**BDRPC187TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM**

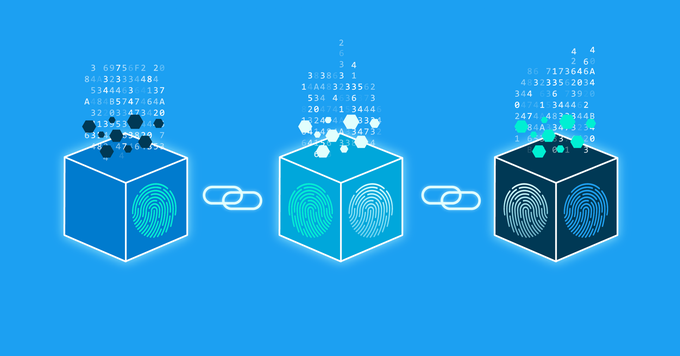
**KHOA ĐÀO TẠO CHẤT LƯỢNG CAO**

**BÁO CÁO MÔN HỌC**

**CÁC CÔNG NGHỆ PHẦN MỀM MỚI**

*ĐỀ TÀI:*

**TÌM HIỂU BLOCKCHAIN**



**Giảng viên: ThS. Nguyễn Minh Đạo**

* **Lê Minh Chương 15110020**
* **Phạm Hồng Cang 15110014**

**MỤC LỤC**

[**I.** **Đặt vấn đề** 4](#_Toc531444005)

[**II.** **Tổng quan về BlockChain (Chuỗi khối)** 4](#_Toc531444006)

[**1.** **Khái niệm BlockChain** 4](#_Toc531444007)

[**2.** **Các thành phần công nghệ của BockChain** 6](#_Toc531444008)

[**3.** **Các đặc điểm chính của BlockChain** 7](#_Toc531444009)

[**4.** **Cách hoạt động của BlockChain** 8](#_Toc531444010)

[**III.** **Tổng quan về Ethereum** 10](#_Toc531444011)

[**1.** **Giới thiệu chung** 10](#_Toc531444012)

[**2.** **Lịch sử ra đời** 10](#_Toc531444013)

[**3.** **Đặc điểm chính của Ethereum** 11](#_Toc531444014)

[**4.** **Những rủi ro khi giao dịch Ethereum** 12](#_Toc531444015)

[**5.** **Các khái niệm cơ bản** 12](#_Toc531444016)

[**5.1.** **Đào mỏ** 12](#_Toc531444017)

[**5.2.** **Ether** 12](#_Toc531444018)

[**5.3.** **Gas** 12](#_Toc531444019)

[**5.4.** **Máy ảo Ethereum** 14](#_Toc531444020)

[**5.5.** **Tài khoản Ethereum** 14](#_Toc531444021)

[**5.6.** **Thông điệp và giao dịch** 15](#_Toc531444022)

[**5.7.** **Thông điệp** 15](#_Toc531444023)

[**5.8.** **Tìm hiểu về Solidity** 16](#_Toc531444024)

[**5.9.** **Ứng dụng phi tập trung** 16](#_Toc531444025)

[**5.10.** **Sự đồng thuận về việc chấp nhận khối** 17](#_Toc531444026)

[**IV.** **Tổng quan về Smart Contract** 17](#_Toc531444027)

[**1.** **Khái niệm** 17](#_Toc531444028)

[**2.** **Ý tưởng ra đời** 18](#_Toc531444029)

[**3.** **Chức năng của Smart Contract** 18](#_Toc531444030)

[**4.** **Cách hoạt động** 18](#_Toc531444031)

[**5.** **Cách lập nên một Smart Contract** 18](#_Toc531444032)

[**6.** **Lợi ích của Smart-Contract** 19](#_Toc531444033)

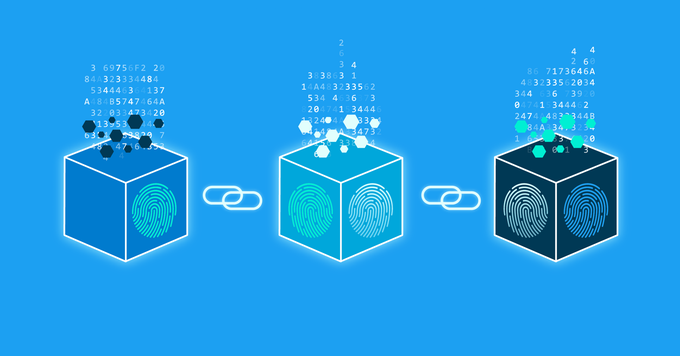
[**7.** **Hạn chế của Smart-Contract** 19](#_Toc531444034)

