DeFi（去中心化金融）重點筆記

只保留：是什麼｜用途｜用在哪｜怎麼 work ｜例子

DeFi Wallet DEX AMM Uniswap Liquidity TVL

快速總結（考前 30 秒）

- **一句話**：DeFi 用**智能合約**把「借貸、交易、資產管理」搬到鏈上，讓**個人即帳戶**、資產不再依賴平台托管。
- **完整金融版圖要含**：不只借貸/收益協議，還要把**錢包 + 交易所（DEX/CEX）**納入理解，才看得見 Web3 的金融基礎設施。
- **錢包的本質**：**私鑰的容器**（丟助記詞＝丟錢包）；地址像卡號，私鑰像最終控制權。
- **DEX 的本質**：不托管資金，交易用**私鑰簽名 + 合約執行**；資產直接到錢包，無須「充值/提現」。
- **AMM 的本質**：用演算法報價做市（常見 CPMM：$xy = k$），**流動性**越大，滑點越低；套利讓價格回到市場。

Contents

1 DeFi 是什麼？(定位與範圍)

一句話定義

DeFi（Decentralized Finance）是基於區塊鏈的去中心化金融系統：透過**智能合約**在鏈上完成交易、借貸、資產管理等金融功能，減少對銀行／券商等中心化機構的依賴。

用途／用在哪（建立 Web3 金融地圖）

- **用途**：讓資產控制權回到個人；規則可驗證、流程可自動化；降低平台托管風險。
- **用在哪**：面向消費者的 DApps 中，DeFi 是最早且數量最多的一類。
- **範圍提醒（文章主張）**：不要只把 DeFi 狹義理解為「借貸/收益」；**錢包與交易所**也屬於 Web3 金融基礎設施的一部分。

文中例子（Web2 vs Web3）

- Web2：你可能同時有**支付寶、微信、網商銀行**等帳戶；資產與權限由不同服務商平台掌控與解釋。
- Web3：錢包可脫離平台存在；**個人即帳戶本身**，資產統一歸屬個人。

怎麼 work（直覺對比：Web2 平台錢包 vs Web3 私鑰錢包）

- **Web2**：帳戶是「平台給你的」；資產（餘額/券/資料/商品與服務權益）都依附平台；平台決定認證、權限、交易型態。
- **Web3**：區塊鏈作為去中心化底座；錢包不是平台帳戶，而是**私鑰系統**；你用私鑰簽名完成資產操作，平台無須成為托管者。

2 Web 3.0 錢包（Wallet）

一句話定義：錢包本質是什麼？

加密錢包的本質是**保存私鑰的容器**：它讓你能簽名交易、證明你對鏈上資產的控制權。(廣義可理解為「存放加密資產的容器」；但核心仍是私鑰。)

用途／用在哪

- **用途**：接收／保管／轉移加密資產；在 Web3 中對應「存款/資產保管」功能。
- **用在哪**：比特幣等加密資產的**轉帳、歸屬、存儲**需要靠錢包完成（點對點支付 + 公開可驗證的交易記錄）。

錢包怎麼 work（地址 / 私鑰 / 助記詞）

組成

- **地址**：由公鑰哈希生成，用於收款（類比「銀行卡號」）。
- **私鑰**：驗證身份並操作資產的鑰匙（類比「最終控制權」）。

非托管錢包（例：MetaMask）的助記詞機制（文章版流程）

1. 建立錢包時生成 **12 個英文單詞**的助記詞（BIP39，來源於 2048 詞庫）。
2. 助記詞對應數字序列（Seed Integer）。
3. Seed Integer 經 SHA256 生成私鑰；再經 ECDSA 等生成公鑰／地址。

文中例子（跨錢包恢復）

> MetaMask 生成的助記詞，輸入到 imToken 仍可進入並控制同一資產。
> 因此錢包 App 只是「殼」，**助記詞才是錢包本體**。

分類（一定要會背的兩軸）

按控制權：托管 vs 非托管

- **托管錢包**：私鑰由平台掌握；登入多是「手機/信箱/帳密」形式（例：各種中心化交易所的錢包）。
- **非托管錢包**：私鑰完全由自己掌握（例：MetaMask）。

按存儲介質：

- 網頁錢包、桌面錢包、手機錢包、**硬體錢包**（最推薦之一）、紙錢包

熱/冷錢包：

- 私鑰實際保存地在網上：**熱錢包**
- 私鑰實際保存地不聯網：**冷錢包**

風險／注意（文章明確點名）

- **資產兼容性**：不同錢包能存的資產種類不同；強行存入不支持資產可能導致**資產丟失**。
- **助記詞/私鑰安全**：助記詞就是錢包全部；丟失＝丟錢包（沒有找回機制）。
- **托管錢包不等於去中心化**：公鑰/私鑰在托管方手中，依然存在平台風險。

