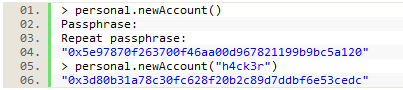
# 以太坊原理與應用開發 – 期中考

* 本期中考試採 Open book 的方式，作答者須誠實回答以下考卷，不可與同學討論或抄襲同學答案，但可上網搜尋或參考課程講義。作答時間為11/16-11/22 午夜截止，總分為 100 分。有任何問題都可以留言至 [期中考題目釋疑區](https://docs.google.com/document/d/1wuqdw8APJDHXSxm0pSNo-JX01LB2B1Rxb00yJl9SVDU/edit)，僅限詢問題目有不清楚的地方。

### (10%) 01. 在以太坊中，存在兩種類型的帳號 (account)，又稱地址 (address)，試問是哪兩種帳號？並敘述產生兩種帳號分別的演算法 (pseudo code即可)？

外部擁有帳戶（EOA）和合約帳戶（CA）。

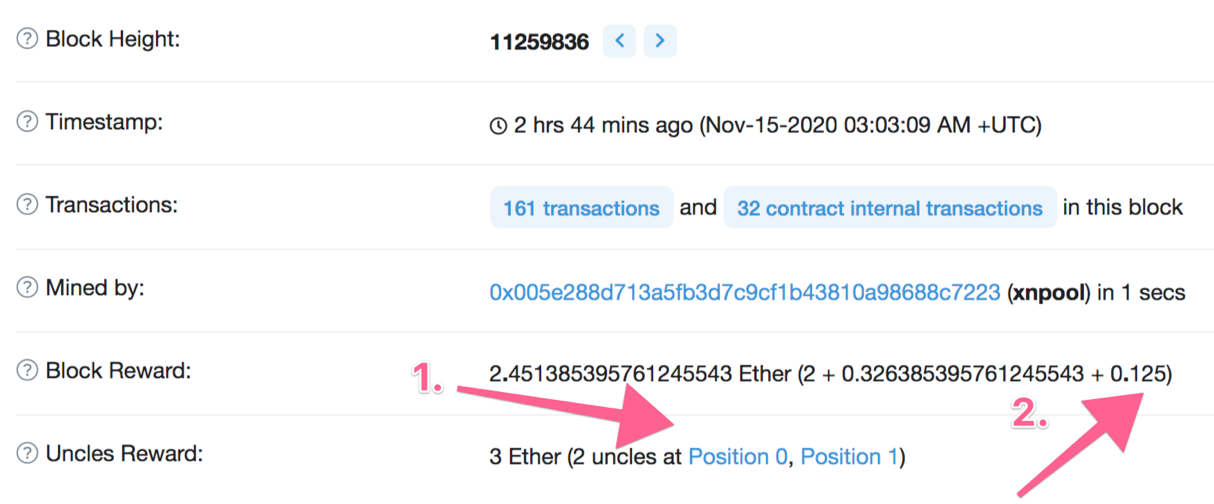
外部擁有帳戶全名 Externally owned account，具有公鑰（public key）和私鑰（private key），由以太坊以外的軟體（如錢包應用程式）控制。私鑰先使用 ECDSA 計算出公鑰，接著對公鑰作出 Keccak 雜湊，接著取其雜湊最右邊的40位元組，並以16進制字串方式表達該40位元組，然後在字串前面加上“0x”字串後，該字串即為該私鑰所對應之以太坊地址。



合約帳戶簡稱 CA，全名（Contract address），沒有私鑰，受智能合約的程式邏輯所掌控，每個智能合約在部署後，都會產一個對應的合約帳戶，用來接收使用者轉帳錢智能合約，由在以太坊虛擬機（EVM）內運行的軟體控制。CA產生來自於使用者的address跟使用者送了多少nonce。



### (10%) 02. 區塊高度 [11259836](https://etherscan.io/block/11259836) 下，點進網頁後，觀察到 Uncles Reward 有兩個，試問 Position 0 與 Position 1 分別獲得的 Uncle Reward 各是多少 (見下圖 1)？且是如何計算得知？並且下圖 2 中 0.125 是代表何意義？又如何計算得知？



1.

Position 0 :1.25, (11259833 + 8 - 11259836) \* 2 / 8 = 1.25

Position 1 :1.75, (11259835 + 8 - 11259836) \* 2 / 8 = 1.75

2.

