使用智能合約實作股票限價交易

1. **研究計畫之背景與目的**

**背景與文獻**

在現今知識經濟的時代，個人累積價值的方式由以往的實體物品、土地、金錢，轉移成以無形的知識為主，由此可得知，有效的傳播與蒐集知識並加以利用將是未來提升競爭力的方式之一。隨著網際網路的發展、硬體設施飛快的成長，網路應用日趨多樣化，與網路相關的服務無所不在，現代人在生活上幾乎已經離不開網際網路這個傳播知識與訊息的寶庫。根據財團法人資訊工業策進會FIND的統計指出，至2008年9月底止，台灣經常上網人口達1025萬人，網際網路連網應用普及率為 45% (資策會 2009)，顯示網際網路已成為一種重要的傳播媒介。透過網際網路讀取新聞、郵件、隨時查詢所需的資訊已是家常便飯，線上交易的商業行為也日益增加。

然而，網路的多樣性、豐富性，可撥放影片、傳達聲音、顯示圖片的多元樣貌，與它覆蓋面積廣大的特性，亦能成為合適的學習媒介。這樣的數位學習(e-Learning)相較於傳統使用書本作為傳播媒介的教學方式更加多元化，期望能增加學習的興趣與效率。學習的方式不僅僅能藉由與網路相連接的電腦，延伸至行動學習 (m-Learning)，手機、PDA、iPod等攜帶裝置都能成為便利性極佳的吸取知識管道。不必受時間地點的限制，讓使用者隨時隨地的接收資訊，其機動性與坐在教室中由老師傳道授業的傳統學習方式大相逕庭。

隨著地球村的來臨，全球化的結果使得國與國之間在政治、經濟貿易上緊密互相依存，各國之間的疆界不像以前那樣明顯，文化、經濟、語言都不再只是屬於各國的專利。透過語言溝通是與其他國家交流的有效方式，而英語儼然成為世界上最重要的語言之一，其重要性在全球化的趨勢下只有與日俱增，學習英文的必要性不言而喻。學好英文當中重要的關鍵要素即是要記憶大量的英文字彙，而就一般民眾而言，閱讀英文文章時，若遇到不了解的單字，便需利用紙本的英漢字典、快譯通、哈電族等的電子辭典查閱、現在相當盛行的網路字典，或其他應用軟體。提供即時翻譯功能的雅虎奇摩迷你筆或譯典通等軟體，任何文章格式之英文單字，僅需輕盈的滑動游標指向單字或做標記就能自動抓取多種字典的翻譯和釋義；但一個常態的問題發生了，使用者往往需要耗費些許時間自己手動將翻譯逐字抄下，也較難匯整出不熟不會或難以辨別的單字，更遑論能隨時攜帶來記憶這些生辭單字，因此可能會衍生出一再重複搜尋同一單字的窘境，也流於毫無效率和記憶能力過於依賴辭典的錯謬。因此本計畫希望能提供一種新方法來替代逐步查字典的繁瑣程序，進而提升學習英文的效率。

使用者所需查詢的資料範圍廣大，重新建立一個完整的資料庫以供搜尋過於龐大，再者，在網路上已有其他現成的資料庫可加以利用，因此本計畫擬以螢幕擷取 (Screen scarping)的方式，建立一個介於使用者與服務提供者中間的系統，以期為使用者提供方便有效率的服務。運用現成的網路資源，一來可重複使用現成資源，可減少資料因重複過多造成的資源浪費，二來可節省開發與建立新的資料庫系統所需的人力與時間。本計畫將以網路服務 (web-service)為基礎，搭配網路摘要 (Web-feed)與螢幕擷取的技術服務，建立新型態的非同步式的網路字典服務，應用於低成本、高互動、高即時性的行動數位學習。

