

Fintech應用與科技風險

Isa Chi

Deloitte Risk Advisory

2018.11

講師簡介



紀宜均

Isa Y. Chi

經理

學歷：

臺灣大學資訊管理 學士

專業資格：

ISO 20000 Lead Auditor

TIIPAS 個人資料管理師

- 台北市民生東路三段156號12樓
- Tel：2725-9988 分機7790
- ischi@deloitte.com.tw

紀宜均小姐現任勤業眾信風險諮詢服務部門經理。她在勤業眾信擁有九年的專案經驗，分別為不同的行業客戶提供數據策略規劃諮詢、數據分析應用規劃、資訊策略規劃、機器人自動化流程(RPA&RCA)、IT服務管理流程諮詢等服務。

目前紀宜均小姐擔任數據科學及分析服務，及數據轉型策略諮詢顧問服務的核心成員，專精於金融業數據科學及人工智慧應用、數據治理設計及規劃、資訊策略規劃分析與建議等方面。曾擔任臺灣縣市政府合併升格時的資訊策略及規劃專案主要成員，在資料科學、分析建模及資料規劃應用與實作方面積累了一定的專案經驗。

經歷：

- 勤業眾信聯合會計師事務所風險諮詢部門經理

主要負責服務之公司包括：

- 政府相關單位：台北市政府、高雄市政府、台南市政府、台灣金融研訓院等
- 電子電信業：遠傳電信、中華電信等
- 金融業：合作金庫商業銀行、土地銀行、台新商業銀行、富邦金控、華南金控、第一商業銀行、遠東商業銀行、中國信託商業銀行、上海商業儲蓄銀行、遠雄人壽、新安東京產險等
- 其他：家樂福集團、越秀地產、悠遊卡、一卡通、賓士汽車、桃園大眾捷運公司等²

Agenda

01

為什麼監理與風險議題在**Fintech**領域相對重要

02

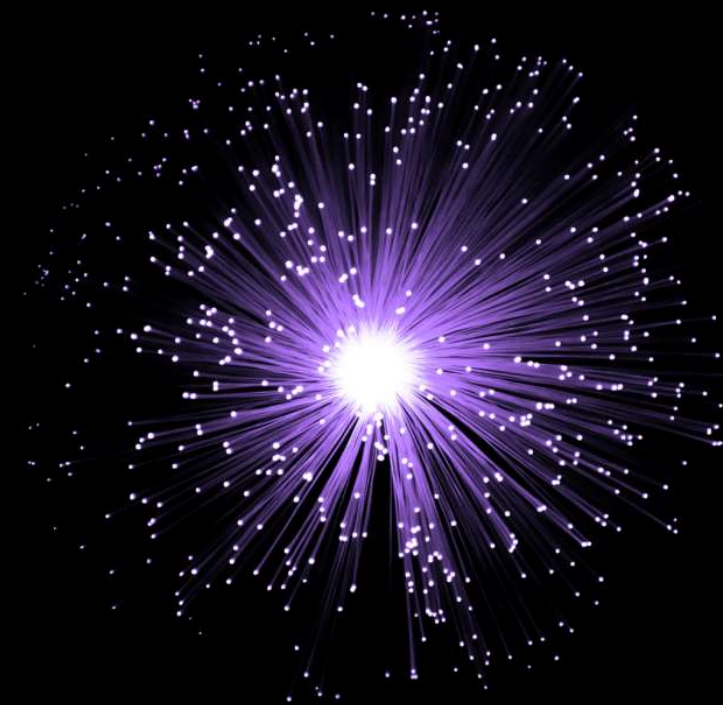
人工智慧的風險與挑戰

03

區塊鏈的風險與挑戰

04

跨領域的風險與挑戰



為什麼監理與風險議題 在Fintech領域相對重要

跨國匯兌新創平臺涉及協助洗錢交易

提供P2P跨國匯兌的櫻桃服務有限公司Cherry Pay，標榜「比銀行還便宜」的抽傭手續費，讓民眾透過該平臺進行第三方支付代儲金流服務，然而因其中金流涉及為詐騙集團洗錢而遭警方鎖定

掛羊頭賣狗肉？App媒合匯兌攏係假 疑涉洗錢遭警搜索

-三立新聞網

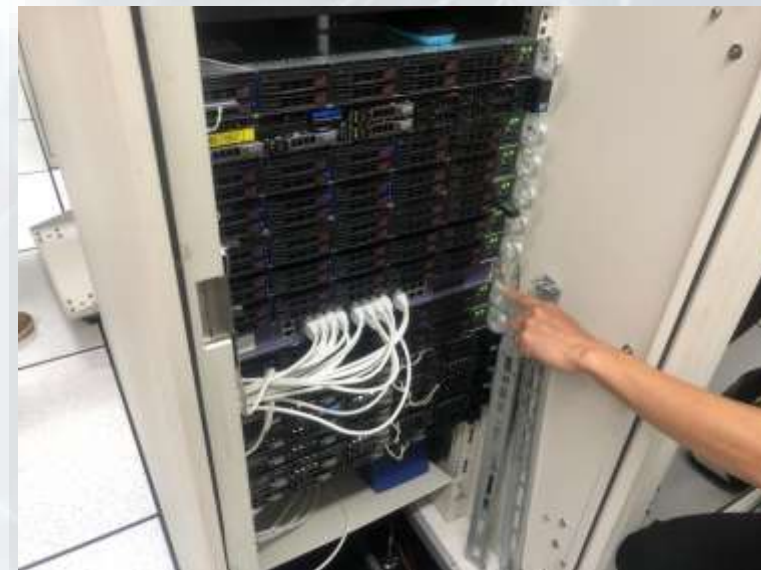
「比銀行還便宜」地下匯兌11億 嫌：是媒合金流交易

-鏡周刊

你網購我洗錢？線上支付遭詐騙集團利用

-TVBS NEWS

國際匯兌平台Cherry Pay，被警方查出其實是地下匯兌公司涉嫌洗錢，原來這公司表面上說只是提供平台讓消費者媒合匯款，打出手續費只要銀行的四分之一，但警方查出她們利用員工和在大陸親友來轉帳付款，因為**沒有身分查核成了詐騙集團洗錢利器**，但業者也出面喊冤，強調自己只是媒合平台沒有觸法。



圖/警方提供



結合金融科技與數位金融進行業務發展和創新的同時，仍應注意相關的法規遵循，透過**監理科技與人工智慧的應用**，能夠協助企業符合政府規範，並降低企業涉及不法活動的風險，也能**減少利用人力進行稽核的資源與時間成本**



