BÁO CÁO CÁC VẤN ĐỀ HIỆN ĐẠI

ĐỀ TÀI: TÌM HIỂU VỀ ETHEREUM

Nhóm 8

Thành Viên:
Nguyễn Mạnh Cường
Phạm Minh Đức
Vũ Nam Tước
Bùi Thị Chung Thủy

Mục lục

1 Lịch sử sửa đổi

Bảng ?? là bảng phân công công việc cho các thành viên trong nhóm.

Ngày	**Thành viên**	**Nội dung công việc**

Bảng 1: Bảng lịch sử sửa đổi

2 Giới thiệu

2.1 Giới thiệu chung về Bl ockChain

BlockChain có thể coi như một quyển sổ ghi chép tài chính được phân phối ngang hàng như Torrent. Không có nhà nước hay công ty nào cai quản, BlockChain được mã hóa một cách rất cầu kỳ để ngăn chặn tuyệt đối việc giả mạo thông tin.

Ba thành phần công nghệ của BlockChain

- Mạng ngang hàng: Một nhóm các máy tính ví dụ như mạng BitTorrent 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: Một cách cho phép những máy tính này gửi các tin nhắn được mã hóa cho những người nhận đã được xác định
- Phép băm mật mã: Một các để sinh một "fingerprint" 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.

2.2 Tổng quan Ethereum

Ethereum (ETH) hay còn được gọi là Bitcoin 2.0

Là một nền tảng điện toán phân tán khối chuỗi, chạy trên blockchain, thông qua việc sử dụng chức năng Hợp đồng thông minh (Smart Contract)

Tiền ảo Ethereum có thể thực hiện các giao dịch, hợp đồng mạng ngang hàng thông qua đơn vị tiền ảo là Ether

2.2.1 Lịch sử ra đời

Ethereum được đề xuất vào cuối năm 2013 bởi Vitalik Buterin người Nga sinh năm 1994, một cậu thanh niên chuyên nghiên cứu về lập trình tiền ảo

Vốn hoá của Ethereum đạt 25 triệu USD trong đợt mở bán lần đầu năm 2014. Kể từ đó Ethereum bắt đầu phát triển Blockchain cho riêng cũng như phát triển ngôn ngữ lập trình của mình

Phiên bản beta được phát hành vào tháng 7/2015

Kể từ đầu năm trở lại đây, giá Ethereum tăng hơn 2000

2.2.2 Các thành phần cơ bản của Ethereum

Gas

- Gas là chi phí nội bộ để thực hiện một giao dịch hoặc hợp đồng trong Ethereum.

- Giá trị của Gas được trả bằng một lượng ether.
- 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 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 hiển thị một cuộc giao dịch hay một tin nhắn thì nó được coi là không hợp lệ.

Hợp đồng thông minh

- Hợp đồng thông minh là một cơ chế trao đổi xác định, được kiểm soát bởi các phương tiện kỹ thuật số mà có thể giúp cho việc thực hiện giao dịch trực tiếp giữa các thực thể mà không cần tin cậy nhau
- Các hợp đồng này được định nghĩa bằng cách lập trình và được chạy chính xác như mong muốn mà không bị kiểm duyệt, lừa đảo hay sự can thiệp từ bên thứ ba trung gian.
- Trong Ethereum, các hợp đồng thông minh được coi là các kịch bản tự trị hoặc các ứng dụng phân cấp được lưu trữ trong chuỗi khối Ethereum để thực hiện sau đó bởi EVM.

Máy ảo Ethereum (EVM)

- Viết tắt của cụm từ Ethereum Virtual Machine.
- Là một môi trường chạy các hợp đồng thông minh Ethereum.
- Nó được hoàn toàn cô lập từ mạng, hệ thống tập tin và các quá trình khác của hệ thống máy chủ.
- Mỗi nút Ethereum trong mạng chạy một EVM và thực hiện các hướng dẫn giống nhau.
- Ethereum Virtual Machines đã được lập trình trong C++, Go, Haskell, Java, Python, Ruby, Rust và WebAssembly.

2.3 Một vài ứng của Ethereum

Hiện tại

- Hệ thống thanh toán
- Đầu tư vàng
- Gây quỹ cộng đồng
- Quản lý tài chính doanh nghiệp

Tương lai

- Internet of Things
- Web hosting
- Thị trường tài chính, bầu cử, bất động sản,...