**文獻探討**

本研究根據  
一. 股票交易模擬系統程式架構

數位學習是使用者以數位媒介學習的過程，數位媒介包含電視、網際網路、電腦、錄影帶、光碟、錄音帶等，應用的範圍包括網路化學習、電腦化學習、虛擬教室及數位合作 (Wikipedia 2009)。數位學習的名詞被提出以前稱為遠距教學，遠距教學是一種透過網路、電視等傳播媒介為主的教學方式，不同於以往在教室與老師近距離互動的上課學習，透過傳播媒介，授課的老師可以在遙遠的一端以同步或非同步的形式授課。它突破了時空的限制，學生在家就可以上課，並彈性選擇上課的時間，造福許多因故無法親自到學校學習的社會大眾，增加便利性；另一方面，透過視訊會議的技術，老師在某一學校授課，其他地區的學校亦可進行同步遠距教學，節省老師舟車勞頓的開銷與成本。而數位學習是遠距教學的一種，使用衛星廣播，互動電視，光碟等來進行授課程教學，但主要以網際網路的界面來傳輸數位教材 (Wikipedia 2009)。

二. 區塊鏈 (Blockchain)

行動學習專注於將學習的方式擴充至行動裝置，如筆記型電腦、PDA、手機、iPod等手持的行動裝置，充分利用可攜式裝置擁有便利性極佳的優勢，使學習不再侷限於地域與時間的限制，增加學習的機會。行動學習亦可使用在固定的場所，例如教室、辦公室等，透過輕便的手持行動裝置，部分取代學習所需的厚重書本，更提供了有別於書本內所述文字圖片的多樣化顯示內容，支援影像、聲音的多媒體格式，為學習增添了豐富性，提升學習的意願與成效。 (Wikipedia 2009)

1. 數位簽章 (Digital Signature)
2. 區塊 (Blocks)
3. 雜湊演算法 (Hash Function)

三. 智能合約 (Smart Contract)

網路服務是一種軟體系統，透過網路使不同機器之間得以進行互動和整合。此系統是以WSDL作為媒介，而並使用其開放標準的UDDI、WSDL和SOAP (W3C 2004)。以下則分別說明web services的公開標準：

UDDI為Universal Description, Discovery, and Integration的縮寫，它是一個基於XML的跨平台的描述規範，可以使世界範圍內的企業在網際網路上發布自己所提供的服務。UDDI是Web Services的核心標準之一，透過SOAP進行訊息的傳輸，以及WSDL來說明Web Service的內容及介面 (Wikipedia 2009)。

WSDL為Web Services Description Language的縮寫，是以XML為主來以描述web services。服務提供者對外發佈Web Services的訊息時，需使用WDSL來描述所提供之服務內容及詳細的操作方式，包含輸入與預期的輸出格式。只要傳送方與接收方在溝通之前達成協議，它可以運用在任何一種語言、平台、瀏覽器。WSDL曾經發布過的版本有1.0、1.1、1.2、2.0，而目前W3C以WSDL2.0作為推薦的標準 (W3C 2004, Wikipedia 2009)。

SOAP為Simple Object Access Protocol的縮寫，它是一種在網際網路中，用HTTP傳送與溝通以XML為格式的訊息，替web services提供資訊交換格式的協定 (W3C 2004)。為了簡化網頁服務器 (Web Server)在從XML數據庫中提取資料時，無需花時間去格式化頁面，使不同的應用程式能以固定格式交換資料，由由IBM、Microsoft、UserLand和DevelopMentor在1998年共同提出，並在2000年提交給W3C，目前以SOAP 1.1作為共同的標準 (Wikipedia 2009)。

四. 以太坊 (Ethereum)

Web feed是一種資料格式，網站透過它將最新資訊傳播給用戶 (Wikipedia 2009)。使用者利用feed閱讀器訂購所需的網址，閱讀器會依設定的周期時間定期檢查網頁是否有更新。當有該網站的網頁內容更新的時候，閱讀器會即時傳送更新的訊息與內容給使用者，使用者不必逐一瀏覽網站也能快速的收到更新的內容，因此廣泛使用於經常更新內容的新聞網站與部落格 (Blog)。

Web feed與訂閱電子報的功能類似，但相較於電子報通常定期發行同樣版本，而非客製化的內容，web feed提供更具有彈性的內容，可以只訂閱想要閱讀的內容。訂閱的方式也非常容易，現今主流的瀏覽器IE、Opera、Firefox、Saferi都有將Web feed的功能整合，只需按下feed的網址即可訂閱，免去提供電子郵件地址等暴露個人資料的風險，更可免於垃圾郵件的騷擾 (Wikipedia 2009)。