監理科技

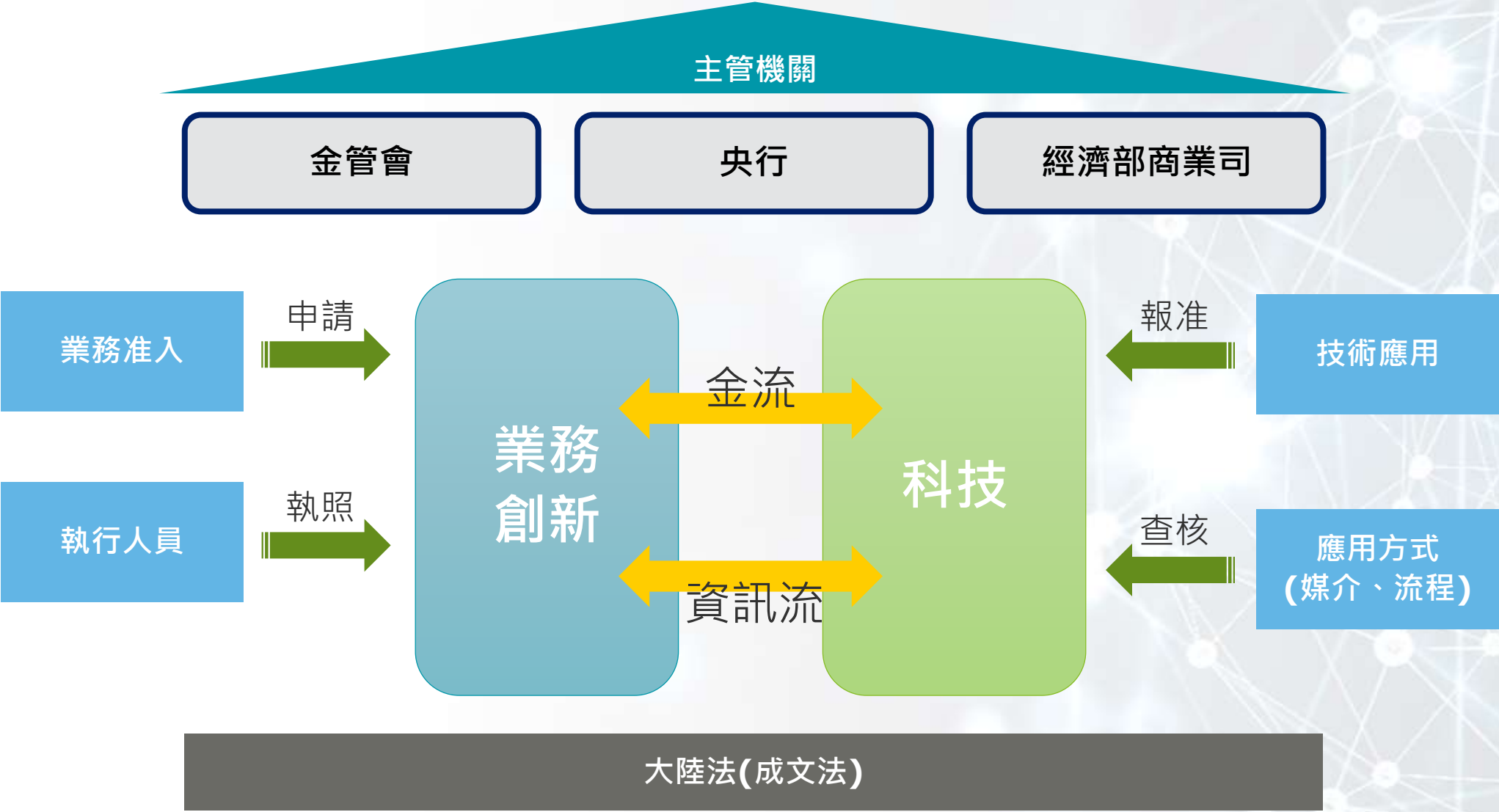


法規遵循



人工智慧

金融科技創新的風險點



金融科技觸法案例

究竟地下錢莊在法律上如何解釋？

地下錢莊，根據民國四十一年五月二十一日行政院公佈的「取締地下錢莊辦法」第二條之規定，地下錢莊，係指非法經營（舊）銀行法第二條第一項第一款（收受各種存款）、第二款（票據承兌）、第三款（辦理各種放款或票據貼現）、第四款（國內匯兌）、第五款（特許經營之國外匯兌）、第六款（代理收付款項）、及第十八條（凡以收存貨幣或款項為常業者，不論其收存方法為給予支票或存單或放據或簿摺或期票或其他類似之證明文件，均視為銀行業務。）規定業務之一者而言。凡「經營生產事業或供應物質之工廠、公司及其他團體行號，向外借用週轉資金.....借入之款項用於其所經營業務範圍以外而轉存、轉放圖利者，應視為地下錢莊」。但如借用之週轉資金，「用於其所經營之事業或因事業上資金之擴充運用，非以收存貨幣或款項為常業圖利者」，不視為地下錢莊。

舊銀行法原將錢莊列為銀行之一種，民國六十四年始將銀行限制為四種（商業銀行，儲蓄銀行，專業銀行，信託投資公司），而將錢莊除外。並明訂，除法律另有規定者外，非銀行不得經營收受存款，辦理國內外匯兌等業務（違反者，處五年以下有期徒刑，拘役或科或併科七千元以下罰金。法人犯此罪者，處罰其行為之負責人）。

GDPR的起源：「被遺忘權」

首宗關於「被遺忘權」的訴訟源於西班牙，一名西班牙男子於2011年向法院要求當地報章刪除一篇有關他16年前因陷入財政危機、無法繳稅而被迫拍賣物業的報導。雖然他早已還清債務，但多年後仍可以Google上搜尋相關內容，該名男子認為相關搜尋結果影響到他的名譽。

歐盟法院最終於2014年5月裁定Google敗訴，確立歐洲公民享有「被遺忘權」。判決出爐後，Google亦隨即推出新服務，容許用戶向Google提出移除涉及個人資料及私隱的超連結，但僅限於歐洲用戶。（目前已經推展到澳洲）

2008年，中華職棒的米迪亞暴龍隊爆發假球案，當時的球團老闆施建新（事件後更名為施允澤）被依詐欺等罪起訴，最後獲判無罪。然而，據媒體報導，施允澤因其名字只要在Google網站搜尋，就會跑出與「施建新 假球」有關的新聞和搜尋字串，因此告上法院，要求Google移除建議的關鍵字，2015年台北地院一審判他敗訴，2016年高等法院駁回其上訴。

金融科技觸法案例（續）

證交所：營業員禁用LINE推介股票



報系資料照

證交所表示，營業員不得向不特定多數人推介買賣有價證券，更不可以用LINE群組推介股票。

這項禁令起因於，最近證交所券商輔導部接獲投資人申訴，某營業員於LINE群組對話中，有推介股票情事。

證交所派員查核後發現，該營業員於LINE群組對話中轉發內容，提及個股買賣建議價及停損價等資訊，該案例營業員已違反證券管理法令相關規定，遭受處置。

證交所提醒證券商從業人員及投資人，依據「證券商推介客戶買賣有價證券管理辦法」，營業員不得向不特定多數人推介買賣有價證券。

另外，營業員對特定客戶推介買賣有價證券之前，應該指派負責解說的業務人員，向客戶說明推介買賣有價證券可能風險後，與客戶簽訂推介契約。

證交所另提醒，交易有價證券可能產生獲利，同時也可能發生虧損，投資人於交易前應審慎考量自身風險承擔能力，在接受證券商及其受僱人以任何方式推介買賣有價證券前，應先與證券商簽訂推介契約，瞭解權利義務及風險，以保障自身權益。

[新聞] 無照卻教人炒股 他獲緩刑3年

【聯合報／記者鄭文正／台中報導】2008.02.26 03:16 am

台鐵退休的賴宣名看準股市熱度，無照經營證券投資顧問的解盤諮詢、開班授課，獲利超過400萬元，台中地院昨以違反期貨交易法及證券投信託及顧問法，判他有期徒刑6個月，緩刑3年，並支付國庫30萬元。

檢方昨天說，網路上很多人在討論股票，當然不違法。但此案重點是，賴宣名還給予會員個別股票的分析意見及推薦購買某一支股票或期貨，他既無證券分析師等相關專業執照，就涉及違法行為。

判決書指出，男子賴宣名（50歲）在台北、台中等地，以「羅威」之名稱，販售自創的「羅威高階趨勢操作技術研討班」授課，每5、12、20堂課，要價2、3、及6萬元不等

的收費，傳授以自創的「波動操作法」。

另外他還將上課教學錄影製成教學DVD，在網路上的「聚財網」網站刊登廣告，以每套2萬8000元至3萬8000元不等金額，以函授方式招收學員，從92年起至96年11月被查獲，共有上百人加入會員，獲利約400萬元。

檢調調查，賴宣名給會員一個電子信箱的帳號，供作學員聯絡之用，還在雅虎奇摩網站設立「活出股市生命力」家族，以個人網站，讓會員以帳號加入家族。

後來有會員認為分析內容不準，發現他根本沒有證券分析師證照，匿名向行政院金融監督管理委員會檢舉，金管會轉送給台北市調查處調查後，移送台中地檢署偵辦。

金融科技觸法案例（續）

除了保險公司，業務員請勿在網際網路招攬保險！



金融監督管理委員會備查壽險公會所提修正「保險業廣告招攬自律規範」(新增第四條之一*)(自律規範可至講義中心下載)

壽險公會規範，未來業務員除非經過公司核可，不可以利用網際網路進行招攬廣告，包含透露特定商品名稱、特色或者足以辨別某種商品的內容。

我們如果上google 搜尋「網際網路」，可以看到對網際網路的定義。相信各位消費者也會認同，現在的「智慧型手機」也是屬於網際網路的一員。大家平常常用的line也是利用網際網路在傳輸資料的。所以，以後在line裏面，業務員們是不是也不能寫「xx人壽的oooo保險商品超讚！」，因為是利用網際網路，且有廣告之實質，也有談到特定的保險商品名稱。加上透過監聽技術，這些資訊絕對是可以在網際網路找到的。

