

多對多配對配合智能合約之雛型架構：以高等教育分發問題為例¹

研究生： 蘇柏菡

指導教授： 蘇雅惠 博士

陳昶吾 博士

摘要

現階段的高等教育入學制度，仍舊存在許多問題。本研究開始探討此一問題本質，發現其問題本質是信任(trust)。所幸，近年來有越來越多的研究單位，對於由機器代理的數位原生信任(machine-made trust)有所研究以及成果展現。與此同時，世界上各個大學、研究單位，都企圖針對高等教育模式提出另類思考方案或新模式，並且進行實踐。有鑒於此，本研究的研究問題：如何用智能合約配合多對多配對以改善高等教育分發問題？

本研究希望可以提出另一種思考模式，以面對現行高等教育模式即將到來的挑戰。並且希望試圖藉由區塊鏈技術及其特性，在現有的高等教育升學制度之下，完成基於此思考模式的另類方案。於實務方面，在探討研究目的時，本研究發現，區塊鏈技術以及智能合約等技術，其特性很適合用來作為建構信任成本的底層架構。於學術方面，台灣有不少的學者致力於高等教育中分發制度的改善，本研究亦希望能夠對此盡上一份心力。本研究希望能夠提出另一個針對台灣高等教育之升學制度另類方案，並且完成一個基於此另類方案的雛型系統。同時本研究在對學校與學生間之多對多配對做分析，比較實際情況與原本穩定配對演算法之間的相異之處，針對其相異之處對穩定配對演算法進行修改並且實作。

關鍵詞：區塊鏈、教育制度、信任、多對多配對、自由移動

¹ 感謝科技部計畫(MOST 107-2633-H-008-001-)的支持與協助

1. 緒論

1.1. 高等教育分發入學制度之現況

隨著數位時代的到來，舊時代的大學模式備受挑戰。自工業革命起，教育制度設計重在將人培養成機械式的知識份子或者是幫助人們擺脫貧窮所需的技能而給予他們相對應的知識；而在未來的數位時代，教育應該是要培養學生批判能力、或是創意力。(Davidson, 2017)。

同時，在培養人才的過程中，如何選才亦是一個重要的環節。以台灣為例，現階段的入學制度，仍舊是承襲傳統的聯考分發方式，統一由單一中心——大考中心負責。思索台灣現在的高等教育之入學制度，以大學入學制度為例，即使經歷了多次的教改，還是依循傳統的聯考分發邏輯。考生向大考中心提交自己的志願序，再由大考中心依照考生成績，將考生分發到所屬的校系，也可以說是學校系所與學生之間的配對。在此情況之下，學生一旦完成分發，就很難轉學或是轉系，若要轉學或是轉系，通常都是選擇重新考試重新分發。

並且這些入學分發一年舉行一次，分發的依據往往是用考試成績決定分發結果，也無法累積學習成果，下一次分發只能用下一次考試成績來分發。這樣的模式其本質依舊是考試，以考試成績為重，導致學生幾乎都是為考試而讀書。

另外，在現階段的入學制度之下，學生及學校雙方配對的自由度是受限的。在目前的情況之中，學校無法自由的決定想要收的學生，只能透過採計科目以及分配權重的方式來收學生，在決定好條件後，只能被動地接收由大考中心分發下來的學生。(再補研究問題跟研究重要性)

1.2. 高等教育分發入學制度之問題本質

本研究開始探討上節的問題本質，發現分發問題之問題本質是信任(trust)。在上節的情況中，學生選擇學校的彈性以及學校選擇學生的選擇權遭受到了忽略。在上述的情況，有想要進入自己理想學校的學生，也有欲收入自己理想學生的學校，即可形成一種多對多配對。在這個多對多配對的情形之中，學生有自己的排序條件，如對於學校、科系的喜好順序；學校也有自己的排序條件，如學生的所有成績、學生過去的經歷……等。配對時所需要的資訊，像是學生的喜好順序、成績或經歷這些個人資訊，都是以信任(trust)做為配對基礎的。在過去這些配對所需要的訊息，都是由一個備受信任的單一中心，也就是大考中心來負責背書，連帶導致配對作業也由一併由大考中心處理。而且為了建立一個備受信任的大考

