TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

LAB02:

Understanding Bitcoin’s Scripting Language

GV hướng dẫn:

Nguyễn Đình Thúc

Ngô Đình Hy

Nhóm sinh viên thực hiện: 07

20127066 - Nguyễn Nhật Quân

20127192 - Trần Anh Huy

20127299 – Trần Hoàng Minh Quang

20127338 – Trương Gia Thịnh

Thành phố Hồ Chí Minh, ngày 18 tháng 12 năm 2023

MỤC LỤC

1. TỔNG QUAN

1.1. THÔNG TIN NHÓM

MSSV	Họ tên	Email	Vai trò
20127066	Nguyễn Nhật Quân	20127066@student.hcmus.edu.vn	Thành viên
20127192	Trần Anh Huy	20127192@student.hcmus.edu.vn	Nhóm trưởng
20127299	Trần Hoàng Minh Quang	20127299@student.hcmus.edu.vn	Thành viên
20127338	Trương Gia Thịnh	20127338@student.hcmus.edu.vn	Thành viên

1.2. THÔNG TIN BÀI TẬP NHÓM

Tên bài tập	Lab 1: Simplified Blockchain Implementation and Verification
Công cụ	GitHub, Google Meet, Google Doc, Visual Code
Ngôn ngữ lập trình	Go lang
Product Owner	Nguyễn Đình Thúc, Ngô Đình Hy

2 BẢNG ĐÁNH GIÁ VÀ PHÂN CÔNG

2.1. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH: 99%

Đồ án hoàn thành đủ các yêu cầu đề bài.

Phần	Các công việc đã hoàn thành
1	Task 1: Basic Script Execution
2	Task 2: Multisignature Transactions
3	Task 3: Analysis and Reflection
4	Report

2.2. BẢNG % ĐÓNG GÓP

Các thành viên đều tham dự các buổi họp trực tuyến, có tinh thần tích cực và đóng góp ý kiến cho đồ án.

MSSV	Tên	% đóng góp
20127066	Nguyễn Nhật Quân	100%
20127192	Trần Anh Huy	100%
20127299	Trần Hoàng Minh Quang	100%
20127338	Trương Gia Thịnh	100%

3. TASK 1: BASIC SCRIPT EXECUTION

3.1. TỔNG QUAN

Task	Basic Script Execution
Thư viện hỗ trợ	bitcoin và bit
Môi Trường	Vmware, Kali Linux
Ngôn ngữ	Python version 3.11

3.2. NỘI DUNG

3.2.1. Mức độ bảo mật

Tạo khóa: Sử dụng thư viện bitcoin và bit để tạo một khóa riêng tư (private key) ngẫu nhiên với độ dài 32 byte và đảm bảo thuộc một khoảng giá trị cụ thể để nằm trong phạm vi chấp nhận của Bitcoin.

Thử nghiệm trên Bitcoin Testnet: **P2PKH** đáp ứng một cách an toàn trong việc công khai public key mà không làm lộ private key. Người gửi chỉ cần biết địa chỉ P2PKH của người nhận để gửi tiền. Sử dụng P2PKH address để tạo một giao dịch Bitcoin Testnet. Chọn một giao dịch đầu vào (UTXO) từ một txid và output index cụ thể. Tạo một giao dịch đầu ra (output) với một địa chỉ Bitcoin Testnet và số lượng BTC cần chuyển đi. Ký giao dịch bằng private key.

3.2.2. Ứng dụng

Sàn giao dịch và ví Bitcoin: Các ví Bitcoin thường hỗ trợ địa chỉ P2PKH, làm cho nó trở thành một lựa chọn phổ biến cho người dùng để nhận và gửi Bitcoin thông qua địa chỉ P2PKH.
Thanh Toán Thương Mại Điện Tử: Địa chỉ P2PKH có thể được sử dụng trong các thanh toán trực tuyến, đặc biệt là khi cần tích hợp với các hệ thống thanh toán hiện có.
Trả phí đào: Khi người đào Bitcoin tạo một khối mới, phần phí đào thường được chuyển đến địa chỉ P2PKH của họ.
Nạp-rút tiền từ Máy ATM Bitcoin: Khi người dùng rút tiền từ máy ATM Bitcoin, địa chỉ P2PKH thường được sử dụng để nhận số tiền rút.
Phát Hành Token: Trong một số dự án phát hành token trên blockchain Bitcoin, địa chỉ P2PKH có thể được sử dụng để lưu trữ và quản lý token.
Giao Dịch Peer-to-Peer: Các giao dịch trực tiếp giữa các cá nhân cũng có thể sử dụng địa chỉ P2PKH cho tính tiện lợi và đơn giản.

