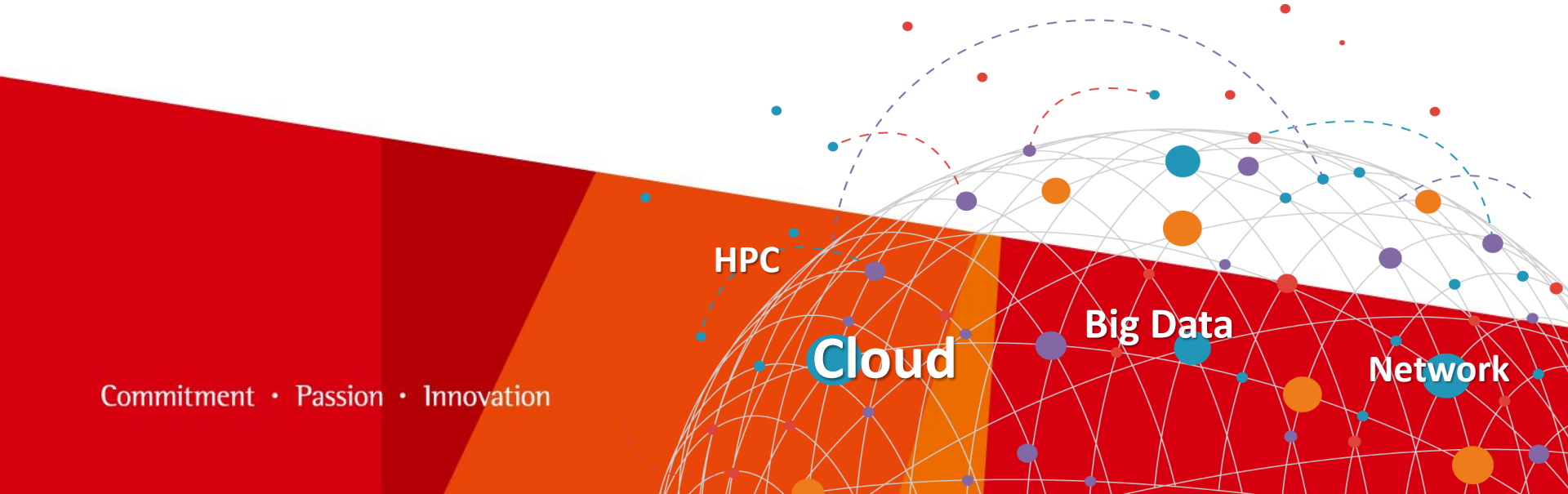
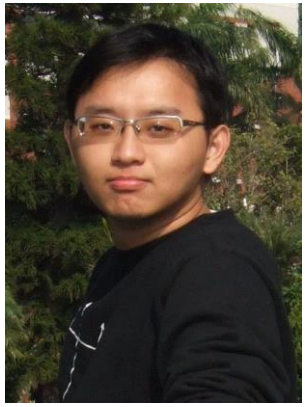
NARLabs
National Applied Research Laboratories
National Center for
High-performance Computing

區塊鏈概念與證書查核系統

葉羅堯 博士
國家實驗研究院國網中心 副研究員
國立暨南國際大學 資訊管理系 兼任助理教授



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
    應用技術發展組 副組長/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)

