**Khảo sát các nền tảng blockchain**

**I.Ethereum**

**A picture containing logo

Description automatically generated**

**\*) Giới thiệu**

Ethereum là một nền tảng phần mềm mã nguồn mở, phân tán dựa trên công nghệ blockchain. Nó có tiền điện tử riêng gọi là Ether và một ngôn ngữ lập trình gọi là Solidity. Ethereum là đối thủ cạnh tranh chính của Bitcoin. Ethereum cho phép các nhà phát triển xây dựng các ứng dụng phi tập trung (Dapps) (Ethereum đóng vai trò như một nền tảng cơ sở. Các Dapps xuất hiện sau này sẽ được xây dựng và phát triển dựa trên nền tảng đó).

Nền tảng Ethereum được sáng lập bởi 1 lập trình viên trẻ người Canada gốc Nga có tên là Vitalik Buterin vào năm 2015.

Nền tảng này cũng hỗ trợ hợp đồng thông minh, là một loại hợp đồng kỹ thuật số.

Hợp đồng thông minh cho phép những người tham gia giao dịch với nhau mà không cần đến sự giám sát của bên thứ 3. Hồ sơ giao dịch là bất biến (không thể thay đổi), có thể xác minh và được phân phối an toàn trên mạng internet, mang lại cho người tham gia toàn quyền sở hữu và khả năng hiển thị dữ liệu giao dịch.

Các thợ đào tạo ra các mã thông báo Ether có thể được sử dụng như một loại tiền tệ và để trả phí sử dụng trên mạng Ethereum. ‘Ether’ hay còn gọi là ETH là đơn vị tiền tệ được sử dụng để chạy các ứng dụng trong mạng lưới này. Nói cách khác, đồng coin Ether đóng vai trò cung cấp “năng lượng” cho mạng Ethereum mỗi khi một giao dịch được thực hiện qua các ứng dụng, hay còn gọi là phí giao dịch. Người tham gia cũng có thể sử dụng nó để thanh toán cho hàng hóa và dịch vụ hữu hình nếu được chấp nhận.

**\*)Lịch sử chia cắt**

Một sự kiện đáng chú ý trong lịch sử của Ethereum là đợt phân tách của Ethereum và Ethereum Classic. Vào năm 2016, một nhóm người tham gia mạng đã giành được quyền kiểm soát phần lớn đối với chuỗi khối Ethereum để đánh cắp số ether trị giá hơn 50 triệu đô la, vốn đã được huy động cho một dự án có tên The DAO. Thành công của cuộc đột kích được cho là nhờ sự tham gia của một nhà phát triển bên thứ ba cho dự án mới. Hầu hết cộng đồng Ethereum đã chọn đảo ngược hành vi trộm cắp bằng cách làm mất hiệu lực của chuỗi khối Ethereum hiện có và phê duyệt một chuỗi khối có lịch sử sửa đổi. Tuy nhiên, một phần cộng đồng đã chọn duy trì phiên bản gốc của chuỗi khối Ethereum. Phiên bản Ethereum không thay đổi đó đã tách vĩnh viễn để trở thành tiền điện tử Ethereum Classic (ETC).

**\*) Ethereum 2.0**

Hiện tại có rất nhiều Dapp đang vận hành trên blockchain Ethereum. Các ứng dụng phi tập trung này tranh giành tài nguyên trên chuỗi khối, sinh ra hàng tỷ giao dịch trên mạng lưới và chính những giao dịch này gây ra một phần nguyên nhân khiến cho mạng lưới Ethereum bị tắc nghẽn.

Mạng lưới Ethereum hiện tại (Ethereum 1.0) đang có những hạn chế lớn như:

**Tốc độ giao dịch chậm, Phí giao dịch cao, Khả năng mở rộng kém, mạng lưới giao dịch trên Ethereum hay bị tắc nghẽn.**

Ethereum 2.0 là quá trình nâng cấp mạng lưới Ethereum chuyển từ cơ chế đồng thuận Proof of Work (PoW) sang Proof of Stake (PoS).

* Các giai đoạn nâng cấp lên Ethereum 2.0:

***Giai đoạn 0*:** Thử nghiện Beacon chain và hoàn thiện cơ chế PoS trên mạng lưới Ethereum

***Giai đoạn 1***: Hoàn thiện Shard chains để cải thiện khả năng mở rộng trên mạng lưới

***Giai đoạn 1.5***: Hợp nhất 2 mạng lưới PoW và PoS thành một mạng lưới Ethereum 2.0

***Giai đoạn 2*:** Cải tiến tài khoản, giao dịch và hợp đồng thông minh của mạng lưới

Khi bản nâng cấp được hoàn thành, chuỗi Ethereum 2.0 sẽ được ra đời với sự hợp nhất giữa chuỗi Ethereum hiện tại và chuỗi Beacon thành 1 mạng lưới duy nhất và sử dụng Pos thay vì PoW.

