

NAR Labs 國家實驗研究院

國家高速網路與計算中心

智慧校園區塊鏈應用

葉羅堯 博士/副研究員

個人簡介

姓名：葉羅堯

現職：

國研院-國家高速網路與計算中心 副研究員
國立暨南國際大學 兼任助理教授

學歷：

國立交通大學 資訊科學與工程研究所 博士

研究領域：

區塊鏈技術、應用密碼學、車載網路安全、雲端安全、Botnet

專業證照：

- Cisco Certified Network Associate certification (CCNA)
- Linux Professional Institute Certification (LPIC LEVEL 1)
- Sun Certified Java Programmer (SCJP)
- Ethical Hacking and Countermeasures (CEHv7)
- Advanced Cloud Security Auditing For CSA STAR Certification
- Computer Hacking Forensic Investigator (CHFIv8)



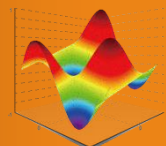
議程大綱

- 國網中心簡介
- 區塊鏈與相關發展
- 證書發展歷程
- 麻省理工Blockcerts 簡介
- 台中市政府國中小區塊鏈畢業證書PoC 簡介
 - QR code驗證之區塊鏈證書檢測平台

國網中心發展架構



應用



工程與科學



生物醫學



環境災防



社會經濟



數位文創



新興應用



雲端服務

設施即服務(IaaS)

- 實體與虛擬計算主機
- 儲存
- 學術研究網路

平台即服務(PaaS)

- 大資料平台(Braavos)
- 算圖農場
- 開放式高速計算平台(simPlatform)

軟體即服務(SaaS)

- 國研院數位服務
- 遠距學習平台(Co-life)
- 科學計算與工程模擬



核心技術

高速計算

雲端中介軟體

大資料

網路與資安

視算



核心設施



WINDRIDER

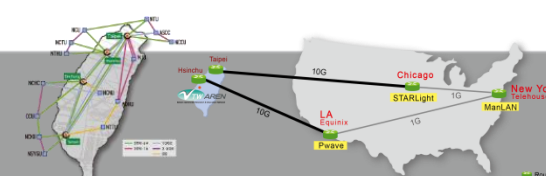
高速計算與大資料分析主機



Braavos



高效能異地儲存



高品質學術研究網路TWAREN

國網中心-高速計算服務

NAR Labs

承諾·熱情·創新



- 25,600 計算核心
- 73,728 GB記憶體
- 1074 TB巨量儲存

2011 TOP 500 第42名

2011 Green 500 第25名

2015 Top500 第445名
Green500 第297名

ALPS - Acer Cluster

2011, 177 TF

國內最大開放叢集電腦主機



IBM Cluster 1350,1350A

2007, 25 TF

分散式平行電腦叢集



Formosa 3 Cluster

2011, 9 TF

自建虛擬主機雲端服務
及台灣第一座算圖農場



Formosa 5 Cluster

2012, 90 TF

自建全台最大GPU叢集系統

760 計畫/年 3,000 帳號/年

30 大型計算專案計畫/年

106年開始建置下一代Peta主機，預定
107年7月開放服務

國網中心-儲存服務



- 儲存總容量 8.1 PB

- **30**重要計畫/年

- 腦科學、基因演算、防災、地科、氣候變遷、人文資料庫等



EMC Connectrix Director



StorageTek L5500

區塊鏈與發展未來性

NAR Labs

承諾·熱情·創新

世界經濟論壇看區塊鏈

區塊鏈的未來性



Google Cloud Joins Amazon, IBM in Serving Blockchain Clients

by Olga Kharif

2016年9月23日 下午12:00 [台北]

→ Banks to use Google data centers for tests of new technology

Expand for our
2017 Year Ahead Outlook

Blue Viewpoint
藍色觀點

智慧焦點

IBM

引領產業變革的智慧交易服務機制

區塊鏈 (Blockchain) 引領未來市場的關鍵技術

金融科技的出現，不但加速了金融服務業變革的腳步，也是推動物聯網 (IoT) 應用的關鍵推手，其中，又以區塊鏈 (Blockchain) 技術的影響性最大。瑞士達沃斯世界經濟論壇 (WEF) 更直接點名區塊鏈技術是帶動「第四次工業革命」的潛力科技之一。

