Web 3.0與人工智慧

郭耀煌 特聘教授

國立成功大學資訊工程學系

2022.07.22

大綱

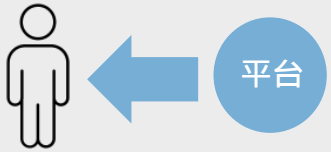
Web世代的演化

Web 1.0

參與者僅可**單向瀏覽、接收網頁訊息**，但無法創造內容

- 缺點：缺乏互動
- 如：電子郵件、BBS、靜態網頁

單向接收資訊



網路化

Web 2.0

參與者可**創造內容與更多價值**，網路互動性更高，但無法掌握數據，**網路為中心化管理**，掌握在少數公司手上

- 缺點：平台主宰，使用者有個資、隱私疑慮
- 如：FB、Twitter、Amazon、Uber等

透過中介雙向互動

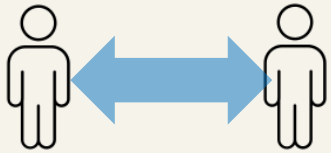
再中心化

Web 3.0

運用區塊鏈技術，參與者既可創造內容，也能**掌握數據**，網路呈現**去中心化**的狀態

- 缺點：技術難度較高，能否真正去中心化仍有爭議
- 如：加密貨幣、NFT、元宇宙、DeFi

無中介直接互動



去中心化

Web 3.0

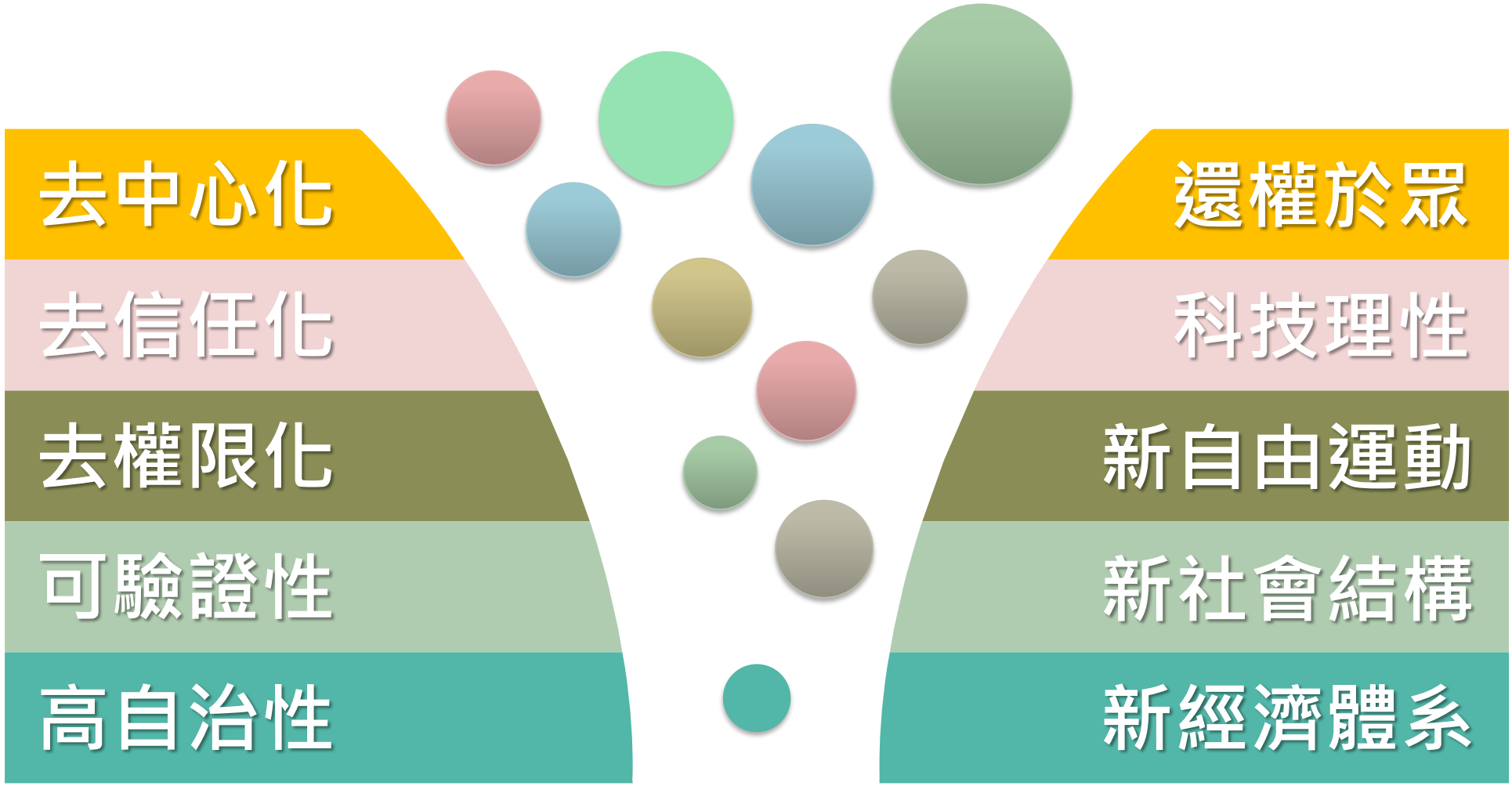
以**區塊鏈去中心化**技術為基礎建構的網路，可在**無集中式平台和中介**的情況下，實現**點對點互動**

特色

- **去中心化**（Decentralization）
- **去信任化與無權限化**（Trustless and Permissionless）
- **人工智慧與機器學習**（Artificial Intelligence and Machine Learning）
- **連通性與無邊界網路**（Connectivity and Ubiquity）