中心，投入了大量的成本在其中，從其起初成立時籌措的資金，再到之後幾年從教育部獲得的研究經費以及捐款，總額共有五億多元供其運作。

所幸，近年來有越來越多的研究單位，對於由機器代理的數位原生信任(machine-made trust)有所研究以及成果展現，如 Blockcerts(MIT Media Lab, 2016)、謝榮軒(2018)。透過由機器所建立的數位原生信任(machine-made trust)，我們得以在區塊鏈上，透過區塊鏈技術的特性，即區塊鏈網路中所有的參與者皆為是一個中心，形成沒有單一中心的 P2P 網路環境，進一步來完成一個不由單一中心處理的多對多配對。

因此本研究希望可以提出另一種思考模式，以面對現行教育模式即將到來的挑戰。並且希望藉由區塊鏈技術及其特性，在現有的高等教育升學制度之下，完成基於此思考模式的另類方案。並且希望能夠使建立備受信任的成本下降，得以讓分發可以一年舉行多次，同時希望可以持續累積學習成果，將這些學習成果也能納入分發時的評量依據，最終建立一個可以讓學校及學生雙方能夠更自由的進行配對的系統。

2. 雛形系統開發

本章將先提到與蔡明宏老師對於高等教育中升學制度的看法，再藉由看法提出系統分析，接著介紹系統與展示本研究所開發之雛型系統。

2.1. 專家訪談

蔡明宏老師提及，很多人都不太了解每個系詳細在做甚麼，學生修課修到了大二了解後才後悔。希望可以用像是聯考成績加上之前大一成績，就能夠直接轉系或是降轉，而且每年都可以後悔。讓學生可以在學習的過程中可以自由移動轉換，透過區塊鏈的技術來實現這種自由移動。舉例來講，學生如果到了大四，他如果原本在某一個科系，他忽然間想轉到別的科系，希望可以透過過去的學習履歷，就能夠直接轉學或是轉系。現在已經進入知識經濟，學校的功能已經超過人才跟新知識，因為學生會自己形成一個知識連結，學校只是在孕育這個知識連結。並且人才可能已經不屬於某一個學校了，搞不好有一部分是屬於一個學校，有另一部分屬於另一個，因為可能已經修他們的課。透過新的分發制度，高等教育的情況就會開始有改善，因為現在的學生被分發制度限制得太緊，資工就是資工，資管就是資管。

2.2. 系統概念架構

圖 1 為本系統的概念架構。Owner 需要先將其決定好的條件，以智能合約的形式部署到區塊鏈上，再由系統於鏈上取得智能合約供使用者進行申請，最後系統再將申請結果寫至鏈上。在這系統中，因為要驅使分散式的虛擬機器就需要花費金錢(Gas)，故本研究將需要信任的步驟放在合約上去運作，例如將學生履歷透過智能合約上 Owner 所公布的喜好條件轉換成 Owner 在配對時對學生的喜好順序；而不需要信任的步驟，或者是較為複雜的步驟，例如執行多對多配對，在智能合約之外來執行，詳細原因，可以參閱附錄一。

