碩士學程讀書計畫

近程

大二進入實驗室以來，進行了多次的 Lab Meeting 。因為這樣，我可以就近觀察研究生是如何透過學習、探索、發現問題到提出自己的解決方案。

不只如此，我也從中瞭解自己還有諸多不足，所以制定了研究所入學前的重點補強方針：

- 研讀 Paper

  找到論文指導教授後，初步討論碩士生涯的研究方向並開始研讀該領域之必讀論文以累積先備知識。若指導教授有額外的時間，我也會積極爭取提前參與 Lab Meeting 的機會。

  此外，若碩士學程決定進行區塊鏈領域的相關研究，我也會針對以下方向的論文進行研讀:

  - **區塊鏈核心技術**
  - **區塊鏈的應用**
  - **區塊鏈攻擊**
- 加強外文能力

  我與 Robert Bosch Taiwan Co., Ltd. 簽訂的實習合約將於大學畢業時結束。在外商公司實習有大量的時間能夠接觸英文，但我認為這還遠遠不夠。我從大三開始便會利用課餘時間去英文補習班上課，在畢業前也會增強 **business communication** 以及 **Technical writing** 的能力 ，讓我在進入碩士學程前就具備撰寫英文論文的能力。
- 學習使用對研究有幫助的生產工具，如:
  - 排版系統: LaTeX, Markdown
  - 製圖軟體: illustrator, gnuplot
  - 文獻管理系統: JabRef, Zotero, BibTeX
  - 寫作輔助工具: grammarly
  - 論文抄襲檢查器: turnitin
  - 論文整理工具: Notion
- 多加利用成大 Wiki 、各所大學的開放式課程學習 Linux 核心以及 C 語言程式能力。

中程

我的專題指導教授--黃柏鈞老師說過：「在研究的過程中不要逃避任何問題，面對它並且專注的研究下去一定會有收穫。」
大學時期，學校通常希望學生有實務能力，而研究生與大學生不同，需要的是探索並解決問題的能力。
在大二時就進入實驗室也讓我對自己的興趣領域有進一步的想法，大學專題是以圖像辨識以及機器學習做為主題，與組員製作了一套課堂自動點名紀錄系統。此外，我也以該題目嘗試投稿科技部的大專生研究計畫，雖然沒有獲得評審委員的青睞，但是，從這次撰寫提案計畫書的經驗，讓我學到了:「撰寫研究計畫的相關文件時必須將每一項細節鉅細靡遺的表達清楚」以及「遵守學術倫理的重要性。」

此外，我也非常幸運的能夠與實驗室的學長姐以及教授一起參與區塊鏈領域的研究，在這個過程中，我能夠近距離的觀察到學術研究是如何進行的並且我也透過這次機會使用了 **Hyperledger Fabric** 這項由 Linux 基金會主導， IBM 貢獻的區塊鏈網路項目，將論文研究的原型實作出來。因此，我希望能夠在碩士期間繼續研究區塊鏈，並且在求學期間利用 貴校豐富的資源進行多方探索，思考哪些領域的問題能夠讓區塊鏈技術變成最佳解答。

遠程

碩士畢業後，我希望自己成為一位能夠獨當一面並具有領導能力和溝通技巧的頂尖開發者。
不過，技術專家並不是我所追求的終點，我在 Bosch 實習單位的主管告訴過我: 不論是否在學，都應該持續學習、探索自己，保持對知識的渴望。
我希望在不斷精進自己之後，可以朝向不同方向發展，像是: 品質管控、技術顧問、產品 / 專案經理等等，我也堅信當自己做足準備時，就算名為機會的繩子再細，我也能將其僅僅抓牢。
此外，我同樣希望跟上各位大學長、前輩的腳步，在行有餘力時，利用自己的資源、知識對社會做出回饋以及效仿 Jserv 等資訊領域的資深專家持續的對開放原始碼專案做出貢獻。