常用的格式有兩種RSS與Atom，最常用的是RSS全名為Really Simple Syndication (RSS 2.0)。RSS首先於1999年由美國網景公司提出，後來出現的主要版本有0.91、1.0、2.0等，主要均以XML的檔案格式為主，如此一來，將feed發布出去，不必只侷限在於某些特定的瀏覽器與裝置才可閱讀，現今支援此格式的包含有電腦、PDA、手機等廣泛的運用 (Wikipedia 2009)。

(一) Geth

(二) Web3.js

(三) Solidity Compiler

五. 將智能合約自動化

Screen scraping是一種利用電腦程式自動將原本的輸出萃取出需要的資料，再以另一種形式呈現原有資料的技術，通常是擷取自結構嚴謹的來源文件。例如從課程網頁中，找尋課程時間、課程名稱、授課老師、課程地點等資訊。當應用程式想要從此網頁擷取資料，必須先讀取此網頁的程式碼，剖析其結構與所需資料存放的位置，抓取所需的相關資訊後，並將結果輸出成一般人容易閱讀的形式，例如加上顏色、格式、排版等(Wikipedia 2009)。Screen scraping是一種與網站互動的程序，不只是把網頁下載下來而已，而將它的HTML加以處理，使其變得更加豐富、多元(Chris 2008)。

**計畫目的**

根據上述之背景與動機，本計畫有下列主要研究目的：

* + - 1. 讓使用者可以透過簡易好操作的UI介面，就能建立一個自己的區塊鏈錢包。
      2. 除了擁有一個區塊鏈錢包之外，本計畫還會有簡易的UI介面，讓使用者設定股票限價交易的條件，系統後端便自動生程一個智能合約，再去自動的編譯和部屬至P2P網路之中。

**重要性**

1. 將股票交易的限價交易以區塊鏈實作，透過區塊鏈特性 達匿名 不可回溯 不可追蹤
2. 有別於傳統T+2交割時間，區塊鏈的應用達到實時交易
3. **研究方法、步驟及執行進度**

**研究方法**

本計畫目的在於使用智能合約實作股票限價交易系統。本計畫初期以建立股市模擬交易系統與本機伺服器中，讓使用者可以在此系統查詢股價、管理帳戶和持有的股票、進行股票交易以及管理者管理資料、帳戶、交易；中期將此本機端系統資料處理部分搬到雲端伺服器上；後期為將此系統結合區塊鏈應用，使限價交易透過智能合約自動化，達到匿名性、不可竄改等，並縮短T+2交割日期。

依據研究架構的設計，將本計畫分為三個部分，第一部分為使用者將所需查詢單字的文件上傳自作業平台；第二部分是將上傳的文件擷取出欲查詢的單字，分別查出的單字解釋與相關資訊；第三部分則以非同步的方式將查詢結果傳送至用戶端。本架構之背景圖如圖一所示，系統作業之流程圖如圖二所示。各部分如下詳述之：

圖一：非同步網路字典服務之背景圖



圖二：網路字典流程圖 (客戶端)

