

**MSSV:** DTH225710

**Họ và tên:** Lê Trí Nhân

**Lớp:** DH23TH2

**Ngày thực hiện:** 15/01/2026

## **LAB 1: METAMASK, ETHEREUM VÀ BLOCK**

### **1. GIỚI THIỆU (INTRODUCTION)**

Trong Bài giảng 1, giảng viên đã giới thiệu rõ ràng về blockchain và mật mã học (cryptography). Để giúp người học hiểu sâu hơn cách các block (khối) hoạt động trong các ứng dụng thực tế, bài thực hành (lab) này sẽ trình bày logic xây dựng block thông qua việc sử dụng ví MetaMask và tạo các giao dịch Ethereum. Nếu bạn muốn tham khảo hướng dẫn chi tiết hơn về MetaMask, có thể xem tài liệu chính thức tại: <https://docs.metamask.io/>

Thông qua việc tạo các tài khoản Ethereum và thực hiện nhiều giao dịch trong MetaMask, chúng ta sẽ phân tích sâu các thuộc tính của giao dịch Ethereum và hàm băm mật mã (Cryptographic Hashing) nhằm hiểu rõ tính xác thực (authenticity) và bảo mật (security) của các giao dịch Ethereum.

### **2. METAMASK**

#### **2.1. Giới thiệu**

MetaMask là một ví tiền mã hóa Ethereum (Ethereum crypto wallet) dạng plug-in cho trình duyệt Chrome. MetaMask có sẵn dưới dạng tiện ích mở rộng trình duyệt và ứng dụng di động. Nó cung cấp

kho khóa (key vault), cơ chế đăng nhập an toàn và ví token, tất cả những gì cần thiết để quản lý tài sản số (digital assets).

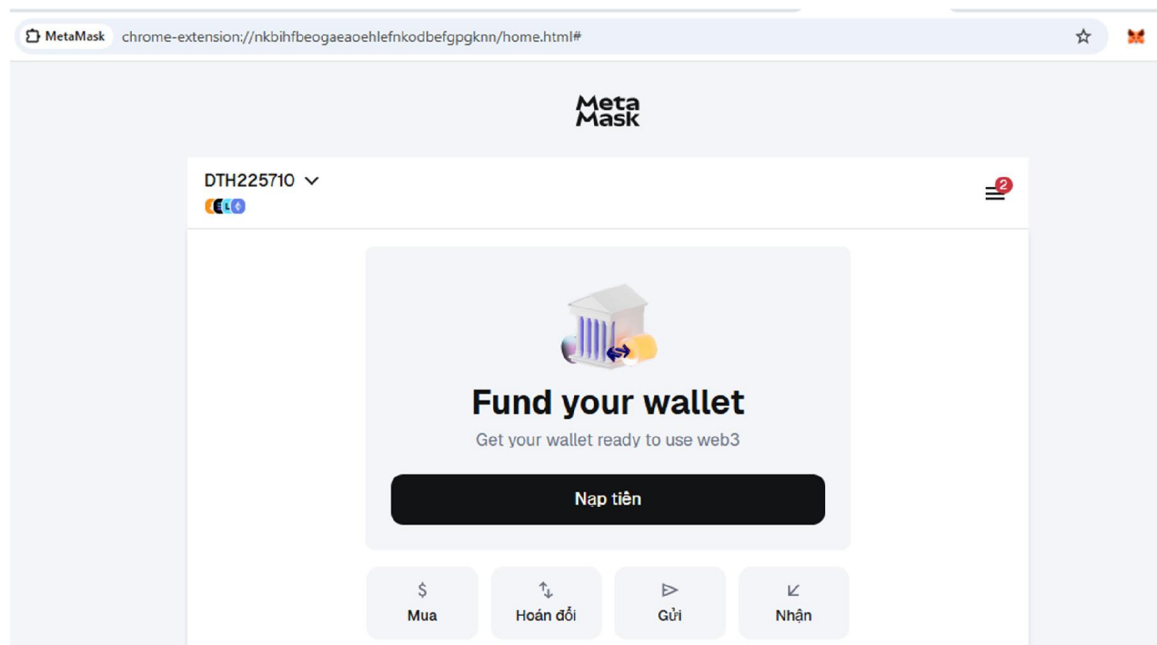
MetaMask cung cấp cách đơn giản nhưng an toàn nhất để kết nối với các ứng dụng dựa trên blockchain. Trong các bài lab này, MetaMask sẽ được sử dụng để lưu trữ và gửi token giữa các tài khoản cũng như tương tác với smart contract (hợp đồng thông minh).

