HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA CÔNG NGHỆ THÔNG TIN I**

# BÀI BÁO CÁO TIỂU LUẬN

## Tìm hiểu về công nghệ chuỗi khối (Blockchain) và các ứng dụng

Nhóm 7

Các thành viên trong nhóm


| | | | |
|---|---|---|---|
| Ninh Chí Hướng | B20DCAT094 | Đỗ Trung Kiên | B20DCAT097 |
| Hoàng Trung Kiên | B20DCAT098 | Cao Vũ Tùng Lâm | B20DCAT106 |
| Phạm Hoàng Lâm | B20DCAT108 | Chu Quang Long | B20DCAT111 |


HÀ NỘI, THÁNG 10/2022

# Giới thiệu

Trong cách mạng công nghiệp 4.0, công nghê chuỗi khối (Blockchain) được xem là một trong những công nghê then chốt cho chuyển đổi số xây dựng nền tảng công nghê thông tin trong tương lai .

Với khả năng chia sẻ thông tin dữ liệu minh bạch theo thời gian thực tế, có tính bảo mật cao, công nghệ blockchain là một trong những xu hướng công nghệ đột phá, có khả năng ứng dụng rộng rãi ở nhiều ngành nghề, lĩnh vực khác nhau.

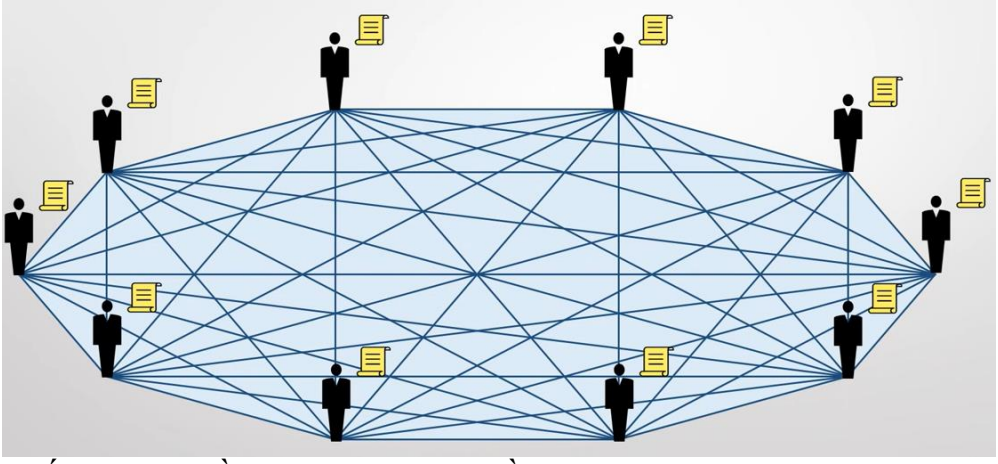
Trong bài tiểu luận này nhóm chúng em sẽ đưa ra khái niệm của blockchain và các ứng dụng của nó .

# Nội dung

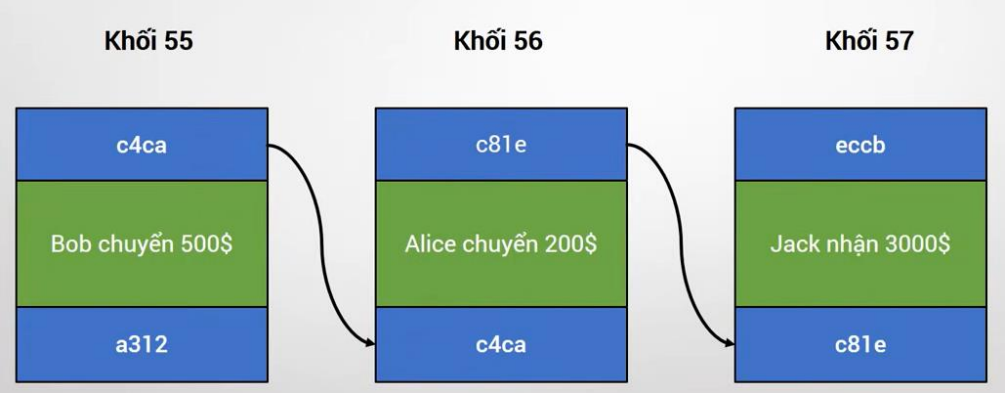
## I. Công nghệ chuỗi khối (Blockchain) là gì?

Blockchain là công nghệ mã hóa tất cả dữ liệu thành các khối và kết nối chúng với nhau thông qua một đoạn mã đã được băm để tạo thành một chuỗi khối dài. Mỗi khi một thông tin hoặc giao dịch mới xảy ra, thông tin cũ sẽ không bị mất đi mà thay vào đó, thông tin mới sẽ được lưu vào một khối mới và lần lượt được nối vào khối cũ để tạo thành một chuỗi mới.

Không chỉ có vậy, Blockchain được xây dựng trên mô hình Peer to Peer (P2P) để thông tin của Blockchain không chỉ nằm trên một máy chủ duy nhất mà được tự động phân phối và sao lưu trên nhiều máy khác nhau kết nối với hệ thống Blockchain để mọi người đều có thể xem và kiểm tra các giao dịch của mình. Điều này có thể ngăn chặn việc sửa đổi hoặc gian lận và đảm bảo tính minh bạch và an toàn thông tin.



Mỗi khối (block) đều chứa thông tin về thời gian khởi tạo và được liên kết với khối trước đó, kèm theo đó là một mã thời gian và dữ liệu giao dịch. Dữ liệu khi đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được. Blockchain được thiết kế để chống lại việc gian lận, thay đổi của dữ liệu. Sau này đồng tiền Bitcoin và các đồng tiền khác tương tự được phát hành, thì công nghệ Blockchain là nền tảng giúp việc xử lý các giao dịch tiền tệ.




Công nghệ chuỗi khối(Blockchain) là sự kết hợp giữa 3 loại công nghệ:

**Mật mã học**: Sử dụng public key và hàm hash function để đảm bảo tính minh bạch, toàn vẹn và riêng tư.

**Mạng ngang hàng**: Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ bản sao ứng dụng.

**Lý thuyết trò chơi**: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (PoW, PoS…) và được thúc đẩy bởi động lực kinh tế.

Trên góc độ business có thể gọi là một sổ cái kế toán, hay một cơ sở dữ liệu chứa đựng tài sản, hay một cấu trúc dữ liệu, mà dùng để ghi chép lại lịch sử tài sản giữa các thành viên trong hệ thống mạng ngang hàng.
Trên góc độ kỹ thuật đó là một phương thức bất biến để lưu trữ lịch sử các giao dịch tài sản.

Trên góc độ xã hội đó là một hiện tượng, mà dùng để thiết lập niềm tin bằng quy tắc đồng thuận giữa các thành viên trong một hệ thống phân cấp.

## 1.2 Đặc điểm của Blockchain.

**Không thể làm giả, không thể phá hủy các chuỗi Blockchain**: theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu.

**Tính phi tập trung (Decentralized):** Blockchain sẽ hoạt động độc lập theo các thuật toán máy tính, hoàn toàn không bị bất kỳ một tổ chức nào nắm quyền kiểm soát. Chính vì vậy blockchain tránh được rủi ro từ bên thứ 3.

**Bất biến**: dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi bởi đặc tính của thuật toán đồng thuận và mã hash

**Bảo mật**: Các thông tin, dữ liệu trong Blockchain được phân tán và an toàn tuyệt đối.

**Minh bạch**: Ai cũng có thể theo dõi dữ liệu Blockchain đi từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

**Hợp đồng Thông minh**: là hợp đồng kỹ thuật số được nhúng vào đoạn code if-this-then-that (IFTTT), cho phép chúng tự thực thi mà không cần bên thứ ba.

