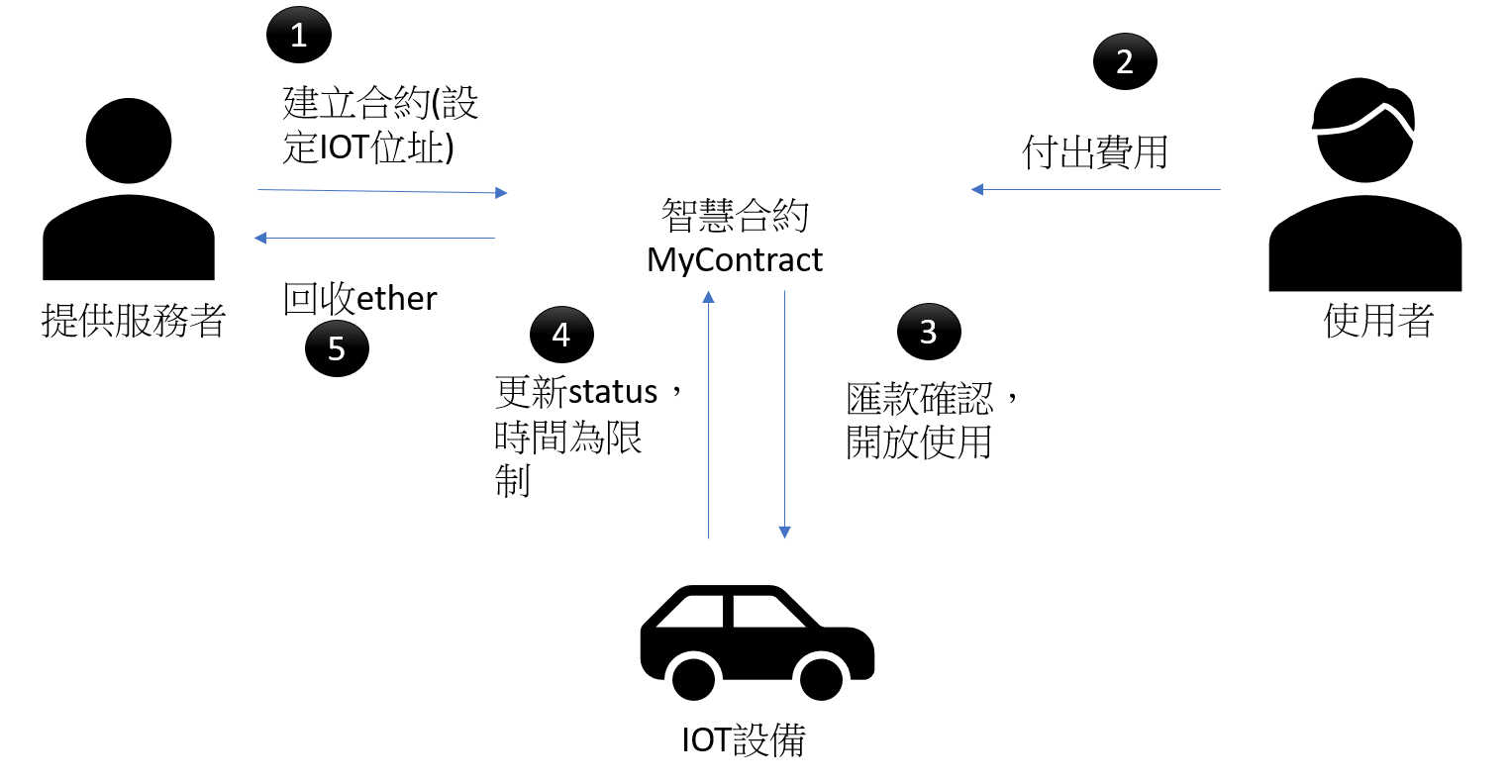
在編寫與運作智慧合約，則使用Mist Wallet，這是以太坊官方所開發的錢包，能夠與私有鏈連線，進行管理帳號、匯款、以及合約發布。