讓 10 年後，甚至是 20 年後的自己是一位讓母校驕傲的傑出校友。

碩士學程研究計畫

利用區塊鏈技術實現身分證與全民公投數位化

摘要

從**拜占庭問題** [1]到中本聰所提出的**比特幣白皮書** [2]，世人開始對這個奇妙的分散式系統架構有了新的認知並將其統稱為**區塊鏈**。在比特幣 [3]中的創世區塊誕生至今的 10 餘年間，從早期用於**暗網** [4]交易進而引起挖礦風潮，再到區塊鏈技術的開枝散葉，如: 以太坊 [5]、狗狗幣 [6]、波場幣 [7]以及在台灣發跡並快速崛起的新創公司: 圖靈鏈 [8]...等。大家都試著利用分布式帳本嘗試解決不同問題。

像是圖靈鏈執行長最初是希望能夠利用數位證書去解決申請海外研究所時遇到: 履歷認證過於耗時的問題。而以太坊創辦人一開始是希望比特幣能夠發展出完整的程式語言以供開發者使用，遭到拒絕後才將方向轉為打造自己的區塊鏈。這些區塊鏈的前輩之所以能獲得成功，皆是出於其擁有**解決問題**的強烈動機。

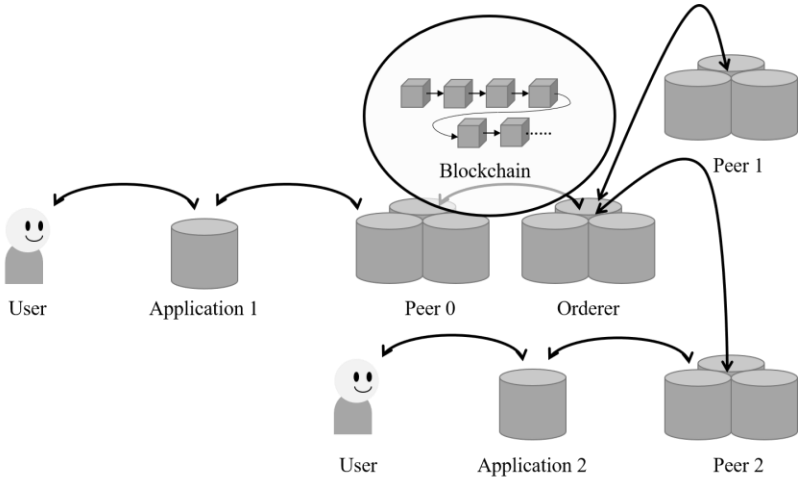
在台灣土生土長的我，享受民主帶來的便利。也因為民主賦予人民的權利，各位國民都有義務參與選舉等公眾事務。在 2018 年的 9 合 1 市長選舉，因為與公投合並舉辦，導致**一邊開票，一邊投票**的亂象發生。透過該事件，便讓我開始思考: 要如何利用資訊技術降低公眾投票所需要的人力以及時間成本。一開始，我對於如何找出問題的答案並沒有具體的想法，直到在實驗室參與區塊鏈技術的相關研究時，我才驚覺: 或許這就是該問題的最佳解答。

由於我擁有開發區塊鏈應用的相關經驗，再加上平常就會關注鏈圈的相關技術。因此，對於區塊鏈應用層面上的實作可以算是十分上手。我希望在我的碩士論文中，能夠從**投票活動的資訊化**作為出發點，設計出完整的身份驗證機制，從遠而近的將投票活動資訊化、數位身份證、戶政資料登記的詳細流程設計出來。熱衷於實作的我，更希望自己能在碩士研讀期間實作出完整的系統原型。

系統架構與動機

以 2018 年的 9 合 1 市長選舉為例，因為與公投議題較往年更為特別並且在公投書的設計上有不易閱讀等疏失，進而導致**一邊開票，一邊投票**的亂象發生。起初，我雖希望能夠**利用資訊技術降低公眾投票所需要的人力以及時間成本**，不過在當時並沒有太具體的實現方式。直到在實驗室參與區塊鏈技術的相關研究並學習使用 Hyperledger fabric 配合網頁開發技術實現研究原型時，我才驚覺: 或許區塊鏈能夠有效解決這個問題。也因為投稿過科技部大專生研究計畫，讓我對於方向探索更有心得，確立初步方向後，我也開始閱讀相關的技術文獻 [12][13][14]。