## 1.3 Các loại Blockchain

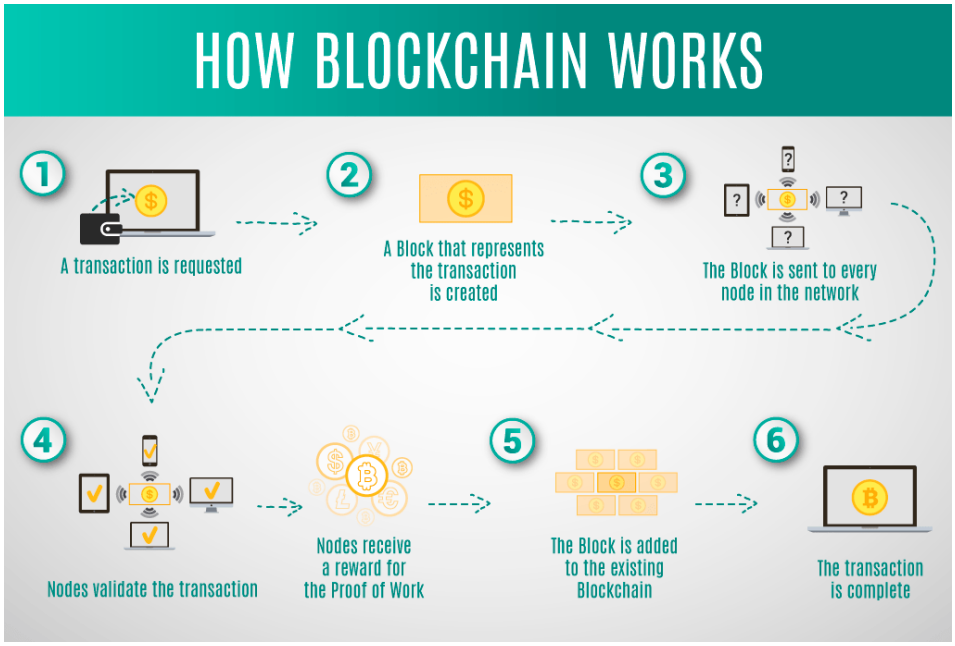
Hệ thống Blockchain chia thành 3 loại chính:

**Public**: Bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có hàng nghìn hay hàng vạn nút tham gia. Do đó để tấn công vào hệ thống Blockchain này là điều bất khả thi vì chi phí khá cao. Ví dụ: Bitcoin, Ethereum…

**Private**: Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Tổ chức 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. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. 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.

**Permissioned**: Hay còn gọi là Consortium, một dạng của Private nhưng bổ sung thêm một số tính năng nhất định, kết hợp giữa "niềm tin" khi tham gia vào Public và "niềm tin tuyệt đối" khi tham gia vào Private. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

## 1.4 Nguyên lý hoạt động

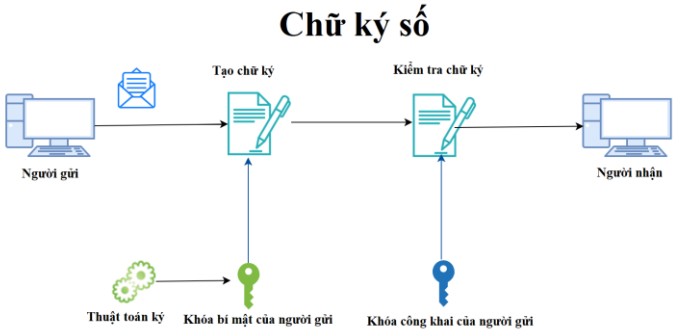



### 1.4.1 Nguyên lý mã hóa

Cuốn sổ cái luôn được duy trì bởi các máy tính trong mạng ngang hàng được kết nối với nhau.

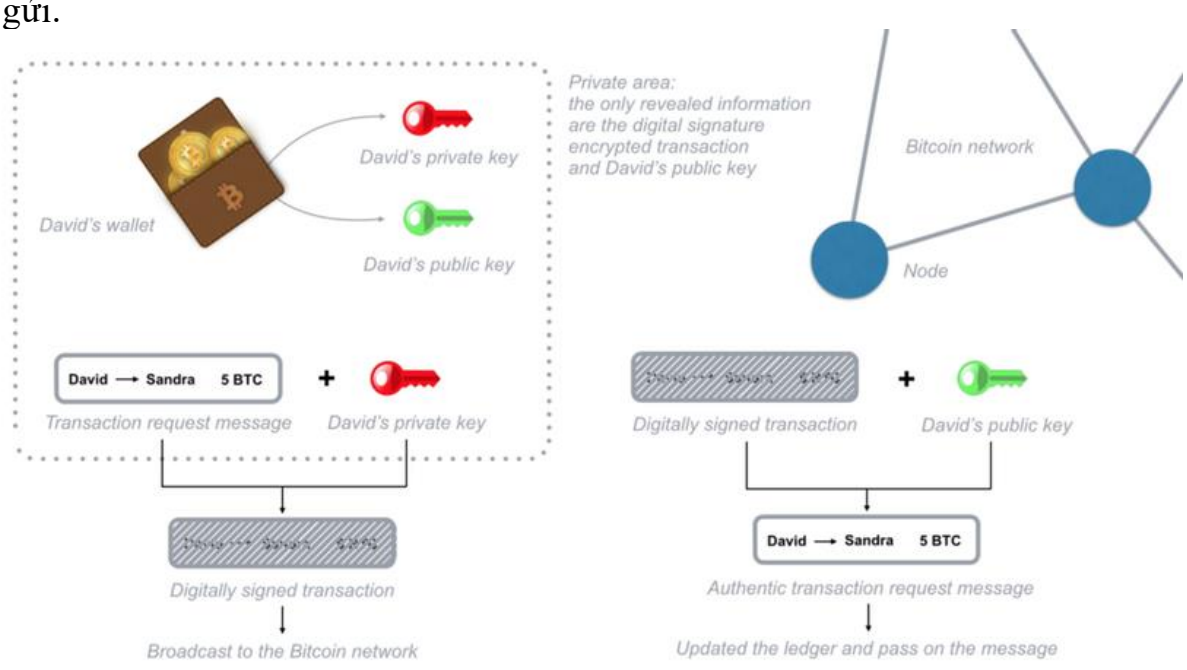
Trong hệ thống ngân hàng, chúng ta chỉ biết các giao dịch và số dư tài khoản của riêng mình thì trên blockchain bạn có thể xem các giao dịch của tất cả mọi người.Ví dụ, mạng lưới Bitcoin là mạng lưới phân tán không cần bên thứ ba đóng vai trò trung gian xử lý giao dịch. Hệ thống blockchain được thiết kế theo cách không yêu cầu sự tin cậy và bảo đảm bởi độ tin cậy có được thông qua các hàm mã hóa toán học đặc biệt. Để có thể thực hiện các giao dịch trên blockchain, bạn cần một phần mềm sẽ cho phép bạn lưu trữ và trao đổi các đồng Bitcoin của bạn gọi là ví tiền điện tử. Ví tiền điện tử này sẽ được bảo vệ bằng một phương pháp mã hóa đặc biệt đó là sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key).

Nếu một thông điệp được mã hóa bằng một khóa công khai cụ thể thì chỉ chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp.




Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư, có nghĩa là bạn đang tạo ra một chữ ký điện tử được các máy tính trong mạng lưới blockchain sử dụng để kiểm tra chủ thể gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và là sự kết hợp của yêu cầu giao dịch và khóa riêng tư của bạn.

Chỉ cần một thay đổi nhỏ thì chữ ký điện tử sẽ thay đổi theo. Vì thế, hacker khó có thể thay đổi yêu cầu giao dịch của bạn hoặc thay đổi số lượng Bitcoin mà bạn đang gửi.