什麼是區塊鏈技術呢？區塊鏈是由一套嚴謹的加密法演變而來的技術，透過複雜的公鑰與私鑰設置，系統會自動將透過區塊鏈網絡進行的金融交易資料分送到每一位參與者手中，而且，每一位參與者都只能針對自己的財產進行修改。

換句話說，透過區塊鏈技術的數位交易紀錄系統，消費者與企業再也不需要透過財力雄厚或權威的金融中

區塊鏈的四大構成要素



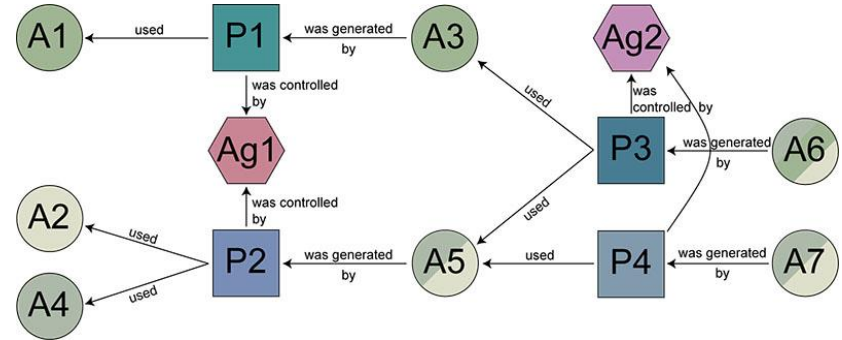
區塊鏈(Blockchain)特色

NAR Labs

承諾 · 熱情 · 創新



Consensus



Provenance



Finality



Immutability

Blockchain 已實現應用

Slock.it

https://www.youtube.com/watch?v=it2X_j-DPmA&feature=youtu.be

解決電動車充電問題

可適用Airbnb 的商業模式，但不需有集中式中介系統(一切公開化)

