ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH

BÁO CÁO

ĐỀ TÀI MỞ RỘNG KSTN

MẠNG MÁY TÍNH - CO309B - HK221

ỨNG DỤNG MẠNG MÁY TÍNH TRONG BLOCKCHAIN

Giảng viên hướng dẫn: TS. Nguyễn Đức Thái

Sinh viên thực hiện: Nguyễn Đức An - 2010102

Email: an.nguyenduc1406@hcmut.edu.vn

Tp. Hồ Chí Minh, Tháng 12/2022

Mục lục

1 Giới thiệu đề tài

Blockchain đã và đang được đề xuất trở thành một giải pháp để giải quyết các vấn đề còn hạn chế của các centralized system. Hiện nay các ứng dụng đang được xây dựng dưới tầng kiến trúc hạ tầng mạng bao gồm switches và routers được kết nối bởi Ethernet, đây là một kiến trúc không ổn định về tính privacy và security, đặc biệt trong các lĩnh vực giao dịch.

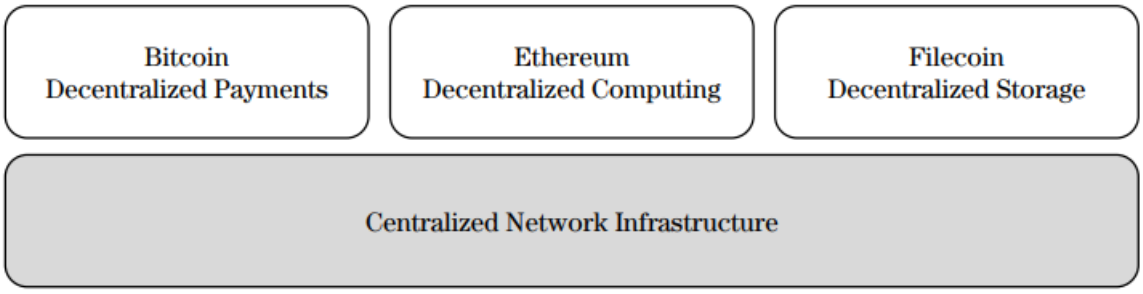
2 Lý do chọn đề tài

Đầu tiên, kiến trúc hạ tầng mạng hiện nay là không bảo mật (insecure) do sử dụng Ethernet. Ethernet mặc dù phổ biến và cải thiện được vấn đề bandwidth tuy nhiên không đảm bảo được các vấn đề về privacy và security do Ethernet không có hỗ trợ các dịch vụ mã hóa (encryption) trong thiết kế của nó. Điều này dẫn đến tình trạng chúng ta thường thấy, các nhà cung cấp dịch vụ Internet và chính phủ có thể dễ dàng theo dõi và điều tra các hoạt động của người dùng.

Thứ hai, việc tích hợp thêm các tính năng như phát hiện xâm nhập hoặc load balancing vào kiến trúc hạ tầng mạng hiện nay yêu cầu một nguồn chi phí rất lớn. Bởi vì cùng với sự phát triển thêm các tính năng mới là sự yêu cầu về các thiết bị phần cứng, tuy nhiên các switches, routers và bridges đều là các phần cứng rất đắt tiền, ngoài ra còn thêm chi phí config và bảo trì tương đối cao. Việc tái cấu trúc lại hệ thống hạ tầng mạng bấy giờ là việc làm rất tốn kém.

Thứ ba, kiến trúc hạ tầng mạng hiện nay theo kiến trúc tập trung (centralized network). Trong một phạm vi nhất định, có các nhà cung cấp dịch vụ mạng Internet cung cấp kết nối cho tất cả người dùng. Khi nhà cung cấp dịch vụ mạng xảy ra sự cố về lỗi đường truyền, sai sót thiết bị hoặc dịch vụ bị ngắt quãng, tất cả người dùng đều không kết nối vào Internet được. Việc tập trung tất cả quyền, dữ liệu vào một bên thứ ba theo kiến trúc hệ thống tập trung (centralized system) không đem lại sự đáng tin cậy (reliability) và sự tin tưởng (trusty) cho người dùng.

Vì vậy, các kiến trúc hệ thống phân tán (decentralized system), tiêu biểu là Blockchain đang được phát triển và đưa vào ứng dụng thực tế. Tuy nhiên, các kiến trúc decentralized system hiện nay, bao gồm blockchain vẫn phải đang phụ thuộc vào kiến trúc hạ tầng mạng tập trung (centralized network infrastructure).



Hình 1: *Sự phụ thuộc của các decentrialized system vào centralized network infrastructure*

3 Mục tiêu nghiên cứu

Trong phần đề tài mở rộng này, em tập trung nghiên cứu vào các vấn đề chính sau:

- **Marconi Protocol**: Marconi là một network và blockchain protocol cho phép ứng dụng smart contract vào network packets. Marconi Protocol được thiết kế ở tầng 2 của mô hình OSI và được sử dụng trong các kiến trúc decentralized network.
- **Blockchain Architecture**: nghiên cứu về kiến trúc các tầng của mạng blockchain.
- **Blockchain Terminology**: nghiên cứu về một số khái niệm trong mạng blockchain.
- **Blockchain Application**: nghiên cứu về các ứng dụng công nghệ blockchain vào các lĩnh vực như Bitcoin, DApp (Web 3.0),...

4 Giới thiệu về Marconi Protocol

4.1 Marconi Protocol

4.1.1 Định nghĩa

Marconi Protocol được định nghĩa là một số rules chung để các peers có thể kết nối và tương tác với nhau một cách bảo mật trong Marconi Network. Marconi network là một loại mạng toàn cục, có thể được xem như network of networks.

Marconi Protocol được ứng dụng để phát triển các tính năng của ứng dụng liên quan đến security, networking và decentralization, ví dụ như phát hiện những cuộc xâm nhập giả mạo, xây dựng mạng blockchain và các hệ thống mạng phân tán (decentralized network).

4.1.2 Cấu trúc

Cấu trúc của Marconi Protocol có thể chia thành 3 component lớn sau:

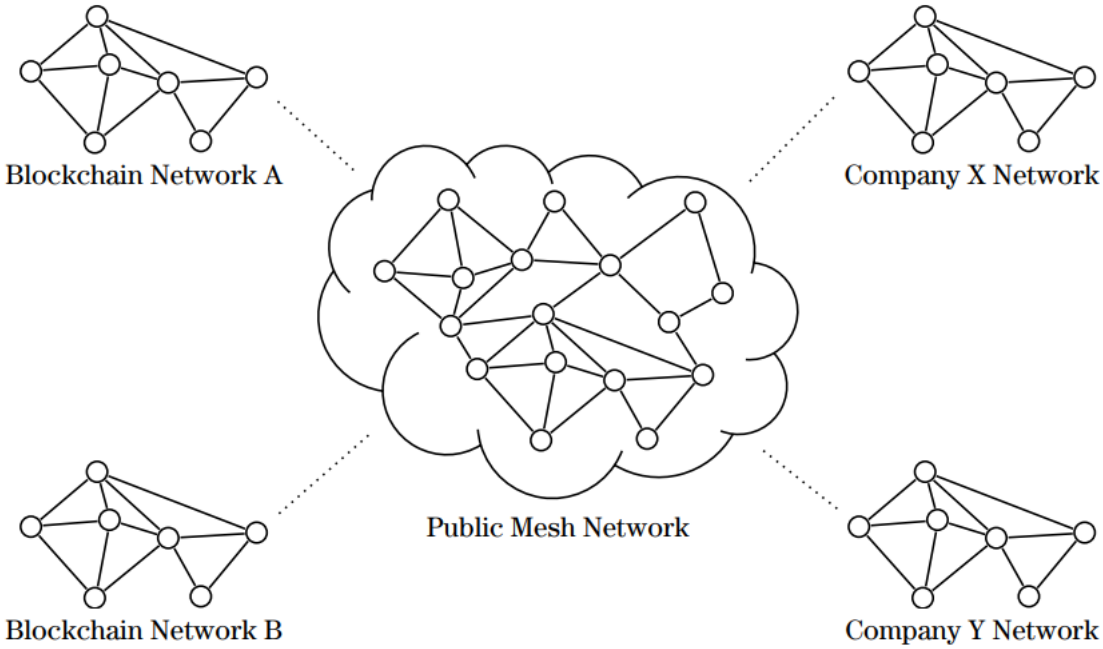
- **Marconi Pipe**
  - Marconi Pipes cung cấp các communication channel cho việc vận chuyển network giữa các peers và đảm bảo tính bảo mật trong quá trình vận chuyển các packet trong pipe. Kiến trúc Marconi Pipe được xây dựng ở layer 2 của OSI model và cung cấp các tính năng như encryption, routing và processing packets. Marconi Pipe được sử dụng với các kiến trúc mạng có dây (wired network) và có thể được hiện thực trong kiến trúc hạ tầng Internet hiện có.
  - Ngoài ra, người ta còn phát triển thêm kiến trúc **Marconi Link** nhằm hỗ trợ các mạng không dây (wireless network) như Bluetooth, Wifi,...
- **Smart Packet Contracts**
  - Các packet của network có thể được routing và processing bằng các đoạn mã lệnh trong smart contracts.
  - Phương pháp này được ứng dụng rộng rãi trong các ứng dụng smart decentralized networking như anti-phishing và anti-malware protection, hệ thống phát hiện và ngăn chặn xâm nhập giả mạo và các distributed virtual private networks.
- **Branch Chains**

– Một mạng blockchain có thể được xem như là một global chain và mỗi branch chains của nó bao gồm những custom rules được quy định bởi một nhánh đặc biệt được gọi là branch contract.

4.2 Marconi Network

4.2.1 Định nghĩa

Marconi Network cho phép hình thành một cấu trúc mạng toàn cục giữa các peers và tổ chức thành một network of networks. Mỗi peers của mạng có thể là một service node, computing device hoặc một network. Marconi Network Contracts là hợp đồng quy ước chung giữa các peers định nghĩa một số thông tin về loại dữ liệu có thể được trao đổi, thời gian tồn tại, loại smart packet contracts nào được enable, chi phí cho các lần vận chuyển dữ liệu,...



Hình 2: *Kiến trúc Marconi Network*

4.2.2 Đặc điểm

– Các đối tượng tham gia vào Marconi Network có thể bao gồm cá nhân, network operators hoặc Internet Service Providers. Các nodes sau khi tham gia sẽ được gửi về các kết quả tính toán các resources và network traffic theo định kỳ ở dạng network token, hay còn gọi là marcos. Marcos là đơn vị để tính toán các chi phí liên quan đến distributed networking and computing, các chi phí cho việc sử dụng, quản lý network và smart contract processing.

– Mặc dù Marconi Network đang vận hành trong kiến trúc hạ tầng Internet hiện có, tuy nhiên nó có thể tự hoạt động độc lập bằng cách hình thành các kết nối peer-to-peer trực tiếp từ các network branch đến mesh networks mà không cần tới các thiết bị phần cứng như switches, routers hay bridges.

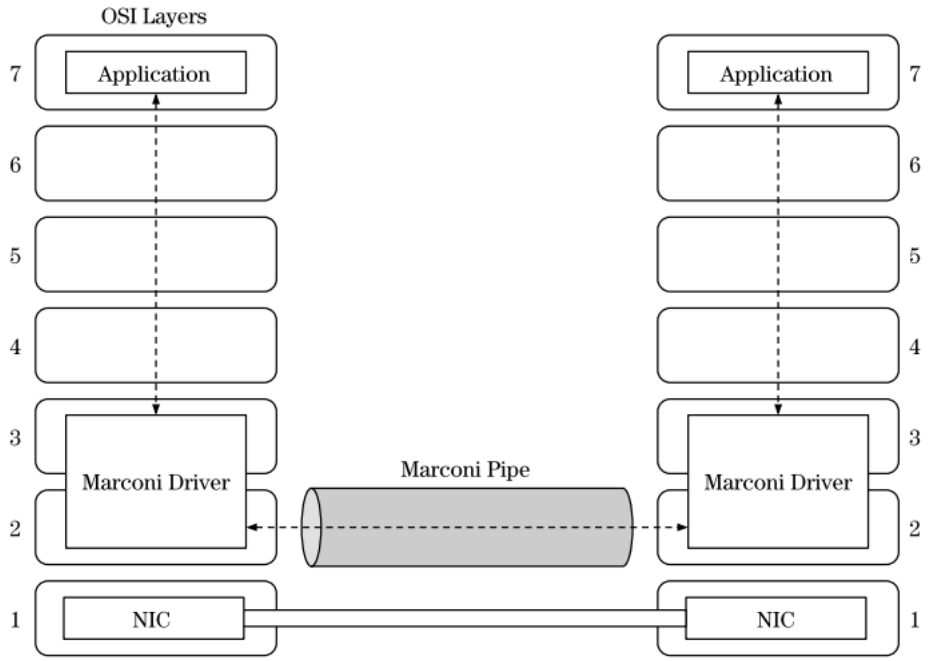
- Marconi Network cho phép người dùng có thể giao dịch các tài nguyên với nhau theo mô hình decentralized, chứ không cần phải thông qua các bên thứ ba trung gian theo cách truyền thống.
- Các đối tượng có thể tham gia vào public mesh network để thực hiện các mục đích như sau:
  - Users có thể tham gia các quá trình mining các marcos thông qua các contributing node.
  - Developers có thể tham gia các quá trình phát triển và deploy các ứng dụng decentralized networking applications.
  - Các doanh nghiệp, công ty có thể tham gia vào quá trình xây dựng và quản lý cơ sở hạ tầng mạng của công ty, cũng như phát triển các dịch vụ smart distributed networking and cybersecurity.

5 Kiến trúc Marconi Protocol

Marconi Network Protocol được thiết kế nhằm hỗ trợ quá trình bảo mật trong quá trình kết nối giữa các peers. Ba thành phần chính trong Marconi Network Protocol là: Marconi Pipe, Smart Packet Contracts và Marconi Link.