在閱讀相關文獻後發現在學術界中已經有人嘗試利用區塊鏈技術解決公民投票的問題。不過，我也發現該研究並沒有對如何落實政策以及實際應用產生的問題進行更深的探討。



圖一、 系統架構圖

因此，在我的碩士論文中，我希望能以**投票活動的資訊化**作為出發點，設計出完整的身份驗證機制，由遠而近的逐步將投票活動資訊化、數位身份證、戶政資料登記的詳細流程設計出來。此外，熱衷於實作的我，期望自己能在碩士研讀期間實作出完整的系統原型。

整個資訊系統共包含了:

- 區塊鏈主網路

  使用由 Linux Foundation [8]所主導的 Hyperledger fabric [9]作為區塊鏈網路主體或是自行設計一套簡易的區塊鏈網路。

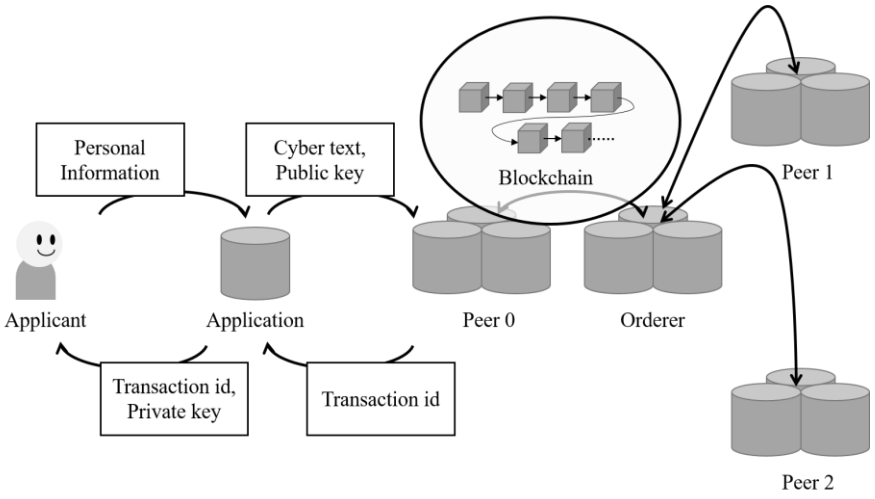
- 節點

  本機制為控制節點數量，以地方戶政機關作為節點。這樣一來，能夠採用較為節省效能的權威證明共識機制 (Proof-of-Authority, PoA) [10]。

- 註冊與註銷身份

  若以 Hyperledger fabric 作為區塊鏈主網路，便可以藉由其官方提供的 SDK [11]開發出註冊與註銷身份的資訊系統供醫院以及有關單位使用。

初步構思



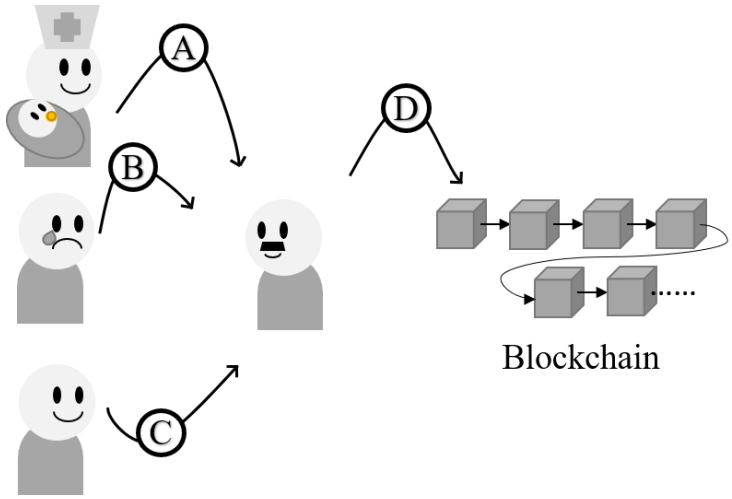
圖二、 身份註冊流程圖

- 身份註冊、身份驗證機制
  送出身份註冊請求後，系統會使用 RSA 加密演算法以獲取公私鑰。
  再將個人資訊使用公鑰進行 RSA [15]加密並且將加密內容以及公鑰作為交易內容提交出去。