3.2.3. Đánh giá và bàn luận

P2PKH	
Ưu điểm	Nhược điểm
Bảo Mật: P2PKH cung cấp một mức độ bảo mật cao với việc giữ private key ẩn, chỉ công bố mã hash công khai.	Kích Thước Giao Dịch Lớn: Giao dịch chi tiêu từ một địa chỉ P2PKH có thể lớn hơn so với một số loại địa chỉ khác, do có nhiều thông tin phải đi kèm.
Quyết định Về Quyền Riêng Tư: Người nhận có quyền quyết định xem họ có muốn công bố public key	Chi Phí Giao Dịch Cao Hơn: Do kích thước giao dịch lớn, việc chi trả phí giao dịch có thể cao hơn so với một số phương thức khác.

của mình hay không, giúp bảo vệ quyền riêng tư.	
Sử Dụng Rộng Rãi: P2PKH là một loại địa chỉ phổ biến và được nhiều ứng dụng và ví Bitcoin hỗ trợ.	Khả Năng Mở Rộng Hạn Chế: Với sự phổ biến của các loại địa chỉ khác như Segregated Witness (SegWit) và P2SH (Pay-to-Script-Hash), P2PKH có thể trở nên hạn chế về mặt khả năng mở rộng trong tương lai.
Kiểm Soát Người Nhận: Người nhận có toàn quyền kiểm soát khi và cách họ công bố public key, điều này có thể làm tăng tính linh hoạt.	Không Hỗ Trợ Đầy Đủ Chức Năng Smart Contract: P2PKH không thể triển khai đầy đủ chức năng của các hợp đồng thông minh so với một số loại địa chỉ khác trong blockchain.
Tiện Lợi Cho Người Gửi: Đối với người gửi, việc gửi tiền đến một địa chỉ P2PKH là đơn giản và dễ dàng hiểu.	Bảo Mật Dựa Trên ECDSA: Hệ thống bảo mật của P2PKH dựa trên thuật toán chữ ký số ECDSA (Elliptic Curve Digital Signature Algorithm), mà một số nghiên cứu chỉ ra rằng có thể bị đánh đồng, có thể dẫn đến vấn đề bảo mật nếu người tấn công có thể tạo ra chữ ký giả mạo.

3.2.4. Bài học và kinh nghiệm rút ra sau khi thực hiện Task 1

Bảo mật của Private Key bằng việc sử dụng os.urandom(32) để tạo private key ngẫu nhiên.
Kiểm Tra Chiều Dài Khóa private key để đảm bảo nó không quá lớn.
Phát Triển Địa Chỉ Bitcoin bằng cách sử dụng thư viện bitcoin.wallet để tạo địa chỉ Bitcoin từ public key. Điều này làm cho mã trở nên dễ đọc và dễ sử dụng hơn so với việc tự viết mã xử lý từng bước.
Gửi Giao Dịch và Ký Giao Dịch thông qua thư viện bit để tạo và ký giao dịch giúp đơn giản hóa quá trình và giảm thiểu lỗi.
Quản Lý Key và Giao Dịch: Bạn đã thực hiện việc tạo khóa riêng tư, tạo địa chỉ Bitcoin và thực hiện giao dịch một cách đầy đủ. Việc này có thể được áp dụng trong các ứng dụng thực tế khi cần tạo và quản lý khóa, địa chỉ và giao dịch Bitcoin.

3.2.5. Chương trình:

Mục tiêu:
Tạo một Bitcoin script đơn giản để locks funds vào một địa chỉ cụ thể bằng cách sử dụng
P2PKH) với một địa chỉ testnet.
Chạy chương trình:
Dùng lệnh python3 testnet.py để chạy chương trình trong môi trường kali linux.

Sau khi có được: Private key, Public key và Bitcoin address. Ta mở website https://coinfaucet.eu/en/btc-testnet/ , và nhập Bitcoin address để tiến hành gửi BTC. Trong source code, ta sẽ điền mã giao dịch vào txid và private_key_hex là Private key ứng với Bitcoin address sử dụng trong Testnet Faucet. Ta cũng có thể theo dõi kết quả chuyển thông qua https://blockstream.info/testnet/ .