保險業廣告招攬自律規範第四條之一 連結

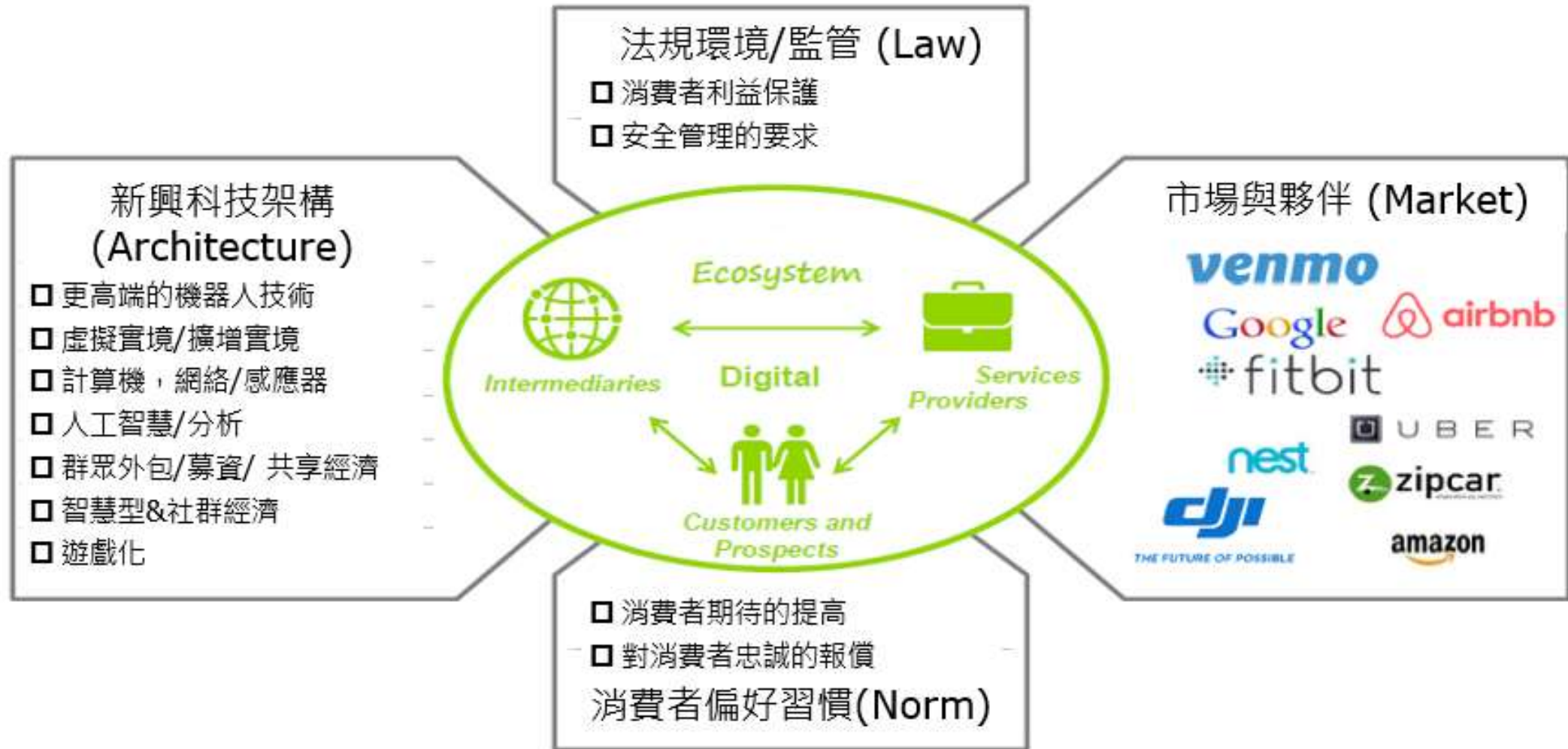
保險業應要求所屬之業務員，除經公司核可之招攬廣告外，不得透過網際網路從事特定保險商品銷售招攬廣告(含透露商品名稱、特色或其他足以辨別為某特定商品之內容)，有關網際網路從事特定保險商品銷售招攬時，招攬廣告應遵守相關程序如附件；另保險業應訂定以下查核機制：

- 一、查核範圍：各大入口網站、各拍賣網站、部落格等。
- 二、查核頻率：至少每季1次。
- 三、異常處理：經查證刊登內容違反本自律規範且為所屬業務員所刊登時，應依保險業務員管理規則及公司管理辦法予以懲處，並要求該業務員限期改善或撤除該廣告；另經查證刊登者為合作往來之保險代理人或保險經紀人公司所屬業務員，保險業應要求其限期改善並撤除該廣告。
- 四、教育宣導：對於網路行銷廣告之相關規定及查核處理原則，應定期對所屬業務員進行教育宣導或發文公告保險業務員，除經公司核可之招攬廣告外，不得透過網際網路從事保險商品銷售招攬廣告。

現行台灣的監理框架：以銀行支付業務為例



影響金融科技發展的環境風險因子



Code v 2.0

Dr. Lawrence Lessig

Stanford University Law School

金融監理沙盒案例



金融監理沙盒首件核准實驗案，由凱基銀行攜手中華電信擔任「開路先鋒」。（圖片來源 / 信傳媒資料照）

台灣第一座「金融科技創新園區FinTechSpace」18日正式開幕，金管會主委顧立雄當天也捎來好消息，宣布凱基銀行與中華電信將進行創新實驗計畫，成為首件核准「金融監理沙盒」的案例。學者認為，此消息對於正積極發展金融科技的台灣來說，無疑是注入一劑強心針；但另一方面，商業機密等同直接攤在陽光下，確實也成為不少金融科技業者卻步的主因。

所謂的「金融監理沙盒」是指在一個風險規模可控的環境下，針對金融相關業務、或遊走在法規模糊地帶的新創業者，在主管機關監督下提供一個實驗場所，讓業者盡情測試創新商品或是新商業模式，同時在主管機關的同意下，可暫時排除法規的要求。

而此次進入監理沙盒實驗的第一案是由凱基銀行攜手中華電信擔任「開路先鋒」，透過手機身分確認技術，結合電信徵信資料及大數據交換等科技營業模式，可辦理新戶線上信貸及信用卡業務。

簡單來說，若是一位剛出社會的新鮮人已經在中華電信累積了足夠的信用紀錄，就可辦理銀行信用卡及信貸，即不用經過銀行業進一步審核，因此對於凱基銀來說，等於是「開拓了以往不在銀行體系內的新客戶」。

而該機制須經過「身分確認」，舉例來說，如果是父母幫小孩辦了手機，而繳款都是由父母繳款的話，小孩用手機申請本人的信用卡之後，該機制會確認到身分不符合，將拒絕申請，意味著「使用者與繳費者」僅能是同一人。

知情人士則分析，中華電信擁有龐大的大數據資料，與凱基銀行早一步合作，不但可加以檢驗該數據資料是否可行，進行模擬信用評等之外，對於正在爭取純網銀執照的中華電信來說，也可作為日後發展純網銀的基礎，

曾擔任金融聯合徵信中心董事、現任東吳大學講座教授兼金融科技中心執行長蔡宗榮則認為，以往銀行業辦理授信最頭痛的莫過於沒有即時資料，而聯徵中心所取得的財務資料多是落後資訊，反觀電信業者所持有的電信帳單是每個月都有，「甚至比水電費資料還來的即時」，因此，就可從客戶帳單內容進一步分析，實際觀察客戶現階段的消費行為。

人工智慧的風險與挑戰

什麼是人工智慧

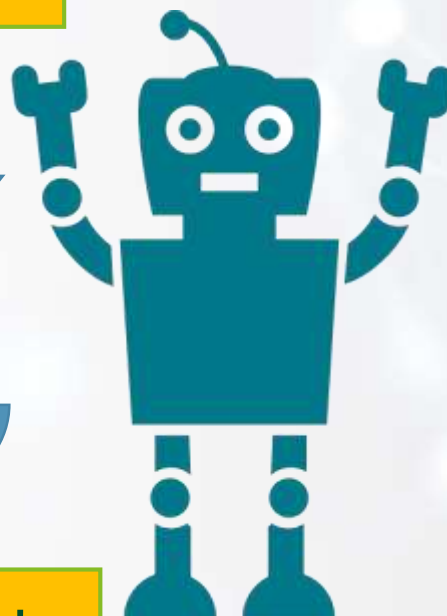
人工智慧是指機器可以在接收資訊後，以自己的方式進行理解並給予回饋；
而機器學習則是讓人工智慧形成理解能力的過程

真實世界
(大數據)