5.1 Marconi Pipe

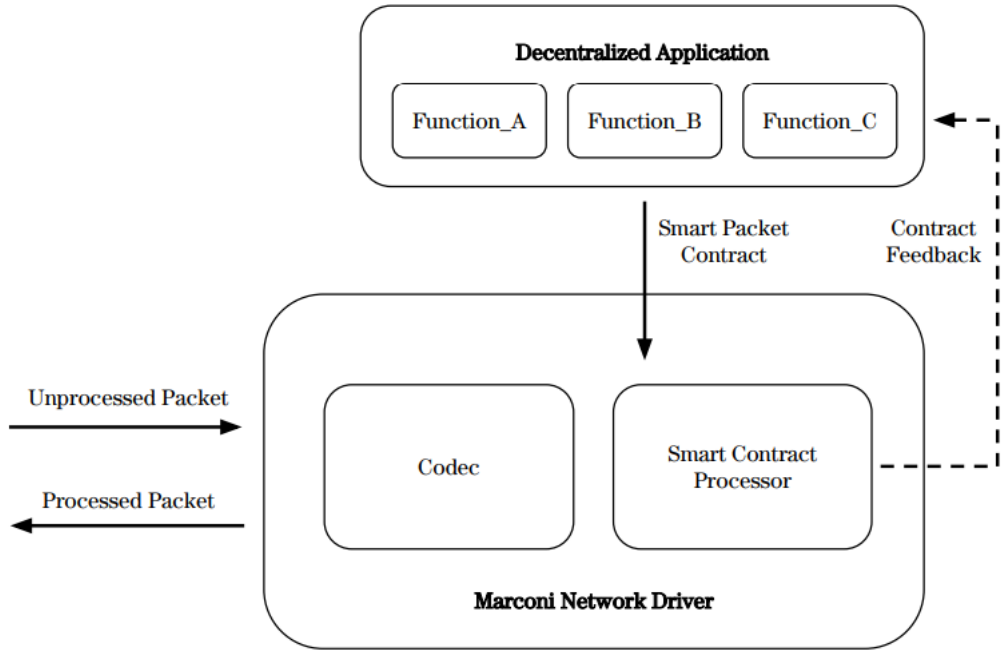
Marconi Pipe được hiện thực như một lớp ảo hóa link layer cho phép giao tiếp giữa các communication channel nhằm hỗ trợ quá trình vận chuyển network traffic giữa các peers. Marconi Pipe hỗ trợ một số tính năng giúp người dùng có thể custom được packet routing và processing, gia tăng tính bảo mật thông qua quá trình packet-level encryption và dễ dàng tìm ra được các peers lân cận.



Hình 3: *Kiến trúc Marconi Pipe*

5.2 Smart Packet Contracts

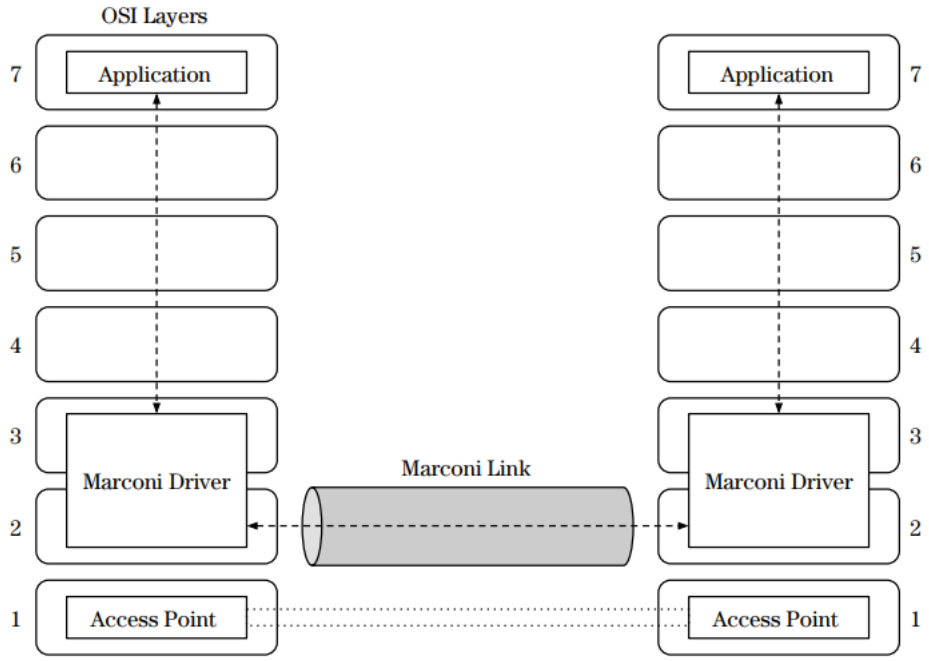
Với smart packet contracts, lập trình viên có thể chạy các smart contracts trong network packets để thực hiện các smart routing and packet processing. Marconi Network cung cấp nền tảng để lập trình viên có thể tạo ra các ứng dụng decentralized networking applications với smart packet contracts.



Hình 4: *Kiến trúc Smart Packet Contracts*

5.3 Marconi Link

Marconi Link cho phép các kết nối không dây (wireless communication), được sử dụng để bảo mật các wireless transmission giữa các nodes, cho phép có thể truy cập vào các network packets và sử dụng smart packet contracts.

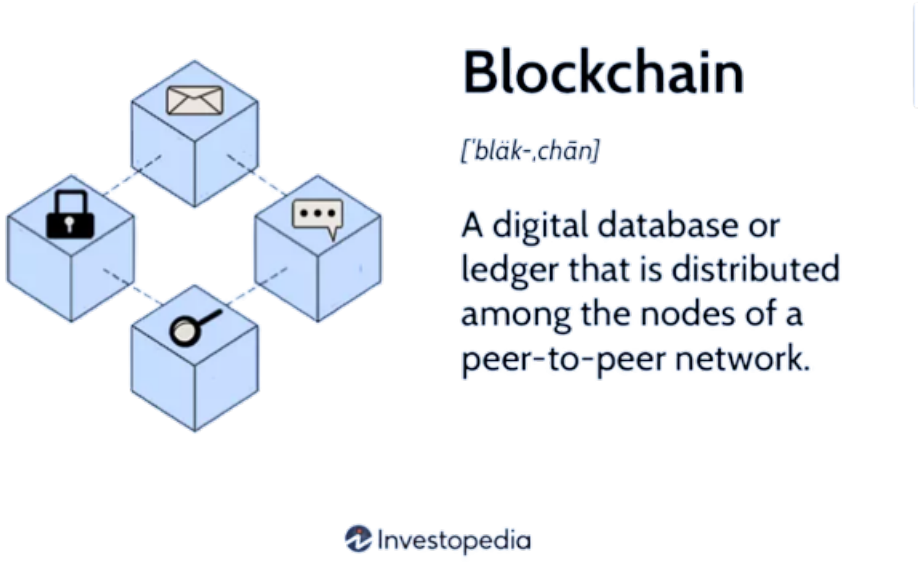


Hình 5: *Kiến trúc Marconi Link*

6 Giới thiệu về Blockchain

6.1 Định nghĩa

- Blockchain là một mô hình sổ cái phân tán (distributed ledger) được phát triển theo mô hình P2P network. Blockchain cho phép một nhóm các peers có thể đạt đến một sự đồng thuận với nhau trong khi thực hiện các giao dịch.
- Khi thực hiện giao dịch cần phải đạt được sự đồng thuận giữa các nodes và tuân thủ các consensus algorithm, giao dịch sau khi được xác nhận và được thêm vào sổ cái và sẽ được gửi cho tất cả các node trong mạng blockchain. Mọi node trong mạng blockchain đều có thể xem được thông tin giao dịch công khai trong sổ cái, do đó không cần phải đặt tất cả niềm tin vào một bên thứ ba duy nhất theo các kiến trúc centralized system.



Hình 6: *Mô hình blockchain*

6.2 Một số tính chất

1. **Immutable**
   - Mỗi node trong network đều có một bản sao của ledger. Khi thêm một transaction, tất cả node kiểm tra tính hợp lệ của transaction. Trong trường hợp số đông các nodes nghĩ rằng đó là một transaction hợp lệ, transaction đó sẽ được thêm vào blockchain. Điều này có nghĩa là nếu không nhận được sự đồng thuận của số đông các node, không ai có thể thêm bất cứ thay đổi gì đến ledger.
   - Bất cứ các records trong block không thể thay đổi. Nghĩa là không có người nào trong network có thể edit, change hoặc delete những records sau khi đã được thêm vào blockchain.
2. **Distributed**
   - Tất cả các node tham gia vào network đều có các bản sao của ledger. Ledger bao gồm các thông tin về tất cả các node tham gia vào network và transactions.

- Có thể dễ dàng kiểm tra những thay đổi trong ledgers dựa vào các bản sao distributed ledger được gửi cho từng node.
- Mỗi node trong blockchain đều phải tham gia vào quá trình validation transaction. Bất cứ thay đổi nào trong ledger sẽ được update trong vòng vài giây hoặc vài phút đối với tất cả các bản sao của ledger.
- Khi một người dùng muốn thêm một block mới, các nodes tham gia khác phải tiến hành xác minh tính hợp lệ transaction. Trong trường hợp số đông các nodes nghĩ rằng đó là một transaction hợp lệ, transaction đó sẽ được thêm vào blockchain.
- Trong blockchain, không ai có quyền quyết định tất cả trong blockchain. Tất cả mọi người đều phải tuân thủ các chuẩn khi thêm một block mới vào network.

3. **Decentralized**
   - Blockchain network được gọi là decentralized có nghĩa là mọi node đều bình đẳng với nhau, không có node nào được quyền quyết định mọi thứ.
   - Người dùng có thể kiểm soát các thông tin của họ và không cần phụ thuộc vào bên thứ ba có nhiều rủi ro trong quá trình quản lý các tài sản của họ.
   - Ngoài ra, kiến trúc decentralized giúp làm tăng độ bảo mật của blockchain. Trong trường hợp kiến trúc hệ thống phụ thuộc vào một bên thứ ba, trong trường hợp này là server. Khi server bị hacker tấn công, hoặc xảy ra lỗi thì tất cả các node tham gia trong hệ thống sẽ bị ảnh hưởng, tuy nhiên nếu theo kiến trúc decentralized network, khi một node bị ảnh hưởng có thể backup từ node khác.
4. **Secure**
   - Tất cả các records trong blockchain đều được mã hóa nhằm tăng độ bảo mật cho các quy trình trong blockchain network. Bởi vì không có central authority, do đó không có bất cứ bên nào có thể dễ dàng giải mã để thêm, chỉnh sửa, xóa dữ liệu trong network.
   - Tất cả các blocks bao gồm mã hash của chính bản thân nó và mã hash của block trước đó. Do đó các blocks được kết nối với các block khác. Bất cứ sự thay đổi dữ liệu ở một block sẽ thay đổi tất cả hash ID.
5. **Consensus**
   - Tất cả các blockchain bao gồm các thuật toán consensus để đảm bảo các node có quyền bình đẳng như nhau. Consensus là một decision-making algorithm dùng để hỗ trợ nhóm các nodes có thể đạt được sự đồng thuận nhanh hơn và tuân thủ các rules thống nhất.
   - Các node không cần phải tin vào các node khác nhưng nó có thể tin vào các thuật toán chung của network để ra quyết định. Có rất nhiều loại consensus algorithm khác nhau, mỗi thuật toán đều có ưu điểm và nhược điểm.
   - Các mạng blockchain bắt buộc phải có một thuật toán consensus algorithm.
6. **Unanimous**
   - Các node phải xác minh sự hợp lệ của các records trước khi được thêm vào blockchain.
   - Khi một node muốn được thêm vào network, nó phải đạt được phần lớn sự đồng thuận của các node khác. Bên cạnh đó một node không thể dễ dàng được thêm, chỉnh sửa, hoặc xóa các thông tin từ blockchain.

– Các thông tin về cập nhật các node được cập nhật liên tục giữa các nodes trong network, do đó không thể thay đổi thông tin của các node mà không tuân qua các thuật toán consensus của network.

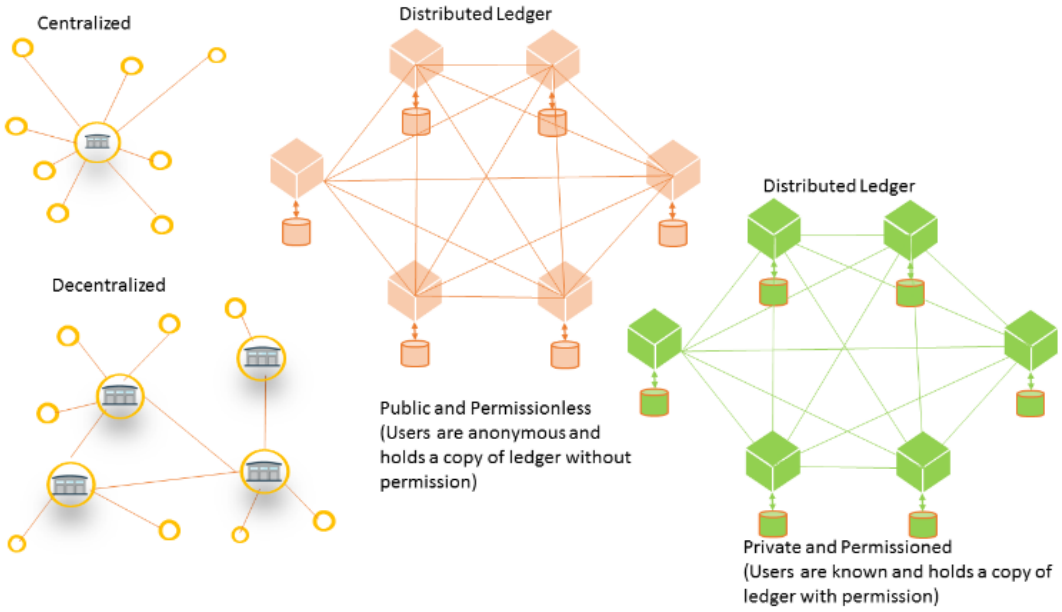
6.3 Mô hình P2P network trong Blockchain

6.3.1 Mô hình distributed ledger

– Các máy tính tham gia vào blockchain sẽ được chạy trên một mạng P2P và sử dụng chung một blockchain protocol. Điều này cho phép mỗi node giữ một bản sao của sổ cái. Sổ cái này bao gồm các thông tin giao dịch được đóng gói trong các khối, trong đó các khối được kết nối với nhau thành một chuỗi blockchain với block ban đầu là generis block. Khi muốn thêm khối mới vào chuỗi, phải được thống nhất dựa trên sự đồng thuận giữa các node và không có qua bất cứ trung gian nào.

– Mô hình sổ cái phân tán cũng được chạy trên một mạng P2P, nơi các giao dịch được xác thực bằng cách giải một mã hash được sinh ra từ các thuật toán đồng thuận (generis algorithm). Mỗi mạng blockchain sẽ tự xác định các consensus algorithm cho nó, về cơ bản là đó là những quy tắc dùng để xác thực các giao dịch trên mạng P2P blockchain. Sau khi đạt được sự đồng thuận, khối mới sẽ được thêm vào sổ cái. Sau đó, các node tham gia vào quá trình xác thực giao dịch sẽ nhận được một phần thưởng khuyến khích, có thể là coin khi mining thành công một block.