4. TASK 2: MULTISIGNATURE TRANSACTIONS

4.1. TỔNG QUAN

Task	Basic Script Execution
Thư viện hỗ trợ	os, struct, ecdsa, hashlib, base58, string, bitcoin.core ,bitcoin.wallet, bitcoin.core.script, bitcoin.core.scripteval
Môi Trường	Vmware, Kali Linux
Ngôn ngữ	Python version 3.11

4.2. NỘI DUNG

4.2.1. Mức độ bảo mật

Mức độ bảo mật của P2SH (Pay to Script Hash) trong mạng lưới Bitcoin được coi là khá cao và có nhiều ưu điểm về mặt bảo mật:

Ẩn địa chỉ script thực: P2SH ẩn đi đoạn mã script thực sự trong một địa chỉ hash, khiến cho việc phân tích và hiểu rõ về script được sử dụng để chi tiêu từ địa chỉ trở nên khó khăn. Điều này giúp ngăn chặn một số loại tấn công và tăng cường bảo mật.

Đa dạng hóa khóa công khai: Một địa chỉ P2SH có thể được liên kết với nhiều khóa công khai hoặc loại script khác nhau. Ví dụ, nó có thể là một địa chỉ đa chữ ký (multisig) yêu cầu sự ký từ nhiều khóa, hoặc một địa chỉ có điều kiện yêu cầu chứng minh điều kiện nào đó mới có thể chi tiêu.

Bảo mật với các loại tấn công: Việc ẩn đoạn mã script trong địa chỉ hash giúp ngăn chặn một số loại tấn công như các cuộc tấn công brute-force hoặc các cuộc tấn công vét cạn thông tin từ các giao dịch.

Ứng dụng trong Lightning Network: P2SH cũng được sử dụng trong Lightning Network, nơi mà việc xử lý các giao dịch nội bộ được thực hiện thông qua các địa chỉ P2SH.

Quản lý rủi ro và Bảo mật tài sản: P2SH cung cấp một phương pháp bảo mật tài sản linh hoạt, đặc biệt trong trường hợp các tài sản được quản lý bởi nhiều bên hoặc đòi hỏi sự đồng thuận từ nhiều bên để chi tiêu.

4.2.2. Ứng dụng

P2SH, viết tắt của "Pay to Script Hash", là một tiêu chuẩn trong hệ thống giao dịch của Bitcoin. Nó cung cấp một cách để tạo địa chỉ Bitcoin mà việc chi tiêu cần phải đáp ứng một điều kiện quy định bởi một đoạn mã script nhất định.

Một số ứng dụng chính của P2SH trong mạng lưới Bitcoin:

Multisig Addresses (Địa chỉ Đa chữ ký): P2SH cho phép tạo ra địa chỉ Bitcoin đa chữ ký. Điều này có nghĩa là để chi tiêu từ địa chỉ đó, cần phải cung cấp chữ ký từ nhiều khóa cá nhân thay vì chỉ một khóa duy nhất. Điều này hữu ích trong việc quản lý và bảo mật tài sản với sự đồng thuận từ nhiều bên.

Giao dịch có điều kiện (Conditional Payments): P2SH cho phép tạo ra các giao dịch có điều kiện. Điều này có thể bao gồm việc thiết lập giao dịch mà chỉ có thể được chi tiêu nếu một điều kiện nhất định được đáp ứng, ví dụ như sau một khoảng thời gian xác định hoặc sau sự chứng minh của một sự kiện cụ thể.

Bảo mật và Quản lý rủi ro: P2SH giúp cải thiện bảo mật và quản lý rủi ro cho các giao dịch Bitcoin. Việc sử dụng P2SH giúp che giấu đoạn mã script thực sự mà cần được thực hiện để chi tiêu từ địa chỉ, điều này giúp ngăn chặn một số loại tấn công và tăng cường bảo mật.

Ứng dụng trong Lightning Network: P2SH cũng được sử dụng trong Lightning Network, một giải pháp mở rộng cho Bitcoin để thực hiện các giao dịch nhanh và chi phí thấp. Các kênh thanh toán Lightning thường sử dụng các địa chỉ P2SH cho các giao dịch nội bộ trong mạng lưới.

