Web3

Web1.0	Web2.0	Web3.0
READ-ONLY	READ-WRITE	READ-WRITE-OWN
- Các Website tĩnh sở hữu bởi các công ty, gần như không có sự tương tác giữa các người dùng, các nội dung hiếm khi được tạo bởi cá nhân	- Thay vì các công ty cung cấp nội dung cho người dùng, thì họ cung cấp nền tảng để chia sẻ nội dung được tạo ra bởi người dùng. - Các công ty kiểm soát các giá trị được tạo ra . - Web 2.0 cũng đã sinh ra mô hình doanh thu dựa trên quảng cáo. Mặc dù người dùng có	- Khái niệm về "Web 3.0" được đặt ra bởi đồng sáng lập Ethereum, Gavin Wood, ngay sau khi Ethereum ra mắt vào năm 2014. Gavin đã diễn đạt thành lời một giải pháp cho vấn đề mà nhiều người dùng tiền mã hóa sớm cảm nhận được: Web đòi

	thể tạo nội dung, họ không sở hữu nó hoặc không được hưởng lợi từ việc thương mại hóa nội dung đó.	hỏi quá nhiều sự tin tưởng. Tức là, phần lớn Web mà mọi người biết và sử dụng ngày nay phụ thuộc vào việc tin tưởng một số ít công ty tư nhân sẽ hành động vì lợi ích tốt nhất của công chúng.

Web3 là gì?

Web3 đã trở thành một thuật ngữ bao quát cho tầm nhìn về một Internet mới và tốt hơn. Cốt lõi của Web3 là sử dụng blockchain, tiền mã hóa và NFT để trao lại quyền lực cho người dùng dưới hình thức sở hữu.

Những nguyên tắc cốt lõi của web3

- Phi tập trung: thay vì quyền kiểm soát và sở hữu tập trung thì nó được phân phối cho người dùng và người xây dựng.
- Không cần sự cho phép: mọi người đều có quyền tham gia vào web3 không ai là ngoại lệ
- Thanh toán: sử dụng tiền mã hóa (cryptocurrencies) để thanh toán mà không cần dựa vào ngân hàng
- Không cần sự tin tưởng (trustless): nó hoạt động dựa trên các cơ chế khuyến khích và kinh tế, thay vì phụ thuộc vào các bên thứ ba đáng tin cậy.

Tại sao web3 lại quan trọng

- Quyền sở hữu

  Web3 trao quyền sở hữu tài sản số theo cách chưa từng có. Trong Web2, vật phẩm trong game gắn với tài khoản và có thể mất nếu tài khoản bị xóa. Khi không chơi nữa, giá trị đã đầu tư cũng mất theo.

  Web3 sử dụng NFT để đảm bảo quyền sở hữu trực tiếp. Ngay cả nhà phát triển game cũng không thể tước quyền này, và vật phẩm có thể được bán hoặc trao đổi để thu lại giá trị.

- Chống kiểm duyệt: đề cập đến tính phi tập trung để ngăn chặn hoặc giảm thiểu kiểm duyệt từ các cơ quan chính phủ, các thực thể tập trung. Mục tiêu tao ra internet mở, được kiểm soát bởi người dùng.
- Tổ chức tự trị phi tập trung (DAO - decentralized autonomous organization):

  Trong Web3, có thể sở hữu dữ liệu và nền tảng như một tập thể thông qua các token giống cổ phiếu công ty. DAO cho phép điều phối quyền sở hữu phi tập trung và đưa ra quyết định về

tương lai của nền tảng. DAO là các hợp đồng thông minh tự động hóa quá trình ra quyết định, nơi người dùng có token bỏ phiếu về cách sử dụng tài nguyên. Các cộng đồng Web3 có thể được coi là DAO với các mức độ phi tập trung và tự động hóa khác nhau.

- **Danh tính**: Web3 cho phép kiểm soat danh tính kỹ thuật số.

- Phương thức thanh toán: web3 sử dụng coin hoặc token để thanh toán

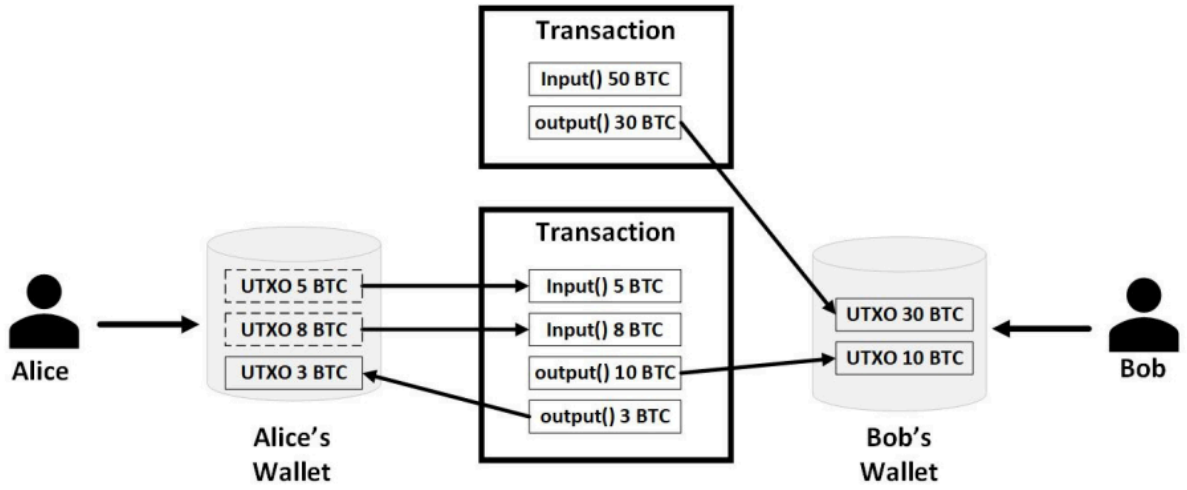
Hạn chế

- Khản năng tiếp cận
  Chi phi giao dịch vẫn là rào cản cho mọi người, đặc biệt là ở các quốc gia đang phát triển, thu nhập thấp
- Trải nghiệm người dùng: kỹ thuật là rào cản bước vào web3 khá cao. Người dùng phải có hiểu về 1 chút bảo mật, các tài liệu phức tạp, và chuyển sang 1 giao diện không trực quan, nhà cung cấp ví …
- Hạ tầng tập trung: web3 đang còn trẻ và phát triển. Do đó, hiện tại chủ yếu vẫn dựa vào hạ tầng tập trung như github, twitter, discord, …. NHiều công ty web3 vẫn đang
  tạo ra cơ sở hạ tầng đáng tin cậy và chất lượng cao