資料來源：各媒體、MIC，MIC整理，2022年4月

Web 3.0的特性與理念



Web 3.0的應用發展方向

智能合約

(Smart Contracts)

用於區塊鏈中制訂合約使用的特殊協議，運用代碼形式在區塊鏈上運行，儲存於網路共享資料庫中，合約透過共享資料執行應用程式，進行交易、轉移

+

- 組織規則
- 圖片、影像、聲音
- 金融產品
- 遊戲幣、遊戲寶物

=

去中心化自治組織 DAO
(Decentralized Autonomous Organization)

是一種扁平化、民主化的組織架構。其決策被記錄於去中心化帳本，營運亦以代幣進行

非同質化代幣 NFT
(Non-Fungible Token)

虛擬商品所有權的電子憑證，包含圖片、影像、聲音，甚至部分實體物品，是區塊鏈數位帳本上的資料單位

去中心化金融 DeFi
(Decentralized Finance)

不受中心化金融受銀行與政府主導，i建立在不可竄改的開放帳本，任何人都可訪問平台的金融基礎架構

遊戲化金融 GameFi
(Game finance)

遊戲中加入金融屬性，主打「Play to Earn」特性，將遊戲中的遊戲幣、寶物，變成虛擬貨幣或NFT

資料來源：MIC，2022年4月

大綱

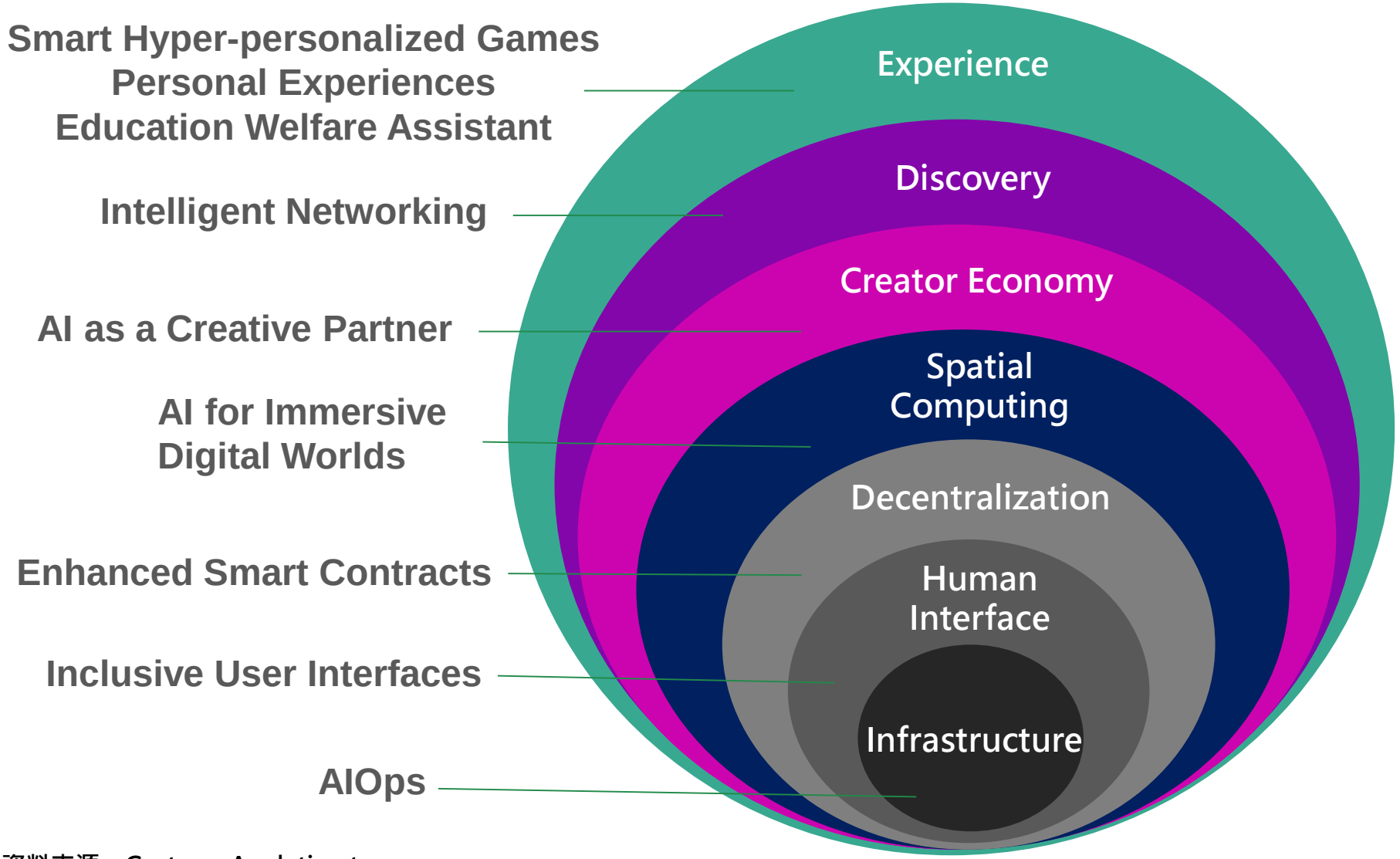
01 Web 3.0

02 **AI in Web 3.0/Metaverse**

03 相關治理議題

04 結語

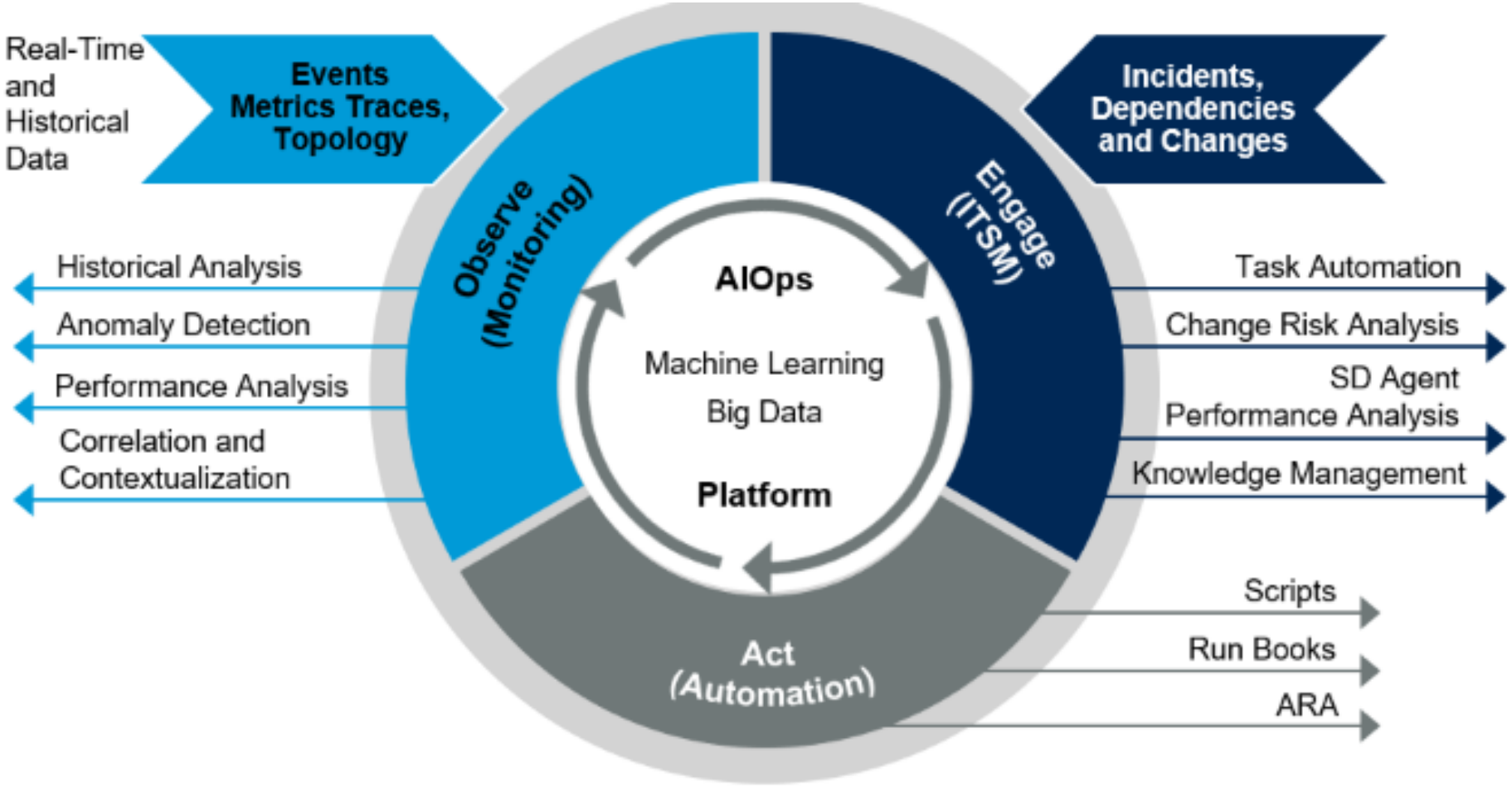
AI in Metaverse (1/4)



資料來源：Gartner; Analyticssteps

AI in Metaverse (2/4)

AIOps: AI協助元宇宙智慧維運基礎架構、網路通訊和基礎應用程式，以實現效能、彈性、產能、正常優化運行。



資料來源：Gartner, Analyticssteps

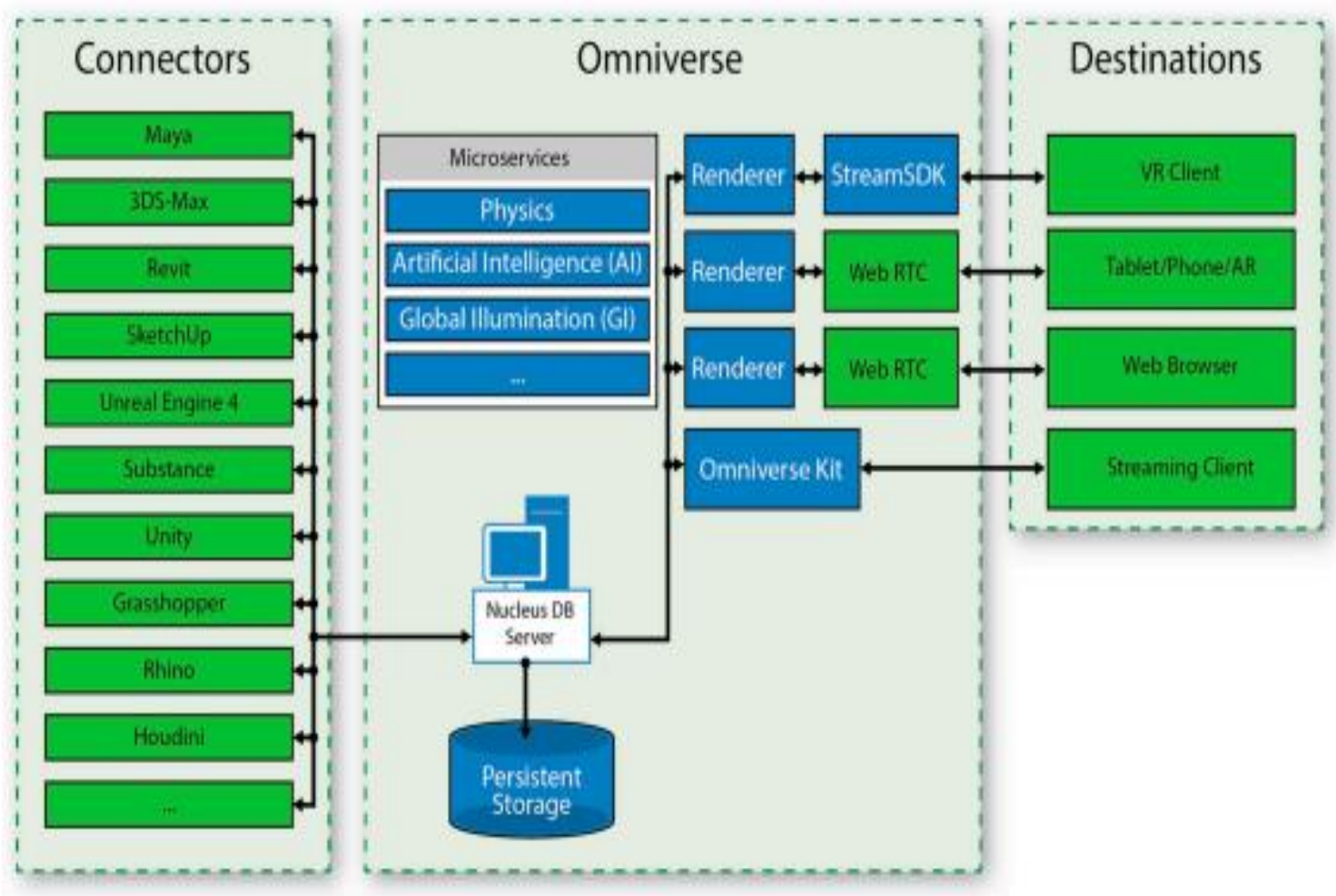
AI in Metaverse (3/4)

