

Tìm hiểu nền tảng Ethereum blockchain

Nguyễn Hồng Đăng 20160988

Bùi Xuân Thái 20163671

Chu Duy Tưởng 20164584

Giao dịch

Giao dịch truyền thống

- Gặp mặt trực tiếp
- Tiền mặt



-> Tiền điện tử: Bitcoin, Ethereum
-> Blockchain

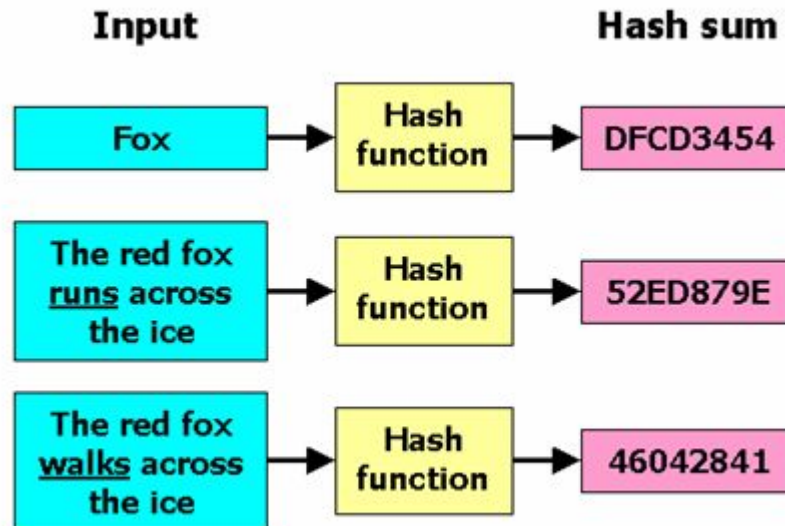
Giao dịch điện tử

- Internet, website
- Ví điện tử



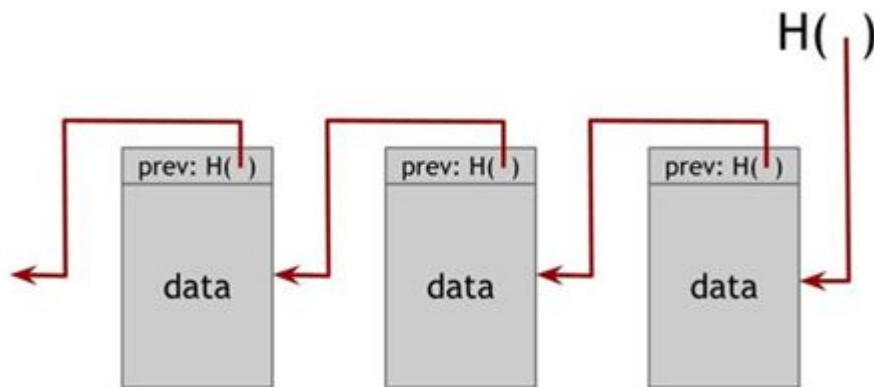
Hàm băm mật mã

- Hàm băm $H()$
- Hàm băm mật mã
 - Chống đụng độ
 $x \# y \rightarrow H(x) \# H(y)$
 - Che dấu một chiều
 $H(x)=y \rightarrow x=?$
 - Puzzle-friendliness
 $z, r \rightarrow ? H(r||x)=z$

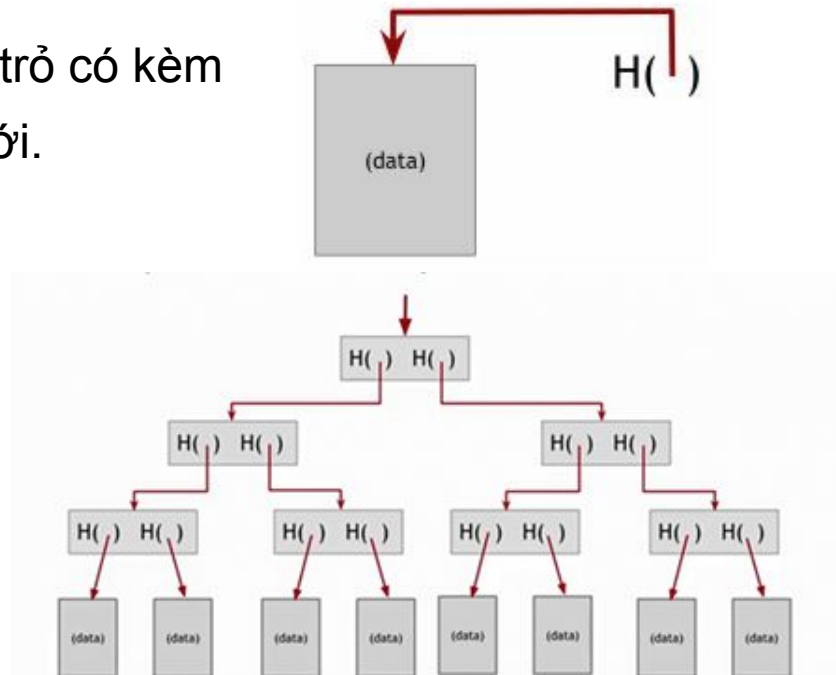


Hash Pointer

- Con trỏ hash (Hash pointers) là một con trỏ có kèm theo giá trị hash của nội dung được trỏ tới.



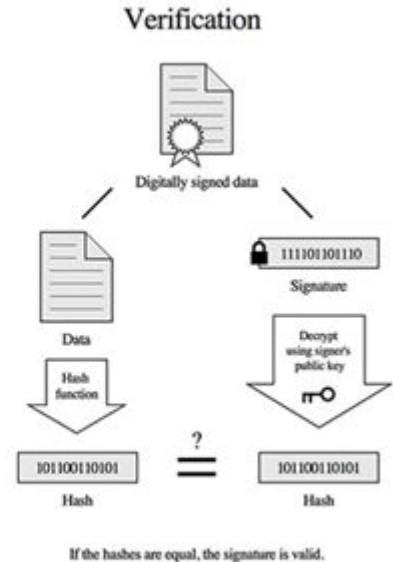
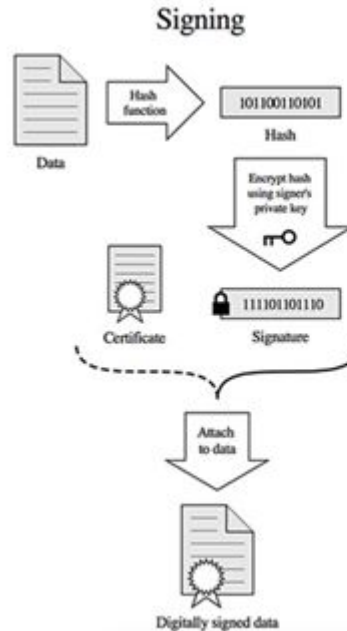
Linked List



Merkle Trees

Digital Signatures

- Public Key - Private Key
- DS
 - Non-repudiation
 - Integrity
 - Authenticity
- Signing / Verification



Bitcoin

Tiền điện tử trước khi Bitcoin ra đời:

- Chủ yếu là các nghiên cứu
- Chưa có sản phẩm thực tế nào thực sự thành công
- B-money, Bit Gold,...