1. 接收資訊的能力

人工智慧



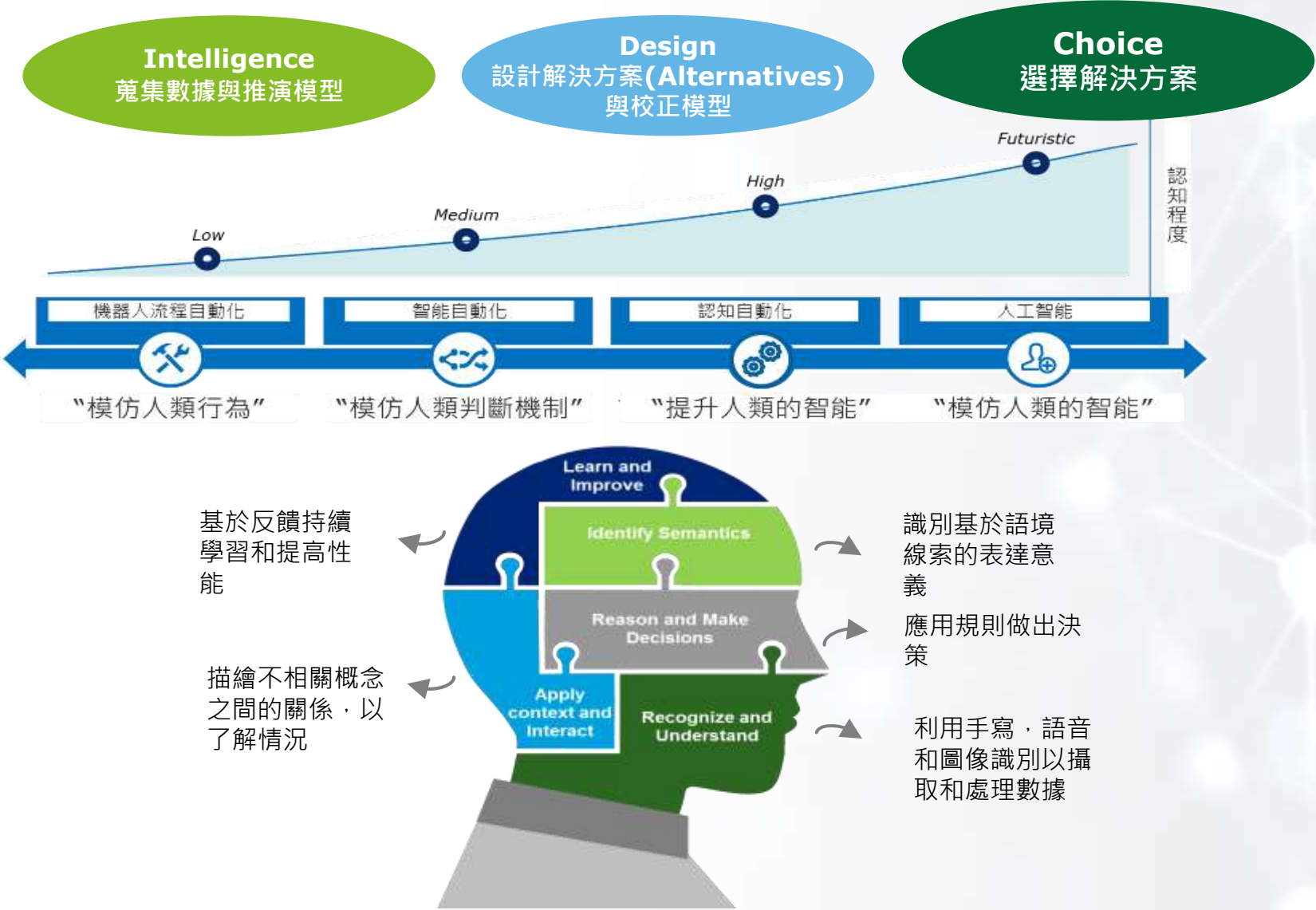
2. 理解資訊的能力



機器學習

3. 回饋資訊的能力

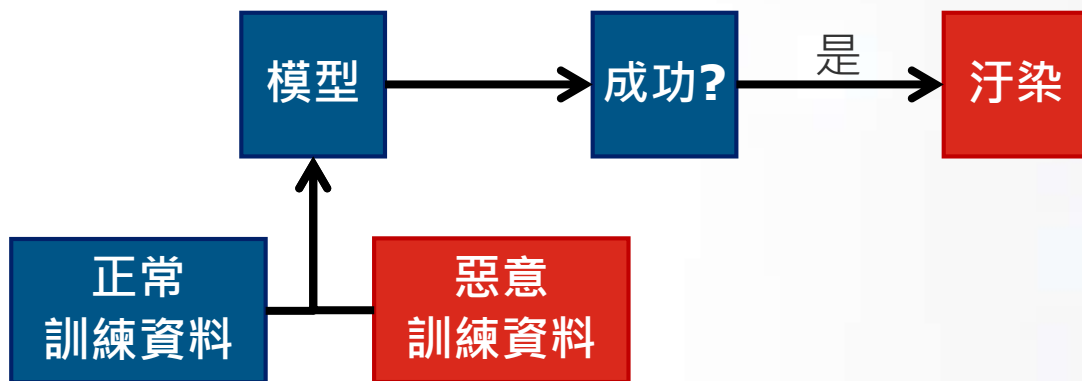
機器學習與人工智能應用



| 核心技術元件 | 1 | 2 | 3 | 4 | 5 |
|---------|---|---|---|---|---|
| 機器學習 | ■ | | | | |
| 概率推理 | ■ | | ■ | | |
| 規則引擎 | ■ | | ■ | | |
| 自然語言處理 | | ■ | | ■ | |
| 語義分析 | | ■ | | | |
| 手寫識別 | | | | | ■ |
| 圖像識別 | | | | | ■ |
| 文本分析引擎 | | ■ | | | |
| 信息檢索 | | | | | ■ |
| 語音識別 | | | | ■ | ■ |
| 自然語言生成 | | | | ■ | |
| 虛擬決策建議 | | | ■ | ■ | |
| 文字蘊涵識別 | | ■ | | ■ | |
| 增強式學習 | ■ | | ■ | | |
| 擴增與虛擬實境 | | | | ■ | |
| 語意合成 | | | | ■ | ■ |