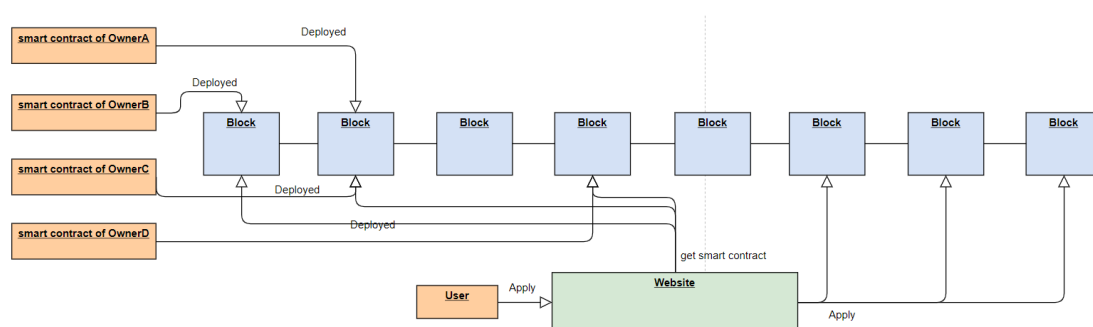


圖 1、系統架構圖

圖片來源：本研究整理

2.3. 系統分析

透過與蔡明宏老師之訪談內容，本研究認為，新的分發制度得以透過區塊鏈技術來實現。在分發的時候，可以透過學生提出存放於區塊鏈之上的學習履歷來分發。而學生的學習履歷，是由過去他在學習時，從各個單位獲得的認證，諸如修課的教育單位、考取證照的發證單位、或者是大考中心……等組合而成的。而由於這些履歷內容的有效性，謝榮軒(2018)以及 MIT Media Lab(2016)對此皆有做出證明，因此學校可以信任學生提出的學習履歷。

系統可以分為鏈上以及鏈下兩個部分，鏈上為智能合約的撰寫以及運作執行，鏈下為外部程式，提供不同使用者進行以下操作。

學校：對自己發起的智能合約進行操作。

學生：利用從獲得的數位原生信任的認證成績，向學校發出的招收學生智能合約提出配對申請。

發證方(數位原生信任)：概念參考並沿用謝榮軒(2018)給予學生認證成績。這個發證方可以包含考試單位、甚至可以是由學校在家長為了投資子女而捐獻給學校後由學校替該名家長之子女進行認證。

2.3.1. 使用案例圖

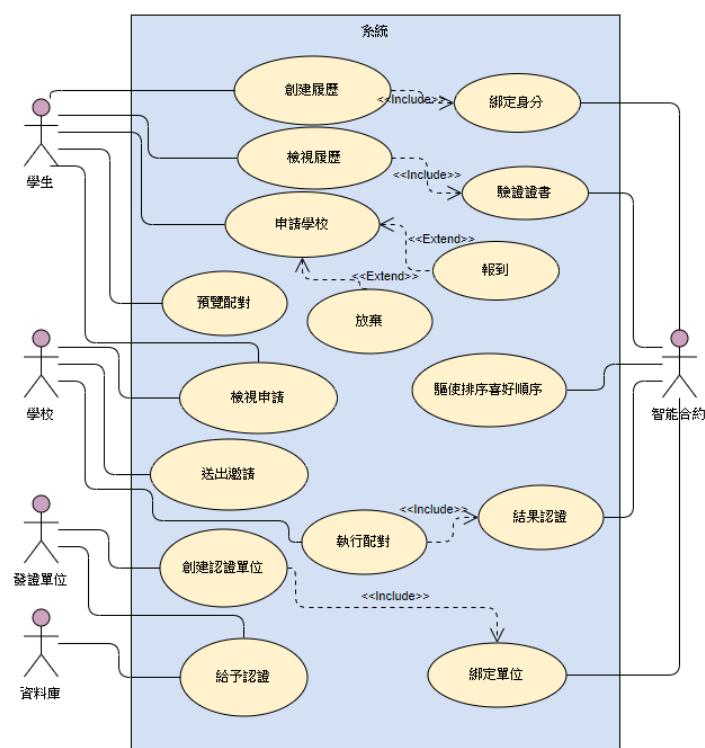


圖 2、使用案例圖

圖片來源：本研究整理

圖 2 為系統之使用案例圖，動作者包含學生、學校、發證單位、資料庫、以及智能合約。雖然智能合約是部屬於區塊鏈之上的，不過因為其具備有基本的邏輯判斷能力，以及其負責擔任使用者與區塊鏈溝通的角色，因此本研究將其視為一個獨立的動作者。本使用案例圖包含以下使用案例：