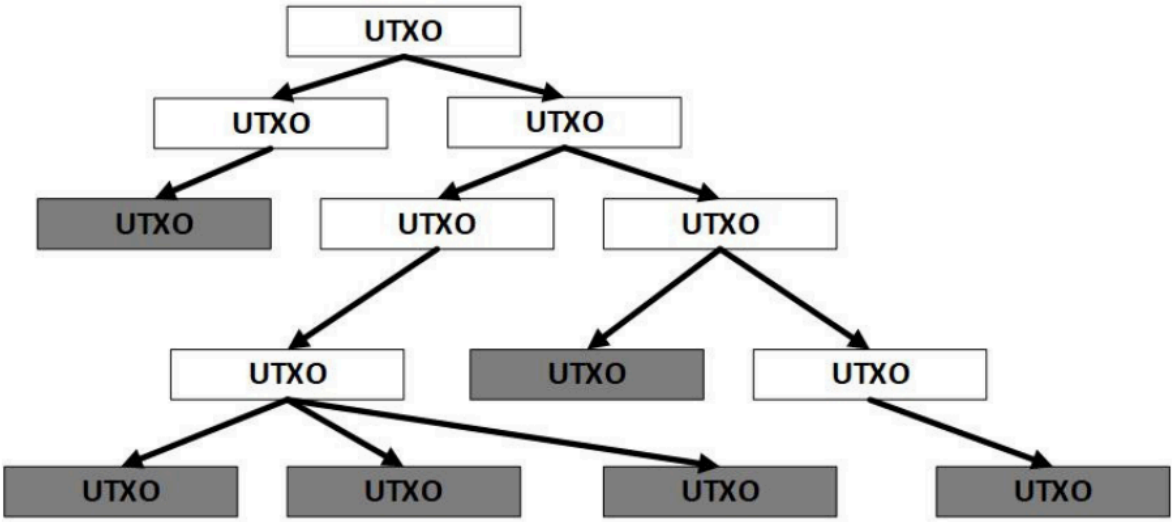
UTXO của Bitcoin

Mỗi khi người dùng kiểm tra tài khoản ngân hàng, họ sẽ thấy số dư phản ánh tất cả các giao dịch trước đó. Tương tự, ví bitcoin hoặc 1 số loại khác có khản năng hiển thị số dư, nhưng hoạt động theo cách khác. Thay vì theo dõi mọi giao dịch, Bitcoin chỉ theo dõi các đồng coin chưa được sử dụng, gọi là UTXO (đầu ra giao dịch chưa chi tiêu). Một giao dịch Bitcoin bao gồm các đầu vào và đầu ra – đầu vào chỉ ra các đồng coin chưa sử dụng nào được dùng, còn đầu ra xác định số lượng được chuyển cho người nhận. Khi giao dịch xảy ra, các đầu ra sẽ trở thành UTXO của người nhận cho đến khi họ sử dụng chúng trong giao dịch sau.

Ví dụ, nếu Alice muốn trả Bob 10 BTC và cô ấy có hai UTXO (5 BTC và 8 BTC), còn Bob đã có một UTXO 30 BTC, thì Alice sẽ dùng cả hai UTXO đó làm đầu vào. Giao dịch sẽ tạo ra một UTXO 10 BTC cho Bob và một UTXO 3 BTC trả lại cho Alice. Sau giao dịch, Alice còn một UTXO 3 BTC, còn Bob có hai UTXO. Khi một trong hai người sử dụng UTXO còn lại, các đầu ra chưa sử dụng từ giao dịch trước sẽ trở thành đầu vào trong giao dịch mới.



Vì mọi giao dịch đều được ký số, nên mỗi Bitcoin về bản chất là một chuỗi chữ ký số. Blockchain hoạt động như một máy trạng thái ghi lại tất cả các giao dịch trên một sổ cái không thể thay đổi. Mỗi UTXO đều có thể được truy ngược lại các đồng coin gốc được khai thác, cuối cùng dẫn đến những bitcoin đầu tiên trong khối khởi nguyên. Nếu tái dựng toàn bộ các giao dịch từ đầu, thì sẽ thấy dòng chảy của bitcoin như một đồ thị có hướng không chu trình (DAG). Để đếm số giao dịch UTXO hoặc tổng lượng bitcoin chưa chi tiêu, thì cần đếm số UTXO lá và tổng số bitcoin trong đó. Để biết có bao nhiêu bitcoin trong ví, chỉ cần cộng tất cả các đồng chưa chi tiêu trong các UTXO lá mà người sở hữu là người nhận.



Kiến trúc và hệ sinh thái của Ethereum

Kiến trúc Ethereum 1.0

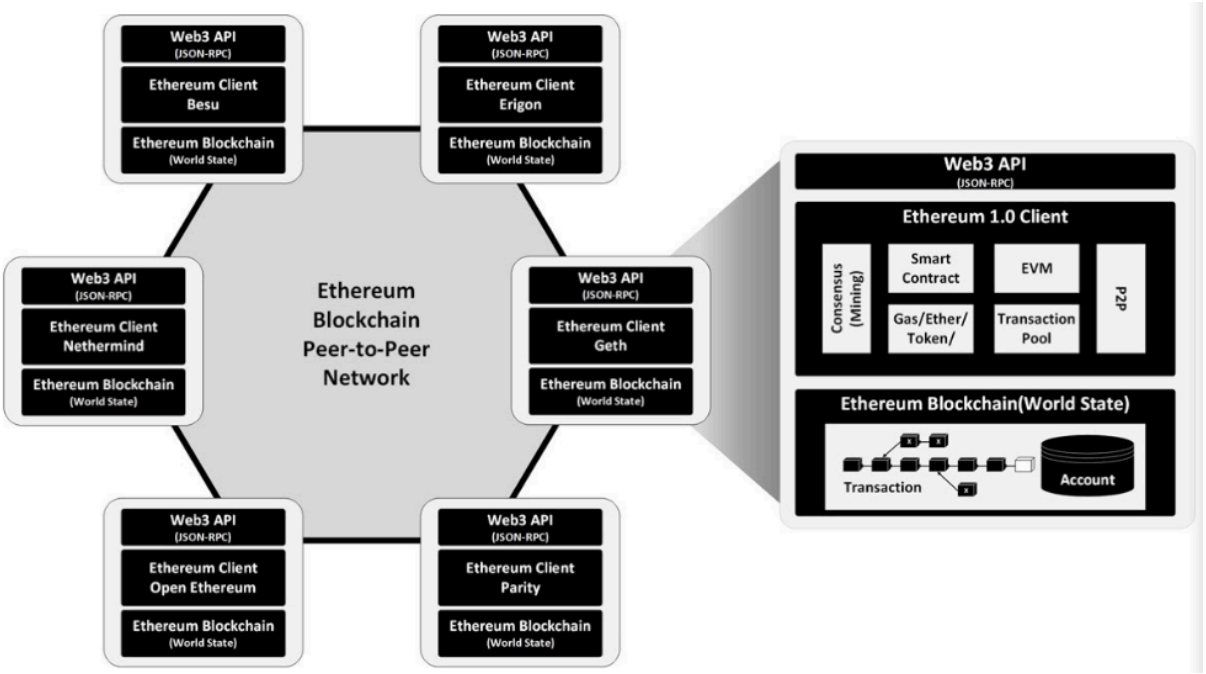
Ethereum client

Ethereum được sử dụng rộng rãi trong nhiều trường hợp, không chỉ đơn thuần là chuyển và thanh toán. Hợp đồng thông minh là 1 chương trình máy tính được triển khai và thực thi trên mạng blockchain Ethereum. Nó có thể thực hiện các giao dịch phức tạp giữa nhiều bên tham gia.
Một mạng blockchain Ethereum là 1 mạng ngang hàng phi tập trung của các Ethereum clients (là các node mạng). Một Ethereum client đề cập đến phần mềm được cài đặt trên node mạng đó có khả năng:

- Xác thực giao dịch
- Thực hiện hợp đồng thông minh
- Xử lý khối mới của chuỗi

Nó là 1 loại biệt lập nằm trong hàng trăm thiết bị kết nối mạng và kết nối với mạng P2P Ethereum

- Ethereum Virtual Machine
- Môi trường thực thi cho hợp đồng thông minh



Ethereum client chạy EVM và có thể được viết bởi nhiều ngôn ngữ lập trình phổ biến miễn là nó tuân theo đặc tả được định nghĩa trong Ethereum Yellow Paper(https://github.com/ethereum/yellowpaper).
Việc đa dạng trong việc phát triển Ethereum client có rất nhiều lợi thế:

- Làm cho mạng bền bỉ trước các lỗi
- Ngăn chặn tập trung hóa của các nhà phát triển
- Cạnh tranh giúp tạo ra nhiều giải pháp tốt hơn

- Mỗi client có thể có một trọng tâm, điểm mạnh và điểm yếu khác nhau trong việc khai thác, thử nghiệm, phát triển DApp và nhiều lĩnh vực khác.