Bitcoin

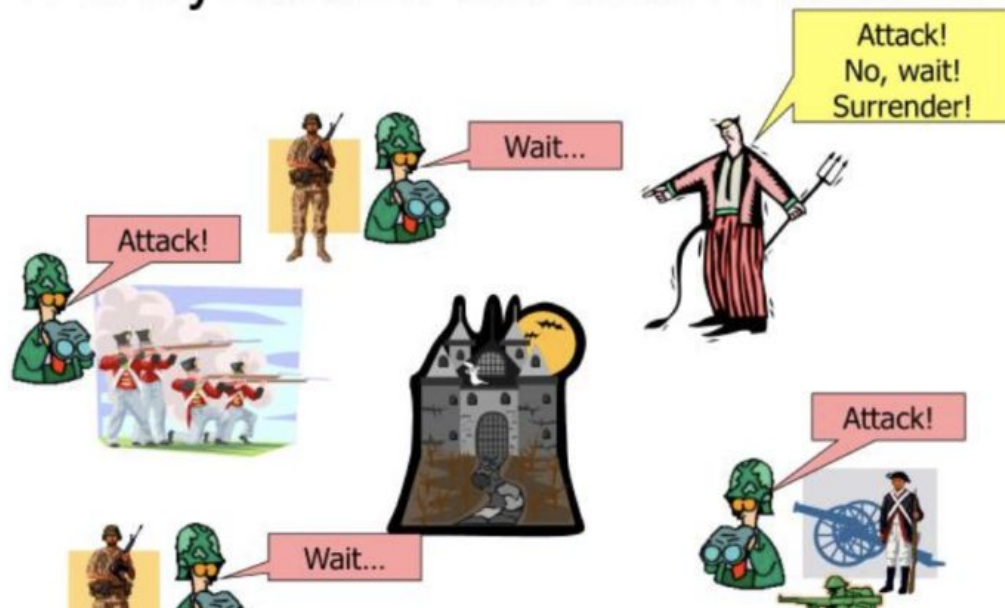
- Có thể coi là đồng tiền điện tử đầu tiên
- Sử dụng công nghệ mã hóa
- Khả năng chống gian lận mạnh mẽ
- Hệ thống tài chính phi tập trung
- Là cảm hứng, nền tảng cho hàng loạt đồng tiền điện tử khác ra đời sau đó

Lịch sử Bitcoin

- 31/10/2008: Satoshi Nakamoto xuất bản “Bitcoin: A peer to peer electronic cash system”
- 3/1/2009: Block đầu tiên được khai thác bởi chính Satoshi Nakamoto
- 2/5/2010: Giao dịch đầu tiên sử dụng BTC
- 3/2010: Bitcoinmarket.com ra đời, sau đó là Mt.Gox
- 2011-2013: Giá trị của đồng BTC ngang với giá của dollar Mỹ
- 2011: Mt.Gox bị hack mất 2000 BTC tương đương 30.000 dollar Mỹ
- 2014: Mt.Gox bị hack mất 850.000 BTC tương đương 460.000.000 dollar Mỹ
- 2014-2016: Giá BTC giảm mất 50%
- 2016 đến nay: Giá BTC tăng trở lại và có giá trị rất cao

Cơ chế đồng thuận

The Byzantine Generals Problem



Cơ chế đồng thuận

- Tính phi tập trung trong mạng blockchain
- Thống nhất trạng thái của sổ cái



Cơ chế đồng thuận

Cơ chế đồng thuận

- Proof of work
- Practical Byzantine fault tolerance
- Proof of stake
- Proof of burn
- Proof of capacity

Proof of work

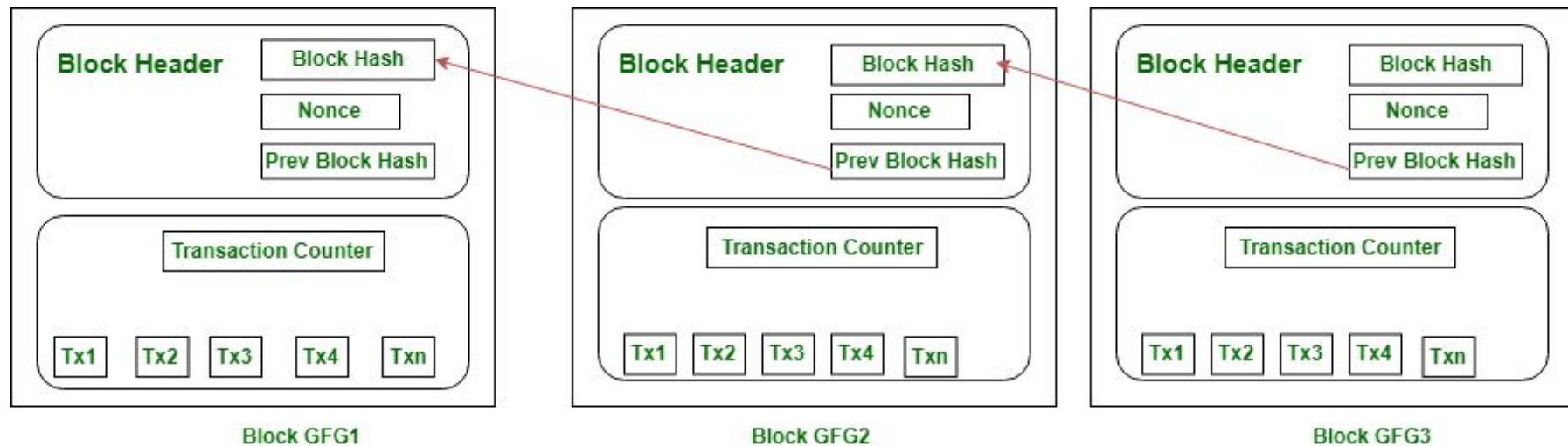
Các vấn đề được đặt ra:

1. Node nào có được block reward tiếp theo
2. Tránh cung cấp dịch vụ một cách miễn phí
3. Bảo vệ khỏi sybil attack



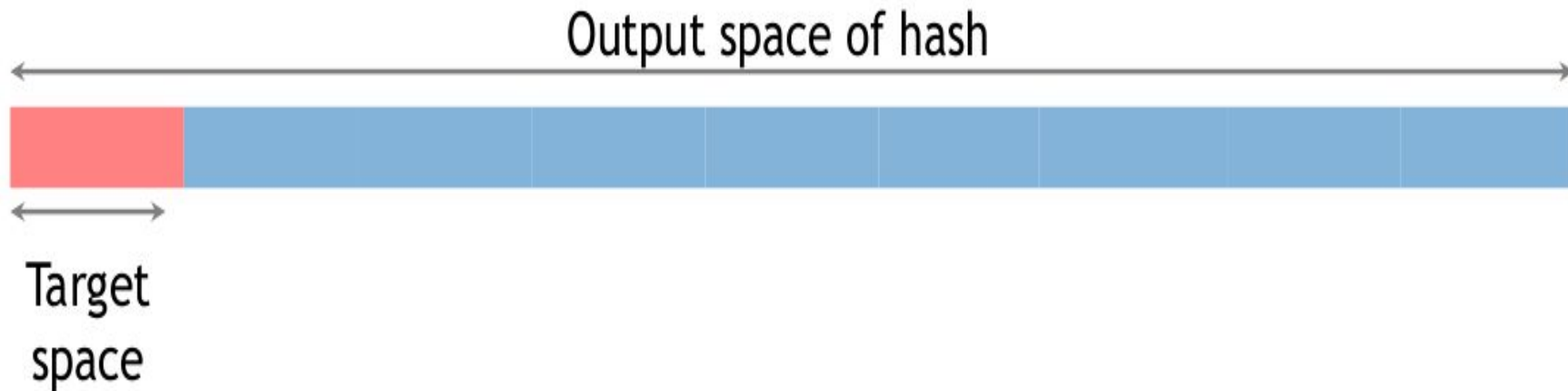
Proof of work

Proof of work



Proof of work

- Tìm nonce để hash của block thỏa mãn trường target space



Proof of work

Tính chất:

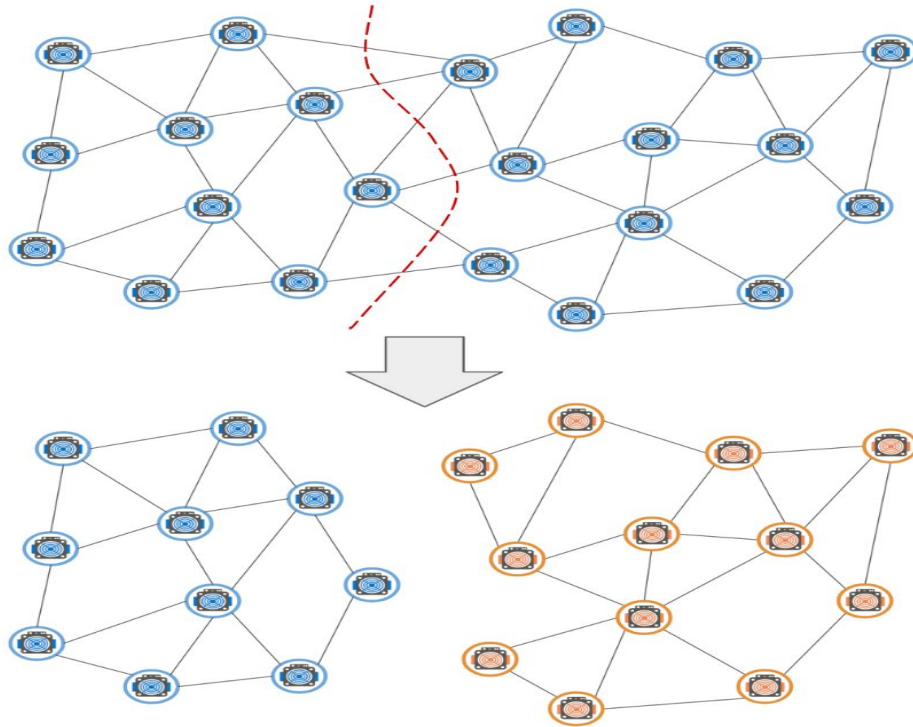
- Mức độ tính toán khó
- Tham số hóa chi phí
- Chi phí kiểm chứng không đáng kể

Proof of work

Vấn đề:

- Nguy cơ tấn công 51%
- Tiêu tốn thời gian
- Tiêu tốn tài nguyên
- Thời gian xác thực giao dịch khoảng 10 đến 60 phút

51% attack



Ethereum

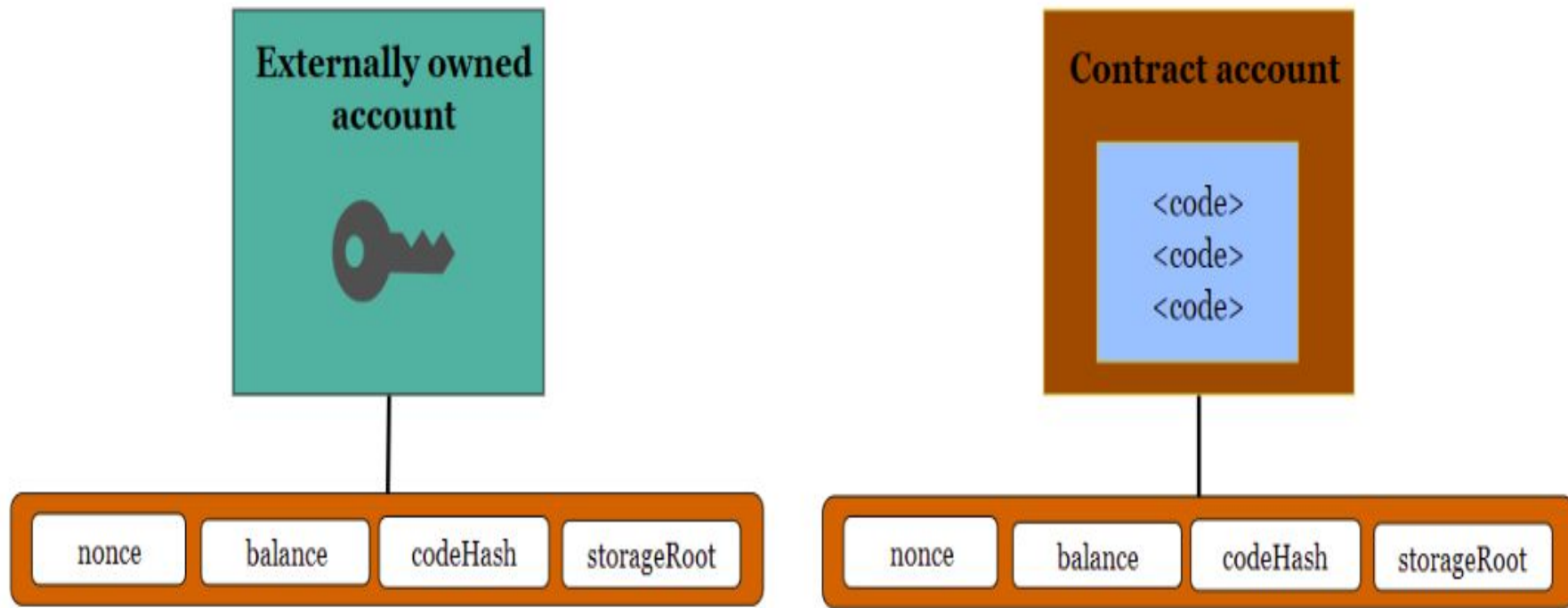
Định nghĩa:

1. Mạng blockchain
2. Nền tảng xây dựng các ứng dụng phi tập trung
3. Đồng tiền ETH
4. Smart contract

Bitcoin vs Ethereum

Bitcoin	Ethereum
A currency	A token
Ethash	Secure hash alg, SHA256
Stack-based language	Turning complete
10-60 minutes for confirmation	10-20 seconds for confirmation
Deflationary	Inflationary

Account Ethereum



Transaction

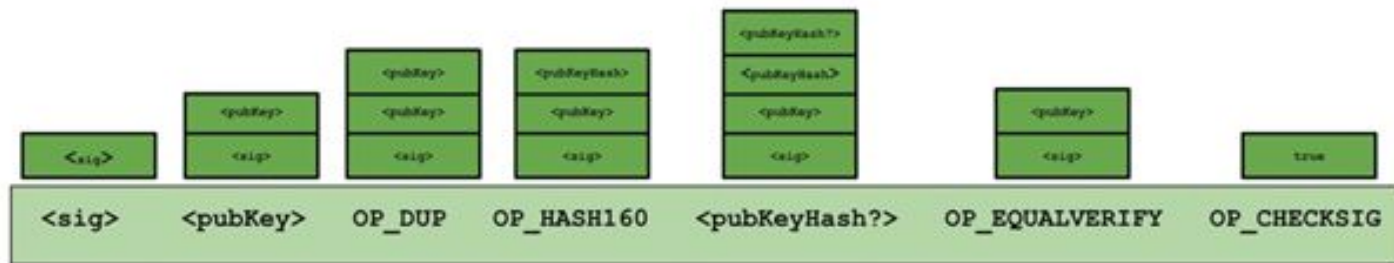
1. Tài khoản nhận
2. Chữ kí người gửi
3. Số ETH gửi
4. Trường dữ liệu tùy chọn
5. STARTGAS
6. GASPRICE

Message

1. Tài khoản nhận
2. Chữ kí người gửi
3. Số ETH gửi
4. Trường dữ liệu tùy chọn
5. STARTGAS

Bitcoin script

- ❖ Giao thức trong Bitcoin tạo điều kiện để tạo một số phiên bản đơn giản, thu nhỏ của một smart contract thông qua khái niệm Bitcoin script.
- ❖ Đơn giản, Turing-incomplete, dựa trên stack.