Để gửi Bitcoin (BTC), bạn cần chứng minh rằng bạn sở hữu khóa riêng tư của một chiếc ví điện tử cụ thể bởi bạn cần sử dụng nó để mã hóa thông điệp yêu cầu giao dịch. Sau khi tin nhắn của bạn đã được gửi đi và được mã hóa thì bạn không cần phải tiết lộ khóa riêng tư của bạn nữa.

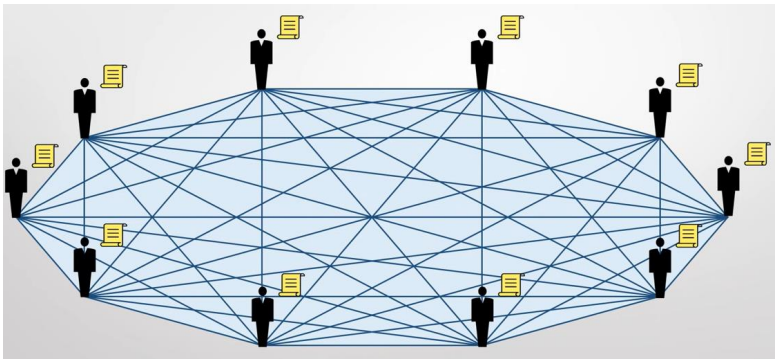
### 1.4.2 Quy tắc của sổ cái

Mỗi nút trong blockchain đều đang lưu giữ một bản sao của sổ kế toán. Do vậy, mỗi nút đều biết số dư tài khoản của bạn là bao nhiêu. Hệ thống blockchain chỉ ghi lại mỗi giao dịch được yêu cầu chứ không hề theo dõi số dư tài khoản của bạn.

Để biết số dư trên ví điện tử của mình thì bạn cần xác thực và xác nhận tất cả các giao dịch đã diễn ra trên mạng lưới mà có liên quan tới ví điện tử của bạn.

LEDGER

| Transactions | Value |
|---|---|
| Mary → John | 10.000 |
| John → Lisa | 0.345 |
| Sandra → David | 18.4332 |
| Lisa → Sandra | 7.156 |
| David → Mary | 12.3402 |
| Brian → Lisa | 3.029381 |
| ... | ... |



Việc xác minh "số dư" này được thực hiện nhờ các tính toán dựa vào liên kết đến các giao dịch trước đó. Nhìn vào hình trên, để gửi 10btc cho John, Mary cần tạo yêu cầu giao dịch bao gồm các liên kết đến các giao dịch đã diễn ra trước đó với tổng số dư bằng hoặc vượt quá 10 btc.

Các liên kết này được xem như là giá trị đầu vào, các nút trong mạng lưới sẽ xác minh xem tổng số tiền của các giao dịch này bằng hoặc vượt quá 10 btc không. Tất cả điều này được thực hiện tự động trong ví điện tử của Mary và được kiểm tra bởi các nút trên mạng lưới Bitcoin, Mary chỉ gửi một giao dịch 10 bitcoin tới ví của John bằng khóa công khai của John

Mary → John 10 BTC

*Simplified transaction request*

**Inputs**

| Previous output | Amount | From address | Signature |
|---|---|---|---|
| n278cojci...1 | 3.451 | Sandra's address | fuw93v2...c3 |
| m8nd53hd...1 | 6.334 | Brian's address | a56fbsuc...s8 |
| cn3792m...1 | 0.14 | Lisa's address | lfue82mc...id |
| u4her83n...1 | 2.193 | David's address | jwc7fks8...2a |

**Outputs**

| Redeemed input | Amount | To address | Signature |
|---|---|---|---|
| j3s8b30f...if | 2.118 | Mary's address | k732cne...21 |
| ks2f9ms7...j3 | 10 | John's address | 87fckwlo...k4 |

*Real transaction request structure*

Vậy, làm thế nào hệ thống có thể tin tưởng các giao dịch đầu vào này và xác thực tính hợp lệ của chúng?

Thực tế là các nút sẽ kiểm tra tất cả các giao dịch có liên quan đến ví tiền điện tử bạn sử dụng trước đó để gửi Bitcoin (BTC) thông qua việc tham chiếu các lịch sử

giao dịch. Có một bản ghi sẽ lưu trữ số BTC chưa được dùng và được các nút mạng lưu giữ giúp đơn giản hóa và tăng tốc quá trình xác minh. Vì thế, các ví tiền điện tử tránh được tình trạng chi tiêu đúp giao dịch.

=> "Như vậy sở hữu Bitcoin có nghĩa là có các giao dịch được lưu trong sổ kế toán liên hệ đến địa chỉ ví của bạn mà chưa được sử dụng làm giao dịch đầu vào."

Mã nguồn trên mạng lưới Bitcoin là nguồn mở, có nghĩa là bất kỳ ai có máy tính kết nối được internet đều có thể tham gia vào mạng lưới và thực hiện giao dịch.

Tuy nhiên, nếu có bất kỳ một lỗi nào trong mã nguồn được sử dụng để phát thông báo yêu cầu giao dịch thì các Bitcoin liên quan sẽ bị mất vĩnh viễn.

### 1.4.3 Nguyên Lý tạo khối

Các giao dịch sau khi được gửi lên trên mạng lưới blockchain sẽ được nhóm vào các khối. Các giao dịch trong cùng một khối được coi là đã xảy ra cùng một lúc và các giao dịch chưa được thực hiện trong một khối được coi là chưa được xác nhận. Mỗi nút có thể nhóm các giao dịch với nhau thành một khối và gửi nó vào mạng lưới như một hàm ý cho các khối tiếp theo được gắn vào sau đó.
Vì bất kỳ nút nào cũng có thể tạo một khối mới nên có một câu hỏi đặt ra là cả hệ thống sẽ đồng thuận với khối nào sẽ là khối tiếp theo?
Để được thêm vào blockchain, mỗi khối phải chứa một đoạn mã đóng vai trò như một đáp án cho một vấn đề toán học phức tạp được tạo ra bằng hàm mã hóa băm không thể đảo ngược.

Cách duy nhất để giải quyết vấn đề toán học như vậy là đoán các số ngẫu nhiên, những số khi mà kết hợp với nội dung khối trước tạo ra một kết quả đã được hệ thống định nghĩa. Do trong mạng lưới luôn có một số lượng lớn các máy tính đều tập trung vào việc đoán ra dãy số này nên mạng lưới quy định mỗi khối được tạo ra sau một quãng thời gian là 10 phút một lần. Nút nào giải quyết được vấn đề toán học như vậy sẽ được quyền gắn khối tiếp theo lên trên chuỗi và gửi nó tới toàn bộ mạng lưới

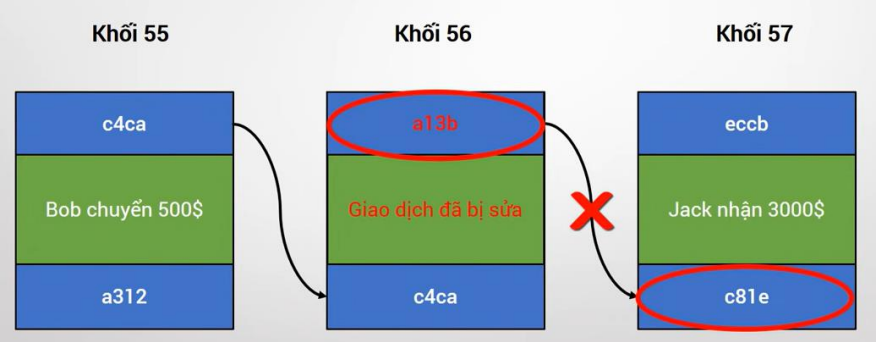
### 1.4.4 Thuật toán bảo mật Blockchain

Nếu có bất kỳ sự bất đồng về khối đại diện sau cùng của chuỗi thì điều này sẽ dẫn đến khả năng gian lận. Nếu một giao dịch xảy ra trong 1 khối thuộc về đuôi ngắn hơn khi khối tiếp theo được giải quyết, giao dịch đó sẽ trở lại thành giao dịch chưa được xác nhận vì tất cả các giao dịch khác được nhóm vào trong khối kia.