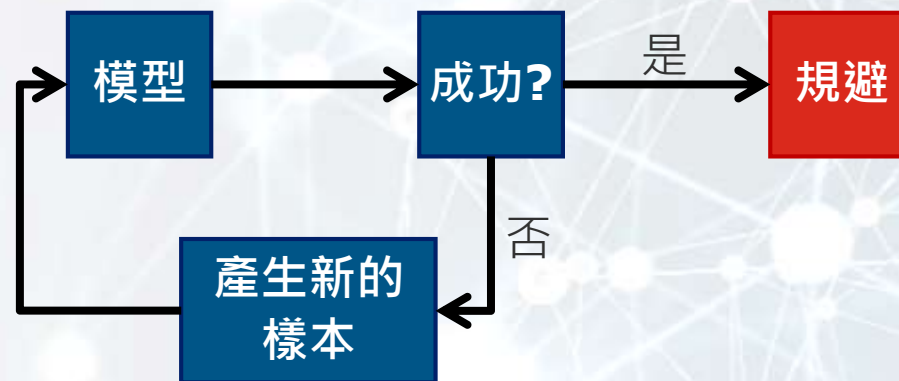
致病性攻擊與探索性攻擊

■ Evasion attacks & Poisoning Attacks



汙染攻擊 POISONING ATTACK

- 在訓練資料加入惡意資料→模型→(成功)汙染模型
- 針對**AI**的致病性攻擊

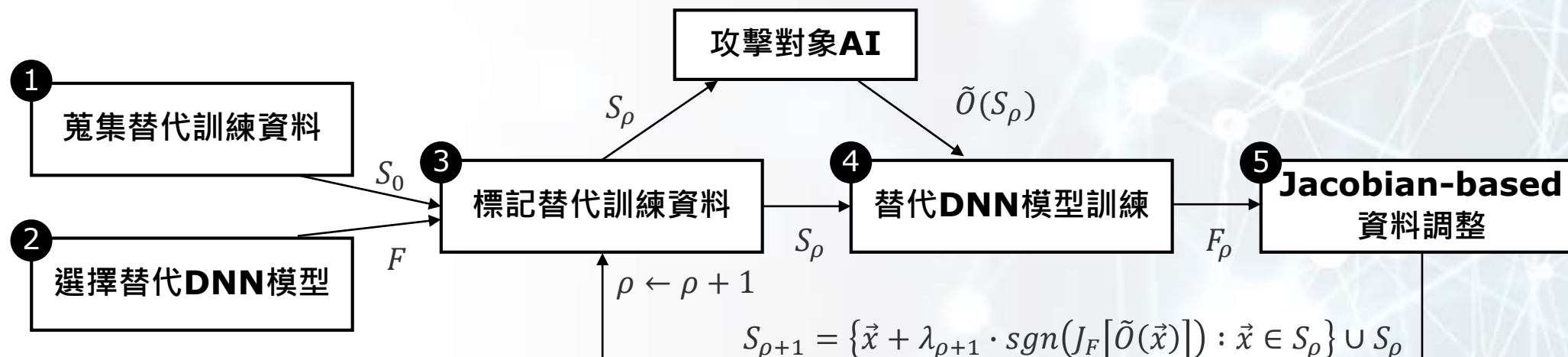


規避攻擊 EVASION ATTACK

- 嘗試輸入資料→模型→(成功)規避
 ↘ (不成功)→嘗試新的資料
- 針對**AI**探索性攻擊

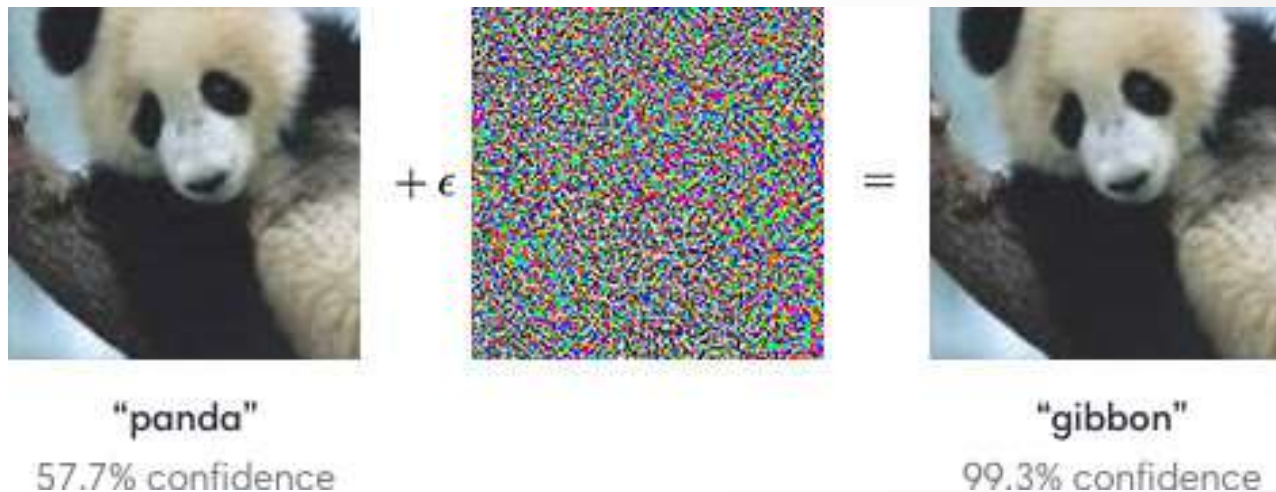
黑箱攻擊

■ Black-box attack



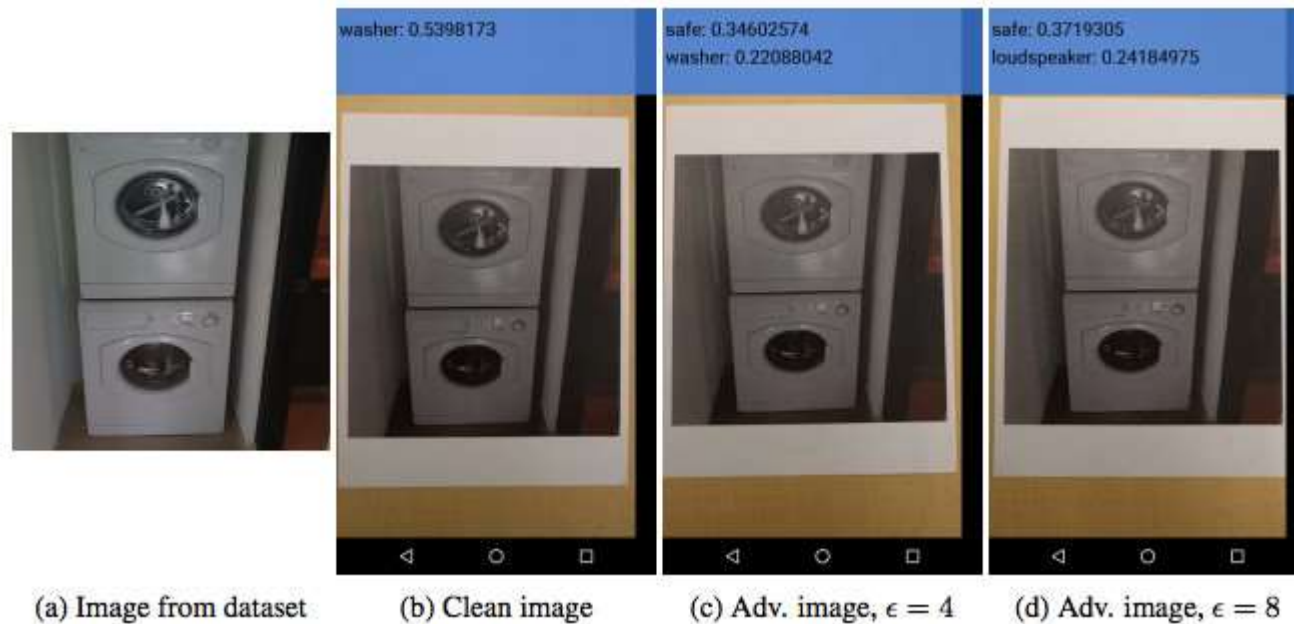
- 前面所提到的攻擊需要攻擊者對**AI**有一定程度的了解(如參數)才能進行攻擊。比較近期的研究則提出了較為真實的攻擊手法：攻擊者只能透過觀察**AI**的輸出預測來產生攻擊圖像。這種手法會有更廣的應用，例如：設計容易得到高分PageRank的網頁、製造無法被偵測的垃圾郵件等。
- 攻擊者會先準備替代資料，並透過輸入給欲攻擊的**AI**來取得輸出，再對攻擊者準備的替代模型進行訓練。同時以Jacobian-based Augmentation對這些替代資料進行干擾。
- 如果被用在路邊的廣告看板，自動駕駛的汽車是否還能安全地行駛？

黑箱攻擊範例



- 熊貓圖片被加入干擾資訊(對抗樣本)後，被模型誤判為長臂猿

- 洗衣機圖片被加入干擾資訊(對抗樣本)後，被模型誤判為保險箱



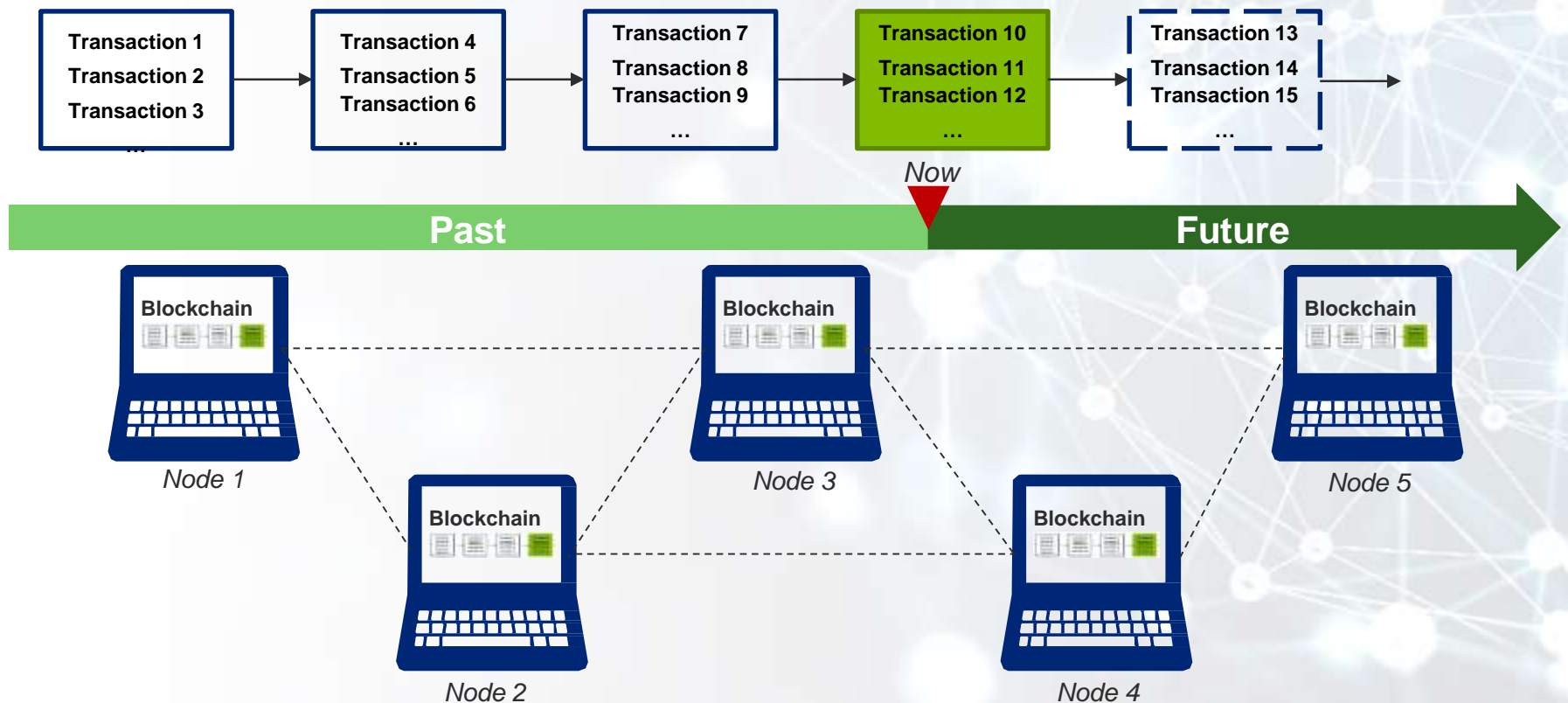
區塊鏈的風險與挑戰

什麼是區塊鏈(Blockchain) ??

何謂區塊鏈?