1. **Đặt vấn đề**

* Trên thế giới hiện nay, nổi lên các hoạt động mua bán, trao đổi tiền ảo rất sôi nổi, trong đó *Bitcoin* và *Ethereum* là hai đồng tiền được nhắc đếnn nhiều nhất, xoay quanh những chủ đề này nhiều người còn quan tâm tới chuỗi khối – một công nghệ đằng sau những tiền ảo này. Công nghệ này đang giúp mọi người dù người lạ hay thân quen, dù ở gần hay ở xa, thậm chí họ không biết đến nhau đều có thể xây dựng một cuốn sổ giao dujch đáng tin cậy cho riêng mình. Đây là yếu tố ý nghĩa vượt xa cả mọi giao thức mã hóa tiền tệ thông thường.
* Với Ethreum, dù ra đời sau nhưng nó cho thấy được những ưu điểm vượt trội hơn Bitcoin về nhiều mặt, người ta xem Ethereum là phiên bản Bitcoin 2.0. Chúng ta sẽ cùng tìm hiểu kỹ hơn về chuỗi khối, về Ethereum và những tiềm năng của chúng.

1. **Tổng quan về BlockChain (Chuỗi khối)**
2. **Khái niệm BlockChain**

* Hệ thống BlockChain được hiện thực hóa vào năm 2018. BlockChain như một cuốn sổ cái kế toán trong kĩ thuật số có khả năng xác thực hiểu quả các giao dịch giữa 2 đối tác. BlockChain đã được thiết lập để ngăn chặn sự thay đổi dữ liệu và mọi thông tin trong BlockChain đều không thể thay đổi và chỉ khi có sự đồng thuận của tất cả các nút trong hệ thống thì thay đổi mới được bổ sung thêm. Đây là công nghệ truyền tải và lưu trữ thông tin bằng các khối liên kết với nhau.



Hình 1: Block trong hệ thống BlockChain

* Trong BlockChain, mỗi khối đều liên kết với các khối trước đó và chứa các thông tin về thời gian khởi tạo đảm bảo thông tin luôn được bảo vệ ngay cả khi một phần của khối bị sụp đổ thì tất cả các thông tin còn lại sẽ không bị ảnh hưởng
* Tóm lại BlockChain về cơ bản là một cơ sở dữ liệu chứa thông tin được người tham gia hệ thống cùng nhau quản lý chứ không phải một cơ quan riêng lẻ như nhà nước hay ngân hàng trung ương… thì thông tin mới muốn được thêm vào cơ sở dữ liệu cần phải có sự chấp thuận của các thành viên trong mạng lưới. Đặc tính này giúp công nghệ BlockChain tạo ra niềm tin về dữ liệu đồng thời giúp giảm đáng kể thời gian và tiền bạc cần phải xác thực giao dịch.
* Khái niệm về **Sổ Cái**:

**+** Sổ cái của BlockChain sử dụng mạng lưới peer-to-peer, có tính phân quyền. (mạng lưới ngang hàng peer-to-peer tức là các node truyền thông tin ngang nhau. Mỗi điểm note đều có thể biết ở đâu diễn ra hoạt động gì và chúng được thực hiện như thế nào, thông tin minh bạch hoàn toàn).

**+** Một sổ cái phân tán là một cơ sở dữ liệu được tổ chức và cập nhật một cách độc lập bởi từng cá nhân tham gia (hay node) trong một mạng lớn. Sự phân phối này là độc nhất: các bản ghi không được truyền đến các node khác, mà thay vào đó là được xây dựng độc lập và tổ chức bởi từng node. Nghĩa là, mỗi node trên mạng xử lý từng giao dịch, đưa ra kết luận của riêng mình và sau đó bỏ phiếu cho những kết luận này để chắc chắn rằng đa số đồng thuận với kết luận đó. Khi đã đồng thuận, sổ cái phân tán sẽ được cập nhật, bản ghi phổ biến nhất sẽ trở thành bản ghi chính thức trên sổ cái.

1. **Các thành phần công nghệ của BockChain**

* Ba thành phần công nghệ của BlockChain:

**+** Mạng ngang hàng: Một nhóm các máy tính có khả năng giao tiếp với nhau mà không phải phụ thuộc vào một người cầm quyền ở trung tâm.

**+** Mật mã bất đối xứng: Cho phép những máy tính này gửi các tin nhắn được mã hóa đến những người nhận đã được xác định vì vậy bất kì ai cũng có thể biết định danh của người gửi, nhưng chỉ người nhận được chỉ định mới có thể đọc nội dung tin nhắn. Ở Bitcoinvà Ethereum, mật mã bất đối xứng được sử dụng để tạo một tập các giấy chứng nhận cho tài khoản của bạn, để chắc chắn rằng chỉ có duy nhất bạn mới có thể chuyển các token của bạn (tiền của bạn).

**+** Phép băm mật mã: Một các để sinh một “dấu vân tay” nhỏ, duy nhất cho bất kỳ dữ liệu nào, cho phép so sánh một cách nhanh chóng các tập dữ liệu lớn và là một cách an toàn để xác nhận rằng dữ liệu đã được thay đổi hay chưa. Ở Bitcoin và Ethereum, cấu trúc dữ liệu cây được sử dụng để ghi lại thứ tự đúng tiêu chuẩn của các giao dịch, sau đó được băm vào một “dấu vân tay” làm cơ sở cho việc so sánh của các máy tính trong mạng.