Mỗi block chứa một tham chiếu đến khối trước đó, và tham chiếu đó là một phần của vấn đề toán học cần được giải quyết để truyền khối sau tới mạng lưới. Vì vậy, rất khó để tính toán trước một loạt các block bởi nó cần tính ra một số lượng lớn các số ngẫu nhiên cần thiết để giải quyết một khối và đặt nó trên blockchain.

Nếu một Hacker muốn thay đổi dữ liệu của một khối 56 thì hàm băm của khối đó sẽ thay đổi như thế thì hàm băm của khối sau nó sẽ không hợp lệ và bắt buộc là

hacker phải đưa mã đã được thay đổi vào khối 57 và mã sẽ lại thay đổi như thế hacker sẽ phải thay đổi toàn bộ các khối còn lại. Như thế sẽ rất tốn thời gian và tài nguyên. Ngoài ra, kể cả hacker đã thay đổi hết các khối thì cũng sẽ phải đổi dữ liệu ở cả các máy khác nữa. Vì dữ liệu được lưu phân tán ở các máy và theo cơ chế đồng thuận phi tập trung thì hacker phải thay đổi tối thiểu là 51% số máy để có thể chiếm quyền trong mạng .




## 1.5 Các phiên bản của Blockchain

**Blockchain 1.0 – Tiền tệ và Thanh toán**: Ứng dụng chính của phiên bản này là tiền mã hoá: bao gồm việc chuyển đổi tiền tệ, kiều hối và tạo lập hệ thống thanh toán kỹ thuật số. Đây cũng là lĩnh vực quen thuộc với chúng ta nhất mà đôi khi khá nhiều người lầm tưởng Bitcoin và Blockchain là một.

**Blockchain 2.0 – Tài chính và Thị trường:** Ứng dụng xử lý tài chính và ngân hàng: mở rộng quy mô của Blockchain, đưa vào các ứng dụng tài chính và thị trường. Các tài sản bao gồm cổ phiếu, chi phiếu, nợ, quyền sở hữu và bất kỳ điều gì có liên quan đến thỏa thuận hay hợp đồng.

**Blockchain 3.0 – Thiết kế và Giám sát hoạt động:** Đưa Blockchain vượt khỏi biên giới tài chính, và đi vào các lĩnh vực như giáo dục, chính phủ, y tế và nghệ thuật. Ở những lĩnh vực này sẽ là lại có nhiều loại như physical, digital hay human in nature.

# II. Ưu nhược điểm của công nghê Blockchain

## 2.1 Ưu điểm

**Tính minh bạch :** Công nghệ Blockchain mang dến nhiều bước tiến trong việc cải thiện tính minh bạch.

**Tính phi tập trung :** Các hệ thống được xây dựng dựa trên công nghệ Blockchain có thể hoạt động trên mạng lưới máy tính phi tập trung, từ đó giảm thiểu các rủi ro bị tấn công, thời gian chết trên máy chủ và gây thất thoát dữ liệu.

**Loại bỏ đơn vị trung gian:** Các hệ thống được xây dựng dựa trên công nghê Blockchain cho phép có thể loại bỏ các đơn vị trung gian liên quan đến hoạt động lập hồ sơ, ghi chép dữ liệu và chuyển giao tài sản.

**Sự tin cậy**: Các hệ thống xây dựng dựa trên công nghệ Blockchain làm gia tăng niềm tin giữa các bên giao dịch nhờ tinh minh bạch được cải thiện và mạng lưới phi tập trung và đồng thời loại bỏ được các đơn vị trung gian không cần thiết.

**Tiết kiệm chi phí**: Sổ cái thiết lập trên nền tảng Blockchain cho phép loại bỏ đơn vị trung gian và các lớp xác nhận trong giao dịch. Các giao dịch dù cần nhiều số cải riêng biệt, đều có thể thiết lập trên một số cái chung, từ đó giảm thiểu chi phi kiếm nhận, xác thực và thẩm tra một giao dịch.

**Độ bảo mật**: Dữ liệu nhập vào Blockchain sẽ không thể sửa đổi, qua đó tránh được tinh trạng gian lận qua việc ngụy tạo giao dịch và giả mạo lịch sử dữ liệu. Các giao dịch đưa vào Blockchain sẽ tạo nên một lịch sử hoạt động rõ ràng minh bạch từ điểm khởi đầu của Blockchain, cho phép dễ dàng thẩm tra và kiểm kê mọi giao dịch.

**Công nghệ dễ tiếp cận**: Cùng với tiềm năng ứng dụng rộng rãi, công nghệ Blockchain còn giúp việc tạo lập các ứng dụng dễ dàng hơn, nhờ các bước tiến hiện nay như nên tàng Ethereum, mà không cần phải đầu tư quá nhiều vào cơ sở hạ tầng. Các ứng dụng phi tập trung, các hợp đồng thông minh và nền tang Ethereum.

**Tăng tốc độ giao dịch**: Do có khả năng loại bỏ đơn vị trung gian và thiết lập trên số cái phân tán cho phép tăng tốc độ giao dịch cao hơn so với nhiều hệ thống hiện nay.

**Tiềm năng ứng dụng rộng**: Đa phần mọi giá trị đều có thể có thể được lập hồ sơ dựa trên Blockchain và nhiều công ty trong nhiều lĩnh vực công nghệ đã phát triển các hệ thống dựa trên công nghệ Blockchain

## 2.2 Nhược điểm

**Tấn công 51%**

Một cuộc tấn công 51% có thể xảy ra nếu có một đơn vị kiểm soát hơn 50% sức mạnh băm của mạng lưới. Điều này sẽ cho phép đơn vị này phá vỡ mạng lưới bằng cách cố ý ngăn chặn hoặc sửa đổi việc đặt các giao dịch.

Mặc dù về mặt lý thuyết là có thể xảy ra, nhưng thực tế là chưa bao giờ có cuộc tấn công 51% thành công nhắm vào blockchain Bitcoin. Khi mạng lưới phát triển lớn hơn, bảo mật sẽ tăng lên và rất khó có khả năng có thợ đào nào đó sẽ đầu tư số tiền và tài nguyên lớn để tấn công Bitcoin nên tốt hơn cả là thợ đào sẽ hành động trung thực để nhận thưởng. Ngoài ra, một cuộc tấn công 51% thành công sẽ chỉ có

thể sửa đổi các giao dịch gần đây nhất trong một khoảng thời gian ngắn vì các khối được liên kết thông qua các bằng chứng mật mã (để thay đổi các khối cũ hơn, sức mạnh tính toán sẽ là không tưởng). Ngoài ra, blockchain Bitcoin rất linh hoạt và sẽ nhanh chóng thích ứng như là một phản ứng trước một cuộc tấn công.

**Sửa đổi dữ liệu**

Một nhược điểm khác của các hệ thống blockchain là một khi dữ liệu đã được thêm vào blockchain thì việc sửa đổi là rất khó. Mặc dù tính ổn định là một trong những lợi thế của blockchain, nhưng nó không phải lúc nào cũng tốt. Việc thay đổi dữ liệu hoặc mã blockchain thường rất phức tạp và thường cần có một hard fork, trong đó một chuỗi sẽ bị bỏ và một chuỗi mới được đưa lên.

**Chìa khóa cá nhân :**

Blockchain sử dụng mật mã chìa khóa công khai (hoặc bất đối xứng) để cung cấp cho người dùng quyền sở hữu đối với các đơn vị tiền điện tử của họ (hoặc bất kỳ dữ liệu blockchain nào khác). Mỗi tài khoan blockchain (hoặc địa chỉ) có hai chia khóa tương ứng, một chia khóa chung (có thể chia sẻ) và một chia khỏa cá nhân (cần được giữ bí mật). Người dùng cần chia khóa cá nhân để truy cập vào tiền của họ, nghĩa là tự họ đóng vai trò như một ngân hàng. Nếu người dùng mất chìa khóa cá nhân, tiền sẽ bị mất và không thể làm gì hơn được nữa.