- 區塊鏈是一個不斷增長的交易資料庫，資料按時間順序來排列，並在網路中的參與者之間共享。
- 依靠加密演算法和分散式儲存技術，網路中的參與者一起維護區塊鏈上的資料，並透過以共識為基礎的處理過程(consensus-based process)驗證新加入的交易資料，並將驗證過的資料加到鏈上。
- 一旦資料被加到鏈上，就被認為是已確認的，因為一旦它們被網路中的參與者所接受，就很難被刪除或改變，且資料越早加到鏈上，改變越困難，信任水平越高。

將交易寫入**區塊**中
鏈結在一起



為什麼區塊鏈技術一直受到注目 ??

關鍵在於，所有參與者都共同持有相同的資料，並運行相同的機制，

- 提升進行資料傳輸及驗證的效率
- 降低資料被私下竄改的可能性
- 增加參與者之間的信任

透明度



所有區塊鏈參與者可以看到加到鏈上的資料，增加透明度及高可用性

信任



所有參與者共同持有相關的資料，運行相同的資料，增加彼此間的信任

去中介化



因為透明化和信任的特性，以區塊鏈技術為基礎的系統可以實現傳統中介者提供的功能

智能合約



是在區塊鏈上執行的一種應用程式，當滿足一組預先設定的條件時，即以合約所協議的交易內容執行應用程式

可審計性



區塊鏈上包含所有寫入的交易資料，且都是確實可驗證的，也不容易被更改或偽造

區塊鏈技術的迷思與事實

雖然區塊鏈可以有很多創新，但重要的是要瞭解區塊鏈“能做什麼”和“不能做什麼”



區塊鏈不代表Bitcoin

- Bitcoin是一種加密貨幣，利用區塊鏈技術安全地記錄貨幣交易過程
- 區塊鏈技術的屬性提供了使Bitcoin和其他加密貨幣的知名度上升的基礎技術



區塊鏈不是一個企業級的資料庫

- 一個組織中大多需要一個可以訪問、儲存需要隱私和保護大量資料的系統，以供檢閱和查詢，即企業資料庫
- 但區塊鏈是被設計用於記錄特定交易、事件，這些交易和事件需要透明性，並在多方參與的網路上共用



區塊鏈不完全代表資料有效性及正確性

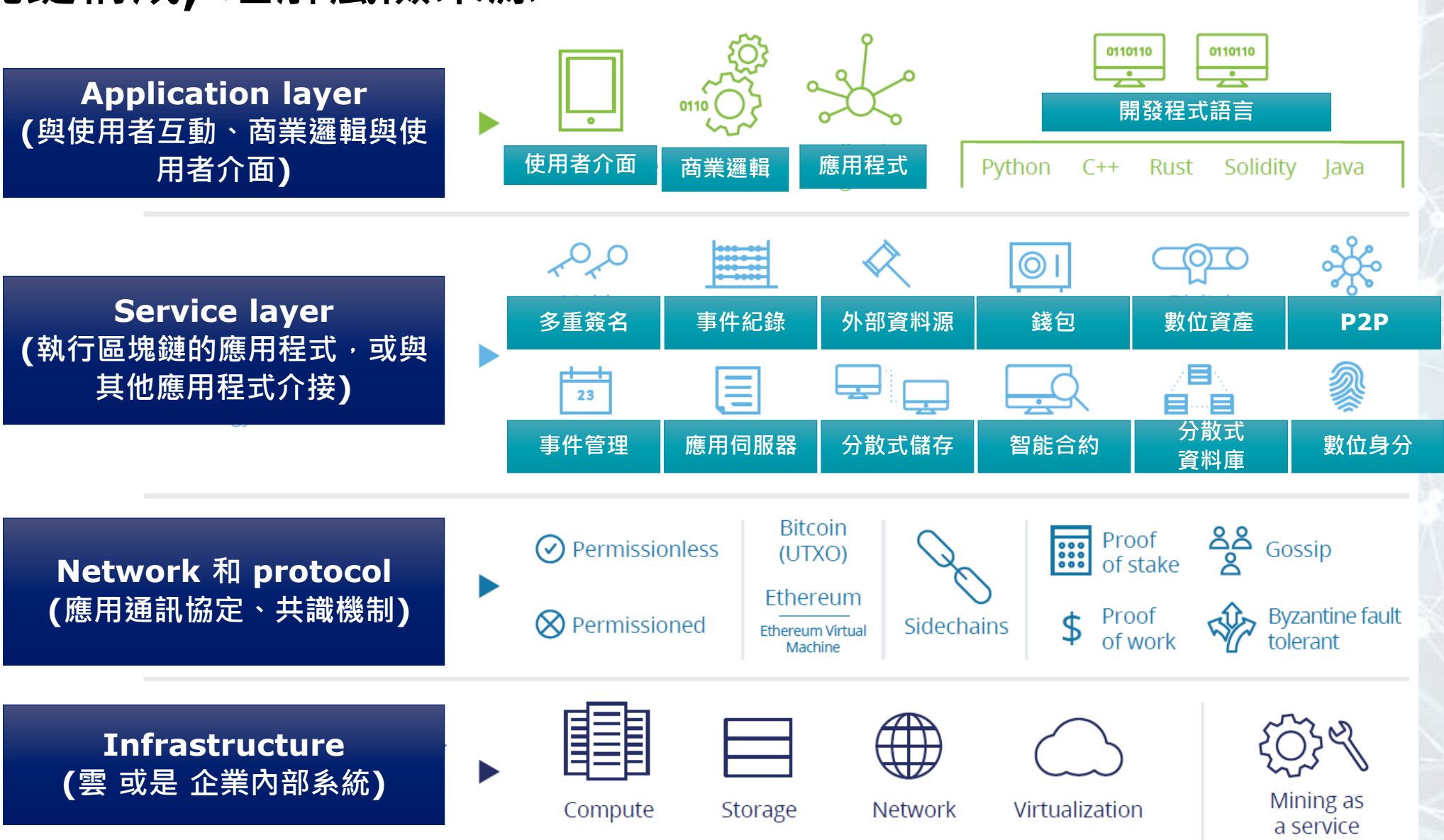
- 雖然提交資料者的身分是透過公私鑰進行確認，因此有了匿名性，但區塊鏈上資料的安全性來自於共識機制與“鏈結”的特性
- 但區塊鏈上的資料是否有效，不同區塊鏈技術會有不同程度的確認機制
- 但區塊鏈上的資料是否正確，須考量將資料寫入區塊鏈的機制



區塊鏈不只有公有鏈

- 公有鏈可以讓每一個人加入，參與共識過程的參與者可以決定哪些區塊是有效的，應該被加進鏈中
- 私有鏈則有權限設定，可設定檢視數據、加入鏈和參與共識的權力

從區塊鏈構成，理解風險來源



區塊鏈技術(DLT)應用的挑戰與攻擊

Application layer

(商業邏輯
與使用者介面)

2018年 有多起51%攻擊
Bitcoin Gold、Litecoin Cash、MonaCoin、
ZenCash與Verge都是自建區塊鏈網路，因
攻擊成本較低而被攻擊

- 2018年1月 Oracle WebLogic漏洞導致受駭系統被植入挖礦程式
- BT網站海盜灣(The Pirate Bay)埋挖礦程式碼，讓訪客電腦協助挖礦

Service layer

(執行程序，可與其他應用程式
式介接)

2018年7月
以色列cryptocurrency交易所發行錢包遭
駭，透過不安全的智能合約盜取
cryptocurrency，市值約1350萬美元

2017年7月
智能合約軟體公司Parity已發布安全警報，
警告其錢包軟件1.5或更高版本具安全弱點，
原因為多重簽名的智能合約有漏洞

網路協議層

(共識演算法、節點維護)

2018年5月
日本公司所發行的Monacoin，遭到selfish mining attack，意圖透過運算效能以側鏈攻擊主鏈，並透過51%攻擊竊取Monacoin

基礎架構層

2018年6月
南韓cryptocurrency交易所Coinrail、
Bithumb被駭，原因為資訊安全控管疏失，
損失超過1億台幣

2018年2月
義大利cryptocurrency交易所聲稱被駭
損失了價值約1.95億美元，但原因遭質疑
疑似金鑰管理人盜領

跨領域的風險與挑戰

為何要做隱私工程？當大數據遇上個資法

政府曾積極推行開放資料（Open data），雖然有些效果，但還是有相當的成長空間與不足之處，主要原因是開放資料常會與個人資料保護有所衝突，在缺乏適當誘因或是壓力之時，即使有相當的社會公益，公司團體仍會以保護個資為由不與外界分享資料。

不只台灣，國際上也意識到個人資料的利用趨勢，在原本的個人資料隱私保護框架上，建構去識別化方法。英國2012年提出「匿名化應用準則」，歐盟2014年公布「匿名化技巧意見書」，日本今年9月修訂「個人情報保護法」，將去識別化納入規範。

兼顧開放分享資料與個人資料保護之間的平衡，隱私工程中的「去識別化」（De-identification）是近年來重要的發展方向，所謂去識別化，是指「**移除或模糊個人資料中任何可識別資訊，其目的在降低個人非意欲揭露其相關資訊的風險**」。

是否完成去識別化，大致從三個方向判定：

1. 執行後是否仍可能識別當事人？
2. 執行後是否仍可能與其他個人資料相連結？
3. 執行後是否仍可能推論出與特定人相關？



企業面臨個資去識別化議題



政府
發展
Open
Data

- ✓ 擁有或處理大量資料，缺少創新思維，不知如何極大化資料價值
- ✓ 開放政府資料催生資料產業創新價值
- ✓ 透過不同來源的資料的彙整與巨量資料的分析和模式建立來產生新的知識



電商業者

- ✓ 電商營運的各個環節，都需要以數據為基礎
- ✓ 分析流量來源能夠更好地了解企業的潛在客戶
- ✓ 從客戶的角度分析，能夠成功分辨客戶屬性



Big Data 大數據 平台

- ✓ 由巨型資料集組成，這些資料集大小常超出人類在可接受時間下的收集、度用、管理和處理能力
- ✓ 大數據的處理分析成為新一代資訊技術融合應用的結點

④ 個資去識別化機制

發揮資料最大價值

解決個資利用爭議

企業大數據運用

政府大數據運用

推動新商業模式需求

去識別化?假名化?匿名化?