Những Ethereum Client phổ biến:

Client	Language	Developers	Link to dowload
Geth	Go	Ethereum Foundation	https://geth.ethereum.org/downloads/
Parity	Rust	Parity	https://www.parity.io/
Besu	Java	Hyperledger Foundation	https://besu.hyperledger.org/en/stable/
OpenEthereum	Rust	Ethereum Foundation	https://openethereum.github.io/
Nethermind	.Net	Nethermind	https://nethermind.io/nethermind-client/
Erigon	Go	A team of devs	https://github.com/ledgerwatch/erigon

Ethereum giới thiệu về khái niệm về trạng thái toàn cầu (world state) và tài khoản (account):
- Mô hình tài khoản dùng để kiểm tra giao dịch tiền và số dư tài khoản thay vì sử dụng mô hình UTXO được sử dụng bởi Bitcoin
- Trạng thái toàn cầu cầu bao gồm 1 ánh xạ đến tất cả tài khoản và địa chỉ của họ
- Chuyển đối trạng thái đại diện cho chuyển đổi từ trang thái ổn định cũ sang trạng thái hiện tại.

Ngoài hợp đồng thông minh và EVM, một Ethereum client cung cấp tất cả các thành phần blockchain cho việc duy trì trạng thái toàn cầu và chuyển đổi trạng thái trong mạng blockchain, bao gồm:
- Quản lý giao dịch và chuyển đổi trạng thái trong mạng blockchain
- Duy trì trạng trạng thái toàn cầu và trạng thái tài khoản.
- Duy trì giao tiếp mạng ngang hàng
- Hoàn tất khối với việc khai thác
- Quản lý bể giao dịch (transaction pool)
- Quản lý tài sản, phí gas, ETH và tokens

Ethereum - máy tính toàn cầu

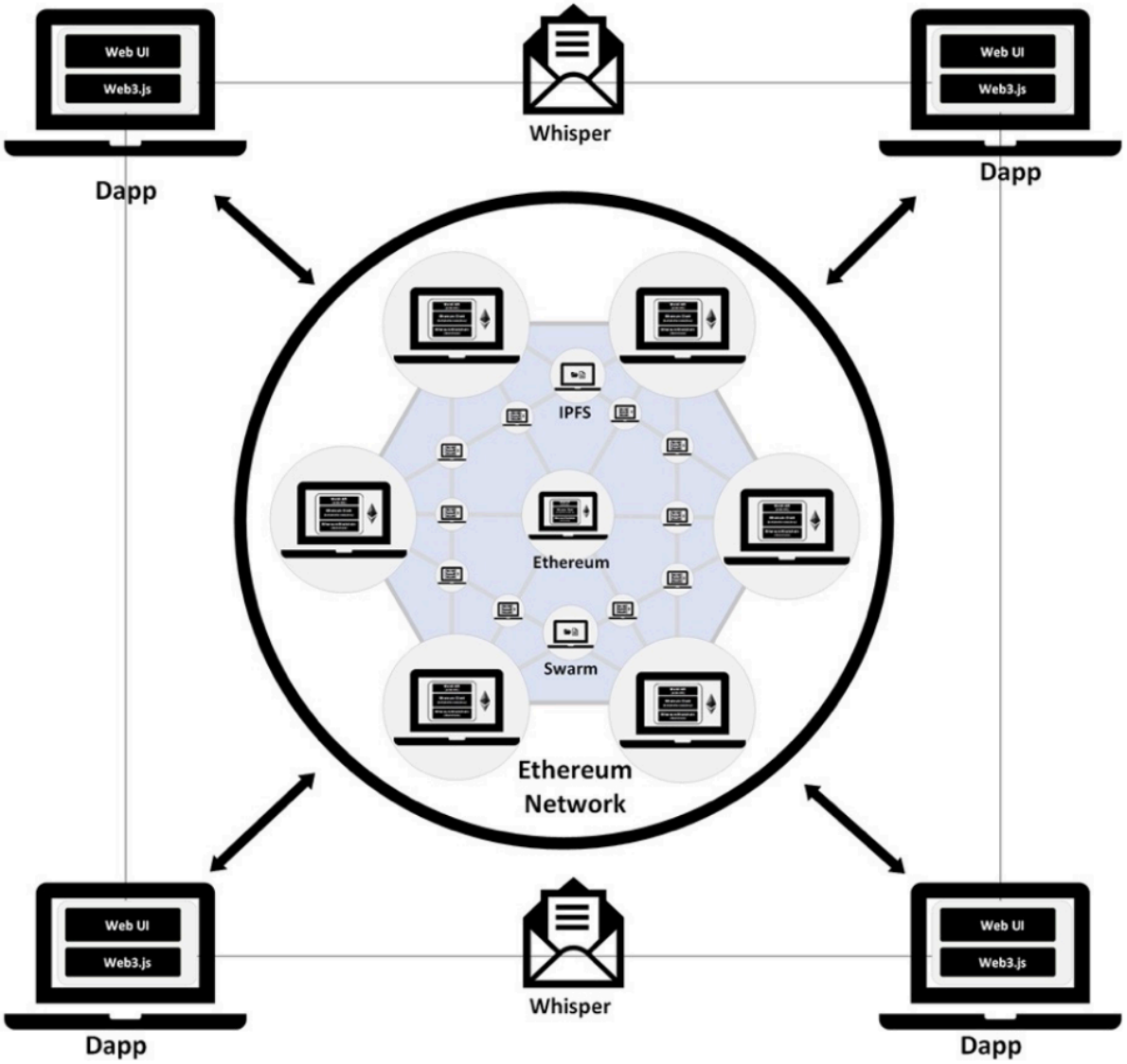
Ethereum được định hướng là máy tính toàn cầu cho thế giới phi tập trung. Để hỗ trợ mục tiêu này, Ethereum đã cung cấp 4 cơ sở tính toán phi tập trung cùng với số lượng lớn các công cụ phát triển và kiểm tra tạo điều kiện cho việc dễ dàng phát triển và chạy dapp trên mạng blockchain Ethereum:

1. Blockchain Ethereum cho trạng thái phi tập trung

2. Hợp đồng thông minh cho tính toán phi tập trung

3. Swarm và IPFS cho lưu trữ phi tập trung

4. Whispers cho nhắn tin P2P (giao tiếp ngang hàng)

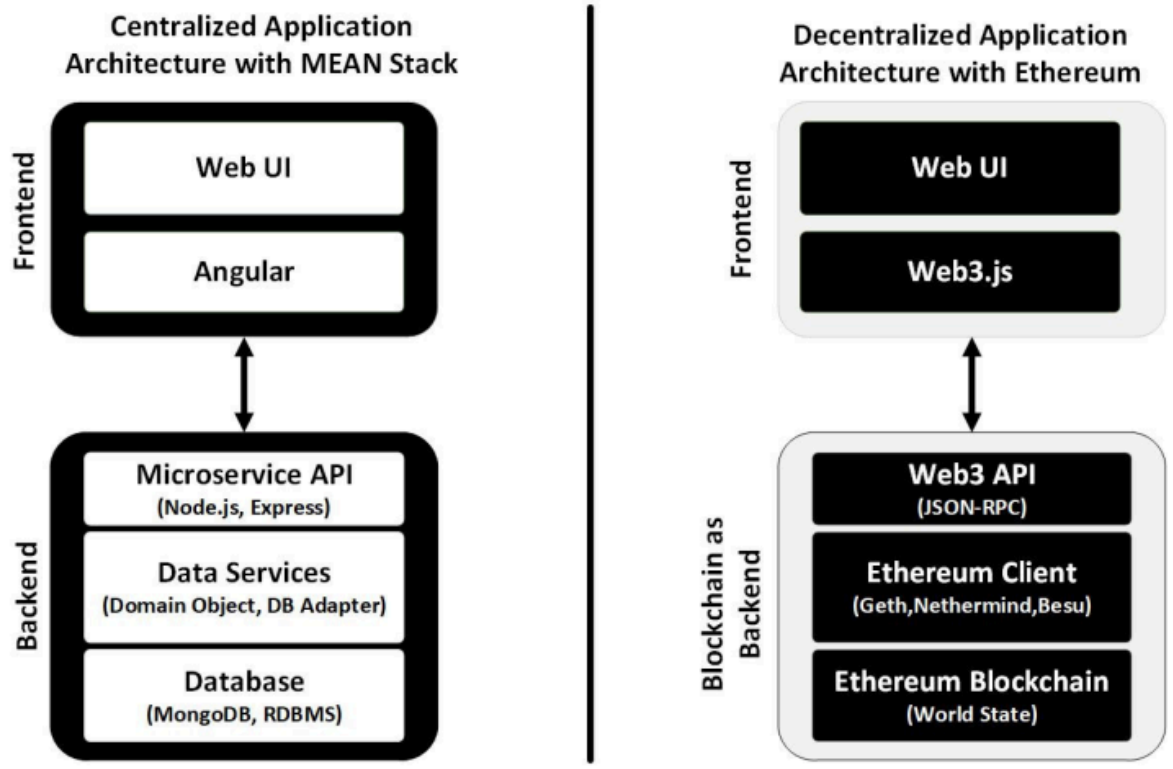


Blockchain và Metaverse

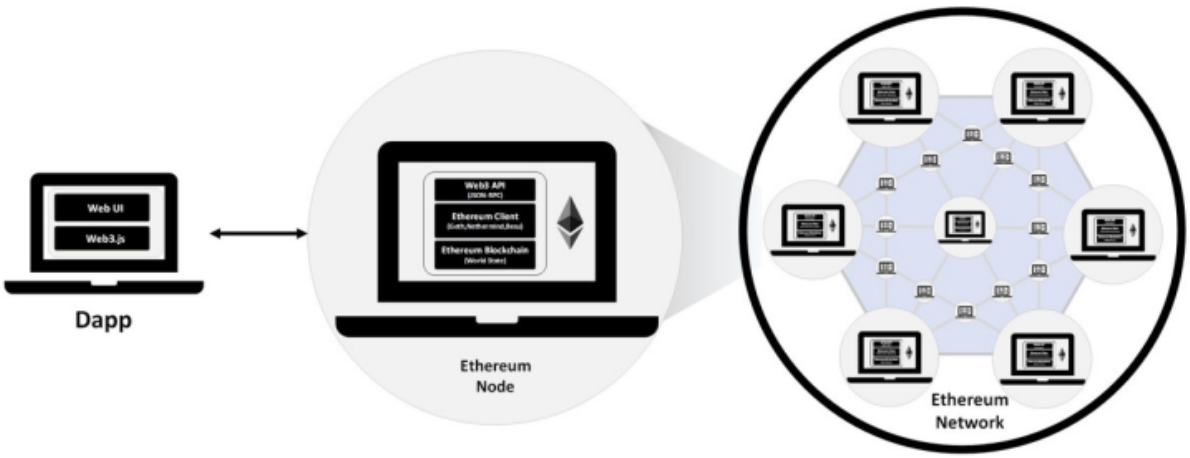
Blockchain và công nghệ Web3 sẽ mở ra Metaverse, một thế giới kỹ thuật số nơi người dùng sở hữu danh tính và tài sản của mình. Metaverse sẽ kết hợp công nghệ AR và VR, cho phép người dùng tương tác trong một thế giới ảo mang tính cá nhân hóa và riêng tư.

DAPPs

Một DAPP là 1 ứng dụng hoặc dịch vụ chạy trên mạng blockchain và cho phép tương tác trực tiếp giữa người dùng và nhà cung cấp.
Giống như cấu trúc của ứng dụng tập trung, dapp thường liên quan đến backend pi tập trung chạy trên mạng blockchain, cho phép người dùng tương tác với ví của họ và tạo giao dịch.



Ethereum client cung cấp1 tập các Web3 API thông qua JSON-RPC cho dapps tương tác với Ethereum blockchain. Từ web hoặc ứng dụng ví, người dùng có thể sử dụng đối tượng Web3 được cung cấp bởi web3.js để giao tiếp với mạng ethereum, nó hoạt động với bất kỳ ethereum client nào bất kể nó là local hay remote, để nó thực hiện các cuộc gọi RPC.



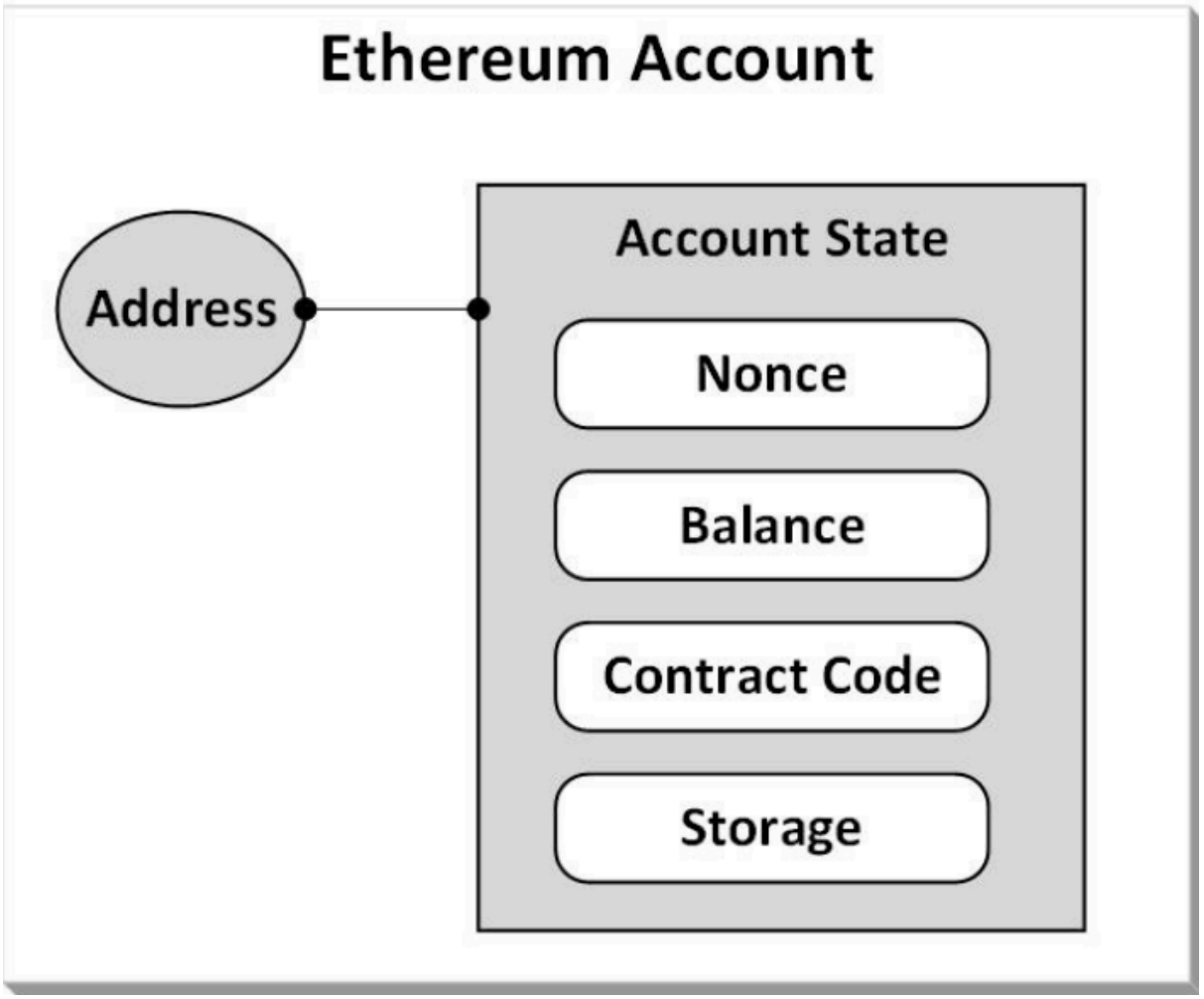
Tìm hiểu sâu hơn về Ethereum 1.0

Account

Thay vì sử dụng mô hình UTXO, Ethereum quản lý tài khoản và giao dịch khác với Bitcoin. Ethereum giới thiệu về khái niệm trạng thái toàn cầu(world state), là tập hợp tất cả tài khoản trên mạng blockchain. Trạng thái này biểu diễn trạng thái toàn cục của mạng blockchain và được cập nhật liên tục sau mỗi lần thực hiện giao dịch. Nó là 1 loại cơ sở dữ liệu toàn cầu được sao chép tới tất cả các node của mạng. Giống như tài khoản ngân hàng, tài khoản ethereum được sử dụng để giữ ETH và gió dịch với người khác.Nó có địa chỉ mật mã 20 bytes và 1 số dư tài khoản. Địa chỉ xác định chủ sở hữu của tài sản.