**Không hiệu quả**

Các blockchain, đặc biệt là những loại đang sử dụng Proof of Work, là rất kém hiệu quả. Lý do là vì đào có tính cạnh tranh cao và cứ sau mười phút lại có một người chiến thắng nên công sức của các thợ mỏ khác sẽ bị lãng phi. Khi các thợ mỏ liên tục cố gắng tăng sức mạnh tinh toán, họ sẽ có cơ hội tìm được lời giải hợp lệ cao hơn. Do đó các tài nguyên được sử dụng bởi mạng lưới Bitcoin đã tăng đáng kể trong vài năm qua, và hiện tại lượng điện tiêu thụ dành cho bitcoin đã vượt qua nhiều quốc gia, chẳng hạn như Đan Mạch, Ireland và Nigeria.

**Lưu trữ**

Các số cái Blockchain có thể phát triển rất lớn theo thời gian. Blockchain Bitcoin hiện cần khoảng 200 GB dung lượng lưu trữ. Tốc độ tăng kích thước hiện tại của blockchain có vẻ như vượt xa tốc độ tăng dung lượng lưu trữ của các ổ đĩa cứng. Mạng lưới có nguy cơ mất các node nếu kích thước của số cái là quá lớn để

các cá nhân tài xuống và lưu trữ.

# III. ỨNG DỤNG CỦA BLOCKCHAIN

Một số ứng dụng Blockchain phổ biến trong hiện nay như:

Những ứng dụng nổi bật của Blockchain: 1, 2, 3, 4, 7

## 1. DỊCH VỤ TÀI CHÍNH & NGÂN HÀNG

Do đặc thù của ngành tài chính ngân hàng rất dễ xảy ra tình trạng tập trung quyền lực, xâm phạm bảo mật dữ liệu người dùng nên với công nghệ Blockchain hiện nay, những vấn đề này sẽ dễ dàng được giải quyết. Nhờ chức năng hợp đồng thông minh, nó có thể bỏ qua các bên trung gian, tiết kiệm chi phí, tăng tốc độ giao dịch, hạn chế rủi ro tài chính trong quá trình thanh toán và cải thiện hệ thống quản lý thông tin công nghệ cũ.

**Một số ứng dụng của Blockchain trong lĩnh vực tài chính & ngân hàng:**

- Xác thực thông tin khách hàng, khả năng tín dụng: Cho phép giao dịch ngay cả không có trung gian xác minh.
- Mạng lưới sẽ xác minh và thanh toán những giao dịch ngang hàng, công việc này được thực hiện liên tục nên sổ cái luôn được cập nhật.
- Quản lý rủi ro, hạn chế rủi ro trong thanh toán vì trục trặc kỹ thuật, vỡ nợ trước khi thanh toán giao dịch.
- Hệ thống quản lý thông minh: Blockchain cho phép liên tục đổi mới, lặp lại và cải tiến, dựa trên sự đồng thuận trong mạng lưới.

## 2. SẢN XUẤT

Trong quá trình sản xuất, chúng ta cần một sổ cái để theo dõi quá trình sản xuất, tồn kho, phân phối, chất lượng, thông tin giao dịch … Blockchain sẽ thay thế các thiết bị thông minh cấp quyền quản lý, nâng cao hiệu quả và tăng đáng kể năng suất của quản lý chuỗi cung ứng quá trình.

Đối với người tiêu dùng, việc kiểm tra được tính xác thực của thông tin sản phẩm có thể ngăn chặn được hàng giả, hàng kém chất lượng trên thị trường.

**Một số ứng dụng của Blockchain trong sản xuất:**

- Theo dõi lịch trình sản xuất, số lượng hàng mua vào và bán ra.
- Quản lý hàng tồn kho, kho bãi sản xuất.

- Truy xuất nguồn gốc sản phẩm được sản xuất qua các khâu.
- Theo dõi nguồn cung cấp nguyên liệu sản xuất trong công nghiệp.

**3. Y TẾ**

Trong thời đại công nghệ 4.0, các nước trên thế giới và Việt Nam đang đẩy mạnh triển khai số hóa thông tin trong quy trình quản lý dữ liệu trong đó có lĩnh vực y tế và chăm sóc sức khỏe. Blockchain được sử dụng trong quản lý tài sản và lưu trữ thông tin sức khỏe của bệnh nhân, quản lý hàng tồn kho, đơn đặt hàng, thanh toán thiết bị y tế và thuốc. Mặc dù có nhiều thiết bị thông minh có thể giám sát các dịch vụ này nhưng vẫn có nhiều hạn chế trong việc bảo mật thông tin cá nhân của bệnh nhân. Do đó, Blockchain là sự lựa chọn hàng đầu.

**Một số ứng dụng của Blockchain trong lĩnh vực y tế:**

- Ứng dụng phát triển bao gồm theo dõi và quản lý bệnh lý (như thuốc thông minh, thiết bị đeo có thể đo các chỉ số về sức khỏe và đưa ra phản hồi) và tăng cường quản lý chất lượng.
- Quản lý chuỗi cung ứng thuốc, thiết bị y tế: Theo dõi đầu vào, nguồn gốc, hạn sử dụng của các vật tư y tế.
- Tăng cường tính minh bạch và tự động hóa trong các giao dịch khám chữa bệnh; xuất xứ xét nghiệm lâm sàng; quyền sở hữu dữ liệu sức khỏe của bệnh nhân.

**4. GIÁO DỤC**

Khi Blockchain được ứng dụng vào giáo dục, thông tin lưu trữ trên Blockchain không chỉ là dữ liệu bảng điểm mà còn là quá trình đào tạo, kinh nghiệm thực tế và kinh nghiệm tuyển dụng của mỗi người. Tránh tình trạng ứng viên gian lận trong quá trình xin học bổng, thăng tiến, v.v …; trình bày sai về trình độ học vấn, kinh nghiệm làm việc, kỷ luật, v.v.

Không chỉ vậy, thông qua chức năng hợp đồng thông minh, Blockchain còn có thể tự động thực hiện các điều khoản của nội quy đào tạo, xử lý các trường hợp vi phạm nội quy, cải thiện các hạn chế trong quá trình giảng dạy khi cần thiết và học viên có thể đưa ra phản hồi.

**Một số ứng dụng của Blockchain trong lĩnh vực giáo dục:**

- Hệ thống quản lý mức độ đánh giá sự uy tín trong nghiên cứu khoa học.

- Ghi lại cơ sở dữ liệu bảo mật về dữ liệu học tập và điểm số cho các hệ thống học trực tuyến, đánh giá năng lực của một cá nhân dựa trên các yêu cầu tuyển sinh đầu vào.
- Theo dõi và lưu trữ bảng điểm và bằng cấp của sinh viên và thông tin của các đơn vị đào tạo.
- Xem xét cá nhân/ứng viên có phù hợp với công việc giảng dạy hay không, từ đó đưa ra quyết định mời cá nhân đó làm việc.
- Hệ thống quản lý thông minh: Blockchain cho phép liên tục đổi mới, lặp lại và cải tiến, dựa trên sự đồng thuận trong mạng lưới.

**5. BÁN LẺ**

Vấn đề nan giải nhất đối với các nhà bán lẻ là quá trình phân phối hàng hoá, kho bãi cũng như quản lý thông tin sản phẩm số lượng lớn. **Blockchain** được ứng dụng như một cuốn sổ cái ghi chép thông tin chính xác với tính bảo mật cao. Nó cho phép quản lý hồ sơ về từng mặt hàng, vị trí của nó, cách xử lý, mọi thiệt hại trong quá trình phân phối, từ đó hỗ trợ hiệu quả cho các nhà bán lẻ.