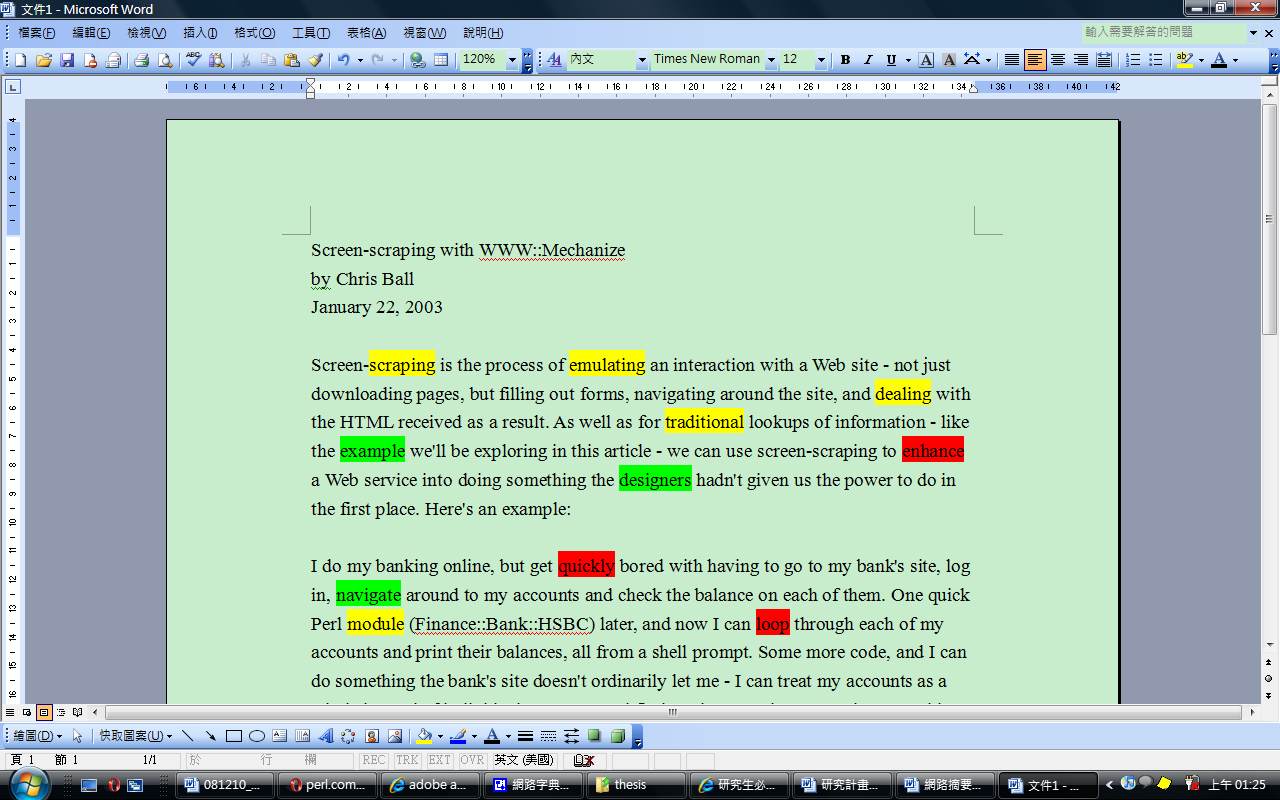


圖三：網路字典流程圖 (伺服器端)

**第一部分：使用者上傳所需查詢之文件**

使用者利用電腦或其他支援HTTP的裝置進入本系統首頁，閱讀使用本網路字典服務的方法與說明。使用說明必須包括系統支援的檔案格式、在文件上標記所需查詢單字的方法、轉換格式的步驟、訂閱RSS的方法。

本系統支援的檔案格式以Microsoft Office Word2003為主。使用者將Word檔案中，文章內欲查詢的單字以“醒目提示”的方式標記，依照網頁上說明所示，以不同顏色的醒目提示代表不同的查詢需求，再將原本的Word檔另存成HTML檔案。



學生經常需要閱讀國外論文、期刊，此類文獻用字較艱深，欲查的單字量也較多，逐字利用網路字典查詢勢必需要花費許多時間和精力。此類型的文件通常以PDF格式為主，大部分的學生無力購買價錢昂貴的Adobe Acrobat Professional軟體，無法編輯PDF檔案，更遑論在不了解意思的單字上做標記了。有鑑於此，本計畫欲提供解決此問題的方法，而可實行方法的有以下三種：

1. 提供將PDF文件轉換成Word文件的免費軟體供使用者下載。
2. 提供將PDF文件轉換成Word文件的線上轉檔服務網頁。
3. 提供Adobe Acrobat Professional試用版下載連結，使用者可下載試用版替文件轉檔。

