VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY

UNIVERSITY OF SCIENCE

VNUHCM-HCMUS

LAB 2

NHÓM 6

MÔN HỌC: BLOCKCHAIN VÀ ỨNG DỤNG

Sinh viên thực hiện:		**Giảng viên:**
Nguyễn Thị Cẩm Nhung	**21127386**	**Nguyễn Đình Thúc**
Bành Minh Phương	**21127398**	**Ngô Đình Hy**
Lương Minh Hiển	**21127273**	
Cao Nguyễn Khánh	**21127627**	
Võ Quang Vinh	**21127732**	

Mục lục

I. Cấu trúc của Đồ án:

```
Code/
├── Task1 # Folder của task 1 (P2PKH-Script)
        ├── bitcoinscript.ipynb  # Source code
        ├── bitcoin_keys.txt # File lưu trữ thông tin ví, khóa của người gửi
        ├── bitcoin_keys2.txt # File lưu trữ thông tin ví, khóa của người nhận
├── Task2 # Folder của task 2 (Multisig-Script)
        ├── bitcoinscript.ipynb  # Source code
        ├── multisig_wallets_info.txt # File lưu trữ thông tin ví, khóa
```

II. Basic Script Execution:

- Cách hoạt động của code P2PKH:
  - Tạo P2PKH Script (chỉ chạy 1 lần):
    - Để thực hiện được P2PKH thông qua code python, đầu tiên sẽ tạo ra các thành phần cần thiết như **ví, khóa bí mật, khóa công khai, địa chỉ**.
    - Sử dụng class **Key** của thư viện **bitcoinlib, khóa bí mật** sẽ được tạo ra dưới dạng chuỗi hexadecimal. Ngoài ra loại network sử dụng cho đồ án này là **testnet**, chỉ có tác dụng thử nghiệm mạng Bitcoin thay vì mạng chính thức (**mainet**)
    - Đặt tên cho ví là **'wallet_1_test'** để có thể phân biệt giữa các ví với nhau
    - Gọi hàm của thư viện **bitcoinlib.wallet** để tạo ví, lưu vào object là wallet
    - Từ chính đối tượng **wallet** đó, tạo ra được **khóa công khai** và **địa chỉ Bitcoin**
    - Chi tiết cách tạo ra **khóa công khai**: Sử dụng Elliptic Curve Cryptography (ECC), cụ thể là đường cong elliptic secp256k1 mà Bitcoin sử dụng. Cuối cùng được xuất ra ở dạng wif (**Wallet Import Format**)
    - Chi tiết cách tạo ra **địa chỉ Bitcoin**: Sử dụng **SHA-256** để băm **khóa công khai** và tạo chuỗi băm 256-bit. Sau đó dùng RIPEMD-160 băm kết quả của SHA-256 để tạo chuỗi băm 160-bit, gọi là PubKeyHash.
    - **Tên wallet, khóa bí mật, khóa công khai, địa chỉ Bitcoin** sẽ được lưu vào file bitcoin_keys.txt để tiện truy xuất thông tin
  - Lock fund:
    - Quá trình Lock fund P2PKH mà ta có thể thực hiện thông qua các website **Bitcoin Testnet Explorer** và **Bitcoin Testnet Faucet**.
    - Đầu tiên nhập **địa chỉ Bitcoin** vào website **Bitcoin Testnet Explorer**, nó dẫn ta đến một API (ví dụ blockstream.info/testnet/address/<BitcoinAddress>).
    - Blockchain lưu tất cả các giao dịch Bitcoin. API sẽ tìm kiếm tất cả các giao dịch liên quan đến địa chỉ đã được cung cấp.
    - API trả về dữ liệu số dư (tính bằng satoshis) và thông tin UTXOs. Website xử lý dữ liệu, chuyển đổi số dư sang tBTC, và hiển thị trên màn hình.

        - Sau đó ta vào **Bitcoin Testnet Faucet,** nhập **địa chỉ Bitcoin** vào để yêu cầu gửi bitcoin vào địa chỉ đó.
        - Các website này thường giới hạn số lượng bitcoin và tần suất nhận để chống các người dùng lạm dụng. Thường ta sẽ phải thực hiện capcha để việc nhận bitcoin hoàn tất
        - Cuối cùng ta chạy hàm **print_info_wallet** để xem số dư hiện có trong địa chỉ Bitcoin đó
    - Spend fund:
        - Ta thực hiện lại quá trình tạo 1 P2PKH script với 1 ví khác tên là **'wallet_1_receive'** để tiện giao dịch. Sau đó lưu các thông tin của chúng vào file bitcoin_keys2.txt
        - Ta truy xuất **địa chỉ Bitcoin** của **wallet_1_receive** để xác nhận địa chỉ sẽ nhận bitcoin trong giao dịch này
        - Ta truy xuất **khóa bí mật** của **wallet_1_test** để có được chữ ký, đảm bảo giao dịch này là hợp lệ
        - Chọn số bitcoin cần gửi, tính theo tBTC.
        - Chi tiết quá trình Spend fund:
            - Cập nhật danh sách UTXOs của ví người gửi. Trong đó UTXOs là các đầu ra từ giao dịch trước đó chưa được chi tiêu, đại diện cho số dư khả dụng của ví.
            - Sử dụng hàm send_to của thư viện để gửi bitcoin từ **wallet_1_test** đến **wallet_1_receive**.
            - Khi đó hàm send_to sẽ khởi tạo giao dịch, thực hiện ký khóa bí mật, tính toán phí giao dịch…
            - Cuối cùng hàm sẽ Broadcast giao dịch này và trả về i thông tin chi tiết: số lượng đầu vào và đầu ra, trạng thái giao dịch (mới, đang chờ, hoặc đã được xác nhận), thông tin mạng.
        - Cập nhật danh sách UTXOs thêm 1 lần nữa. Người dùng có thể tự Lock fund lên wallet_1_receive để kiểm tra số dư