## 2.2. Cài đặt MetaMask (MetaMask Setup)

Thông tin đầy đủ và tài liệu hướng dẫn MetaMask có tại website chính thức: <https://metamask.io>

Khi tạo tài khoản MetaMask mới, cần lưu ý:

- Mật khẩu mạnh (strong password) rất quan trọng vì nó dùng để mã hóa private key.
- Private key cho phép truy cập toàn bộ Ether và token.
- Secret Backup Phrase (cụm từ khôi phục gồm 12 từ) phải được ghi lại và lưu trữ an toàn, vì nó cho phép khôi phục tài khoản khi đăng xuất hoặc xóa dữ liệu trình duyệt.



-

### 2.3. Nạp Ether (Deposit Ether)

Trong bài lab này, chúng ta sử dụng mạng thử nghiệm Sepolia (thay vì Main Ethereum Network) để tránh tốn Ether thật. Ether thử nghiệm có thể nhận miễn phí từ:

- <https://faucet.quicknode.com/ethereum/sepolia>
- <https://www.alchemy.com/faucets/ethereum-sepolia>

### YÊU CẦU (TO DO 1):

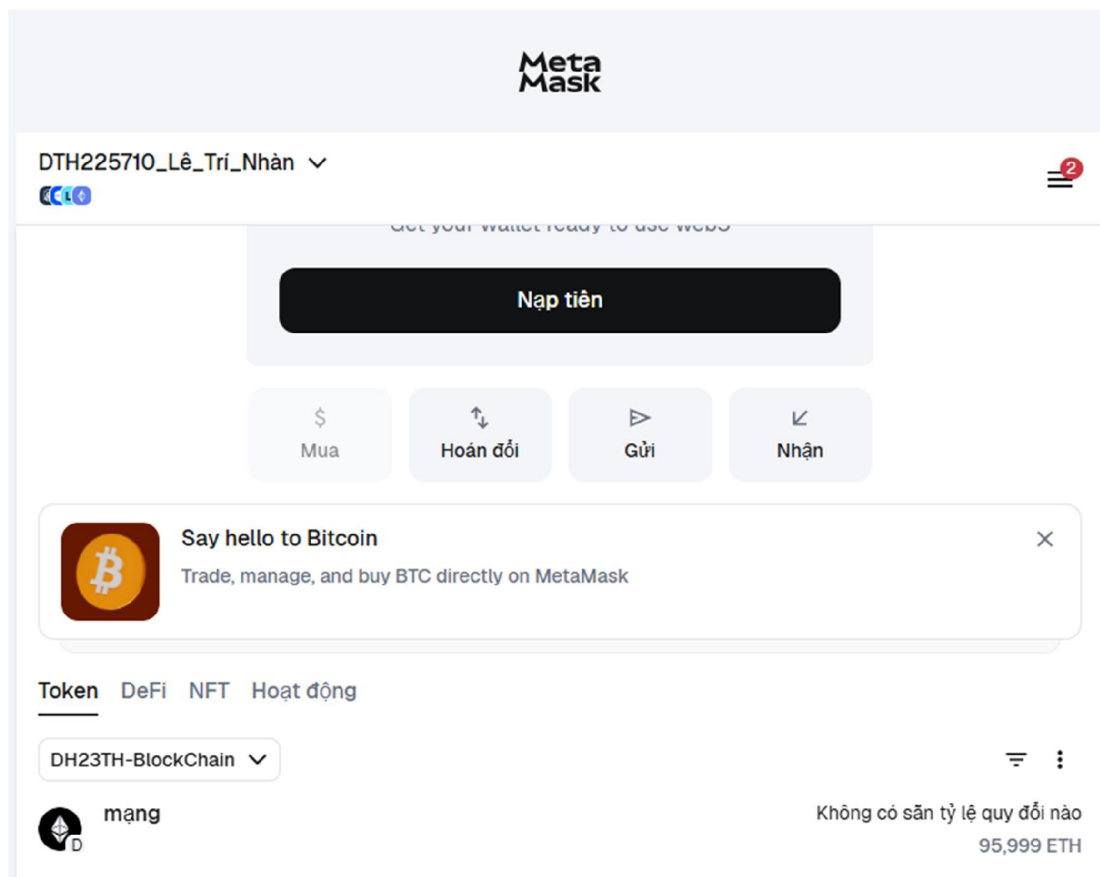
Nạp Ether vào tài khoản MetaMask của bạn.