Mục đích của Ethereum 2.0 là nâng cao tốc độ giao dịch, xử lý nhiều giao dịch, giảm thiểu nghẽn mạng và mở rộng mạng lưới cho các tránh tình trạng tắc nghẽn.

**\*) Cách hoạt động**

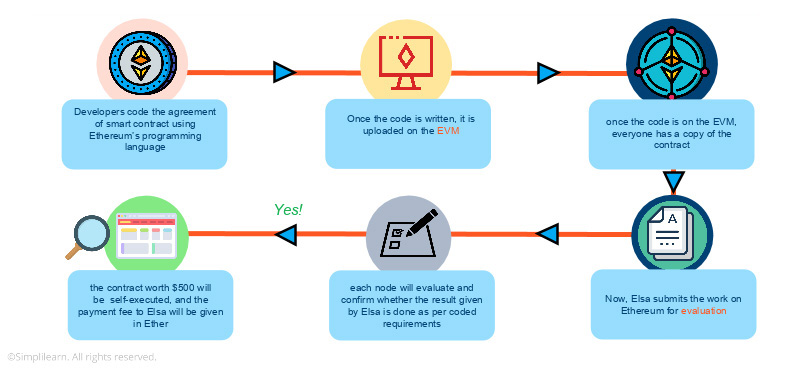
Ethereum hoạt động bởi mạng lưới các máy tính gọi là Nodes, để tham gia vào mạng lưới này, các Nodes phải cài đặt phần mềm Ethereum Client. Sau khi cài đặt thì Nodes sẽ chạy chương trình ảo Ethereum Virtual Machine – EVM.

Máy ảo EVM thực thi hoạt động như lệnh giao dịch, smart contract(hợp đồng thông minh),… Mạng lưới cần đến một lượng phí gọi là Gas – phí thanh toán bằng đồng tiền kỹ thuật số gọi là Ether (ETH).

Khi giao dịch được thực thi, Thợ đào sẽ xác nhận xem giao dịch đó có hợp lệ hay không. Ethereum sử dụng cơ chế Proof Of Work (PoW) để các thợ đào chứng minh công việc của họ đã hoàn thành và thông báo đến toàn mạng lưới. Sau đó các thợ đào khác sẽ xác nhận xem bằng chứng hợp lệ hay không.

Block mới được tạo ra bằng cách giải mã với thuật toán Ethash, sau đó xác nhận mạng lưới giao dịch khi PoW được thông qua, dữ liệu giao dịch ghi vào Blockchain của Ethereum và không thể thay đổi.

Tháng 9 năm 2022, Ethereum đã chuyển sang thuật toán proof of stake, rẻ hơn và thân thiện với môi trường hơn PoW. Thay vì các thợ đào xác minh giao dịch, Ethereum sẽ sử dụng chủ sở hữu của các khoản cổ phần quan trọng để xác thực giao dịch. Những người xác thực này “đặt cược” tiền tệ của họ và kiếm phần thưởng dưới dạng ether để xác minh các giao dịch. Tuy nhiên, các nhà đầu tư có thể mất khoản đầu tư nếu họ xác thực các giao dịch không tuân thủ các quy tắc của Ethereum. Ngay cả những nhà đầu tư nhỏ hơn cũng có thể tham gia vào hệ thống đặt cược - và kiếm phần thưởng - bằng cách cam kết đồng tiền của họ với một trình xác nhận.



**\*)Wallet (Ví):**

Chủ sở hữu Ethereum sử dụng ví để lưu trữ ether của họ. Ví là một giao diện kỹ thuật số cho phép bạn truy cập ether của mình được lưu trữ trên blockchain. Ví của bạn có một địa chỉ, tương tự như một địa chỉ email, nó là nơi người dùng gửi ether, giống như họ gửi email. Ether không thực sự được lưu trữ trong ví của bạn. Ví của bạn giữ các khóa cá nhân mà bạn sử dụng như mật khẩu khi bạn bắt đầu giao dịch. Bạn nhận được một khóa riêng cho mỗi ether mà bạn sở hữu. Chìa khóa này rất cần thiết để truy cập ether của bạn.