Inclusive User Interfaces

- AI考量不同類型使用者的感知能力、認知能力與移動能力，協助元宇宙建立包容性的使用者介面
- AI協助元宇宙建立科技無礙服務接取 (AI for Accessibility)

資料來源：Gartner; Analyticssteps

AI in Metaverse (4/4)



AI for Immersive Digital Worlds (NVIDIA OMINVERSE)

圖片來源：NVIDA

Enhanced Smart Contracts

AI協助強化智能合約，例如分析智能合約交易行為，偵測惡意交易

AI as a Creative Partner

AI是元宇宙內容創造的伙伴，搜尋&分析大量的資料帶來新的創造力

Intelligent Networking

AI協助元宇宙在社群網絡應用，包含強化數位自我與數位個人化

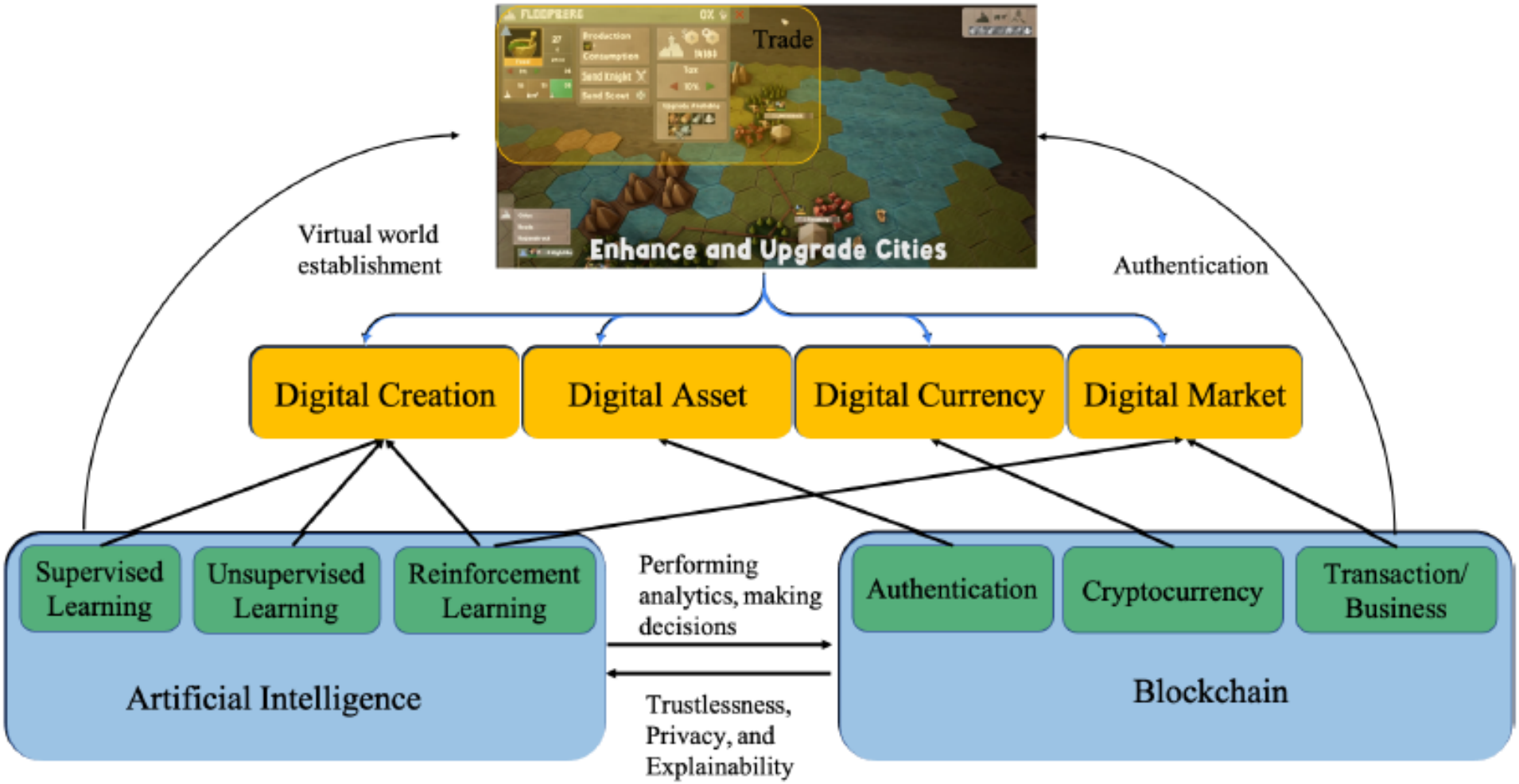
Web 3.0 Intelligence