De-identification(去識別化) 是**通稱**，指個人資料不再具有直接或間接識別性，而Pseudonymization(假名化)與Anonymization(匿名化)是去識別化時最常見的**技術**。

De-identification(去識別化):

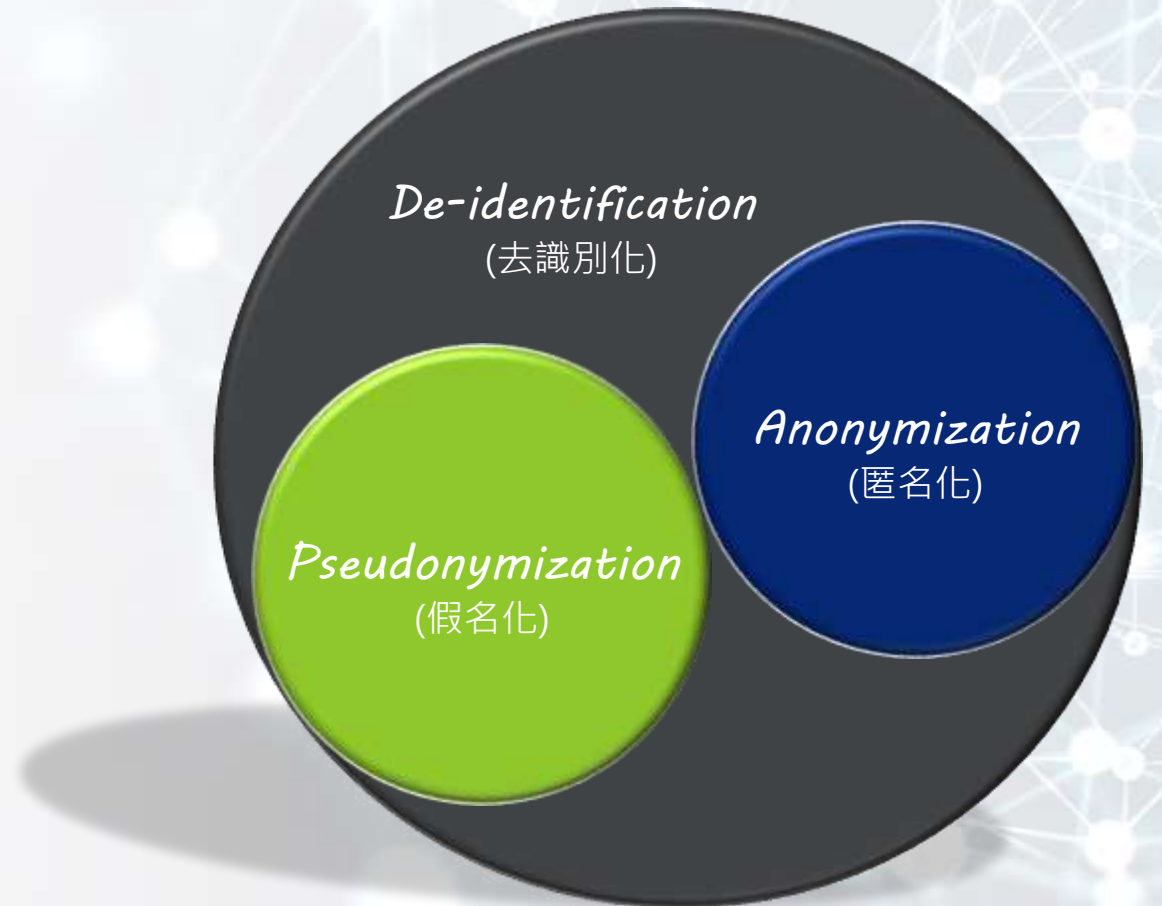
通稱，指個人資料不再具有直接或間接識別性。

Pseudonymization(假名化):

可以逆轉，使用單獨保存資訊的方法，可以在需要時檢索可識別信息，以將數據鏈接回個人。

Anonymization(匿名化):

不可以逆轉，一旦數據被匿名化，它就永遠不會被鏈接回個人。匿名化是永久性的。



假名化 vs 匿名化

假名化是可逆的，用一致的值替換可識別數據的方法。匿名化則是不可逆的，對可識別數據的破壞。

如右例，使用**假名化**，我們可能不知道數據主體的身份，但我們可以將資料與特定主題相關聯（*ex. 條列1與條列7為同一個人，條列2與條列5為同一個人.....*）。

如果我們有權限**讀取查找表**，則可以**重新識別資料真實身份**。

若使用**匿名化**，我們只知道有7條記錄，而**沒有方法可以重新識別數據**。

| Name (原始資料) | Token/Pseudonym (假名化後資料) | Anonymized (匿名化後資料) |
|----------------|-----------------------------|------------------------|
| Clyde | qOred | xxxx |
| Marco | Loqfh | oooo |
| Les | Mcv | kkkk |
| Les | Mcv | aaaa |
| Marco | Loqfh | cccc |
| Raul | BhQl | dddd |
| Clyde | qOred | gggg |

人工智慧AI正在改變全球產業環境

2018年8月世界經濟論壇 (World Economic Forum, WEF) 合著報告 - 《新金融服務地景：理解人工智慧如何翻轉金融生態體系》



超過**200**場與專家領袖的訪談



七場全球workshops



歷時**10**個月研究

核心發現

資料與技術共享

- ✓ AWS、Google等雲端AI平台使企業可以共享尖端AI技術，同時加速企業發展更加客製化的AI應用來達到差異化競爭優勢
- ✓ 透過跨機構間分享資料與AI技術，企業可以合作解決反洗錢、詐欺等過去各企業共同面臨的問題

市場分化與監管

- ✓ AI技術的發展使部分產業呈現大者越大的趨勢，中型企業開始式微。反觀新創企業若能找到特定利基，則仍然有機會進入市場
- ✓ 發展中的監管體系對企業如何應用AI有關鍵性影響，企業需要更積極投入到資料與AI監管設計的討論中

人才與社會影響

- ✓ 以AI為驅動力的企業成長需要長期人才發展與組織改造計畫。如何在短期成果與長期投資間取得平衡是企業轉型的關鍵
- ✓ AI對人才就業、產業發展、消費者與公眾利益等社會經濟議題帶來的影響需要多方合作來共同解決

金融組織雖然擁有大量數據，卻難以有效運用於AI服務

值得注意的數據挑戰

數據是AI最重要的組成部分；AI模型的預測能力由輸入數據的廣度、深度和質量來定義。相比之下，機器學習模型相對容易取用



碎片化的內部數據儲存

現有企業的財務數據分散於不同系統中，需要進行大量昂貴的數據工程作業才能創建出可用AI輸入的大型通用數據庫。



廣度和深度不足

更成熟的AI服務仰賴跨數據集提供的資訊。為了應對這種複雜性，需要在傳統和非傳統利益者之間建立新的以數據為中心的夥伴關係。



數據質量問題

現有機構已經擁有大量的數據，但其中大部分資料格式缺乏一致性，且可能包含錯誤。這使得AI應用變得困難，也增加跨企業部屬AI服務的成本。



不完善的合作&APIs

未來金融服務將依賴整個金融生態系統的數據，AI應用使跨機構獲取實時數據流的需求增加。在新的合作與系統整合出現之前，缺乏共同的數據共享標準是應用AI的瓶頸與障礙。



缺乏數據數位化

許多機構仍仰賴傳統數據採集方式（e.g. 紙張）。數據輸入的數位化將改善數據管理並提高流程的效率、準確性和一致性。



對客戶的理解不完整

如果我們使用AI來深化客戶理解，使用者必須能在跨機構和帳戶間訪問客戶信息，以全面了解客戶需求。目前，這些數據存在於各種不兼容的系統和格式中，使得AI驅動的數據分析無法充分發揮其潛力。