**Ứng dụng của Blockchain trong lĩnh vực bán lẻ:**

- Theo dõi các mặt hàng sản xuất qua từng mã định danh lưu trên hệ thống Blockchain.
- Hợp đồng thông minh: khi có sự trao đổi hàng hóa giữa nhà sản xuất và công ty vận tải, cả hai đều đồng ý rằng mặt hàng đó đảm bảo chất lượng.
- Quản lý thông tin mặt hàng, thời gian vận chuyển, lưu kho, tồn kho.
- Hợp đồng thông minh trên Blockchain chứa đựng các thỏa thuận giữa các thực thể này để quản lý dòng tiền của các giao dịch hoặc xử lý thiệt hại khi cần thiết

**6. THƯƠNG MẠI ĐIỆN TỬ**

Theo chuyên gia, thị trường bán lẻ hiện nay đang dần chuyển hướng sang thương mại trực tuyến đặc biệt là với sự phát triển của các sàn thương mại điện tử. Sự dịch chuyển này đặt ra vấn đề về tính bảo mật, quản lý chuỗi cung ứng, quá trình vận chuyển hàng hoá đến người tiêu dùng, chi phí từ cách làm truyền thống tạo nên nhiều rào cản giữa người tiêu dùng và nhà sản xuất.

**Công nghệ Blockchain** giải quyết vấn đề đó bằng các hợp đồng thông minh, tạo

điều kiện cho các bên có thể dễ dàng ký kết, liên kết với các doanh nghiệp đa quốc gia. Việc lược bỏ trung gian cũng giúp tiết kiệm chi phí, giải pháp thanh toán cũng được gắn trực tiếp trên các website, sàn thương mại điện tử.

**Một số ứng dụng của Blockchain trong lĩnh vực thương mại điện tử:**

- Quản lý thông tin dữ liệu khách hàng.
- Theo dõi thông tin, tình trạng sản phẩm thông qua **số serial**, **QR**.
- Xây dựng hệ thống thanh toán và chấp nhận ví điện tử, khách hàng thân thiết, thẻ quà tặng, tri ân khách hàng….
- Vận hành và quản lý chuỗi cung ứng

## 7. VẬN TẢI VÀ LOGISTICS

Trong vòng đời của một sản phẩm, qua mỗi bước trong chuỗi cung ứng, dữ liệu được tạo ra và được ghi lại dưới dạng các giao dịch, tạo ra lịch sử vĩnh viễn cho sản phẩm. **Blockchain** chính là công cụ để quản lý kho dữ liệu khổng lồ đó. **Blockchain** có thể giúp tăng tính hiệu quả trong việc chia sẻ thông tin về quá trình sản xuất, vận chuyển, bảo quản, sự hao mòn giá trị của sản phẩm tới các bên liên quan. Giải quyết những vấn đề thách thức trong logistics như độ trễ trong giao nhận hàng, mất các giấy tờ, chứng từ, tài liệu, nguồn gốc sản phẩm không rõ ràng, cùng các lỗi khác trong quá trình chuyển giao giữa các thành viên trong chuỗi hoạt động logistics.

**Một số ứng dụng của Blockchain trong lĩnh vực vận tải và logistics :**

- Truy xuất nguồn gốc, xác thực giấy tờ minh bạch, rõ ràng.
- Đóng gói thông minh.
- Kết hợp trí tuệ nhân tạo (AI) và Internet vạn vật để giám sát hành trình vận chuyển cũng như các phương tiện vận chuyển.
- Giảm chi phí trung gian, tiết kiệm chi phí nhờ áp dụng hợp đồng thông minh.

## 8. NÔNG NGHIỆP

Chuỗi thực phẩm cần trở nên bền vững hơn để nâng cao lòng tin và sự trung thành của người tiêu dùng, và chìa khóa để nâng cao lòng tin là khả năng truy xuất nguồn gốc hiệu quả. Hệ thống sổ cái phân tán sẽ giúp nhà bán lẻ và người tiêu dùng lưu trữ thông tin giao dịch, đồng thời tăng tính minh bạch của thông tin trong suốt quá trình sản phẩm từ cơ sở sản xuất đến cơ sở chế biến. Nhà phân phối, siêu

thị, cửa hàng bán lẻ và cuối cùng là người tiêu dùng.

Các dữ liệu liên quan tới quản lý chất lượng, quản lý giá cả, quản lý tài chính, quản lý bán hàng đều có thể được tiếp tục cập nhật vào trong chuỗi **Blockchain.**

**Một số ứng dụng của Blockchain trong lĩnh vực nông nghiệp:**

- Quản lý chuỗi cung ứng sản phẩm, chuỗi phân phối hàng tồn kho.
- Lưu trữ thông tin hàng hóa, quy trình chăm sóc, các tiêu chuẩn cho thực phẩm sạch.
- Truy xuất nguồn gốc, vòng đời sản xuất nông sản.

## 9. DU LỊCH

Thông tin khách hàng được chuyển đổi từ nhiều hệ thống từ khâu lựa chọn đại lý, đặt vé xe, đặt phòng khách sạn đến các địa điểm thăm quan, do đó đòi hỏi tính ổn định và bảo mật cao. Bên cạnh đó chi phí giao dịch cũng là yếu tố được cân nhắc trong quá trình khai thác ngành dịch vụ không khói này. **Blockchain** tham gia giải quyết các vấn đề trên, thay thế hệ thống quản lý truyền thống nhiều trục trặc, sai sót.

**Một số ứng dụng của Blockchain trong lĩnh vực du lịch:**

- Theo dõi hành lý, đặt phòng khách sạn, vé máy bay.
- Dịch vụ nhận dạng: Tiết kiệm thời gian cho quá trình check in tại các sân bay, khách sạn, địa điểm du lịch.
- Thanh toán đa dạng: Cho phép thanh toán đến từ nhiều ngân hàng toàn cầu, ví điện tử, tiền điện tử…
- Thông tin khách hàng thân thiết, khách VIP…

## 10. TRUYỀN THÔNG VÀ VIỄN THÔNG

Triển khai các giải pháp **Blockchain** trên nền tảng đám mây sẽ giúp các nhà cung cấp dịch vụ truyền thông tối ưu hóa các quy trình hiện có trong khi tăng cường bảo mật mạng, rà soát lại toàn bộ quy trình vận hành, các quy trình như chuyển vùng và quản lý danh tính trong mô hình kinh doanh của mình. Từ đó cải thiện và phát triển dịch vụ tốt hơn.

**Một số ứng dụng của Blockchain trong lĩnh vực truyền thông và viễn thông:**

- Phòng chống gian lận trong chuyển vùng: các thỏa thuận chuyển vùng giữa các nhà khai thác sẽ trở nên minh bạch, các nút được chỉ định có thể đóng vai

trò là trình xác nhận (người khai thác) để xác minh từng giao dịch được phát trên mạng.

- Quá trình chuyển đổi 5G: các quy tắc và thỏa thuận giữa các mạng khác nhau sẽ có dạng hợp đồng thông minh, tự thực hiện có thể kết nối các thiết bị với nhà cung cấp dịch vụ gần nhất đồng thời đánh giá sự liên tục của kết nối và tính phí dịch vụ.
- Kết nối Internet vạn vật: tạo ra một môi trường an toàn hơn để truyền dữ liệu bằng cách tạo các mạng lưới tự quản ngang hàng an toàn cao.