大綱

- 區塊鏈概念簡介
- 區塊鏈應用實例介紹
- 國網中心區塊鏈服務

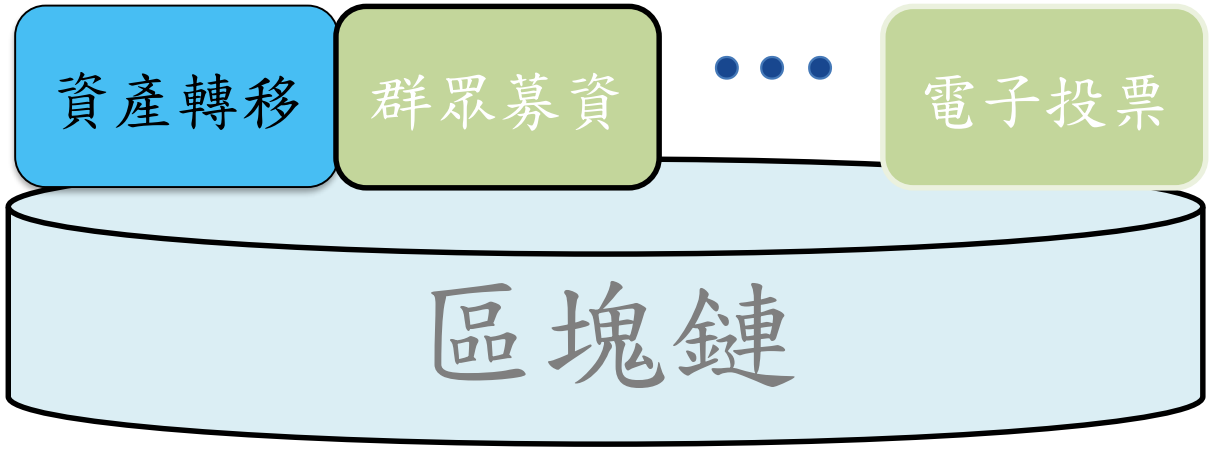
- 區塊鏈概念簡介

區塊鏈 vs. 比特幣

NARLabs

區塊鏈 ≠ 比特幣

比特幣 → 區塊鏈



為何有比特幣的由來

NARLabs

2008年Satoshi Nakamoto(中本聰)覺得現有的「集中式」銀行很惡質，「(跨國)轉帳」的問題一直都不解決

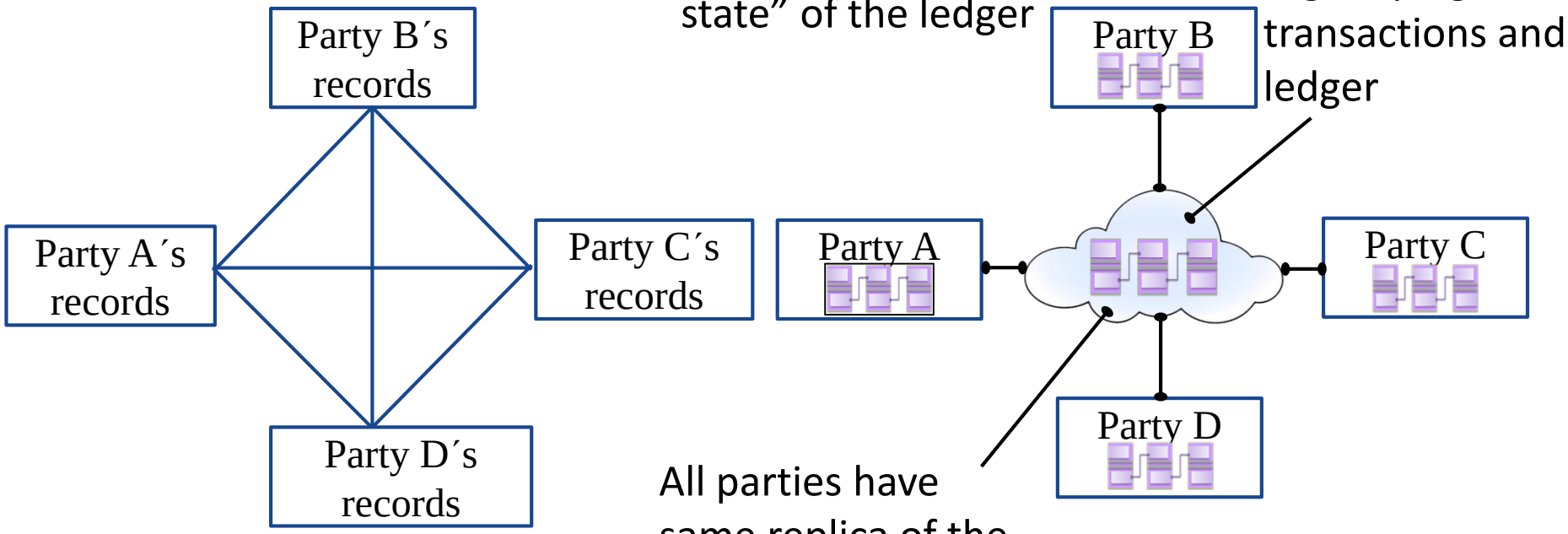
慢

- 需經由多方銀行相互轉帳

貴

- 經濟學人估計在2014年全世界銀行對客戶收取約 1.7 Trillion（兆）的轉帳手續費
- 銀行手續費約佔2014年全世界經濟活動的2%

傳統帳本 vs. 區塊鏈帳本

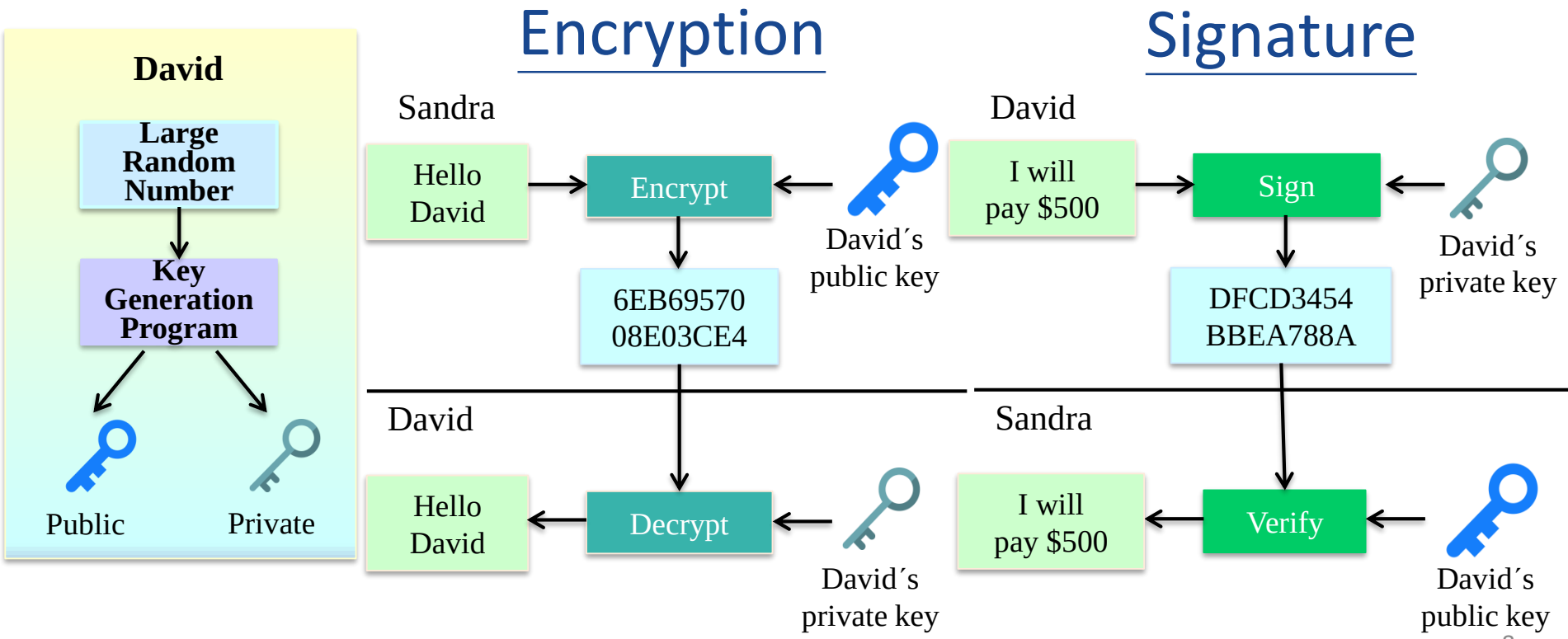


<Conceptual ledger>

公開金鑰密碼系統概念

NARLabs

- 區塊鏈安全性基礎：每個帳戶皆需有對應的公、私鑰
- 區塊鏈以「簽章」(Signature) 方式來證明「擁有權」



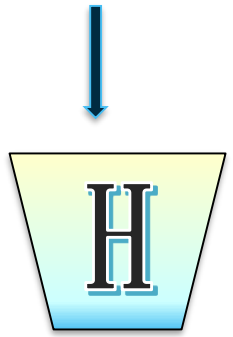
雜湊函數(Hash Function)

NARLabs

➢ 雜湊函數 (Hash Function)

- ✓ 可輸入任意長度訊息，並產生固定長度的「指紋」
- ✓ 不需要KEY
- ✓ 僅可「單向」計算，回推不易
- ✓ EX: SHA1, SHA256, Keccak 256

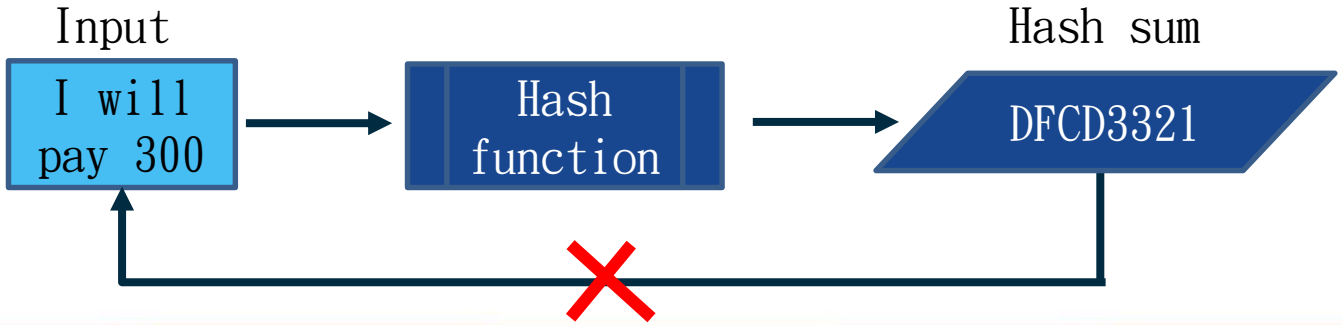
Message M



Message Digest D
D=H(M)

➢ 應用範圍 Applications

- ✓ 訊息驗證碼(MAC)的產生
- ✓ 數位簽章、密碼檔儲存、資料完整性、隨機數產生器



比特幣交易-實例步驟

NARLabs

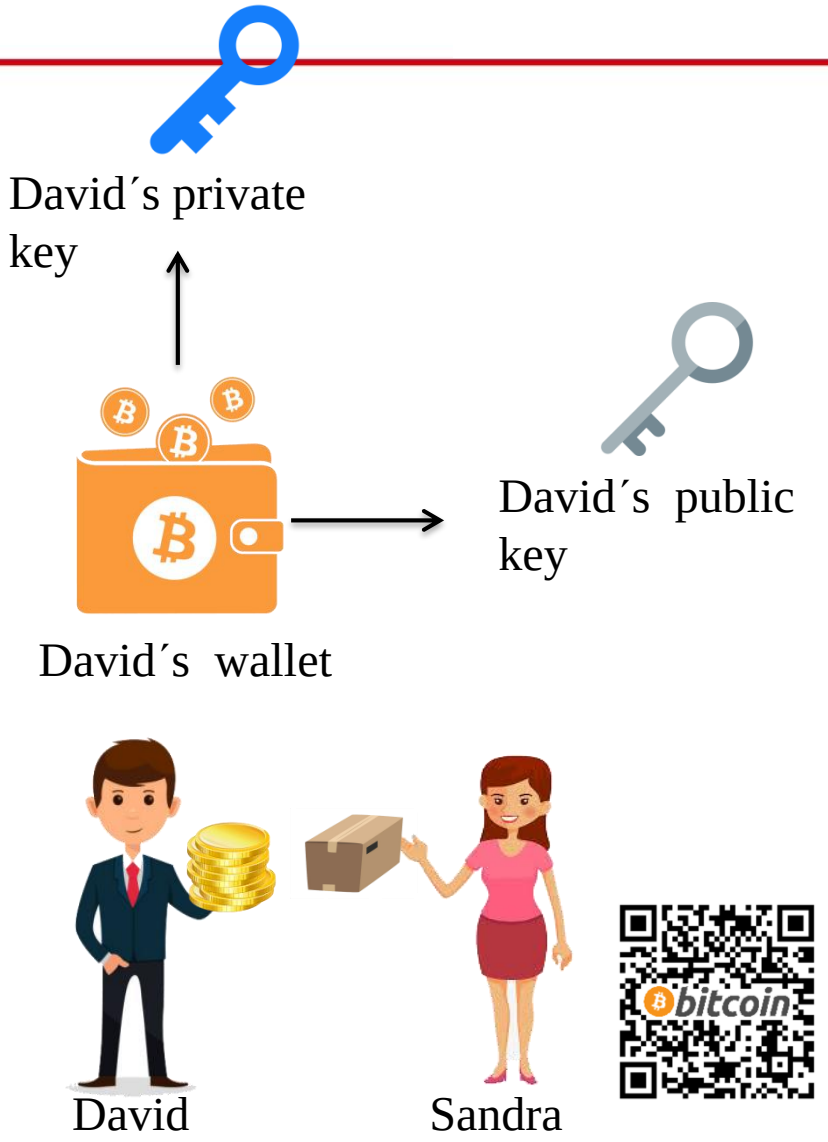
(1) Sandra 給 David 看她的 Bitcoin address or QR code

(2) David 輸入「位址、金額」並以自身的私鑰簽章後送出

(3) Sandra 看到手機裡有「收入」(pending 狀態)，尚未確認。

(4)約十分鐘過後，手機上表示「收入」已完結(finalized)，確認成功。

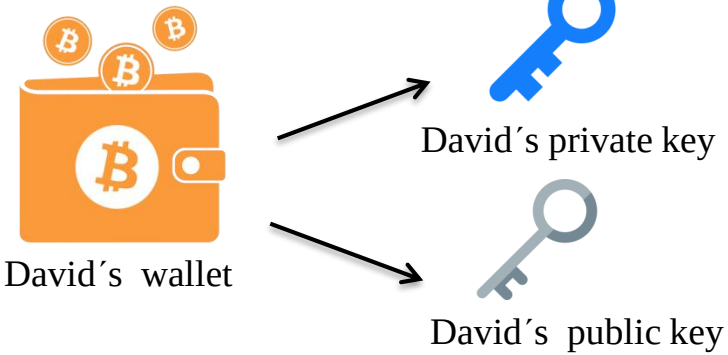
➔ **當金額大時（官方比特幣客戶端軟體)，其實要約60分鐘後才更可確認錢不會被取消（沒有被攻擊）**

