TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN MÔN BẢO MẬT THÔNG TIN**

**XÂY DỰNG PHƯƠNG THỨC OHIE TRONG BLOCKCHAIN**

*Người hướng dẫn*: **Ph.D Huỳnh Ngọc Tú**

*Người thực hiện*: **Nguyễn Văn Long**

**Nguyễn Trường Giang**

**Nguyễn Trọng Hiếu**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN MÔN BẢO MẬT THÔNG TIN**

**XÂY DỰNG PHƯƠNG THỨC OHIE TRONG BLOCKCHAIN**

*Người hướng dẫn*: **Ph.D Huỳnh Ngọc Tú**

*Người thực hiện*: **Nguyễn Văn Long**

**Nguyễn Trường Giang**

**Nguyễn Trọng Hiếu**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

# LỜI CẢM ƠN

Nhóm tôi xin được gửi lời cảm ơn đến trường Đại học Tôn Đức Thắng, nơi đã tạo cho chúng tôi môi trường và điều kiện học tập hiệu quả. Trường cũng đã tổ chức hợp lý công tác học tập trực tuyến trong giai đoạn dịch Covid để nhóm có thể phát huy tối đa khả năng bản thân để hoàn thành đồ án môn học Bảo mật thông tin.

Tôi xin dành tặng lời cảm ơn đến cô Huỳnh Ngọc Tú. Cô đã trực tiếp hướng dẫn, gợi ý các phương pháp trong suốt quá trình thực hiện đề tài.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của chúng tôi và được sự hướng dẫn của cô Huỳnh Ngọc Tú;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác dẫn đều có trích và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Nguyễn Văn Long*

*Nguyễn Trường Giang*

*Nguyễn Trọng Hiếu*

# PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

# TÓM TẮT

Trong phần báo cáo lần trước, nhóm em đã trình bày chi tiết lý thuyết về Blockchain cũng như phương thức đồng thuận Nakamoto và Ohie. Sự khác nhau về 2 giao thức này và ưu điểm đem lại từ Ohie. Trong báo cáo lần này nhóm em xin được trình bày về thực nghiệm của nhóm.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc86357516)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc86357517)

[TÓM TẮT iv](#_Toc86357518)

[DANH MỤC HÌNH VẼ 2](#_Toc86357519)

[CHƯƠNG 1 - THỰC NGHIỆM 3](#_Toc86357520)

[1.1 Yêu cầu về hệ thống 3](#_Toc86357521)

[1.2 Các điểm chính của thực nghiệm 3](#_Toc86357522)

# DANH MỤC HÌNH VẼ

[Hình 1.1 Tạo public và private key 4](#_Toc86356516)

[Hình 1.2 Nhúng private vào transaction 4](#_Toc86356517)

[Hình 1.3 Tạo block mới 5](#_Toc86356518)

[Hình 1.4 Nhập liệu cho block 5](#_Toc86356519)

[Hình 1.5 Mã hóa block bằng hash 6](#_Toc86356520)

[Hình 1.6 Kiểm tra block đã hash 6](#_Toc86356521)

[Hình 1.7 Kiểm tra tính xác thực của người gửi 6](#_Toc86356522)

[Hình 1.8 Phương thức đồng thuận Nakamoto 7](#_Toc86356523)

# THỰC NGHIỆM

## Yêu cầu về hệ thống

Cần cài đặt python và một số gói của python như flask, requests, flask-cors, pycryptodome

Chúng ta cần khởi động Server và client để thực hiện giao dịch

* Server theo cú pháp: *python -m blockchain* port mặc định sẽ là 5000
* Client theo cú pháp: *python -m client <PORT-HERE>*