– Điểm nổi bật là, trong mạng P2P theo mô hình sổ cái phân tán như blockchain, các giao dịch được xác minh bằng mật mã và được xác thực bằng sự đồng thuận.



Hình 7: *Mô hình sổ cái phân tán (distributed ledger)*

6.3.2 So sánh giữa mô hình centralized và decentralized network

1. **Centralized network**

- Centralized network có một central node xác định và chi phối việc xác thực và xác minh của tất cả các giao dịch. Tất cả các node khác đều dựa vào central node. Central node có toàn quyền truy cập và kiểm soát dữ liệu, thông tin và trạng thái của các giao dịch. Mặc dù theo mô hình centralized network, các node trong mạng được cấu trúc và quản lý chặt chẽ, nhưng nó cũng gặp phải những hạn chế bởi mô hình kiểm soát tập trung.
- Để vận hành được mô hình centralized network cần có sự tin tưởng giữa central node và các node tham gia. Ngoài ra còn có nhiều rủi ro như lòng tham của con người, ý định muốn vụng lợi cho bản thân, việc tập trung quyền lực vào một bên thứ ba duy nhất có những rủi ro cao khi bên đó muốn chiếm lấy toàn bộ tài sản hoặc vụng lợi cho bản thân.
- Mô hình này phù hợp với các tổ chức nhỏ, nơi các quyết định có thể được đưa ra nhanh chóng và mọi người trong tổ chức đều có thể dễ dàng nhìn thấy được những quyết định của người ra quyết định.

2. **Decentralized network**

- Mô hình mạng decentralized network về bản chất khi hiện thực ở tầng kiến trúc cũng tương đối giống với centralized network, tuy nhiên quyền quyết định được phân phối đều cho tất cả các node. Trong một mạng phi tập trung (decentralized network), mỗi node có quyết định bình đẳng như nhau, quyết định tổng thể được xác định bằng sự đồng thuận của phần lớn các node tham gia.

6.4 Một số thuật ngữ trong blockchain

6.4.1 Block

- Block có thể được xem như một basic containter bao gồm các thông tin trong blockchain.
- Block bao gồm dữ liệu của các transaction.
- Mỗi khi block được thêm vào blockchain, dữ liệu của block đó là không được thay đổi (immutable).
- Block được xác định bằng một mã hash được mã hóa bằng các thuật toán hash như RSA256, MD5,...
- Phần trình bày về cấu trúc của một block được trình bày ở **Phần 7.Kiến trúc mạng Blockchain - Data Layer**.

6.4.2 Ledger

- Có thể hiểu đơn giản ledger là một cuốn sổ cái dùng để ghi lại lịch sử giao dịch của một block.
- Một đặc điểm nổi bật của blockchain là cuốn sổ cái này được gửi cho tất cả các node tham gia trong mạng, chứ không phải tập trung vào một bên thứ ba duy nhất.

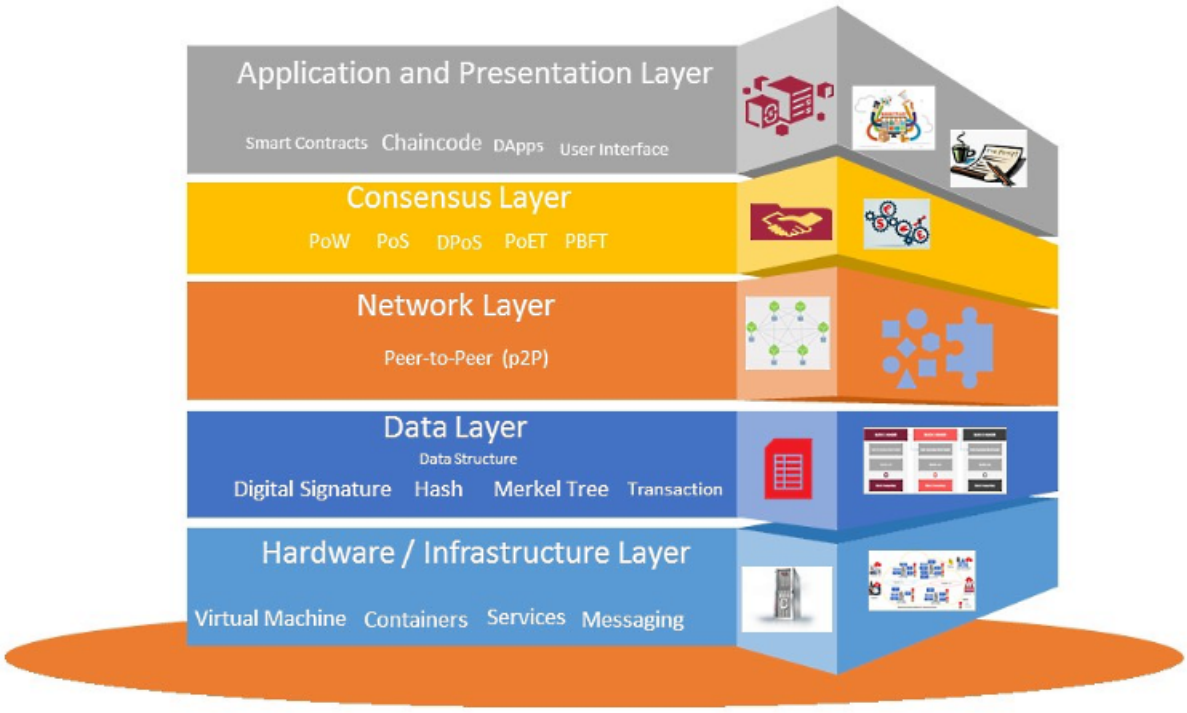
6.4.3 Smart Contract

- Smart Contract là một đoạn mã nguồn sẽ được tự động thực thi trên mạng blockchain trong trường hợp thỏa mãn các precondition của giao dịch,
- Smart Contract được sử dụng để nhằm đảm bảo các giao dịch đều tuân theo các thuật toán consensus algorithm được quy định trong mỗi blockchain.

6.4.4 Consensus

- Consensus là cơ chế nhằm đảm bảo các node trong peers đều có quyền lực như nhau, việc xác minh giao dịch phải tuân theo sự đồng thuận của số đông các node trên tinh thần tự nguyện.
- Consensus algorithm được sử dụng để đảm bảo tính chất đồng thuận phi tập trung (decentralized), đảm bảo không có node nào có quyền kiểm soát toàn bộ giao dịch.

7 Kiến trúc mạng Blockchain



Hình 8: *Kiến trúc mạng blockchain*

7.1 Hardware & Infrastructure layer

7.1.1 Hardware layer

Blockchain được xây dựng với kiến trúc như một mạng P2P gồm các node bao gồm là các máy tính được sử dụng để tính toán và xác minh các giao dịch, sau khi được xác thực các node được lưu trữ một cách có thứ tự trong một sổ cái chung, bản sao của số cái được gửi cho các node tham gia.

Mỗi máy tính trong mạng P2P được gọi là một node. Các node chịu trách nhiệm xác thực các giao dịch, sau đó thêm block mới vào mạng blockchain,...Sau khi đạt được sự đồng thuận, các node tiến hành commit và thêm khối vào chuỗi blockchain sau đó cập nhật lại bản sao sổ cái cục bộ của chúng.

7.1.2 Infrastructure layer (Ethereum)

- Tất cả client đều có thể cài đặt Ethereum trên máy của họ và tham gia với vai trò như một node trong mạng blockchain. Một node có thể là light node hoặc full node. Các light node lưu trữ cache,

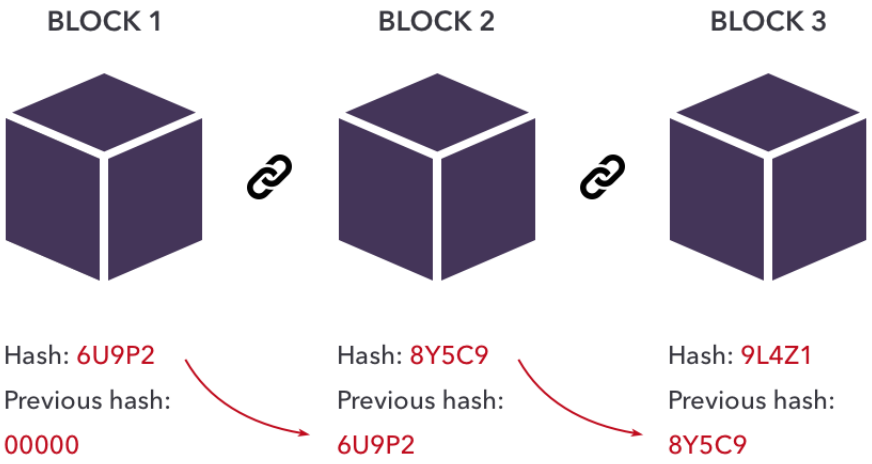
trong khi full node lưu trữ dữ liệu, dữ liệu này phát triển tuyến tính theo thời gian. Ngoài ra light node có thể tham gia để xác minh việc thực hiện các giao dịch.

- Mặt khác, bất kỳ node nào tham gia đầy đủ vào việc xác minh các consensus algorithm đều phải download đầy đủ dữ liệu từ full node. Full node tham gia vào quá trình xác minh chữ ký, format dữ liệu, check double spending (giao dịch hai chiều), ngoài ra full node còn có thể tham gia vào quá trình xác minh giao dịch.
- Các node Ethereum phía client sẽ được chạy trên **Ethereum Virtual Machine (EVM)**. EVM là một máy ảo cho phép các smart contracts có thể được thực thi trong mạng blockchain.

7.2 Data layer

7.2.1 Cấu trúc Block

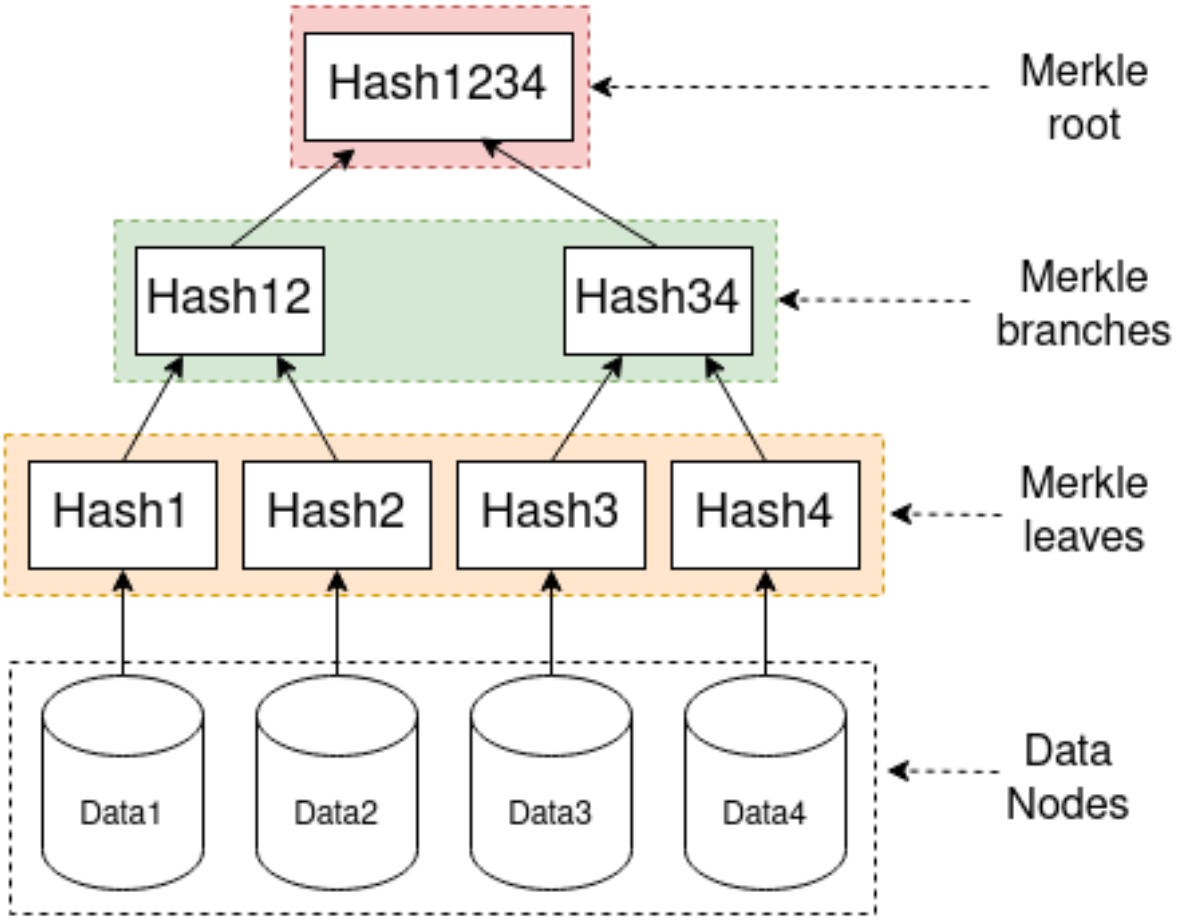
- Blockchain là một decentralized network, lưu trữ dữ liệu theo mô hình sổ cái phân tán (distributed ledger), mọi transacations được lưu trữ trong block và mỗi node được đặt trong một mạng P2P.
- Dữ liệu trong blockchain có thể được hiện thực bằng cấu trúc dữ liệu linked-list của các blocks, trong đó các transactions là có thứ tự. Mỗi block lưu trữ hai mã hash, một mã hash có vai trò như địa chỉ của chính nó và một mã hash trỏ tới block trước nó.



Hình 9: *Hình ảnh block trong blockchain*

7.2.2 Cấu trúc Merkel Tree

– Để lưu trữ các transaction trong một block, người ta sẽ sử dụng một cấu trúc dữ liệu dạng cây đặc biệt được gọi là **Merkel Tree**.



Hình 10: *Cấu trúc của Merkel Tree*

– Mỗi block bao gồm các thông tin như mã hash của previous block, timestamp, nonce, block version number, difficulty target. Cấu trúc dữ liệu Merkel Tree cùng với các thuật toán mã hóa tạo nên tính bảo mật và đảm bảo các dữ liệu trong blockchain là không thể thay đổi được sau khi dữ liệu đã được thêm vào block.