差異性：

建置時效

去中間化較少的手續費

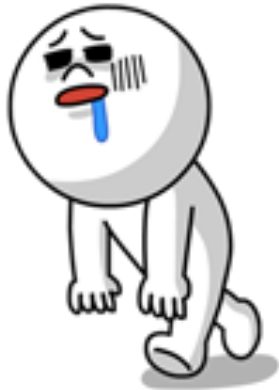
安全性

證書發展歷程

➤ 聲望

在小型的社會中，我們很容易地知道誰才是專家。

我好像生病了，應該
看一下醫生…

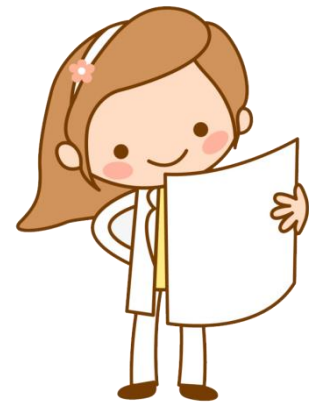


Ken

你可以找Emily阿~



Ben

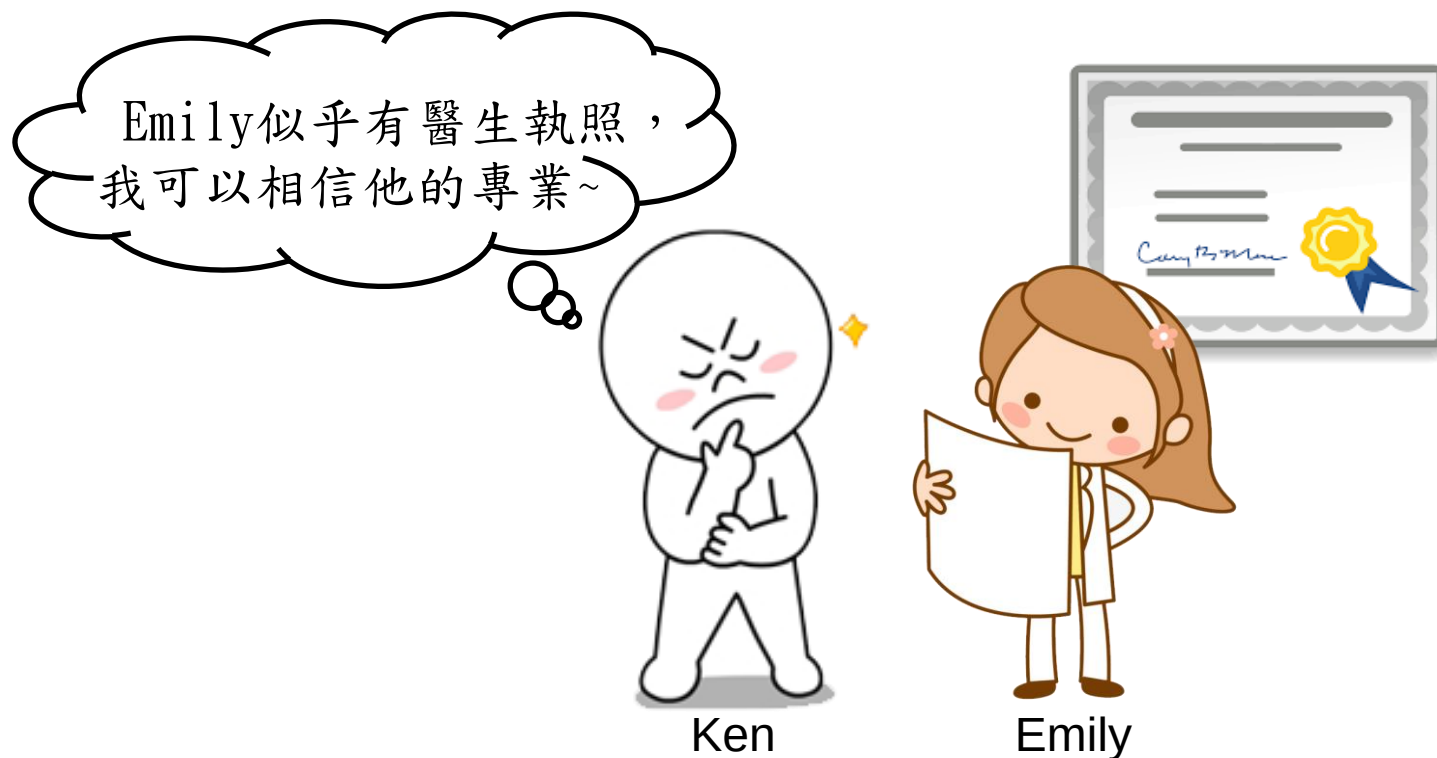


Emily

證書發展歷程

➤ 證書

隨著科技進步，人們追求更便利形式，我們需要拿出更有公信力的方式來證明自己的專長，因此，證書的需求油然而生。



證書發展歷程

➤ 現今證書的缺點

- 全權由畢業學校教務處負責產生，亦曾有發行假學歷之案例

賣假學歷助升等 三立新聞HD

黃聰亮


UNIVERSIDAD EMPRESARIAL
Costa Rica
Educación a Distancia Mundial
Distance Learning for the World