Intelligent Blockchain		**AI 促成 Web 3.0 的 Blockchain 應用及共識機制(Consensus mechanism)、內存池(Mempool)、預言機(Oracle)等關健元件智慧化**
Intelligent Protocols		**AI促成Web 3.0的智能合約與協定智慧化，例如DeFi自動化市商(Automated Market Makers)智慧化與DeFi 借貸協議 (lending protocols)的自動評分**
Intelligent dapps		**AI 促成 Web 3.0 的去中心化應用 (Decentralized applications, dapps)智慧化，例如NFTs會具備智慧化行為，根據擁有者屬性智動化調整成合適狀態**

資料來源：Gartner; Analyticssteps

Intelligent Blockchain

AI協助區塊鏈應用的分析與決策



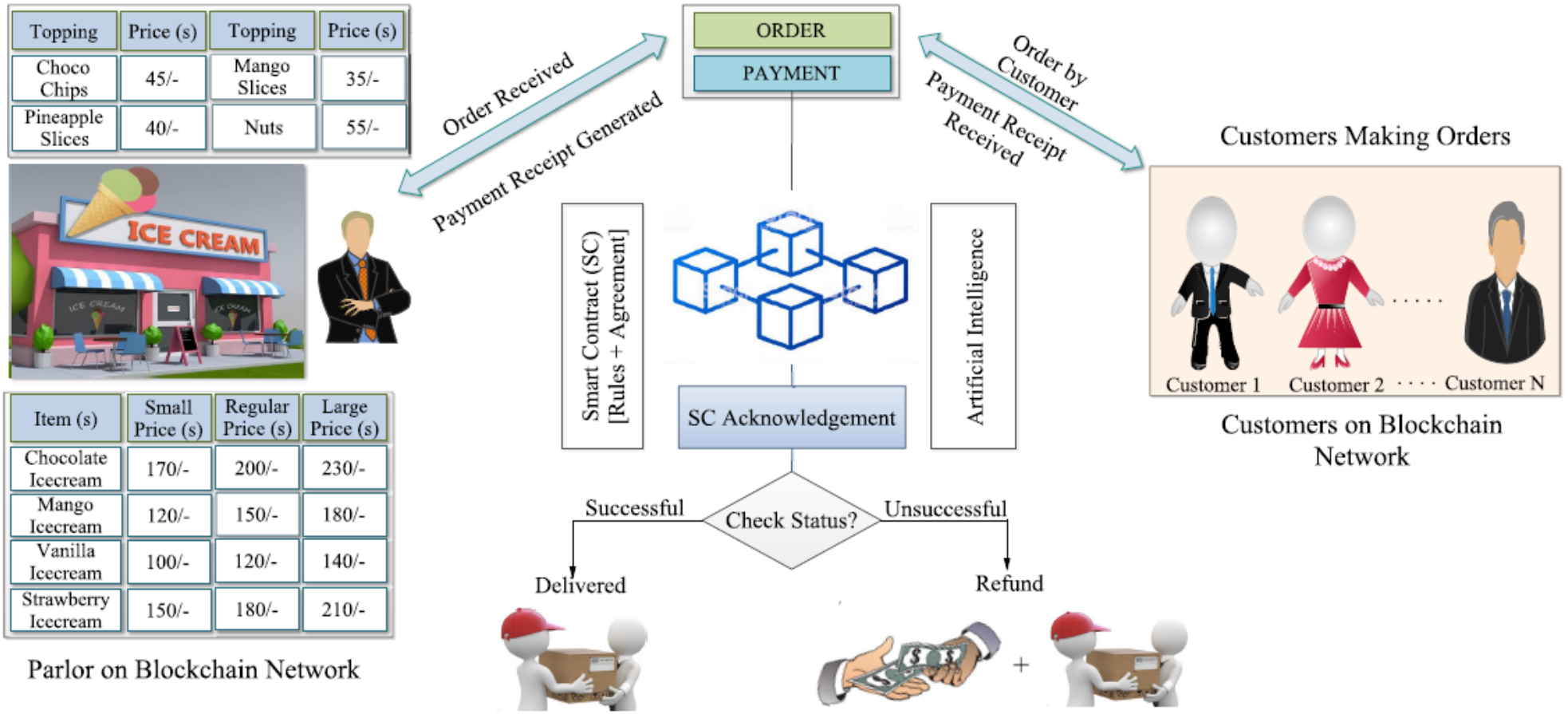
圖片來源： **Fusing Blockchain and AI with Metaverse: A Survey**