* Cấu trúc: Mọi thông tin, mọi giao dịch đều được ghi lại trong các khối. Một khối sẽ chứa các thông tin sau:

**+** Index: Thứ tự của khối trong chuỗi

**+** Hash: Giá trị đại diệu cho khối đó. Có đầu vào là Index, Previos Hash, Data, Timestamp và Nonce.

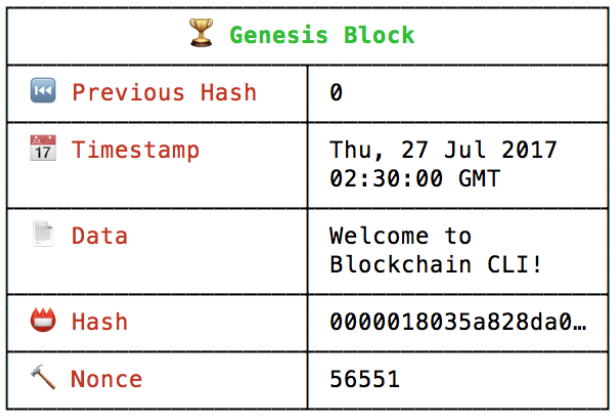
**+** Previos Hash: Giá trị của khối hợp lệ của khối trước đó.

**+** Timestamp: Thời gian khối được thêm vào chuỗi.

**+** Data: Thông tin chứa trong Block, như thông tin giao dịch, hợp đồng…

**+** Nonce: Là giá trị được tìm thất và thêm vào để sau khi băm, ta có giá trị băm hợp lệ.

**+** Genesis block (khối “nguyên thủy”): Mỗi BlockChain sẽ bắt đầu với Block Genesis.



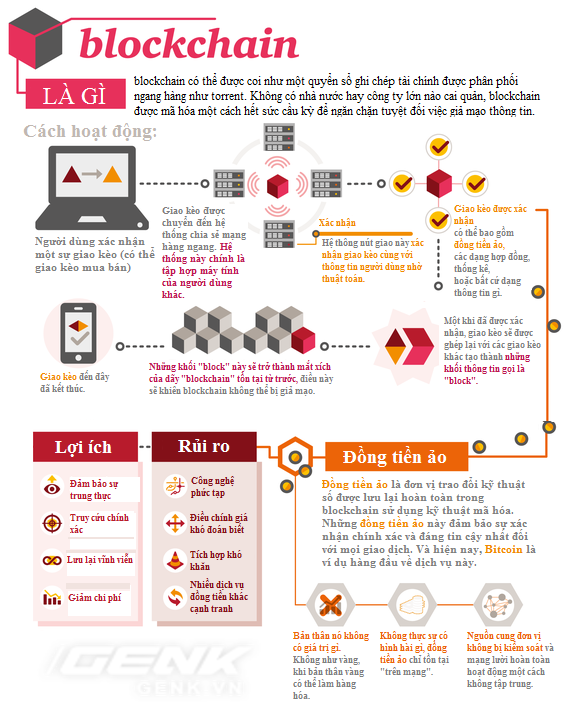
Hình 2: Genesic Block

1. **Các đặc điểm chính của BlockChain**

* Các BlockChain không thể làm giả và không thể phá hủy.Theo lý thuyết thì BlockChain chỉ bị phá hủy khi máy tính lưỡng tử trên thế giới không còn Internet.
* Tính bất biến: Một khi các giao dịch dữ liệu được ghi bởi những người nắm giữ mã khóa bí mật và riêng biệt cho người khởi tạo gọi là Private key, thì dữ liệu đó không thể sửa chữa và nó sẽ được lưu lại mãi mãi.
* Tính bảo mật dữ liệu: Các thông tin dữ liệu của các BlockChain phân tán sẽ được giữ an toàn tuyệt đối và chỉ có người nắm giữ Private key mới có quyền truy xuất dữ liệu ấy.
* Tính minh bạch: Bất cứ ai cũng có thể theo dõi toàn bộ lịch sử đường đi của BlockChain từ địa chỉ nào đến địa chỉ khác nên nó rất minh bạch.
* Hợp đồng thông minh (Smart Contract): Các kĩ thuật số được thực thi nhờ được nhúng bởi một đoạn code là **if-this-then-that(IFTTT) .** Các đoạn code này thay thế cho bên trung gian và nhờ hợp đồng thông minh này thì BlockChain không cần bên thứ 3 như là ngân hàng mà vẫn có thể đảm bảo tất cả các bên tham gia đều biết được chi tiết hợp đồng và các tự động điều khoản đều được thực hiện một khi các điều kiện đều được đảm bảo.