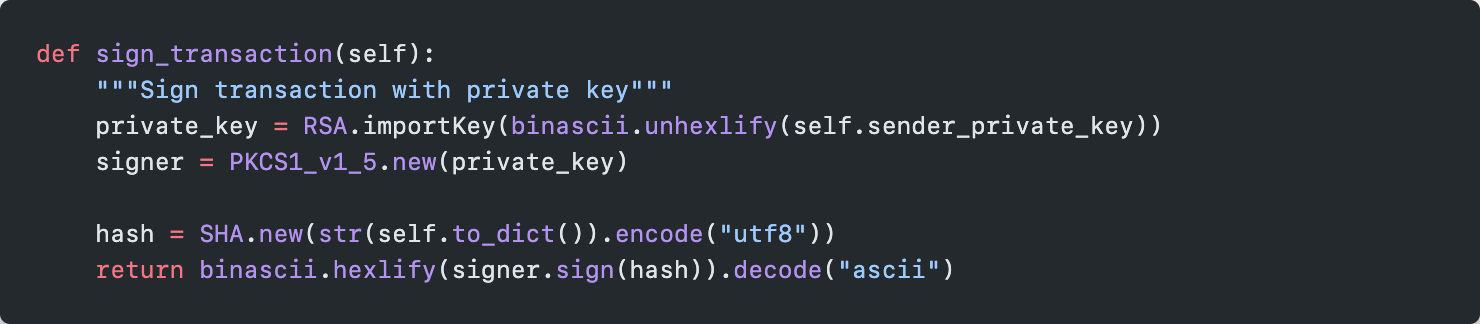
## Các điểm chính của thực nghiệm

Đầu tiên chúng ta cần tạo mã public key và private key cho ví tiền bằng hàm hash đơn giản



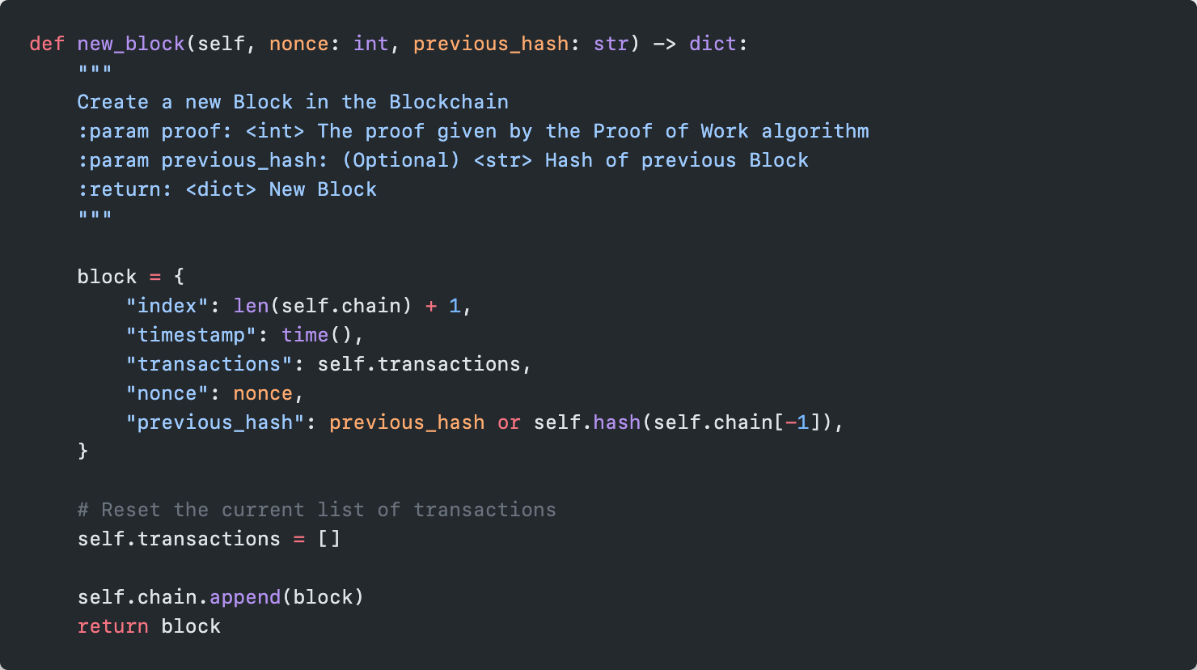
Hình 1.1 Tạo public và private key

Sau khi đã có 2 key, ta tiến hành nhúng private key vô giao dịch để đảm bảo sự xác thực và tính an toàn