III. Multisignature Transactions:

- Multisig Wallet (ví đa chữ ký) là ví yêu cầu nhiều hơn một Private Key để thực hiện giao dịch
- Triển khai Multisignature transaction:
    - Tạo Multisignature Script (chỉ chạy 1 lần):
        - Để thực hiện được Multisig Script thông qua code python, đầu tiên sẽ tạo ra các thành phần cần thiết như **ví, khóa bí mật, khóa công khai, địa chỉ**.
        - Sử dụng class **HDKey** của thư viện **bitcoinlib, khóa bí mật** sẽ được tạo ra dưới dạng chuỗi hexadecimal. Ngoài ra loại network sử dụng cho đồ án này là **testnet**, chỉ có tác dụng thử nghiệm mạng Bitcoin thay vì mạng chính thức (**mainet**), tạo 2 khóa bảo mật cho cơ chế multisig (đa khóa).

        - Tạo Ví Multisig: Hai ví multisig 2-trong-2 được tạo trên Bitcoin Testnet:

            wallet1: Yêu cầu chữ kí từ private_key1 và pubkey2

            wallet2: Yêu cầu chữ kí từ pubkey1 và private_key2

        - **Tên wallet, khóa bí mật, khóa công khai, địa chỉ Bitcoin** sẽ được lưu vào file multisig_wallets_info.txt để tiện truy xuất thông tin
    - Lock fund:
        - Quá trình Lock fund Multisig Wallet cũng tương tự như ở task 1, có thể thực hiện thông qua các website **Bitcoin Testnet Explorer** và **Bitcoin Testnet Faucet**.
        - Đầu tiên nhập **địa chỉ Bitcoin** vào website **Bitcoin Testnet Explorer**, nó dẫn ta đến một API (ví dụ blockstream.info/testnet/address/<BitcoinAddress>).
        - Blockchain lưu tất cả các giao dịch Bitcoin. API sẽ tìm kiếm tất cả các giao dịch liên quan đến địa chỉ đã được cung cấp.
        - API trả về dữ liệu số dư (tính bằng satoshis) và thông tin UTXOs. Website xử lý dữ liệu, chuyển đổi số dư sang tBTC, và hiển thị trên màn hình.
        - Sau đó ta vào **Bitcoin Testnet Faucet,** nhập **địa chỉ Bitcoin** vào để yêu cầu gửi bitcoin vào địa chỉ đó.
        - Các website này thường giới hạn số lượng bitcoin và tần suất nhận để chống các người dùng lạm dụng. Thường ta sẽ phải thực hiện capcha để việc nhận bitcoin hoàn tất
    - Spend fund:
        - Tạo 1 ví mới để nhận tBTC từ Multisig Wallet
        - Ta truy xuất **địa chỉ Bitcoin** của **receiver_wallet** để xác nhận địa chỉ sẽ nhận bitcoin trong giao dịch này
        - Khác với task 1, ở task 2 **multisig wallet** sẽ yêu cầu chữ ký **ở cả 2 ví** để có thể giao dịch chuyển coin
        - Chọn số bitcoin cần gửi, tính theo tBTC.
        - Chi tiết quá trình Spend fund:
            - Cập nhật danh sách UTXOs của ví người gửi. Trong đó UTXOs là các đầu ra từ giao dịch trước đó chưa được chi tiêu, đại diện cho số dư khả dụng của ví.
            - Tạo một **transaction (t)** yêu cầu chữ kí từ wallet2 bằng hàm **transaction_create**
            - Với **multisig wallet**, một **spend locked funds** chỉ được thực thi và xác nhận khi **có đủ chữ kí của 2 wallet**, tiếp tục sử dụng hàm **transaction_import,** yêu cầu chữ kí từ **wallet1 và thêm vào transaction t2** (thêm chữ kí từ transaction t phía trên)
            - Sau đó tiến hành **broadcast transaction t2** khi đã kí đủ 2 chữ kí

- Cuối cùng, trả về thông tin của transaction t2:số lượng đầu vào và đầu ra, trạng thái giao dịch (mới, đang chờ, hoặc đã được xác nhận), thông tin mạng.