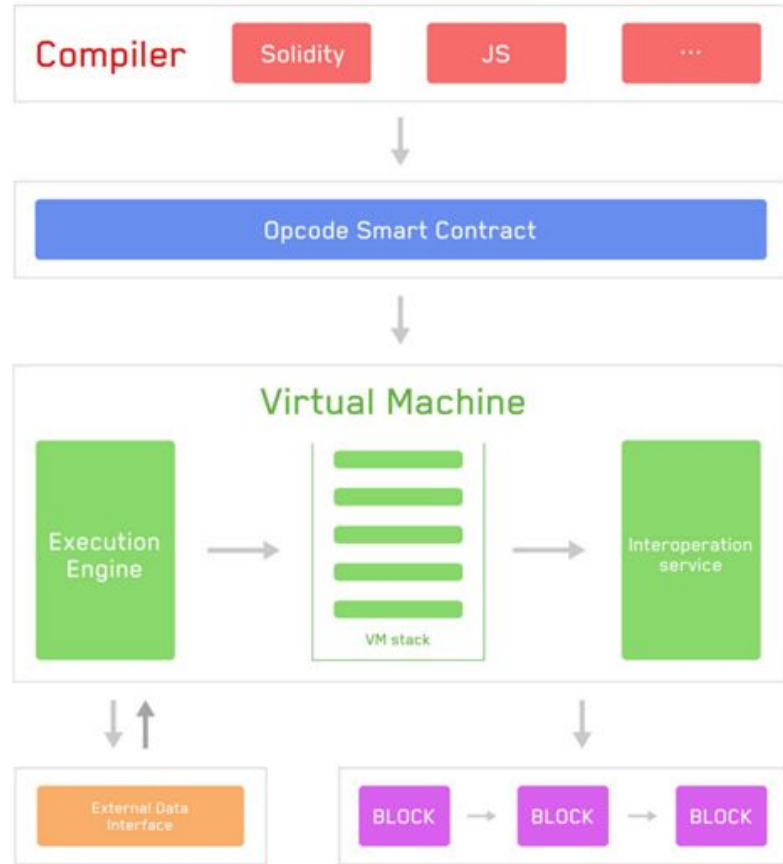


Ethereum

- ❑ Giải pháp thay thế/mở rộng Bitcoin
- ❑ Dễ dàng phát triển các ứng dụng phân tán, hợp đồng thông minh
- ❑ Đảm bảo tính đơn giản, lightweight cho client
- ❑ Chia sẻ với môi trường kinh tế, tiền điện tử nhờ ưu điểm của công nghệ blockchain

Ethereum










- ❑ Turing-complete
- ❑ Opcode chạy trên máy ảo EVM
- ❑ Phát triển smart contract đơn giản, nhanh chóng
 - Solidity
 - Vyper



ETH

- ❑ 1: wei
- ❑ 10¹² : szabo
- ❑ 10¹⁵ : finney
- ❑ 10¹⁸ : ether

Các Loại Tiền Điện Tử Hàng Đầu »

Tên :	Ký hiệu :	Giá (USD)
 Bitcoin	BTC	8,091.0
 Ethereum	ETH	143.28
 Ripple	XRP	0.21065
 Bitcoin Cash	BCH	262.95
 Tether	USDT	1.0014
 Litecoin	LTC	49.417
 Bitcoin SV	BSV	164.05
 EOS	EOS	3.0935
 Binance Coin	BNB	15.0248
 Monero	XMR	57.780

Smart contract

Hợp đồng thông minh (smart contract) cần thỏa mãn 3 tính chất:

- ❑ Tính tất định (Deterministic)
- ❑ Tính khả dừng (Terminable)
- ❑ Tính cô lập (Isolated)

Virtual machine vs Docker

	Virtual Machines	Docker
Deterministic	The contracts have no un-deterministic functions and the data is limited to on-chain information only. However, it executes dynamic calls which can be un-deterministic in nature. Thankfully the data accessible is deterministic	Because of the design of the docker, the system is reliant on users to create contracts which are deterministic. That is not really the best of solutions.
Terminable	Ethereum uses the "Fee-meter" for termination. Every step in the contracts costs "gas" and once the gas cost exceeds the pre-paid fee, the contract is killed.	Fabric uses the timer. However, since the timer can change from node to node because each node has its own computational power there is a risk to the consensus process.
Isolated	Has good isolation properties.	Is namespace-reliant and not capable of proper isolation

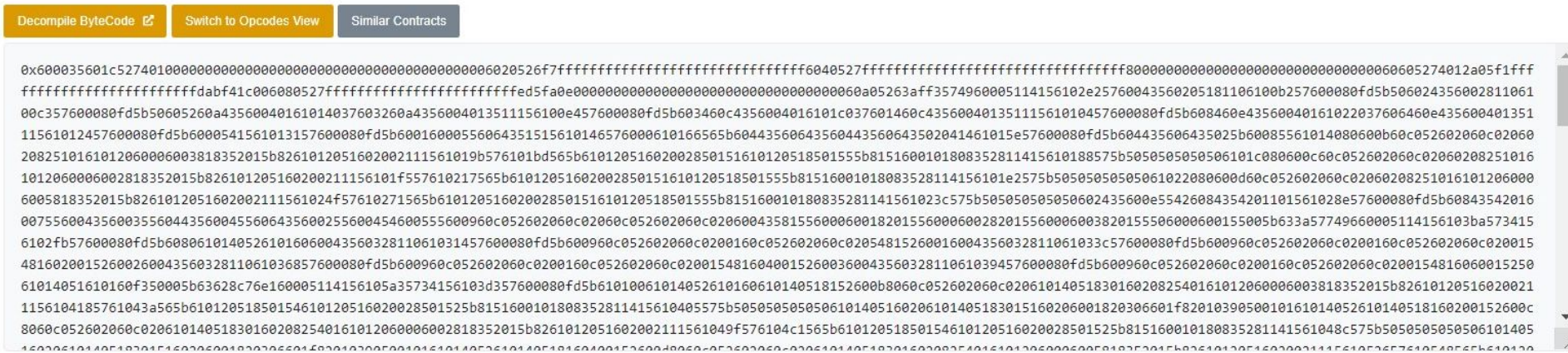
Ethereum Virtual Machine (EVM)

- ❖ Virtual Machine, runtime environment
- ❖ Stack base
- ❖ Turing - complete
- ❖ Được triển khai thành công bằng nhiều ngôn ngữ lập trình khác nhau bao gồm C++, Java, JavaScript, Python, Ruby và nhiều ngôn ngữ khác
- ❖ Bất kì ai cũng có thể cài EVM và tham gia vào hệ sinh thái không tin cậy