### 2.4. Thực hiện giao dịch (Make a Transaction)

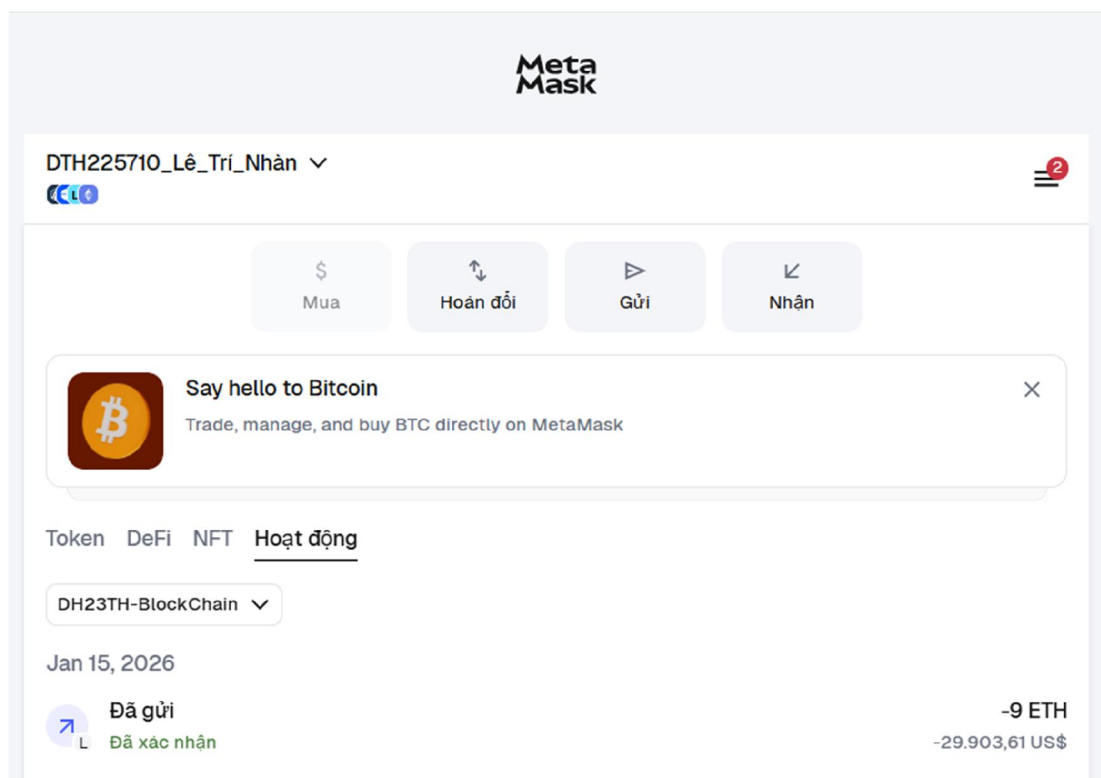
Người học tạo nhiều tài khoản trong MetaMask và thực hiện giao dịch chuyển Ether giữa các tài khoản này. Thông tin giao dịch có thể xem chi tiết trên Etherscan, bao gồm Transaction Hash, Block, Timestamp, From, To, Value và Transaction Fee.