4.2.3. Đánh giá

Ưu điểm	Nhược điểm
Đa dạng hóa điều kiện chi tiêu: P2SH cho phép định nghĩa các điều kiện chi tiêu linh hoạt bằng cách sử dụng đoạn mã script, từ việc yêu cầu nhiều chữ ký từ nhiều người dùng cho đến điều kiện thời gian, sự kiện cụ thể hoặc điều kiện phức tạp hơn.	**Độ phức tạp cao:** Việc sử dụng P2SH yêu cầu hiểu rõ về cách thức hoạt động của mã hash và script. Điều này có thể tạo ra sự phức tạp và khó khăn cho người mới sử dụng.
Tính bảo mật cao: Khi sử dụng P2SH, script thực tế được che giấu trong mã hash, giúp ngăn chặn việc tiết lộ thông tin về điều kiện chi tiêu, cải thiện bảo mật cho các nguồn tài sản Bitcoin.	**Chi phí cao**: Một số giao dịch sử dụng P2SH có thể có chi phí giao dịch cao hơn so với các giao dịch thông thường. Điều này phụ thuộc vào kích thước của mã hash và script.
Quản lý rủi ro: Việc sử dụng P2SH có thể giúp giảm thiểu rủi ro từ các loại tấn công như mạng lưới, phishing, và lừa đảo. Nó cũng giúp ngăn chặn việc tiết lộ thông tin về điều kiện chi tiêu.	**Khả năng tương thích với legacy**: Mặc dù P2SH đã trở nên phổ biến, nhưng vẫn có một số ví Bitcoin hoặc dịch vụ không hỗ trợ tốt với P2SH.
Mở rộng tính năng: P2SH mở ra nhiều ứng dụng tiềm năng, bao gồm việc triển khai các giao dịch thông minh (smart contracts) và tích hợp vào các nền tảng lớn như Lightning Network.	Phụ thuộc vào mã hash: P2SH phụ thuộc vào việc mã hash được chấp nhận rộng rãi trong cộng đồng Bitcoin. Nếu có sự thay đổi trong chuẩn hoặc xu hướng sử dụng, điều này có thể gây ra vấn đề về tương thích.

4.2.4. Chương trình:

Mục tiêu:

Tạo ra và xử lý một giao dịch Bitcoin đa chữ ký (Multisig), bao gồm các bước sau:

- Tạo một địa chỉ Bitcoin đa chữ ký (2-of-2 Multisig Address) từ hai khóa cá nhân.
- Lock funds vào địa chỉ Multisig được tạo.
- Xác nhận giao dịch đã khóa bằng cách sử dụng một Bitcoin faucet trên mạng thử nghiệm (testnet).
- Viết code Python để xử lý và chuyển tiền từ địa chỉ Multisig đã khóa.

Cấu trúc chương trình:

Chương trình gồm 2 file:

multi.py: Tạo khóa và địa chỉ Multisig

tx.py: Xử lý và chuyển tiền từ địa chỉ Multisig đã khóa và xác nhận giao dịch hợp lệ

Các bước thực hiện:

Tạo Multisig Address:

- Sử dụng thư viện Bitcoin trong Python để tạo hai khóa cá nhân ngẫu nhiên.
- Tạo khóa công khai và khóa cá nhân.
- Tạo script đa chữ ký 2-of-2 từ hai khóa công khai.
- Tạo địa chỉ Multisig từ script đa chữ ký đã tạo.

Lock funds vào địa chỉ Multisig:

- Sử dụng Bitcoin faucet trên mạng thử nghiệm để gửi một số tiền Bitcoin testnet vào địa chỉ Multisig vừa tạo.

Xử lý và chuyển tiền từ địa chỉ Multisig đã khóa:

- Sử dụng thư viện Bitcoin trong Python để tạo giao dịch đầu vào và đầu ra.
- Lấy script đa chữ ký từ Multisig address.
- Tính toán hash của giao dịch để ký và xác nhận chữ ký từ hai khóa cá nhân.
- Đưa chữ ký vào scriptSig của giao dịch.
- Kiểm tra tính hợp lệ của giao dịch.