Intelligent Protocols

零售應用的AI智能合約

分析每次智能合約機制，提供異常偵測與告警

分析客戶的喜好與訂閱頻率評分，提供季度的折扣

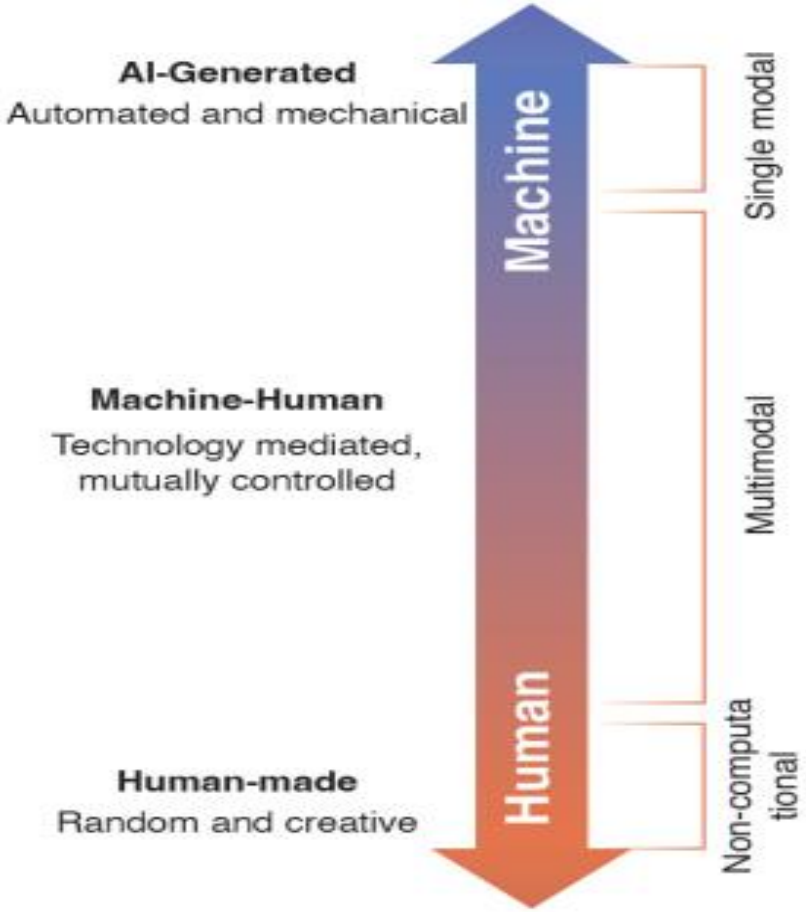


資料來源： **R. Gupta eta l.. Smart contract privacy protection using Ai in CPS: Tools, Techniques and Challenges**

Intelligent dapps

Humans.ai NFT: 使用者輸入文字，由AI技術經由文字建立聲音NFTs

Mirror World NFT: 透過AI技術創造智慧NFTs角色



Cases	Input	Interaction method
GAN	Non-human elements	Machine Features
VQGAN+CLIP DALL·E	Text-to-image	Type text
Human.ai NFT	Text-to-Voice	Type text
AI generates unique sounds		
Mirror World NFT	Text-to-AI, text-to-image	Intelligent dialogue
Intelligent AI characters		
Loot NFT	Human-huamn communication	Completely created by human
Bottom-up generating		

資料來源： **Decentralized, not Dehumanized in the Metaverse: Bringing Utility to NFTs through Multimodal Interaction; Mirror World**

AI in Web 3.0發展趨勢

WEB 3.0發展建立個人數位資產創建新的經濟合作網絡，AI技術往個人化、去中心化與可信賴發展

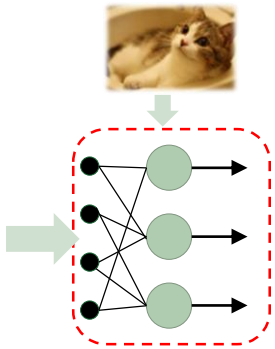
- 個人化學習模型
- 聯邦式學習模型
- 可信賴學習模型

一般化 → 個人化	使用者 → 擁有者	消費者 → 參與者	訂閱者 → 投資者
Web 3.0的個人數位資產應用多元，AI模型由一般化應用需求，往個人化應用需求發展	Web 3.0讓數位資產由使用者轉變成擁有者，AI模型往擁有者在創造、分析與決策應用發展	Web 3.0讓數位應用消費者轉變成參與者，AI模型往協助參與者在互動溝通、媒合應用發展	Web 3.0讓數位應用的訂閱者轉變成投資者，AI模型往協助投資者在推薦、創造價值應用發展

近期人工智慧發展趨勢

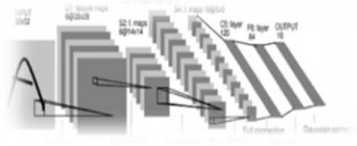
Meta Learning

自主找最適合的學習參數



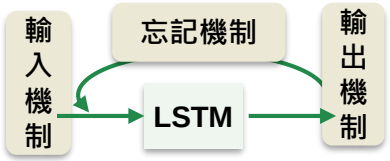
「學習如何學習」的方法，思考運用不同方法（演化法、貝式法、增強學習...等）讓AI在訓練時得以自行找到最適化的調校參數