3 Chi tiết trong Ethereum

3.1 Tổng quan

Có nhiều mục đích của dự án này; một mục tiêu chính là tạo thuận lợi cho các giao dịch giữa các cá nhân đồng ý, những người khác sẽ không có phương tiện để tin tưởng lẫn nhau. Điều này có thể do khoảng cách địa lý, gặp khó khăn, hoặc có thể là sự không tương thích, không đủ năng lực, không sẵn lòng, chi phí, sự không chắc chắn, sự bất tiện hoặc tham nhũng của các hệ thống pháp luật hiện hành. Bằng cách xác định một hệ thống thay đổi nhà nước thông qua một ngôn ngữ phong phú và rõ ràng, và hơn nữa kiến trúc một hệ thống như vậy mà chúng ta có thể hy vọng một cách hợp lý rằng một thỏa thuận sẽ được thi hành tự trị, chúng ta có thể cung cấp một phương tiện để kết thúc này.

Giao dịch trong hệ thống đề xuất này sẽ có một số thuộc tính không thường thấy trong thế giới thực. Tính không mệt mỏi của phán đoán, thường khó tìm, xuất phát tự nhiên từ một thông dịch thuật toán không quan tâm. Sự minh bạch, hoặc có thể nhìn thấy chính xác cách thức một quốc gia hoặc phán quyết thông qua đăng nhập và các quy tắc hoặc mã hướng dẫn, không bao giờ xảy ra hoàn hảo trong các hệ thống con người vì ngôn ngữ tự nhiên là nhất thiết mơ hồ, thông tin thường thiếu và những thành kiến xưa cũ rất khó lắc.

Nói chung, chúng tôi muốn cung cấp một hệ thống sao cho người dùng có thể được đảm bảo rằng bất kể cá nhân, hệ thống hay tổ chức nào họ tương tác với nhau, họ có thể làm như vậy với sự tự tin tuyệt đối vào những kết quả có thể xảy ra và những kết quả đó có thể xảy ra như thế nào.

Giá trị: Để khuyến khích tính toán trong mạng, cần phải có một phương pháp đồng bộ để truyền giá trị. Để giải quyết vấn đề này, Ethereum có một đồng tiền nội tại, Ether, được biết đến như là ETH và đôi khi được đề cập bởi Old English Đ. Sự phân chia nhỏ nhất của Ether, và do đó là một trong đó tính tất cả các giá trị số nguyên của tiền tệ, là Wei. Một Ether được định nghĩa là 10^18 Wei. Có tồn tại các mức của đồng tiền khác của Ether:

$$10^{12} Wie = Szabo \tag{1}$$

$$10^{15} Wie = Finney \tag{2}$$

$$10^{18} Wie = Ether \tag{3}$$

3.2 Mô hình BlockChain

Ethereum được xem như một máy trạng thái dựa trên các giao dịch. Chúng ta bắt đầu với trạng thái khởi tạo và thực hiện các giao dịch để dần biến đổi nó tới trạng thái kết thúc. Mỗi trạng thái có thể bao gồm một số thông tin như số dư tài khoản, tên tài khoản, dữ liệu liên quan đến thông tin về thế giới vật lý hay bất cứ điều gì mà có thể đại diện bởi một máy tính chấp nhận được. Vì vậy, các giao dịch phải đại diện cho đường vòng cung nối giữa hai trạng thái hợp lệ. Sự hợp lệ là vô cùng quan trọng. Quá trình chuyển đổi trạng thái hợp lệ là một quá trình chuyển đổi

thông qua giao dịch. Như sau:

$$\sigma_{t+1} \equiv \Upsilon(\sigma_t, T) \tag{4}$$

Trong đó Υ là hàm chuyển đổi trạng thái trong Ethereum. Trong Ethereum,Υ cùng với σ mạnh hơn đáng kể so với bất kỳ hệ thống nào đang có. Υ cho phép các thành phần có thể tính toán tùy ý, trong khi đó σ cho phép các thành phần lưu các trạng thái tùy ý giữa các giao dịch.

Các giao dịch được sắp xếp thành các khối; các khối được nối liền với nhau bằng cách sử dụng một băm mật mã như một ý nghĩa tham khảo. Các khối hoạt động như một nhật ký, ghi lại một loạt các giao dịch cùng với khối trước đó và một định danh cho trạng thái cuối cùng (mặc dù không lưu trữ trạng thái cuối cùng chính nó | sẽ quá lớn). Họ cũng chấm dứt chuỗi giao dịch với ưu đãi cho người đào. Sự khuyến khích này diễn ra như là một chức năng chuyển đổi trạng thái, bổ sung giá trị cho một tài khoản được chỉ định.