7.3 Network layer

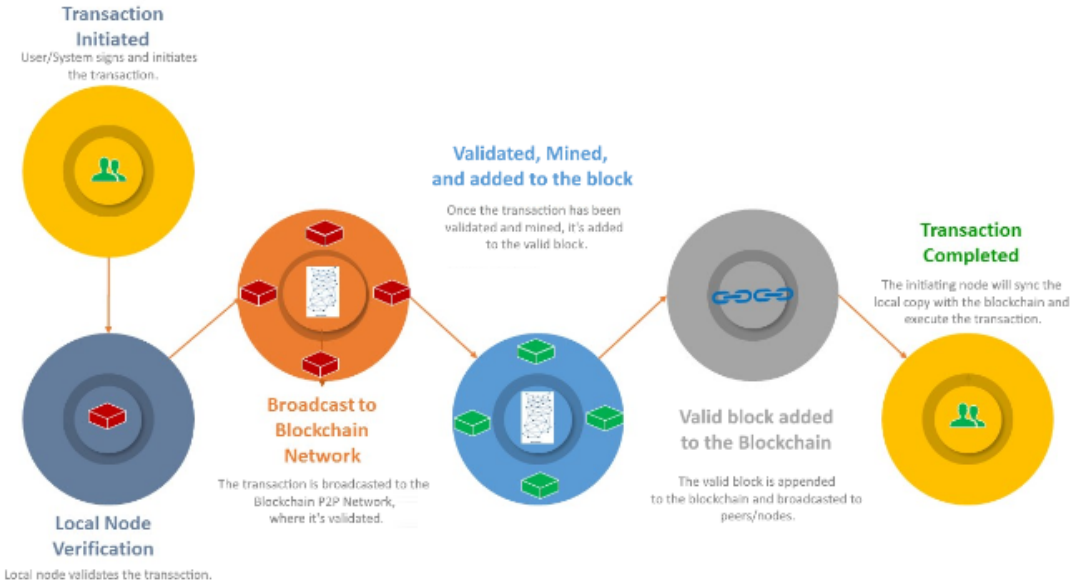
7.3.1 Mô hình P2P Network trong Blockchain

– Network layer còn được gọi là P2P layer, có trách nhiệm cho việc giao tiếp giữa các node.

– Kiến trúc của blockchain là một kiến trúc P2P network bao gồm nhiều node. Trong blockchain có hai loại node đó là light node và full node. Full node được sử dụng để xác thực và xác minh các giao dịch giữa trên các consensus rules. Trong khi đó light node được sử dụng để gửi các transactions.

7.3.2 Transaction Flow

– Transaction Flow mô tả luồng của giao dịch trong quá trình tương tác giữa các P2P node.



Hình 11: *Transaction Flow*

– Trong đó:

- **Transaction Initiated:** một light node hoặc full node chạy trên máy ảo Ethereum tiến hành thực hiện ký bằng chữ ký điện tử (digital signature) sẽ khởi tạo một transaction.
- **Local Node Verification:** Mỗi khi một Ethereum node nhận được một transaction, các local Ethereum node sẽ tiến hành kiểm tra các bước sau:
  – Kiểm tra sự tương thích giữa chữ ký số với địa chỉ người gửi và nội dung giao dịch.
  – Kiểm tra xem người gửi có đủ điều kiện để thực hiện giao dịch không (đủ coin hay không).
  – Kiểm tra xem giao dịch có thỏa mãn các smart contracts của hệ thống hay không.
- **Broadcast to Blockchain Network:** Transaction sẽ được broadcast trong blockchain P2P network để các full nodes kiểm tra các bước sau:
  – Tiếp tục kiểm tra các điều kiện ngữ nghĩa xem giao dịch có hợp lệ không.
  – Các full nodes sẽ tiến hành giao tiếp với các full node khác để xác minh giao dịch.
  – Miner node sẽ thêm giao dịch vào pending block và bắt đầu chạy ra các giải mã (consensus algorithm) như PoW, PoS để giải mã hash của block.
- **Validated, mined, and added to the block**: Tiếp theo là quy trình xác thực block.
  – Sau khi trải qua các bước trên, nếu một block đã được validated và mined, nó được xem như là một block hợp lệ (valid block).
  – Miner sẽ tiến hành giải mã và xác thực block, block sau khi được xác thực sẽ được thêm vào blockchain.
- **Valid Block added to the Blockchain:** Tiếp theo là quy trình thêm block vào blockchain.
  – Miner sẽ tiến hành thêm valid block vào blockchain.
  – Miner sẽ broadcast các block đó cho các node khác và các node lại tiếp tục xác thực block đó để đảm bảo tính nhất quán giữa block đó với địa chỉ block trước đó (previous block).
  – Mỗi khi node được thêm vào blockchain, các node sẽ tiến hành broadcast tiếp sang các node khác.

- **Transaction Completed:** Cuối cùng là quy trình thực thi giao dịch.
  - Node khởi tạo sẽ tiến hành đồng bộ với blockchain và tiến hành thực thi giao dịch.
  - Transaction sẽ được đánh giá xem như đã hoàn thành.
  - Giao dịch sau khi được thực hiện sẽ được cập nhật vào sổ cái (ledger) của các node.

7.4 Consensus layer

7.4.1 Consensus Protocol

– Consensus Protocol là phần core của mọi nền tảng blockchain. Như đã nói ở trên, đằng sau mỗi mạng blockchain đó là các consensus algorithm. Consensus layer là phần quan trọng nhất của các mạng blockchain.

– Consensus layter chịu trách nhiệm cho các hoạt động xác thực các block, sắp xếp các block và quy định một số consensus rule mà các node trong mạng blockchain phải tuân thủ trong khi thực hiện các giao dịch.

– Một số đặc điểm quan trọng của consensus layer:

- Consensus protocol quy định một số consensus rule mà các node trong mạng blockchain phải tuân thủ trong khi thực hiện các transaction.
- Consensus đảm bảo các node là đồng bộ với nhau.
- Consensus là phần quan trọng nhất để tạo nên tính chất distributed và decentralized của các node. Không có bất cứ node nào có quyền quyết định toàn bộ giao dịch trong mạng blockchain.
- Consensus Protocol được ứng dụng trong mô hình mạng P2P.

7.4.2 Consensus Algorithm

– Mỗi blockchain có một consensus algorithm khác nhau. Consensus algorithm làm nên giá trị cho tính decentrailized của blockchain.

Facts	PoW	PoS	PBFT
Type of Blockchain	Permissionless	Permissionless and Permissioned	Permissioned
Finality of Transaction	Probabilistic	Probabilistic	Deterministic
Needs Token	Yes	Yes	No
Example Usage	Bitcoin, Ethereum	Ethereum	Hyperledger Fabric

Hình 12: *Consensus Algorithm trên các mạng blockchain khác nhau*

7.5 Application layer

Application Layer của blockchain bao gồm smart contracts, chaincode và dApps (Decentralized Apps). Ngoài ra, application layers còn có thể chia thành hai sub-layers nhỏ hơn đó là application layer và execution layer.

7.5.1 Application Layer

– Application layer là tầng bao gồm những ứng dụng được sử dụng bởi các end users khi tương tác với blockchain network. Tầng ứng dụng hỗ trợ các APIs, user interface, framework cho các lập trình viên phát triển DApps.

- Trong một số ứng dụng DApps, có thể sử dụng blockchain như phần backend của hệ thống, các lập trình viên có thể kết nối với blockchain thông qua APIs.

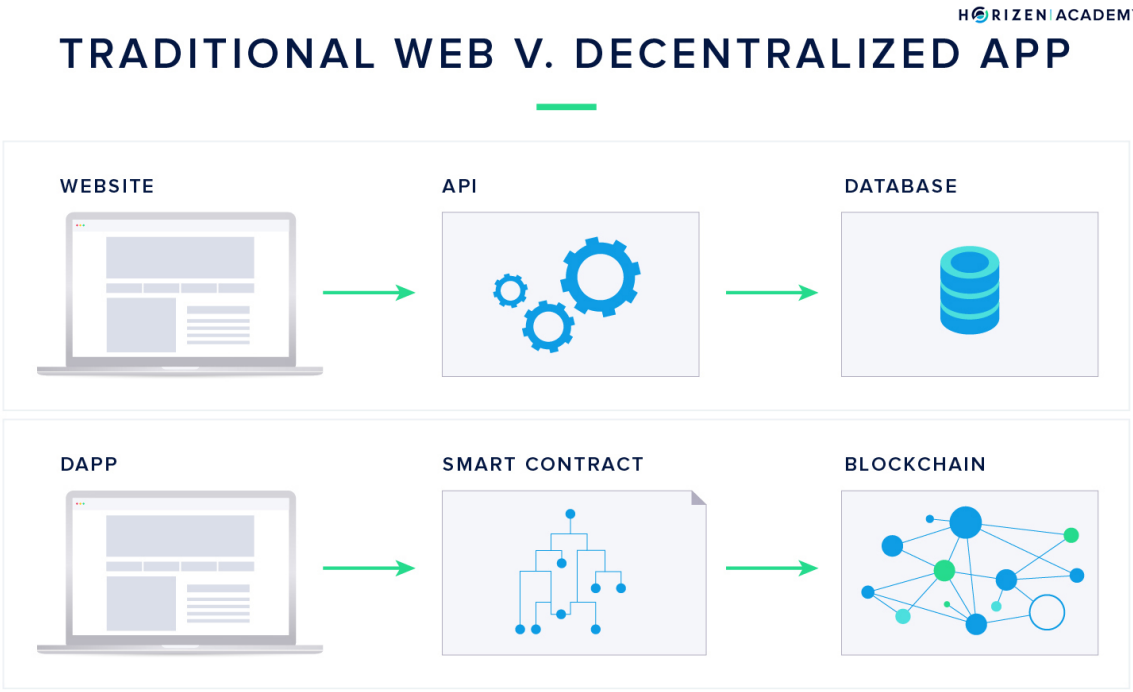
7.5.2 Execution layer

- Execution layer là tầng bao gồm các smart contracts, rules hoặc chaincode. Tầng này bao gồm các đoạn code có thể được tự động thực thi khi thỏa mãn các điều kiện precondition cho trước.
- Một transaction sẽ được gửi từ application layer sang execution layer, nơi mà transaction sẽ được xác minh và thực thi bởi các smart contracts và consensus rules.

7.5.3 DApps

1. **Smart Contracts:**
   - Smart contracts là đoạn code bao gồm một số hàm quy định các consensus rule trong quá trình xác minh các transaction. Smart contracts được thực thi trên các Ethereum runtime engine.
   - Smart contract được viết bởi high language như Solidity và được deploy to EVM ở dạng bytecode để thực thi.Smart contract cần complier để biên dịch mã nguồn. Đoạn code sẽ được biên dịch thành bytecode và được chạy trên EVM.
   - Smart contract bao gồm các hàm được tự động thực thi khi giao dịch thỏa mãn các precondition cho trước. Dựa vào phần logic của smart contract, transaction sẽ thay đổi state của contract.
   - Sau khi được deploy, một unique address sẽ được trỏ tới smart contract. Tất cả người dùng tham gia vào mạng blockchain có thể sử dụng smart contract để xác minh các transaction.
   - Một số ứng dụng có sử dụng smart contract như oracles và dApps.
2. **Oracles:**
   - Oracle có thể hiểu đơn giản như một dịch vụ bên thứ ba nhằm cung cấp các biến giá trị đầu vào cho smart contract.
3. **Chaincode:**
   - Smart contract được đóng gói với nhau trong chaincode, sau đó được deploy lên mạng blockchain.
   - Chaincode hỗ trợ các tính năng như khởi tạo, cập nhật, thực hiện các lệnh query data trong ledger.
4. **DApps:**
   - Decentralized Application (hay còn gọi là dApps) là ứng dụng được hiện thực theo kiến trúc phi tập trung (decentralized), chạy trên các nền tảng công nghệ blockchain như Ethereum, Bitcoin hoặc Hyperledger Fabric. DApps có thể được xem như một ứng dụng web cho phép client tương tác với smart contract và chaincode.
   - Điểm nổi bật của DApps là nó không phụ thuộc duy nhất vào bất cứ bên thứ ba, các node tham gia vào DApps đều có quyền bình đẳng như nhau.
   - Sau khi được deploy, dApps phụ thuộc vào blockchain network. Sau khi client kết nối vào mạng blockchain, client có thể sử dụng dApps để thực hiện các transaction, các transaction đó sẽ được xác thực bằng smart contracts và chaincode ở dưới.

- Khác với các loại ứng dụng bình thường, DApps là một API-based web application kết nối trực tiếp với smart contracts, tiến hành thực thi các transaction trong ledger.
- Một số ứng dụng DApps phổ biến có thể kể đến các ứng dụng trong lĩnh vực kinh tế như invoice factoring, KYC,...