當使用者將檔案上傳至伺服器，系統檢查檔案格式是否有誤，檢查完畢後，即產生一個獨一無二的訂閱網址，顯示在用戶端的螢幕上，使用者即可訂閱此網址來閱讀查詢結果。

將欲查詢的文件轉換成HTML檔案，對於使用者而言，似乎有些不甚方便的地方，因此未來將以支援多種格式為方向思考，而非侷限於HTML，減少瑣碎的轉換步驟，以期能更符合使用者的需求。

**第二部分：伺服器端的資料解析與收集**

伺服器端收到使用者上傳的文件後，隨即檢查格式是否符合要求，確認無誤後，讀取文件內容，將使用者欲查詢的單字與文章分離出來。以HTML文件為例，只需字串的處理即可分析出使用者標記的位置，如以下所示：

<span style='background:yellow'>Advanced</span>

<span style='background:red'>experiences</span>

閱讀文件的原始檔即可發現，標記顏色的字包含在span標籤內，標籤內敘述的background顏色是使用者標記的顏色。假設標記黃色的字要查詢英文解釋和例句，紅色要查詢中文解釋和發音檔，上述例子中，單字Advanced要查詢的是前者，experiences則屬於後者。利用程式找出查詢的單字，便將其集中至待查詢的單字清單。

將蒐集完成的單字清單分別向現有的網路字典查詢，如Yahoo!奇摩字典以及Dictionary.com，運用該網路字典的網址輸入單字查詢。以Yahoo!奇摩字典為例，其搜尋單字的網址為：

http://tw.dictionary.yahoo.com/search?ei=UTF-8&p=**[word]**

[word]的位置即表示查詢的單字為何，因此只需將欲查詢的單字放入網址中word的位置就可查詢該單字。取得該查詢頁面的原始檔後，以類似於之前取得用戶上傳文件之查詢單字的方式，找尋規則，並依據使用者的需求，將結果蒐集至結果清單。

市面上的網路字典處於百家爭鳴的時代，有許多網站均提供類似的服務，甚至入口網站也有加入戰局，企圖分一杯羹的趨勢，每間不同的網路字典都有一套與其他網站不同的編寫方式，其資料存放的位置不甚相同。然而本計畫初期選定的網路字典不見得為使用者習慣使用的，因此將來可考慮以提供多家網路字典作查詢為方向思考，以更多選擇滿足使用者需求，達到客製化的目標。

**第三部分：以非同步方式將查詢結果傳送至客戶端**

最後將查詢完的資料轉換成XML的格式的Web feed，寫入之前使用者上傳檔案成功後顯示在螢幕上的RSS網址，當此網頁更新時，使用者即可在訂閱的裝置中收到最新消息。支援Web feed的裝置有許多，電腦、PDA、行動電話都在其中，使用者可依據自己的需求，在不同的裝置中訂閱此RSS，如此一來，即可將搜尋結果隨身攜帶，不必攜帶書本筆記也能隨時隨地的背誦單字。

**進行步驟**

本計畫預定的進行步驟如下：

第一年

1. 閱讀網路服務、Web feed、Web 2.0等相關議題的技術與現有情況之文獻探討。
2. 建立非同步式網路字典服務之雛型系統
3. 測試並修正其問題

第二年

1. 對於使用者閱讀網頁的習慣進行探討，針對此平台介面以增加可讀性與可用性為目標。
2. 此雛型系統之完成與探討
3. 論文撰寫

**本計畫預定之執行進度如下**



**預計可能遭遇之困難及解決途徑**

1. 使用者將Word文件標記單字位置後，需先將文件儲存為HTML格式。為了簡略使用本網路字典服務的步驟，考慮開放上傳文件的格式，除了HTML之外，增加doc或PDF格式，上傳後的文件在伺服器端轉換成程式需的HTML檔。若要增加此功能，則需針對文件格式的轉換作進一步的研究，利用現有的技術轉換，亦或使用其他更好的方式需再加以考量；另一方面增加此功能亦需考量到伺服器的負擔問題。
2. 行動裝置的螢幕普遍較一般電腦小，使用者利用行動裝置訂閱Web feed時，排版不佳的文件會造成閱讀上的困難，減低使用者利用行動裝置閱讀的意願。因此頁面的配置需考慮各種裝置的可能性，增加行動學習的可行性。
3. 發音在英文學習中亦屬於重要的一環，考慮到行動裝置不會隨時上網，只將發音檔的連結傳送給使用者，為了聽取發音檔而上網，不僅增加上網傳送封包的費用，也增加等待的時間。因此考慮將發音檔一併下載至用戶端，然而各家行動裝置支援聲音的格式不盡相同，如何達到最好的學習效果還需再詳加考慮。
4. **預期完成之工作項目及成果**