Nó được giải thích như sau:

$$\sigma_{t+1} \equiv \Pi(\sigma_t, B) \tag{5}$$

$$B \equiv (..., (T_0, T_1, ...)) \tag{6}$$

$$\Pi(\sigma, B) \equiv \Omega(B, \Upsilon(\Upsilon(\sigma, T_0), T_1)...) \tag{7}$$

Trong đó Ω là chức năng chuyển trạng thái hoàn thiện khối(chức năng thưởng cho bên chỉ định); B là khối này, bao gồm một loạt các giao dịch giữa một số thành phần khác; và Π là cấp của khối trong hàm chuyển trạng thái

Đây là cơ sở của mô hình BlockChain, một mô hình tạo thành xương sống không chỉ của Ethereum, mà còn cho đến nay tất cả các hệ thống giao dịch dựa trên sự đồng thuận.

3.3 Những qui tắc

chúng tôi sử dụng một số công ước đánh máy cho các ký hiệu chính thức, một số trong đó là khá cụ thể cho công việc hiện tại:

Hai bộ các giá trị được cấu trúc cao, 'cấp trên cùng', trạng thái, được đánh dấu bằng chữ cái Hy Lạp in đậm. Chúng rơi vào các trạng thái của thế giới, được biểu thị bằng σ (hoặc một biến thể ở đó) và các trạng thái của máy, μ.

Các hàm hoạt động dựa trên các giá trị có cấu trúc cao được biểu thị bằng chữ hoa tiếng Hy Lạp, ví dụ: Υ, Ethereum chức năng chuyển trạng thái.

Đối với hầu hết các chức năng, một chữ cái viết hoa được sử dụng, ví dụ C: hàm về chi phí chung. Đây có thể được ký hiệu để biểu thị các biến thể chuyên biệt, ví dụ: CSSTORE, chức năng chi phí cho hoạt động SSTORE. Đối với các chức năng chuyên biệt và có thể được xác định bên ngoài, tôi có thể định dạng dưới dạng văn bản đánh máy, ví dụ: chức năng băm Keccak-256 (theo mục nhập chiến thắng của cuộc thi SHA-3) được biểu thị là KEC (và thường được gọi là Keccak đơn giản). Ngoài ra KEC512 là đề cập đến chức năng băm Keccak 512.

Giá trị vô hướng và các chuỗi byte có kích thước cố định (hoặc, synony-mously, mảng) được biểu thị bằng một trường hợp thường thấp hơn, ví dụ: n được sử dụng trong tài liệu để biểu thị nonce giao dịch. Những người có một ý nghĩa đặc biệt đặc biệt có thể là tiếng Hy Lạp, ví dụ: δ, số lượng các mục cần thiết trên ngăn xếp cho một hoạt động nhất định.

Trong toàn bộ, chúng ta giả sử các đại lượng vô hướng là các số nguyên dương và do đó thuộc về tập hợp P. Tập các dãy tất cả các byte là B, được định nghĩa chính thức trong Phụ lục B. Nếu như một chuỗi các trình tự được giới hạn ở những đoạn có độ dài đặc biệt, một subscript, do đó tập của tất cả các chuỗi byte có độ dài 32 được đặt tên B_{32} và tập hợp của tất cả các số nguyên dương nhỏ hơn 2^{256} được đặt tên P_{256}. Điều này được định nghĩa chính thức trong phần tiếp theo

Dấu ngoặc vuông được sử dụng để lập chỉ mục và tham chiếu các thành phần riêng lẻ hoặc các chuỗi con của các trình tự, ví dụ: $\mu_s[0]$ biểu thị mục đầu tiên trên ngăn xếp của máy. Đối với chuỗi con, các điểm elip được sử dụng để xác định phạm vi dự định, bao gồm các phần tử ở cả hai giới hạn, ví dụ: μ_m [0 :: 31] biểu thị 32 đầu tiên của bộ nhớ máy

Khi xem xét việc sử dụng các hàm hiện có, cho một hàm f, hàm f * biểu thị một phiên bản tương đương, phần tử của việc lập bản đồ chức năng thay vì giữa các trình tự. Nó được định nghĩa chính thức trong phần tiếp theo

3.4 Khối, Trạng thái và các giao dịch

Sau khi giới thiệu các khái niệm cơ bản đằng sau Ethereum, chúng tôi sẽ thảo luận chi tiết hơn về ý nghĩa của giao dịch, khối và trạng thái