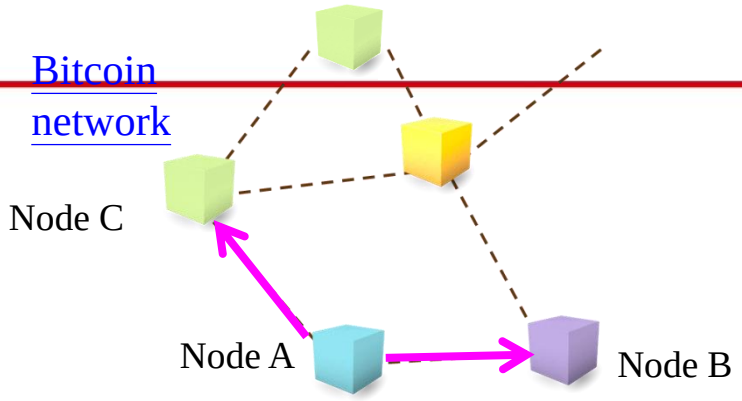


比特幣交易驗證

NARLabs

➢ 想要轉帳時，節點需要做什麼呢?





<Broadcast message>

David → Sandra 5 BTC

Digitally signed transaction

David´s public key

David → Sandra 5 BTC

Transaction request message

David´s private key

David → Sandra 5 BTC

Digitally signed transaction

Broadcast to the Bitcoin network

交易驗證重點步驟（由其他所有 nodes 執行）

1. 驗證 public key 與signature 是否可相符
2. 確認 David 的帳戶有足夠的Bitcoin.
   若「不正確」，則丟棄此訊息並終止；
   若「正確」，則存入自己的「交易池(transaction pools)」中，並執行下一步。
3. 傳播此交易訊息給鄰近節點

交易

紀錄

交易池

- Alan → Rachel 1 BTC
- Greg → Aaron 4 BTC
- Leo → Yuri 1 BTC
- Milo → Jim 2 BTC
- Tiffany → Cara 5 BTC

選擇交易

BLOCK #1304

Block ID

????

Previous Block

Kckj86khsd03

.....

Transactions

Erin → Helen 1 BTC

Joy → Myra 5 BTC

.....

Brain → Jane 2 BTC

挑選交易並寫入候選區塊

#1302

- Lisa → Sandra 2 BTC
- Mary → John 3 BTC
- Tom → Tony 3 BTC
- Brian → Jenny 2 BTC

#1303

Kckj86khsd03

- Alice → Janice 2 BTC
- Polly → Ivy 2 BTC
- Bella → Amy 1 BTC
- Alison → Flora 5 BTC

#1304

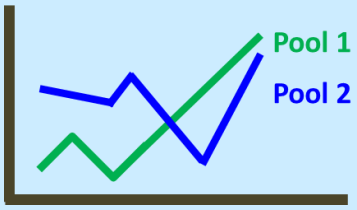
jwif83nsdke9

- Erin → Helen 1 BTC
- Joy → Myra 5 BTC
- Betty → Janet 2 BTC
- Brian → Jane 2 BTC

比特幣區塊鏈

產生新區塊

挖礦比賽



算力↑ 機率↑

接上獲選者的候選區塊

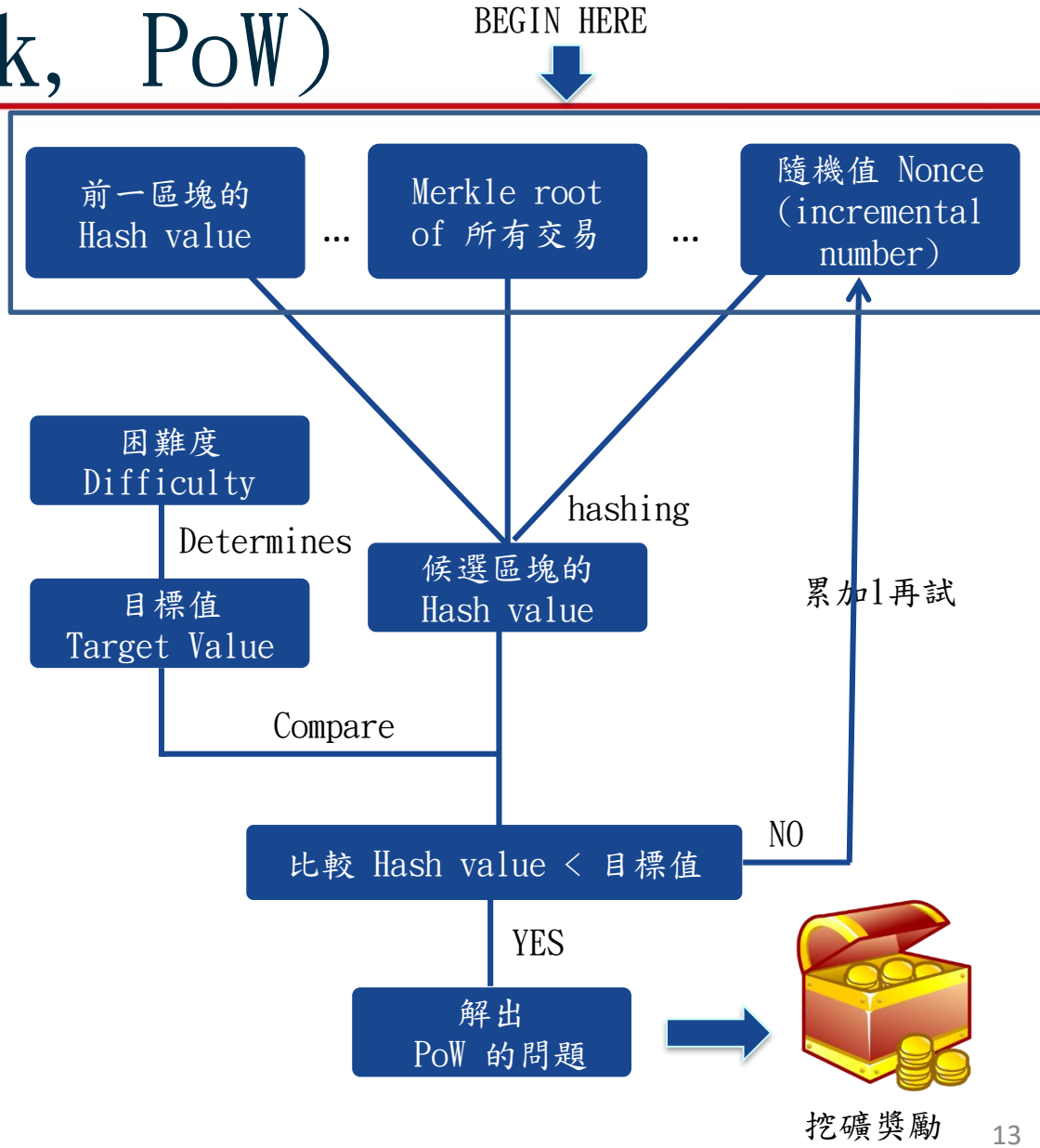
區塊鏈節點（full node）

比特幣挖礦 (Proof of Work, PoW)

NARLabs

比特幣區塊標頭 (Block header)