一張含有 螢幕擷取畫面 的圖片

自動產生的描述

圖四: Geth與MistWallet開發環境

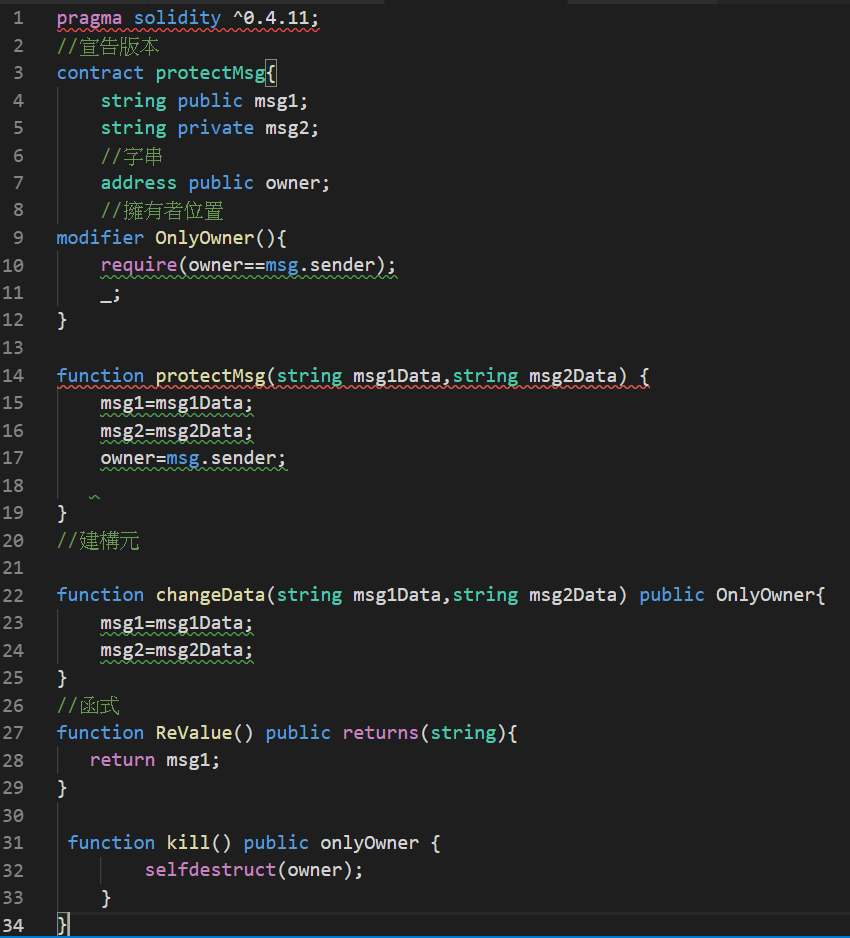
智慧合約是使用Solidity語言，是一種合約導向的語言，可應用於區塊鏈平台上。當合約內容完成後，使用Mist Wallet發布。進行IOT架構時，需要有三方，分別為服務提供者、IOT設備與使用者，如下圖五



圖五: 智慧合約與IOT設備關係示意圖

首先必須由服務提供者進行撰寫合約內容並設定IOT裝置的位址，並且發行置區塊鏈網路上。此時使用者即可使用此合約，在進行合約前先進行扣款，並將款項儲存至合約之中，扣款成功後，即可開放該IOT設備的使用權限。當使用者使用完畢或是使用效期已過，再度更改使用權限。最後，提供服務者即可從合約中獲得使用者所支付的乙太幣。

在智慧合約發行中，可以限定資料傳輸的位址，只有在設定的位址有效時，所做的更動才具備效果，以此可確保資料不被他人做更動。如下圖: 將此智慧合約發行至私有鏈後，即可在geth底下的console或是Mist Wallet下執行。



圖六: 智慧合約內容

在22行程式碼中，最後包含了OnlyOwner。這個指令會呼叫第九行的modifier，使用modifier可使函式受到存取限制，以OnlyOwner內容為例，它包含了”require(owner == msg.sender);”這行程式碼會進行判斷，如果在中間參數為true時才會才會正常運作，否則將直接進行例外處理，不進行函式呼叫。用此方法可確保資料的傳輸者位址。由圖九可知此合約的擁有者為Account2，而目前Msg1的內容是Data1，若想更改Msg1，則必須發出交易。

一張含有 螢幕擷取畫面 的圖片

自動產生的描述

圖七:合約內容與執行

在此張圖發起交易的為MainAccount，並且成功上傳至區塊鏈之中。不過因為該函式具備權限限制，所以即使成功發起交易，試圖更改，但也會被視為例外處理而無法成功，如圖八。

一張含有 螢幕擷取畫面 的圖片

自動產生的描述

圖八: 執行最終狀況

檢測裝置使用體溫作為判斷依據，需要使用到溫度感測裝置。此設備需具備測量、連網、傳輸等功能。由於市面上所發售的體溫感測裝置多數無法合於該計畫目的，所以該設備將自行製作。製作所需工具則使用Arduino。Arduino是由可使用專屬的主機板，加上各式不同套件去製作各式各樣的工具，例如:四軸飛行器[4]、掃地機器人[5]。然而，此計畫的需求需要結合需多功能，包含溫度感測、連網或藍牙、以及資料傳輸，但在Arduino中都有相對應功能的模組，所以選擇以Arduino開發所需要的檢測工具。