假學歷

▶ 碩士40萬
▶ 博士70萬

▶ 講師升等
15~55萬

獲利600萬

鎖定三立新聞

18:18:26 注意防曬 紫外線幾全過量級 台南PM2.5達紅色警戒

證書發展歷程

➤ 現今證書的缺點

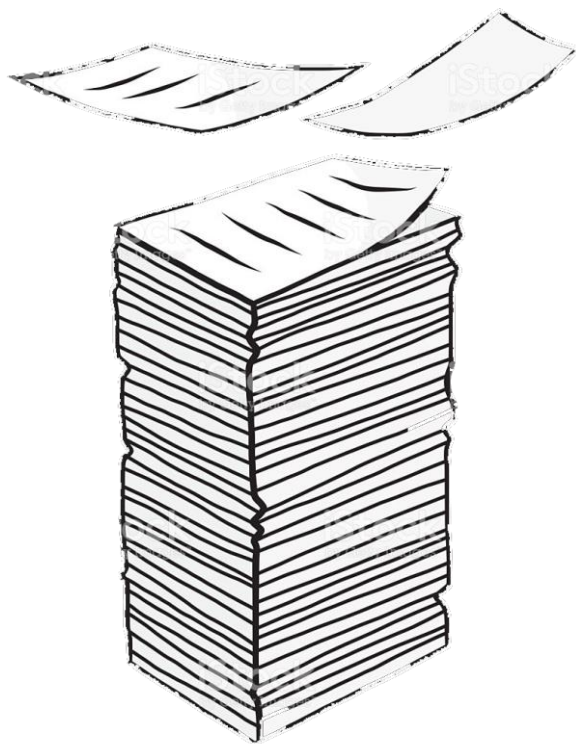
- 離校手續繁雜，當事人需要到處辦手續，過程完全由人工紙本審核簽署



證書發展歷程

➤ 現今證書的缺點

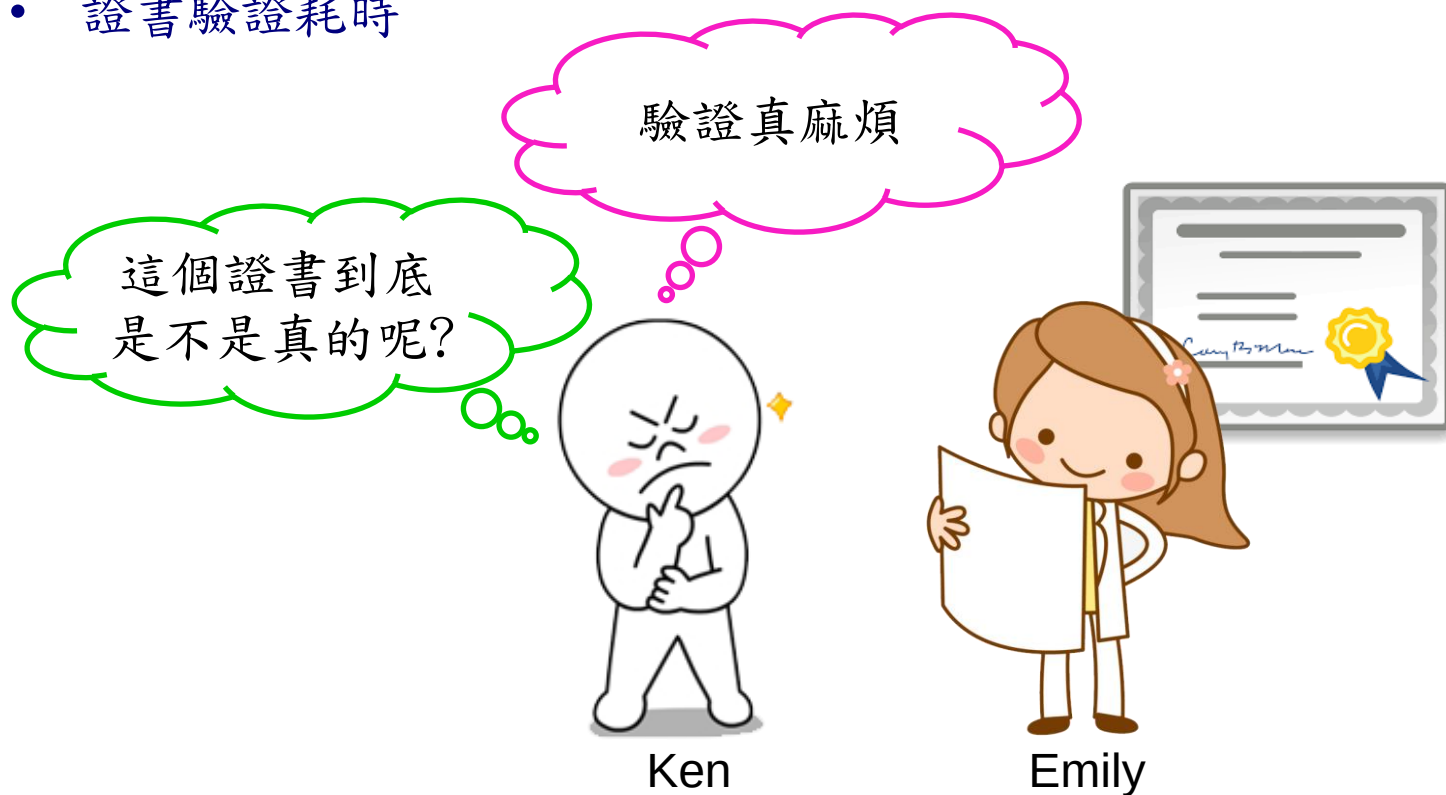
- 時間、紙張成本耗費過高



證書發展歷程

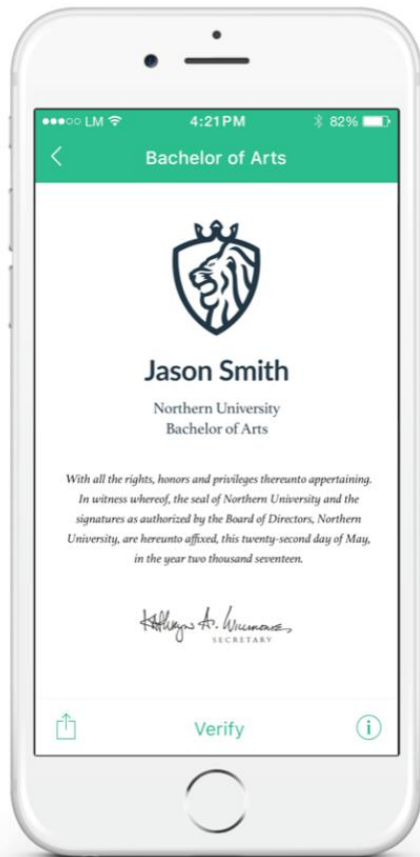
➤ 現今證書的缺點

- 證書驗證耗時



MIT Blockcerts

➤ 麻省理工學院使用Blockcerts系統頒發了111個文憑



Verify Certificate

Please enter the certificate URL below to verify its validity.