Tài khoản Ethereum chứa 4 trường:

- Nonce: 1 bộ đếm dùng cho việc xác định các giao dịch khác nhau
- Số dư: số dư ETH hiện tại của tài khoản
- Lưu trữ: mã băm mật mã tùy chọn trỏ đến lưu trữ của tài khoản
- Contract code: Mã băm mã hóa tùy chọn chỉ đến mã hợp đồng thông minh liên kết với việc tạo hợp đồng.



Trong Ethereum, một giao dịch là một sự chuyển trạng thái của tài khoản từ trạng thái này sang trạng thái khác, được khởi xướng bởi một thực thể bên ngoài. Tất cả các giao dịch, dù là chuyển ETH từ tài khoản này sang tài khoản khác hay thực thi mã hợp đồng thông minh, sẽ được tập hợp vào một khối. Ngoài ra, các trạng thái tài khoản kết quả và biên lai giao dịch cũng sẽ được thêm vào khối. Khối mới sẽ được khai thác bởi mạng blockchain và thêm vào blockchain. Dữ liệu trong blockchain được lưu trữ trong bộ lưu trữ hỗ trợ, thường là một cơ sở dữ liệu. Tùy thuộc vào việc triển khai client Ethereum, nó có thể được lưu trữ trong một loại cơ sở dữ liệu khác. Ví dụ, việc triển khai Geth sử dụng Google LevelDB làm cơ sở dữ liệu nền tảng cho trạng thái toàn cầu.

Hai loại tài khoản trong Ethereum

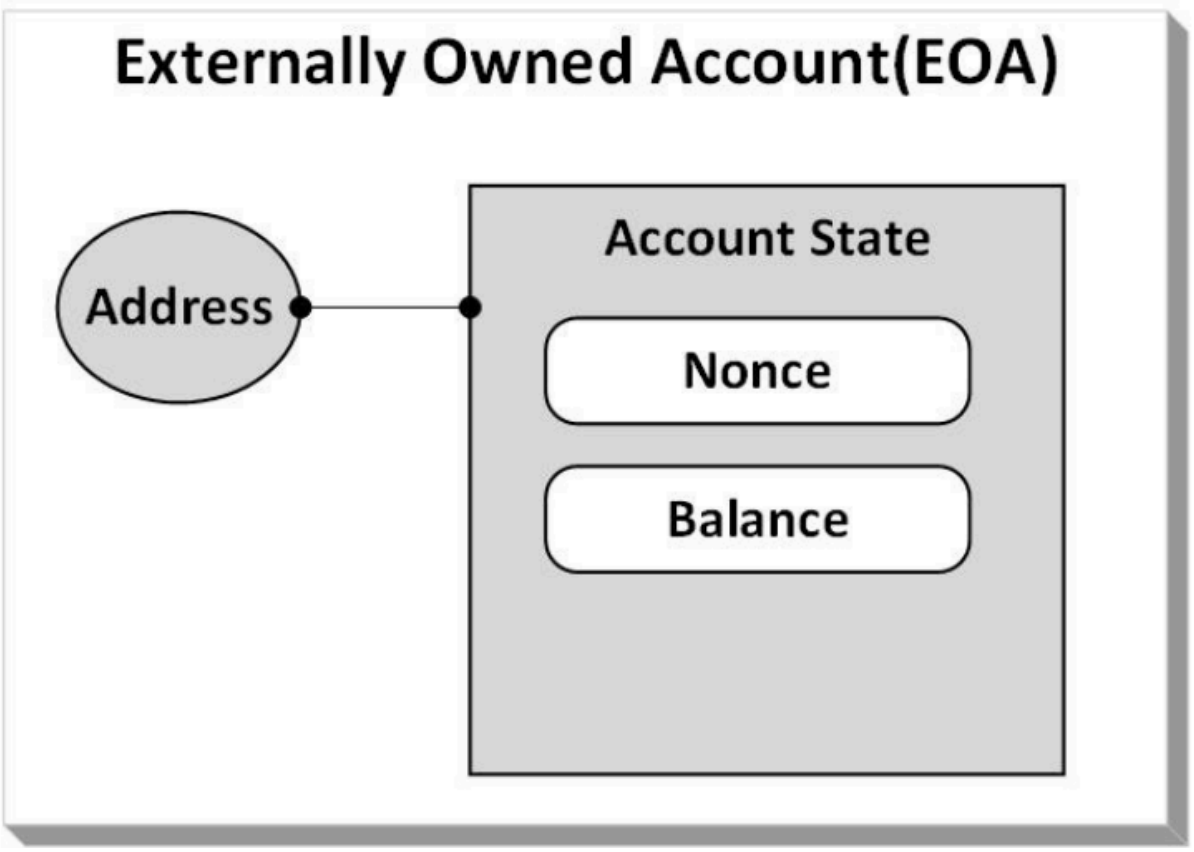
- EOA(externally owned account) được sử dụng cho việc chuyển ETH và được kiểm soát bởi khóa riêng. Không có mã(code) kết hợp với nó
- CA(Contract Account) Là tài khoản đại diện cho một hợp đồng thông minh. Được EVM (Ethereum Virtual Machine) kích hoạt và thực thi mã của nó bất cứ khi nào nhận được một giao dịch hoặc tin nhắn. Ngoài việc thực thi các hành động theo mã lập trình sẵn, CA còn có thể đọc/ghi dữ liệu vào bộ lưu trữ của nó hoặc gọi các hợp đồng thông minh khác.

Cả 2 đều là đối tượng trạng thái: EOA có số dư(balance) và CA có balance và lưu trữ(storage). Không có CA thí ethereum chỉ có thể chuyền giá trị đơn thuần như bitcoin

EOA

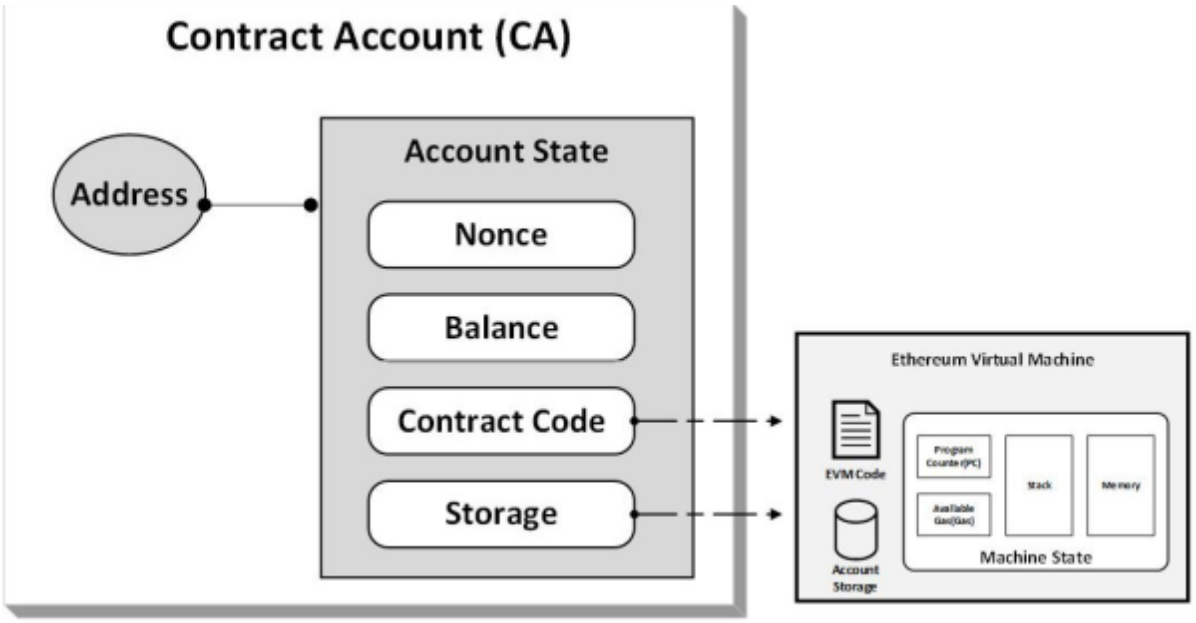
Một EOA được kết hợp với 1 thực thể bên ngoài là chủ sở hữu, người có quyền lợi và sở hữu các tài sản liên quan. Mỗi EOA có 1 cặp khóa mật mã(khóa riêng tư và khóa công khai). EOA được kiểm soát bởi khóa riêng tư của chủ sở hữu, được sử dụng để ký số tất cả các giao dịch, cho phép Máy ảo Ethereum (EVM) xác thực an toàn danh tính của người gửi. Trong trạng thái toàn cầu của Ethereum, tài khoản này được liên kết với một địa chỉ công khai, được tạo dựa trên khóa công khai của chủ sở hữu.

