**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

A picture containing logo

Description automatically generated**🙡🕮🙣**

**BÁO CÁO ĐỒ ÁN 2**

**UNDERSTANDING BITCOIN`S SCRIPTING LANGUAGE**

MÔN : BLOCKCHAIN VÀ ỨNG DỤNG

Lớp CSC15010\_20CNTThuc

NHÓM 5

GVLT: Nguyễn Đình Thúc

HDTH: Ngô Đình Hy

Thành phố Hồ Chí Minh, tháng 12 năm 2023

1. **THÔNG TIN NHÓM 5:**

|  |  |  |
| --- | --- | --- |
| **MSSV** | **Họ Và Tên** | **Email** |
| 20127090 | Lê Thanh Tú | thanhtuhr01@gmail.com |
| 20127308 | Phan Minh Sáng | pmsang20@clc.fitus.edu.vn |
| 20127318 | Phan Trí Tài | phantritai69@gmail.com |
| 20127569 | Tô Đình Phương Nam | tonam870@gmail.com |
| 20127607 | Phạm Việt Quang | pvquang0703@gmail.com |

1. **THÔNG TIN VỀ ĐỒ ÁN:**

* Project yêu cầu: Để hiểu sâu hơn về Bitcoin Script và Bitcoin kèm theo cách nó hoạt động trong mạng Bitcoin.
* Bitcoin là một loại tiền điện tử được tạo ra vào năm 2009 bởi một người (hoặc nhóm người) giấu tên dưới bí danh Satoshi Nakamoto. Nó là đồng tiền kỹ thuật số đầu tiên và phổ biến nhất trên thế giới, được sử dụng như một phương tiện thanh toán trực tuyến.
* Một trong những đặc điểm quan trọng của Bitcoin là scripting language được biết đến là Bitcoin Script.
* Và ở đây chúng em sử dụng ngôn ngữ là: Python
* Thư viên được sử dụng chính ở đây là: bitcoin-utils 0.6.4

1. **CÁC NHIỆM VỤ CHÍNH:**
2. ***Task 1: Basic Script Execution***

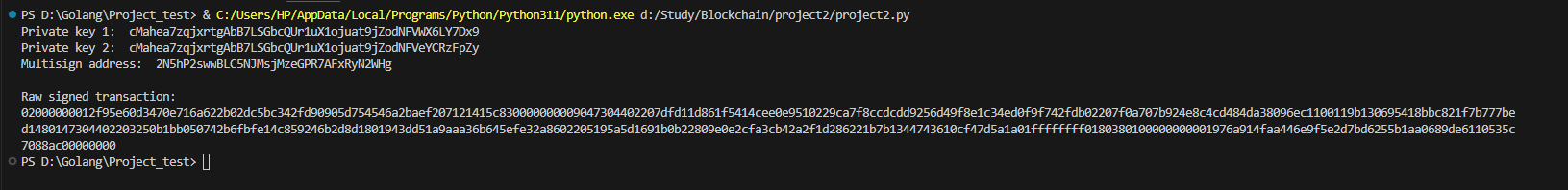
* Task:
  + Bước đầu tiên là tạo một đoạn mã Bitcoin script đơn giản để khóa quỹ vào một địa chỉ cụ thể, sử dụng lệnh Pay-to-Public-Key-Hash (P2PKH).
  + Ta sẽ nhận được một địa chỉ testnet để thực hiện nhiệm vụ này.
* Requirements:
  + Tạo P2PKH Script:
    - Tạo priv, pub (lấy từ private key) và address (lấy từ testnet).
  + Tạo transaction input (*input\_tx*):
    - **txid** (biến này lưu trữ ID giao dịch (TxID) của UTXO bạn muốn chi tiêu).
    - **output\_index** (biến này lưu trữ chỉ số của đầu ra trong giao dịch được tham chiếu bởi txid).
  + Tạo transaction ouput (*output\_tx*):
    - **output\_script** (biến này lưu trữ địa chỉ của người nhận mà bạn muốn gửi Bitcoin).
    - **output\_value** (biến này chứa số lượng Bitcoin bạn muốn gửi, được đo bằng satoshi).
  + Tạo Transaction từ *input\_tx* + *output\_tx* và kí bằng *private\_key.*

A black screen with a black background

Description automatically generated

1. ***Task 2: Multisignature Transactions***

* Task:
  + Phát triển một tập lệnh đa chữ ký 2-of-2 bằng cách sử dụng đúng hai khóa công khai đã được cung cấp.
* Requirements:
  + Tạo 2-of-2 Multisig Script
    - Tạo hai khóa riêng: priv\_key1 và priv\_key2.
    - Tạo hai khóa công khai từ khóa riêng: pub\_key1 và pub\_key2.
    - Tạo redeem script nhiều chữ ký 2-2.
    - Tạo địa chỉ P2SH từ redeem script.
    - Tạo transaction giống cách tạo transaction của task 1.
  + Tạo transaction giống task 1(có 2 Tx từ priv\_key1 và priv\_key2).
  + Tạo tx\_in.script\_sig (kí bằng priv\_key1 và priv\_key2):
    - Tạo sig1 dựa trên priv\_key1 và pub\_key1.
    - Tạo sig2 dựa trên priv\_key2 và pub\_key2.