Code execution

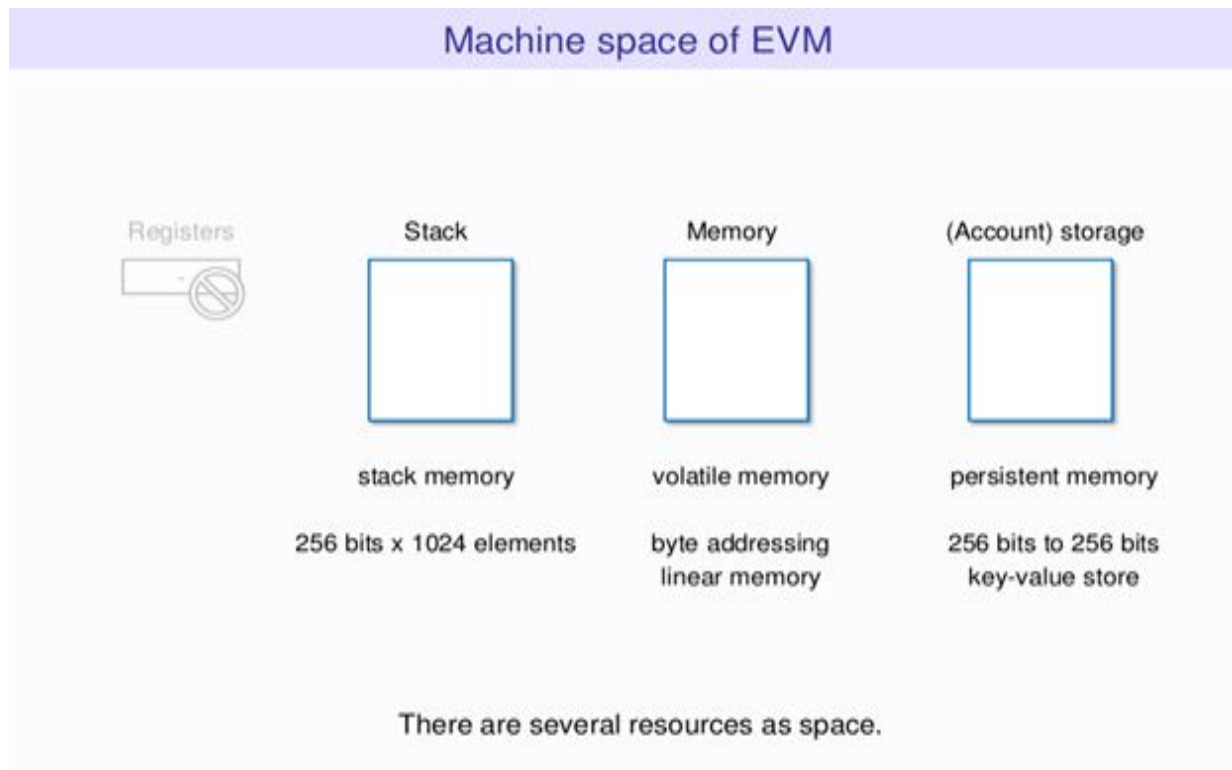
Mã lệnh trong các contract trên Ethereum được viết bằng ngôn ngữ bytecode dựa trên ngăn xếp, là ngôn ngữ bậc thấp.

Bao gồm một chuỗi các byte, trong đó mỗi byte đại diện cho một chỉ thị.



Bộ nhớ

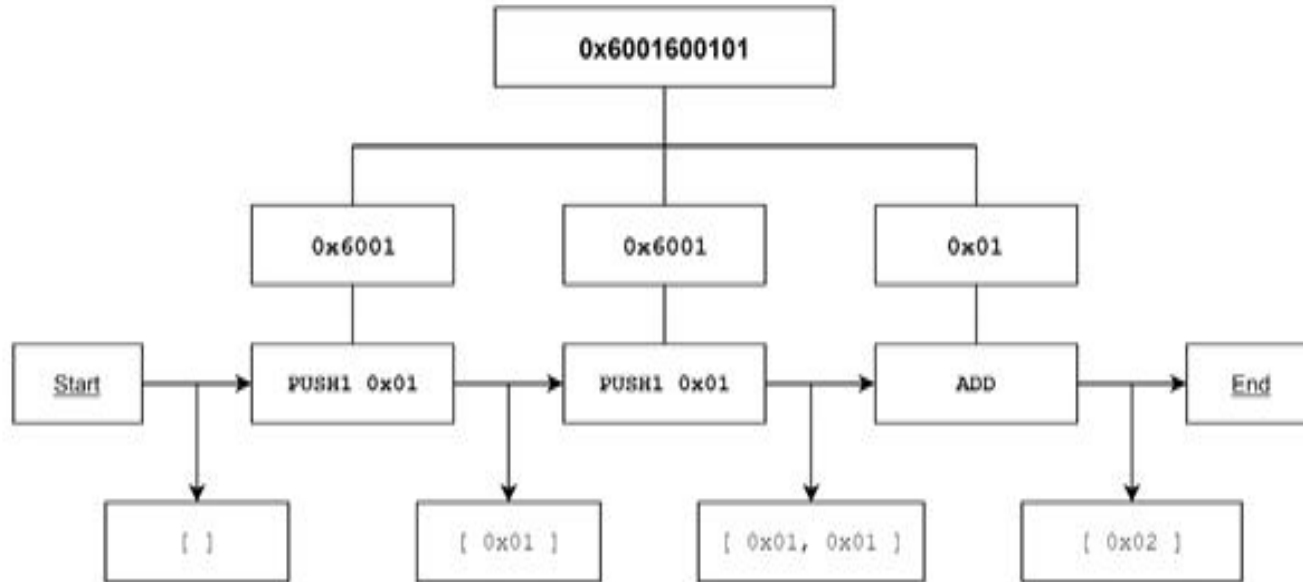
- ❑ Stack
- ❑ Memory
- ❑ Storage



Opcodes (140 uniques)

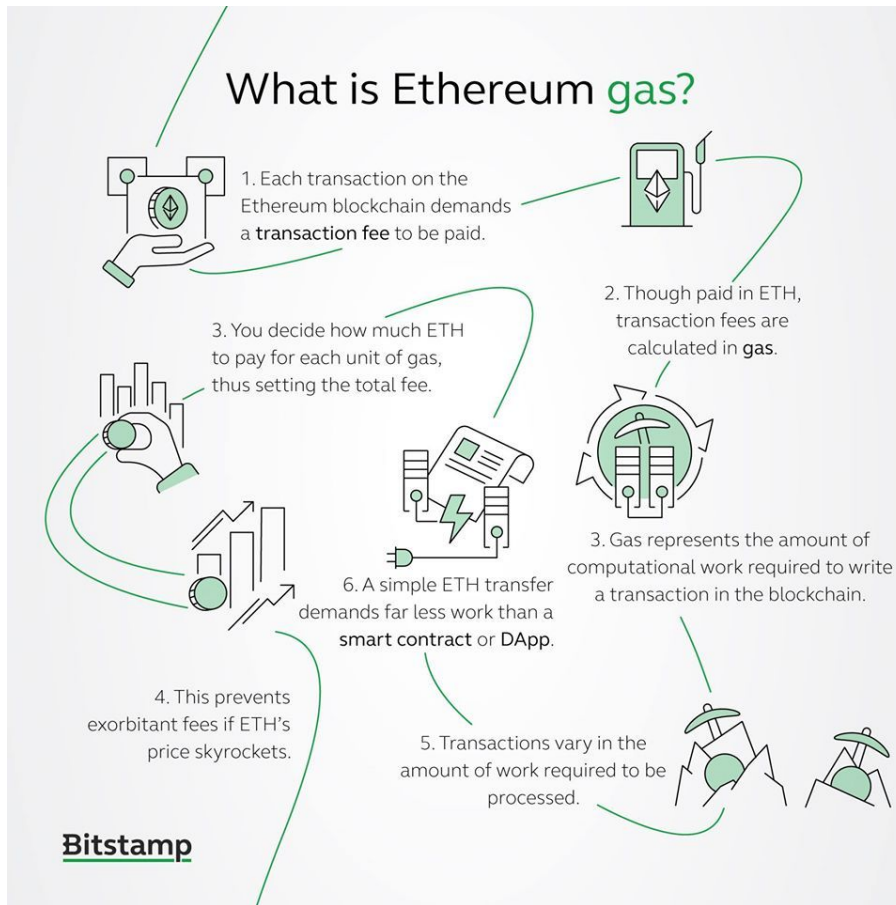
- Các opcode điều khiển ngăn xếp: POP, PUSH, DUP, SWAP
- Các opcode thực thi phép toán số học, bitwise, so sánh: ADD, SUB, GT, LT, AND, OR
- Các opcode môi trường: CALLER, CALLVALUE, NUMBER
- Các opcode điều khiển bộ nhớ: MLOAD, MSTORE, MSTORE8, MSIZE
- Các opcode điều khiển bộ nhớ dài hạn: SLOAD, SSTORE
- Các opcode chuyển điều khiển: JUMP, JUMPI, PC, JUMPDEST
- Các opcode dừng thực thi: STOP, RETURN, REVERT, INVALID, SELFDESTRUCT

Bytecode



Ethereum Gas

Dự trữ một số ETH để có thể sẵn sàng trả phí cho việc thực thi mã trên các EVM tại các node trong mạng.