Cấu trúc của EOA



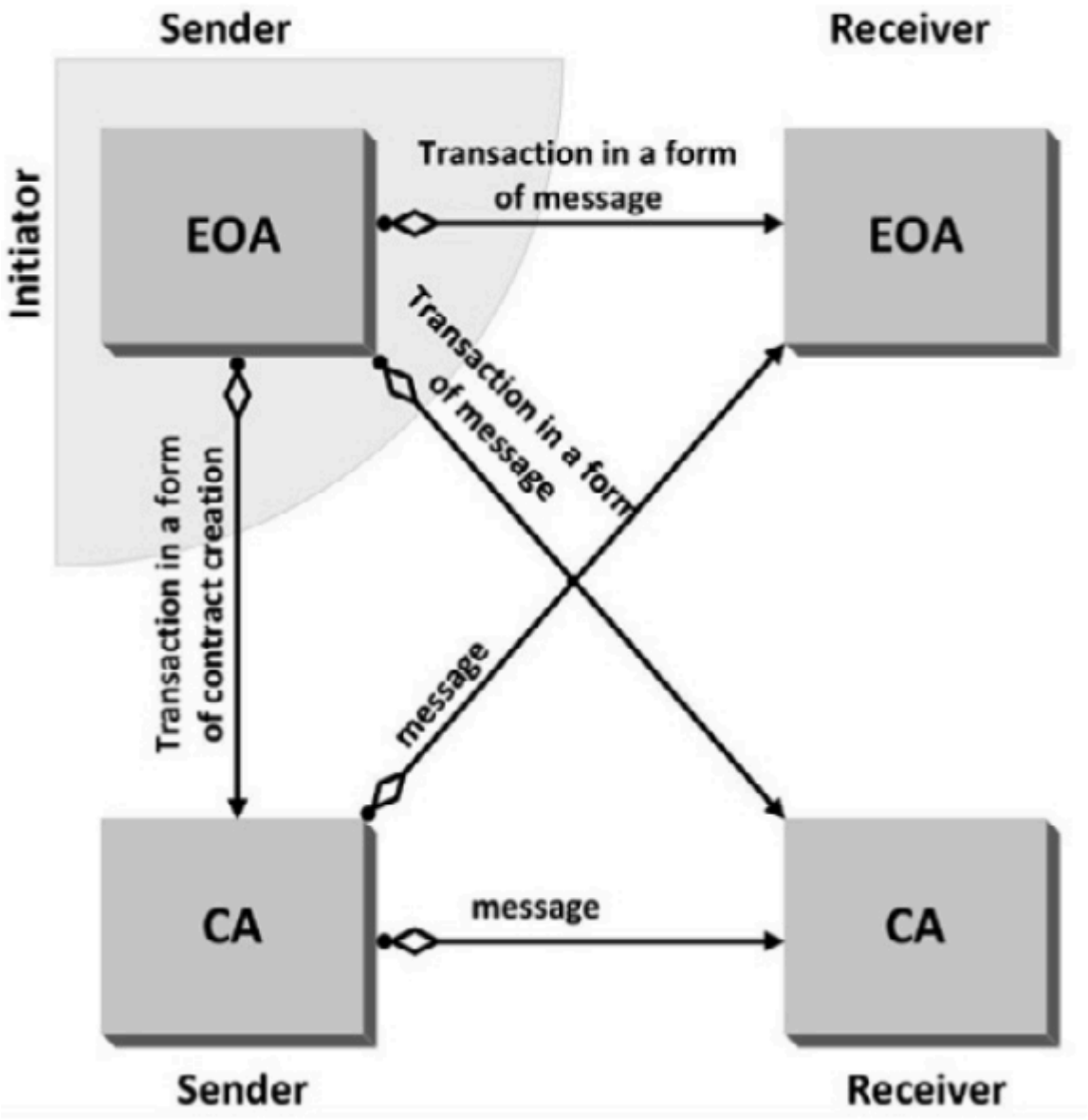
Contact Accounts - CAs

Một CA hoặc là 1 hợp đồng, có 1 số dư ETH (ETH balance) và được liên kết với mã hợp đồng thông minh trong Máy ảo Ethereum (ethereum virtual machine). Nó có thể có bộ lưu trữ(storage) trỏ đến bộ lưu trữ của EVM. Một sự thay đổi trạng thái trong CA có thể kích hoạt do cập nhật số dư ETH, dữ liệu trong lưu trữ hoặc là cả 2. CA cũng có địa chỉ kết hợp với nó, được tính toán thông qua hàm băm keccak-256, dựa trên địa chỉ của người tạo ra và giá trị nonce.



Giao dịch và thông điệp (transactions and messages)

Giao dịch và thông điệp trong Ethereum có sự khác biệt với nhau.



Trong Ethereum, thuật ngữ "transaction" (giao dịch) đại diện cho một gói dữ liệu đã được ký số, chứa một thông điệp (message) được gửi từ một EOA (tài khoản sở hữu bên ngoài) đến một tài khoản khác.

Thông điệp trong giao dịch này sẽ chỉ định hành động cần thực hiện trên blockchain.

Tất cả các giao dịch đều yêu cầu người khởi xướng (initiator) phải ký số thông điệp, và các giao dịch sẽ được ghi lại trên blockchain.

Có ba loại giao dịch có thể xảy ra.

1. Triển khai CA (Contract Account):
   Trong trường hợp này, một EOA hành động như người khởi tạo, gửi một giao dịch để triển khai một hợp đồng thông minh mới (tức là tạo ra một CA mới).

2. Giao dịch giữa hai EOA:
   Một EOA gửi ETH cho một EOA khác, bằng cách gửi một giao dịch chứa thông điệp chuyển ETH đến địa chỉ đích.

3. Giao dịch giữa EOA và CA:
   Trong trường hợp này, EOA gửi một giao dịch đến một CA, chứa thông điệp gọi hàm của hợp đồng thông minh, và CA sẽ thực thi mã hợp đồng tương ứng.

CA có thể gửi thông điệp đến CA khác hoặc EOA. Không giống 1 giao dịch, những thông điệp là 1 đối tượng ảo (virtual objects) trong quá trình thực hiện và không được ghi trong blockchain. Nếu 1 EOA là người nhận, trạng thái tài khoản của người nhận sẽ được cập nhật và được ghi vào trạng thái toàn cục (world state). Nếu 1 CA là nhận thông điệp, nó sẽ được xem như là 1 lời gọi hàm và mã hợp đồng kết hợp với nó sẽ thực hiện.