■ Cập nhật danh sách UTXOs thêm 1 lần nữa

IV. Analysis and Reflection:

1. So sánh ví đơn chữ kí và ví đa chữ kí:

Tính năng	**Ví thông thường (đơn chữ ký)**	**Ví Multisig (đa chữ ký)**
Số lượng khóa	1	Nhiều (ví dụ: 2/3, 3/5)
Bảo mật	Thấp	Cao hơn
Độ phức tạp	Đơn giản	Phức tạp hơn
Khả năng quản lý tài sản chung	Khó khăn	Hiệu quả
Khả năng chống mất cắp	Thấp	Cao hơn
Tính minh bạch	Thấp	Cao hơn
Tính linh hoạt	Hạn chế	Linh hoạt hơn
Khả năng phục hồi khi mất khóa	Rất khó, gần như không thể	Vẫn có khả năng nếu đủ số khóa còn lại

2. Ưu và nhược điểm của Bitcoin Script:
    - Ưu điểm:

- **Tính bảo mật cao**: Công nghệ blockchain, nền tảng của tiền điện tử, đảm bảo an ninh cho các giao dịch, ngăn chặn truy cập trái phép và tăng cường bảo mật tổng thể của các giao dịch Bitcoin.
- **Tính minh bạch:** Bitcoin loại bỏ các trung gian tài chính, giúp các giao dịch trở nên rõ ràng và minh bạch hơn.
- **Tốc độ giao dịch nhanh chóng**
- **Tính linh hoạt:** Dữ liệu được chia sẻ và có thể truy cập bởi tất cả các người dùng của hệ thống, người dùng có thể giao dịch trực tiếp với nhau mà không cần dựa vào một trung gian.
    - Nhược điểm:

- **Tính biến động:** Tính biến động của tiền điện tử phụ thuộc vào các yếu tố như nguồn cung giới hạn, nhu cầu thị trường ngày càng tăng,... Nguồn cung hạn chế và nhu cầu tăng khiến giá trị của nó rất dễ biến động. Sự không chắc chắn và các nguy cơ vi phạm bảo mật có thể khiến đầu tư Bitcoin trở thành một lựa chọn rủi ro.
- **Không thể đảo ngược giao dịch và khả năng sử dụng hạn chế:** Tính không thể đảo ngược của Bitcoin góp phần làm tăng tính ẩn danh và không được kiểm soát của nó. Bất kỳ khoản thanh toán nhầm lẫn nào đều không thể truy vết và do đó rất rủi ro. Trong khi các nhà đầu tư thường lưu trữ tiền điện tử trong ví kỹ thuật số, mất quyền truy cập vào những ví này có thể dẫn đến những tổn thất nghiêm trọng. Vì vậy, Bitcoin không được sử dụng phổ biến trong các mạng lưới an toàn như một phương tiện giao dịch. Thanh toán bằng Bitcoin yêu cầu bên thứ ba, không giống như tiền mặt, thẻ ghi nợ hoặc thẻ tín dụng.
- **Lỗi kỹ thuật và hiệu ứng giảm phát:** Vì Bitcoin là một khái niệm tương đối mới, mạng blockchain vẫn còn nhiều lỗi và lỗ hổng. Điều này giải thích tại sao Bitcoin chưa được chấp nhận rộng rãi trong các giao dịch thông thường. Giới hạn trong tổng số Bitcoin sẵn có gây áp lực lên số Bitcoin hiện có và làm tăng giá trị của chúng. Một sự gia tăng chi tiêu Bitcoin trong tương lai có thể xảy ra, tiềm ẩn nguy cơ làm bất ổn nền kinh tế.

V. Kinh nghiệm thực tiễn sau đồ án:

- Khi thực hiện nhận tBTC từ Bitcoin testnet faucet cần chú ý về tần suất sử dụng để tránh gặp rủi ro khi test chuyển/nhận coin giữa các ví.
- Có thêm kiến thức về các thư viện bitcoin, tránh thư viện lỗi.
- Phân biệt được sự khác nhau giữa ví đơn chữ kí và ví đa chữ kí, cách hoạt động, bảo mật, tạo transaction,...

VI. Tham khảo:

1. Bitcoinlib documentation: https://bitcoinlib.readthedocs.io/en/latest/

2. Ưu nhược điểm của bitcoin: https://cleartax.in/s/advantages-and-disadvantages-of-bitcoin

3. Advantages of Bitcoin's Scripting Language: https://www.nadcab.com/blog/bitcoin-scripting-language#:~:text=Bitcoin's%20scripting%20language%20enhances%20the,environment%20for%20defining%20transaction%20conditions.