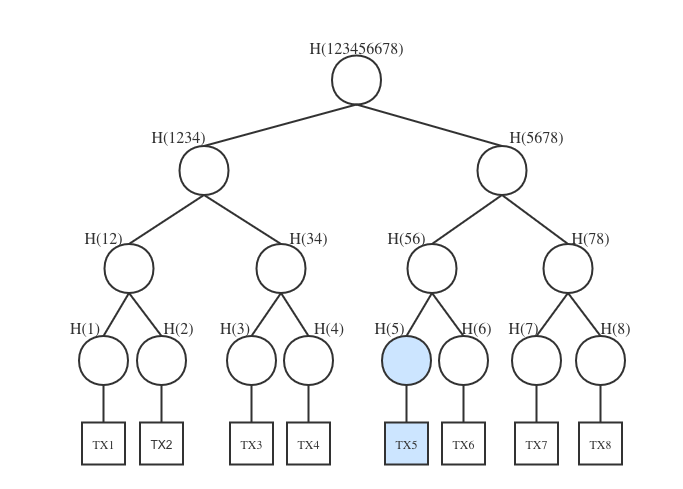
0.125: Uncle Inclusion Reward.

11259836 – 11259835 + 11259836 – 11259833 = 4 blocks

4/32 = 0.125

### (20%) 03. 在區塊鏈中，除了鏈的結構外，也常使用到 Merkle Tree 的資料結構方法。下圖中，為方便表示，H(1) 表示 H(TX1) 的結果，H(12) 表示Hash(1 || 2) 的結果，依此類推。試問：

* 1. (5%) 以 Merkle Tree 表示的資料結構有哪些優點？
  2. (5%) 何謂 Merkle root？
  3. (10%) 若要證明 TX5 存在於 Merkle Tree 之中，要如何證明？



a. 儲存任意長度的key-value鍵值對資料；提供了一種快速計算所維護資料集雜湊標識的機制；提供了快速狀態回滾的機制。

b. 雜湊樹（hash tree；Merkle tree），在密碼學及電腦科學中是一種樹形資料結構，每個葉節點均以資料塊的雜湊作為標籤，而除了葉節點以外的節點則以其子節點標籤的加密雜湊作為標籤 。雜湊樹能夠高效、安全地驗證大型資料結構的內容。

c. 計算Tx5的Hash(5)，計算Hash(6)與Hash(5)的Hash(56)，計算Hash(78)與Hash(56)的Hash(5678)，最後確認計算出來的Hash(5678)跟區塊裡的Merkle Root Hash(5678)有沒有一致，一致則該筆交易存在這個區塊，不一致則該筆交易不存在於這個區塊。

### (10%) 04. 在以太坊中，手續費的計費方式為按計算的工作量而定，試問：

* 1. (2%) 何謂 gas？
  2. (2%) 為何設計 gasLimit？
  3. (2%) txhash 為[0xdf4735e94328a6945cbd9299617448d6f6963d940dbb0e35bac57029b73684ef](https://etherscan.io/tx/0xdf4735e94328a6945cbd9299617448d6f6963d940dbb0e35bac57029b73684ef) 的交易，**Transaction Fee: 0.00031128 Ether** 是如何計算得出的？
  4. (4%) 若是 gasPrice 給過低，造成交易無法被打包，該如何處理？

a. Gas 是指測量在以太坊網路上執行特定操作所需的計算單位。

b. 不同的操作會產生不同的 Gas 成本。Gas 用完時，礦工將停止執行。如果有剩餘 Gas，將立即退還給發起交易的人員或智能合約創建者。但是，如果Gas Limit太低，交易被認為是無效的，並且會因為“Gas不足”錯誤而被取消，並且其中用於計算的 Gas 不會退回。所以無論交易是否通過，發送者總需要向礦工支付計算費用。

c. Transaction Fee = Gas Price \* Gas Used by Transaction: 0.000000006 Ether (6 Gwei) \* 51,880 = 0.00031128 Ether

d. 你可以設一個更高的 Gas Price，這樣你就跳到了別人的前面，就會被優先確認交易， 或是提高原手續費10%。

### (20%) 05. ERC20 問題

* 1. (5%) 何謂 EIP？EIP-155 的作用是什麼？
  2. (5%) 何謂 ERC20 Token？設計的優點在哪？
  3. (10%) ERC20 Token 的介面定義了，6 個 function，2 個event
     1. (2%) 如果要從 EOA 轉移代幣，要呼叫哪個函數？
     2. (8%) 如果要從有代幣的合約，轉移代幣到其他地址，執行的步驟為何？