3 DEX vs CEX（去中心化交易所 vs 中心化交易所）

一句話定義

DEX（去中心化交易所）是鏈上交易基礎設施：不要求用戶把資金與個資轉入交易所，只用智能合約完成撮合與結算，交易發生在參與者之間。**CEX（中心化交易所）**則由平台負責充提、撮合、結算與托管（像把交易所 + 券商 + 投行功能集合在一個中心化系統）。

用在哪（文章提到的例子）

- **CEX 代表**：Binance、Coinbase、FTX（文章列舉）
- **DEX 代表**：Uniswap（交易量最大的 DEX；本質是以太坊上的協議）

怎麼 work（核心流程差異）

交易所核心環節（文章）：充提、下單、訂單撮合、資金結算、提現

- **CEX**：撮合與結算在平台內完成（不上鏈），速度快、深度好，但資產集中托管。
- **DEX**：上述環節**全部上鏈**由智能合約執行；下單需用**私鑰簽名**；撮合成功後資產**直接到錢包**，無須提現。

文中例子（資產是否觸碰）

- CEX：用戶資金集中在交易所帳戶，資金量大 → 更容易成為黑客目標。
- DEX：平台不托管資金；只在交易瞬間由合約撮合與驗證；資產直接回到錢包。

取捨（文章點出的現實問題）

- **DEX**：完全鏈上 → 可能流動性較差、成本高、速度慢。
- **CEX**：集中托管 → 一旦出事可能影響幾乎所有用戶。

4 Uniswap（DEX 協議）

是什麼

Uniswap 並非「公司式交易所」，而是部署在以太坊上的一套**協議（智能合約集合）**。V1（2018）到 V3 的核心升級主線：**提高資本使用效率**。

用途／用在哪（文章列出的設計目標）

- **易用性**：Token A 換 Token B，可**一筆交易**完成
- **Gas 高利用率**：相對主流 DEX，交易 Gas 較低
- **零抽租**：協議不抽走交易費；費用回到**流動性提供者（LP）**
- **抗審查**：上架新通證門檻低（任何人可上架任意通證）

文中例子（易用性對比）

> 在某些交易所你可能要兩筆：A 先換成 ETH/DAI 等媒介，再換成 B；
> 而 Uniswap 一筆交易即可完成 A → B。

5 AMM（自動做市商）與 CPMM：$xy = k$

一句話定義

AMM（Automated Market Maker）是 DEX 的核心引擎：用演算法自動報價並與交易者成交；**流動性質押（Liquidity Staking）**則是 AMM 的能量來源（提供資產池彈藥）。

AMM 至少要滿足的 4 件事（文章列舉）

- 持有兩種資產（雙向報價）
- 資產池可充值/提現
- 能隨市場自動調價
- 能靠交易費等獲利/分配收益

怎麼 work（CPMM：恒定乘積做市）

最常見 AMM 模型：**恒定乘積**（CPMM）

$$x \cdot y = k$$

其中 x、y 是池內兩種資產數量，k 維持不變；交易會改變 x, y，價格隨之自動調整。
文中例子（“無人超市：雞蛋 × 牛奶 = 5000”）

- 初始：100 顆雞蛋、50 瓶牛奶，$100 \times 50 = 5000$。
- 買 2 顆雞蛋後：雞蛋剩 98，牛奶需變為 $5000/98 \approx 51.02$，所以要付 $51.02 - 50 = 1.02$ 瓶牛奶。
- 若一次買走 50 顆雞蛋：雞蛋剩 50，牛奶需 $5000/50 = 100$，要付 50 瓶牛奶（價格急升）。
- **套利者**會在外部市場換到雞蛋再來池子換牛奶，靠套利修正價格，使池內價格回到合理區間。

注意：流動性不足會放大滑點（文章給的直覺算例）

- 若池子很小（100/50），買 2 顆雞蛋就出現約 2% 的價差。
- 若池子很大（100 萬/50 萬），同樣買 2 顆雞蛋，報價接近 1.000002（約 0.002% 的價差）。
- **結論**：流動性越大，價格越穩、滑點越低。

6 流動性質押（Liquidity Staking / Mining）與 TVL

一句話定義

流動性質押（又稱流動性挖礦）是 LP 把資產質押進 AMM 資產池，為交易/借貸提供流動性以獲取回報。**TVL（Total Value Locked）**是協議中被鎖定的資產總額。

