

MSSV:	DTH225710
Họ và tên:	Lê Trí Nhàn
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).

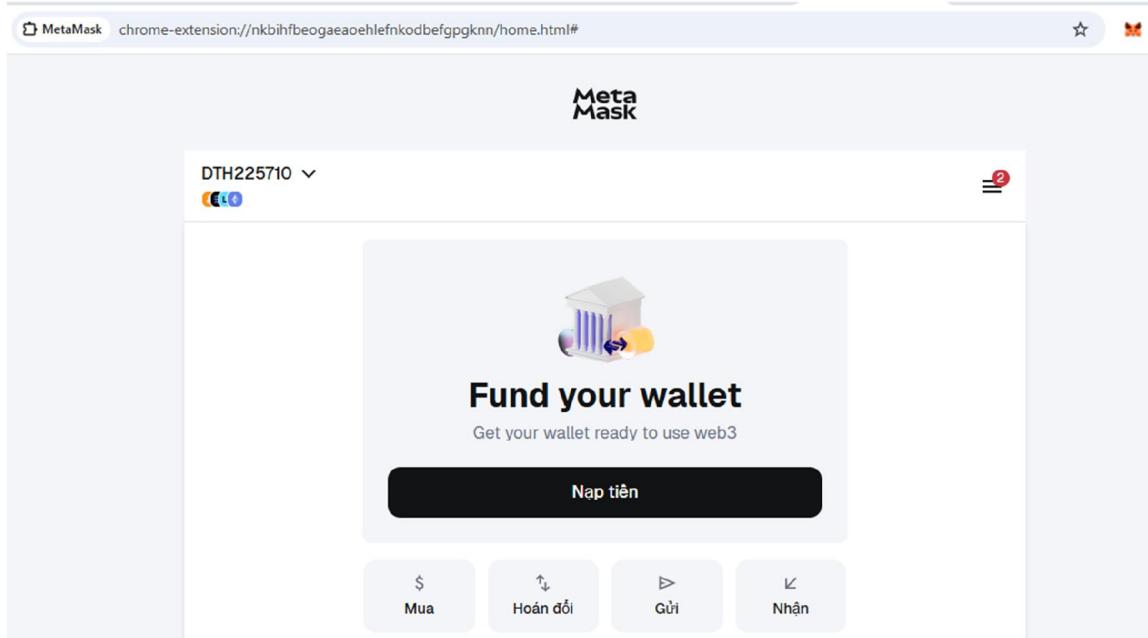
MetaMask cung cấp cách đơn giản nhưng an toàn nhất để kết nối với các ứng dụng dựa trên blockchain. Trong các bài lab này, MetaMask sẽ được sử dụng để lưu trữ và gửi token giữa các tài khoản cũng như tương tác với smart contract (hợp đồng thông minh).

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.

