數字金融犯罪偵查 --- 搜查區塊鏈上可疑交易模式

題目內容：

由於匿名性，加密貨幣被廣泛運用於洗錢和違禁物品交易，不過加密貨幣上的匿名其實只是“偽匿名” (pseudoanonymous)，加密貨幣的交易仍可以追本溯源到交易者本身。

因為每一筆加密貨幣的交易歷史，都儲存在一個叫做“區塊鏈”(blockchain) 的公共記 錄中，包括關聯賬戶的信息以及交易的數量。不過目前對於監管機構來說，加密貨幣的交易還不像信用卡交易那麼透明。

德國和瑞士學者的一項研究顯示，約 40% 加密貨幣用戶的真實身份可被發現。日後，通過大宗交易追蹤到交易者的真實身份將變得容易，這最終可能會使得如今被大量用於洗錢等非法活動的加密貨幣不再受寵。

常見的可疑交易模式包括：

- Looping: 交易形成迴圈，在經過數筆交易之後，金流再度回到同一人帳戶。
- Unusual activity: 該地址在短時間內出現高頻交易活動
- Instant high volume: 該地址出現單筆大額交易活動

本題將給定時間區間，並提供區塊鏈上的真實交易資料，由參賽者扮演數字金融犯罪偵查官的角色，在時間內試圖辨識所有可疑交易活動。

提示：

- 部分非用於一般交易的交易紀錄 (例如 coinbase transaction)，可能會出現輸入端或輸出端不包含地址的情況，此類交易紀錄不影響金流。
- 區塊鏈上的時間區間是以 block index (or block height) 做表示，意即參賽者僅需要搜查給定的 block indices 區間是否存在可疑交易。請不要嘗試下載整個區塊鏈，僅需要透過 API 下載給定 block indices 區間的資料即可
- 可以併發呼叫 API，以增進吞吐量

評分說明：

- 由參賽團隊提交可疑的交易活動，列出相關交易，並且提出其所列可疑交易的判斷思路
- 評分依據包含量性與質性標準
    - 系統可辨識之可疑交易數量
    - 系統設計之判斷標準合理性

Financial investigation in the blockchain world --- Searching for suspicious trading activities

Question:

Due to anonymity, cryptocurrency could be involved in money laundering and illegal trading, but the virtual currency based on the blockchain is only "pseudo-anonymous", meaning that the investigator can still trace the transactions to their origins.

Because the transaction history of the cryptocurrency are stored in a distributed ledger called "blockchain", including information of the addresses (the identity in the blockchain network) involved in the transactions. Currently, inspecting these transaction details is a technical issue for the regulators, for information on the blockchain cannot be easily interpreted as it is for normal transaction records.

A study conducted by German and Swiss researchers showed that about 40% of the user's true identity on the blockchain can be found. In the future, tracking the true identity of the traders on the blockchain will become easier, which may eventually make illegal tradings via cryptocurrency no longer favored.

Common patterns of suspicious activities including:

- Looping: Transactions involving several addresses and forming a cycle.
- Unusual activity: Transient high frequency trading activities
- Instant high volume: Large trading volume involving a few addresses

In this question, transaction data on the blockchain are provided. A specific time interval is given. Participant will try to list all suspicious trading activities and provide the transaction hashes.

Hints:

- Some transactions (e.g. coinbase transactions) have no address in input or output, and can be neglected during the investigation of suspicious activities.
- Time interval on a blockchain is provided as the block index (or block height), the number of blocks preceding a particular block on the blockchain. For example, the genesis block has a height of zero because zero block preceded it. It is NOT recommended that participants download the whole blockchain data. Instead, please use the API(s) to access the blockchain data between the block indices interval that is specified.
- Invoking API calls parallely is recommended to increase the throughput.

Rating:

- Participant will submit a list of suspicious activities, and list all transaction hashes for each case of suspicious activity.
- Participant will demo to reproduce their result, and illustrate the thinking process.
- Quantitative and qualitative criteria:
    - Numbers of suspicious transactions identified.
    - Reasons for identifying suspicious transactions.