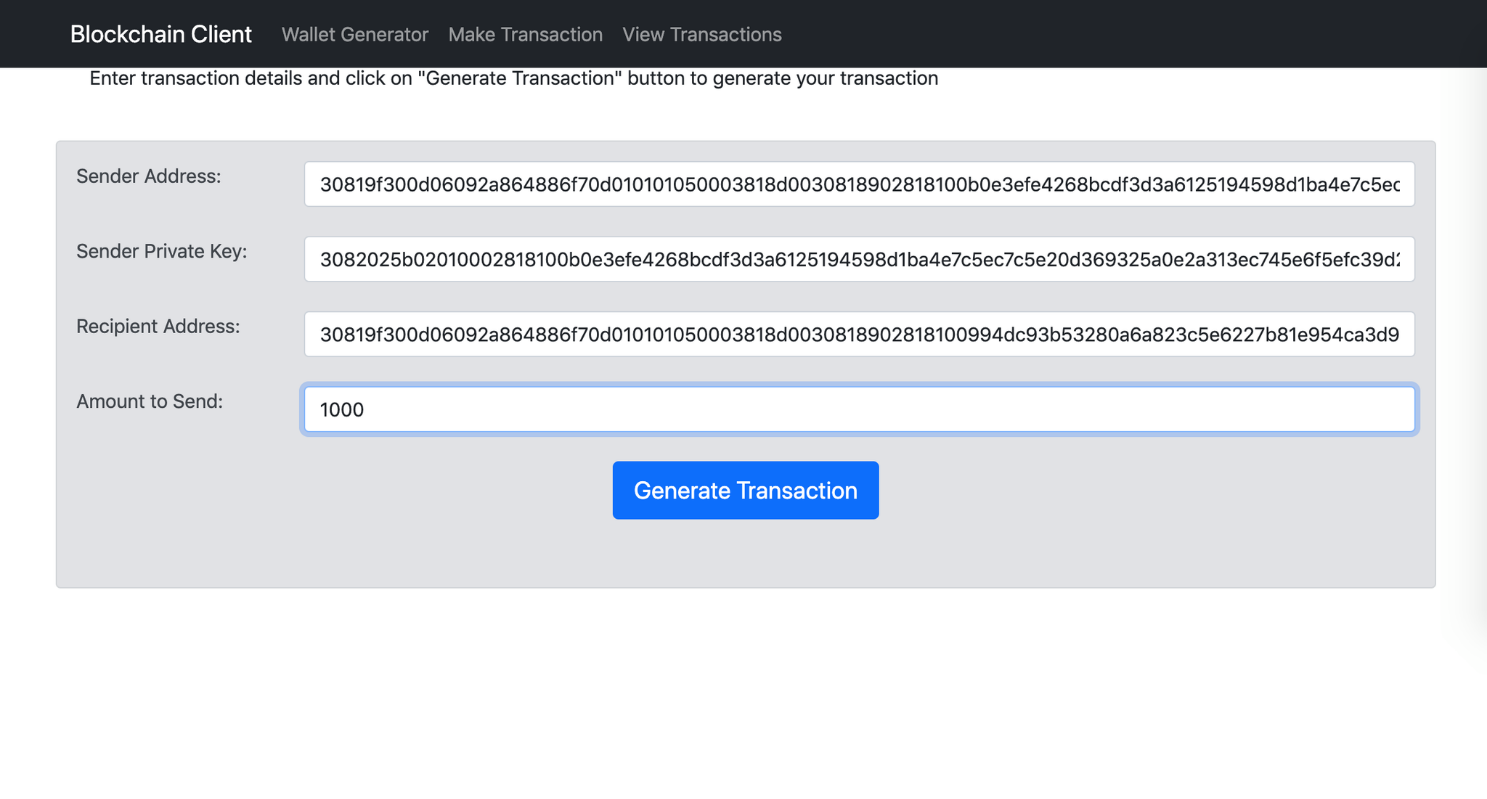


Hình 1.2 Nhúng private vào transaction

Tiếp theo sẽ tạo block mới và tiến hành nhập thông tin, những thông tin cần chú ý đó là địa chỉ người gửi, mã xác thực của người gửi, địa chỉ người nhận và số tiền trong giao dịch