3.4.1 Thê Giới Trạng Thái (World State)

Trạng thái thế giới (state), là một ánh xạ giữa các địa chỉ (các định danh 160-bit) và các trạng thái tài khoản (một cấu trúc dữ liệu được sắp xếp theo RLP, xem Phụ lục B). Mặc dù không được lưu trữ trên blockchain, giả định rằng việc thực hiện sẽ duy trì bản đồ này trong một cây Merkle Patricia được sửa đổi (trie, xem Phụ lục D). Trie yêu cầu một backend cơ sở dữ liệu đơn giản duy trì một bản đồ của bytearrays để bytearrays; chúng ta đặt tên cơ sở dữ liệu cơ bản là cơ sở dữ liệu trạng thái. Điều này có một số lợi ích; đầu tiên nút gốc của cấu trúc này tùy thuộc mật mã vào tất cả các dữ liệu bên trong và do đó băm của nó có thể được sử dụng như một bản sắc an toàn cho toàn bộ trạng thái hệ thống.

Thứ hai, là một cấu trúc dữ liệu không thay đổi, nó cho phép bất kỳ trạng thái trước đó được gọi lại bằng cách đơn giản thay đổi gốc rễ tương ứng. Vì chúng ta lưu trữ tất cả các rễ gốc như vậy trong BlockChain, chúng ta có thể trở lại trạng thái cũ. Trạng thái tài khoản bao gồm bốn lĩnh vực sau:

nonce :Giá trị vô hướng bằng số lượng các giao dịch được gửi từ địa chỉ này hoặc, trong trường hợp tài khoản có mã liên quan, số lượng hợp đồng tạo ra bởi tài khoản này. Đối với địa chỉ một trong tiểu bang σ, điều này sẽ được biểu hiện chính thức $\sigma[a]_n$.

balance:A scalar value equal to the number of Wei owned by this address. Formally denoted $\sigma[a]_n$.

storageRoot:Một băm 256 bit của nút gốc của cây Merkle Patricia mã hóa nội dung lưu trữ của tài khoản (một bản đồ giữa các giá trị số nguyên 256-bit), được mã hoá thành trie như một bản đồ từ 256-bit băm Keccak của 256 -bit các phím số nguyên đến các giá trị số nguyên 256-bit mã hóa RLP. Băm được biểu thức chính thức là $\sigma[a]_s$.

codeHash: là mã băm của máy ảo EVM của tài khoản đó-đây là đoạn mã được thực hiện khi địa chỉ này nhận được một cuộc gọi tin nhắn; nó là không thay đổi và do đó, không giống như

tất cả các lĩnh vực khác, không thể thay đổi sau khi xây dựng. Tất cả các đoạn mã như vậy được chứa trong cơ sở dữ liệu trạng thái dưới các giá trị tương ứng của nó để truy xuất sau đó. Băm này được biểu hiện chính thức là $\sigma[a]_c$, và do đó mã có thể được ký hiệu là b, và KEC (b) = $\sigma[a]$.

3.4.2 Địa chỉ(Homestead)

là một số khối quan trọng mang tính công khai đánh dấu giữa sự chuyển tiếp giữa hai trạng thái, chúng ta biểu thị nó bằng N_h, được định nghĩa như sau:

$$N_h \equiv 1150000 \tag{8}$$

Giao thức này đã được nâng cấp tại mỗi block, do đó biểu tượng này xuất hiện trong một số phương trình để giải thích cho sự thay đổi.

3.4.3 Giao Dịch(Transaction)

Giao dịch (giao dịch chính thức, T) là một chỉ lệnh được mã hoá bằng ký tự được xây dựng bởi một diễn viên bên ngoài phạm vi của Ethereum. Mặc dù giả định rằng các diễn viên bên ngoài cuối cùng sẽ là con người trong tự nhiên, các công cụ phần mềm sẽ được sử dụng trong xây dựng và phổ biến1. Có hai loại giao dịch: những kết quả trong các cuộc gọi thư và những kết quả tạo ra các tài khoản mới có mã liên quan (được gọi là "hợp đồng tạo ra"). Cả hai loại chỉ định một số trường phổ biến:

nonce: là một giá trị vô hướng bằng số lượng các giao dịch của người gửi. Giá trị đó được gọi là T_n.

gasPrice:một giá trị vô hướng bằng số lượng Wei được thanh toán cho mỗi đơn vị khí cho tất cả chi phí tính toán phát sinh do kết quả của việc thực hiện giao dịch này; chính thức là T_n.

gasLimit: Giá trị vô hướng bằng lượng khí tối đa cần được sử dụng trong quá trình thực hiện giao dịch này. Điều này được thanh toán trước, trước khi bất kỳ tính toán được thực hiện và không thể được tăng lên sau đó; được biểu thị bằng T_g.