Chạy chương trình:

Đầu tiên, ta chạy file **multi.py** để tạo khóa và địa chỉ đa chữ ký. Kết quả output như sau:

```
┌──(kali㉿kali)-[~/Downloads/lab2]
└─$ python3 multi.py
Private Key 1: KyX98RyyawygEaGcCDhYYAuSMuRmvU6AkbwAoyPbeHGdf4F8S7rx
Private Key 2: KxjdRe3A1DoYwRCN3E3k3HmU4J7n6VFXzkXaEHSsH4kWYBCTHZkF
Redeem Script: 5221038156cbb3d1ea74100e3a8edea3142190d0e4d8c1b75b1a2f8657f5f941b8e4012103156d5ea616
6e5cb453c0926c0e3efa5102d55a6969735e1ffc718dcab58fa4a352ae
Multisig Address: myZLqhbeNvpoMDUYRMzaqMTdEABExE5kc7
```

Sau khi tạo địa chỉ đa chữ ký thành công, ta truy cập coinfaucet.com và nhập địa chỉ vào. Sau đó, ta lấy được txid của địa chỉ. Trong source code, ta sẽ điền mã giao dịch vào txid các thông tin vừa tạo vào các biến tương ương. Ta cũng có thể theo dõi kết quả chuyển thông qua https://blockstream.info/testnet/ .

Sau khi ghi xong các thông tin, ta thực hiện chạy file **tx.py**, thu được kết quả như sau:

```
┌──(kali㉿kali)-[~/Downloads/lab2]
└─$ python3 tx.py
tx: 0100000001eeb0a442d5c924ae74db2610ff6504ee194cd8fcff0ab8bf41cada5807b2168500000000da00483045022100 93dbb8924251fdb2d16e2a405158513bc
9cb866731ee5e827f0981ffa140888a022006e1feeec6e49dcdee9752d5e033d1add03776e918f77db25c324636a719403b0147304402202eabf97878b2ce0b1cdae3dd
365a0d9ab29491d7ff212c447d0fff9a9fc81aa9022063cfc4e25d889b24f76e333085ae49df2e591a3705b8fc5c3e0acd8cb2bd519e01475221038156cbb3d1ea74100
e3a8edea3142190d0e4d8c1b75b1a2f8657f5f941b8e4012103156d5ea6166e5cb453c0926c0e3efa5102d55a6969735e1ffc718dcab58fa4a352aeffffffff01000000
000000000017a914c5e5ea8ab092e84a4cb160c3d735dfc06608af5f8700000000
Transaction ID: 285c411bb5ba627a17fbd63b3610152fed98d94cd96126b9dd3ba778ca948b17
Transaction is valid
```

Xác nhận giao dịch hợp lệ.

4.2.5. Bài học và kinh nghiệm rút ra sau khi thực hiện Task 2

Có cơ hội được thực hành và hiểu rõ hơn về cách thức tạo và xử lý giao dịch Bitcoin đa chữ ký. Kinh nghiệm từ nhiệm vụ này sẽ giúp cải thiện kiến thức và kỹ năng trong việc làm việc với tiền điện tử và cải thiện độ chính xác và an toàn trong các giao dịch tương lai.

Hiểu rõ về Giao dịch Đa chữ ký (Multisig): Để thực hiện giao dịch Bitcoin đa chữ ký, hiểu rõ về cách hoạt động của giao dịch này là quan trọng. Điều này bao gồm quá trình tạo khóa công khai, khóa bí mật, mã đúng, và cách xử lý giao dịch sau khi đã được ký bởi nhiều người dùng.

Bảo mật và Quản lý khóa cá nhân: Việc quản lý và bảo mật các khóa cá nhân (private keys) rất quan trọng. Chúng cần được lưu trữ một cách an toàn và không bị mất, đồng thời tránh chia sẻ không cần thiết. Mất khóa cá nhân có thể dẫn đến mất mát hoặc không thể truy cập vào tài sản.

Kiểm thử và Thực hành trên môi trường thử nghiệm (Testnet): Việc thực hiện các giao dịch trên mạng lưới thử nghiệm (testnet) trước khi triển khai trên mạng lưới chính thức rất quan trọng. Điều này giúp tránh lỗi và xác nhận rằng quá trình tạo và xử lý giao dịch hoạt động như mong đợi.

Không chia sẻ thông tin khóa cá nhân và luôn kiểm tra lại trước khi gửi giao dịch trên mạng lưới chính thức.