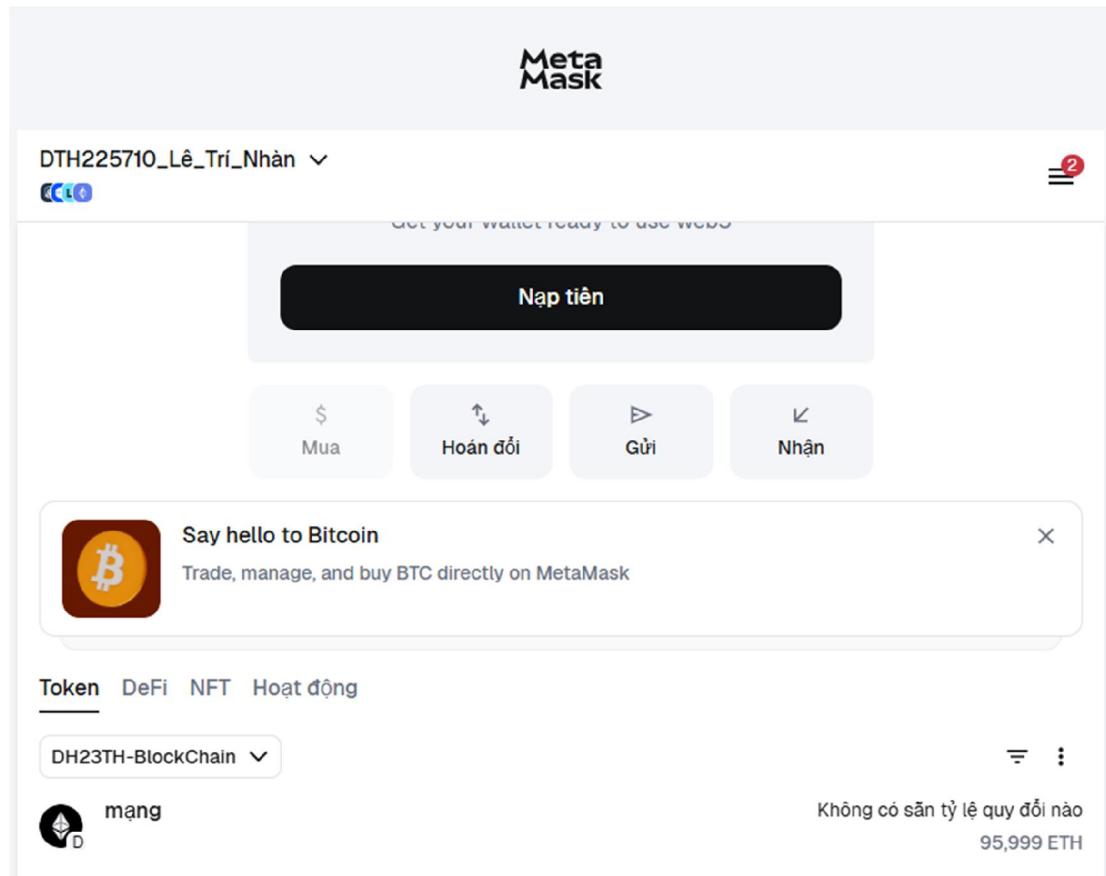


Figure 1. trước khi thực hiện giao dịch

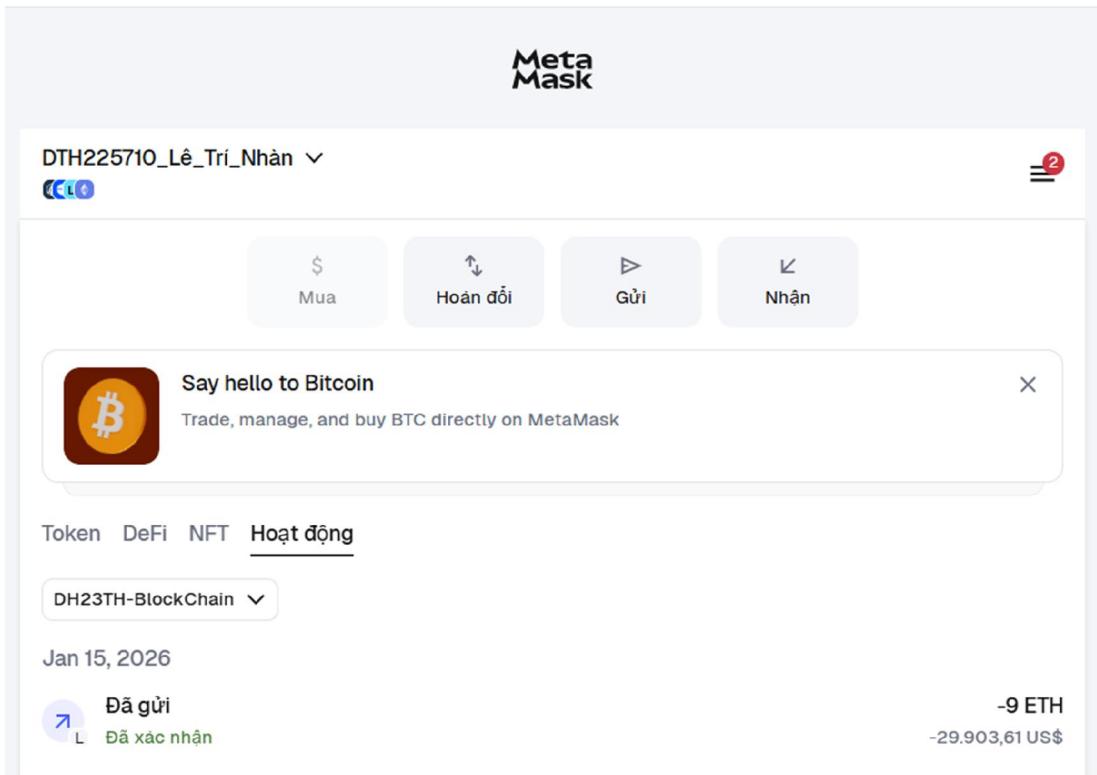


Figure 2. giao dịch thành công

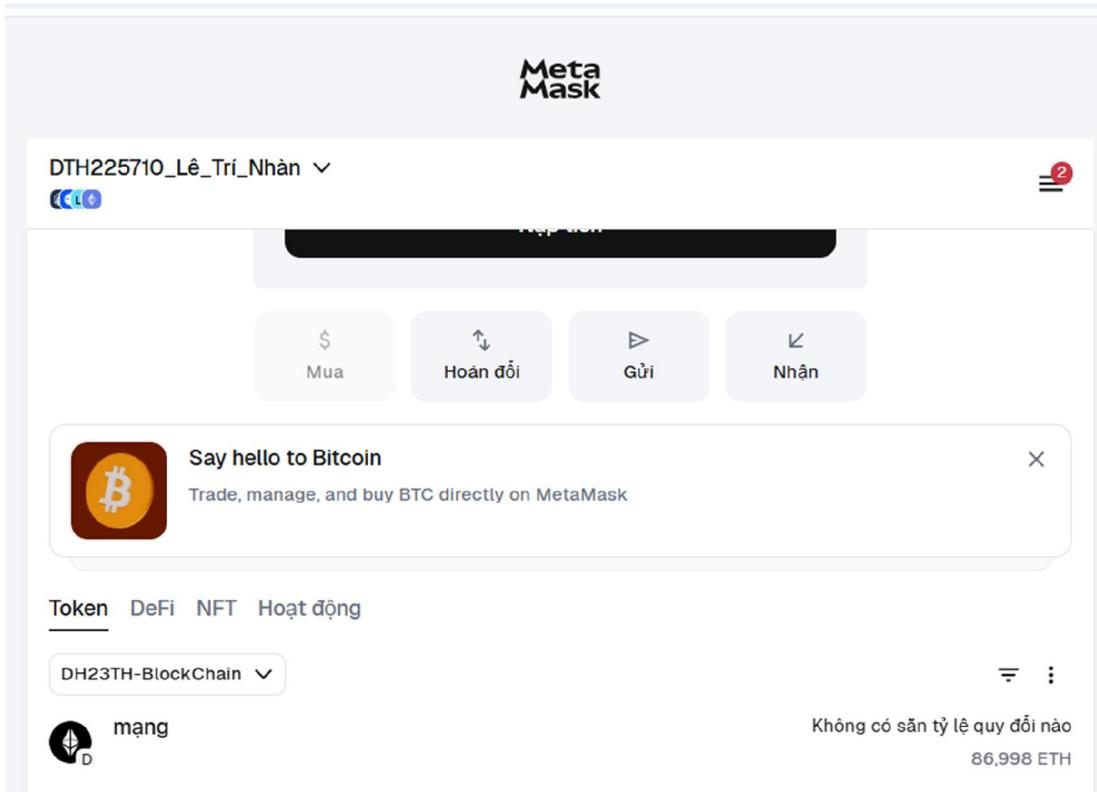


Figure 3. Kết quả sau khi thực hiện giao dịch thành công

3. HÀM BĂM 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:	a0516fdbacf11129a6e6fb693feac714bb1db981fcfee17ef64549c09cac30e