-Hiện nay ở Việt Nam, công nghệ Blockchain được áp dụng chủ yếu trong các lĩnh vực tài chính-ngân hàng, chuỗi cung ứng, bảo hiểm, bất động sản, y tế, tiêu dùng và quản lý tổ chức. Trong đó hơn 80% là ứng dụng trong lĩnh vực tài chính ngân hàng, cụ thể như:

+Thanh toán quốc tế

+Thanh toán bù trừ, giao dịch liên ngân hàng

+Xác minh danh tính kĩ thuật số

+Cho vay, bảo lãnh, thu thuế, kiểm toán

+Tín dụng

+Mua bán tài sản

-Tuy nhiên việc ứng dụng công nghệ Blockchain ở Việt Nam còn gặp nhiều khó khăn về cơ sở hạ tầng, chi phí, các tiêu chuẩn, quy chuẩn kỹ thuật và nguồn nhân lực chất lượng cao, … Tuy nhiên đó chỉ là những bước đầu trong việc phát triển công nghệ Blockchain ở Việt Nam

# IV. Khảo sát các nền tảng chạy công nghệ chuỗi khối

## 4.1 .Ethereum

**Giới thiệu**

Ethereum là một nền tảng phần mềm mã nguồn mở, phân tán dựa trên công nghệ blockchain.

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.

**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.

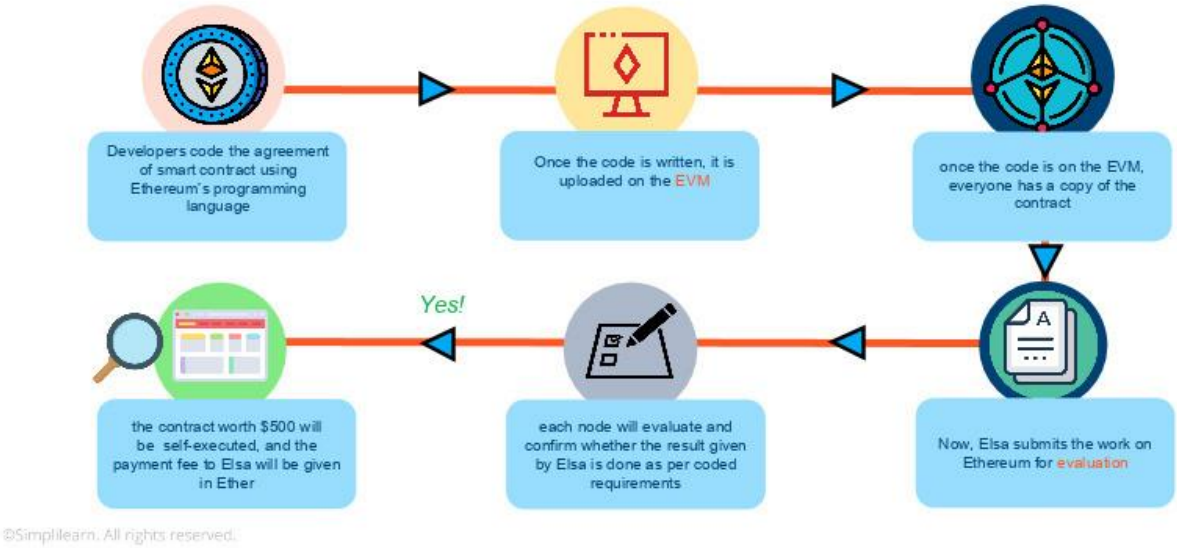
Máy ảo EVM thực thi hoạt động như lệnh giao dịch, smart contract(hợp đồng thông minh),… Mạng lưới cần đến một lượng phí gọi là Gas – phí thanh toán bằng đồng tiền kỹ thuật số gọi là Ether (ETH).

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.




**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

## 4.2 Stellar

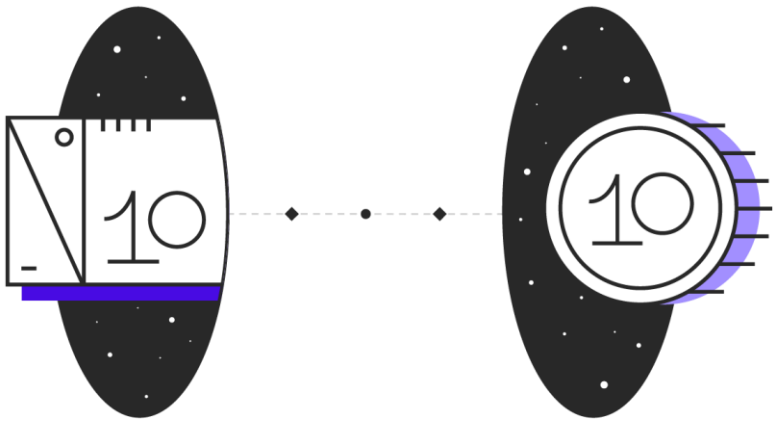
Stellar là một dự án mạng mã nguồn mở, hướng tới việc giải quyết các vấn đề về tiền tệ và thanh toán. Stellar cung cấp khả năng tạo, gửi và trao đổi các token biểu diễn các loại tiền như dollars, pesos, bitcoin,... dưới dạng kĩ thuật số. Nó được thiết kế với mục tiêu đưa toàn bộ hệ thống tài chính thế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



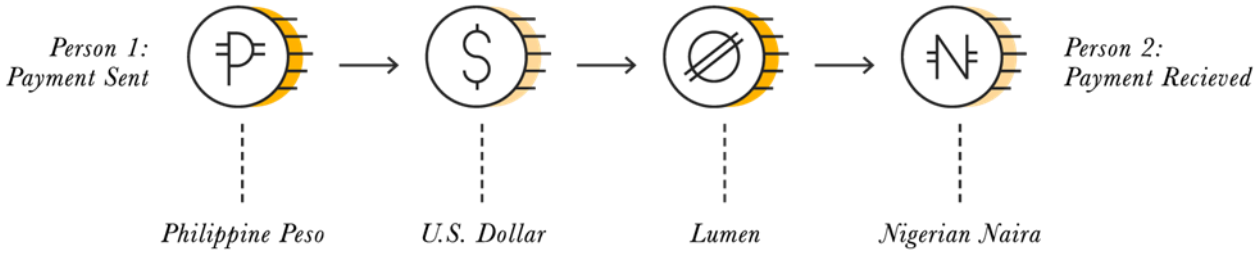

*Traditional Dollar* *"Dollar Token"*

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.

| mechanism | decentralized control | low latency | flexible trust | asymptotic security |
|---|---|---|---|---|
| proof of work | ✓ | | | |
| proof of stake | ✓ | maybe | | maybe |
| Byzantine agreement | | ✓ | ✓ | ✓ |
| Tendermint | ✓ | ✓ | | ✓ |
| SCP (this work) | ✓ | ✓ | ✓ | ✓ |

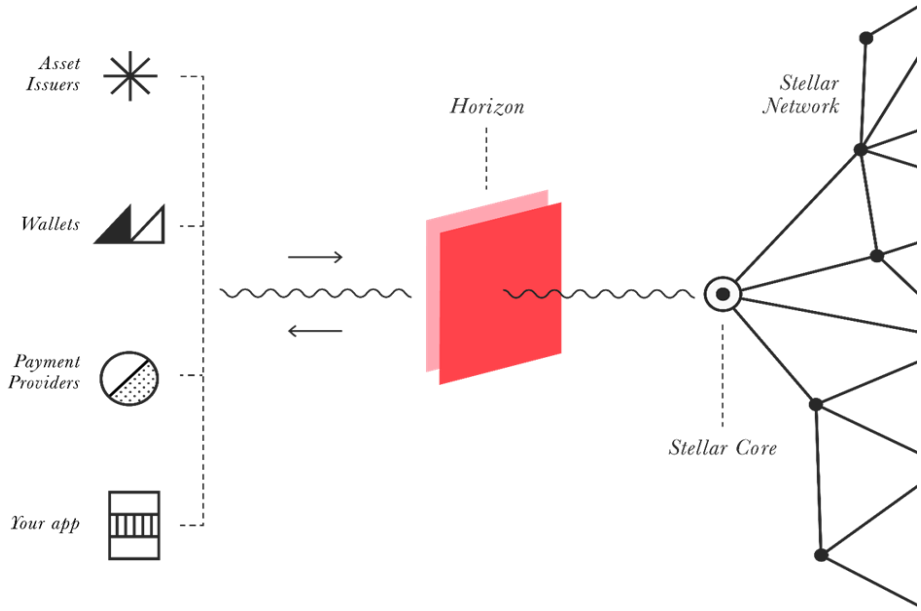
Fig. 1. Properties of different consensus mechanisms

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**



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.
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.

