2024-Spring-Midterm

- Blockchain
  - What is the PoW consensus mechanism in Bitcoin Network, and PoS in Ethereum Network?
    - PoW共識機制 (Bitcoin Network)：工作證明(PoW)是比特幣網絡使用的共識機制，要求參與者解決一個難度較高的數學難題來證明其工作量。這種方式能夠確保網絡的安全性和去中心化，因為想要控制網絡，攻擊者需要擁有過半數的計算能力。
    - PoS共識機制 (Ethereum Network)：權益證明(PoS)是以太坊網絡目標的共識機制。在PoS中，區塊的創建者是通過其持有的幣的數量和時間長短來選出的，而不是依靠計算能力。這種方式更加節能且安全。
  - What is the gas mechanism prior to EIP-1559 and how does it work?
    - Gas機制 (EIP-1559前)：在以太坊中，執行交易或智能合約操作需要消耗Gas。Gas是一種內部計費單位，用來度量執行操作的計算工作量。交易發起人需按Gas消耗量和Gas價格支付ETH作為手續費。
  - What is EIP-1559 and what does it solve?
    - EIP-1559：是一項以太坊改進提案，旨在改善Gas費用的市場，引入基本費用概念和尖峰費用機制，並且每筆交易的一部分手續費會被永久燒毀，這有助於減少網絡擁堵和手續費的波動，同時使ETH更加稀缺。
  - What is testing network and mainnet? What is a faucet? What can it do?
    - 測試網絡和主網(Mainnet)：測試網絡是用於開發和測試智能合約的區塊鏈網絡，不涉及真實資產。主網是運行真實交易的區塊鏈網絡。
    - 水龍頭(Faucet)：是在測試網絡中用來獲取測試幣的應用程序。開發者可以使用這些測試幣來測試他們的應用程序，而無需使用真實的資產。
  - What is the difference between Externally-owned account (EOA) and Contract Account(CA)?
    - 外部擁有賬戶(EOA)和合約賬戶(CA)：EOA是由私鑰控制的賬戶，用於發送交易。合約賬戶是智能合約的賬戶，由合約代碼控制，並且能夠執行合約代碼定義的操作。
- Smart Contract
  - What is the difference between the private, internal, public and external functions?
    - private：只能在合約內部被調用。
    - internal：只能在合約內部或繼承的合約中被調用。
    - public：可以在任何地方被調用。
    - external：只能從合約外部被調用。
  - What is the difference between pure and view functions?
    - pure：不讀取也不修改合約狀態的函數。
    - view：只讀取但不修改合約狀態的函數。
  - Are private visibility state variables able to be fetched from the blockchain?
    - 私有狀態變量的訪問：即使是private的狀態變量，也可以通過區塊鏈上的資料直接讀取，但不可以透過合約的方法直接訪問。
  - What is the difference between call, staticcall and delegatecall?
    - call：用於發送ETH和調用合約函數。
    - staticcall：類似call，但只能調用view和pure函數。
    - delegatecall：允許一個合約在其自身的上下文中執行另一個合約的代碼。
  - What is the storage slot and its rules?
    - 存儲槽(Slot)規則：在以太坊智能合約中，狀態變量是存儲在存儲槽中。每個槽可以存儲256位的資料。狀態變量的布局是按照宣告的順序來決定的。
  - What is the difference between receive and fallback?
    - receive()：當合約接收到ETH而沒有其他數據時自動調用。

        - fallback()：當合約接收到ETH且調用的函數不存在時調用。
    - What does a modifier work? What is the execution order if there are multiple modifier?
        - 修飾符(Modifier)執行順序：當一個函數有多個修飾符時，它們會按照宣告時的順序被執行。
    - What is the difference between tx.origin and msg.sender?
        - tx.origin：交易的原始發起人。
        - msg.sender：當前調用的發起人。
    - How to send native ether? What is the difference between call, send, transfer?
        - 發送Ether：可以使用call、send、transfer方法來發送Ether，其中call是推薦的方式，因為它提供了更大的靈活性和安全性。
    - What is event, what is the purpose of emitting an event?
        - 事件(Event)和發射事件：事件是智能合約用於在區塊鏈上記錄日誌的機制。發射事件可以讓外部監聽器有效地監聽到合約的活動。
- ERC-20 / ERC-721
    - What is the difference between transfer and transferFrom in ERC20?
        - transfer函數：用於代幣持有者將自己的代幣直接轉移給另一個地址。這是一個較為簡單的操作，只需要指定接收者地址和轉移的代幣數量。調用transfer函數的是代幣的當前持有者。
        - 例如，如果Alice想要直接給Bob轉移100個代幣，Alice會在她自己的錢包中調用transfer函數，指定Bob的地址和轉移的數量100。
        - transferFrom函數：用於一個地址代表另一個地址進行代幣轉移。在調用transferFrom之前，代幣的持有者需要先通過approve函數授權一個第三方地址（例如一個智能合約）轉移代幣的權限，包括最大轉移數量。然後，被授權的第三方可以使用transferFrom來從原持有者的賬戶中將代幣轉給任何地址。
        - 例如，如果Alice想允許一個智能合約從她的賬戶中轉移最多100個代幣給任何人，Alice首先需要調用approve函數，授權該合約操作最多100個代幣。之後，該合約就可以根據需要使用transferFrom函數，從Alice的賬戶中將代幣轉給其他地址，直到達到她授權的限額。
        - 總結來說，transfer是用於代幣持有者自己將代幣轉給其他人，而transferFrom則允許一個被授權的第三方代表代幣持有者轉移代幣，這需要事先通過approve函數進行授權。
    - What is the mechanism for approve function? What does it do?
        - approve函數是ERC-20代幣標準中的一部分，允許代幣持有者授權第三方地址（例如一個智能合約或另一個用戶）從其賬戶中轉移一定數量的代幣。這樣，當需要透過智能合約執行操作，如交易所交易或參與某些DeFi應用時，就不必將代幣直接轉給合約，從而降低風險。授權後，第三方可以使用transferFrom函數進行轉賬，直到達到被授權的額度。
    - What is the difference between ERC-20 and ERC-721? Why is ERC-721 equivalent to NFT?
        - ERC-20 和 ERC-721 的區別：ERC-20代表一種同質化代幣標準，適用於代幣可以無差別替換的場景。ERC-721代表非同質化代幣(NFT)，每個代幣都是獨一無二的，適合用於證明所有權和身份的場景。
    - What is the difference between transferFrom and safeTransferFrom in ERC-721?
        - transferFrom：允許代幣的所有者或被授權者將ERC-721代幣從一個地址轉移到另一個地址。它不檢查接收者是否能夠接收代幣，可能導致代幣被鎖在無法與代幣交互的合約中。
        - safeTransferFrom：增加了一個安全檢查，以確保接收代幣的合約知道如何處理ERC-721代幣。如果目標合約沒有實現特定的接口（onERC721Received），轉移將會失敗。這可以防止代幣不慎丟失。
    - What is the difference between approve and approveForAll in ERC-721?
        - approve：允許代幣的當前所有者授權單個代幣給另一個地址（通常是智能合約），使其能夠轉移指定的代幣。
        - approveForAll：允許代幣的所有者授權另一個地址轉移其名下的所有代幣。這適用於希望一次授權多個代幣給同一地址的場景，使得管理多個代幣更加方便。