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

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 1</td></tr> <tr><td>Nonce:</td><td>10651</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 → Anders</td></tr> <tr><td>Tx:</td><td></td></tr> <tr><td>Prev:</td><td>0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0</td></tr> <tr><td>Hash:</td><td>0000baea5b2a60f9a5fa5535438d97c672a15494fcba517064d931</td></tr> </table> <p>Mine</p>	Block:	# 1	Nonce:	10651	Coinbase:	\$ 100.00 → Anders	Tx:		Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0	Hash:	0000baea5b2a60f9a5fa5535438d97c672a15494fcba517064d931	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 2</td></tr> <tr><td>Nonce:</td><td>215458</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 → Anders</td></tr> <tr><td>Tx:</td><td>\$ 10.00 From: Anders → Sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison</td></tr> <tr><td>Prev:</td><td>0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0</td></tr> <tr><td>Hash:</td><td>0000baea5b2a60f9a5fa5535438d97c672a15494fcba517064d931</td></tr> </table> <p>Mine</p>	Block:	# 2	Nonce:	215458	Coinbase:	\$ 100.00 → Anders	Tx:	\$ 10.00 From: Anders → Sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison	Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0	Hash:	0000baea5b2a60f9a5fa5535438d97c672a15494fcba517064d931	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 3</td></tr> <tr><td>Nonce:</td><td>146</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 → A</td></tr> <tr><td>Tx:</td><td>\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace</td></tr> <tr><td>Prev:</td><td>0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0</td></tr> <tr><td>Hash:</td><td>0000df1d632d734f5a5fc126a0fe8894fb4</td></tr> </table> <p>Mine</p>	Block:	# 3	Nonce:	146	Coinbase:	\$ 100.00 → A	Tx:	\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace	Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0	Hash:	0000df1d632d734f5a5fc126a0fe8894fb4
Block:	# 1																																					
Nonce:	10651																																					
Coinbase:	\$ 100.00 → Anders																																					
Tx:																																						
Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0																																					
Hash:	0000baea5b2a60f9a5fa5535438d97c672a15494fcba517064d931																																					
Block:	# 2																																					
Nonce:	215458																																					
Coinbase:	\$ 100.00 → Anders																																					
Tx:	\$ 10.00 From: Anders → Sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison																																					
Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0																																					
Hash:	0000baea5b2a60f9a5fa5535438d97c672a15494fcba517064d931																																					
Block:	# 3																																					
Nonce:	146																																					
Coinbase:	\$ 100.00 → A																																					
Tx:	\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace																																					
Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0																																					
Hash:	0000df1d632d734f5a5fc126a0fe8894fb4																																					

- Dữ liệu ban đầu hoàn toàn không có xung đột

Coinbase Transactions

Peer A

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 2</td></tr> <tr><td>Nonce:</td><td>215458</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 → Anders</td></tr> <tr><td>Tx:</td><td>\$ 50.00 From: Anders → sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison</td></tr> <tr><td>Prev:</td><td>0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0</td></tr> <tr><td>Hash:</td><td>8050d9f6a09bf1ba00c9cae2a97dbe69f7e06646e72671e88fea69974</td></tr> </table> <p>Mine</p>	Block:	# 2	Nonce:	215458	Coinbase:	\$ 100.00 → Anders	Tx:	\$ 50.00 From: Anders → sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison	Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0	Hash:	8050d9f6a09bf1ba00c9cae2a97dbe69f7e06646e72671e88fea69974	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 3</td></tr> <tr><td>Nonce:</td><td>146</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 → Anders</td></tr> <tr><td>Tx:</td><td>\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace</td></tr> <tr><td>Prev:</td><td>8d50d9f6033bf1ba00c9cae2a97dbe69f7e06646e72671e88fea69974</td></tr> <tr><td>Hash:</td><td>2dc436bb5c7e2d52c734d84b8d72d46065430493437952d983faae6</td></tr> </table> <p>Mine</p>	Block:	# 3	Nonce:	146	Coinbase:	\$ 100.00 → Anders	Tx:	\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace	Prev:	8d50d9f6033bf1ba00c9cae2a97dbe69f7e06646e72671e88fea69974	Hash:	2dc436bb5c7e2d52c734d84b8d72d46065430493437952d983faae6	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 4</td></tr> <tr><td>Nonce:</td><td>18292</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 →</td></tr> <tr><td>Tx:</td><td>\$ 15.00 From: Jackson \$ 5.00 From: Emily \$ 8.00 From: Sophia</td></tr> <tr><td>Prev:</td><td>2dc436bb5c7e2d52c734d84b8d72d46065430493437952d983faae6</td></tr> <tr><td>Hash:</td><td>See1029ac669c7c3955ddd90dd15c37</td></tr> </table> <p>Mine</p>	Block:	# 4	Nonce:	18292	Coinbase:	\$ 100.00 →	Tx:	\$ 15.00 From: Jackson \$ 5.00 From: Emily \$ 8.00 From: Sophia	Prev:	2dc436bb5c7e2d52c734d84b8d72d46065430493437952d983faae6	Hash:	See1029ac669c7c3955ddd90dd15c37
Block:	# 2																																					
Nonce:	215458																																					
Coinbase:	\$ 100.00 → Anders																																					
Tx:	\$ 50.00 From: Anders → sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison																																					
Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0																																					
Hash:	8050d9f6a09bf1ba00c9cae2a97dbe69f7e06646e72671e88fea69974																																					
Block:	# 3																																					
Nonce:	146																																					
Coinbase:	\$ 100.00 → Anders																																					
Tx:	\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace																																					
Prev:	8d50d9f6033bf1ba00c9cae2a97dbe69f7e06646e72671e88fea69974																																					
Hash:	2dc436bb5c7e2d52c734d84b8d72d46065430493437952d983faae6																																					
Block:	# 4																																					
Nonce:	18292																																					
Coinbase:	\$ 100.00 →																																					
Tx:	\$ 15.00 From: Jackson \$ 5.00 From: Emily \$ 8.00 From: Sophia																																					
Prev:	2dc436bb5c7e2d52c734d84b8d72d46065430493437952d983faae6																																					
Hash:	See1029ac669c7c3955ddd90dd15c37																																					