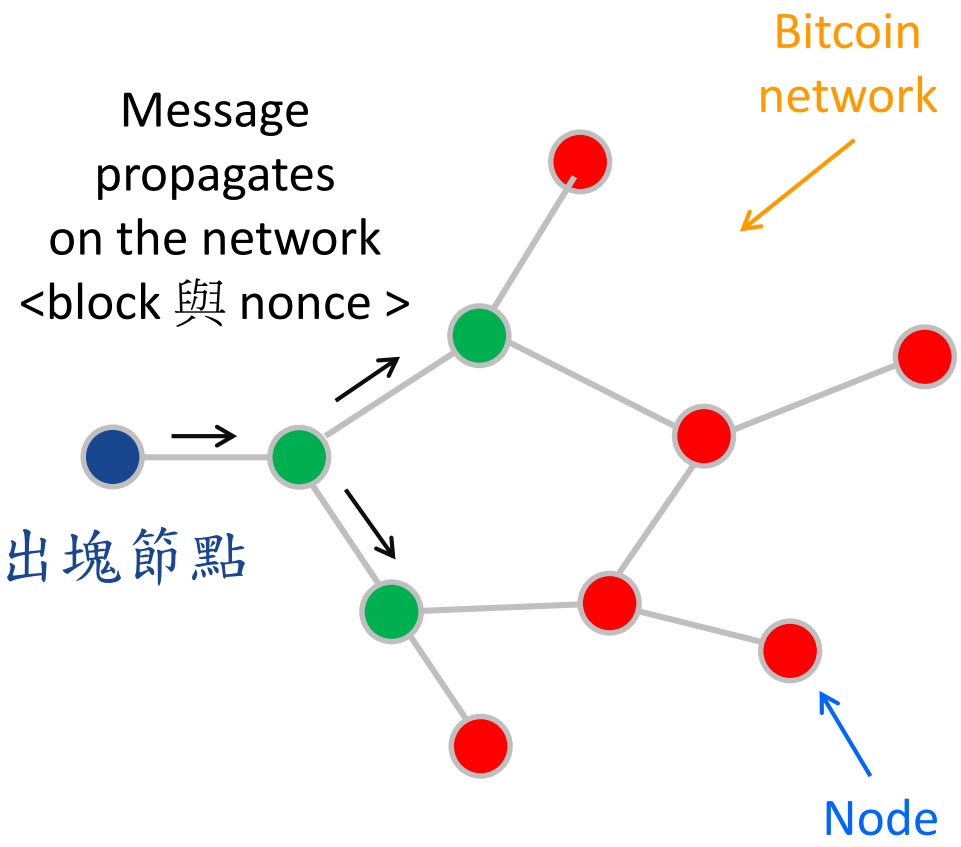
- 計算一個「隨機值」來符合預訂的困難度➔讓作弊者成本、難度變高
- 決定由「誰」來編區塊(選交易)
- 選出的節點「背書」新區塊所含交易內容正確性
- 給予獎勵



挖礦成功後帳本變化

NARLabs

- 當有「區塊」被「挖礦成功」節點驗證成功時，則會有下列變化



BITCOIN TRANSACTION REQUEST MESSAGE

"David sends 5 BTC to Sandra"

David → Sandra 5 BTC

LEDGER

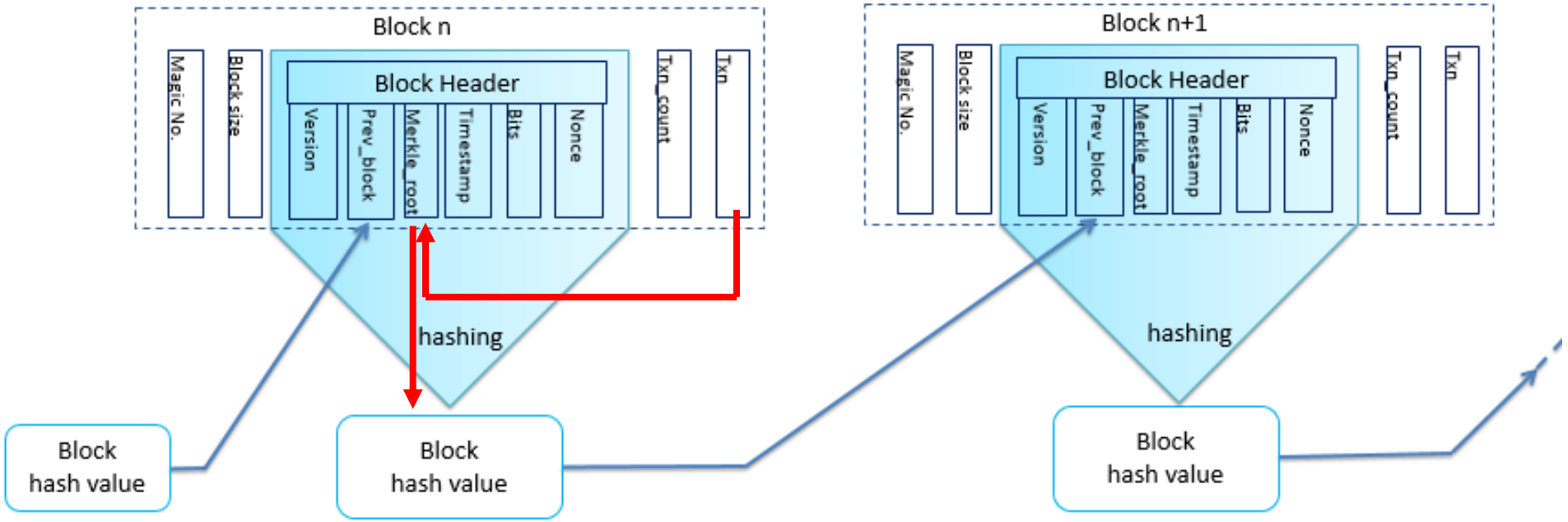
Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23
…	…

LEDGER

Account owner	Value
Mary	4
John	56
Sandra	88
Lisa	16
David	182
Brian	23
…	…

為何有「鏈」的概念

NARLabs



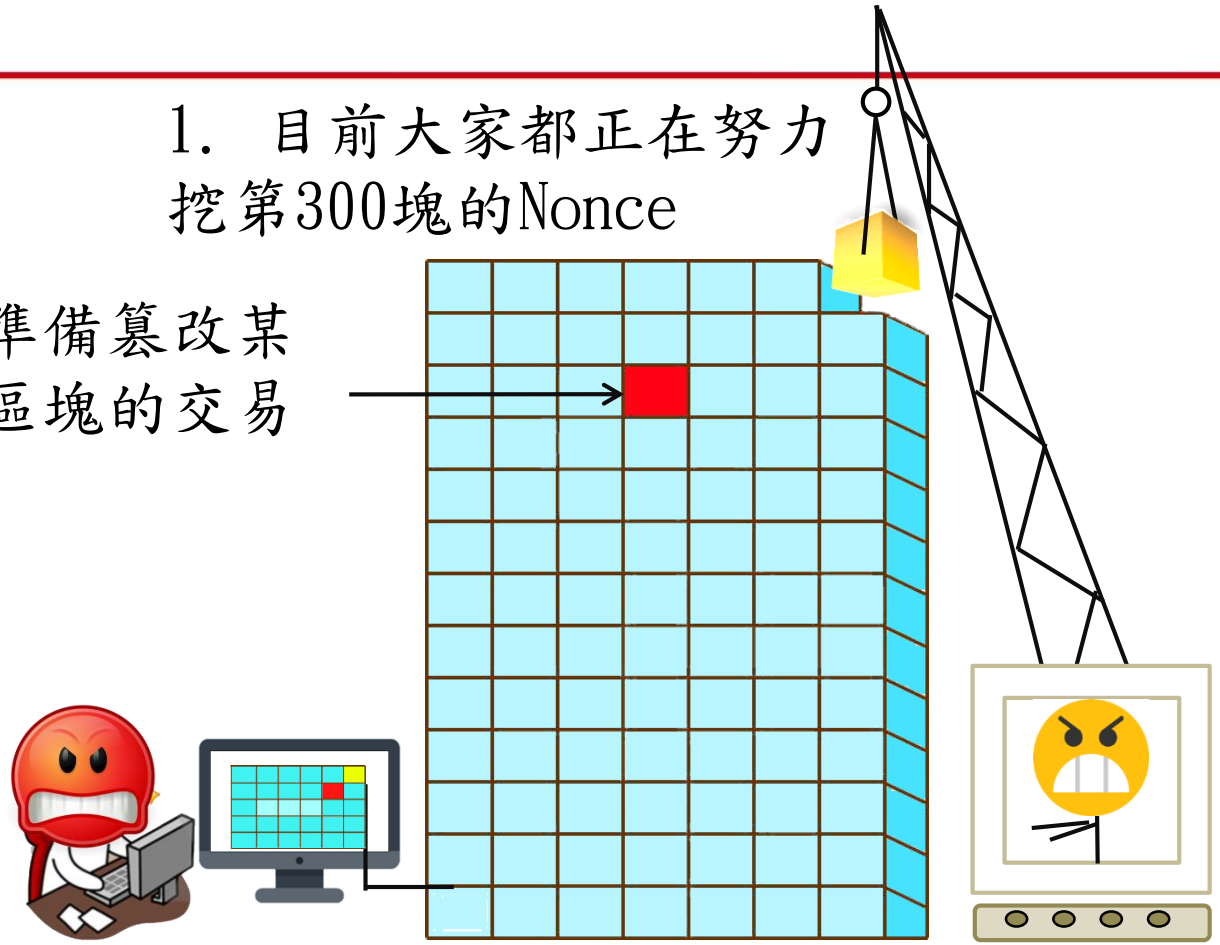
區塊鏈不可篡改性強度

NARLabs

1. 目前大家都正在努力挖第300塊的Nonce

2. 攻擊者正準備篡改某個存於第283區塊的交易

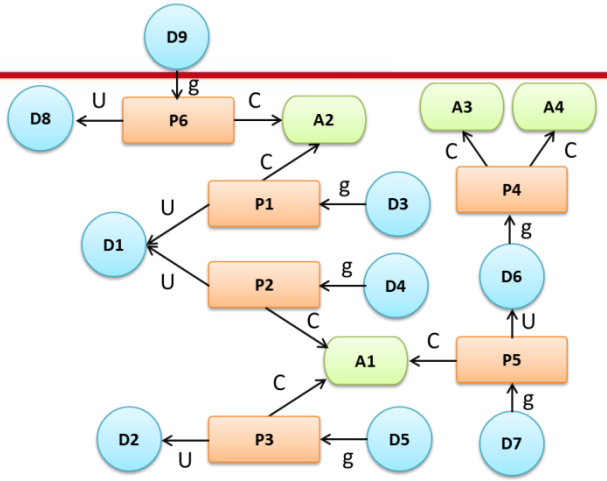
3. 若攻擊者要「合法地」篡改交易，則需要先重算283~299的Nonce



4. **更重要的是，攻擊者還必須搶到，第300塊的Nonce**，才可以讓其他節點相信他的 chain 是最長的。
(總結: 攻擊者必須有超過其他 miners 18倍的計算能力)