1. ***Task 3: Analysis and Reflection***

* Ưu điểm của Bitcoin Script:
  + Hợp đồng thông minh:
    - Bitcoin Script cho phép triển khai các hợp đồng thông minh cơ bản. Người dùng có thể đặt điều kiện và quy tắc phức tạp cho việc chi tiêu Bitcoin, mở ra nhiều ứng dụng trong lĩnh vực tài chính và giao dịch.
  + Đa chữ ký:
    - Bitcoin Script hỗ trợ việc tạo các địa chỉ có thể được kiểm soát bởi nhiều chữ ký. Điều này tạo ra khả năng sử dụng giao dịch đa chữ ký (multisig), giúp cải thiện bảo mật và quản lý rủi ro.
  + Bảo mật cao:
    - Bằng cách sử dụng hash của khóa công khai thay vì khóa công khai trực tiếp, Bitcoin Script tăng cường bảo mật. Mã hóa SHA-256 được sử dụng trong quá trình này, và cho đến thời điểm kiến thức của tôi được cập nhật, không có thuật toán lượng tử nào được biết đến có thể phá vỡ SHA-256.
  + Khả năng mở rộng:
    - Khả năng mở rộng của Bitcoin Script cho phép các cập nhật và nâng cấp trong tương lai, mở ra các cơ hội mới cho sự phát triển và tích hợp các tính năng mới.
* Nhược điểm của Bitcoin Script:
  + Đơn giản:
    - Mặc dù tính đơn giản của Bitcoin Script là một ưu điểm trong việc đảm bảo tính an toàn, nhưng cũng là một hạn chế khi muốn triển khai các hợp đồng thông minh phức tạp. So với một số nền tảng blockchain khác, Bitcoin Script có khả năng lập trình hạn chế hơn.
  + Khả năng mở rộng hạn chế:
    - Quá trình mở rộng của Bitcoin có thể đối mặt với các thách thức liên quan đến khả năng thay đổi Bitcoin Script mà không làm ảnh hưởng đến sự đồng thuận của toàn bộ mạng lưới. Sự đồng thuận là một yếu tố quan trọng để bảo đảm tính ổn định của mạng lưới.
  + Thời gian chờ có thể gây phiền toái:
    - Việc sử dụng thời gian chờ (locktime) để đặt điều kiện về thời gian cho một giao dịch có thể gây phiền toái khi người dùng phải chờ đến một khoảng thời gian cụ thể trước khi có thể chi tiêu quỹ.
  + Khả năng quản lý cao có thể tăng rủi ro:
    - Trong một số trường hợp, việc sử dụng các tính năng phức tạp trong Bitcoin Script có thể tăng nguy cơ lỗi lạc hoặc rủi ro bảo mật, đặc biệt nếu không được triển khai đúng cách.
* Ứng dụng thực tế của Bitcoin Script:
  + Hợp đồng thông minh:
    - Bitcoin Script cho phép triển khai các hợp đồng thông minh cơ bản. Ví dụ, người ta có thể thiết lập điều kiện để một khoản thanh toán chỉ được thực hiện khi cả hai bên đều đồng ý, hoặc tạo ra các hợp đồng đa chữ ký.
  + Giao dịch đa chữ ký (Multisig):
    - Bitcoin Script hỗ trợ giao dịch đa chữ ký, nơi một quỹ chỉ có thể được chi tiêu khi có sự chấp thuận từ nhiều chữ ký. Điều này thích hợp cho việc quản lý tài sản có giá trị lớn hoặc tài khoản cộng đồng.
  + Bảo mật giao dịch:
    - Bitcoin Script được sử dụng để tạo ra các quy tắc và điều kiện cho việc chi tiêu Bitcoin, cải thiện tính bảo mật của các giao dịch. Điều này có thể bao gồm việc đặt điều kiện về thời gian, ngày, hoặc sự chấp thuận từ nhiều bên.
  + Phòng ngừa rủi ro và quản lý rủi ro:
    - Các điều kiện trong Bitcoin Script có thể được sử dụng để xây dựng các biện pháp phòng ngừa rủi ro và quản lý rủi ro trong các giao dịch tài chính và hợp đồng.

1. **TÀI LIỆU THAM KHẢO:**

* [Gitbub thư viện python-bitcoin-utils](https://github.com/karask/python-bitcoin-utils/blob/master/examples/p2pkh_transaction.py).
* [Tìm hiểu về p2pkh](https://trezor.io/learn/a/pay-to-public-key-hash-p2pkh).
* [Ưu và nhược điểm của Bitcoin](https://cleartax.in/s/advantages-and-disadvantages-of-bitcoin).
* [Tài liệu trong Project2 của thầy](https://courses.ctda.hcmus.edu.vn/mod/assign/view.php?id=76847).