To: Địa chỉ 160-bit của người nhận cuộc gọi tin nhắn hoặc, đối với giao dịch tạo hợp đồng. ký hiệu: T_t.

Giá Trị(Value): Một giá trị vô hướng bằng số lượng Wei được chuyển đến người nhận cuộc gọi của tin nhắn hoặc, trong trường hợp tạo hợp đồng, như một khoản tài trợ cho tài khoản mới được tạo; ký hiệu: T_v.

v,r,s: Giá trị tương ứng với chữ ký của giao dịch và được sử dụng để xác định người gửi giao dịch; chính thức là T_w, T_r và T_s.

3.4.4 Khối(block)

Khối trong Ethereum là bộ sưu tập các mẩu thông tin có liên quan (gọi là tiêu đề khối), H, cùng với thông tin tương ứng với các giao dịch bao gồm, T và một tập hợp các phần đầu khối U khác được biết là có một cha mẹ bằng cha mẹ của cha mẹ của khối hiện tại (các khối như vậy được gọi là ommers[2]). Tiêu đề của khối chứa nhiều mẩu thông tin:

parentHash: Kiểu băm 256-bit Keccak của tiêu đề của khối cha, trong toàn bộ; ký hiệu là H_p.

ommerHash: : băm Keccak 256-bit của phần danh sách ommers của khối này; ký hiệu: H_o.

beneficiary: Địa chỉ 160-bit mà tất cả các khoản phí thu được từ việc khai thác thành công khối này sẽ được chuyển giao; ký hiệu H_c.

stateRoot: Băm 256 bit Keccak của nút gốc trong cấu trúc cây trie được điền vào trong mỗi giao dịch; ký hiệu H_r.

transactionsRoot: Băm 256 bit Keccak của nút gốc của cấu trúc trie được điền với mỗi giao dịch trong phần danh sách giao dịch của khối; ký hiệu H_t.

receiptsRoot: băm Keccak 256-bit của nút gốc của cấu trúc trie với các biên nhận của mỗi giao dịch trong phần danh sách giao dịch của khối; ký hiệu: H_e.

logsBloom: Bộ lọc Bloom bao gồm thông tin có thể lập chỉ mục (địa chỉ logger và chủ đề đăng nhập) chứa trong mỗi mục nhập nhật ký từ mỗi lần nhận được trong danh sách giao dịch; ký hiệu H_b.

difficulty: một giá trị vô hướng tương ứng với mức độ khó khăn của khối này. Điều này có thể được tính từ mức độ khó khăn của khối trước đó và dấu thời gian;ký hiệu H_d.

number: Một giá trị vô hướng bằng số khối tổ tiên. Khối nguồn có một số không; ký hiệu H_i.

gasLimit : một giá trị vô hướng bằng mức giới hạn hiện tại của chi phí khí trên mỗi block; chính thức Hl. gasUsed: một giá trị vô hướng bằng tổng lượng khí được sử dụng trong các giao dịch trong khối này; ký hiệu H_g.

gasUsed: một giá trị vô hướng bằng tổng lượng khí được sử dụng trong các giao dịch trong khối này; ký hiệu H_g

timestamp: Một giá trị vô hướng bằng sản lượng hợp lý của thời gian Unix () tại thời điểm khởi đầu của khối này; ký hiệu H_s

extraData: Một mảng byte tùy ý chứa dữ liệu liên quan đến khối này. Đây phải là 32 byte trở xuống; ký hiệu H_x

mixHash: Một băm 256 bit chứng minh rằng kết hợp với nonce rằng một số lượng đầy đủ các tính toán đã được thực hiện trên khối này; ký hiệu H_m

nonce: Một băm 64 bit chứng minh kết hợp với hỗn hợp-băm rằng một số lượng đầy đủ các tính toán đã được thực hiện trên khối này; ký hiệu H_n.

3.5 Gas và sự thanh toán

3.6 Thực hiện giao dịch

4 Cài đặt

5 Voting app

6 Tài Liệu Tham Khảo