5. TASK 3: ANALYSIS AND REFLECTION

5.1. ĐÁNG GIÁ

Phản ánh và nhận định:

Khi thực hiện nhiệm vụ tạo và xử lý các giao dịch Bitcoin Script, có một số điểm cần lưu ý sau:

Ưu điểm của Bitcoin Script:

- Linh hoạt và đa dạng: Bitcoin Script cung cấp khả năng lập trình linh hoạt để xác định các điều kiện chi tiêu. Điều này mở ra rất nhiều cơ hội trong việc xây dựng các giao dịch thông minh, đặc biệt là đa chữ ký và các điều kiện chi tiêu phức tạp hơn.
- Bảo mật tăng cao: Script cung cấp lớp bảo vệ cho các giao dịch và tài sản Bitcoin. Điều này giúp ngăn chặn một số loại tấn công và làm tăng tính an toàn trong quá trình giao dịch.

Hạn chế của Bitcoin Script:

- Độ phức tạp: Việc thao tác và xử lý các giao dịch Bitcoin Script đôi khi phức tạp, đặc biệt là với những người mới bắt đầu hoặc không có nền tảng vững chắc về lập trình.
- Chi phí giao dịch: Một số loại giao dịch Script có thể có chi phí cao hơn so với các giao dịch thông thường. Điều này có thể tăng cường chi phí trong quá trình sử dụng và triển khai.
- Khả năng tương thích: Một số dịch vụ và ví Bitcoin không hỗ trợ hoặc không tương thích tốt với các giao dịch Script, điều này có thể tạo ra những trở ngại trong việc sử dụng.

Các ứng dụng tiềm năng và tác động bảo mật:

Bitcoin Script mở ra một loạt các ứng dụng tiềm năng như đa chữ ký, giao dịch có điều kiện và smart contracts trong rất nhiều lĩnh vực khác nhau. Tuy nhiên, cần phải xem xét kỹ lưỡng về các yếu tố an toàn và tính khả dụng của nó trong từng trường hợp cụ thể.

Kết luận:

Bitcoin Script có những ưu và nhược điểm riêng, và việc sử dụng nó phụ thuộc vào các yếu tố cụ thể của mỗi tình huống giao dịch. Hiểu biết sâu sắc về Script giúp tận dụng hết tiềm năng và đồng thời đảm bảo an toàn trong quá trình sử dụng.

5.2. BẢNG SO SÁNH P2PKH VÀ P2SH

Đặc điểm	P2PKH	P2SH
Mục đích chính	Giao dịch đến một địa chỉ dựa trên Public Key Hash	Giao dịch đến một địa chỉ dựa trên Script Hash
Định dạng địa chỉ	Bắt đầu bằng '1'	Bắt đầu bằng '3'
Quy trình chi tiêu	Gửi Bitcoin đến địa chỉ Public Key Hash	Gửi Bitcoin đến địa chỉ Script Hash
Sử dụng	Được sử dụng phổ biến trong giao dịch	Được sử dụng cho các giao dịch

	thông thường	đa chữ ký và thông minh
Phát triển	Phát triển từ phiên bản cũ hơn của Bitcoin	Được giới thiệu sau khi Bitcoin đã phát triển
Tính linh hoạt	Thấp	Cao
Bảo mật	Tốt	Tốt
Đa dạng hóa	Hạn chế	Linh hoạt
Chi phí	Thấp	Có thể cao hơn so với P2PKH

6 NGUỒN THAM KHẢO

SST	Link tham khảo
1	https://komodoplatform.com/en/academy/p2pkh-pay-to-pubkey-hash/
2	https://river.com/learn/terms/p/p2pkh/
3	https://academy.binance.com/vi/articles/an-introduction-to-bitcoin-script
4	https://learn.saylor.org/mod/book/view.php?id=36364&chapterid=18952
5	https://pypi.org/project/bitcoin/
6	https://pypi.org/project/bit/
7	https://bitcoinmagazine.com/guides/what-is-a-multisignature-wallet
8	https://www.bitcoin.com/get-started/how-to-set-up-and-use-shared-multisig-bitcoin-wallet/
9	https://en.bitcoin.it/wiki/Multi-signature
10	https://bitcoin.stackexchange.com/questions/80528/python-library-for-multisignature-hd-wallets

HẾT