1. 創建履歷：學生可以透過系統建立履歷，同時藉由智能合約綁定學生身分，以此在區塊鏈上建立永久的個人履歷。
2. 檢視履歷：學生可以透過系統檢視履歷，系統透過智能合約確認該名學生是否擁有履歷後，向資料庫取得該名學生所擁有的履歷資料，並透過雜湊演算法(sha256)計算並向智能合約核對驗證後，呈現履歷內容。

3. 創建認證：認證單位可以透過系統創建認證，同時藉由智能合約綁定認證單位身分。
4. 給予認證：發證單位可以透過系統建立認證證書，並將其儲存置資料庫，同時透過雜湊演算法計算其證書內容的雜湊值，發送給學生履歷。
5. 申請學校：學生可以透過系統，向學校提交配對申請。
6. 檢視申請：學生以及學校可以透過系統，查看目前已申請配對的所有履歷地址以及該地址在此配對學校中的概況。
7. 送出邀請：學校可以透過本系統，直接向自己屬意的學生履歷送出邀請。
8. 排序喜好順序：學校可以透過本系統，驅使智能合約，將目前所有申請配對的學生，依照一開始部屬智能合約時學校開出的喜好條件內容，將所有學生排序成學校的喜好順序。
9. 預覽配對：學生可以透過本系統，預先觀看多對多配對結果。
10. 執行配對：學校可以透過本系統，執行多對多配對，並將其結果透過智能合約儲存至區塊鏈上。

2.4. 分發配對雛型系統使用流程

由於學生要進行配對時需要有履歷資訊，學校也需要先將智能合約部署至鏈上，因此有前置條件：學生需要先獲得成績認證、學校需要先完成招收條件的智能合約並且將智能合約佈署到區塊鏈上。故本章節的介紹順序會是發證單位、學生、學校。而學校會於一開始就事先將其學校智能合約部屬上去。另外，由於篇幅因素，本章節僅展示雛型系統中之分發配對使用流程。

2.4.1. 學生

檢視履歷並選擇學校：

My Score

Name	StudentA										
ID number	A123456789										
Score address	0x96cf682c1104750a896552e5867181a0c8d914fd										
Chinese	10	English	11	Math	15	Society	13	Science	12		
Performance	Algorithm.										

Show

Sclect School

School_A

School_B

School_C

School_D

圖 3、檢視履歷並選擇學校

資料來源：本研究整理

成功建立學生個人履歷後，會顯示進入個人履歷及選擇學校頁面，點及該按鈕後進入頁面後，頁面上半部會顯示個人履歷，下半部會出現學校選擇按鈕，點選學校按鈕後會進入該學校頁面，如圖 3。

申請學校：

School B Information

錄取人數

Capacity	1
----------	---

各科加權

Chinese	0	English	0	Math	10	Society	0	Science	3
---------	---	---------	---	------	----	---------	---	---------	---

必要條件

必要需求	algorithm
------	-----------

圖 4、申請學校(續)

資料來源：本研究整理

進入學校頁面後，頁面上會顯示學校對於配對學生的需求，此需求可以客製化，如圖 4。點選申請按鈕，此時系統會將學生合約地址、學生履歷轉換成的分數等資料，傳送給智能合約，即可送出並且完成申請。

檢視申請：

School A Result

Total Score	80	Rank	-	Apply Result	尚未排名
-------------	----	------	---	--------------	------

檢視申請

申請情況

顯示目前schoolA申請狀況

99 = default, 0 = fales, 1 = pass, 2 = check in, 3 = give up

Address : 0x96cf682c1104750a896552e5867181a0c8d914fd

Total Score : 80

Result : 99

圖 5、檢視申請(學生)