比特幣區塊鏈(Blockchain)特色

共識
Consensus



溯源
Provenance

假名制
Pseudonymous

不可篡改性
Immutability

知名開源區塊鏈

NARLabs

	bitcoin	ethereum	HYPERLEDGER FABRIC	IOTA
種類	Permissionless	Permissionless	Permissioned	Permissionless
共識演算法	PoW	PoW (Ethash), PoS	Solo, Raft, SBFT	Coordinator (current)
共識最終性 (finality)	No	No	Yes	No
資料隱藏性	No	No	Yes	No
攻擊數量	51% attack	51% attack	1/3 節點	34% attack
安全假定	No needed	No needed	Trusted validator nodes	No needed
交易產量	7 TPS	20TPS (8-15 TPS)	Thousands TPS	7-12 TPS (Coordinator)

Source: [2]

以太坊簡介

NARLabs

智慧合約（Smart Contract）

Conditional purchase

CONTRACT 

Holder：Sandra
Seller：David

The holder is entitled to purchase 150 shares of CRD Inc from the seller at a defined price of $30 per share.

The contract expires at March 28, 2019.

將「邏輯條件」轉為程式碼

以傳入「參數」後則可自動執行

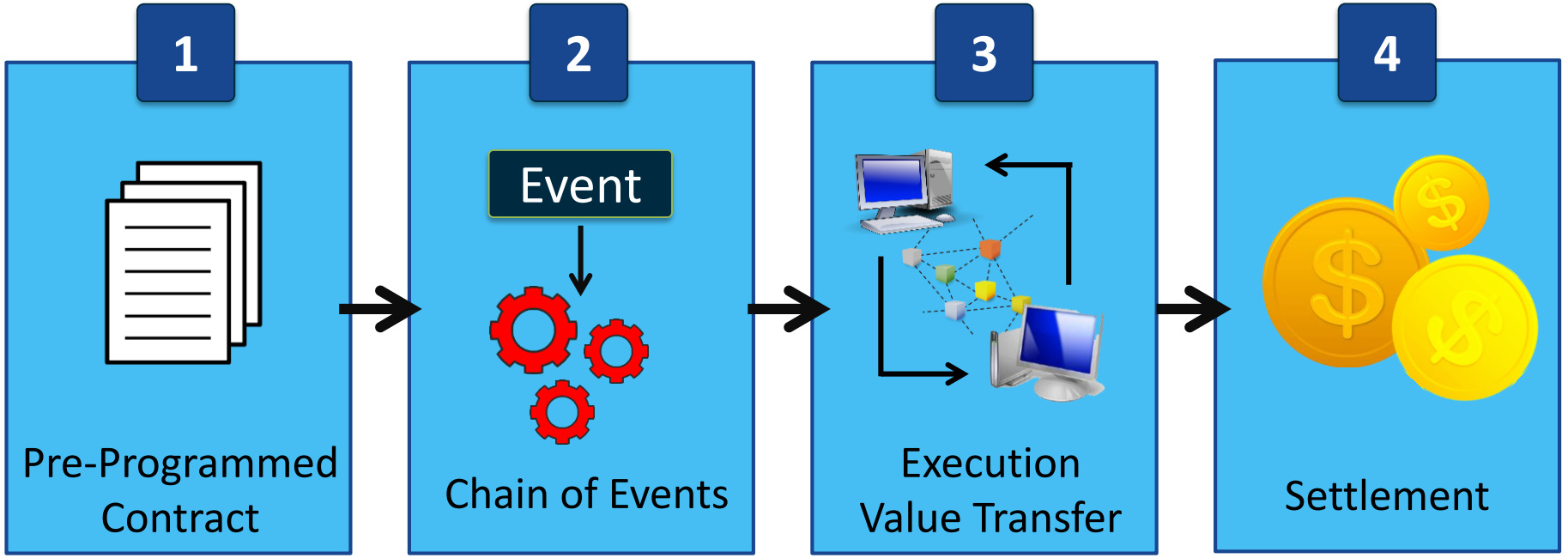
```
Pragma solidity ^0.4.20;
contract Purchase (
    uint strikePrice = $50
    string holder = Sandra
    string seller = David
    uint asset = 150  // shares of CRD
Inc.
   string expiryDate = March 28th, 2019

Function exercise() returns (bool){
    If Message Sender = holder,
        and
    If Current Date < expiryDate, then
        holder send($3,000) to seller, and
        seller send(asset) to holder
         return true;
          .....
}
```

以太坊簡介

NARLabs

智慧合約運作流程



千萬不要覺得區塊鏈是全能的!

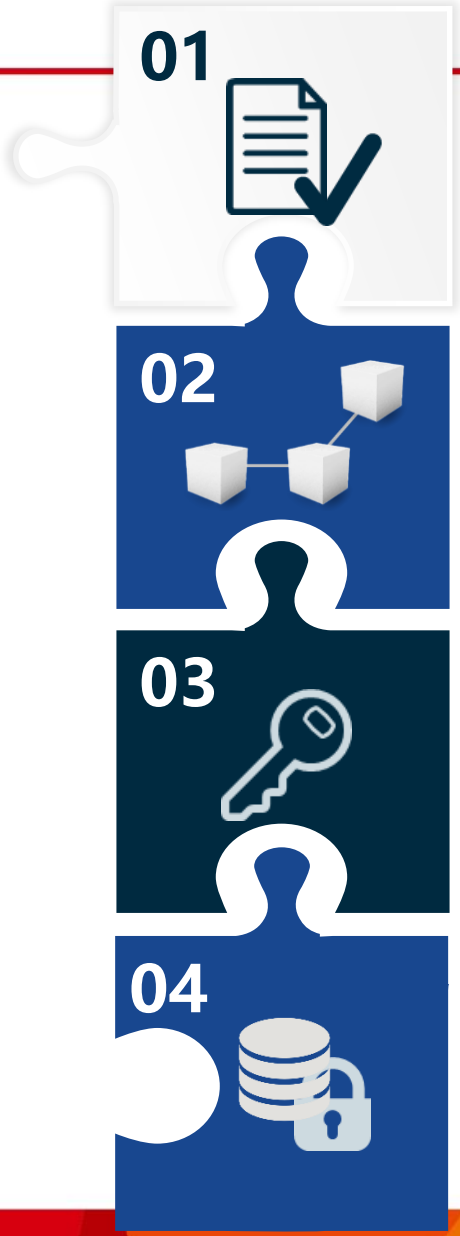
傳統區塊鏈技術並不適合：

- 容易找到「集中式管轄單位」的環境
- 需要高效率（毫秒級)交易
- 可直接以分散式資料庫取代的案例
- 大資料量儲存需求（有可能從其他方式補足）
- 高隱私性需求（有可能從其他方式補足）
- 具資料刪除性需求（ex: GDPR）

1. 跨組織分享（中介者不易找尋）
2. 建立自動化執行信任（智慧合約）
3. 強調資料不可篡改性
4. 獎勵機制需求

區塊鏈專案應用考量因素

NARLabs



- **區塊鏈 DApp 資料輸入需額外驗證**

- **聯盟區塊鏈節點安全性**
  - 節點數量
  - 驗證節點數量、安全強度

- **區塊鏈私鑰議題**
  - 儲存
  - 遺失

- **區塊鏈資料儲存、隱私議題**
  - 智慧合約內容公開
  - 資料加密、儲存方式
  - GDPR 可刪除權

• 區塊鏈應用實例介紹
–以臺中市政府國小畢業證書為例


獨家
民視新聞台 HD
民視新聞 FTVNEWS HD
假學歷應徵工作屢見不鮮 企業與人力銀行防不勝防

National

Fake diploma? Florida candidate apologizes, stays in race

By **Associated Press**
August 13

TALLAHASSEE, Fla. — A Republican candidate for the Florida Legislature is apologizing for saying she had a college degree that she didn't complete, but says she will still stay in the race.

State House candidate Melissa Howard last week posted a photo of herself with a Miami University diploma after being accused of lying about her degree, but on Monday she said she made a mistake.

It's also a mistake that might be a crime — it's a first-degree misdemeanor in Florida to forge a diploma.