Hình 13: *Mô hình DApps trong Blockchain*

8 Một số consensus algorithm trong Blockchain

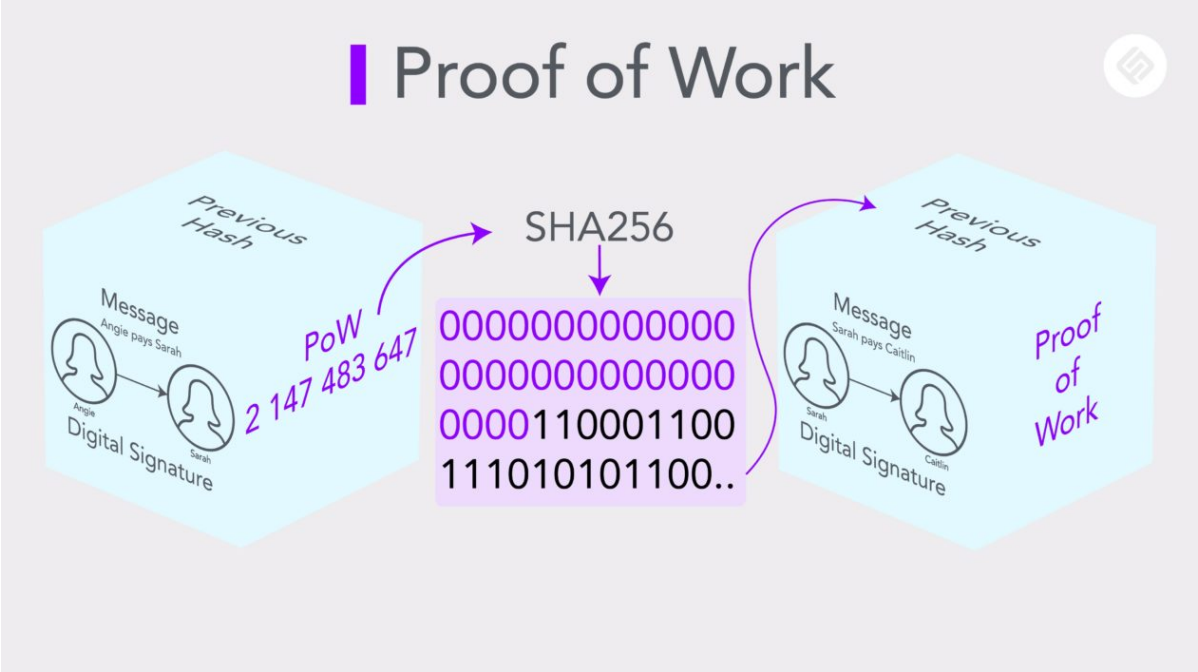
8.1 Proof of Work (PoW)

8.1.1 Cơ chế hoạt động

- Đây là một trong những consensus algorithm đầu tiên. PoW được sử dụng trong Bitcoin và các loại tiền điện tử khác. PoW là một thuật toán xác minh các giao dịch trong block và thêm chúng vào blockchain khi nhận được sự đồng thuận của các node tham gia.
- Trong PoW, quá trình thêm một block vào blockchain được gọi là mining, và các nodes tham gia vào quá trình mining được gọi là miners. Trước khi miner thêm block vào blockchain, PoW sẽ yêu cầu miners giải mã của block đó (hay còn gọi là solve a puzzle). Khi giải mã thành công sẽ góp phần xác thực giao dịch, miners sẽ nhận được một phần thưởng cho công sức giải mã của mình được gọi là rewards.
- Tất cả mọi người trong mạng blockchain đều có thể tham gia vào quá trình mining, hay còn được gọi là trở thành miners.
- Việc giải mã của miners là tìm ra được mã hash chính xác của block cần xác thực. Trong một thời điểm có thể có nhiều người cùng tham gia giải mã, nhưng chỉ người giải được kết quả nhanh nhất mới nhận được phần thưởng, sau khi việc giải mã thành công, mã của block đó sẽ được broadcast

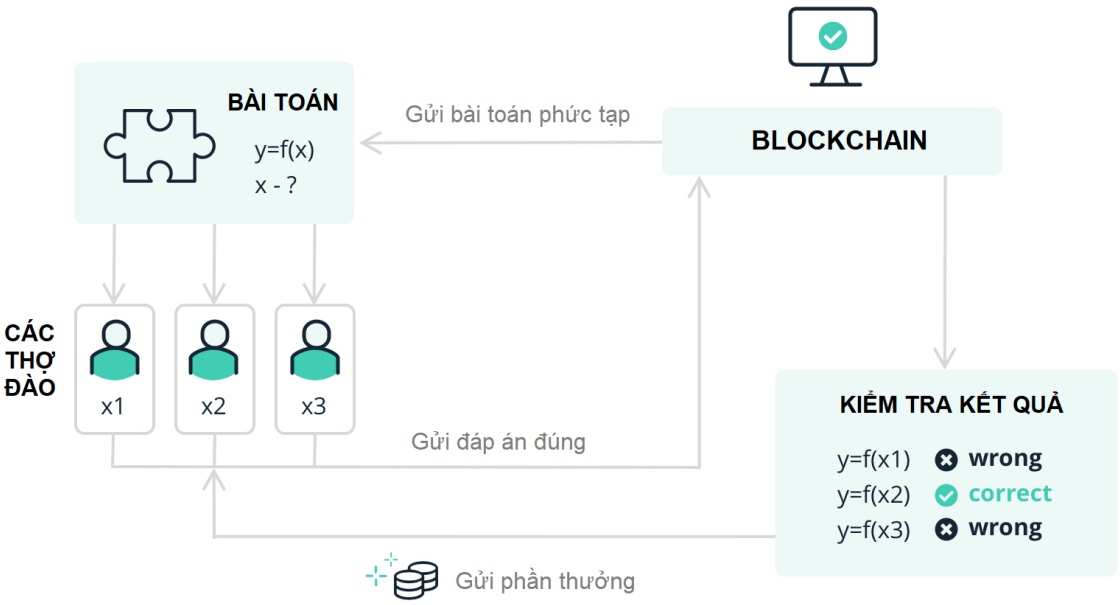
cho các nodes khác trong mạng blockchain. Lúc này các node khác sẽ tiến hành xác minh giao dịch đó một lần nữa trước khi block đó được thêm vào blockchain.

– Thuật toán này được gọi là Proof of work bởi vì nó tiêu tốn nhiều thời gian, công sức, tài nguyên của các máy để chạy và giải mã hash từ các thuật toán phức tạp như SHA256.



Hình 14: *Mô hình PoW*

– Dưới đây là quy trình hoạt động của PoW.



Hình 15: *Thuật toán PoW trong Blockchain*

8.1.2 Ưu điểm và nhược điểm

1. **Ưu điểm**

   - **Đảm bảo sự an toàn của toàn mạng lưới:** Với khối lượng công việc lớn cần phải giải quyết thì việc hack vào một blockchain theo cơ chế Proof of Work là không thể. Khi một hệ thống ngày càng phát triển, số lượng giao dịch ngày càng tăng thì việc tấn công vào mạng lưới sẽ ngày càng khó.
   - **Thúc đẩy đội ngũ miners:** Với việc thưởng cho các thợ đầu giải quyết block đầu tiên, PoW sẽ khuyến khích các thợ đầu làm việc nghiêm túc, nhanh chóng và chính xác.
   - **Độ chính xác:** PoW giúp các thông tin trên Blockchain được cập nhật một cách chính xác, minh bạch và phi tập trung.

2. **Nhược điểm**

   - **Thời gian giao dịch chậm:** Với việc mỗi block chỉ chứa được một số lượng giao dịch và các giao dịch phải chờ sau một khoảng thời gian để block được thành lập để xác nhận giao dịch thì khi mạng lưới ngày càng mở rộng và số lượng giao dịch ngày càng nhiều dẫn đến thời gian giao dịch tương đối chậm.
   - **Không hoàn toàn phi tập trung:** Bởi vì phần thưởng chỉ dành cho các thợ đào đầu tiên và các thợ đào khác không có thu nhập nên các thợ đào có xu hướng kết hợp lại với nhau, tạo nên các mining pool để có thể có một sức mạnh đủ lớn để tới đích trước. Việc này sẽ tạo ra một hệ quả khi một mining pool quá lớn (trường hợp tấn công 51%) tổng số máy đào thì việc xác minh giao dịch sẽ không còn phi tập trung nữa và có thể bị thao túng bởi chính mining pool đó gây ra tính không mình bạch cho mạng lưới.
   - **Tiêu hao nhiều tài nguyên:** với việc một mạng lưới càng phát triển, số lượng giao dịch ngày càng nhiều thì bài toán ngày càng khó giải. Việc càng nhiều năng lượng hơn để giải bài toán đó là một vấn đề nan giải đôi khi năng lượng cung cấp cho máy đào Bitcoin có thể bằng một năng lượng cho một quốc gia nhỏ.

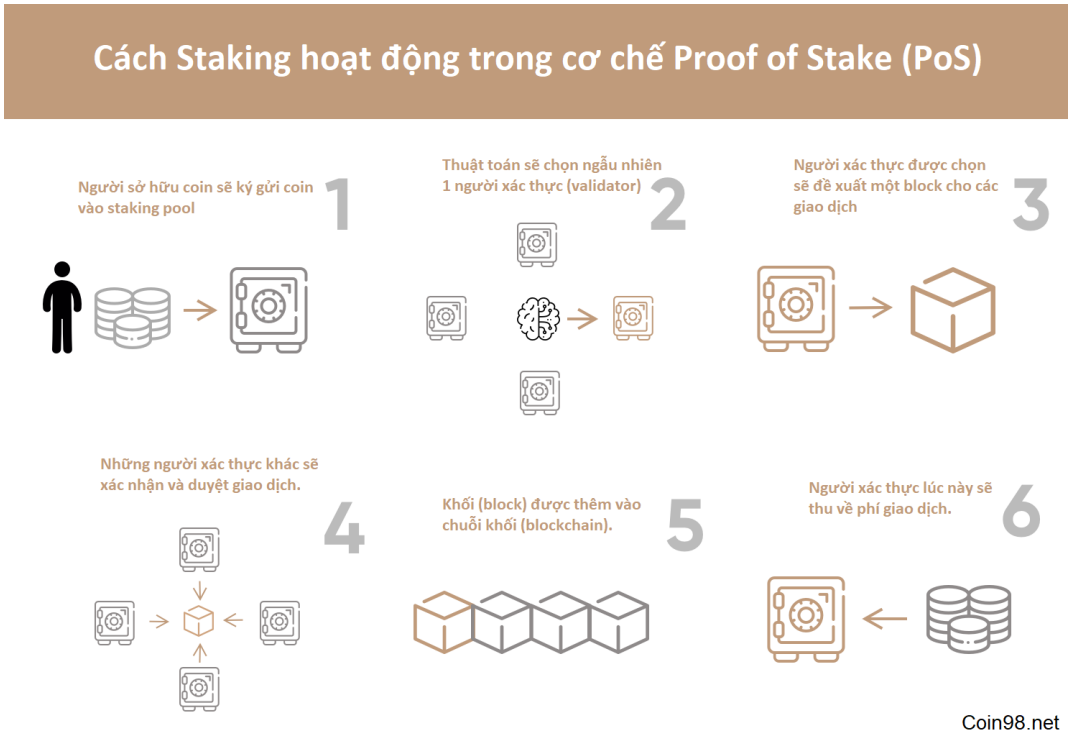
8.2 Proof of Stake (PoS)

8.2.1 Cơ chế hoạt động

– Cũng như PoW, PoS là một trong những consensus algorithm dùng để xác thực block và thêm block vào blockchain. Tuy nhiên một trong nhũng điểm khác biệt lớn nhất là người dùng cần phải đầu tư một một lượng tài sản nhất định (stake) để trở thành validator của Blockchain.

– Không giống như Proof of Work (được sử dụng bởi Bitcoin), người dùng không cần phần cứng mining đắt tiền hoặc lượng điện lớn. Thay vào đó, mạng lưới lựa chọn các cá nhân để tham gia vào quá trình xác nhận các block dựa trên lượng coin mà họ sở hữu. Lượng coin sở hữu càng cao, người dùng càng có nhiều khả năng được chọn để validate - do đó có tên là Proof of Stake. Việc này nhằm giảm tải số lượng miners tham gia quá lớn như PoW.

– Các Validator này sẽ xác minh các giao dịch và gửi các kết quả mình đã tìm ra. Nếu đúng, họ sẽ nhận được rewards là phần thặng dư của giao dịch, ngược lại họ sẽ bị mất phần tiền mình đã cược vào.



Hình 16: *Mô hình mining trong Bitcoin*

8.2.2 Ưu điểm và nhược điểm

1. **Ưu điểm**
   - Tiết kiệm năng lượng.
   - Xử lý giao dịch nhanh chóng và không tốn kém.
   - Không yêu cầu thiết bị phần cứng quá mạnh để tham gia.
   - Giảm tải được cơ chế centralize.
2. **Nhược điểm**
   - Khi đã trở thành Validator, bạn sẽ được nhận thưởng từ việc xác thực, nhưng bị giảm vốn. Đôi khi sẽ bị thâm hụt mất phần đã stake ban đầu.
   - Validator nắm lượng lớn có thể ảnh hưởng đến xác minh giao dịch. Giống như người có quyền hạn lớn, tiếng nói có trọng lượng hơn. Đây là lý do vì sao, Validator cần ủy thác token cho họ.
   - Một số loại token dùng PoS yêu cầu Unlock 1 khoảng thời gian ngắn (1,2 tuần). Điều này khó trong việc điều chỉnh giá token.

9 Một số loại mạng Blockchain

9.1 Public Blockchain

9.1.1 Khái niệm

Đây là một nền tảng blockchain mà bất kỳ ai cũng có quyền truy cập và ghi dữ liệu trên chuỗi. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có hàng nghìn hay thậm chí là hàng vạn nút tham gia. Do đó để tấn công vào hệ thống Blockchain này là điều bất khả thi vì chi phí rất cao. Ví dụ về Public blockchain phổ biến như Bitcoin hay Ethereum,...

9.1.2 Một số đặc điểm

- Khả năng truy cập: Không giới hạn.
- Tốc độ truy cập: Chậm.
- Khả năng bảo mật: Proof of Work hoặc Proof of State.
- Xác định danh tính: Ẩn danh.
- Loại giao dịch: Giao dịch cơ bản.
- Chi phí khởi tạo: Rẻ, chỉ cần tham gia và xây dựng ứng dụng.
- Chi phí giao dịch: Đắt.

9.1.3 Ưu điểm và nhược điểm

1. **Ưu điểm**
   - **Tính đáng tin cậy:** Public blockchain hoàn toàn không có sự tham gia của bên thứ 3 nên đã loại bỏ được những rủi ro do bên trung gian gây ra dưới bất kỳ hình thức nào. Vì vậy trên thực tế, những người tham gia giao dịch không cần phải đặt niềm tin ở bất kỳ ai mà yêu cầu vẫn được xử lý và bảo mật.
   - **Tính an toàn:** Có rất nhiều nút tham gia vào quá trình xác thực Public Blockchain nên muốn tấn công hệ thống này là hoàn toàn không khả thi. Các yếu tố xấu không thể tập hợp và làm việc cùng nhau để giành quyền kiểm soát mạng lưới đồng thuận.
   - **Tính minh bạch:** Tất cả các tính năng trên Public Blockchain đều công khai và vô cùng minh bạch. Dữ liệu liên quan đến giao dịch đều được mở cho cộng đồng xác minh. Ngoài ra, bất kỳ ai cũng có thể truy xuất dữ liệu để kiểm tra tính hợp lệ của giao dịch đó.
   - **Tính không bị quản lý:** Public Blockchain có thể chống lại sự kiểm duyệt do quy mô mạng lưới quá rộng, hơn nữa còn đa quốc tịch. Chính phủ không thể nào điều khiển và kiểm soát được.
2. **Nhược điểm**
   - **Tốc độ xử lý chậm:** Public Blockchain phải mất thời gian cho toàn mạng để đạt được sự đồng thuận về một trạng thái giao dịch nên tốc độ xử lý sẽ bị ảnh hưởng. Ngoài ra Public Blockchain còn giới hạn về số lượng giao dịch có thể phù hợp cũng như thời gian cần thiết để xử lý một khối duy nhất.
   - **Tiêu hao năng lượng:** Các thuật toán đồng thuận của Public Blockchain yêu cầu tiêu hao một nguồn năng lượng đáng kể, điều này đã làm dấy lên những lo ngại về mặt môi trường. Đã từng có khảo sát cho thấy rằng, Bitcoin đang tiêu thụ số điện năng tương đương với của quốc gia Ireland.