## 4.3 Nền tảng thử nghiệm Coursera.

1.Coursera là gì ?

Coursera, một trong những nền tảng học trực tuyến hàng đầu thế giới.

Coursera là một công ty công nghệ giáo dục chuyên cung cấp các khoá học trực tuyến đại chúng mở (massive open online course - MOOC). Công ty được thành lập bởi hai giáo sư khoa học máy tính Andrew Ng và Daphne Koller thuộc Đại học Stanford. Coursera hợp tác với nhiều trường đại học trên thế giới để cung cấp một số khoá học trên mạng của các trường này cho người đăng ký, các khoá học có thể thuộc ngành khoa học kỹ thuật, nhân văn học, y học, sinh học, khoa học xã hội, toán học, kinh tế học, khoa học máy tính và một số lĩnh vực khác.


Coursera là sự kết hợp giữa "Course" mang nghĩa khóa học và "era" được hiểu là kỷ nguyên. Qua đó chúng ta cũng có thể thấy được tầm nhìn và định hướng phát triển cho nền tảng học trực tuyến này từ những nhà sáng lập.

Nó cung cấp hàng nghìn khóa học trực tuyến với sự hợp tác của hơn 200 trường đại học và công ty hàng đầu thế giới, bao gồm Yale, Princeton, UPenn, Google, IBM, Amazon, Facebook , …Các khóa học trên mạng miễn phí trong các ngành học như Nhân văn, Y Dược, Sinh học, Khoa học Xã hội, Toán học, Kinh tế học, Khoa học máy tính, và một số ngành khác.

Cơ sở hạ tầng CNTT

Coursera triển khai chương trình phục vụ mạng nginx trên hệ điều hành Linux trên nền của Amazon Web Services. Dữ liệu được lưu trữ ở Amazon S3 và việc tìm kiếm địa chỉ trang mạng được thực thi bởi chương trình CloudSearch với hơn 4,3 triệu tài liệu trên trang mạng. Trong mỗi tháng, cơ sở dữ liệu của chương trình phục vụ của Coursera (chạy trên RDS) trả lời hơn 10 tỉ truy vấn SQL, và Coursera phục vụ khoảng 500TB lưu lượng dữ liệu hàng tháng.

**2.Vấn đề của Coursera**.

Với một lượng dữ liệu vô cùng lớn liên quan đến các khóa học, dữ liệu giảng viên, bài học, dữ liệu tài khoản sinh viên, dữ liệu bảng điểm trong quá trình đào tạo. Để tránh các vấn đề gian lận về kết quả, cũng như vấn đề vi phạm bản quyền, kinh nghiệm làm việc, trình độ học vấn. Thì BlockChain được áp dụng để bảo đảm các vấn đề trên. Thông qua chức năng hợp đồng thông minh, thì blockchain có thể tự động thực hiện các điều khoản của nội quy đòa tạo, xử lý các trường hợp vi phạn nội quy, cải thiện các hạn chế trong quá trình giảng dạy.

Với quá nhiều khóa học BlockChain có thể quản lý mức độ đánh giá sự uy tín trong nghiên cứu khoa học. Đảm bảo vấn đề bản quyền sở hữu trí tuệ với mỗi khóa học được cung cấp.

Ghi lại cơ sở dữ liệu bảo mật về dữ liệu học tập và điểm số cho các hệ thống học trực tuyến, đánh giá năng lực của một cá nhân dựa trên các yêu cầu tuyển sinh đầu vào. Với một nền tảng học trực tuyến hàng đầu thế giới, Coursera cần giải quyết vấn đề dữ liệu học viên một cách triệt để. Với nền tảng BlockChain vấn đề này sẽ được giải quyết.

Đây cũng là những ứng dụng của BlockChain đối với vấn đề giáo dục trong đời sống.

## 4.4 Ví điện tử Metamask.

1. Giới thiệu.

Metamask là ví Ethereum cho phép kết nối với chuỗi khối Ethereum. Có nghĩa là ta có thể sử dụng nó để quản lý, chuyển , nhận đồng ETH của mình , đồng thời cũng có thể sử dụng ví này để tương tác với hàng ngàn mã thông báo ERC20 đang phát triển trên BlockChain Ethereum.

Metamask cũng cung cấp cho chúng ta quyền truy cập vào thế giới của website phi tập trung bằng cách cho phép sử dụng một số Ethereum Dapps thông qua nó.


2. Tính năng nổi bật.

- Sử dụng mã nguồn mở.
- Ví Metamask là ví HD. Ưu điểm là thực hiện backup cặp khóa công khai hay riêng tư với tốc độ nhanh và đơn giản hóa công việc.
- Dễ sử dụng.Từ giao diện đến dịch vụ tiền điện tử
- Hỗ trợ khách hàng.
- Giao diện người dùng đơn giản

3. Độ an toàn.

Từ thời điểm chính thức đưa vào sử dụng năm 2016 và tính với thời điểm hiện tại, chưa từng có trường hợp nào bị tấn công khiến mất tiền được ghi nhận. Ví sử dụng các cài đặt sao lưu HD và bản thân các nhà phát triển cũng cam kết thường xuyên cập nhật mã nguồn mở để đảm bảo ví luôn trong trạng thái bảo mật tốt nhất.

Cho phép quản lý danh tính. Khi một Dapp muốn chạy một giao dịch và viết trên Blockchain Ethereum, nó cung cấp cho người dùng một giao diện tính bảo mật.

4. Đặc tả chức năng.

Chức năng đặt hàng

Chức năng chuyển tiền đặt cọc

Chức năng xác nhận người mua hàng đã nhận hàng

Chức năng xác nhận hàng hỏng

Chức năng phân xử nếu 2 bên không tự thỏa thuận được

Chức năng kết nối với trạm BlockChain

Chức năng theo dõi smart contact

# Kết luận

Qua bài báo cáo tìm hiểu về công nghệ chuỗi khối (blockchain) và các ứng dụng, bài báo cáo đã trình bày về các nội dung như :

- Trình bày tổng quan về công nghệ blockchain và các tính chất của blockchain.
- Các ứng dụng của blockchain vào đời sống hiện nay.
- Khảo sát các nền tảng đang chạy công nghệ blockchain

# Tài liệu tham khảo

https://viblo.asia/p/tim-hieu-ve-cong-nghe-blockchain-cac-ung-dung-cua-cong-nghe-chuoi-khoi-blockchain-RQqKLkoO57z

sách công nghệ Blockchain https://thuvienpdf.com/cong-nghe-blockchain

Khảo sát các nền tảng blockchain:

https://vn.beincrypto.com/learn/ethereum-eth-la-gi/

https://www.investopedia.com/terms/e/ethereum.asp#toc-ethereum-vs-bitcoin

https://ethereum.org/en/

https://www.stellar.org/learn/intro-to-stellar

https://viblo.asia/p/stellar-la-gi-stellar-hoat-dong-nhu-the-nao-Az45bzG65xY#_iii-kien-truc-he-thong-stellar-3

giải thích công nghệ blockchain : https://youtu.be/auMA7jIHYvQ

Nghiên cứu công nghệ Blockchain và ứng dụng trong thanh toán điện tử : https://bom.so/rdaMZL (thư viện ptit)