資工碩一 113598043 張育丞 Quiz 1

1. Node

節點是區塊鏈構成的主要成分，並且可分為三種：

a. Blue Node：採Peer-to-Peer方式連結，名為積極型節點。

b. Red Node：泛指user，在整個節點網路中，只會提出請求，但不會貢獻。

c. Grey Node：又稱死節點(dead)，在整體區塊鏈中，無請求，無貢獻。

2. Reward (Award)

區塊鏈挖礦如同解一個難題，對於每一回合最先出塊(解完難題者)有對應的獎勵機制，並獲得獎勵，僅有一位贏家，贏家獎勵全拿。

3. Puzzle

在區塊鏈中的密碼學難題，難度介在P~NP之間，每一回合依參與者狀況改變難度，屆時來決定最後的贏家，獲得獎勵。

4. Transactions

如同一個記帳系統，記錄交易過程，在交易的細節也包含在內。

5. Structure (format) of a block

a. Block Header: Pre Hash, Datetime, Difficuly value, Nonce

b. Block Body: Transaction Data

c. Merkle Root: Every transaction encryption abstract.

6. Hash Function

Give H, it's hard to find $H(x) = H(x')$, where $x \neq x'$

Give $H(x)$, it's hard to find x, Hash function is a "compression" function.

在區塊鏈中，不論輸入的字串多長，最終所得到輸出長度皆是相同的，結果不可逆。

7. Merkle Tree

在區塊鏈中做為資料壓縮角色，能有效且安全地存放交易資料。

(背面尚有內容)

資工碩一 113598043 張育丞 Quiz 1

8. Digital Signature

名為「數位簽章」，具有 1. Authentication ; 2. Integrity ; 3. Non-repudiation，確認區塊鏈的合法性，以及驗證交易資料。

9. Proof of work / Proof of stake

• Proof of work :

名為「工作量證明」，具有「高算力需求」、「耗電」、「耗時」三大特點，透過挖礦(解難題)來獲取下一區塊記帳權，進而確保區塊更新，既真實又唯一，進而達防篡改。

PoW : H(pre_hash , tx's root , nonce) < t

• Poof of stake :

名為「權益證明」，透過質押的數量和時間，增加獲得出塊權利，當第一位未成功出塊，接著會在選第二人，以此類推，由於每次僅有一位在嘗試出塊，因未出現多人相爭，以此來省電。

10. Smart Contract

「智能合約」在區塊鏈的交易系統中使「程式碼」，藉此實現「自動化交易」，然而在執行後，仍不具修改，一切公開在網路上，可供驗證。

11. ERC20 (token)

以太坊 造幣標準，確立了每種代幣等值，代幣亦可交換。

12. ERC721 (NFT , Non-Fungible Token)

非同質化貨幣，可能是音樂 or 畫作，任何數收藏皆具獨立且唯一性，不可交換，有版稅(交易分潤)和永久性交易，兩種方式。