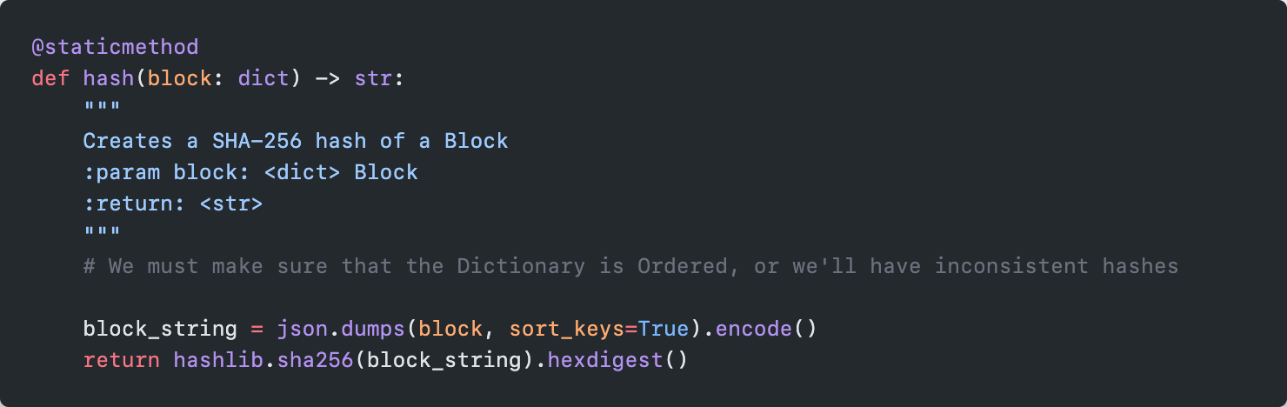


Hình 1.3 Tạo block mới

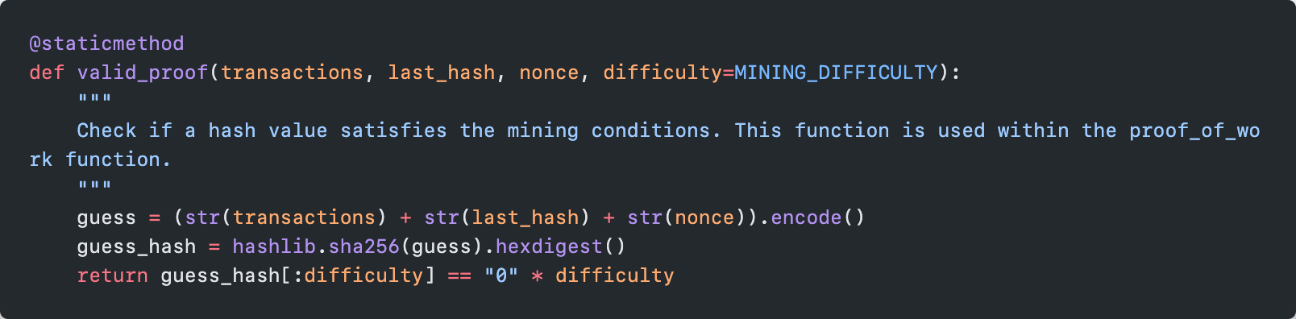


Hình 1.4 Nhập liệu cho block

Sau khi đã có block thì tiến hành mã hóa nó với hàm hash sha256, và chúng ta cũng cần kiểm tra hàm hash đó có hợp lệ không, hợp lệ là khi kết thúc của hàm hash là số 0

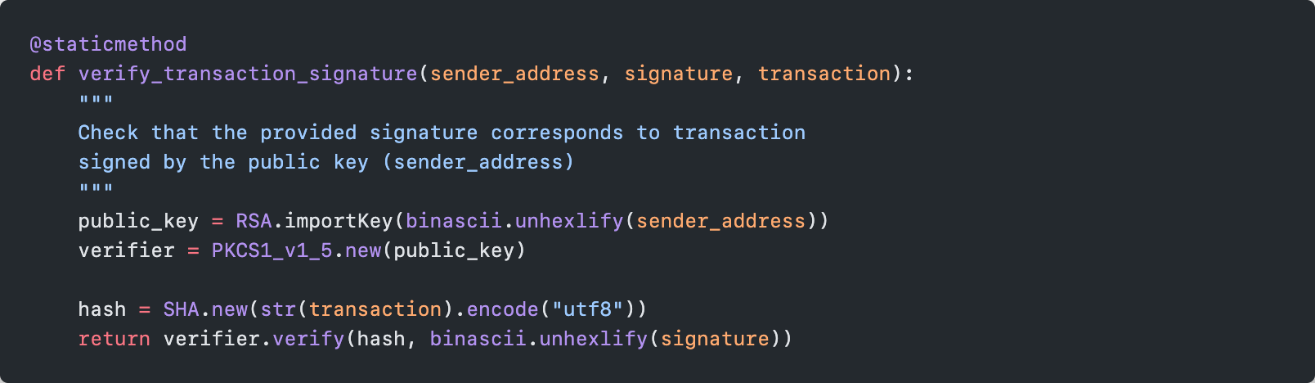


Hình 1.5 Mã hóa block bằng hash



Hình 1.6 Kiểm tra block đã hash

Một điều đáng quan tâm là cần xác thực người gửi có phải chính chủ hay không để tranh những trường hợp lừa đảo.



Hình 1.7 Kiểm tra tính xác thực của người gửi

Và phần cốt yếu nhất đó là phương thức đồng thuật Nakamoto



Hình 1.8 Phương thức đồng thuận Nakamoto