Từ góc nhìn của cấu trúc dữ liệu, 1 giao dịch là 1 thông điệp được ký kĩ thuật số. Theo thư viện web3.js, 1 thông điệp chứa các thuộc tính như ảnh dưới đây:

Attribute	Data type	Length	Description
from	DATA	20	This is a required field as the sender's address.
to	DATA	20	This represents the receiver's address.
gas	QUANTITY		This represents the gas value provided for the transaction execution.
GasPrice	QUANTITY		This represents the unit gas price used for each paid gas.
value	QUANTITY		This represents the ether value to be sent with this transaction.
data	DATA		This represents the compiled code of a contract when creating a contract account or the hash of the invoked method signature and encoded parameters during the contract invocation.
nonce	QUANTITY		This represents a nonce. This allows you to overwrite your own pending transactions that use the same nonce.

Hợp đồng thông minh - Smart contracts

Một hợp đồng thông minh là đoạn mã có thể thực thi, được triển khai bởi một người dùng (EOA) để tạo ra một Contract Account (CA).
Hành động triển khai này là một giao dịch đã được **ký số bằng khóa riêng của người tạo**.

Nó giống như thỏa thuận được lập trình giữa các bên giao dịch.Mã xây dựng nên hợp đồng được lưu trữ trên mạng Ethereum blockchain và không thể làm giả hoặc xóa nó, điều này tăng độ tin cậy của tài liệu pháp lý.

Dapps Developer viết smart contract bằng 1 số ngôn ngữ lập trình bậc cao và biên dịch chúng trở

thành bytecode. Bytecode sẽ nằm trên mạng blockchain và được thực thi bởi EVM. Dưới đây là 1 số lựa chọn ngôn ngữ lập trình trong Blockchain Ethereum

- Solidiy
- Vyper

ETH và Gas

Mạng lưới Bitcoin sử dụng Bitcoin như một loại tiền mã hóa để khởi động mạng lưới và có một thuật toán tinh vi để kiểm soát nguồn cung của đồng coin.
Thợ đào (miner), bằng cách cung cấp năng lực tính toán cho quá trình đào tốn kém, sẽ được thưởng bằng các đồng Bitcoin mới được tạo ra và phí giao dịch.

Ether là đồng tiền mã hóa cung cấp năng lượng cho mạng blockchain Ethereum.
ETH là ký hiệu chính thức được niêm yết cho Ether.
Gas là "nhiên liệu" để thực thi các smart contract trong EVM, và có thể được mua bằng Ether.

Để có được Ether, cần giao dịch trên thị trường tiền mã hóa hoặc tham gia làm thợ đào.
Trong Ethereum, nguồn cung sẽ giảm khi chuyển sang cơ chế PoS (Proof of Stake), đơn giản vì không còn cần đến hoạt động đào tốn kém để bù đắp nữa.

Ether sẽ được phát hành với tốc độ tuyến tính ổn định trong quá trình tạo khối (block-mining).

Wei là đơn vị tiền tệ nhỏ nhất của ether trong Ethereum.

Unit	Wei value	Wei
Wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
Microether (szabo)	1e12 wei	1,000,000,000,000
Milliether (finney)	1e15 wei	1,000,000,000,000,000
Ether	1e18 wei	1,000,000,000,000,000,000

Ethereum là một nền tảng máy tính phi tập trung, hoạt động nhờ đồng tiền ether. Khi thực hiện giao dịch, tất cả các nút mạng phải chạy các bước tính toán theo hợp đồng thông minh để xác minh giao dịch và khối.

Hệ thống tính phí thực thi (execution fee) dựa trên:

- Lượng gas cần thiết cho hợp đồng.
- Giá gas tại thời điểm đó.

Gas là đơn vị nội bộ trong Ethereum dùng để đo chi phí cho các hành động như tính toán, lưu trữ, và truy cập bộ nhớ.

Sau bản nâng cấp London (EIP-1559), Ethereum giới thiệu base fee – phí cơ bản do mạng tự điều chỉnh theo cung-cầu của kích thước khối. Khối có thể thay đổi kích thước nếu nhu cầu tăng hoặc giảm. Ngoài base fee, người gửi có thể thêm priority fee (tiền tip) để ưu tiên giao dịch của mình.

Người gửi cần đặt:

- Gas limit: lượng gas tối đa cho phép dùng.
- Giá mỗi đơn vị gas: tính bằng ether.

Tổng chi phí = gas * (base fee + priority fee).
Nếu không dùng hết gas, phần còn lại sẽ được hoàn trả. Nhưng nếu gas không đủ, giao dịch bị hủy và phí vẫn mất.

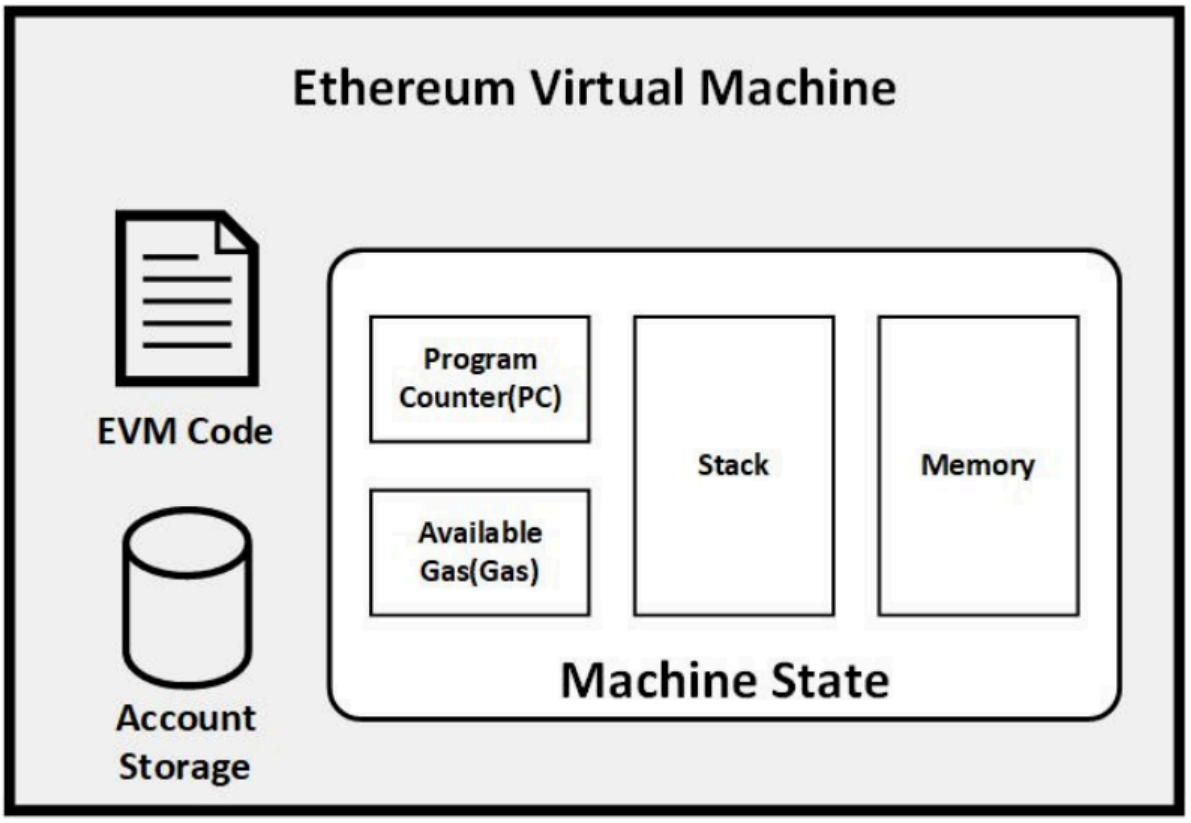
EVM - Ethereum virtual machine

Hợp đồng thông minh trong Ethereum thường được viết bằng solidity và được biên dịch thành bytecode và tải lên blockchain cho việc gọi và thực thi. EVM là môi trường thực thi cho hợp đồng thông minh. Nó được thực thi theo các cách khác nhau dựa vào các ethereum client khác nhau(mỗi cách thực hiện đều theo đặc tả được định nghĩa trong ethereum yellow paper)

EVM là một kiến trúc dựa trên ngăn xếp (stack-based). Khi thực thi một smart contract, nó thực hiện tất cả các thao tác — hay theo thuật ngữ kỹ thuật là opcode — được định nghĩa trong mã bytecode của hợp đồng. Ethereum cung cấp ba loại không gian lưu trữ trong EVM để các opcode truy cập và thao tác dữ liệu:

- Stack:
  Là cấu trúc LIFO (Last-In-First-Out) với độ sâu tối đa 1024 phần tử, mỗi phần tử có kích thước 256-bit (32 byte).
  Được sử dụng để thực thi các phép toán (ADD, MUL, JUMP,...) và lưu trữ dữ liệu tạm thời.
  Phù hợp với các phép tính toán Keccak-256 và ECDSA (đường cong elliptic).
- Memory:
  Là một mảng byte có thể mở rộng động trong quá trình thực thi, được đánh địa chỉ theo từng word (32 byte).
  Chỉ tồn tại tạm thời trong phạm vi một lần gọi hàm (external call).
  Opcode truy cập: MLOAD (đọc), MSTORE (ghi).
- Storage:
  Là key-value store 256-bit → 256-bit, lưu trữ dữ liệu vĩnh viễn trên blockchain.
  Không dùng để lưu trữ thông tin tài khoản (account state) mà chỉ lưu trữ dữ liệu riêng của hợp đồng thông minh (ví dụ: biến state trong Solidity).

Trong quá trình thực thi hợp đồng thông minh, EVM quyền truy truy cập vào thông điệp (message) cũng như là block header. Ngoài ra, EVM theo dõi gas có săn và PC (program counter) trong quá trình thực thi

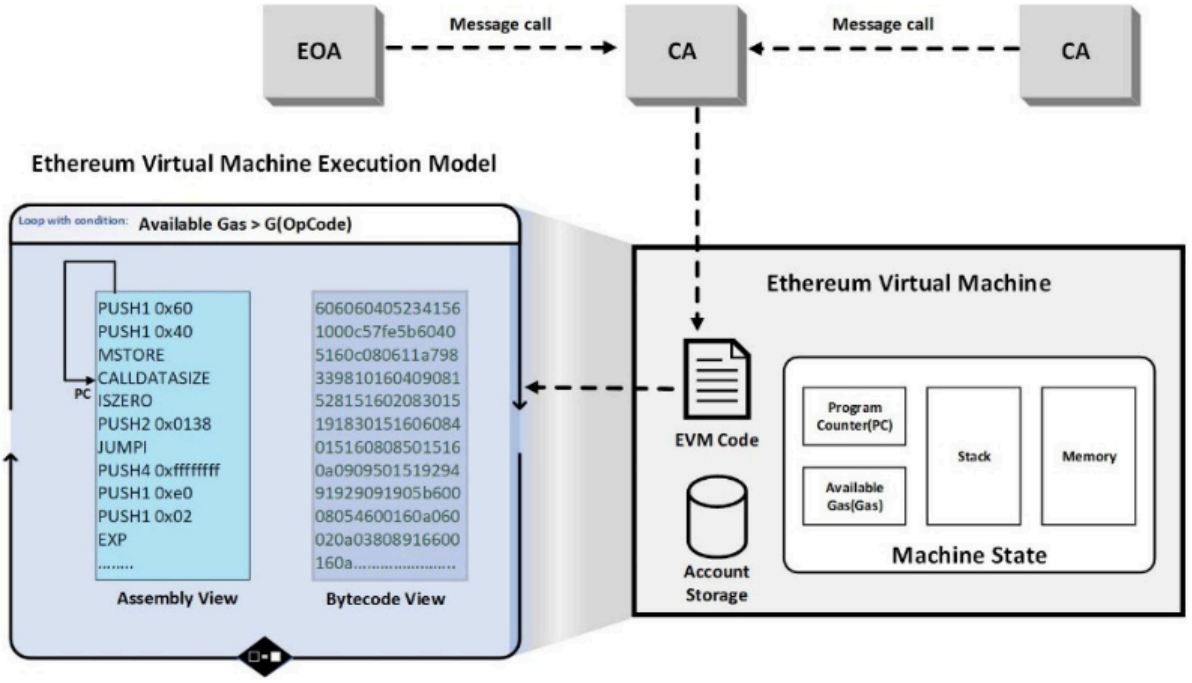


Byte code của hợp đồng thông minh được tải lên mạng Ethereum thông qua ‘giao dịch tạo hợp đồng’ được tạo ra và ký kỹ thuật số bởi EOA.
Dưới dưới đây là các bước cần thiết khi triển khai 1 hợp đồng thông minh

1. nhà phát triển viết hợp đồng thông minh trong solidity và biên dịch nó thành bytecode
2. họ sử dụng tài khoản ethereum của riêng họ để ký cho giao dịch tạo hợp đồng với bytecode
3. họ gửi giao dịch đó lên mạng ethereum và nó sẽ tải mã vào blockchain cho việc tạo tài khoản trong trạng thái toàn cục (world state) thông qua quá trình khai thác

Hợp đồng có thể được kích hoạt bởi giao dịch của 1 EOA hoặc là CA thông qua lời gọi hàm.

Hình ảnh mô tả cách EVM thực thi hợp đồng thông minh



Mô tả các bước thực thi trong ảnh

1. Sau khi được gọi, EVM tải bytecode vào Memory lặp qua từng opcode trong khi kiểm tra gas còn lại và thực thi các thao tác trên Stack
2. Trong quá trình thực thi nếu không đủ gas hoặc lỗi xuất hiện, luồng thực thi sẽ kết thúc
3. Giao dịch không được hoàn thành và người gửi sẽ mất các gas đã được tiêu trở lại.

EVM thực hiện khoảng 140 opcode, được chia thành 11 nhóm.

- Stop and arithmetic operations (0x00-0x0b)
- Comparison and bitwise logic operation (0x10-0x1a)
- SHA3 (0x20)
- Environmental information (0x30-0x3e)
- Block information (0x40-0x45)
- Stack, memory, storage, and flow operations (0x50-0x5b)
- Push operations (0x60-0x7f)
- Duplication operations (0x80-0x8f)
- Exchange operations (0x90-0x9f)
- Logging operations (0xa0-0xa4)
- System operations (0xf0-0xff)

Node thêm được blockmới vào blockchain sẽ nhận được phí thanh toán cho mỗi hợp đồng thông minh được thực thi. Chi phi được tính toán dựa trên các thao tác lưu, tính toán, thực thi hợp đồng thông minh. Đặc tả EVM xác định 1 bảng phí cho mỗi opcode được đề cập ở (https://github.com/crytic/evm-opcodes)

Địa chỉ trong Ethereum

Một EOA có 1 cặp khóa công khai - riêng tư (public-private). Khóa riêng tư (private) được sử dụng để ký kỹ thuật số cho bất kỳ giao dịch nào. Public key được sử dụng để tạo địa chỉ tài khoản và được liên kết đến trạng thái tài khoản trong trạng thái toàn cục (world state).

Để tạo một địa chỉ Ethereum, hãy lấy hàm băm Keccak-256 của khóa công khai (public key). 20 byte bên phải của hàm băm đó, kèm với tiền tố `0x` như là định danh hệ thập lục phân (hexadecimal), chính là địa chỉ Ethereum của EOA.
CA cũng có địa chỉ tài khoản. Thông thường nó được tạo ra dựa trên khóa công khai của người gửi và nonce của giao dịch.

Ví của Ethereum

Với Ethereum nên chọn các vi tương tích ERC-20.
ERC-20 là một tiêu chuẩn token của Ethereum, định nghĩa các tiêu chuẩn, giao diện hợp đồng thông minh và các quy tắc để phát hành các mã thông báo (crypto-token) trên mạng lưới Ethereum.
Danh sách các ví tương tích với ERC-20

- Atomic
- Trezor
- MyEther
- MetaMask
- Mist

Tài liệu tham khảo

- https://ethereum.org/en/web3/
- https://web3.lifeitself.org/concepts/censorship-resistence
- https://ethereum.stackexchange.com/questions/7358/what-is-the-difference-between-transaction-and-message
- Learn Ethereum - Second Edition(2024, Packt)