Most Read World

1 In horrifying detail, women accuse U.S. customs officers of invasive body searches


2 Pope Francis: 'No effort must be spared' to tackle Catholic Church's abuses


3 A woman fell from her cruise ship — then spent 10 hours treading water


4 Manafort jury begins third day of deliberations


Fake Diplomas Reflect Indonesia's Broken Education System

Jessie Prasetya *Apr 25, 2017* Education, Scams In The City **Comments Off On Fake Diplomas Reflect Indonesia's Broken Education S** ♡6

With chop shops camouflaged as "foreign-licensed" universities or "economic institutes", the demand for fake diplomas continues to thrive in Indonesia.

Around the world, many businesses, organizations and institutions don't officially recognize university diplomas from Indonesia. Part of the reason for this is the country's prevalence of counterfeit degrees and a lax rule of law that allows people with enough money to simply buy degrees from corrupt university officials. This dynamic often makes it difficult for honest local graduates to get employed outside the country, but it also leads to Indonesia's students aiming to attend university abroad if they hope to truly invest in their futures.

The fake diploma scam is nothing new in Indonesia. It's been around for years, but the trend came

#News #Technology

MIT Introduces Digital Diplomas

Some of the technology institute's graduates can now choose to receive secure virtual credentials protected by block-chain technology.

By Lindsay McKenzie // October 19, 2017

2 COMMENTS

The Massachusetts Institute of Technology is offering some students the option to be awarded tamper-free digital degree certificates when they graduate, in partnership with Learning Machine. Selected students can now choose to download a digital version of their degree certificate to their smartphones when they graduate, in addition to receiving a paper diploma.

Using a free, open-source app called Blockcerts Wallet, students can quickly access a digital diploma that can be shared on social media and verified by employers to ensure its authenticity. The digital credential is protected using block-chain technology. The block chain is a public ledger that offers a secure way of making and recording transactions, and is best known as the underlying technology of digital currency Bitcoin.

A news release Tuesday described how MIT has been thinking about using block-chain technology to secure digital credentials for the past two years. In 2015 Philipp Schmidt, the director of learning innovation at the MIT media lab, began issuing nonacademic digital credentials to his team, but he

THE WALL STREET JOURNAL.

Blockchain May Offer a Résumé You Can Trust

Colleges and tech companies are using the digital ledger to develop easily verifiable diplomas and employment records

By Henry Williams

March 11, 2018 10:02 p.m. ET

Employers have struggled for years with the question: How do I know these job candidates are telling the truth about their background?

New assurance may come from a surprising place: blockchain technology.

A handful of educational institutions and technology companies are working on developing trustworthy, quickly verifiable digital diplomas...

From The Experts →

The Six Biggest Mistakes Multinationals Make in China

The Problem With Popular Employees

How Leaders Can Stop Employees from Deliberately Hiding

區塊鏈證書查核系統

本平台為國家高速網路與計算中心區塊鏈團隊所開發，為配合台中市政府「智慧校園」之推廣，以此畢業證書區塊鏈驗證系統，提供台中市中、小學試用。

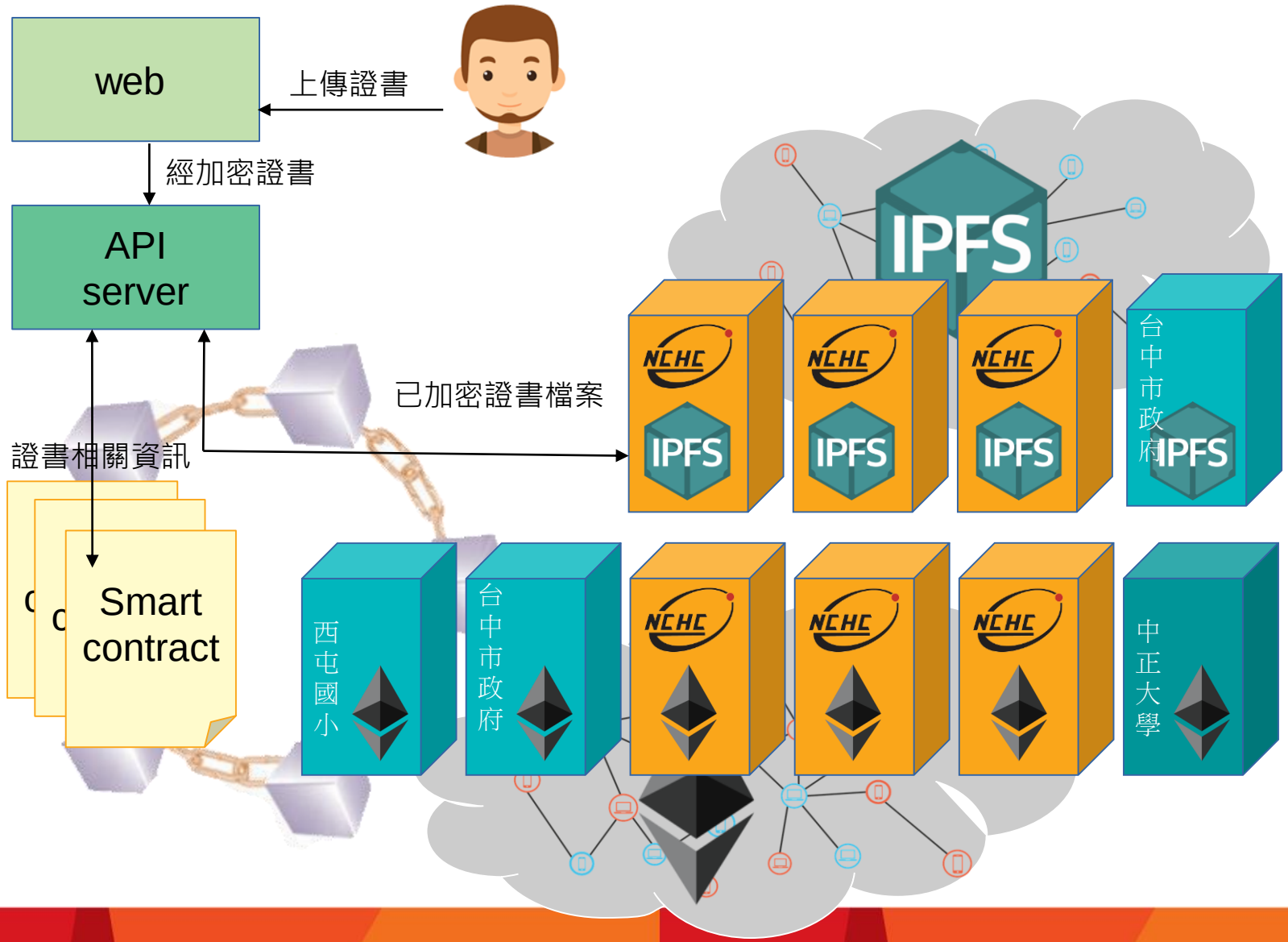
NARLabs

區塊鏈證書查核系統

Why Blockchain Certificate Proof System?

- 安全性
  - 改良資料庫管理員議題(可更新10年前資料而不被發現)
- 可用性
  - 改良集中式資料庫可用性(硬體故障等)
- 便利性
  - 快速查核證書合法性
  - 無紙化

系統架構圖


web
上傳證書
經加密證書
API server
已加密證書檔案
證書相關資訊
Smart contract
IPFS
NCHC
台中市政府
西屯國小
中正大學

不可竄改性 + 便利性 + 隱私性

Ethereum + QR code + IPFS

不可竄改性

- 採用以太坊(Ethereum)作為底層技術，利用區塊鏈的「不可竄改性」來確保證書的真實性

- 防止現有管理員新增十年前畢業記錄

便利性

- 提供電子檔與QR code 讓驗證者能快速進行驗證

證書詳細資訊

與證書相關的資訊

證書ID：	58999204
發行版本：	1.0.0
發行日期：	2018/06/11 16:57:37
發行名稱：	mycert
描述：	certtest
擁有人位址：	0xfb46bc13130be5bc1ad5d15dd3d704ad77774c78
發起人位址：	0xc305b68e32fb5c9033f30b1d1edc68221bea7801
簽署人位址：	0xc305b68e32fb5c9033f30b1d1edc68221bea7801