1. **Cách hoạt động của BlockChain**

* BlockChain có những tính năng rất đặc biệt đó là có thể truyền tải dữ liệu mà không thông qua trung gian để các nhận thông tin. Hệ thống BlockChain tồn tại nhiều nút độc lập với khả năng xác nhận thông tin. Mọi thông tin trong chuỗi khối có thể thay đổi hoặc bổ sung thêm khi có sự chấp nhận của tất cả các nút trên hệ thống. Hệ thống này có độ bảo mật cực cao mọi hành động đánh cắp dữ liệu đề sẽ bị chặn đứng.
* BlockChain thậm chí vẫn hoạt động bình thường khi một phần của hệ thống sụp đổ, những máy tính và các nút vẫn hoạt động để bảo vệ thông tin, giữ cho BlockChain không bị mất dữ liệu.

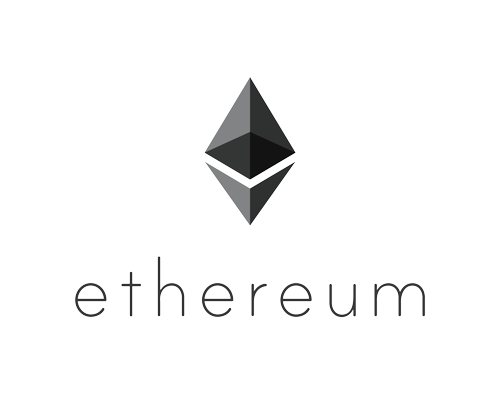


Hình 3: Minh họa cách hoạt động của BlockChain

1. **Tổng quan về Ethereum**
2. **Giới thiệu chung**

* 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 Smart Contract (nó tập trung vào các mạng như Smart Contract, 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 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.

1. **Lịch sử ra đời**



Hình 4: Logo Ethereum

* Ethereum ban đầu được mô tả trong một văn bản của Vitalik Buterin, một lập trình viên liên quan đến Bitcoin vào cuối năm 2013 với mục tiêu xây dựng các ứng dụng phân quyền. Buterin đã lập luận rằng Bitcoin cần một ngôn ngữ kịch bản để phát triển ứng dụng. Không đạt được thỏa thuận với nhóm phát triển Bitcoin, ông đề xuất phát triển một nền tảng mới với một ngôn ngữ kịch bản tổng quát hơn.
* Bốn thành viên ban đầu của nhóm Ethereum là Vitalik Buterin, Mihai Alisie, Anthony Di Iorio và Hoskinson. Phát triển chính thức của dự án phần mềm Ethereum bắt đầu vào đầu năm 2014 thông qua một công ty Thụy Sĩ tên là Ethereum Switzerland Gmb H (EthSuisse). Sau đó, một tổ chức phi lợi nhuận tại Thụy Sĩ với tên gọi là Ethereum Foundation cũng được thành lập. Việc phất triển Ethereum được tài trợ bởi đám đông trực tuyến trong suốt tháng 7 và thánh 8 năm 2014, với những người tham gia mua Ethereum bằng các loại tiền kỹ thuật số khác như Bitcoin. Mặc dù đã có những lời khen ngợi đầu tiên về những đổi mới kỹ thuật của Ethereum, nhưng cũng có các nghi ngờ về tính an toàn và khả năng mở rộng của nó.
* 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.
* 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

1. **Đặc điểm chính 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.

1. **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.

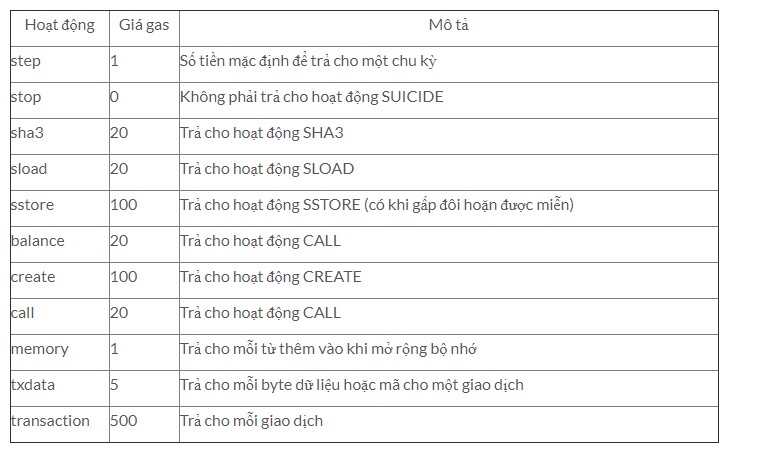
1. **Các khái niệm cơ bản**
   1. **Đào mỏ**