- 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

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 2</td></tr> <tr><td>Nonce:</td><td>62287</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 → Anders</td></tr> <tr><td>Tx:</td><td>\$ 50.00 From: Anders → Sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison</td></tr> <tr><td>Prev:</td><td>0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0</td></tr> <tr><td>Hash:</td><td>00005dbbfe5f34b78902c043348bd9c7c99c5e82de1d9d098a1c0d17</td></tr> </table> <p>Mine</p>	Block:	# 2	Nonce:	62287	Coinbase:	\$ 100.00 → Anders	Tx:	\$ 50.00 From: Anders → Sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison	Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0	Hash:	00005dbbfe5f34b78902c043348bd9c7c99c5e82de1d9d098a1c0d17	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 3</td></tr> <tr><td>Nonce:</td><td>15380</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 → Anders</td></tr> <tr><td>Tx:</td><td>\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace</td></tr> <tr><td>Prev:</td><td>00005dbbfe5f34b78902c043348bd9c7c99c5e82de1d9d098a1c0d17</td></tr> <tr><td>Hash:</td><td>000065cda61519d0efffb75e5c675b264c-e811e17f1a43ff450bf</td></tr> </table> <p>Mine</p>	Block:	# 3	Nonce:	15380	Coinbase:	\$ 100.00 → Anders	Tx:	\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace	Prev:	00005dbbfe5f34b78902c043348bd9c7c99c5e82de1d9d098a1c0d17	Hash:	000065cda61519d0efffb75e5c675b264c-e811e17f1a43ff450bf	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Block:</td><td># 4</td></tr> <tr><td>Nonce:</td><td>18292</td></tr> <tr><td>Coinbase:</td><td>\$ 100.00 →</td></tr> <tr><td>Tx:</td><td>\$ 15.00 From: Jackson \$ 5.00 From: Emily \$ 8.00 From: Sophia</td></tr> <tr><td>Prev:</td><td>000065cda61519d0efffb75e5c675b264c-e811e17f1a43ff450bf</td></tr> <tr><td>Hash:</td><td>951774d50533169a7d61765c61ea2t</td></tr> </table> <p>Mine</p>	Block:	# 4	Nonce:	18292	Coinbase:	\$ 100.00 →	Tx:	\$ 15.00 From: Jackson \$ 5.00 From: Emily \$ 8.00 From: Sophia	Prev:	000065cda61519d0efffb75e5c675b264c-e811e17f1a43ff450bf	Hash:	951774d50533169a7d61765c61ea2t
Block:	# 2																																					
Nonce:	62287																																					
Coinbase:	\$ 100.00 → Anders																																					
Tx:	\$ 50.00 From: Anders → Sophia \$ 20.00 From: Anders → Lucas \$ 15.00 From: Anders → Emily \$ 15.00 From: Anders → Madison																																					
Prev:	0000438d7625b06a6f366545b1929975a0d3ff1f8847e56cc587cadd0																																					
Hash:	00005dbbfe5f34b78902c043348bd9c7c99c5e82de1d9d098a1c0d17																																					
Block:	# 3																																					
Nonce:	15380																																					
Coinbase:	\$ 100.00 → Anders																																					
Tx:	\$ 10.00 From: Emily → Jackson \$ 5.00 From: Madison → Jackson \$ 20.00 From: Lucas → Grace																																					
Prev:	00005dbbfe5f34b78902c043348bd9c7c99c5e82de1d9d098a1c0d17																																					
Hash:	000065cda61519d0efffb75e5c675b264c-e811e17f1a43ff450bf																																					
Block:	# 4																																					
Nonce:	18292																																					
Coinbase:	\$ 100.00 →																																					
Tx:	\$ 15.00 From: Jackson \$ 5.00 From: Emily \$ 8.00 From: Sophia																																					
Prev:	000065cda61519d0efffb75e5c675b264c-e811e17f1a43ff450bf																																					
Hash:	951774d50533169a7d61765c61ea2t																																					

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