  交易內容的格式如下:

```
Key: transaction_id,
Value: {
   rsaEncryptionWithPublicKey(personalInformation),
   publicKey
}
```

  當交易請求驗證成功並儲存至帳本 (在 Hyperledger fabric 中，官方偏好以帳本作為區塊鏈的代稱)後，會回傳交易序號以及個人私鑰給申請人。
  同時，我們以該交易序號作為個人的身份序號 (若是用於取代現有的身份系統，該交易序號可視為身份證字號)。
  利用該機制，能讓身份序號完全公開，因為帳本上的個人隱私資訊僅能透過個人持有的私鑰解密獲得。



圖三、 實際應用情境圖

- 實際應用時可能發生的情況

Case A: 出生

1. 由醫院、婦產科利用身份註冊系統發起身份登記請求 (交易請求)。
2. 交易會被提交到可靠節點 (地方戶政機關)進行驗證。
3. 經過節點驗證以後會返回交易編號給發起交易的機構，並且將交易資訊新增到帳本中。

Case B: 死亡

1. 由相關單位發起註銷身份請求 (交易請求)。
2. 交易會被提交到可靠節點 (地方戶政機關)進行驗證。
3. 經過節點驗證以後會返回交易編號給發起交易的機構，並且將交易資訊新增到帳本中。

Case C: 政策推出前出生的國民

回到現實層面，要將國內人口全數換發成數位化身份登記是非常困難的，因此本研究將政策落實分為兩階段:

輔導階段~??年

可根據戶政機關既有的資料庫，額外新增一筆紀錄有無登記新數位身份的欄位，並且透過需要實名制度的活動將尚未登記的國民納入管理，舉例:

- 進入小學階段前:
  - 就醫時透過健保系統進行驗證並協助身份登記。
  - 國民小學入學時，透過學校統一進行身份登記。
- 小學、國高中、五專二技及大專院校就讀中
  - 就醫時透過健保系統進行驗證並協助身份登記。
  - 透過學校統一進行身份登記。

- 符合參與選舉、公投身份者，在進行投票前協助身份登記。

– 就業國民

- 申報所得稅時，協助進行身份登記。
- 透過勞保系統，要求資方協助勞方登記。
- 就醫時透過健保系統進行驗證並協助身份登記。
- 符合參與選舉、公投身份者，在進行投票前協助身份登記。

– 待業、退休國民

- 就醫時透過健保系統進行驗證並協助身份登記。
- 領取退休金、失業給付等相關社福措施時協助身份登記。
- 符合參與選舉、公投身份者，在進行投票前協助身份登記。

強制落實階段

– 過戶政資訊系統查詢尚未登記人口並實行強制登記輔導。

– 將**輔導階段**小節提到的方法，全面轉為強制登記。

Case D: 交易驗證並提交至帳本

若採用 Hyperledger fabric 開發，交易流程如下:

1. 用戶透過 Application 向 Peer 發出請求。
2. Peer 收到請求後，會檢查資料的正確性並且依據設定尋找其他節點背書。
3. 待指定節點背書後，智能合約會依據下列事項逐一進行驗證:
   - 背書是否有效。
   - 背書數量是否正確。
   - 背書是否來自預期節點。
4. 驗證完成後資料會被記錄到帳本上並且將交易序號傳回給發出請求的用戶。

- 投票活動資訊化

假設 2024 總統大選是利用該機制進行投票並且假設本機制採用利用 Hyperledger fabric 開發。便可以利用 Hyperledger fabric 中帳本資料可修改的特性 (有開啟該功能的前提下)，在每個用戶的專屬區塊內新增一筆欄位 vote :

```
Key: transaction_id,
Value: {
  rsaEncryptionWithPublicKey(personalInformation),
  publicKey,
  vote:[] //new
}
```