* Do một hệ thống phân phối không có chủ sở hữu duy nhất, các máy có thể được tự do tham gia các mạng Ethereum theo ý thích và bắt đầu các nhận giao dịch. Quá trình này được gọi là đào mỏ.
* Việc đào mỏ đi đến một sự đồng thuận về thứ tự của các giao dịch trên toàn hệ thống, điều này là cần thiết để lập bảng cân đối tài khoản của tất cả mọi người một cách nhanh chóng, ngay cả khi nhiều giao dịch thông qua mạng. Quá trình này tiêu thụ điện năng, đó là chi phí tiền bạc, và vì vậy người thợ đào mỏ được trả một khoản cho mỗi khối họ khai thác: khoảng 5 **ether.**
  1. **Ether**
* Tiền mã hóa được giao dịch trong mạng lưới Ethereum được gọi là ether. Nó được niêm yết dưới mã ETH và giao dịch trên các sàn giao dịch tiền mã hóa. Nó cũng được sử dụng để trả phí giao dịch và dịch vụ tính toán trên mạng Ethereum.
* Đối với tiền ảo, thách thức để được chấp nhận vẫn còn tồn tại. Ngày nay, những tiền ảo này vẫn là một lớp thanh toán, bảo mật và minh bạch nhất trong các hệ thống tiền tệ đang tồn tại được công nhận. Sự triển khai thử nghiệm các đồng tiền ảo này một ngày nào đó có thể thay thế các công nghệ mạng thanh toán tập trung như Visa hay MasterCart ngày nay.
  1. **Gas**
* Gas là một đơn vị được sử dụng để đo lường mức chi phí tính toán (compulationally expensive) có thể tiêu tốn cho một giao dịch trên Ethereum. Giá trị của Gas được quy đổi bằng một lượng ether tương ứng.
* Nói cách khác, Gas không phải là một đơn vị tiền tệ, và chúng ta không thể sử dụng hay tích trữ nó. Nó chỉ đơn giản đo đạc mức tiêu hao của các phép tính toán mà hệ thống phải chịu nếu thực hiện thành công giao dịch. Để có thể trả chi phí Gas, chúng ta chỉ cần thêm ether vào tài khoản. Mọi thứ trên EVM đều có một giá trị Gas nhất định.
* Có 2 lý do chính để Gas ra đời:

**+** Thứ nhất, nó là một phần thưởng đảm bảo được đặc tả trước cho các thợ đào trong việc thực thi mã nguồn và bảo mật, ngay cả khi việc thực thi bị thất bại vì một lý do nào đó.

**+** Thứ hai, nó đảm bảo việc thực thi không thể dài quá thời gian đã được ước lượng trước đó.

* Việc này khác so với Bitcoin, nơi àm chi phí được tính bằng kích thước của giao dịch (tính bằng kilobytes), ta có thể thấy việc tính chi phí dựa trên khối lượng tính toán hợp lý hơn nhiều.
* Hệ thông Gas cũng không khác lắm so với việc đo lượng điện dân dụng. Điểm khác biệt với thị trường năng lượng thực chính là người tạo giao dịch sẽ quyết định giá Gas (thợ mỏ có thể chấp nhận giá này hoặc không).
* Giá Gas cho mỗi giao dịch hay hợp đồng được thiết lập để xử lý bản chất Turing Complete của Ethereum và EVM của nó (tức là mã Ethereum Virtual Machine) – đây là một trong những ý tưởng được đưa ra để hạn chế vòng lặp vô hạn. Ví dụ như 10 szabo, tương đương với 0.00001 ether hay 1 Gas có thể thực hiện một dòng mã hay vài câu lệnh. Nếu không có đủ ether trong tài khoản để hiện thị một cuộc giao dịch hay một tin nhắn thì nó được coi là không hợp lệ. Ý tưởng này sẽ phần nào ngăn chặn được những cuộc tấn công từ vòng lặp vô hạn, khuyến khích tính hiệu quả trong chuỗi mã – và bắt những kẻ tấn công phải trả cho tài nguyên mà mình sủ dụng. Câu lệnh càng phức tạp thì chúng ta càng phải trả nhiều Gas hơn.



Hình 5: Danh sách hoạt động của Ethereum Virtual Code và giá Gas.

* 1. **Máy ảo Ethereum**

Máy ảo Ethereum (Ethereum Virtual Machine, viết tắt là EVM) là một máy chủ toàn cầu mà mọi người có thể sử dụng với một chi phí nhỏ, có thể trả bằng ether.

1. Mạng ngân hàng trung tâm

Chúng ta đang chi rất nhiều tiền cho việc xây dựng, vận hành và bảo trì các hệ thống thanh toán tập trung. Mỗi ngân hàng xây dựng riêng cho mình một hệ thống và việc thanh toán liên ngân hàng sẽ đòi hỏi thêm một khoản phí nữa, chưa kể đến các chi phí để đảm bảo an toàn, an ninh cũng như tính tin cậy cho cả hệ thống. Những chí phí ấy không hề rẻ dẫn đến việc chúng ta phải chi trả nhiều hơn cho các giao dịch của mình cũng như các giao dịch sẽ bị châm đi đáng kể khi phải liên kết nhiều dịch vụ.

1. Máy ảo

Trong ngữ cảnh của Ethereum, đó là một máy tính toàn cầu bao gồm rất nhiều nút cấu thành và chính các nút đó cũng là các máy tính. Nói chung, máy ảo là mô phỏng một hệ thống máy tính này bằng một hệ thống mát tính khác. Việc mô phỏng này trên EVM sử dụng cả phần cứng và phần mềm, mỗi nút tỏng mạng có thể chạy bất kì hệ điều hành nào.