**\*) So sánh Ethereum và Bitcoin**:

Về nguồn gốc, Bitcoin được tạo ra như một loại tiền tệ và để lưu trữ giá trị. Còn Ethereum được tạo ra như một nền tảng giao dịch hợp đồng thông minh phân tán. Lưu ý rằng Bitcoin cũng có thể xử lý được hợp đồng thông minh, và Ethereum cũng có thể được sử dụng như một loại tiền tệ. Ngoài ra, giữa Bitcoin và Ethereum còn có những điểm khác biệt cơ bản sau:

Bitcoin có thể sử dụng để thanh toán hàng hóa và dịch vụ tại bất cứ nơi nào đồng tiền này được chấp nhận, còn đồng tiền Ether của mạng lưới Ethereum không được thiết kế như một giải pháp thanh toán thay thế, mà là để thúc đẩy các lập trình viên và các tổ chức sáng tạo và vận hành các ứng dụng phi tập trung trong mạng Ethereum.

Cả hai cho phép bạn sử dụng tiền kỹ thuật số mà không cần nhà cung cấp thanh toán hoặc ngân hàng. Nhưng Ethereum có thể lập trình, vì vậy bạn cũng có thể xây dựng và triển khai các ứng dụng phi tập trung trên mạng của nó. Ethereum có thể lập trình có nghĩa là bạn có thể xây dựng các ứng dụng sử dụng blockchain để lưu trữ dữ liệu hoặc kiểm soát những gì ứng dụng của bạn có thể làm. Điều này dẫn đến một blockchain mục đích chung có thể được lập trình để làm bất cứ điều gì. Vì không có giới hạn cho những gì Ethereum có thể làm, nó cho phép sự đổi mới tuyệt vời xảy ra trên mạng Ethereum. Mặc dù Bitcoin chỉ là một mạng lưới thanh toán, Ethereum giống như một thị trường của các dịch vụ tài chính, trò chơi, mạng xã hội và các ứng dụng khác tôn trọng quyền riêng tư của bạn và không thể kiểm duyệt bạn.

Ethereum và Bitcoin đều hoạt động trên hệ thống bằng chứng công việc (PoW), được sử dụng để xác thực các giao dịch.Nhưng vào năm 2022, Ethereum sẽ chuyển sang một hệ thống mới được gọi là bằng chứng cổ phần (PoS) như một phần của bản nâng cấp Ethereum 2.0

**2. Stellar**

**A picture containing graphical user interface

Description automatically generated**

Stellar là một dự án mạng mã nguồn mở, hướng tới việc giải quyết các vấn đề về tiền tệ và thanh toán. Stellar cung cấp khả năng tạo, gửi và trao đổi các token biểu diễn các loại tiền như dollars, pesos, bitcoin,... dưới dạng kĩ thuật số. Nó được thiết kế với mục tiêu đưa toàn bộ hệ thống tài chính thế giới vào trong một mạng lưới duy nhất.

Stellar không được sở hữu bởi bất kì cá nhân hay tổ chức nào, mà thuộc về toàn bộ cộng đồng. Hệ thống được chạy trên một mạng lưới mở, phi tập trung và xử lý hàng triệu giao dịch mỗi ngày. Giống như Bitcoin và Ethereum, Stellar dựa vào blockchain để giữ cho mạng được đồng bộ hóa, nhưng lại mang lại trải nghiệm giống với sử dụng tiền mặt cho người dùng. Stellar nhanh hơn, rẻ hơn và tiết kiệm năng lượng hơn các hệ thống dựa trên blockchain thông thường.

**\*) Stellar dùng để làm gì**

Mạng lưới Stellar ra mắt vào năm 2015. Kể từ đó đến nay, nó đã xử lý hơn 450 triệu hoạt động được thực hiện bởi hơn 4 triệu tài khoản cá nhân. Các công ty lớn như IBM và Franklin Templeton hay các công ty nhỏ như các công ty khởi nghiệp đã chọn Stellar để chuyển tiền và tiếp cận các thị trường mới.

Ngay từ ban đầu, Stellar đã mang những đặc điểm của hệ thống tiền điện tử, tuy nhiên stellar luôn hướng tới việc nâng cao thay vì hủy hoại hay thay thế hệ thống tài chính hiện có. Trong khi mạng Bitcoin sinh ra chỉ để giao dịch Bitcoin thì Stellar là một hệ thống phi tập trung tuyệt vời để giao dịch bất kì loại tiền nào một cách minh bạch và hiệu quả.