Ethereum Gas

- ❖ Ethereum Gas là đơn vị để đánh giá chi phí tính toán cần thiết để thực thi một số tác vụ (thường là dãy chỉ thị thực thi trong smart contract), trên máy ảo Ethereum (EVM).
- ❖ Mỗi thao tác, giao dịch diễn ra trên Ethereum đều cần thiết/tiêu tốn một số lượng Gas nhất định
- ❖ Các miner được trả lượng ether tương ứng với tổng số lượng Gas cần thiết để hoàn thành một thao tác.

Ethereum Gas

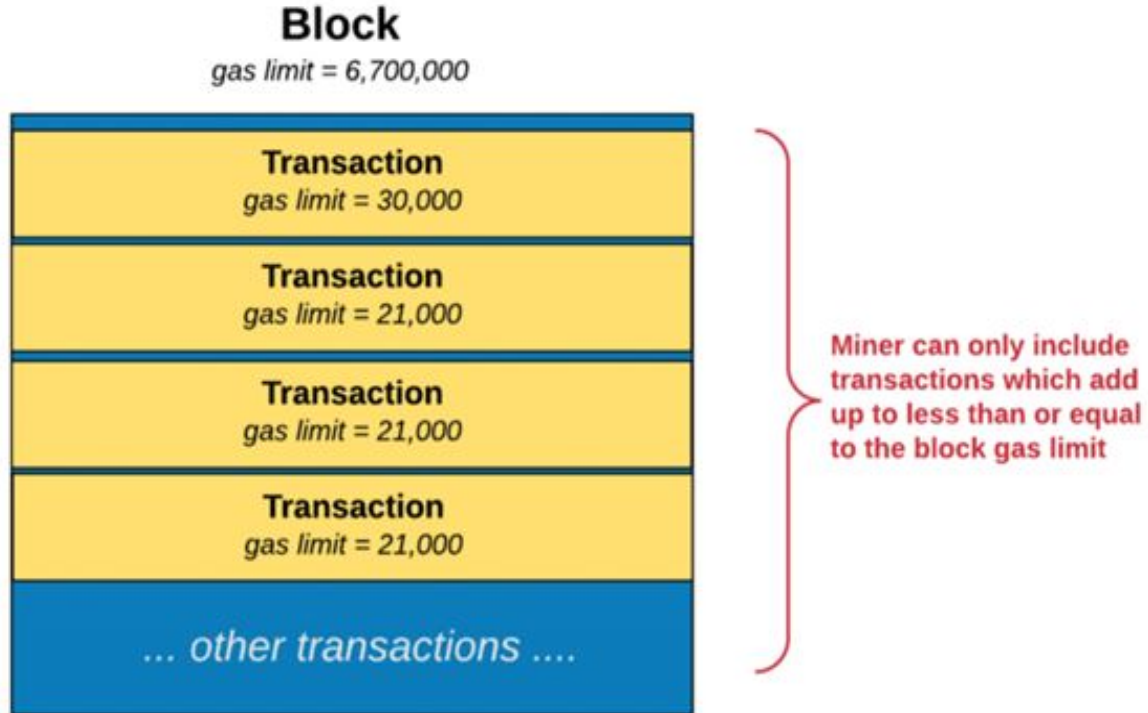
2 vấn đề chính được giải quyết:

- ❑ Những node có vai trò xác nhận các giao dịch(thường là full-node) được đảm bảo nhận được số tiền trả trước ban đầu (pre-paid), ngay cả khi việc thực thi không thành công (exception, hoặc gas cung cấp không đủ).
- ❑ Một dãy chỉ thị trong một contract không thể chạy với thời gian lâu hơn số tiền trả trước đã cung cấp cho phép. Việc thực thi sẽ chạy cho đến khi hết Gas, tránh các vòng lặp vô hạn.

Gas limit

- Chủ giao dịch phải chỉ định Gas limit trước khi họ gửi nó đến mạng. Gas limit là lượng gas tối đa mà người gửi sẵn sàng trả cho giao dịch đó.
- Đơn vị: gas
- Các giao dịch khác nhau sẽ có chi phí gas khác nhau
- Các miner sẽ ngừng thực hiện giao dịch tại thời điểm hết gas
- Nếu có bất kỳ gas dư sẽ được hoàn trả ngay lập tức cho chủ giao dịch

Gas limit



Gas price

- ❑ Chủ giao dịch có thể quyết định giá trị Gas price mà họ muốn sử dụng là bao nhiêu tùy ý
- ❑ Miner ưu tiên xác nhận các giao dịch mới giá trị Gas price cao nhất (có lợi nhất cho họ)
- ❑ $\text{Gas fees} = \text{Gas limit} * \text{Gas price}$

Recommended Gas Prices

(based on current network conditions)

Speed	Gas Price (gwei)
SafeLow (<30m)	2
Standard (<5m)	3
Fast (<2m)	14

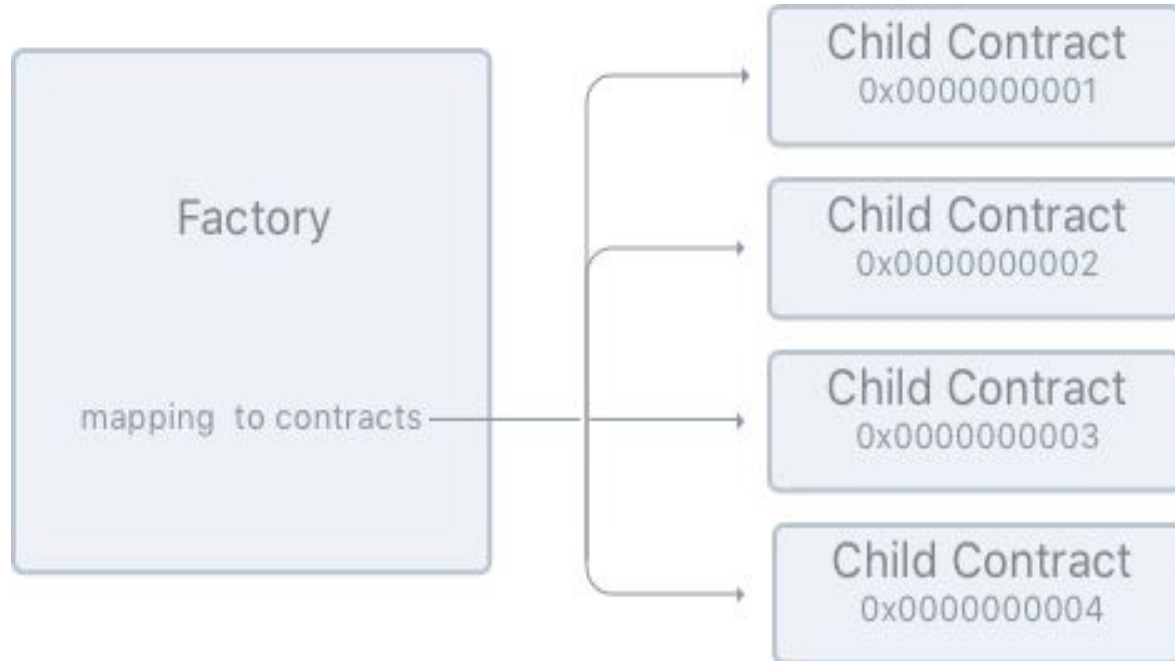
Smart contract

- Thường được viết bởi ngôn ngữ bậc cao: Solidity, Vyper
 - ❑ Solidity: Mạnh mẽ và thông dụng nhất hiện nay
 - ❑ Vyper: Thiên về tính an toàn bảo mật, dễ viết, dễ hiểu
- Trình biên dịch biên dịch từ ngôn ngữ bậc cao sang **Bytecode** và **ABI** để có thể deploy lên nền tảng Ethereum
- ABI: Application Binary Interface