資料來源：本研究整理

於學校頁面中，按下檢視申請按鈕，即可觀看目前該校所有學生的申請狀況，如圖 5 所示，由於尚未開始進行配對，申請結果會顯示尚未排名。而按下顯示目前學校申請狀況鈕後，下方的申請情況會顯示出該學校目前所有申請中的學生履歷地址、履歷轉換後的總分、以及目前的申請結果。

3. 研究結論與討論

3.1. 研究成果：新思考模式與分散式多對多配對雛型系統

本研究提出台灣高等教育入學制度之新思考模式，並以此新思考模式開發出一個分散式多對多配對雛型系統，此雛型系統可以透過區塊鏈上之數位原生信任進行多對多配對，解決傳統高等教育分發時，必須要透過單一中心配對而導致只能透過考試成績作為配對依據，致使配對雙方的自由度受限之問題，使學校及學生雙方能夠更自由的進行配對。

本研究透過觀察台灣高等教育之入學制度，發現即使經過多次教改，其本質依舊是以考試為中心，探討其原因本質，本研究認為其問題本質是信任(trust)。在以往的情況，只能透過考試成績來建立信任，並且此信任是由單一中心來建立的。所幸，近年來有越來越多的研究單位，對於另一種信任方式—由機器代理的數位原生信任(machine-made trust)有所研究以及成果展現。

因此本研究提出之思考模式：在未來台灣高等教育的入學方式，可以透過數位原生信任所形成之學習履歷作為配對時的參考依據，同時此履歷可以持續累積，日後配對亦能繼續使用。在現行的模式下，學生一旦進入了某個科系，要再轉系只能透過轉系申請、轉學考試、或者是重新考一次大學聯考，本研究認為原因是因為大多數的學校，只能夠採納並且信任大考中心幫忙分發的學生，就好比學校科系是一條跑道，而學生只能透過大考中心來分配跑道，並且跑道間的轉換由於學校科系沒有別的信任方式可以採納，導致學生轉換跑道困難；而在新思考模式之下，學生得以透過數位原生信任所形成之學習履歷，作為轉換科系時提供給學校科系的參考依據，讓轉換跑道這件事情變得更為容易。

本研究於第 3 章中，針對大學與學生之配對，也就是多對多配對，進行分析以及與各種演算法進行比較。對此，本研究認為，大學與學生之多對多配對，與 Gale & Shapley 的穩定配對之演算法有些微的情況差異，包含兩者的演算法中兩邊配對數量不同、且配對容量可以不只一個，以及雙方喜好順序可不必填滿，並且允許有學生或是學校在合理情況之下沒有配對到對象。因此本研究試圖針對上述之不同點，對演算法進行修改並且實作。同時，為了能夠運行分散式多對多配對，本研究對此提出了一套想法，並透過一系列的證明，證明其可用性。

最後，本研究基於第 3 章之思考模式，以及第 4 章中蔡明宏老師對高等教育中升學制度的看法，於第 4 章中提出架構並且完成可以透過區塊鏈上之數位原生信任之另類方案，也就是分散式多對多配對離型系統。管理意涵

本研究認為，此離型系統的價值在於：改變高等教育取才制度的驅動力或是契機：

本研究對於台灣高等教育之入學制度，提出另的思考模式，就是透過對於區塊鏈底層技術之信任，採用數位原生信任之認證方式，作為學生與學校配對時的依據，並且基於此思考模式，本研究完成此分散式多對多配對離型。而配對時的依據，可以按照配對雙方本身的需求，可以是學生的學習經歷，如修習過某些學分，也可以是對於某些機構或是社會的貢獻。並且同時，這些學習經歷在進入大學之後，亦可以繼續累積，形成一個終身學習的履歷，以此激勵所有人持續學習，持續累積自己的學習履歷，活到老學到老。