<https://auto-certificates.yourname.edu/certificate/2380d326-a402>

Verify



Bachelor of Arts

Jason Smith



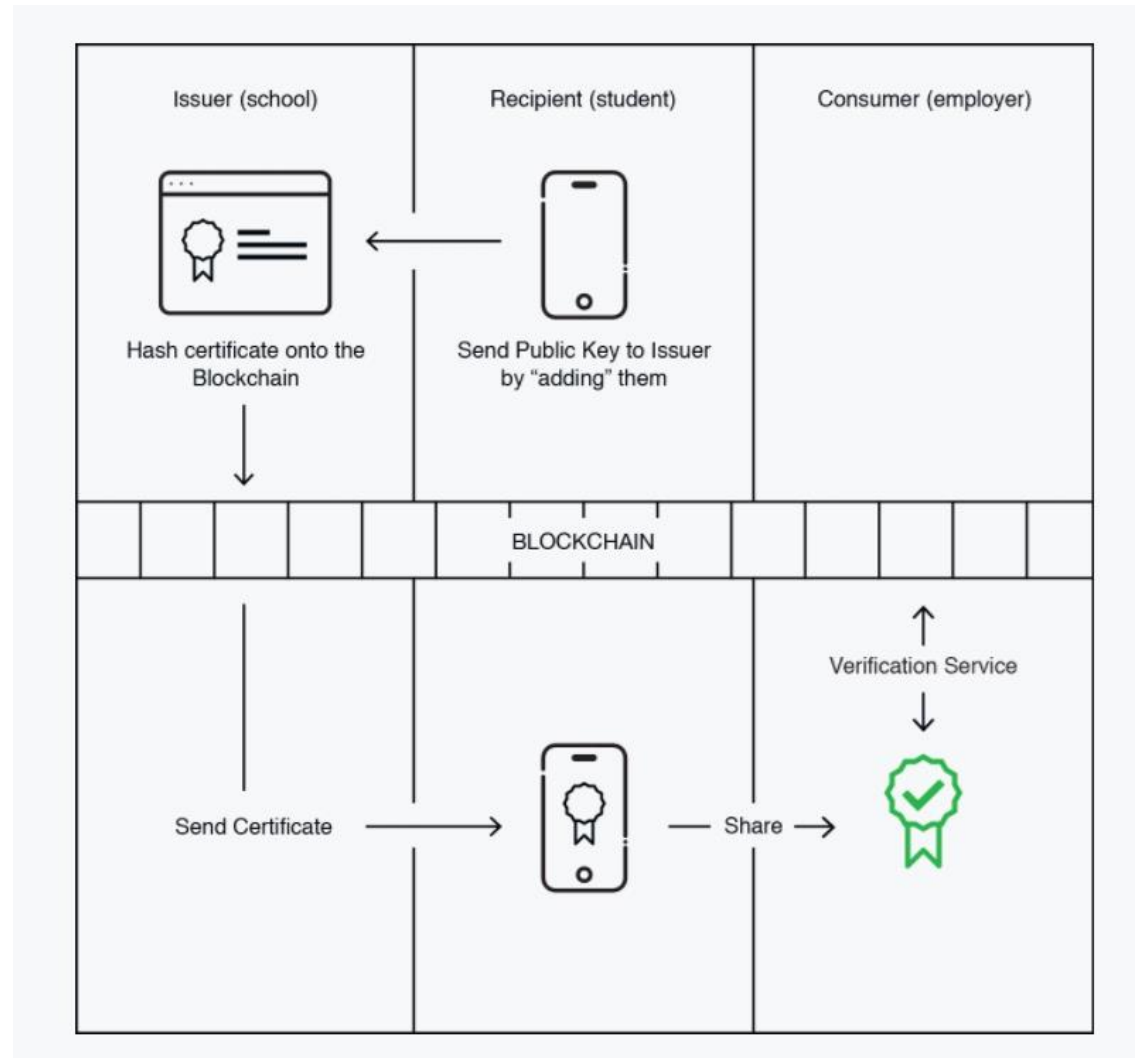
Verified

Public Key: 1H1TT15428JDS7HDFGKKAGD9e1019R1

Blockchain Address: 47651a51eaTR51g7156hCKee12980w7EA18ee18761

MIT Blockcerts

➤ 系統流程



MIT Blockcerts 特色

➤ 發起者

- 大學創建數位證書，並註冊於比特幣區塊鏈上

➤ 證書

- 證書驗證碼將公開紀錄在區塊鏈上

➤ 驗證者

- 任何人都可驗證證書，且不須issuer介入
 - (1) 利用區塊鏈不可篡改性，安全確保證書有效性
 - (2) 證書必須由特定的機構發行
 - (3) 指定對象進行認證

