1. **Tìm hiểu về Ethereum:**
2. **Khái niệm**

****

* Ethereum là một nền tảng điện toán có tính chất phân tán công cộng, mã nguồn mở, dựa trên công nghệ chuỗi khối Blockchain. Đặc trưng của Ethereum là hợp đồng thông minh SmartContract (nó tập trung vào các mạng như SmartContract, nhận diện vân tay  ). Khả năng tự đưa ra điều khoản và thực thi thỏa thuận một cách chính xác của hệ thống máy tính mà không hề ngừng nghỉ, chịu sự tác động hay gian lận của bên thứ ba.
* Ethereum (ETH)  không chỉ là một đồng tiền tệ mà nó còn là nền tảng tạo ra nhiều ứng dụng khác thông qua các ngôn ngữ lập trình của mình.
* Ethereum cũng cung cấp một đơn vị tiền mã hoá gọi là ETH. Có thể đựơc chuyển giữa các tài khoản và sử dụng để trả phí giao dịch hay dịch vụ tính toán trên mạng Ethereum.
* Ethereum đã được ra đời cuối 2013 bởi **Vitalik Buterin,** một nhà nghiên cứu tiền mã hóa và nhà lập trình.
* Việc phát triển Ethereum được tài tài trở qua hình thức tài trở đống băng, và đã nhanh chống thu hút được số tiền 156 triệu USD,
* Mặc dù giá trị của Ethereum có giá trị thấp hơn đồng tiền Bitcon, nhưng loại tiền ảo này được đánh giá có tiềm năng rất lớn nhờ những ưu điểm thời gian tạo khối và tiến hành giao dịch nhanh hơn, độ bảo mật cao và lượng.
* Ethereum không bị giảm giá trị trong các năm. Bên cạnh đó không chỉ là tiền ảo, Ethereum còn có thể tạo ra thị trường trực tuyến cho phép người dùng dễ dàng mua bán, trao đổi . Với những đặc tính này, Ethereum được coi là mục tiêu hấp dẫn với nhiều nhà đầu tư

2. Lợi ích của Ethereum

* Vì mạng Blockchain Ethereum được vận hàng bởi hàng ngàn máy tính trên khắp thế giới, các ứng dụng có thể được vận hàng nhờ công suất tính toán của một mạng lưới máy tính toàn cầu đồ sộ.
* Một trong những vấn đề với mạng lưới Bitcoin là, dù mạng này mạnh hơn cả những siêu máy tính hàng đầu thế giới cộng lại nhưng công suất xử lý của nó lại bị lãng phí vào việc tạo ra những số ngẫu nhiên để thêm các khối vào Blockchain.
* Ethereum đưa toàn bộ các máy tính trong mạng lưới kết nối lại với nhau và công suất xử lý của chúng lên mức hiệu dụng cao hơn. Từ đó, giúp các lập trình viên tạo ra nhiều ứng dụng vận hàng nhờ công xuất xử lý gộp của mạng lưới cùng công nghệ Blockchain. Các lập trình viên không cần tạo lập Blockchain của riêng họ và kết nối máy tính vào đó. Ethereum đã xây dựng mạng lưới các máy tính trên Blockchain Ethereum.
* Vitalik Buterin, người sáng lập Ethereum, đã tạo ra một cách tiếp cận độc đáo để phát triển [Blockchain](https://phanlonghi.com/7-cach-blockchain-co-the-bao-ve-moi-truong-va-ngan-can-viec-bien-doi-khi-hau/), EVM. Máy ảo Ethereum (EVM) là một phần mềm hoàn chỉnh Turing chạy trên Blockchain Ethereum. Do đó, thay vì phải xây dựng blockchain riêng biệt cho mọi ứng dụng, các nhà phát triển có thể đơn giản sử dụng mạng Ethereum hiện có và chạy ứng dụng của sự lựa chọn.
* Nền tảng Ethereum còn có máy ảo Ethereum và ngôn ngữ lập trình Solidity. Solidity có thể được sử dụng để sáng tạo nên những ứng dụng phi tập trung hoặc các hợp đồng thông minh mà sau đó được Máy ảo Ethereum thông dịch và vận hành trên Blockchain.