本研究希望透過本研究，試圖成為改變現代科舉制度之驅動力或式契機。在未來的數位時代，由於許多事情可以讓電腦代為操作，因此教育應該是要培養學生應用創意、或是批判思考能力。並且同時，十二年國教之興趣選修，作為幫助學生探索並培養興趣之用途，等同於試圖將以往讓所有學生在同一畫好的跑道上競賽的跑道消除掉。然而若是高等教育人才的取得方法上，仍舊採用傳統聯考的方式，會抑制原本高中端的努力成果，同時學生仍會因現實問題，也就是要上好學校只要考試就好，興趣選課因為不列入考試中而可以不用花太多心力。因此高等教育需要跟著銜接，以免學生已經在高等教育之前找出自己的興趣，卻只能回歸考試成績決定科系。

以大學的角度而言，大學主要的目的有兩個，一個為產出知識，另一個為產出人才。而在產出人才的流程中，分為獲取人才、培養人才、最後才是產出人才。然而在過去，對於如何獲取人才上，台灣的高等教育多數的情況只能透過考試分發來完成，難免或出現一些遺珠之憾。若能透過除了考試之外的方式獲取學生，例如過去的學習經歷、事蹟等，本研究認為，對於學校所能獲取到的人才，會更加優秀。

3.2. 未來研究

關於教育制度之議題，非常廣泛，本研究期望後續能夠持續增加此議題之研究廣度以及深度。在廣度方面，本研究認為區塊鏈對於教育制度上的應用，不僅止於認證以及分發上，能擴及至其他應用。在深度方面，在教育分發議題上，本研究僅止於提出另一種另類模式以及學生學校之先的多對多配對問題上，然而以議題後續尚有許多可以繼續探討之內容。

參考文獻

- 楊宏章，2015，“三管道聯合分發”，數學傳播 39 卷 4 期，頁 71-86。
- 顏裕，2017，“以 Solidity 語言實作之多對多配對離型系統”，國立中央大學資訊管理研究所碩士論文。
- 謝榮軒，2018，“區塊鏈履歷離型架構初探_招募過程之數位原生信任機制”，國立中央大學資訊管理研究所碩士論文。
- Atila Abdulkadiroğlu & Parag A Pathak & Alvin E Roth & Tayfun Sönmez, 2005, “The Boston public school match,” American Economic Review, Vol. 95, Iss. 2, pp368–371.
- Alvin E Roth & Tayfun Sönmez & M Utku Ünver, 2004, “Kidney exchange,” The Quarterly Journal of Economics, Vol. 119, Iss. 2, pp457–488.
- Cathy N. Davidson, 2017, The new education, Basic Books.
- D. Gale & L. S. Shapley, 1962, “College Admissions and the Stability of Marriage,” The American Mathematical Monthly, Vol. 69, No. 1, pp. 9-15
- L. Shapley & H. Scarf, 1973, “On Cores and Indivisibility,” Journal of Mathematical Economics 1, p23-37.
- Marc-David L. Seidel, 2017, “Questioning Centralized Organizations in a Time of Distributed Trust,” Journal of Management Inquiry, Thousand Oaks, Vol. 27, Iss. 1, pp40-44
- Marten Risius & Kai Spohrer, 2017, “A Blockchain Research Framework,” Business & Information Systems Engineering, Vol. 59, Iss. 6, pp385-409.
- MIT Media Lab, 1986, 取自 <https://www.media.mit.edu/> Accessed: 12 April 2019.
- MIT Media Lab, 2016, “What we learned from designing an academic certificates system on the blockchain,” 取自 <https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196> Accessed: 19 April 2019.
- MIT Schwarzman College of Computing, 2018, 取自 <http://news.mit.edu/2018/mit-reshapes-itself-stephen-schwarzman-college-of-computing-1015> Accessed: 12 April 2019.
- Nick Szabo, “Smart Contracts,” 1994, 取自 <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> Accessed: 10 April 2019.