➤ Wallet

- 使用者可以儲存自己的證書，並安全與他人分享，例如：雇主

MIT Blockcerts 可改良之處

➤ 隱私性

- 由於建構於Bitcoin 中，可能推論出來某人的畢業學校

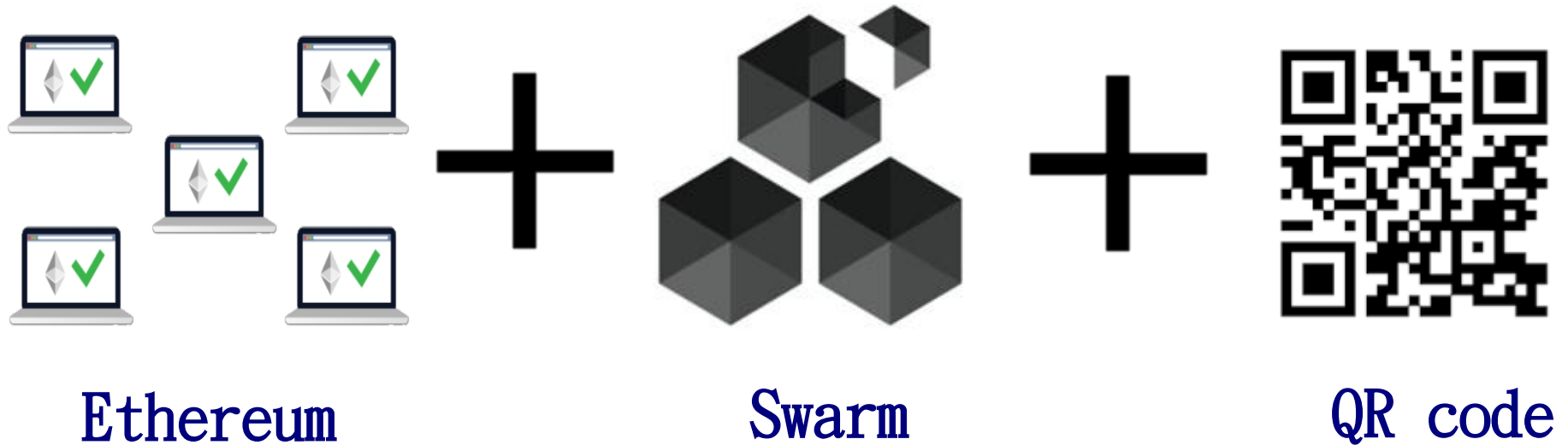
➤ 驗證方便性

- 每次驗證皆需取得「證書電子檔」，於應用環境中不甚合理

區塊鏈畢業證書趨勢

- MIT Blockcerts
- 新加坡區塊鏈畢業證書
 - 新加坡義安理工學院 (Ngee Ann Polytechnic)
- 賽普勒斯共和國
 - University of Nicosia

具QR code驗證之區塊鏈證書檢測平台



具QR code驗證之區塊鏈證書檢測平台

➤ 系統功能及服務

- 多人驗證性：以多簽形式加強證書發行安全性
- 不可竄改性：證書驗證碼儲存於區塊鏈上
- 可追蹤性：可找出證書簽署狀態
- 便利性：不須電子檔即可以 QR code 進行驗證
- 隱私性：資料以加密形式傳輸及儲存於Swarm中