Smart contract

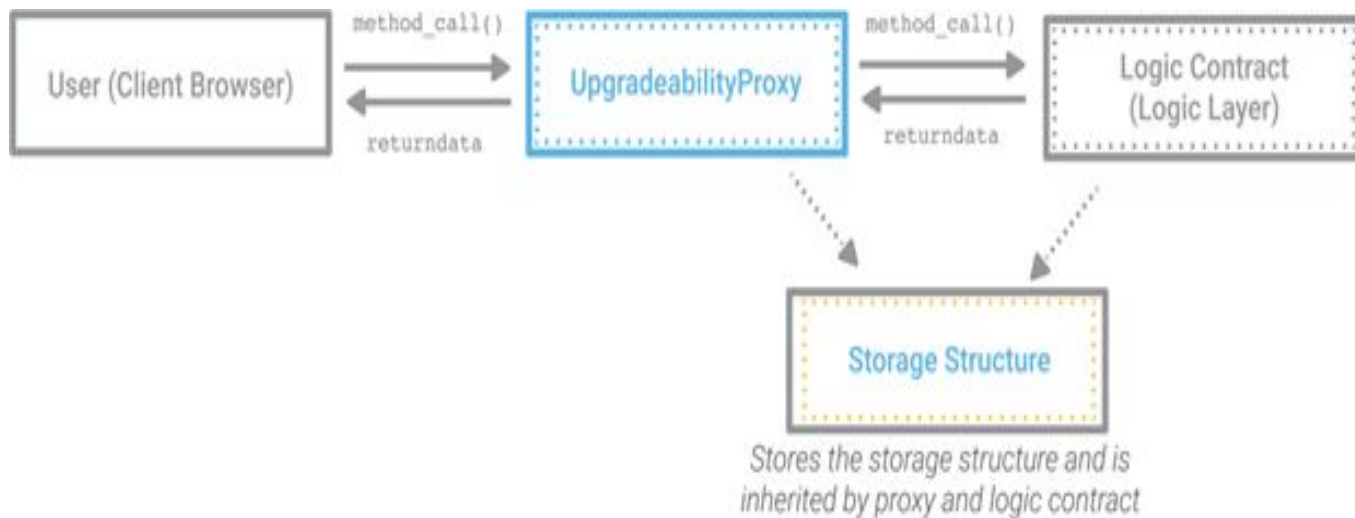
- Các biến trạng thái contract (storage) cần được khai báo và khởi tạo trước khi sử dụng
- Các hàm (function) có thể có các chỉ định truy cập khác nhau: private, public
- Event:
 - Cách thức mà contract giao tiếp với client khi có một sự kiện xảy ra trên blockchain, client lắng nghe event và gọi tới các callback function.
 - Cung cấp cơ chế index cho phép client sử dụng các bộ lọc (filter) để lọc các event quan tâm → Cơ chế đọc dữ liệu từ blockchain

Factory design pattern



Proxy design pattern

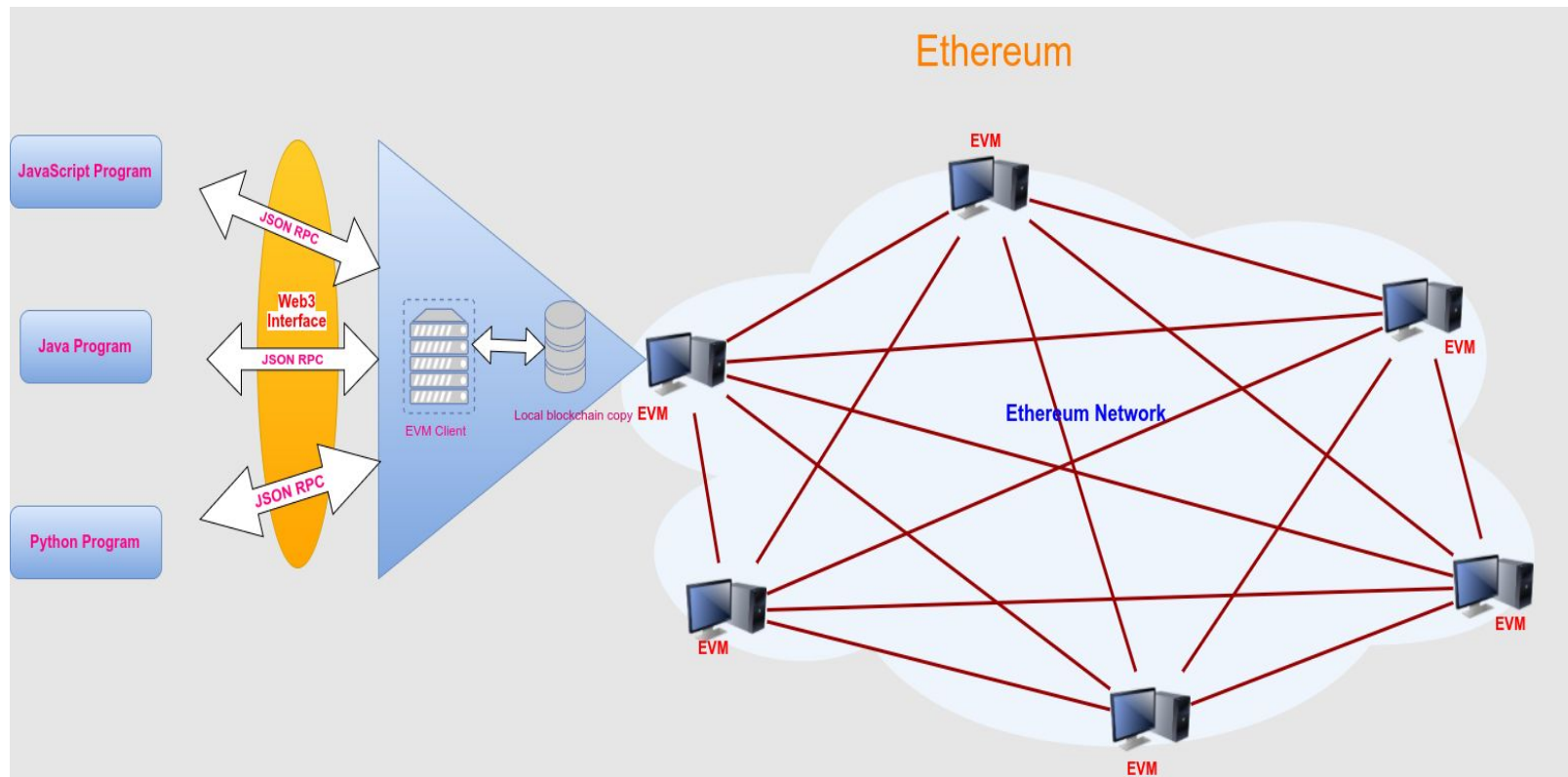
Ủy quyền, nhờ vào opcode DELEGATECALL



Web3

- Web3 nói chung là các công nghệ, thư viện được phát triển trên nhiều ngôn ngữ, ví dụ : **web3.py** cho Python, **web3.js** cho JavaScript, **web3j** cho Java
- Hỗ trợ phát triển các ứng dụng phân tán (Dapp – Decentralized application) ở phía client, giúp tương tác với máy ảo Ethereum cục bộ hoặc từ xa.
- Các thư viện này triển khai giao diện JSON-RPC client API, thông qua kết nối HTTP và IPC