9.2 Private Blockchain

9.2.1 Khái niệm

Private Blockchain là nền tảng chỉ cho phép người dùng được đọc dữ liệu, không có quyền ghi. Quyền ghi này sẽ thuộc về một tổ chức thứ 3 hoàn toàn đáng tin cậy. Bên thứ ba này có thể hoặc không

cho phép người dùng đọc dữ liệu trong một số trường hợp. Bên thứ ba toàn quyền quyết định mọi thay đổi trên Blockchain. Ví dụ Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.

9.2.2 Một số đặc điểm

- Khả năng truy cập: Phân quyền đọc/ghi.
- Tốc độ truy cập: Nhanh.
- Khả năng bảo mật: Pre-approved participants.
- Loại giao dịch: Tất cả các giao dịch.
- Chi phí khởi tạo: Đắt do tự xây dựng mạng lưới.
- Chi phí giao dịch: Rẻ.

9.2.3 Ưu điểm và nhược điểm

1. **Ưu điểm**
   - **Tốc độ xử lý nhanh:** So với Public Blockchain, số lượng giao dịch mà Blockchain xử lý được cao hơn rất nhiều. Nó có thể xử lý hàng ngàn hoặc thậm chí hàng trăm ngàn giao dịch mỗi giây so với 7 TPS của Bitcoin.
   - **Dễ mở rộng:** Do chỉ có một vài nút ủy quyền và chịu trách nhiệm quản lý dữ liệu, mạng có thể hỗ trợ mở rộng để tăng thêm tốc độ xử lý các giao dịch.
2. **Nhược điểm**
   - **Cần phải có sự tin tưởng giữa các node:** Nếu như Public Blockchain không yêu cầu bạn phải tin tưởng ai thì tính toàn vẹn của mạng riêng tư lại phụ thuộc vào độ tin cậy của các nút được ủy quyền. Ngoài ra, tính hợp lệ của một hồ sơ không thể được xác minh độc lập. Các tác nhân bên ngoài phải hoàn toàn tin tưởng Private Blockchain mà không có bất kỳ hình thức kiểm soát nào đối với quá trình xác minh.
   - **Tính bảo mật thấp:** Cũng dễ hiểu bởi vì vận hành càng với ít nút thì khả năng bị xâm nhập lại càng cao. Một mạng riêng dễ bị thao túng dữ liệu hơn nhiều so với mạng công khai.
   - **Tính tập trung hóa:** Các Private Key phải được xây dựng và duy trì bởi một dự án, một doanh nghiệp hay một tập đoàn.

9.3 Consortium Blockchain

9.3.1 Khái niệm

Consortium là sự kết hợp giữa Public Blockchain và Private Blockchain. Nó kết hợp giữa "niềm tin" khi tham gia vào Public và "niềm tin tuyệt đối" khi tham gia vào Private. Trong mạng này, một số bên có quyền lực ngang nhau sẽ hoạt động như các trình xác nhận. Ví dụ các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

9.3.2 Một số đặc điểm

- Quy tắc hệ thống linh hoạt: Khả năng hiển thị của chuỗi có thể giới hạn ở các trình xác nhận, có thể được xem bởi những cá nhân được ủy quyền hoặc cũng có thể là tất cả.
- Tiết kiệm chi phí giao dịch: Tuy Public Blockchain luôn được biết đến là loại nền tảng có chi phí giao dịch thấp nhất. Tuy nhiên càng nhiều người tham gia, giao dịch càng chậm thì hiệu quả cuối cùng so với Consortium Blockchain lại có phần không bằng. Ở đây, các giao dịch nhanh hơn và ít phức tạp hơn nhiều. Vì vậy giá thành tổng thể giảm đi đáng kể.
- Bảo mật: Vừa công khai được một số dữ liệu, vừa giữ những thông tin khác được bảo mật trong hệ thống tư.

9.3.3 Ưu điểm và nhược điểm

1. **Ưu điểm**
   - Consortium là sự kết hợp giữa Public Blockchain và Private Blockchain, do đó kế thừa được ưu điểm và khắc phục được một số nhược điểm của hai loại blockchain trên.
2. **Nhược điểm**
   - Bên cạnh một số ưu điểm nói trên, còn một số nhược điểm của hai loại blockchain phía trên chưa khắc phục được ví dụ như trường hợp tấn công 51%.

10 Một số ứng dụng của Blockchain

10.1 Bitcoin

10.1.1 Nguyên nhân ra đời của tiền mã hóa

1. **Vấn đề của giao dịch truyền thống**
   - Với giao dịch truyền thống thông thường, khi bạn muốn chuyển tiền cho bất kỳ ai hay muốn cất trữ tiền của mình thì đều sẽ phải thông qua một bên trung gian, đó chính là ngân hàng. Mô hình này được gọi là mô hình tập trung, khi tất cả các thông tin giao dịch, nguồn tiền cất trữ, cũng như vấn đề bảo mật đều sẽ do một bên duy nhất chịu trách nhiệm đó chính là ngân hàng.
   - Tuy nhiên, đó cũng là một vấn đề, vì nếu hacker muốn chiếm đoạt tài sản của chúng ta, chúng chỉ cần tấn công một mục tiêu duy nhất đó là máy chủ ngân hàng để có thể chiếm đoạt được tài sản đó. Tiếp theo nữa là việc hầu hết các ngân hàng thường chỉ lưu thông tin của chúng ta duy nhất (không có bản sao), nên nếu máy chủ của ngân hàng đó có vấn đề gì – ví dụ như hỏa hoạn, hay việc nhập liệu của nhân viên gặp sai sót, thì rất khó có bản sao hay tài liệu khác để xác nhận lại, dẫn đến việc chúng ta có thể bị thất thoát tài sản.
2. **Giải pháp cho các giao dịch truyền thống - Bitcoin**
   - Với những vấn đề do giao dịch tập trung còn tồn đọng, bằng cách ứng dụng công nghệ blockchain. Một hình thức lưu trữ thông tin giao dịch mới đã ra đời, được gọi là hình thức giao dịch phi tập trung. Giúp thông tin giao dịch của chúng ta được xác thực và lưu trữ ở rất nhiều máy tính khác nhau trên toàn thế giới và được mã hóa/bảo mật bằng công nghệ

blockchain, nhờ đó mà việc bị hacker tấn công hay việc bị sai khác dữ liệu sẽ gần như không thể xảy ra. Và việc mã hóa thông tin để giao dịch đó bằng công nghệ blockchain đã tạo ra tiền mã hóa.

Hình 17: *Đồng tiền Bitcoin*

10.1.2 Quy trình chi tiết quá trình đào coin

- **Bước 1: Băm các giao dịch (Hashing)**
  - Bước đầu tiên của việc khai thác một khối là nhận các giao dịch đang chờ được xử lý từ nhóm bộ nhớ và gửi từng giao dịch thông qua một hàm băm (hash function). Một khi chúng ta gửi một phần dữ liệu thông qua một hàm băm, chúng ta sẽ tạo ra một đầu ra có kích thước cố định được gọi là mã băm. Mã băm của giao dịch bao gồm một chuỗi số và chữ cái hoạt động như một định danh. Mã băm giao dịch đại diện cho tốt cả thông tin có trong giao dịch đó
- **Bước 2: Tạo cây Merkle**
  - Sau khi mọi giao dịch được băm, các mã băm sau đó được tổ chức thành một cấu trúc dữ liệu gọi là Merkle Tree. Còn được gọi là cây băm, Cây Merkle được hình thành bằng cách sắp xếp các mã băm giao dịch thành từng cặp và sau đó băm chúng.
  - Các đầu ra băm mới sau đó được tổ chức thành từng cặp và băm lại một lần nữa, và quá trình này được lặp lại cho đến khi tạo ra một hàm băm duy nhất. Hàm băm cuối cùng này còn được gọi là mã băm gốc (hoặc Merkle root) và về cơ bản là hàm băm đại diện cho tất cả các hàm băm trước đó đã được sử dụng để tạo ra nó.
- **Bước 3: Tiến hành tìm tiêu đề khối (header block)**
  - Tiêu đề khối (block header) hoạt động như một mã định danh cho từng khối riêng lẻ, có nghĩa là mỗi khối có một mã băm duy nhất. Khi tạo một khối mới, các thợ đào kết hợp mã băm của khối trước đó với mã băm gốc của khối ứng viên của họ để tạo ra một mã băm khối mới.Nhưng ngoài hai yếu tố này, họ cũng cần thêm một thứ gọi là nonce.

- Vì vậy, khi cố gắng xác thực khối ứng viên của họ, thợ đào cần kết hợp hàm băm gốc, mã băm của khối trước đó và một nonce và gửi tất cả chúng thông qua một hàm băm. Mục tiêu của họ là tạo ra một mã băm được coi là hợp lệ.
- Không thể thay đổi mã băm gốc và mã băm của khối trước đó, vì vậy thợ đào cần thay đổi giá trị nonce nhiều lần cho đến khi tìm thấy mã băm hợp lệ.
- Để được coi là hợp lệ, đầu ra (mã băm khối) phải nhỏ hơn một giá trị đích nhất định, được xác định bởi giao thức. Khi đào Bitcoin, mã băm khối phải bắt đầu bằng một số không nhất định. Đây là những gì chúng ta gọi là khó khăn trong khai thác

- **Bước 4: Broastcard khối đã đào**
  - Như chúng ta vừa thấy, các thợ đào cần phải băm tiêu đề khối nhiều lần, với các giá trị nonce khác nhau. Họ lặp đi lặp lại công việc này cho đến khi tìm thấy một mã băm khối hợp lệ. Thợ đào tìm thấy mã băm hợp lệ sau đó sẽ phát khối của mình lên mạng. Tất cả các node khác sẽ kiểm tra xem khối và mã băm của nó có hợp lệ hay không và nếu có, khối mới sẽ được thêm vào blockchain bản sao mà các node này lưu giữ.
  - Tại thời điểm này, khối ứng cử viên trở thành một khối được xác thực và tất cả các thợ đào chuyển sang khai thác khối tiếp theo. Tất cả những thợ đào không thể tìm thấy mã băm hợp lệ đúng lúc sẽ loại bỏ khối ứng viên của họ và cuộc đua khai thác lại bắt đầu.

10.1.3 Một số ưu điểm và nhược điểm của Bitcoin

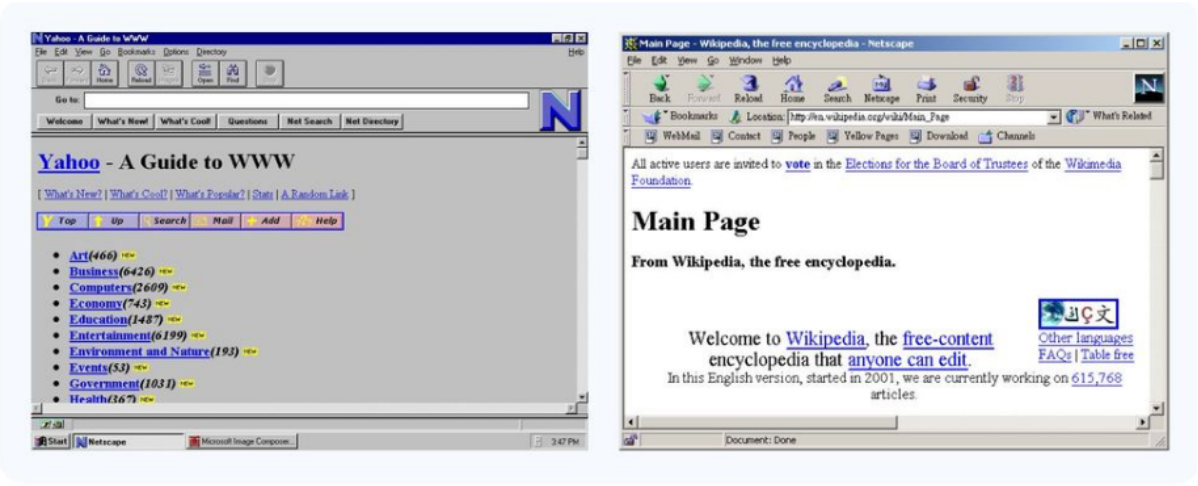
1. **Ưu điểm**
   - **Giao dịch nhanh chóng:** Người sử dụng có thể nhận tiền và chuyển tiền mọi lúc mọi nơi một cách nhanh chóng.
   - **Chi phí giao dịch thấp:** Chi phí giao dịch của tiền điện tử hầu hết là miễn phí hoặc phí rất thấp.
   - **Tính an toàn, bảo mật:** Thông tin của khách hàng sẽ được bảo mật một cách tốt nhất. Với công nghệ tiên tiến, việc gian lận sẽ được hạn chế và không phải phụ thuộc vào bên trung gian.
   - **Tính minh bạch:** Với công nghệ blockchain, mọi thông tin giao dịch đều được lưu trữ trong chuỗi khối. Do đó, 2 bên giao dịch hoàn toàn có thể xác minh và theo dõi tiền điện tử một cách dễ dàng và nhanh chóng.
2. **Nhược điểm**
   - **Rủi ro xuất hiện tội phạm:** Bởi vì hoạt động dưới trạng thái ẩn danh, nên tiền mã hóa rất khó kiểm soát. Tội phạm có thể sử dụng lợi thế này để thực hiện hành vi rửa tiền.
   - **Khó dự đoán:** Biên độ dao động giá của tiền điện tử là rất lớn. Điều này gây rủi ro cho người nắm giữ vì đồng tiền có thể rớt giá rất mạnh.
   - **Giá trị chưa ổn định:** do nguồn cung và nhu cầu sử dụng đang chưa thật sự ổn định. Cũng như tuổi đời non trẻ của các loại tiền ảo dẫn đến việc các cơ sở pháp lý của nhà nước đối với loại tiền này vẫn chưa được ban hành cụ thể. Dẫn đến việc có rất nhiều người lợi dụng việc này mà bán những loại tiền mã hóa không có giá trị gì nhằm thu lợi bất chính.