怎麼 work（收益從哪來）

1. LP 把資產存入池子（提供流動性）
2. 交易者在 DEX 交易支付**手續費**
3. 手續費按 LP 佔池子總量的比例分配

文中例子（按占比分成）

> 若你提供的質押價值佔資產池 1%，那你可獲得該池交易費總收益的 1%。

文中歷史例子

- IDEX（2017）提出流動性質押概念
- Compound 在 2020 年 DeFi Summer 引入流動性質押

7 Uniswap V1 / V2 / V3：交易機制進化史

V1 → V2 → V3（只記升級主線）

V1（基礎 CPMM）

- 典型恒定乘積池，主要靠套利修正價格偏離

V2（TWAP + Flash Swap）

- **TWAP（時間加權平均價）**：用一段時間的累積價格/持續時間得到平均價；**平均時間越長、流動性越高**，操縱成本越高。
- **Flash Swap**：可先取走想要的 ERC-20 通證，**交易結束時歸還**即可（降低套利前置資本門檻）。

文中例子（Flash Swap 的意義）

> 如果套利者沒有本錢也借不到資產，價格異常可能無法及時被修正；
> Flash Swap 讓套利可在無前置成本下完成，促進價格回歸。

V3（集中流動性：Concentrated Liquidity）

- V2：LP 資金沿 $xy = k$ 的**全價格區間**均勻分布（理論 0 到無窮）。
- V3：LP 可自選**特定價格區間**提供流動性，把資金集中在交易最活躍區間，提高資本效率並**降低滑點**。

8 DeFi 的未來：對傳統金融功能的映射與缺口

金融「三駕馬車」映射（文章框架）

- **銀行**：借貸 → 借貸池（Lending Pool）；存款 → 錢包
- **券商**：做市/經紀 → AMM + LP（已相對成熟）
- **保險**：相對容易遷移，但難在**定價與核保**

文章提到的對應案例（只留點名 + 直覺）

借貸池（銀行借貸對應）

- Aave（規模最大）、MakerDAO、Compound、Anchor
- 無抵押借貸：TrueFi、Wing（規模小，偏向 Web3 資管公司，難以評估實體經濟信用）

投行/資管探索

- Ondo：把鏈上資產彙集後，按風險收益拆分重包裝成多種產品
- Cult DAO：去中心化風投；資金來自 CULT 交易費；持幣者投票決定投資

保險（產品點名）

- Nexus Mutual、Unslashed、inSure、Solace、Bridge Mutual
- 定價多仍靠中心化方式（如精算）；核保常用投票（或委託 Kleros 這類陪審團機制）

最大瓶頸：KYC / 身份與信用（文章收束點）

- 金融業關鍵要素之一是 **KYC**；DeFi 若要擴到更複雜場景，需要更成熟的鏈上身份與信用機制。
- 文中引用觀點：需要一種與人深度綁定的**身份通證**，能在加密世界還原人際關係並綁定個人信用（提及維塔利克 2022/5 的相關論述）。

9 快速複習題（自測用）

Q1：為什麼文章說理解 DeFi 要把錢包與交易所也算進來？

A：因為 Web3 的金融活動（存儲、轉移、交易、借貸）都離不開**錢包（私鑰/資產控制）**與**交易所（資產交換）**這兩個基礎設施；只看借貸會漏掉「資產如何被你真正擁有與交換」。

Q2：錢包的兩個核心組件是什麼？

A：**地址**（收款，類比卡號）＋**私鑰**（簽名與控制權，丟了找不回）。

Q3：托管錢包 vs 非托管錢包差在哪？

A：**私鑰誰掌握**。托管錢包私鑰在平台；非托管錢包私鑰在自己（例：MetaMask）。

Q4：DEX 為什麼說「平台不碰資產」？

A：因為用戶資產不需要充值到平台；交易靠**私鑰簽名**與**智能合約**撮合驗證，資產**直接回到錢包**，無須提現。

Q5：AMM 的 CPMM 為什麼需要套利者？

A：因為 $xy = k$ 會在大額交易後造成價格偏離；套利者利用外部市場價格差來交易，從而把池內價格推回合理區間。

最後一句（考前記這句）

Web2 的錢包是「平台帳戶」；Web3 的錢包是「**私鑰系統**」。
DEX 用**合約**替代平台撮合，AMM 用**演算法**替代訂單簿；流動性與套利共同維持市場可用性。