1. Vai trò của EVM

EVM tạo ra môi trường để chạy các chương trình bất kì (được gọi là các hợp đồng thông minh) được viết bằng ngôn ngữ Solidity. Nhưng chương trình này các định đầy đủ và đảm bảo là được thực hiện nếu chúng ta trả đủ chi phí giao dịch.

Các chương trình viết bằng Solidity có khả năng thực hiện tất cả các nhiệm vụ có thể thực hiện bằng mát tính. Khi một hợp đồng được triển khai bằng việc tải lên từ một nút của mạng, các bản sao của hợp đồng sẽ được phát tán ra các nút khác.

* 1. **Tài khoản Ethereum**

Mỗi tài khoản Ethereum được đại diện bởi 20 ký tự. Các thông số sau được lưu trong dữ liệu trạng thái (state) của Ethereum cho mỗi tài khoản:

* Số Nonce: Để đảm bảo mỗi giao dịch chỉ được xử lý một lần.
* Số dư tài khoản.
* Mã nguồn hợp đồng (nếu có)
* Phần lưu trữ của tài khoản (mặc định là rỗng)

Các giao dịch giữa các tài khoản được trả tiền bằng ether. Có hai loại tài khoản: tài khoản ngoại vi được quản lý bởi khóa riêng tư, và tài khoản hợp đồng được quản lý bởi mã hợp đồng. Tài khoản ngoại vi không chứa mã hợp đồng, có thể gửi thông điệp đi bằng các tạo và ký kết một giao dịch, giống như tài khoản Bitcoin. Về phía tài khoản hợp đồng, mỗi khi nó nhận được 1 thông điệp, mã hợp đồng sẽ chạy và cho phép đọc và ghi vào phần lưu trữ của nó, kèm theo việc gửi thông điệp đi và tạo ra hợp đồng khác lần lượt.

* 1. **Thông điệp và giao dịch**

Thuật ngữ “giao dịch” được sử dụng để chỉ tới gói dữ liệu bào gồm thông điệp. Một giao dịch bao gồm:

* Tài khoản nhận thông điệp.
* Chữ ký tài khoản gửi.
* Số ether chuyển đi.
* Trường dữ liệu tùy chọn.
* Giá trị STARTGAS, đại diện cho số lượng tối đa các bước tính toán thực hiện giao dịch được phép thực hiện.
* Giá trị GASPRICE, đại diện cho khoản phí mà người gửi trả cho mỗi bước tính toán.

Nếu muốn tiết kiệm hơn cho một giao dịch, hãy giảm số tiền chúng ta trả thông qua Gas Price. Con số Gas Price này quyết định tốc độ giao dịch của chúng ta diễn ra nhanh hay chậm.

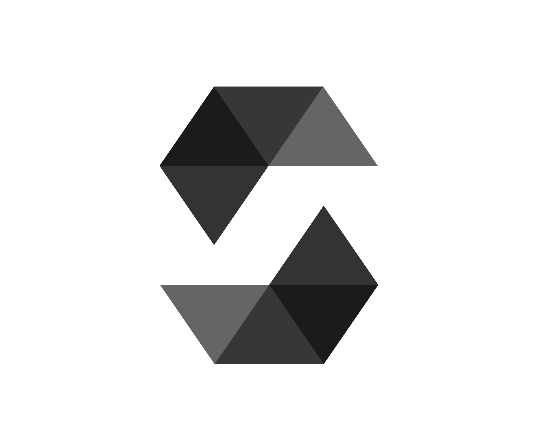
* 1. **Thông điệp**

Một hợp đồng có khả năng gửi “thông điệp” đến các hợp đồng khác. Thông điệp là các đối tượng ảo chỉ tồn tại trong môi trường thực thi Ethereum. Một thông điệp chứa:

* Tài khoản gửi tin nhắn (ẩn)
* Tài khoản nhận tin nhắn
* Số lượng ether để truyền tải cùng với thông điệp
* Trường dữ liệu tùy chọn
* Giá trị STARTGAS

Về cơ bản, một thông điệp giống như một giao dịch, ngoại trừ nó được tạo ra bởi hợp đồng chứ không phải là tài khoản ngoại vi. Một thông điệp được tạo ra khi hợp đồng hiện đang thực thi mà gọi đến mã lệnh CALL, lệnh tạo ra và thực hiện một thông điệp. Giống như giao dịch, một thông điệp được gửi tới tài khoản nhận. Do đó, các hợp đồng có thể có mối quan hệ với các hợp đồng khác giống như mối quan hệ của các bên tham gia bên ngoài.