- Decentralized Finance
  - What is DEX? What is the difference between AMM and order book?
    - DEX和AMM：去中心化交易所(DEX)允許用戶在沒有中心化交易所介入的情況下交換加密資產。自動做市商(AMM)是一種用於提供流動性的算法，它允許資產在預設的規則下自動交換。
  - What is slippage in AMM? How to prevent them?
    - 滑點是指在交易前後資產價格的變化。在自動做市商（AMM）中，由於交易大小對資產價格有直接影響，大規模交易可能會導致價格變動，從而與交易發起時預期的價格不同。預防滑點的方法包括設定交易的最小接受價格，或者選擇流動性更高的交易對進行交易。
  - What is impermenant loss? How to calculate the loss?
    - 不恆定損失（Impermanent Loss）是提供流動性時可能面臨的一種風險，當提供流動性的資產價格相對於存入時發生變化時，相比直接持有這些資產，流動性提供者可能會遭受虧損。計算不恆定損失涉及比較存入流動性池的資產組合的當前價值與在沒有價格變化情況下的價值。
  - What is sandwitch attack? How can it affect your swap?
    - 三明治攻擊是指攻擊者在看到一個即將進行的交易後，迅速地在這個交易之前和之後插入自己的交易。這樣做的目的是利用原交易對資產價格的影響，從而在短時間內從交易者那裏賺取差價。預防三明治攻擊的策略之一是使用足夠的滑點保護，或者在流動性更好的池子中進行交易。
  - What is the structure of Uniswap V2 (Related to core/periphery and Router/Pair/Factory)
    - Uniswap V2採用核心/周邊架構，其中核心合約包括Factory合約、Pair合約等，負責創建代幣對和執行交易。周邊合約，如Router合約，為用戶提供更加友好的交互接口，支持多種交易路徑和複雜操作。
  - What is the formula for Uniswap V2 and how it works?
    - Uniswap V2使用x*y=k公式來確保交易後代幣池的產品保持不變。鑄造流動性時，流動性提供者需要按目前池中代幣比例存入等價值的兩種代幣，並根據提供的流動性份額獲得代表其份額的LP代幣。
  - What is the formula when minting liquidity in Uniswap V2 and how it works?
    - Uniswap V2的pairFor函數根據Factory合約地址、兩種代幣的地址（並且是按一定順序排列的），以及特定的創建代碼，透過一種稱為創建2（CREATE2）的方式來計算出代幣對合約的地址。
  - How to calculate the pair address in pairFor function?
    - Uniswap V2的pairFor函數根據Factory合約地址、兩種代幣的地址（並且是按一定順序排列的），以及特定的創建代碼，透過一種稱為創建2（CREATE2）的方式來計算出代幣對合約的地址。
  - What is arbitrage and how it works? How to calculate the reward?
    - 套利：是指利用不同市場或不同產品之間價格差異來獲利的策略。在DeFi中，套利者尋找並利用這些價差，通過快速買入低價並賣出高價來獲利。
  - What is liquidity mining?
    - 流動性挖礦：是一種獎勵機制，通過為DeFi應用提供流動性來賺取額外的代幣作為獎勵。
- Security
  - What is DoS (Denial of Service) issue? Are there any real-world examples?
    - DoS攻擊和重入攻擊：DoS攻擊通過滿足或耗盡資源來阻止系統正常運作。重入攻擊是指攻擊者重複調用合約的函數，試圖提取更多資金。
  - What is reentrancy attack and examples of such vulnerability? How to mitigate the risk of potential exploit?
    - 重入攻擊：當合約在完成一次支付後，未更新其狀態，攻擊者可以在同一個交易中多次調用該合約的函數，提取超過本應獲得的資金。防範措施包括使用重入鎖或改變函數的順序，先更新狀態再支付。
  - What is front-run attack, how can it affect your transaction?
    - 前置攻擊（Front-Running）：是指攻擊者在交易被確認前，看到了即將發生的交易，並快速提交一個具有更高礦工費的交易，以期在原交易之前被處理。這可能會對原交易的執行結果產生不利影響。防範措施包括使用隱私方案或限制交易的可預見性。