Hw0 b10902124陳昕

1a) What's new in Uniswap v4, compared with Uniswap v3?

Hooks and custom pools: Hooks是可客製化的 Smart Contract，可由任何人、任何協議部署，並和單一個 Uniswap Pool 綁定，Hooks 能夠在liquidity pool's lifecycle中指定的key points執行。提供開發者巨大的彈性創建客製化的liquidity pool來滿足他們的需要。

Singleton: 在v3中，每創建一個liquidity pool就必須部署一張新合約，使得creating pools和multi-pool swaps價格昂貴。而v4把所有liquidity pool都放在1張contract上，極大的減省了gas fee，這是因為不需在不同contracts中轉移token，uniswap預估此創新可以減少creating pools 99%的gas costs。

Flash accounting: 在之前Uniswap中，每個操作，如token交換或增加liquidity到pool中，都以token轉移結束。在v4 中，每個操作不是立即轉移token，而是更新到一個稱為 delta 的內部淨餘額。這意味著在操作期間，token不會立即在帳戶之間移動，外部轉移在最後才執行，這簡化了pool operation並大幅降低了成本。

1b) An easier question is as follows: What's new in Uniswap v3, compared with Uniswap v2?

Concentrated Liquidity: 在v3中，lp可以將資金集中在自定義的範圍內，以期望的價格提供更多的流動性，而非像v2版本的流動性在0到無窮大之間，導致絕大多數的流動性從未被使用。

Improved Price Oracle: 在v3中，通過使用儲存累積價格，我們可以在一次鏈上調用中計算過去約 9 天內的任何 TWAP。而非像v2儲存1個，此外，更高的粒度和更新頻率，使得在高交易量的時期，也能得到更精準的價格資料。

Multiple Fee Tiers: 提供三種不同的fee tiers (0.05%, 0.30%, and 1.00%)，讓lp可以彈性的調整其利潤。

2a) As Uniswap's Singleton smart contract (See Uniswap) 在 ERC 4337 的定義當中出現, explain ERC 4337 in the light of Singleton smart contract.

從Singleton smart contract的角度來看，ERC-4337的核心是確保所有操作都通過一個中央化的檢查點，這個檢查點就是EntryPoint contract。所有符合ERC-4337的智能合約錢包都必須使用它來在EVM上進行交易，這有助於提高安全性且簡化各個智能合約錢包的邏輯。

2b) Uniswap mentioned hook. Explain the hook here.

Hooks是可客製化的智能合約，可由任何人、任何協議部署，並和單個 Uniswap Pool 綁定，Hooks能夠在liquidity pool's lifecycle中指定的key points執行，帶來了極大的彈性。

2c) Uniswap mentioned flash accounting. How is flash accounting enabled by "transient storage" in ERC 1153?

在1a)中有提到flash accounting透過存儲淨餘額來減少外部轉移的數量，然而，利用傳統的方法在每次餘額變動時去永久化存儲在區塊鏈中，這會消耗掉大量的gas，所以Uniswap v4利用transient storage，根據EIP-1153的規定（如果storage slots在交易結束前設置為原始值，則退還Gas），允許臨時更改而不產生長期存儲的gas，大大減少用戶成本。

3) Why does VItalik emphasize AA (Account Abstraction) and intent-centric recently?

EOA錢包依賴單一私鑰，並存在以太坊之外，用戶保管能力是一大風險；AA則將帳戶的概念移植到智能合約中，可以有多組私鑰管理，可以使用各種簽章演算法，可以執行多個calls，也不像CA一樣無法作為交易發起者，還要透過relayer去發起交易，極大改善了原生以太體系的缺點。Intent-centric旨在讓用戶不需了解詳細的交易細節，而是用戶發送他想要的請求，就可以透過resolver來設計出最適合的交易流程，或許能大規模降低用戶需要了解的區塊鏈程度，VItalik認為這樣也能提升用戶的隱私和安全。