* 1. **Tìm hiểu về Solidity**



Hình 6: Logo Solidity

* Solidity là một ngôn ngữ lập trình sử dụng để viết các chương trình hợp đồng thông minh, thứ mà sẽ được chạy trên EVM. Ngôn ngữ mới này là một sự pha trộn các quy ước từ mạng, hợp ngữ và phát triển web.
* Solidity là một ngôn ngữ hướng hợp đồng (Contract-oriented) bậc cao, có cú pháp tương tự ngôn ngữ C và JavaScrip. Nó cho phép phát triển hợp đồng và biên dịch sang mã EVM. Hiện nay nó là ngôn ngữ hàng đầu của Ethereum. Mặc dù nó là ngôn ngữ phổ biến nhất để viết cho Ethereum nhưng nó không phải là ngôn ngữ đầu tiên và có lẽ cũng không phải ngôn ngữ cuối cùng.
* Ngôn ngữ Solidity định kiểu mạnh, hỗ trợ thừa kế, thư viện và kiểu định nghĩa người dùng phức tạp cùng với các tính năng khác.
  1. **Ứng dụng phi tập trung**
* Ứng dụng phi tập trung (Decentralized App, viết tắt là DApp) là ứng dụng mã nguồn mở hoàn chỉnh, hoạt động độc lập, không có thực thể nào kiểm soát phần lớn các tokens của ứng dụng này. Dữ liệu và hồ sơ hoạt động của ứng dụng phải được lưu trữ dưới dạng mã hóa công khai, phân quyền chuỗi khối.
* Ứng dụng này tạo các mã thông báo thông qua thuật toán theo một tiêu chuẩn hoặc bộ tiêu chuẩn và có thể phân phối một số hoặc tất cả các tokens của nó khi bắt đầu hoạt động. Các tokens này cần thiết cho việc sử dụng ứng dụng và bất kỳ đóng góp nào từ người dùng sẽ được thưởng bằng các tài khoản thanh toán tỏng các tokens của ứng dụng. Ứng dụng có thể thích ứng các giao thức của nó để đáp ứng với những cải tiến đề xuất và phản hồi thị trường nhưng tất cả thay đổi phải được giải quyết bởi sử đồng thuận của người dùng. Dapp rất có giá trị và có khả năng sẽ phá vỡ một số ngành công nghiệp.
* Phân loại DApp:

**+** Các ứng dụng phân cấp có chuỗi khối riêng như Bitcoin.

**+** Giống loại 1 nhưng có thêm token và các giao thức cần thiết như giao thức ommi.

**+** Giống loại 2 nhưng có các mã thông báo cần thiết.

* Lợi ích của DApp:

**+** The Safe Network: có sự bảo mật lớn nhất.

**+** Factom: Đơn giản hóa quá trình quản lý dữ liệu lớn.

**+** BURST: Giải quyết các vấn đề làm lưu trữ đám mây đắt đỏ và không đáng tin cậy.

**+** Augur: Được biết đến như một thị trường sự đoán phân quyền để thưởng cho người sử dụng về các sự kiện dự báo.

**+** BlockAuth: Cung cấp một hệ thống đa chữ ký để chia sẻ dữ liệu cá nhân với các bên thứ ba.

* 1. **Sự đồng thuận về việc chấp nhận khối**

1. **Tổng quan về Smart Contract**
2. **Khái niệm**

* Hợp đồng thông minh(Smart Contract): là một thuật ngữ mô tả một bộ giao thức đặc biệt có khả năng tự động thực hiện các điều khoản.

Các thỏa thuận giữa các bên trong hợp đồng ở trường hợp này là các máy tính nhờ sự hỗ trợ của công nghệ BlockChain.

* Toàn bộ hoạt động của Smart Contract đều được thực hiện một cách tự động và không có sự can thiệp từ bên ngoài hay thông qua một bên thứ 3 trung gian.

Những giao dịch được thực hiện bằng hợp đồng thông minh rất minh bạch và có thể dễ dàng truy xuất được và không thể bị can thiệp hoặc đảo chiều.

* Các điều khoản trong Smart Contract tương đương với một hợp đồng có pháp lý và được ghi lại dưới ngôn ngữ của lập trình.
* Điểm nội bật nhất của SmartContract là cho phép 2 bên tham gia thực hiện hợp đồng một cách chính xác, an toàn và nhanh chóng mà không cần các bên biết về nhau từ trước và cũng không cần phải gặp trực tiếp để có thể làm việc với nhau hay một bên trung gian thứ 3 mà chỉ cần có kết nối Internet.

1. **Ý tưởng ra đời**

* Khái niệm SmartContract được biết đến lần đầu tiên bởi Nick Szabo vào năm 1993. Tại thời điểm đó, ông đã nêu ra những hoạt động chính nhưng ở thời điểm ấy chưa có đủ công nghệ và môi trường thích hợp để thực hiện hóa nó. Công nghệ BlockChain ra đời đã thay đổi mọi chuyện.
* Bitcoin đã đặt ra những nền tảng cơ bản cho việc thiết lập hợp đồng trên Blockchain. Tuy nhiên, nó vẫn chưa thể thỏa mãn mọi yêu cầu. Chỉ đến khi Ethereum xuất hiện thì ý tưởng smart contract mới được phổ biến đến cho mọi người dùng, cung cấp cho ta thêm một phương thức mới để thiết lập hợp đồng.