學生

1. 學生申請畢業證書
/ 榮譽表現驗證



6. 下載電子檔與
QRcode



7. 學生將電子畢業證書
或提供QRcode至國中



國中招生組



2. 將申請送至
學校進行審查

5. 提供電子檔
QRcode下載點



國小

3. 將學生
畢業證書
紀錄於區
塊鏈上

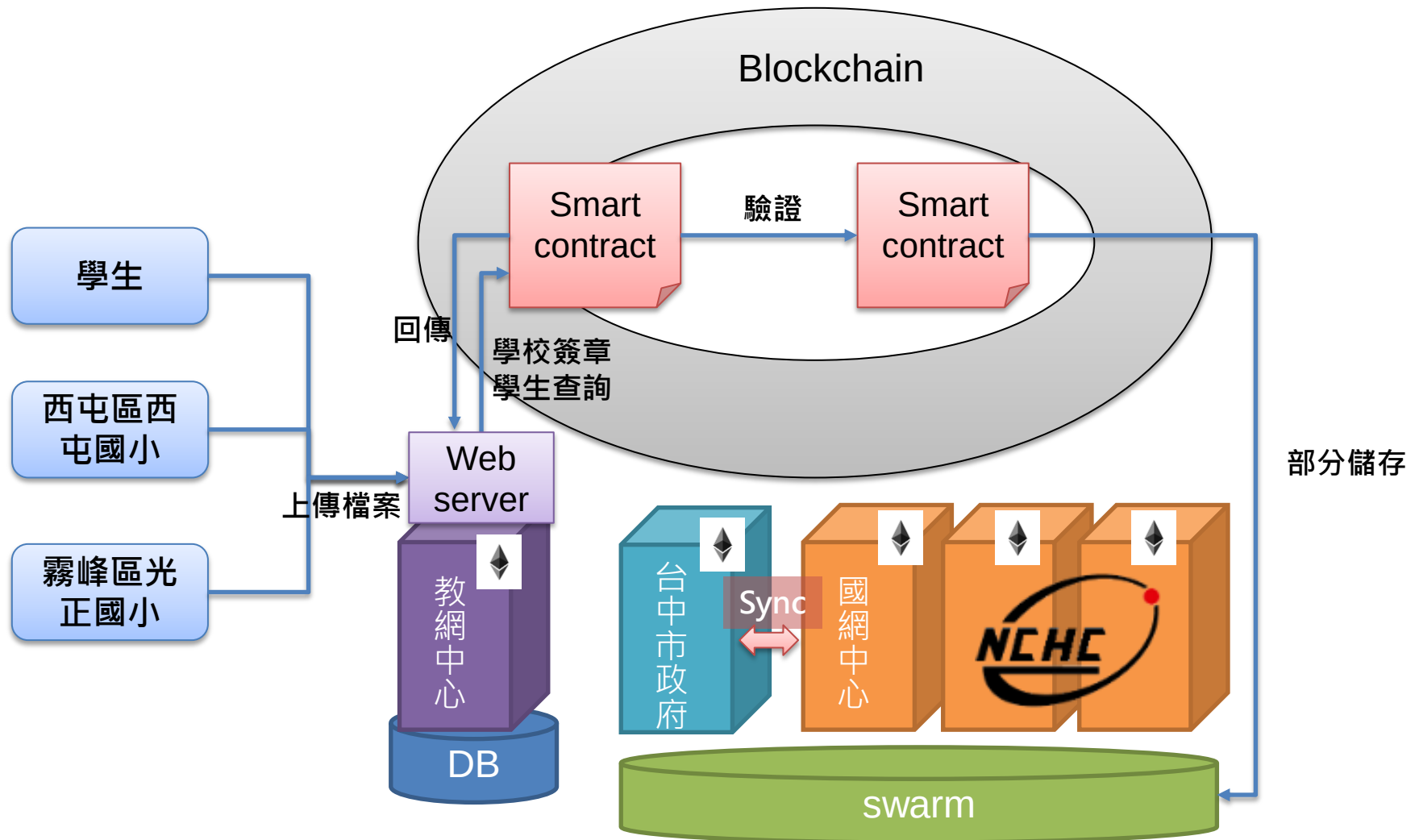
4. 取得已
簽章支電
子檔

8. 至區塊鏈進行驗證

9. 取得驗證結果



系統架構



具QR code驗證之區塊鏈證書檢測平台

➤ 發起驗證

- 創建一個JSON文件，包含姓名，地址，證書
- 將區塊鏈上傳輸的每一筆資料進行加密混淆(obfuscated)，使他人無法直接看到傳遞的內容，也無法推估此證書由誰簽署的