掃描驗證

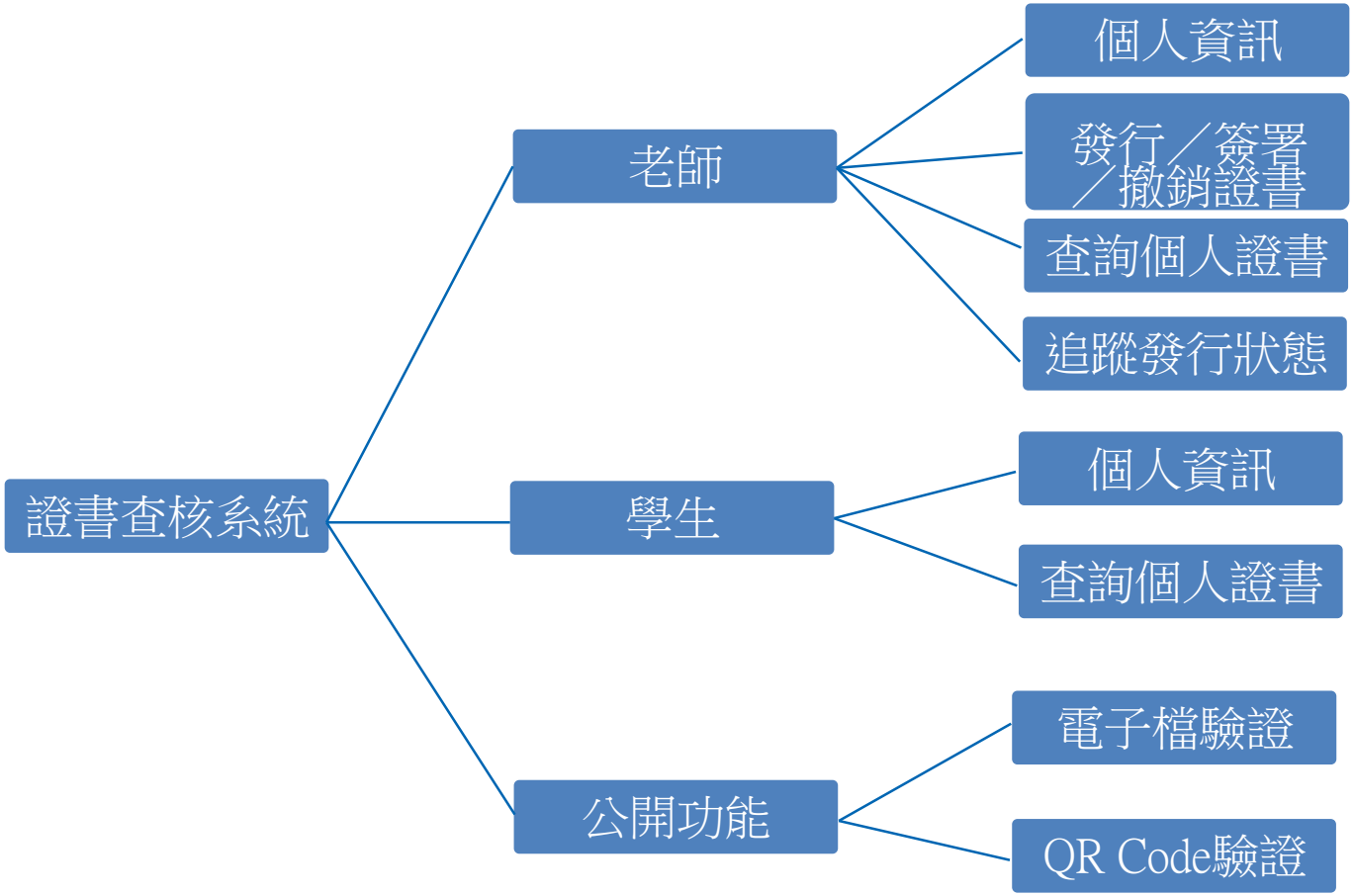
隱私性

- 加密：將資料以AES技術加密並儲存於P2P 儲存協定IPFS中。
- 浮水印：驗證者取得之證書上有「本檔案僅供查驗」以及時間之浮水印。
- 限時驗證：使用者下載電子檔與QR code 具有時效性，必須於期限內查驗證書，逾期則失效必須重新申請。［國網中心獨家研發］

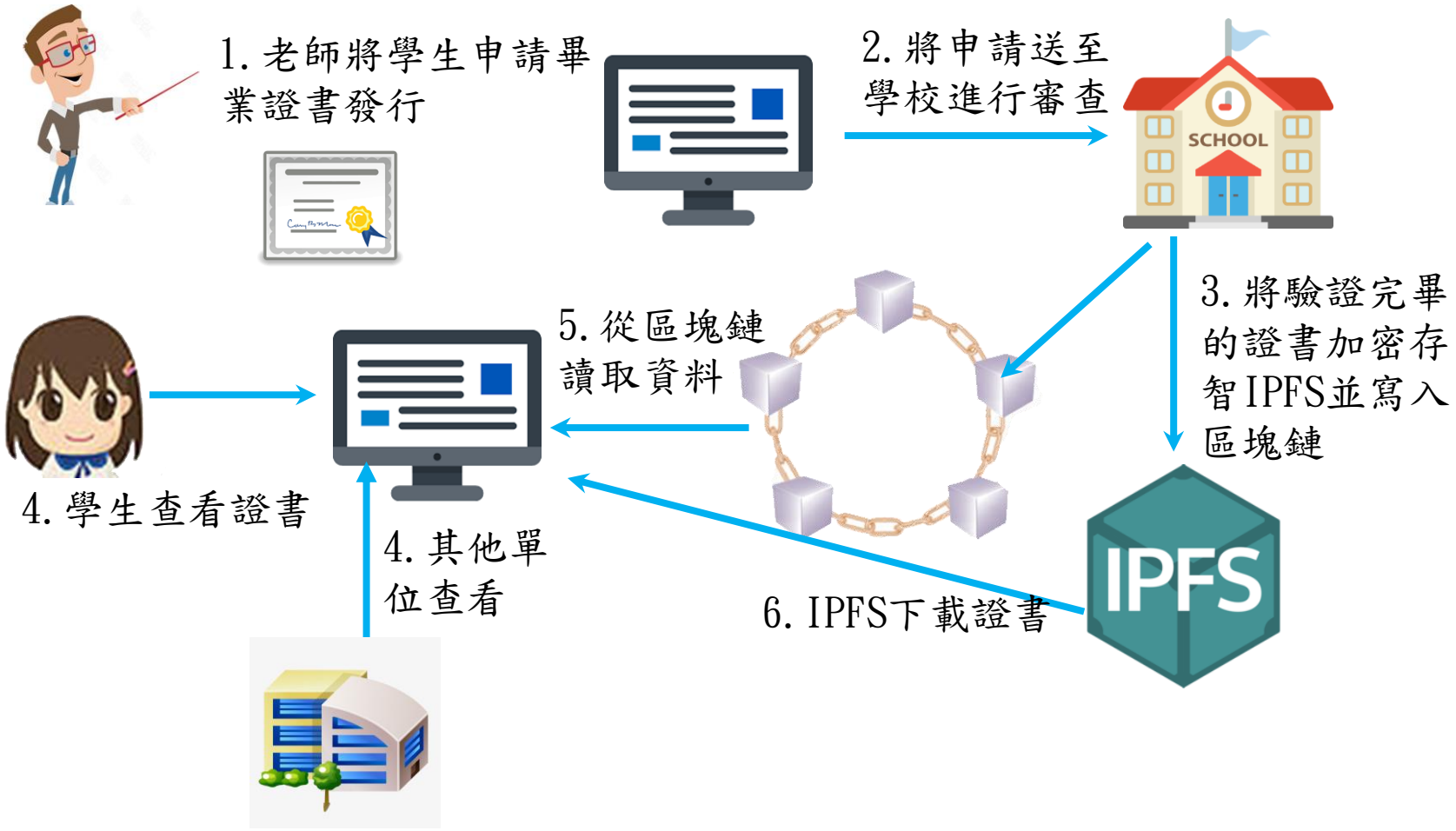
分散式儲存協定 IPFS特點

- P2P去中心化網路，避免single point failure 、DDoS攻擊
- Content addressing 及分散式儲存避免在 IPFS network 資料被竄改及重覆儲存
- P2P網路使檔案存取更快(CDN)