1. **Chức năng của Smart Contract**

* Tài sản được mã hoá
* Các điều khoản hợp đồng được mã hoá
* Điều kiện hợp đồng và tài sản được kết hợp thành một khối trong blockchain
* Khi cả hai bên thỏa thuận các điều khoản hợp đồng thành công, hợp đồng được thực hiện
* Bất kỳ chuyển giao tài sản nào được hoàn thành dựa trên các điều khoản của hợp đồng

1. **Cách hoạt động**

* Nguyên lí vận hành của smart contract có thể đem so sánh với một chiếc máy bán hàng tự động.
* Chúng chỉ tự động thực hiện những lệnh mà đã được lập trình sẵn từ trước. Đầu tiên, tài sản và điều khoản hợp đồng đều được mã hóa và chuyển vào một block thuộc Blockchain. Smart contract này tiếp đó sẽ được phân phối và sao chép lại bởi các node hoạt động trên nền tảng đó.
* Sau khi có nhận lệnh triển khai thì hợp đồng sẽ được triển khai theo đúng như điều khoản định sẵn. Đồng thời, smart contract cũng sẽ tự động kiểm tra quá trình thực hiện những cam kết nêu trong hợp đồng.

1. **Cách lập nên một Smart Contract**

* Chủ thể hợp đồng:

Chương trình phải được cấp khả năng truy cập đến sản phẩm/dịch vụ liệt kê trong hợp đồng để có thể tự động khóa hay mở khóa chúng.

* Chữ kí điện tử

Tất cả các bên tham gia đồng ý triển khai thỏa thuận bằng các khóa cá nhân của họ.

* Điều khoản hợp đồng

Điều khoản của smart contract có dạng một chuỗi các hoạt động. Các bên tham gia hợp đồng đều phải ký chấp nhận nó.

* Nền tảng phân quyền

Smart contract sau khi hoàn tất sẽ được tải lên Blockchain của nền tảng phân quyền tương ứng và được phân phối về cho các node của nền tảng ấy.

1. **Lợi ích của Smart-Contract**

* Tiết kiệm chi phí: Thay vì phải trả phí cho bên làm chứng thì chúng ta chỉ cần trả một khoản phí nhỏ cho mạng lưới BlockChain.
* Linh hoạt: Hệ thống máy tính tự động sắp xếp và thực thi chính xác những quy điinh trong hợp đồng thông minh. Từng trường hợp có thể được xử lý linh hoạt và hiểu quả cho người sử dụng.
* Minh bạch, rõ ràng: Mọi giao dujch đều được ghi nhận trên BlockChain, có thể truy dấu ra nguồn gốc và không thể đảo nghịch giao dịch.
* Độ tin tưởng cao: Với SmartContract và BlockChain mã hóa, không bên nào có thể can thiệp vào quá trình thực thi cũng như thỏa thuận của hợp đồng một khi đã được hoàn tất.
* Nhanh, gọn và tiện lợi: Với sự trợ giúp của BlockChain, một hợp đồng thông minh có thể thiết lập và thực thi chỉ trong vài giây. Hợp đồng cũng có thể cùng lúc thiết lập với nhiều người khác nhau và dùng đi dùng lại nhiều lần, rất tiện lợi.

1. **Hạn chế của Smart-Contract**

Sau đây là một số các khiếm khuyết còn tồn đọng của smart contract:

* Nhân tố con người

Vì toàn bộ phần mã được soạn thảo bởi con người, và họ vẫn có thể mắc lỗi. Nếu smart contract đã được tải lên Blockchain, các nhà lập trình sẽ không thể nào thay đổi được nó.

Một ví dụ nổi tiếng về nhân tố con người đó chính là sự kiện DAO. Lỗi lập trình của đội ngũ phát triển đã bị một số tin tặc phát hiện và tận dụng, từ đó cướp đoạt đến 60 triệu USD tiền vốn của người dùng

* Tình trạng pháp lý chưa rõ ràng

Hiện tại, smart contract vẫn chưa được quản lí bởi bất kì chính phủ nào cả. Vì thế cho nên vẫn tiềm ẩn khả năng xuất hiện mâu thuẫn nếu như các thể chế quản lí quyết định xây dựng bộ khung pháp lý dành cho hình thức smart contract còn khá mới mẻ này.

* Chi phí thực hiện

Smart contract không thể nào được lập nên mà không cần thông qua công đoạn lập trình. Do đó, điều cần thiết là phải có một chuyên gia lập trình dày dặn kinh nghiệm trong đội ngũ phát triển để hạn chế tối đa những sai sót có thể xảy ra đối với hợp đồng và bảo đảm cơ sở hạ tầng của công ty tương thích được với công nghệ Blockchain.