### YÊU CẦU (TO DO 2):

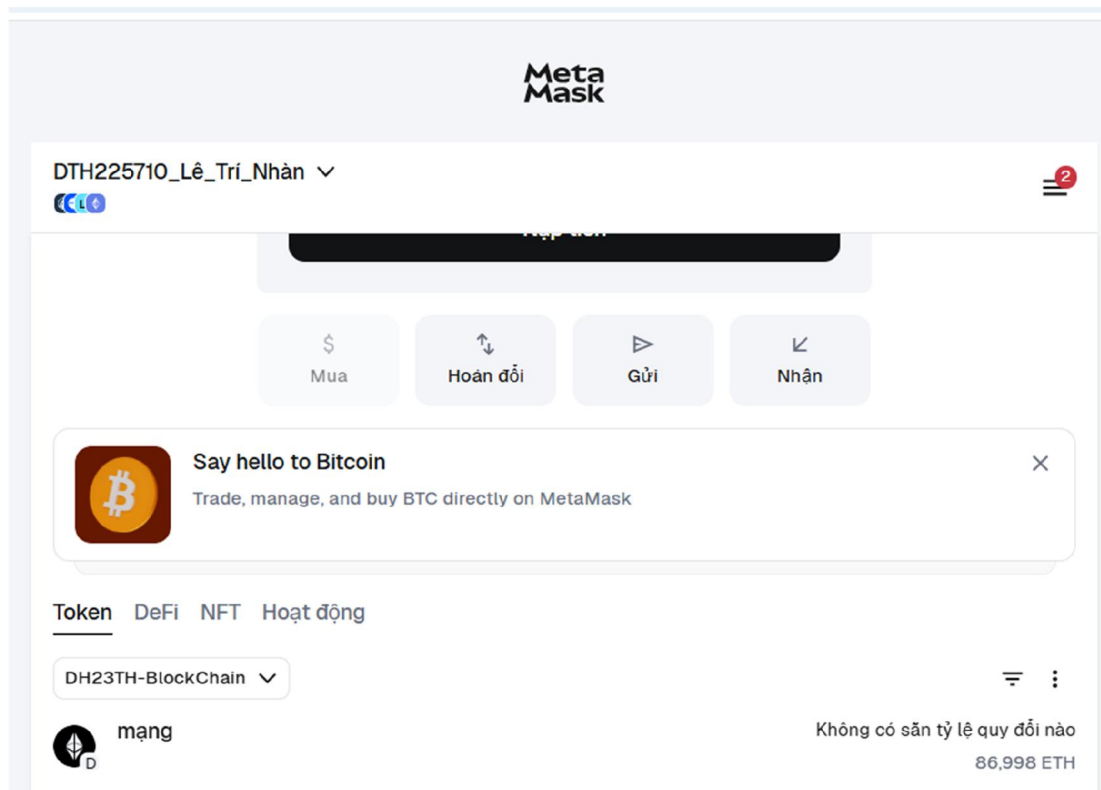
Tạo nhiều tài khoản và thực hiện các giao dịch giữa chúng.



**Figure 1. trước khi thực hiện giao dịch**



**Figure 2. giao dịch thành công**



**Figure 3. Kết quả sau khi thực hiện giao dịch thành công**

### **3. HÀM BẮM MẬT MÃ (CRYPTOGRAPHIC HASHING)**

#### **3.1. Giới thiệu**

Hàm băm mật mã (Cryptographic Hash Function) đóng vai trò cốt lõi trong blockchain. Thông qua việc phân tích các đặc tính của hàm băm, chúng ta hiểu cách các block được liên kết với nhau và cách mạng Ethereum vận hành.

#### **3.2. Các thuộc tính của hàm băm mật mã**

- Tính xác định (Deterministic)
- Tính toán nhanh (Quick to compute)
- Không thể đảo ngược (Pre-image resistance)
- Thay đổi nhỏ đầu vào → thay đổi lớn đầu ra

## SHA256 Hash

Data:	DTH225710_LeTriNhan
Hash:	c212d0c953919f5e09c00d2100a9500ee36f53a18d5cd25bc133e999601c3d01

## SHA256 Hash

Data:	DTH225710_LeTriNhan_0
Hash:	a0516fdbacf11129a6e6fb693feac714bb1db981fcbfee17ef64549c09cac30e

**Figure 4. chuỗi hash của data được tạo ra sau khi người dùng nhập nội dung mới vào và luôn được thay đổi thành chuỗi hash mới mỗi khi có sự thay đổi so với chuỗi hash ban đầu**

- Hai thông điệp khác nhau → hai giá trị băm khác nhau

### **YÊU CẦU (TO DO 3):**

Thử nghiệm các thuộc tính của hàm băm tại:

<https://andersbrownworth.com/blockchain/hash>

## **4. GIAO DỊCH ETHEREUM (ETHEREUM TRANSACTION)**

### **4.1. Giới thiệu**

Phần này phân tích chi tiết cấu trúc và tính xác thực của giao dịch Ethereum, bao gồm cách ký giao dịch (transaction signature) và xác minh người gửi.