當票選進行時，投票人可依據政府機關發布的應用程序進行投票，投票流程如下:

- 用戶透過 Application 向 Peer 送出交易請求，交易內容為:

```
userId: 'XXX',
decision: 'XXX'
```

- Peer 收到請求後，會以 userId 作為關鍵字查詢帳本，檢查該用戶是否已經進行此次投票。
- 若用戶已經投票，則回傳錯誤訊息。否則，系統會產生亂碼並使用用戶的公鑰進行加密作為檢查碼傳回 application ，這時用戶會收到輸入驗證碼的請求，要獲取驗證碼必須將檢查碼使用私鑰解密。
- 待用戶輸入正確的驗證碼，基於保密原則， Peer 會將投票結果以用戶公鑰進行加密並儲存至帳本:

```
Key: transaction_id,
Value: {
  rsaEncryptionWithPublicKey(personalInformation),
  publicKey,
  vote:[
    {
      "2024presidentialElection": rsaEncryptionWithPublicKey(decision)
    }
  ]
}
```

同時，第三方 (投票舉辦方，在此為政府)會收到 Peer 發出的請求，以不記名的方式記錄投票候選人獲得此票。

- 待開票時間到，只需查看第三方資料庫的資訊便能完成計票流程。

- 可延伸的方向

1. 搭配電子錢包，統整電子支付、數位貨幣等服務。
2. 將個人財產列表和不動產、汽車交易整合到該機制。

預計行程表

- 階段一
  正式確定方向並開始準備相關工作。
- 階段二
  將完整的實驗機制設計出來並實作原型。
- 階段三
  完成實驗並設計相關測試以獲得實驗數據。
- 階段四
  準備論文口試以及任何申請碩士資格的必需資料。
- 階段五
  通過口試並完成論文後，檢查論文的抄襲涵蓋率並提交論文。

參考資料

1. “Byzantine Generals Problem” https://coincentral.com/byzantine-generals-problem/. Accessed: 2020-09-09.
2. “Bitcoin Whitepaper” https://bitcoin.org/bitcoin.pdf. Accessed: 2020-09-09.
3. “Deep Web” https://en.wikipedia.org/wiki/Deep_web. Accessed: 2020-09-09.
4. “Ethereum” https://en.wikipedia.org/wiki/Ethereum. Accessed: 2020-09-09.
5. “Dogecoin” https://en.wikipedia.org/wiki/Dogecoin. Accessed: 2020-09-09.
6. “Tron” https://en.wikipedia.org/wiki/Tron. Accessed: 2020-09-09.
7. “TuringCerts.” https://certs.turingchain.tech/. Accessed: 2020-09-09.
8. “Linux Foundation” https://en.wikipedia.org/wiki/Linux_Foundation. Accessed: 2020-09-09.
9. “Hyperledger fabric.” https://www.hyperledger.org/use/fabric. Accessed: 2020-09-09.
10. “Proof-of-Authority” https://en.wikipedia.org/wiki/Proof_of_authority. Accessed: 2020-09-12.
11. “Hyperledger Fabric SDK” https://hyperledger.github.io/fabric-sdk-node/release-1.4/module-fabric-network.html. Accessed: 2020-09-12.
12. Liu P.T.S. (2016) Medical Record System Using Blockchain, Big Data and Tokenization. In: Lam KY., Chi CH., Qing S. (eds) Information and Communications Security. ICICS 2016. Lecture Notes in Computer Science, vol 9977. Springer, Cham.
13. I. Kubjas, “Using blockchain for enabling internet voting,” 2017.
14. V. Ko and A. Verity, “Blockchain for the humanitarian sector: future opportunities,” UN Office for the Coordination of Humanitarian Affairs, Digital Humanitarian Network, 2016.
15. “RSA encryption algorithm.” https://en.wikipedia.org/wiki/RSA_(cryptosystem). Accessed: 2020-09-13.