- Satoshi Nakamoto, 2008, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 取自 <https://bitcoin.org/bitcoin.pdf>
- Vitalik Buterin, 2013, “Ethereum White Paper: A next-generation smart contract and decentralized application platform,” 取自 <https://github.com/ethereum/wiki/wiki/White-Paper> Accessed: 12 April 2019.
- Wikipedia, “Top trading cycle,” 取自 https://en.wikipedia.org/wiki/Top_trading_cycle Accessed: 28 November 2018.
- Woolf Building the first Blockchain University, Joshua David Broggi, Martin Albert Gallagher, Johann Lilly, Jonathan Duquette, Courtney Nimura, Miles Pattenden, Felix Richter, LolaSan Martín Arbide, Shahar Avin, Kate Kelley, Maria Lidova, Diana Rodríguez-Pérez, Andreas Winkler, 2018, 取自 <https://medium.com/the-woolf-company-blog> Accessed: 25 October 2018.
- Yuval Noah Harari, 21 Lessons for the 21st Century, 2018, Jonathan Cape.

附錄一、智能合約多對多配對關鍵問題釋疑

本研究在開發系統以及撰寫智能合約時，陳老師對於本研究的碰上的關鍵問題做出了下述之釋疑。

Gas limit：由於每次運行智能合約時，EVM 每執行智能合約的一個動作都會耗費 gas，而且 gas 的使用量是有一定上限的，因此如果要將多對多配對演算法全部的步驟都納入智能合約之中，需要對演算法中的函式拆分成多個部分，例如：原本的函式運作 $\text{fun}() = \text{fun3}(\text{fun2}(\text{fun1}()))$ ，就要將其拆分，讓 $\text{fun1}()$ 先運行並暫存結果，再將暫存結果給 $\text{fun2}()$ ，依此類推；或是減少使用迴圈，或沒有邊界的寫法。以拆分的方式來降低單一筆交易所耗費的 gas 量，有機會讓該筆交易的 gas 用量少於 Gas limit。

通常智能合約使用原則：將需要受到信任的步驟，交給智能合約來執行；相對而言較不需要運作的步驟，在外部執行。

因此，本研究認為，多對多配對，由於其本身是透過迴圈的方式，找出沒有配對到的人，並將之進行配對，過程過於繁瑣，容易耗費大量 gas，導致配對成本大幅上升。又由於多對多配對本身相較於其他事項，因其可信任度背後為數學公式來證明，故其需要受到信任的程度相對較低，可以於智能合約外執行，只需要將執行結果儲存在合約上即可。

附錄二、從雛型系統到產品系統待開發事項

本研究完成的是雛型系統，在此雛型系統中，本研究主要要解決的問題為分散式多對多配對。本研究將此問題，分成三個部分，分別是多對多配對背後技術理論釐清、多對多配對演算法修改並實作、以及分散是多對多配對證明。

然而，要從雛型系統轉換到產品系統，本研究認為還有不少問題要去解決以及完成，因此條列了下述內容：

1. 並無使用加密錢包：若真的要於區塊鏈上使用 Dapp，勢必是要使用加密錢包，而本研究目前直接透過測試鏈給予的 10 組錢包帳號進行開發測試，而這 10 組錢包帳號可於首頁最上方的切換帳號處做切換選擇。
2. 內容寫死：於多對多配對頁面中，由於本研究在演算法中，將學校學生宣告為物件類別，使用動態處理，程式會將之識別為字串而不是物件類別，因此配對中兩邊的數量，需要事先宣告好，無法再變動人數。
3. 部分該自動化處理之內容用手動處理：在多對多配對程式中，原先該使用自動化處理之方式，將配對雙方的喜好順序直接帶入到程式中。然而由於在抓取那些參數時，原先頁面會將參數存成物件傳送，傳送完後程式只能讀取到物件名稱，詳細的內容如喜好順序皆無法讀取。故目前喜好順序只能採用手動輸入。
4. 介面簡陋：由於系統為雛型系統，目前以能夠執行正確即可，因此在介面設計上本研究沒有加以著墨。