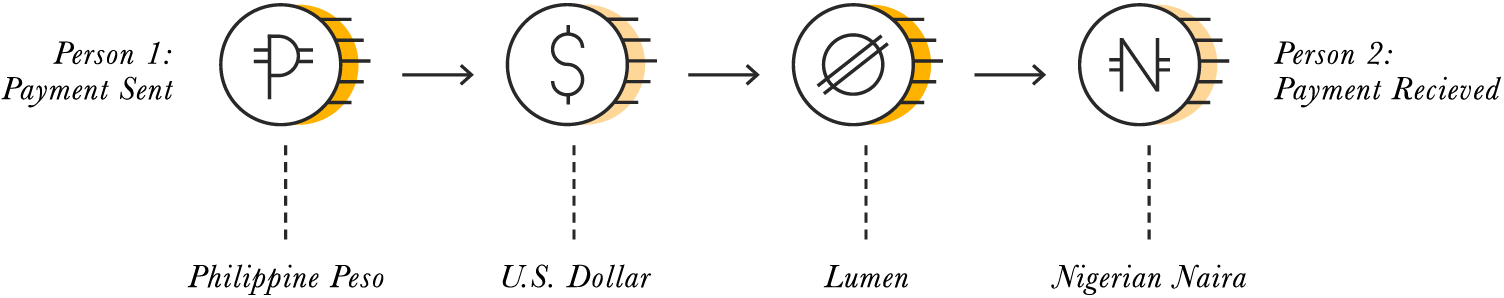
A picture containing shape

Description automatically generated

Ví dụ : Bạn muốn tạo một biểu diễn kĩ thuật số của đồng US dollar trên Stellar và gọi nó là "dollar token". Sau đó bạn sẽ bảo với thế giới rằng, bất cứ khi nào ai mang 1 dollar đến cho bạn, bạn sẽ đưa họ 1 "dollar token" và ngược lại, khi một người mang "dollar token" trở lại thì bạn phải đảm bảo có thể đưa lại cho họ dollar. Khi đó bạn đã tạo mối quan hệ 1:1 giữa đồng tiền kĩ thuật số của bạn và dollar . Vậy nên khi mọi người giữ đồng dollar token, họ có thể sử dụng với các tính năng như tiền truyền thống và có thể quy đổi ra tiền khi họ muốn. Tất nhiên ngoài dollar bạn cũng có thể tạo biểu diễn kĩ thuật số cho bất cứ loại tiền nào khác.

Điều này khá giống với công việc mà các ngân hàng lớn nhỏ trên toàn thế giới đang hoạt động mỗi ngày. Tuy nhiên điểm khác biệt ở đây nằm ở chỗ token có thể dùng để trao đổi và mua bán trên toàn thế giới mà không cần phải qua giải quyết và phê duyệt của ngân hàng. Chính nhờ điều này, Stellar network khiến cho tiền tệ không có bất cứ biên giới nào. Một người làm việc ở Mỹ hay châu Âu có thể gửi dollar token về Việt Nam bất cứ khi nào. Một công ty Việt Nam có thể trả tiền cho công nhân đang ở Lào qua Stellar network,...

Stellar còn cho phép người dùng gửi một loại tiền và người nhận sẽ nhận được một loại tiền khác. Về cơ bản, bạn có thể gửi và trao đổi tiền trong một automic transaction ( tức các token sẽ được tự động trao đổi theo tỉ giá hiện tại trên stellar network).



Giống như các mạng blockchain khác, Stellar cũng có native crypto currency là lumen. Hệ thống sẽ yêu cầu người dùng phải có một lượng rất nhỏ lumen để khởi tạo tài khoản cũng như gửi transaction ( 0.00001 lumen mỗi giao dịch). Ngoài yêu cầu trên thì Stellar không ưu tiên bất cứ loại tiền nào.

**\*) Stellar hoạt động như thế nào**

Ở mức thấp nhất, Stellar có thể hiểu là một hệ thống để theo dõi quyền sở hữu. Giống như việc kế toán đã làm nhiều thế kỷ, nó sử dụng một sổ cái để làm như vậy. Sự khác biệt là Stellar không có kế toán viên thực sự. Thay vào đó, có một mạng lưới các máy tính độc lập, mỗi máy tính kiểm tra và rà soát lại công việc của các máy tính khác. Stellar là một hệ thống không có cơ quan trung ương, có nghĩa là không ai có thể dừng mạng hoặc bí mật điều chỉnh các số theo ý thích của mình ngay cả khi không có cơ quan trung ương, các sổ cái được xác minh và cập nhật, cứ sau 5 giây.