**預期完成之工作項目**分年敘述如下：

第一年

1. 相關文獻探討
2. 建立網路字典服務雛型系統
3. XML格式之Web Feed服務之實作
4. 撰寫系統文件

第二年

1. 相關文獻探討
2. 改善雛型系統之介面使其完整
3. 雛型系統的測試與修改
4. 論文撰寫

**預期之具體貢獻與成果:**

1. 一般網路字典採取逐一輸入單字查詢的方式，本計畫突破傳統，以文章為單位，批次查詢整篇文章內的單字，有效提升查單字的效率；另一方面也將單字彙整成一份完整文件，使用者不需另外抄寫筆記，就能將此份文件隨身攜帶。若有其他人同時也須閱讀此篇文章，第一人先快速瀏覽文章並將生詞做標記，之後的其他人就可訂閱同一份RSS文件，達到資源共享的特點。
2. 行動裝置例如行動電話，一般被定義為具備娛樂功能的通訊工具，使用Web feed的作法將文件傳送至行動裝置，使行動電話成為學習工具。轉變為兼具娛樂與學習功能的行動裝置，期望使用者以輕鬆的態度隨時隨地的學習，使學習不再枯燥乏味。
3. 本計畫採用XML結合Web feed的形式將使用者的需求傳送至用戶端，以本實作採用的英文字典服務為基礎，亦可利用更多網路字典延伸至其他語言的字典查詢服務。除了字典查詢服務以外，可應用此種非同步的概念至其他領域，例如公車路線查詢、旅遊資訊查詢等，隨身攜帶所需的最新資訊，不必費心將資料在不同裝置之間連結轉換，對於社會大眾有數不盡的益處。

**參與之人員可獲得之訓練:**

1. Web feed、XML、程式語言、螢幕擷取、行動裝置支援格式等技術的學習與應用。
2. 行動學習、網路服務之概念的學習。
3. 雛型系統的建置、測試與修正。
4. 論文撰寫之訓練。

**參考文獻**

Chris Ball, 2003. Screen-scraping with WWW::Mechanize [online]. Available from http://www.perl.com/pub/a/2003/01/22/mechanize.html [Accessed 18 February 2009]

Wikipedia, 2009. *e-learning* [online]. Available from: http://en.wikipedia.org/wiki/Electronic\_learning [Accessed 17 February 2009].

Wikipedia, 2009. *m-learning* [online]. Available from: http://en.wikipedia.org/wiki/m-learning [Accessed 17 February 2009].

Wikipedia, 2009. *UDDI* [online]. Available from: http://en.wikipedia.org/wiki/UDDI [Accessed 17 February 2009].

Wikipedia, 2009. *SOAP* [online]. Available from: http://en.wikipedia.org/wiki/SOAP\_(protocol) [Accessed 17 February 2009].

Wikipedia, 2009. *Web Services Description Language* [online]. Available from: http://en.wikipedia.org/wiki/Web\_Services\_Description\_Language [Accessed 17 February 2009].

Wikipedia, 2009. *Web feed* [online]. Available from: http://en.wikipedia.org/wiki/Web\_feed [Accessed 17 February 2009].

Wikipedia, 2009. *RSS* [online]. Available from: http://en.wikipedia.org/wiki/RSS [Accessed 17 February 2009].

Wikipedia, 2009. *screen scraping* [online]. Available from: http://en.wikipedia.org/wiki/Screen\_scraping

[Accessed 17 February 2009].

W3C, 2004. *Web services architecture* [online]. Available from: http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/ [Accessed 17 February 2009]

資策會, *2009. 2008年9月底止台灣上網人口* [online]. Available from: http://www.find.org.tw/find/home.aspx?page=many&id=210 [Accessed 18 February 2009]