10.2 Web 3.0

10.2.1 Nguyên nhân ra đời của Web 3.0

1. **Web 1.0**

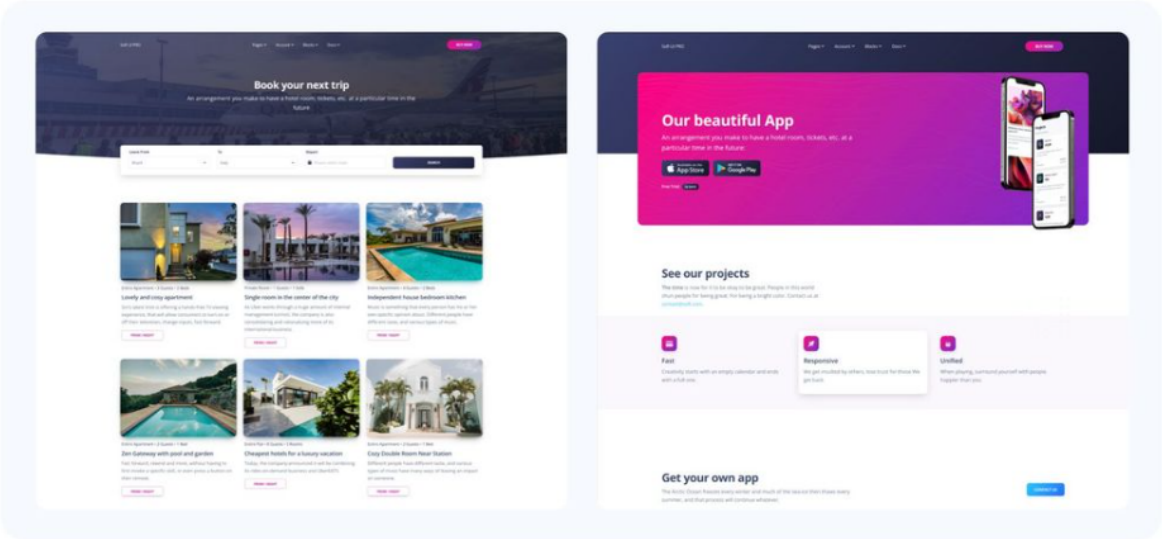
   - Được gọi là thế hệ web hiển thị thông tin (static website). Web 1.0 đời vào năm 1989 cùng với sự xuất hiện của internet. Web 1.0 đã tạo ra một nơi giúp người dùng có thể tiếp cận thông tin tự xa thông qua internet một cách dễ dàng hơn.
   - Tuy nhiên, Web 1.0 lúc đó căn bản là chỉ là những dòng text được gắn thêm các đường link dẫn đến các bài khác. Người dùng hầu hết chỉ là những người tra cứu thông tin (consumers) và không thể tương tác với nội dung mình đọc được. Việc sáng tạo nội dung để đăng lên web cũng rất bị hạn chế vào thời điểm đó.



Hình 18: *Web 1.0*

2. **Web 2.0**

   - Cùng với sự phát triển của internet và số lượng người dùng, các nhu cầu mới trên nền tảng web cũng phát sinh. Thế hệ web 2.0 phát triển mạnh mẽ cho tới tận ngày nay. Web 2.0 khắc phục được việc truyền tải thông tin một chiều, cho phép người dùng tương tác với trang web theo các yêu cầu riêng biệt.
   - Với web 2.0 người dùng có thể đăng ký tài khoản, bình luận, tạo bài viết, post video trên youtube hay tạo trang mạng xã hội riêng của mình trên Facebook... Về mặt công nghệ thì có thể hiểu web 2.0 là những web có mã nguồn gồm cả phần front end và back end tức là có thêm ngôn ngữ server kèm theo như PHP, Node JS, Java,... cùng với một hệ quản trị cơ sở dữ liệu như Mysql, Mongodb,...
   - Tuy nhiên sau một thời gian dần dần các ông lớn công nghệ như Twitter, Facebook,... dần thống trị web 2.0 và họ đã khai thác thông tin người dùng để triển khai các dịch vụ khác như quảng cáo để kiếm lợi cho bản thân. Dù bạn là người góp phần xây dựng nên web 2.0 nhưng nó lại thuộc về các ông lớn trên. Chính vì còn một số bất cập của web 2.0 nên web 3.0 đã ra đời nhằm giải quyết các vấn đề đó.



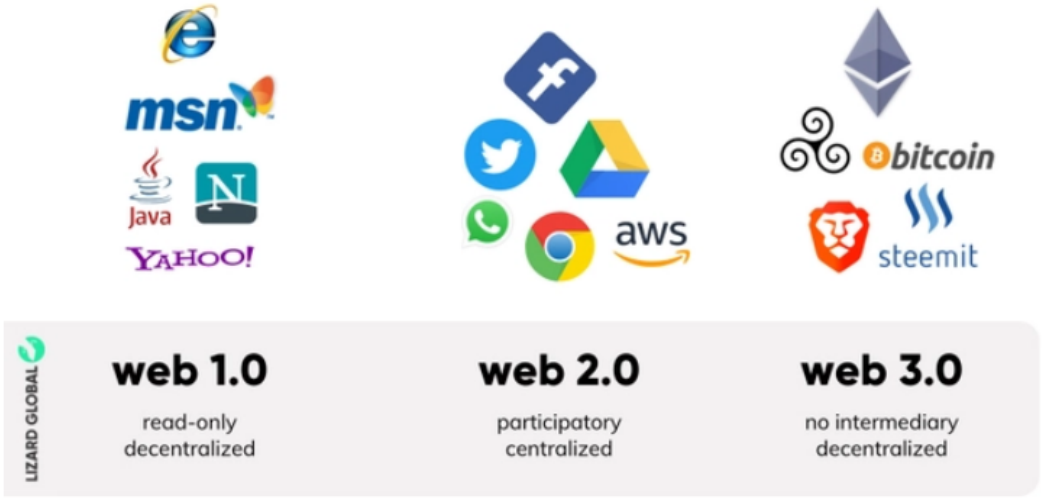
Hình 19: *Web 2.0*

3. **Web 3.0**

   – Web 3.0 (còn được gọi là web3), là thế hệ thứ ba của các dịch vụ Internet kết nối dữ liệu với nhau theo cách phi tập trung để mang lại trải nghiệm người dùng nhanh hơn và được cá nhân hóa hơn. Web 3.0 được xây dựng bằng trí tuệ nhân tạo (AI), máy học (machine learning) và web ngữ nghĩa (Semantic Web), đồng thời sử dụng hệ thống bảo mật blockchain để giữ cho thông tin được an toàn và bảo mật.

   – Web 3.0 là phiên bản nâng cao của Web 2.0, hứa hẹn sẽ linh động hơn với tính tương tác cao hơn. Bằng cách triển khai trí tuệ nhân tạo và công nghệ blockchain, Web 3.0 sẽ xác định lại trải nghiệm web với những thay đổi về cấu trúc để nâng cao trải nghiệm người dùng.

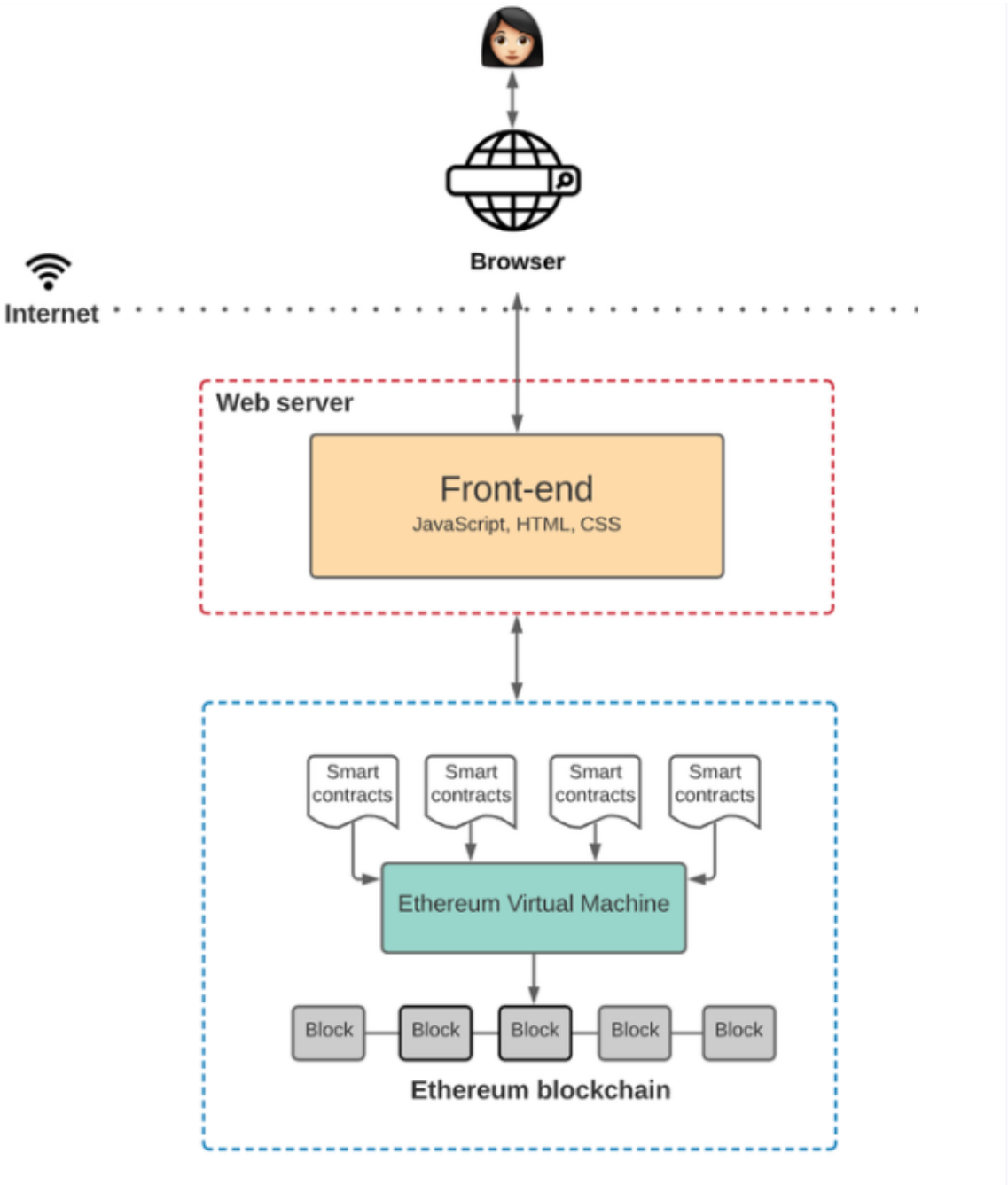
   – Trong Web 3.0, dữ liệu được lưu trữ an toàn và được phân phối trên nhiều thiết bị, loại bỏ nhu cầu về các máy chủ tập trung. Thiết kế này cũng làm giảm nguy cơ rò rỉ dữ liệu lớn vì dữ liệu không còn được lưu trữ tập trung - làm cho nó trở nên linh hoạt hơn và ít bị xâm phạm hơn.



Hình 20: *Bảng so sánh các loại web 1.0, web 2.0 và web 3.0*

10.2.2 Cơ chế hoạt động của web 3.0

- Web 3.0 không có cơ sở dữ liệu tập trung lưu trữ trạng thái ứng dụng cũng như không có máy chủ web tập trung nơi chứa logic backend. Thay vào đó, có một blockchain để xây dựng ứng dụng trên một máy trạng thái phi tập trung và được duy trì bởi các nút ẩn danh trên web.
- Logic của các ứng dụng của bạn được xác định trong các Smart Contracts, được viết bởi các nhà phát triển, được triển khai trên mô hình phi tập trung. Giao diện chương trình vẫn có thể được hiện thực bằng các công nghệ trong web 2.0.



Hình 21: *Kiến trúc Web3*

– Kiến trúc Web3 bao gồm các thành phần chính sau:

- **Ethereum Blockchain**: Đây là các máy trạng thái có thể truy cập toàn cầu được duy trì bởi một mạng lưới các nút ngang hàng. Bất kỳ ai trên thế giới đều có thể truy cập vào máy trạng thái và ghi vào nó. Về cơ bản, nó không thuộc sở hữu của bất kỳ thực thể nào mà là của tất cả mọi người trong mạng. Người dùng có thể ghi vào Ethereum Blockchain, nhưng họ không bao giờ có thể cập nhật dữ liệu hiện có.
- **Smart Contracts**: Đây là các chương trình chạy trên Ethereum Blockchain. Chúng được viết bởi các nhà phát triển ứng dụng bằng các ngôn ngữ cấp cao, chẳng hạn như Solidity hoặc Vyper, để xác định logic đằng sau các thay đổi trạng thái.
- **Máy ảo Ethereum (EVM)**: Mục đích của các máy này là thực thi logic được xác định trong các Smart Contracts. Chúng xử lý các thay đổi trạng thái diễn ra trên máy trạng thái.
- **Front-end (Giao diện người dùng)**: Giống như bất kỳ ứng dụng nào khác, giao diện người dùng xác định logic giao diện người dùng. Tuy nhiên, nó cũng kết nối với các Smart Contracts xác định logic ứng dụng.

10.2.3 Một số ưu điểm và nhược điểm của web 3.0

1. **Ưu điểm**

   – **Quyền riêng tư và kiểm soát dữ liệu:** Người dùng cuối sẽ nhận được lợi thế quan trọng nhất của mã hóa dữ liệu để bảo vệ thông tin của họ khỏi bị tiết lộ. Mã hóa sẽ không thể phá vỡ trong bất kỳ trường hợp cụ thể nào. Nó sẽ ngăn các tổ chức lớn như Google và Apple kiểm soát hoặc sử dụng thông tin cá nhân của mọi người vì lợi ích riêng của họ. Do đó, người dùng sẽ có toàn quyền sở hữu và quyền riêng tư đối với thông tin của họ.

   – **Dịch vụ liền mạch:** Lưu trữ dữ liệu phi tập trung sẽ đảm bảo rằng người dùng có thể truy cập dữ liệu trong bất kỳ trường hợp nào. Người dùng sẽ nhận được nhiều bản sao lưu, điều này có lợi cho họ ngay cả trong trường hợp máy chủ bị lỗi. Ngoài ra, không thực thể hoặc tổ chức chính phủ nào có khả năng dừng bất kỳ dịch vụ hoặc trang web nào. Do đó, khả năng bị tạm ngưng tài khoản và từ chối các dịch vụ được phân phối sẽ được giảm bớt.

   – **Tính minh bạch:** Bất kể người dùng cuối sử dụng nền tảng blockchain nào, họ sẽ theo dõi dữ liệu của mình và kiểm tra mã đằng sau nền tảng. Các tổ chức phi lợi nhuận phát triển phần lớn các nền tảng blockchain, có nghĩa là họ cung cấp một nền tảng blockchain mã nguồn mở cho phép các quy trình thiết kế và phát triển mở. Điều này sẽ giúp loại bỏ sự phụ thuộc của người dùng vào tổ chức phát triển nền tảng.