Điều này có thể thực hiện được nhờ một thuật toán duy nhất được gọi là Giao thức đồng thuận Stellar (SCP), giữ mọi thứ được đồng bộ hóa thông qua Proof-of-Agreement (PoA). Có nhiều cách để đạt được đồng thuận trên một hệ thống phi tập trung, proof of work của Bitcoin là phương pháp đầu tiên và vẫn là nổi tiếng nhất. Tuy nhiên chính vì việc là người tiên phong, proof of work còn rất nhiều vấn đề để cải thiện. SCP và PoA phấn đấu để trở nên tốt hơn bằng cách có thể cấu hình, hệ thống chạy nhanh hơn và tiết kiệm năng lượng.

Diagram, table

Description automatically generated

Đối với mọi chủ tài khoản, Stellar’s ledger lưu trữ hai thứ quan trọng: những gì họ sở hữu (số dư tài khoản, như số tiền 100 peso tokens hay hoặc 5000 5000 lumens) và những gì họ muốn làm với những gì họ sở hữu (hoạt động, như cách bán 10 token trong 50 lumens, hoặc, gửi 100 peso token vào tài khoản tương tự như vậy.) Cứ sau năm giây, tất cả số dư và tất cả các hành động được giải quyết và lan truyền toàn bộ mạng.

Các máy tính chạy Stellar core, lưu trữ và kiểm tra ledger được gọi là các nodes. Vì vậy, khi bạn gửi cho ai đó euro token trên ứng dụng sử dụng Stellar, các nodes sẽ kiểm tra xem số dư chính xác đã được ghi hay chưa, và mỗi node đảm bảo mọi node khác đều thấy và đồng thuận với giao dịch. Mạng Stellar hiện tại được xác minh bởi hàng trăm nodes trên toàn cầu; các nodes và cách chúng giao tiếp là thông tin công khai và bất kỳ ai cũng có thể cài đặt phần mềm Stellar và tham gia vào quy trình đồng thuận. Điều này khác với cách hoạt động của kế toán tại một ngân hàng, nơi một tập đoàn đơn phương quyết định những gì xảy ra.

Ngay bên trên lớp lõi này chứa API để để xây dựng trên Stellar, cung cấp cho các developer khả năng xây dựng ứng dụng Stellar mà không cần phải tìm hiểu quá sâu về các thuật toán đồng thuận.

**\*) Kiến trúc hệ thống Stellar**

Diagram

Description automatically generated

Sử dụng mạng Stellar, bạn có thể xây dựng ví di động, công cụ ngân hàng, thiết bị thông minh tự trả tiền và bất kỳ thứ gì khác bạn muốn liên quan đến thanh toán.

* **API Horizon**

Horizon là API để tương tác với Stellar. API này phục vụ cầu nối giữa các ứng dụng và Stellar core. Các dự án như ví, trao đổi phi tập trung và nhà phát hành tài sản sử dụng Horizon để gửi giao dịch, truy vấn số dư tài khoản hoặc phát trực tuyến các sự kiện như giao dịch vào tài khoản.

Hầu hết các ứng dụng tương tác với mạng Stellar thông qua Horizon, máy chủ API RESTful. Horizon cung cấp cho bạn một cách đơn giản để gửi giao dịch, kiểm tra tài khoản và theo dõi các sự kiện. Bởi vì nó chỉ là HTTP, bạn có thể giao tiếp với Horizon bằng trình duyệt web, các công cụ dòng lệnh đơn giản như cURL hoặc Stellar SDK cho ngôn ngữ lập trình yêu thích của bạn. Cách dễ nhất để cài đặt Horizon là sử dụng[stellar / quickstart docker image](https://hub.docker.com/r/stellar/quickstart/).

[Stellar.org](http://stellar.org/) duy trì các SDK dựa trên JavaScript, Java và Go để giao tiếp với Horizon. Ngoài ra còn có SDK do cộng đồng duy trì cho Ruby, Python và C#.

* **Stellar Core**

Mọi máy chủ Horizon kết nối với Stellar Core, xương sống của mạng Stellar. Phần mềm Stellar Core thực hiện công việc xác nhận trạng thái của mọi giao dịch thông qua Stellar Consensus Protocol (SCP).

Mạng lưới Stellar là một tập hợp các Stellar Cores trên toàn thế giới, mỗi nhóm được duy trì bởi những người và tổ chức khác nhau. Tất cả các nodes cùng đồng thuận về các giao dịch. Mỗi giao dịch trên mạng có chi phí nhỏ: 100 stroops (0,00001 XLM). Phí này giúp ngăn chặn các tác nhân xấu gửi spam mạng.