資料庫建構需要使用到MYSQL，MYSQL是一個資料管理系統，把所有資料處理技術統合在一起。而其結構為關聯式資料庫，是使用許多資料表進行處理。由於MYSQL是一套開源軟體，可任由任何人都可使用且修改，且不需費用[7]。對於java、C++、C、Python、PHP皆有支援。當資料上傳後，則使用java設計一套程式，將所蒐集到的資訊進行判斷，以體溫為例，超過37.5℃為發燒情況，這時就需要將該名使用者資訊傳達至系統上，讓相關人員進行處置。

手機APP使用Android studio去進行實作，使用語法為Kotlin。現代人手一機，且幾乎不會離身。使用GPS作為定位，確保需自我管理者有確實自行隔離。並在不特定時間(正常作息時間)下，提醒且要求用戶進行自我健康檢查，由於是在不特定時間可對用戶進行監督，有效避免惡意外出或不進行自我管理者。最後使用藍牙或wifi與檢測裝置進行資料傳遞，並上傳至區塊鏈，確保資料上傳後無法被修改，也可進一步追蹤病情。若發生資料異常或是認定為高風險患者，則需要立即通報主管單位並且進行進一步處理。

1. 預期結果

本計畫執行將開發需要有物聯網以及製造設備的技術，能與最近趨勢接軌。本計畫執行預期可以產出下列成果:

* 1. 健康資訊收集區塊鏈: 在區塊鏈架構環境下連結IOT設備，從IOT模擬設備上定期收集資訊並簽署進區塊鏈，同時也提供在區塊鏈上查閱健康資訊功能。此外，預期能結合手機APP連線進行提醒與監測等功能。
  2. 建立合適的智能合約: 本計畫在收集使用者的健康偵測資訊之後，透過智能合約的條件判斷，當健康資訊達到警示條件時智能合約的對應提示動作將被觸發以通知相關人員。

1. 參考文獻
2. 陳世昕（2015）。物聯網智慧住宅 APP 與藍牙安全實作。僑光科技大學資訊科技研究所碩士論文，台中市。 取自<https://hdl.handle.net/11296/m34gb2>
3. 凃羿凡（2015）。架構導向智慧醫療服務系統之研究。國立中山大學資訊管理學系研究所碩士論文，高雄市。 取自<https://hdl.handle.net/11296/63ggg8>
4. 田篭 照博(2018)。區塊鏈智慧合約開發與安全防護實作。朱浚賢譯。旗標。
5. 何昭毅（2013）。基於Arduino之自我平衡四軸飛行器。南台科技大學電子工程系碩士論文，台南市。 取自<https://hdl.handle.net/11296/4yyv2k>
6. 郭冠宏（2014）。利用Arduino及Wi-Fi實現具無線遠端監控功能的掃地機器人。國立臺灣海洋大學電機工程學系碩士論文，基隆市。 取自<https://hdl.handle.net/11296/b4e9bd>
7. 以太坊学习路线——（一）私有链搭建与基本操作<https://blog.csdn.net/GDUYT_gduyt/article/details/88807348?depth_1-utm_source=distribute.pc_relevant.none-task&utm_source=distribute.pc_relevant.none-task>
8. 白明宜（2008）。開放原始碼MySQL資料庫在多種同步架構下的實作及效能分析。靜宜大學管理碩士在職專班碩士論文，台中市。 取自<https://hdl.handle.net/11296/6ke546>
9. 需要指導教授指導內容
10. 智慧合約安全性及建議

智慧合約開發不會有太多邏輯思考問題，但是在現實生活中，有多種可能，不全然會依照實驗狀況去進行。所以如何將合約的效益提升至最大，排除在生活中有可能發生的各種意外狀況，或有惡意人試圖修改資料，導致訊息回傳錯誤等，智慧合約實用化及安全性考量需要有相對經驗的老師進行提點。

1. Arduino設備準備與調整

Arduino應用方面在網路上的例子十分的多，許多有創意的物品被創造出來。作為開源硬體設備，市面上也充斥著各種可用套件，導致無法決定該使用哪種開發版以及套件。這方面需要老師提供一些建議，能夠利用最少的資源去作出需求工具。

1. 手機APP與相關單位以及設備的資料傳輸

如果將手機APP、伺服器、以及設備的準備進行分散處理，難度並不高。但是在於溝通管道上，需要理解這些程式與設備的各種連線管道如何處理資料。在系統與系統間的連線，需要老師指導相關概念。

1. 程式邏輯及優化

程式設計時有時會有邏輯上問題，或者因觀念錯誤導致程式無法正常運行，以及在系統優化處理部分，需要老師指導。