   – **Khả năng tiếp cận dữ liệu mở:** Dữ liệu sẽ có thể truy cập được từ mọi nơi và từ mọi thiết bị. Tăng cường thu thập dữ liệu và khả năng tiếp cận của nó đối với người dùng trên toàn thế giới bằng cách cho phép điện thoại thông minh và các thiết bị được kết nối khác truy cập dữ liệu trên máy tính nếu được đồng bộ hóa.

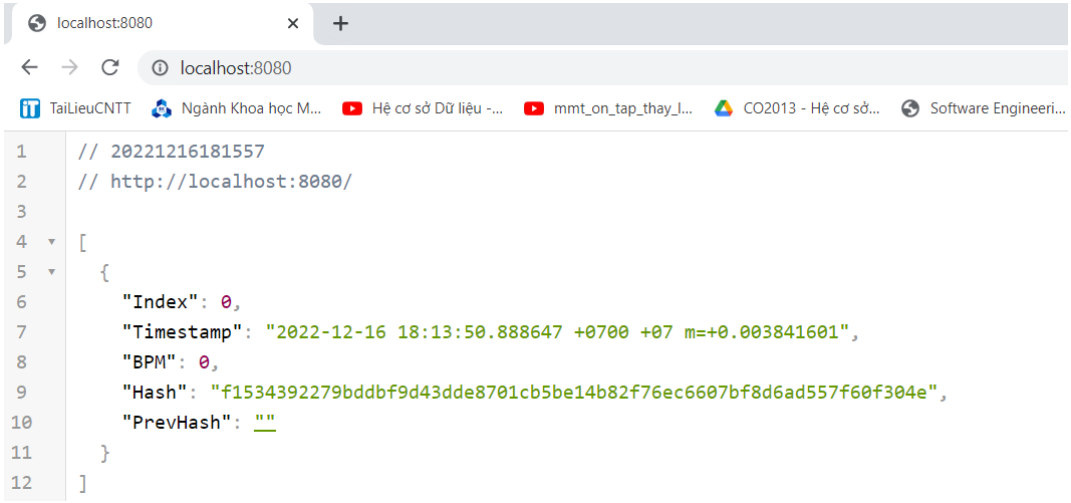
2. **Nhược điểm**

   – **Yêu cầu thiết bị nâng cao**: Các máy tính kém tiên tiến hơn sẽ không có khả năng cung cấp các lợi ích của web 3.0. Các tính năng và đặc điểm của thiết bị sẽ cần được mở rộng để làm cho công nghệ có thể tiếp cận với nhiều người hơn trên toàn cầu. Theo như hiện tại, sẽ chỉ có một số lượng hạn chế người có thể truy cập web 3.0.

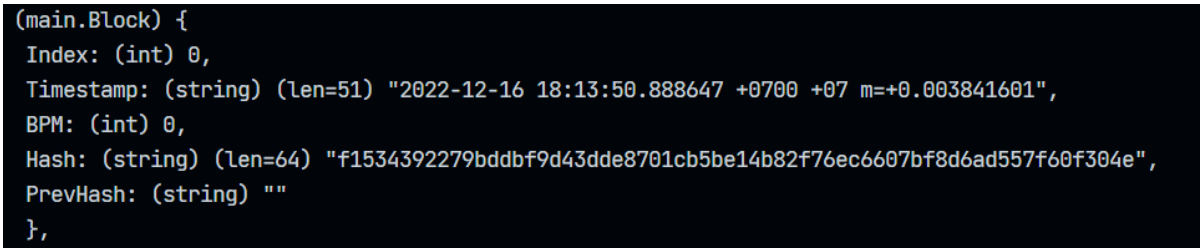
- **Chưa sẵn sàng cho việc áp dụng rộng rãi**: Công nghệ Web3 ngày càng thông minh, hiệu quả và dễ tiếp cận. Tuy nhiên, công nghệ này vẫn chưa hoàn toàn sẵn sàng để áp dụng rộng rãi. Cần nhiều nghiên cứu về tiến bộ công nghệ, luật bảo mật và sử dụng dữ liệu để đáp ứng nhu cầu của người dùng.
- **Chức năng phức tạp**: Web 3.0 là một công nghệ phức tạp đối với bất kỳ người dùng mới nào, điều này khiến họ do dự khi sử dụng nó. Nó là sự kết hợp của các công cụ web thế hệ cũ với các công nghệ tiên tiến, chẳng hạn như AI và blockchain, cũng như sự kết nối giữa người dùng và việc sử dụng Internet ngày càng tăng.

11 Hiện thực mạng blockchain bằng ngôn ngữ Golang

- Trong đề tài mở rộng này, em đã nghiên cứu và hiện thực được một mạng blockchain nhỏ để minh họa cho mô hình chuỗi khối trong mạng blockchain bằng ngôn ngữ Golang.
- Source code hiện thực mạng blockchain được gửi kèm báo cáo trong file zip.
- Link youtube video demo: https://youtu.be/xFeYXpnSWQI
- Để chạy source code, chúng ta sẽ thực hiện các bước như sau:
  - Đầu tiên, chúng ta cần cài đặt Golang và set up một số thư viện liên quan.
  - Tiếp theo, chạy file **main.go** bằng câu lệnh **go run main.go**.
  - Chúng ta có thể xem giao diện của các block ở trang **localhost:8080** hoặc trong terminal. Ở đây chúng ta có thể xem mã hash của **Genesis Block** đầu tiên trong chain.

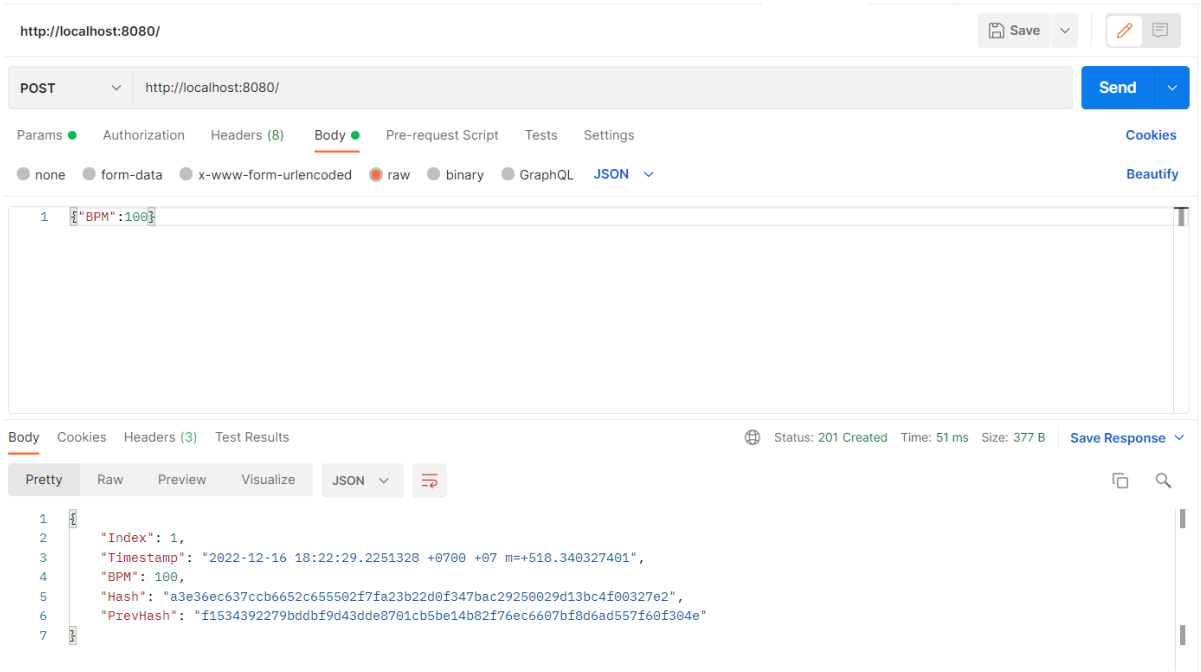


Hình 22: *Hình ảnh của Genesis Block trong chain ở trang localhost:8080*



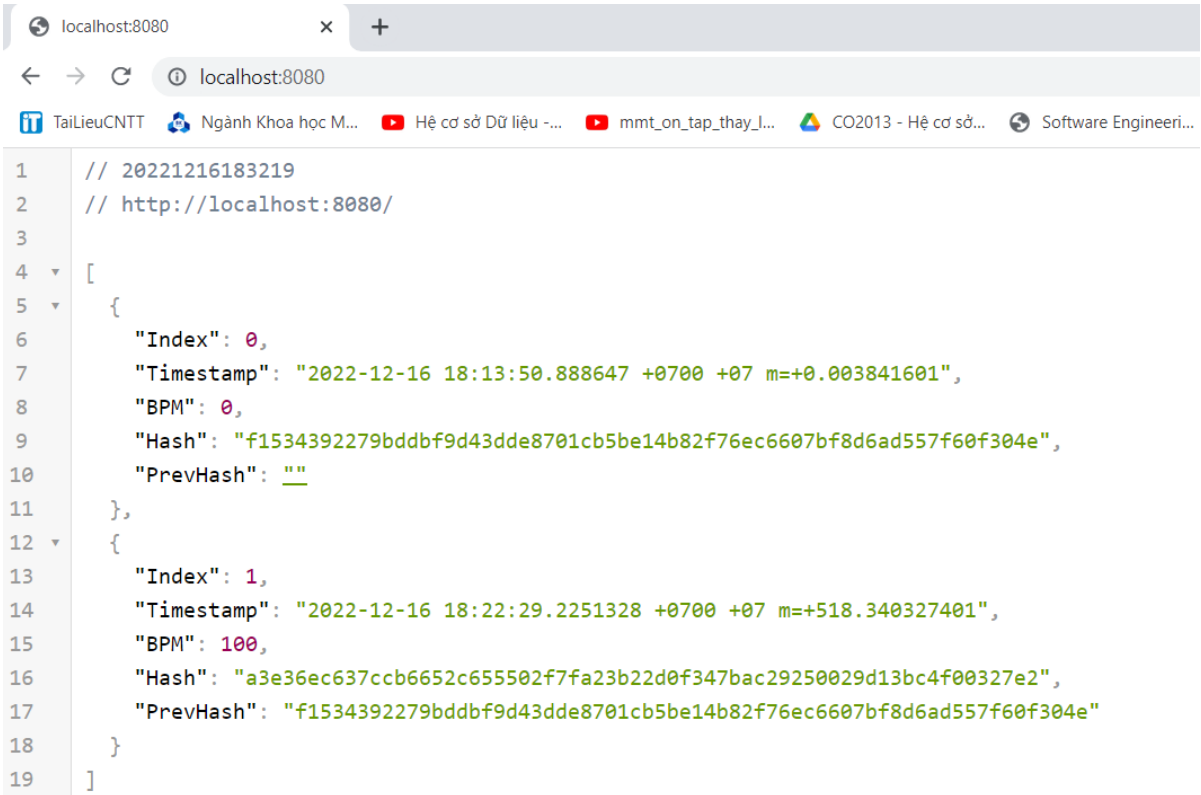
Hình 23: *Hình ảnh của Genesis Block trong chain trong terminal*

- Để thêm dữ liệu mới vào chain, chúng ta có thể sử dụng một tool hỗ trợ tính năng HTTP request POST đó là **Postman**



Hình 24: *Thực hiện một transaction để thêm block mới vào trong chain*

- Xem kết quả cập nhật của chain mới ở trang **localhost:8080**



Hình 25: *Hình ảnh chain sau khi được thêm block mới vào ở trang localhost:8080*

```
2022/12/16 18:13:50 HTTP Server Listening on port : 8080
(main.Block) {
 Index: (int) 0,
 Timestamp: (string) (len=51) "2022-12-16 18:13:50.888647 +0700 +07 m=+0.003841601",
 BPM: (int) 0,
 Hash: (string) (len=64) "f1534392279bddbf9d43dde8701cb5be14b82f76ec6607bf8d6ad557f60f304e",
 PrevHash: (string) ""
 },
 (main.Block) {
  Index: (int) 1,
  Timestamp: (string) (len=54) "2022-12-16 18:22:29.2251328 +0700 +07 m=+518.340327401",
  BPM: (int) 100,
  Hash: (string) (len=64) "a3e36ec637ccb6652c655502f7fa23b22d0f347bac29250029d13bc4f00327e2",
  PrevHash: (string) (len=64) "f1534392279bddbf9d43dde8701cb5be14b82f76ec6607bf8d6ad557f60f304e"
 }
}
```

Hình 26: *Hình ảnh chain sau khi được thêm block mới vào trong terminal*

12 Tài liệu tham khảo

Tài liệu

[1] Packt Publishing, "Oracle Blockchain Quick Start Guide: A practical approach to implementing blockchain in your enterprise", September 6, 2019.

[2] Marconi Foundation, "Marconi Protocol", May 2, 2018.

[3] Going the distance, Jeiwan, "A blog about blockchains and smart contracts development", truy cập từ: https://jeiwan.net/

[4] Oracle Blockchain Services Quick Start Guide, "Layered structure of the blockchain architecture", truy cập từ: https://subscription.packtpub.com/book/data/9781789804164/1/ch01lvl1sec07/layered-structure-of-the-blockchain-architecture

[5] Oracle Blockchain Services Quick Start Guide, "Types of blockchain networks", truy cập từ: https://subscription.packtpub.com/book/data/9781789804164/1/ch01lvl1sec07/layered-structure-of-the-blockchain-architecture

[6] Cpinbase, "What is PoW and PoS?", truy cập từ: https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake

[7] PWC, "Making sense of bitcoin, cryptocurrency and blockchain", truy cập từ: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

[8] Coral Health, "Building blockchain with Golang!", truy cập từ: https://mycoralhealth.medium.com/code-your-own-blockchain-in-less-than-200-lines-of-go-e296282bcffc

[9] Creative Tim Blog, "What is Web 3.0?", truy cập từ: https://www.creative-tim.com/blog/educational-tech/web-1-0-vs-web-2-0-vs-web-3-0-what-are-the-differences/

[10] Bizfly Cloud, "How web 3.0 work?", truy cập từ: https://bizflycloud.vn/tin-tuc/web-30-la-gi-tim-hieu-chi-tiet-ve-web-30-ky-nguyen-moi-cua-internet-phan-1-20220316164228356.htm