具QR code驗證之區塊鏈證書檢測平台

[Certificate System](#) [About](#) [Verify](#) [Contact Us](#) 333 ▾ [Logout](#)

Issue

version	1.0.0
name	
recipient	ffe5ef3e6f2b059bda7a3924b718ede3841f3277
contract	b2ed4168a045d8a35066e1704328499c0864b517
revocation	
type	School Gra ▾
description	
cert	選擇檔案 未選擇任何檔案
signSchool	
signDepartment	
signTeacher	1 ▾

具QR code驗證之區塊鏈證書檢測平台

➤ 簽署

- 指定特定對象進行簽署（至少三個）
- 發起人先自我簽署，接著送出交易，邀請其他人進行簽署
- 使用ecrecover驗證簽名

具QR code驗證之區塊鏈證書檢測平台

GEPT

version	1.0.0
name	GEPT
recipient	ffe5ef3e6f2b059bda7a3924b718ede3841f3277
contract	b2ed4168a045d8a35066e1704328499c0864b517
mapping	1649
revocation	GEPT
description	English
timestamp	2017-11-9 10:26:18
certhash	5ad0fa0a2bacf063a44cd7e5f2c7de247e6f9f5163f6d3929ab8579909f512dc
cert	



signSchool	e4df8e1b20c8bfa140e9290d94308b475ace6c31
signDepartment	
signTeacher	1 dafd09b505546815d5eecad8f754d3da6058fbde

[選擇檔案](#) 未選擇任何檔案

Sign

具QR code驗證之區塊鏈證書檢測平台

➤ 追蹤

- 若簽章已被驗證成功則智慧合約將更改其狀態為true

Result

recipient	true
signSchool	false
signTeacher1	false

具QR code驗證之區塊鏈證書檢測平台

➤ For QR code 儲存程序

- 將JSON檔拆剪並加密
- 上傳到Swarm

name	333
recipient	ffe5ef3e6f2b059bda7a3924b718ede3841f3277
contract	b2ed4168a045d8a35066e1704328499c0864b517
mapping	2101
revocation	333
description	333
timestamp	2017-11-8 13:48:57
certhash	5ad0fa0a2bacf063a44cd7e5f2c7de247e6f9f5163f6d3929ab8579909f512dc
cert	
signSchool	e4df8e1b20c8bfa140e9290d94308b475ace6c31
signDepartment	
signTeacher	1
	dafd09b505546815d5eecad8f754d3da6058fbde
qrcode	
download	

具QR code驗證之區塊鏈證書檢測平台

➤ QR code/JSON驗證

- 掃描QR code則可解密集取得完整JSON
- 從區塊鏈取得證書驗證資訊，進行驗證
- 顯示證書資訊內容

Verify(JSON)

Please upload JSON file.

3/3 Verified

選擇檔案 Yn2TDe0ladlHX...TCrIKFZiBt5g

具QR code驗證之區塊鏈證書檢測平台

➤ 系統特色

- 資料傳輸時加密混淆處理，避免惡意使用者知道其他人資訊
- 可透過QR code驗證學生畢業證書的正確性（MIT證書系統並未提供）
- TCEB（台中市教網中心）為證書發行人，但無法追溯到學校
- 學生查詢畢業證書資訊、畢業證書進度確認
- 純分散式儲存，教務處、驗證伺服器、Swarm皆無儲存完整證書檔案

配合國小畢業證書發行

➤ 由學校代表學生發起

- 批次發行

➤ 帳號管理

- OpenID

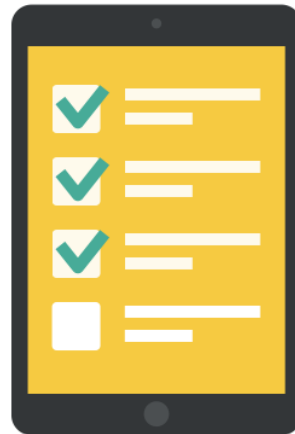
具QR code驗證之區塊鏈證書檢測平台

➤ 未來展望

- 結合學生其他特殊表現證書



- 課程回饋



- 與人力資源部門合作



具QR code驗證之區塊鏈證書檢測平台