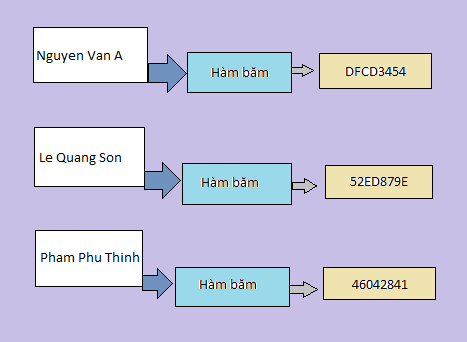
3. Những rủi ro khi giao dịch Ethereum

Vì toàn bộ giao dịch Ethereum đều phải thông qua mạng Internet khiến cho vấn đề an toàn đảm bảo uy tín khi mua bán trở thành một vấn đề vô cùng quan trọng. Những sai sót trong giao dịch, những lỗi bảo mật thông tin sẽ tạo điều kiện cho tội phạm lừa đảo hoặc các hacker khai thác để chiếm đoạt tài sản. Chính vì vậy các nhà đầu tư phải tìm cho mình được một nơi cung cấp, *mua bán Ethereum an toàn* để đầu tư. Đối với những người mới nên ưu tiên thiết lập giao dịch với bạn bè, người thân hoặc các địa chỉ uy tín có tiếng trên thị trường.

**II. Tìm hiểu Hask Function(Hàm Băm)**

1. Khái niệm

* Hash function (hàm băm): tạo ra giá trị băm cho các tương ứng với dữ liệu đầu vào.
* Giá trị băm được xem như là một khóa để phân biệt giữa các dữ liệu đầu vào.
* Mục đích của hàm băm là từ một dữ liệu đầu vào (input) với dung lượng bất kỳ nó sẽ mã hóa dữ liệu này về một dữ liệu khác với dung lượng nhất định

- Tuy nhiên vẫn còn xảy ra hiện tượng trùng khóa khi sử dụng hàm băm.

* Hàm băm thường được dùng trong bảng băm.

-Bảng băm (hash table): là một loại cấu trúc dữ liệu mà mỗi phần tử trong bảng băm là một cặp (khóa, giá trị).

-Hàm băm (hash function): có thể thự hiện nhanh.

-Độ phức tạp của thuật toán là O(n).

-Hàm băm (hash function): dùng để xây dựng cấu trúc dữ liệu.

1. **Hàm băm mật mã (cryptographic hash functions).**

-Là một hàm băm có tính bảo mật, có thể sử dụng hàm băm mật mã trong bảo mật thông tin.

-Các hàm băm thông dụng nhất là MD5 và SHA.

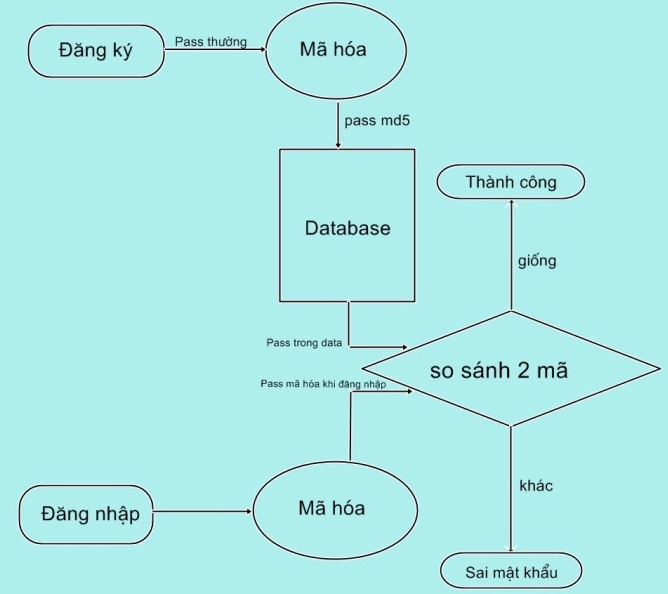
1. MD5

-MD5 là hàm băm mật mã được sử dụng phổ biến với giá trị hash là 128bit. Được thiết kế bởi Ronald Rivest vào năm 1991.

-MD5 được dùng trong các ứng dụng bảo mật cũng như dùng để kiểm tra tính toàn vẹn của thông tin, lưu trữ mật khẩu.

-Giá trị sau khi băm qua MD5 là di nhất và không thể suy ngược lại giá trị ban đầu hay nói một cách khác là hàm băm MD5 không có phần giải mã.

-Ví dụ: Hệ thống sử dụng MD5 để băm mật khẩu của người dùng trước khi lưu vào database. Khi người dùng đăng nhập thì mật khẩu của người dùng nhập trên giao diện đăng nhập sẽ được băm và so sánh với mật khẩu trong database xem có hợp lệ hay không.