傳統技術基礎設施和嚴格的運營模式是現有的障礙

值得注意的營運挑戰

AI功能必須與核心系統基礎設施緊密整合才能提升價值，但許多機構仍然不願意優先考慮提升核心技術，特別是當升級無法立即獲得回報



舊系統和技術債務

現有機構的舊系統已經累積巨大的技術債務，需要進行大規模的整修才能實現AI技術。
(e.g. 配置API、導入實時數據流)



流程的重新設計

大部分的金金融服務現有流程考慮的主要是人與人之間的資訊流動。隨著AI的發展，新的流程需要更多考慮機器和人互動帶來的步驟與架構。



中介組織抵制變革

價值鏈中的流程轉型需要中介組織的投入合作。這些中介組織可能會抵制變革，並試圖影響營運的變化方向。



缺乏敏捷的雲端架構

為了發揮AI最大效能，機構需要可以快速存取與更新數據。背後的核心基礎架構可以由敏捷度高的雲端架構來提供。



重新設計組織結構

為配合AI的使用及效能，需要重新設計陳舊的組織結構，使其變得更為敏捷，並改變人才的定位以適應新的工作方式。



特定且任務導向的應用

目前的AI技術尚無法應用到所有情境，因此必須為每個情境案例設計模型。由於許多金融服務流程非常複雜和模糊，AI開發需要增加技術專家和領域專家的共同投入。

金融機構尚未發展合適方法管理AI帶來的人才轉型

值得注意的人才挑戰

機構若要透過AI發展優勢，需要應對不斷變化的人才需求。如何在AI發展與傳統政策下培養人才與有效工作方式，將為機構帶來不確定性與風險



不靈活的僱傭關係

金融機構的僱傭關係需要從傳統僵固的就業模式，轉型為以彈性為導向、獎勵生產力、以技術和能力為核心的僱傭關係。



技術與能力無法匹配

不只是市場上AI人才缺乏，機構也會因內部組織結構導致在招聘、留用或轉換機構需求的人才方面缺乏足夠能力。



不確定的變革願景

AI對於金融機構的變革規模要求常難以界定和維持。機構似乎還沒有關於個別工作職能如何轉換，以及如何在團隊和角色之間推廣變革的明確願景。



培訓能力不夠健全

由於AI人才的供應有限，迫切需把資源投入在企業內提升人員技能和意識。但現階段推廣受到培訓教師短缺，人員學習速度和個人能力的限制。



不兼容的企業文化

以權威、規則與日常作業為基礎的企業環境與文化，較難以過渡到以敏捷為核心能力的企業環境。



不完善的領導能力

傳統領導方式需要被打破，取而代之的是讓人才更積極的參與，提供更暢通的溝通管道和合作標準。現行有許多管理者在創造變革方面能力不足，使團隊的績效面臨風險。

現行監管制度難以跟上新興技術，為AI創新與應用帶來障礙

值得注意的監管挑戰

不靈活的要求和監管機構有限的資源使之難以跟上快速變化步伐的能力，為尋求新技術的機構帶來重大的監管不確定性。

監管框架的複雜性

監管框架過於複雜，而且沒有把AI應用考慮進去，大幅增加企業開發AI技術的難度。

缺乏身分與個資標準

要達到AI帶來的效益，需要機構間持續共享個人數據。為了確保安全性和隱私，企業必須要有健全的身分認證和標準化的驗證方法來降低風險。

創新與風險的平衡

由於AI系統過於複雜，監管體系在考量促進創新與降低風險兩者之間的平衡時，易傾向於優先降低風險。

零碎的數據共享法規

企業全球化的成敗取決於當地地區的監管環境。各國監管法規的不一致易阻礙跨國企業投資部署AI的速度。

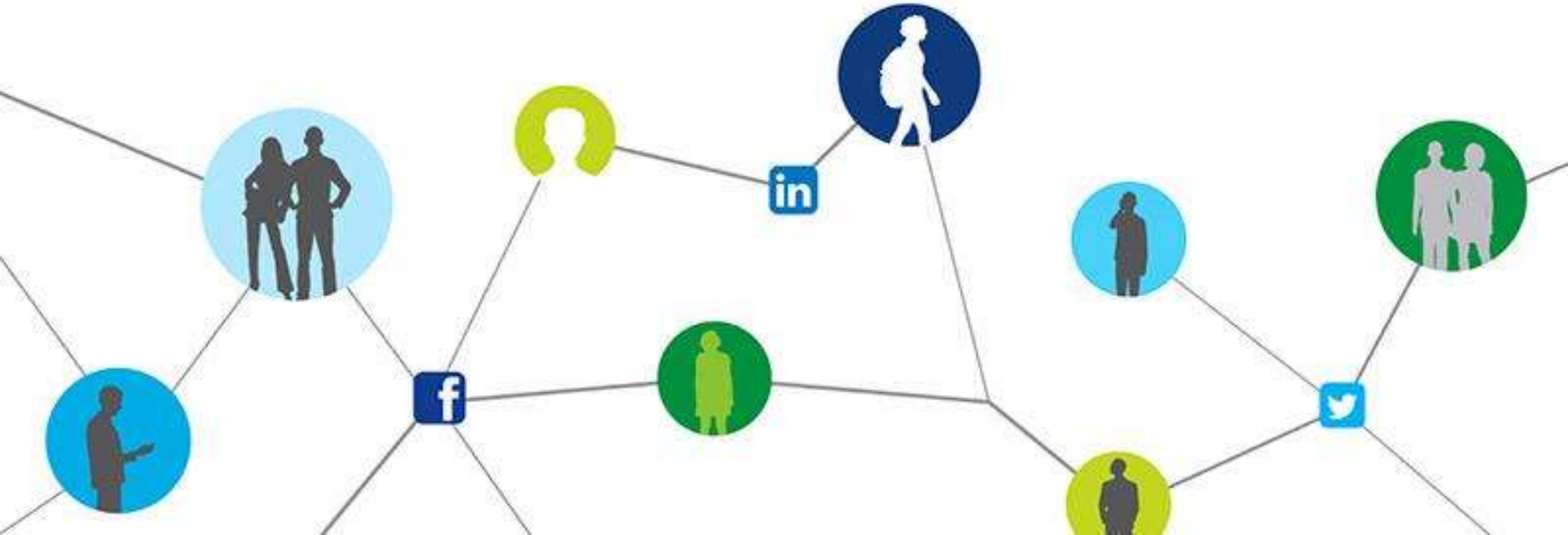
新系統的可審計性

監管機構要求對新的AI系統進行審核，但許多AI驅動的解決方案通常是複雜的黑盒子，何時與如何審核成為新的問題。

未定義的責任模型

對於AI導致損失的責任劃分模糊，以致企業對應用第三方AI技術有所猶豫，因為如果造成損害的話監管機關可能會要求主要企業負責。

Q & A



About Deloitte

Deloitte 泛指Deloitte Touche Tohmatsu Limited(即根據英國法律組成的私人擔保有限公司，簡稱"DTTL")，以及其一家或多家會員所。每一個會員所均為具有獨立法律地位之法律實體。Deloitte("DTTL")並不向客戶提供服務。請參閱 www.deloitte.com/about 了解更多有關Deloitte及其會員所。

Deloitte為各行各業的上市及非上市提供審計、稅務、風險諮詢、財務顧問、管理顧問及其他相關服務。Fortune Global 500大中，超過80%的企業皆由Deloitte遍及全球逾150個國家的會員所，以世界級優質專業服務，為客戶提供因應複雜商業挑戰中所需的卓越見解。如欲進一步了解Deloitte約245,000名專業人士如何致力於“因我不同，惟有更好”的卓越典範，歡迎瀏覽我們的[Facebook](#)、[LinkedIn](#)、[Twitter](#)專頁。

About Deloitte Taiwan

勤業眾信(Deloitte & Touche)係指Deloitte Touche Tohmatsu Limited("DTTL")之會員，其成員包括勤業眾信聯合會計師事務所、勤業眾信管理顧問股份有限公司、勤業眾信財稅顧問股份有限公司、勤業眾信風險管理諮詢股份有限公司、德勤財務顧問股份有限公司、德勤不動產顧問股份有限公司、及德勤商務法律事務所。

勤業眾信以卓越的客戶服務、優秀的人才、完善的訓練及嚴謹的查核於業界享有良好聲譽。透過Deloitte資源整合，提供客戶全球化的服務，包括赴海外上市或籌集資金、海外企業回台掛牌、中國大陸及東協投資等。

本出版物係依一般性資訊編寫而成，僅供讀者參考之用。Deloitte及其會員所與關聯機構(統稱“Deloitte聯盟”)不因本出版物而被視為對任何人提供專業意見或服務。在做成任何決定或採取任何有可能影響企業財務或企業本身的行動前，請先諮詢專業顧問。對信賴本出版物而導致損失之任何人，Deloitte聯盟之任一個體均不對其損失負任何責任。