Web3



Web3

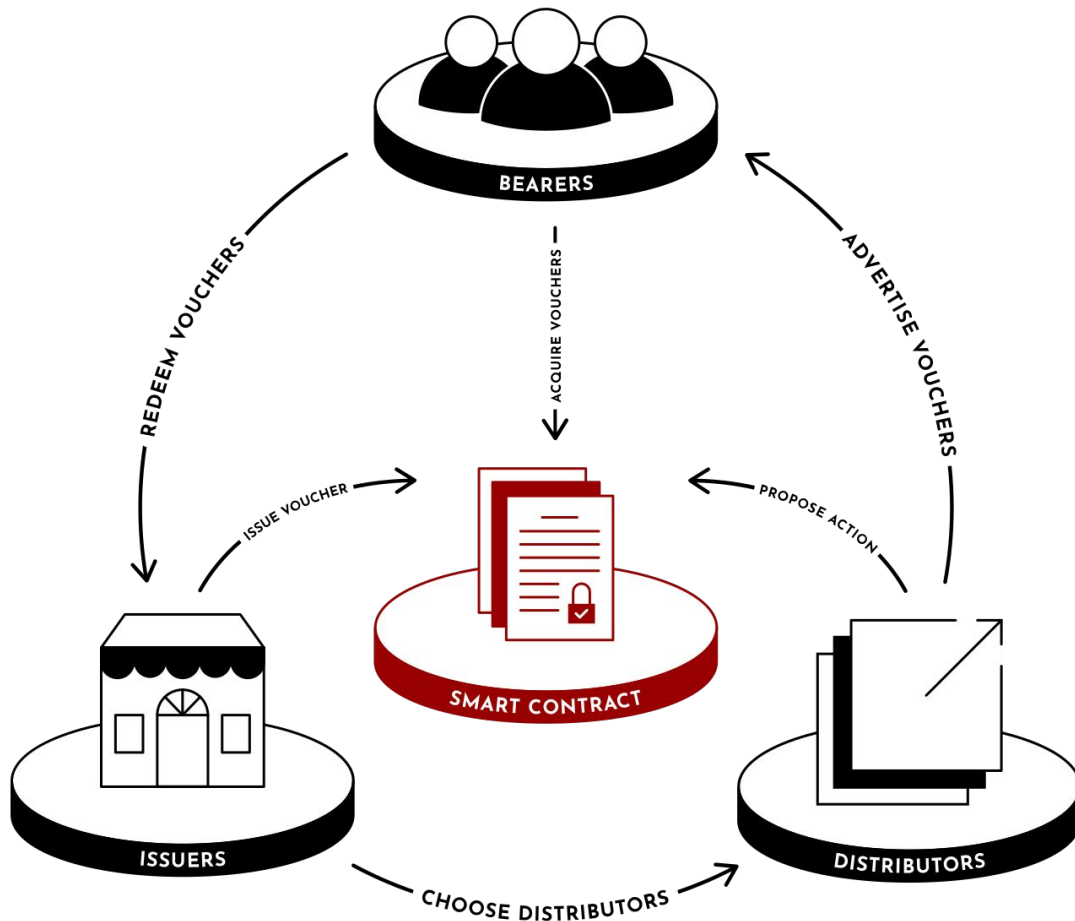
- Deploy contract mới
- Tạo, gửi các giao dịch đơn giản
- Tạo, gửi các giao dịch, lời gọi hàm tới contract
- Lắng nghe sự kiện (Event) xảy ra trên mạng
- Event filter, logging
- ...

Applications

- ❑ Token System
- ❑ Các công cụ tài chính phái sinh và tiền tệ ổn định
- ❑ Hệ thống định danh và xác thực
- ❑ Lưu trữ phi tập trung
- ❑ Các tổ chức tự trị phi tập trung

DEMO

Hệ thống phát hành mã giảm giá (coupon) trên nền tảng Ethereum

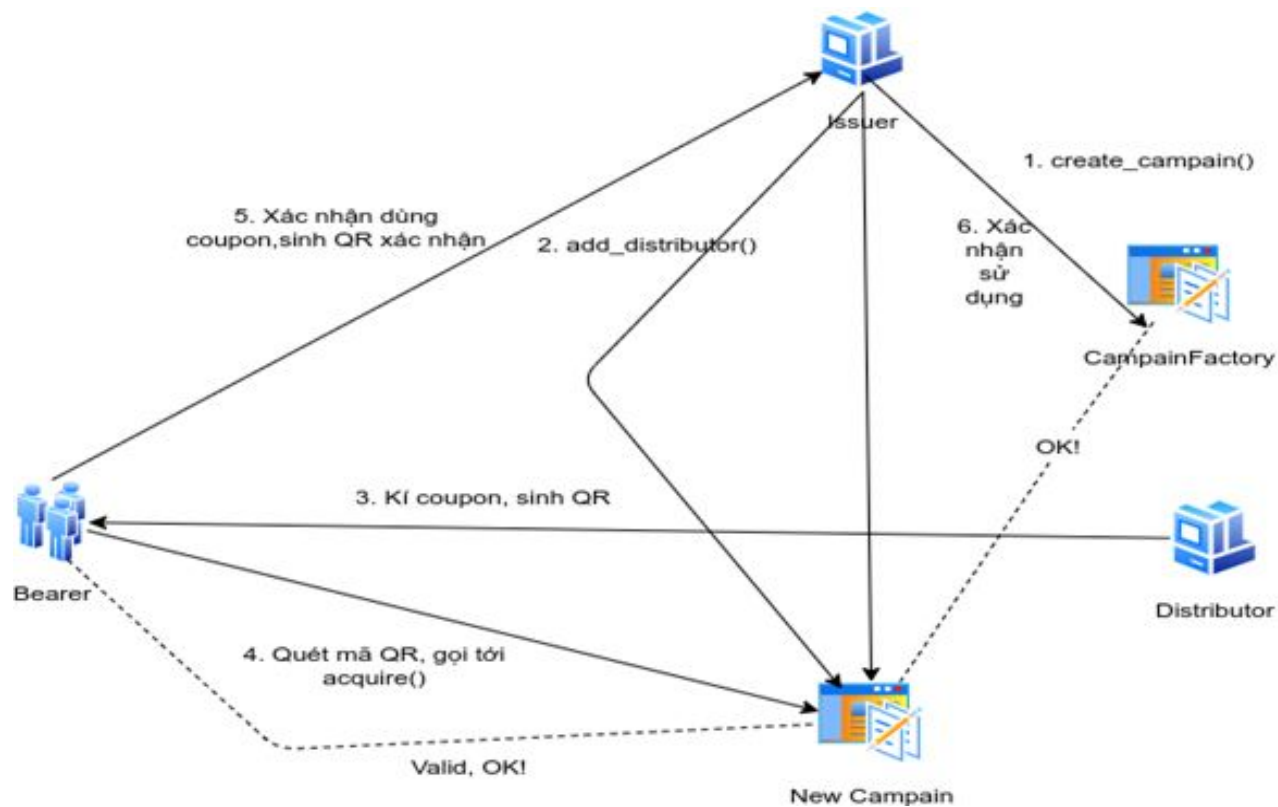


The Rouge Protocol
<https://rouge.network/>

Issuer, Distributor, Bearer

- ❑ Issuer là các nhà phát hành các mã giảm giá - coupons. Các coupons chỉ có hiệu lực khi được issuer chứng nhận hợp lệ
- ❑ Distributor là những nhà phân phối các mã giảm giá. Nói cách khác, họ là những người đưa coupons tới tay người dùng. Thông thường, họ là những cá nhân/ tổ chức có sức ảnh hưởng lớn, ví dụ như streamer, blogger, các trang web, .. Issuer phải trả phí (ETH) cho họ tùy theo số khách hàng được giới thiệu nhờ distributor đó.
- ❑ Bearer là những người dùng thông thường, muốn tìm những cơ hội giảm giá.

Kịch bản



Dapp