附錄三、智能合約交易成本估算

表 1、各功能花費成本估算

功能	花費 gas	估算成本(Gwei)	估算成本(Ether)	U.S. dollars
部屬初始合約	3180809	57572642.9	0.0575726429	US\$8.85
建立履歷	1343228	24312426.8	0.0243124268	US\$3.74
成為發證單位	693246	12547752.6	0.0125477526	US\$1.93
發放證書	383830	6947323	0.006947323	US\$1.07
部屬學校合約	1876176	33958785.6	0.0339587856	US\$5.22
申請學校配對	25048	453368.8	0.0004533688	US\$0.07
Gas Price	18.1 Gwei/gas	Ether Price	153.68 U.S. dollars/ether	

資料來源：本研究整理

Statista(<https://www.statista.com/statistics/806453/price-of-ethereum/>)

Eth Gas Station(<https://ethgasstation.info/>)

當我們想利用區塊鏈(本研究為以太坊)做交易時(如：轉帳、與智能合約互動時)，我們就需要支付費用給區塊鏈上的礦工幫助將交易寫至區塊鏈上，並確認交易紀錄，形成區塊。

而在以太坊上，每一行程式碼在 EVM(Ethereum Virtual Machine 虛擬機器)中執行運算都會有成本費用，該成本是利用 gas 為單位去計算。

Gas Limit—指發起交易者最多願意花費多少 Gas 去完成這個交易(如：執行智能合約)。

Gas Cost—指本次交易實際花費的 Gas，當 Gas Cost 等於 Gas Limit 時表示花費超過上限，則交易失敗，計算過程全部無效，並且還是會要將花費 gas 所對應到的金錢支付給礦工。

Gas Price—指發起交易者願意支付多少酬勞給區塊鏈(以太坊)上的礦工幫你將交易寫至區塊鏈上並確認這筆交易。

實際消耗成本也稱為交易費用(Transaction Fees)為： $\text{Gas Cost} * \text{Gas Price}$ 。

在本研究中，採計 2019 年四月的平均 Ether Price 以及 2019 年五月之 Gas Price 來估算，如表 1 所示。

在中並沒有檢視履歷等與檢視資料之相關功能，由於該類功能僅從區塊鏈上讀取資訊，並無進行交易等運算，因此無須花費 gas。而從表中可以得知，越複雜的功能或所發佈的合約內容越多，所消耗的成本越高，且該花費的成本遠遠高於現階段使用網路傳遞或儲存資訊的成本。

附錄四、多對多配對演算法修改後程式碼

```
function engageEveryone(gals) {  
    var done;  
  
    var count = 0;  
  
    do {  
  
        done = true;  
  
        count += 1;  
  
        console.log(count);  
  
        for (var i = 0; i < gals.length; i++) {  
  
            var gal = gals[i];  
  
            if (!gal.fiance) {  
  
                done = false;  
  
                var guy = gal.nextCandidate();  
  
                console.log(gal.name);  
  
                if(guy == null)break;  
  
                console.log(guy.name);  
  
                console.log(guy.fiance);  
  
                console.log(iscalCandidate(guy, gal));  
  
                if(iscalCandidate(guy, gal)){  
  
                    if (!guy.fiance){  
  
                        console.log('guy.fiance :' + guy.fiance);  
  
                        guy.engageTo(gal);  
  
                        console.log('engage1bynull');  
  
                    }else{  
  
                        console.log('guy.fiance :' + guy.fiance.name);  

```

```

        console.log(guy);

        console.log(gal);

        console.log(guy.rank(gal.name));

        console.log(guy.rank(guy.fiance));

        if(guy.rank(gal) < guy.rank(guy.fiance.name)){

            guy.engageTo(gal);

            console.log('engage1byprefer');

        }

    }

}

}

}

}

    if(count>100)break;

} while (!done);

}

```