1. SHA.

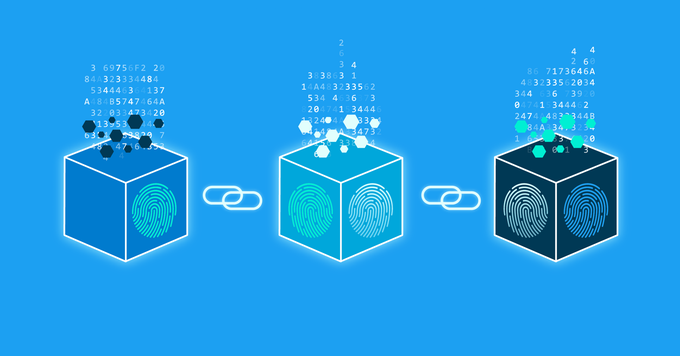
-SHA là giải thuật băm an toàn. SHA là năm giải thuật được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi.

-Năm giải thuật SHA là:

* SHA-1 trả về kết quả 160 bit.
* SHA-224 trả về kết quả 224 bit.
* SHA-256 trả về kết quả 256 bit.
* SHA-384 trả về kết quả 384 bit.
* SHA-512 trả về kết quả 512 bit.
* SHA được phát triển bởi [cục an ninh quốc gia Mĩ](https://vi.wikipedia.org/wiki/C%C6%A1_quan_An_ninh_Qu%E1%BB%91c_gia_Hoa_K%E1%BB%B3) (National Security Agency hay NSA) và được xuất bản thành chuẩn của chính phủ [Mĩ](https://vi.wikipedia.org/wiki/Hoa_K%E1%BB%B3) bởi [viện công nghệ và chuẩn quốc gia Mĩ](https://vi.wikipedia.org/w/index.php?title=NIST&action=edit&redlink=1) (National Institute of Standards and Technology hay NIST).
* SHA-224, SHA-256, SHA-384, SHA-512: được gọi chung là SHA-2
* SHA-1 được sử dụng rộng rãi trong nhiều ứng dụng và giao thức an ninh khác nhau. SHA-1 được xem là giải thuật thay thế cho MD5.
* Hiện nay thì SHA-1 không còn được xem là an toàn nữa. Ba nhà mật mã học người [Trung Quốc](https://vi.wikipedia.org/wiki/Trung_Qu%E1%BB%91c) đã phát triển thành công một giải thuật dùng để tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi SHA-1.

**III. Tìm hiểu về BlockChain**

1.Khái niệm



* Blockchain là hệ thống lưu trữ thông tin trên mạng máy tính cá nhân giúp cho dữ liệu không chỉ được phân phối đến người dùng mà còn được phân nhánh.Điều này có nghĩ là không một công ty doanh nghiệp hay cá nhân nào sở hữu hệ thống, nhưng vẫn có thể sử dụng nó và giúp nó hoạt động.
* Mọi thông tin, mọi giao dịch đều được ghi lại trong các **block**, đều gọi là **Khối**. Một khối sẽ chứa các thông tin sau:
* Index: Chỉ số vị trí của block trong BlockChain.
* Hask: Mã hask là sự kết hợp của các thoogn tin như dữ liệu, mã hask của các khối trước đó, index.
* Previous hask: Mã hask của khối trước đó.
* Data: Thông tin chứa trong Block, như thông tin giao dịch, hợp đồng…
* Timestamp: Thời gian Block được thêm vào BlockChain.
* Loại dữ liệu được lưu trữ bên trong một khối phụ thuộc vào loại BlockChain(Vào vấn đề mà BolckChain đang giải quyết. )
* Điểm nổi bật của BlockChain là đảm bảo rằng các khối đã được ghi lại mọi thông tin thì sẽ không bao giờ bị giả mạo hoặc thay đổi bởi bất kì ai.
* Mỗi một khối mới xuất hiện, cả mạng lưới sẽ biết ngay lập tức. Tính năng này đảm bảo tính công bằng và minh bạch cho cả hệ thống.
* Một khối cũng gần giống như một cơ sở dữ liệu nhưng nó được công khai.
* BlockChain lưu giữ thông tin trên một mạng gồm hàng trăm hàng nghìn máy tính cá nhân khiến cơ sở dữ liệu không chỉ phân cấp mà còn phân tán độc lập. Khi dữ liệu được lưu vào một khối thì nó được mã hóa một cách phức tạp để ngăn chặn việc giả mạo thông tin.
* Hệ thống BlockChain không có máy chủ, khả năng truyền tải dữ liệu mà không đòi hỏi trung gian để xác nhận thông tin. Không có quyền sở hữu bởi 1 ai,mà mọi người có trong hệ thống đều có quyền hạn tương đương và giúp vận hành hệ thống.
* BlockChain có tính bảo mật cao, Vì không có máy chủ và dữ liệu được phân tán độc lập nên khi một máy bị tấn công thì chỉ có máy đó bị ảnh hưởng, phần còn lại của hệ thống vẫn được bảo toàn.