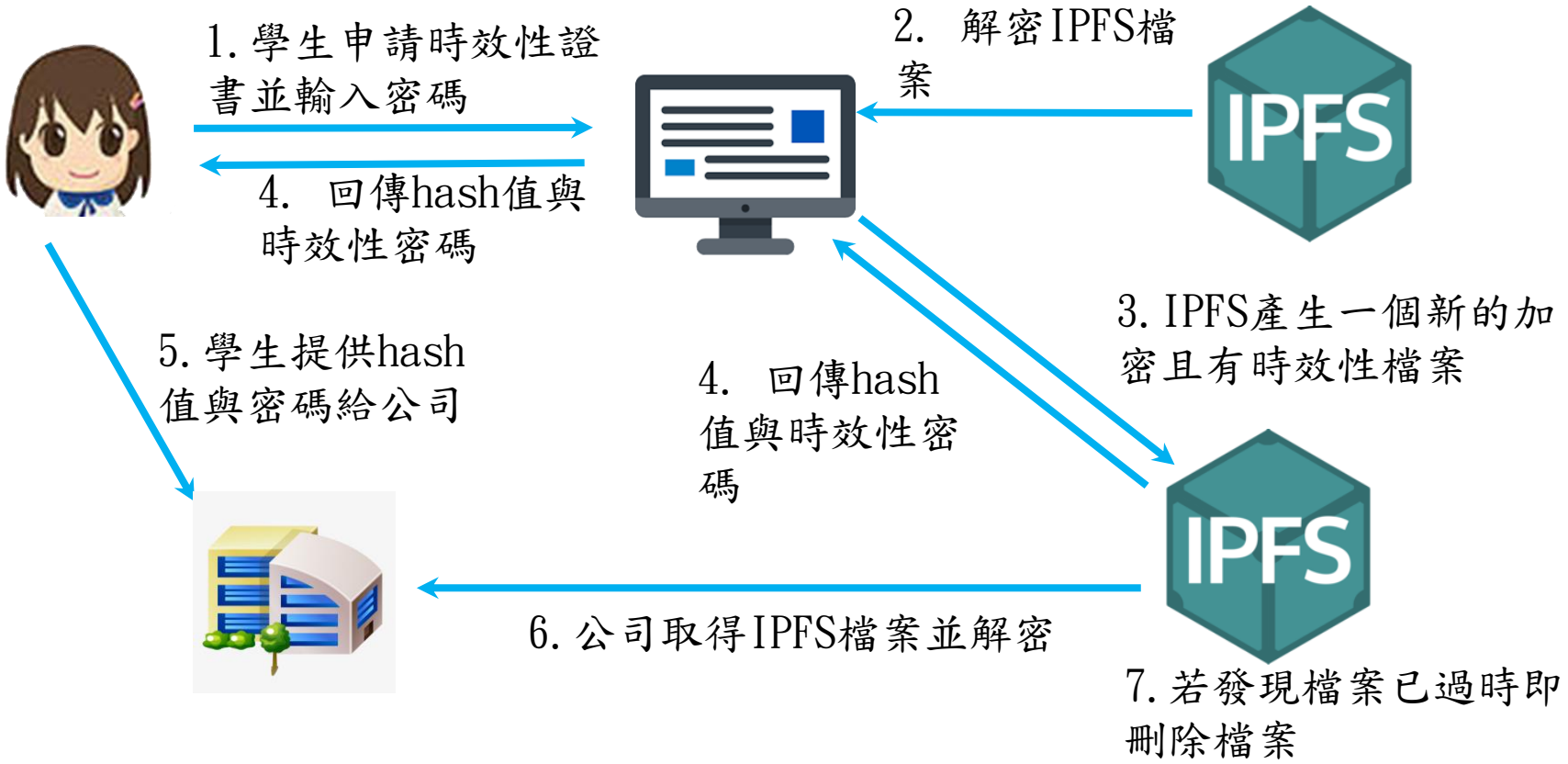
證書查核系統功能


證書查核系統
老師
學生
公開功能
個人資訊
發行／簽署／撤銷證書
查詢個人證書
追蹤發行狀態
個人資訊
查詢個人證書
電子檔驗證
QR Code驗證
使用者
功能

發起證書


1. 老師將學生申請畢業證書發行
2. 將申請送至學校進行審查
SCHOOL
3. 將驗證完畢的證書加密存智IPFS並寫入區塊鏈
IPFS
5. 從區塊鏈讀取資料
4. 學生查看證書
4. 其他單位查看
6. IPFS下載證書

限時驗證


1. 學生申請時效性證書並輸入密碼
2. 解密IPFS檔案
IPFS
4. 回傳hash值與時效性密碼
3. IPFS產生一個新的加密且有時效性檔案
5. 學生提供hash值與密碼給公司
4. 回傳hash值與時效性密碼
IPFS
6. 公司取得IPFS檔案並解密
7. 若發現檔案已過時即刪除檔案

證書撤銷

1. 老師發起證書撤銷

2. 將申請送至相關單位審查

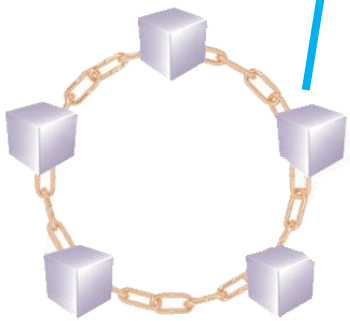
3. 將證書撤銷資訊紀錄於智能合約

4. 刪除被撤銷證書之檔案

大學招生組、公司

5. 詢問證書時會查詢撤銷狀況

6. 取得驗證結果



區塊鏈證書查核平台Demo

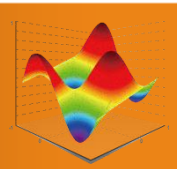
實機操作

- 國網中心區塊鏈服務

國網中心服務架構

NARLabs

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

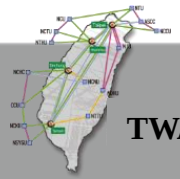
核心技術

高速計算 | 雲端中介軟體 | 大資料 | 人工智慧 | 網路與資安 | 區塊鏈

核心設施

高速計算、大資料分析與AI主機


高效能異地儲存



高品質學術研究網路

資料

資訊安全國際認證

- 資訊安全管理系統國際認證
  - 2006: ISO 27001:2005
  - 2011: ISO 27001:2007
  - 2014: ISO 27001:2013
- 雲端安全國際認證
  - 2015：CSA STAR Level 2 金牌
  - 全球研究機構中第一個取得CSA STAR金牌的
    - 雲端安全聯盟 Cloud Security Alliance, CSA；雲
      STAR (Security, Trust and Assurance Registry)
- 個資管理系統國際認證
  - 2015: BS 10012

學研骨幹網路

台灣高品質學術研究網路TWAREN

- 100G國內骨幹
  - 光網路、專屬頻寬、SDN實驗網路
- 12 區網中心
- 94 所大專院校及研究單位，50萬用戶

TWAREN台灣骨幹連網圖

台灣學術網路TANet (教育部)

- 維運TANet骨幹網路(100G)
  - TANET與TWAREN光網路共構
- 約**4000**所各級學校，約**450**萬人
- 線路平均可用率達99.99%以上

國際連線

- 20G
- 35個國際研網互連，遍及五大洲

TWAREN跨國連網圖

異地備份儲存平台

新竹、台中、
台南三地互
為備援

- 儲存總容量 8.7 PB
- 每年支援30個重要計畫
  - 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

TANet南區ASOC防護機制特色 (Academic-Security Operation Center)

- 建置於國家高速網路與計算中心
- 涵蓋範圍
  - TANet出口、雲嘉區網、高澎屏區網
  - 花蓮區網、台中區網
  - 台南區網、台東區網
- 全天候資訊安全監控中心
  - 具備全天候資訊安全事件偵測、分析與應變能力
  - 主動發佈資訊安全事件
  - 結合國際資訊安全情資進行偵蒐
- 擁有被動與主動偵測系統
  - 區網中心建置入侵偵測系統與誘捕網路
  - 收集惡意程式樣本與進行威脅分析
  - 具備快速分析與分享惡意網站能力，提供各級網管單位進行防護

國網區塊鏈服務架構

API Gateway

Smart Contract/ Dapps

Blockchain as a Service

Encryption as a Service

Oracle Service

國網區塊鏈服務BaaS優勢

	NARLabs 國家實驗研究院 國家高速網路與計算中心 National Center for High-performance Computing	雲端 BaaS*
資料國內化	OOO	X
智能合約客製服務	OOO	O
網路速度	OOO	OOO
成本優勢	OOO	O
國營產業	O	X

*雲端BaaS平台廠商: IBM, Microsoft, Oracle, SAP, Amazon, Google

IBM Blockchain Service Plan

Enterprise Plan

$1000 / month

Plus $1000 / month for each peer deployed.

Get all the features of starter plan, plus everything you need for a full production environment; including HSM availability, fault tolerant ordering service, added layers of security and premium support options.

4 x nodes/ month

1k + 4k
= 5k USD
(約每月150000元)

IBM Blockchain Platform
https://console.bluemix.net/docs/services/blockchain/enterprise_plan.html?pos=2#-

學術領域研發成果

- 國際學術會議論文
  - Peggy Joy Lu, **Lo-Yao Yeh**, Jiun-Long Huang, "A Privacy-preserving Cross-organizational Authentication/Authorization/Accounting System using Blockchain Technology," *IEEE ICC 2018*.
  - **Lo-Yao Yeh**, Peggy Joy Lu and Jen-Wei Hu, "NCHC Blockchain Construction Platform (NBCP): Rapidly Constructing Blockchain Nodes around Taiwan," *ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL 2017), 2017*.
  - **Lo-Yao Yeh**, Woei-Jiunn Tsaur, Shih-Wei Liao, Cheng-Feng Huang, Jen-Chun Chang, Ching-Ching Lin, "E-university Applications: A Privacy-Preserving Diploma Notarization Platform in Taiwan," *17th International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'18), 2018*.
- 專利申請
  - 區塊鏈可撤銷式分散式檔案平台(美國、台灣)

Reference

[1] Michele D'Aliessi, How Does the Blockchain Work?, https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

[2]B.-S. Liang, "Blockchain for IoT and Deep Learning Applications," Blockchain summit conference, 2016.

[3] Ladislav Beranek, JOnline: Auditing Electronic Auction Systems, ISACA Journal, 2010.

[4]F. Tschorsch, and B. Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communications Surveys & Tutorials, Vol. 18, No3, 2016.

[5] 陳恭, "Smart contracts: a software engineering perspective," Blockchain summit conference, 2016

[6] Andreas M. Antonopoulos, " Mastering bitcoin," oreilly, 2015.