a. Ethereum Improvement Proposals， EIP是一個為Ethereum社群提供資訊的設計文件，或是用來為Ethereum描述一些新的功能或環境；EIP-15: 交易不是在特定一條鏈上，如果你在一個私人的以太坊網路，其他人可以在這個網路攔截你的交易，並將其散播到公共網路上令交易生效。因此，如果你在不同網路使用相同的位址，可能會導致交易意外地發送，所以就衍伸出了EIP-155，作用為防止Replay Attack。

b. 一種基於ERC20 Token Standard所創立的代幣；為了要讓代幣能擁有合理的貨幣機制。若一個 Token 符合 ERC20，即代表他是一種具有完整貨幣交易功能的代幣。

c. use eth.sendTransaction；先在ERC20的標準創立一個自己的token，再加入至account，之後就可以使用transfer函數進行轉移代幣。

### (20%) 06. 2020/11/04，Eth2 deposit contract 正式上線，象徵 Ethereum 2.0的第 0 階段正在準備啟動， 以下有幾個關於 Eth2 相關的問題。

* 1. (2%) 請問 Eth2 deposit contract 的合約 ENS 地址為何？何謂 ENS 域名？
  2. (2%) 需要達到多少驗證者 (Validator) 數量的門檻，Phase 0 才算正式啟動呢？
  3. (4%) 如果要參與 Phase 0 的 staking，可透過哪些方法來參與？參考[文章](https://blog.ethereum.org/2020/11/04/eth2-quick-update-no-19/)，至少有 2 種方法，擇一敘述即可
  4. (2%) 請舉出以太坊 2.0 其中一項主要的技術突破？
  5. (10%) 以太坊 2.0 預計有 Phase 0, Phase 1, Phase 1.5, Phase 2 等四個主要階段，請分別敘述不同階段的目標與工作？

a. **0x00000000219ab540356cbb839cbe05303d7705fa；**ENS是一個使人們可以方便得記憶/訪問以太坊區塊鏈地址的服務。

**b. 16384**

c. 送32-eth至Eth2 deposit contract 的合約裡面。

d. 2.0 之後則會採用 PoS，是 PoW 的升級版本。

e. Phase 0: 此階段會推出 Eth2 全新共識機制的核心—信標鏈（Beacon Chain）。信標鏈是所有系統層活動發生的場所，也是系統內協作溝通的地方。Phase 0 的開發目標是讓分佈在全世界、圍繞著數千個節點、數以十萬計的共識單元（驗證者）能同時參與。

Phase 1: 提倡分片鏈的概念，來自信標鏈的驗證者會被隨機分配短期的任務，內容為到某一分片鏈上構建及驗證區塊。為該分片鏈的狀態、可用性以及有效性提供密碼經濟學承諾、最終發回到核心系統（分片鏈）。

Phase 1.5: 把以太坊主網作為一個分片整合進 Eth2 的共識機制（作為 Phase 1 階段創造的許多分片之一，繼續存在）。

Phase 2: 為初始以太坊分片以外的其它分片添加狀態和執行機制。

### (10%) 07. 既然合約程式碼是開源的，意味著任何人都可以部署相同的合約，因此惡意的攻擊者可部署一份相同的 [USDT](https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7) 合約。

試問：

1. (4%) 在以下的情境中，如果你的錢包收到一筆 USDT $1000 的金額，你該如何分辨這筆入金是真或是假？
2. (6%) 什麼是 ERC20 代幣的假充值攻擊？查詢關鍵字：「ERC20, 代幣, 假充值攻擊」或參考[文章](https://mp.weixin.qq.com/s/3cMbE6p_4qCdVLa4FNA5-A)

1. 假幣攻擊的判斷方式為觀察智能合約地址，每個代幣項目都有一個獨有的智能合約地址，這是不能重複與偽造的。

2. 當使用者調用代幣合約的 transfer 函數進行轉帳時，如果 transfer 函數正常運行未拋出異常，該交易的 status 即是 true。但某些代幣合約的 transfer 函數對轉帳發起人 (msg.sender) 的餘額檢查用的是 if 判斷，當發起人餘額比轉帳的數目低時，將會return false，但執行不會異常。僅使用 if/else 這種溫和的判斷方式在 transfer 這類敏感函數中是不嚴謹的。如果交易所僅判斷如 TxReceipt Status 是 success（即上文提的 status 為 true 的情況）就以為充值成功，就可能存在假充值的風險。