CNN



卷積神經網絡，從一塊塊矩陣中向一層層網路進行歸納

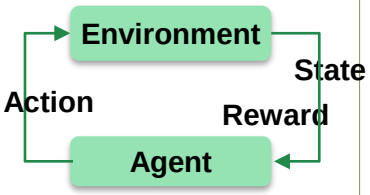
RNN/LSTM



運用神經網絡的方式處理具時間序列的問題

聯邦式學習（Federated Learning）

Deep RL



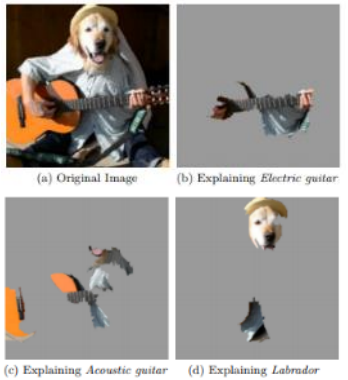
深度學習結合增強學習後來達到領域的自主學習能力

GAN

「生成模型」不斷與「判別模型」彼此訓練，收斂後再加模仿應用

XAI

（Explainable AI）



針對圖像、聲音、文句辨識或判讀上的進行部分解釋，與使用者共同獲得的判斷基礎，進行下一步決策

Transfer Learning

運用之前訓練的模型（如: Cat model）轉移到另一個事物的辨識，以較少的樣本規模的訓練則可獲得目標模型（如:Leopard）

資料來源：MIC，2021年5月

聯邦式AI:「模型共享」取代「資料共享」

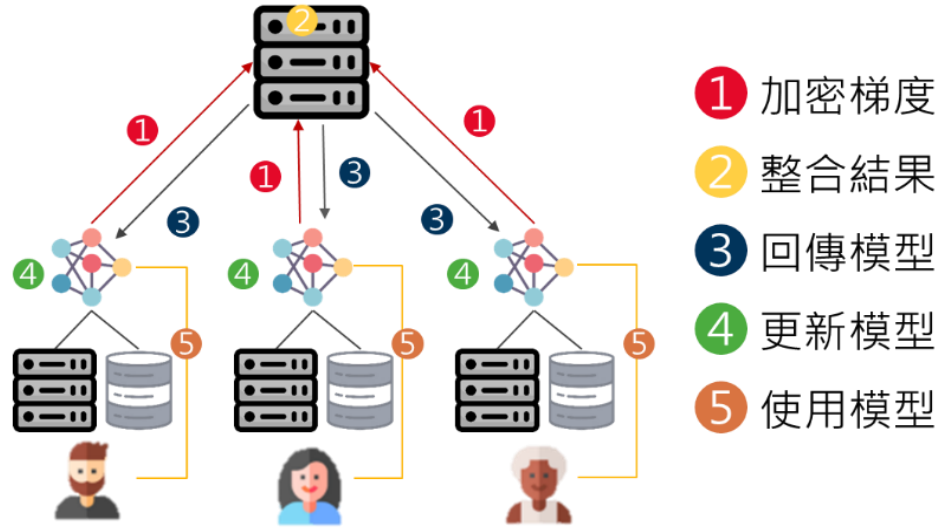
聯邦式AI可以達到不同角色間在資料隱私性的保護，並同時解決數據孤島（Data Silos）情況，運用這樣的特性，有利協助產業界在不用分享資料的情況下，訓練出共同的模型，藉此來改善產業的AI模型訓練議題

傳統「資料共享」訓練模式

- 過去為了優化AI演算法，會將用戶資料上傳到資料中心進行訓練，但歐盟通過GDPR法案後，明確規定對個人資料的使用行為必須要有用戶的授權與同意，這讓資料使用、整合與共享形成一道難以跨越的高牆

聯邦式AI「模型共享」訓練模式

- 聯邦式AI突破「資料共享」與「患者隱私」之間的難題，以「模型共享」方式，在資料不用離開用戶裝置的情況下，進行AI演算法訓練



備註：GDPR（General Data Protection Regulation）
資料來源：MIC，2022年4月

Privacy Preserving AI (1/2)

個人

消費者購買產品產生偏好數據，但可能涉及消費者**隱私**，擔心曝露。

提供偏好數據

企業

從消費者或客戶所收集的數據可以帶來**競爭優勢**；也可以幫助企業改進和客製化產品和服務。

提供產品優化

如何信任企業？

如何去識別化？

目前瓶頸：個體數據難以確實匿名化

解決方案：Privacy Preserving AI

又稱為差分隱私(Differential Privacy)

Privacy Preserving AI 概念：「為一種資料共享演算法，當從數據資料庫查詢時，**最大化資料查詢的準確性，同時最大限度減少識別其記錄的機會；主要是透過在資料加上雜訊(noise)**，在保留統計學特徵的前提下，隱藏個體特徵以保護使用者隱私。」

Privacy Preserving AI (2/2)

Privacy Preserving AI (差分隱私) 目前兩種主要技術

局部差分隱私 (Local differential privacy)

將雜訊(noise)添加到數據集中的每個單獨數據資料。

全局差分隱私 (Global differential privacy)

在數據集查詢輸出中添加保護隱私所需雜訊(noise) 。

然而 Privacy Preserving AI 在實務上仍存在限制

大型數據較能見成效

差分隱私適合運用在有多個大型數據集，並有一定營運流程和數據管理框架的大型企業，例如大型電子商務網站，數據規模大也較易埋入雜訊保護隱私。

隱私洩漏另有原因

中小型企業數據規模小，埋入雜訊反而更顯突兀易洩漏隱私。且中小型企業數據洩漏的主要來源是密碼薄弱、數據未加密、軟體未更新或缺乏存取控制等因素。

演算法透明度標準仍未訂

即使開發人員、Google，以及其他大型技術公司(如：Apple)…等，宣稱會在用戶數據中加入一定程度的雜訊來保護隱私，用戶也無法知道其內部具體保護標準。

大型企業

中小型企業

領導業者

個人數據隱私將成價值主張，具隱私承諾的服務將為關鍵

大綱

01 Web 3.0

02 AI in Web 3.0/Metaverse

03 **相關治理議題**

04 結語

Web 3.0發展之主要議題

	產業面	法規面	安全面
DAO	去中心、去階層化的管理方式未必更有效率	DAO的法律地位不明確，責任歸屬問題亦存在爭議	DAO的安全性並非牢不可破，可信任程度有待更多驗證
DeFi	去中心化交易所（DEX）交易門檻高	DeFi處於法律模糊地帶，較難適用現有法規管制	DEX不受監管的去中心化機制仍面臨駭客攻擊威脅
NFT、GameFi	NFT投資泡沫、加密貨幣價格波動等議題不斷	NFT未被列入監管，僅提醒為高投資風險商品	NFT資安事件頻傳，持有者被駭後將難以追溯