### **4.2. Các tham số giao dịch**

Một giao dịch Ethereum gồm:

- from: địa chỉ gửi
- to: địa chỉ nhận
- value: giá trị Ether (Wei)
- gas, gasPrice: chi phí tính toán
- data: dữ liệu ABI cho smart contract
- nonce: số chống phát lại (replay attack)

### **4.3. Chữ ký giao dịch Ethereum**

Ethereum sử dụng:

- ECDSA (Elliptic Curve Digital Signature Algorithm)
- Keccak-256 hash
- ECRECOVER để khôi phục địa chỉ từ chữ ký

## **YÊU CẦU (TO DO 4):**

Thực hành thêm giao dịch vào blockchain và xác thực chữ ký.

## Coinbase Transactions

Peer A

Block: # 1

Nonce: 16651

Coinbase: \$ 100.00 -> Anders

Tx:

Prev: 0000430d7625b066f366545d1929975a0d3ff1f8047e56cc587cadd

Hash: 0000430d7625b066f366545d1929975a0d3ff1f8047e56cc587cadd

Mine

Block: # 2

Nonce: 215458

Coinbase: \$ 100.00 -> Anders

Tx:

Prev: 0000430d7625b066f366545d1929975a0d3ff1f8047e56cc587cadd

Hash: 0000baeb58c2a09f9a5f5635543d97c672a15494fcea617064d931

Mine

Block: # 3

Nonce: 146

Coinbase: \$ 100.00 -> A

Tx:

Prev: 0000baeb58c2a09f9a5f5635543d97c672a15494fcea617064d931

Hash: 0000df10632b734f5a5fc126a8f0e8094f04

Mine

- Dữ liệu ban đầu hoàn toàn không có xung đột

## Coinbase Transactions

Peer A

Block: # 2

Nonce: 215458

Coinbase: \$ 100.00 -> Anders

Tx:

Prev: 0000430d7625b066f366545d1929975a0d3ff1f8047e56cc587cadd

Hash: 8d5d9f6839f1ba08c9cae2a970be9f7e06646e72671e88fea89974

Mine

Block: # 3

Nonce: 146

Coinbase: \$ 100.00 -> Anders

Tx:

Prev: 8d5d9f6839f1ba08c9cae2a970be9f7e06646e72671e88fea89974

Hash: 2dc436b5c7e2d52c734d84b0dd72d460604304934379520d933fae6

Mine

Block: # 4

Nonce: 18292

Coinbase: \$ 100.00 ->

Tx:

Prev: 20c436b5c7e2d52c734d84b0dd72d460604304934379520d933fae6

Hash: 5ee1029ac669c7c3955d0df90d15c37

Mine

- Sau khi thay đổi giá trị gửi đến Sophia thì đã xảy ra thay đổi toàn bộ các mã hash phía sau nó

## Coinbase Transactions

Peer A

Block: # 2

Nonce: 63287

Coinbase: \$ 100.00 -> Anders

Tx:

Prev: 0000430d7625b066f366545d1929975a0d3ff1f8047e56cc587cadd

Hash: 00005dbbfef34b78902c043348b09c7c9c5e20e11d9008a1c0d17

Mine

Block: # 3

Nonce: 15388

Coinbase: \$ 100.00 -> Anders

Tx:

Prev: 00005dbbfef34b78902c043348b09c7c9c5e20e11d9008a1c0d17

Hash: 000065c8a61519d0eefdbb75e5c675b264ce811e17f1a149ff50bf

Mine

Block: # 4

Nonce: 18292

Coinbase: \$ 100.00 ->

Tx:

Prev: 000065c8a61519d0eefdbb75e5c675b264ce811e17f1a149ff50bf

Hash: 050774d50833169a7d661755c61e0a20

Mine

- Sau khi Mine lại các các block đã thay đổi thì sẽ được chấp thuận và không còn xung đột nữa