AI倫理與監管

隨著AI逐步落地及擴散，使用風險及造成傷害隨之增加，各國政府已開始重視對AI監管，特別是高風險應用，而AI用於重要決策時，需具備可解釋性

歐盟可信賴AI倫理準則

4項倫理原則

- *尊重人類自主權*
- *避免傷害*
- *公平*
- *可解釋性*

7項具體要求

- 人為監督
- 技術健全和安全性
- 隱私和資料治理
- 透明性
- 環境和社會福祉
- 可歸責性
- 多元化、非歧視性和公平性

LF AI

Linux Foundation 開源工具

- AI Explainability 360
- AI Fairness 360
- Adversarial Robustness Toolbox

資料來源：歐盟，IBM，MIC整理，2022年1月

科技演算法治理

- 演算技術儼然已成為經濟社會的底層架構，演算技術決定巨量數據利用的深度與功用，是數據利用最為廣泛且核心的工具
- 當科技嵌入大眾生活的比例攀升又缺乏人工干預時，有缺陷的軟體演算法將導致算法黑箱
- 透明度與問責制對於給消費者選擇及為政策制定者提供必要資訊以制定關鍵決策至關重要

加拿大

2019年公佈「關於自動決策指令」，提出算法影響評估程序

美國

公佈「2022年算法責任法」(草案)，目的為確保及強化對軟體演算與其他自動決策系統的透明度與問責制監管，避免算法歧視

歐盟

- 2018年公佈「一般資料保護規則」，規範若數據主體認為算法決策結果與預期不符合時，有權要求對算法設計以及運行(即數據分析處理過程)進行解釋的權利
- 2019年公佈「可信賴AI倫理指南」，目的為幫助評估正在開發、部署、採購或使用的AI系統是否符合可信賴原則

國際清算銀行

在支付和其他金融服務領域發揮關鍵作用的科技公司應如傳統銀行一樣接受嚴格的監管，避免發生資料治理、反壟斷或其他系統性風險問題

VISA

提出「金融科技夥伴連接」計畫，目的是為提供客戶能夠快速與經過審查的技術提供商(資服業者)建立聯繫

中國大陸

- 2022年中央網信辦公佈「互聯網信息服務算法推薦管理規定」，聚焦算法的開發、設計至結果的產出必須公正透明，保護用戶權益，確保算法的公平性
- 中國人民銀行制定「人工智慧演算法金融應用評價規範」，針對AI可能存在的風險問題，建立一套評估架構，從安全性、可解釋性、精准性及性能等方面提出基本要求、評估方法與判定準則

紐西蘭

2020年公佈「算法章程」，規定政府機關在採用可能對社會大眾產生重大影響的算法技術前應提交評估報告

資料來源：各新聞網站資料，MIC整理，2022年6月

數據隱私保護

- 當數位足跡成為大眾生活的表彰，數據所有權與數據隱私問題將更重要
- Gartner評估至2023年全球65%的人口的個人數據將受到現代隱私法規的保護(2021年只有10%)

美國
- 加州「CPRA」2023年生效
- 科羅拉多州「CPA」2023年生效
- 維吉尼亞州「CDPA」2023年生效
- 紐約州「僱員監控和紐約民權法的修正案」 2022年生效
- 阿拉斯加州、佛羅里達州、馬里蘭州、麻薩諸塞、明尼蘇達州、密西西比州、紐澤西州、北卡羅來納州、俄亥俄州、賓夕法尼亞州、華盛頓州 等隱私權立法正在審議中

德國
「德國民法典」第327q條於2022年1月生效，加強對消費者個人數據保護

歐盟
預估2022年完成相關數據隱私保護立法，包含：「數位服務法」、「數位市場法」及「資料治理法」等

日本
2022年4月「個人資訊保護法」修正案開始生效

印度
預估2022年通過2019年提案的「個人數據法」，該法案將涵蓋個人與非個人數據

新加坡
2019年頒布「新加坡可信資料共享框架」

中國大陸
頒布「網絡數據安全管理條例」與「跨境數據傳輸安全評估辦法」，旨在強化對數據跨境傳輸的管理

澳洲
預估2022年將公佈「2021年隱私立法修正案」，強化對用戶線上隱私的保護

- 愛爾蘭：預計2022年開始實施「2019年數據共享與治理法案」
- 韓國：2022年可能針對「個人信息保護法」進行修訂
- 斯里蘭卡：預計2022年「個人數據處理規定法」生效
- 瑞士：預計2022年修訂後的「瑞士聯邦數據保護法」將生效
- 泰國：預計2022年「2019年個人數據保護法」生效

資料來源：各新聞網站資料，Gartner，MIC整理，2022年6月

大綱

01 Web 3.0

02 AI in Web 3.0/Metaverse

03 相關治理議題

04 結語

建構*formosa@metaverse*新世界

發展策略

高值創新	科技自主	社經共榮	全球運籌

發展重點

元宇宙 創新經濟	智慧生活 國民經濟	地球永續 轉型經濟	數位韌性 國安產業鏈

發展目標

扶植具無邊界市場拓展活力之元宇宙創新創業生態系	成為智慧城市、智慧製造及智慧醫療系統之國際供應樞紐	扶植數位、零碳雙轉型服務鏈，開發SDG/ESG新商機	扶植提升國家數位韌性之資安、自主載具與先進通訊產業鏈

配套措施

促進投資	吸引人才	產業環境
吸引企業投資與活絡資本	跨域、跨境人才延攬與培育	數位沙盒、資料流通、創新採購