BÁO CÁO TRIỂN KHAI ỨNG DỤNG SMART CONTRACT MULTI-SIG WALLET TRÊN ETHEREUM

THÀNH VIÊN :

PHAN BÁ VĂN: 20154317

PHẠM VĂN DUY: 20150632

Mục Lục

[1. Giới thiệu về Blockchain. 2](#_Toc28766503)

[2. Ethereum và Smart contract trên Ethereum. 4](#_Toc28766504)

[2.1 Ethereum và các khái niệm cơ bản. 4](#_Toc28766505)

[2.2 Hợp đồng thông minh (Smart contract). 7](#_Toc28766506)

[A. Khái niệm: 7](#_Toc28766507)

[B. Cách thức hợp đồng thông minh hoạt động. 8](#_Toc28766508)

[C. Sự khác nhau hợp đồng thông minh và hợp đồng truyền thống. 8](#_Toc28766509)

[3. Triển khai Multi-Sig Wallet trên Ethereum. 9](#_Toc28766510)

[3.1 Khái niệm và chức năng Multi-Sig Wallet. 9](#_Toc28766511)

[3.2 Triển khai project Multi-Sig Wallet. 9](#_Toc28766512)

[3.2.1 Các công cụ áp dụng. 9](#_Toc28766513)

[3.2.2 Xây dựng Multi-Sig Wallet Smart Contract. 10](#_Toc28766514)

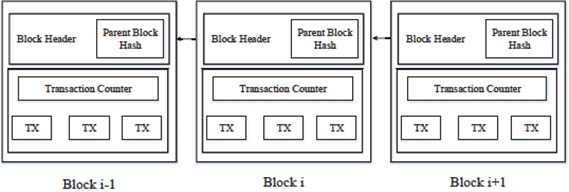
[Tài Liệu Tham Khảo 20](#_Toc28766515)

# 1. Giới thiệu về Blockchain.

Blockchain là một cơ sở dữ liệu phân cấp cho phép lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa. Các khối thông tin này hoạt động độc lập và có thể mở rộng theo thời gian. Chúng được quản lý bởi những thành phần tham gia hệ thống chứ không thông qua bên trung gian. Nghĩa là một khối thông tin khi đã được chấp nhận ghi vào hệ thống thì không có cách nào có thể thay đổi được, và chỉ có thể bổ sung thêm khi đạt được sự đồng thuận của tất cả các thành phần trong hệ thống.

Mỗi khối thông tin chứa đều chứa thông tin về thời gian khởi tạo, và được liên kết với khối trước đó, kèm theo thông tin về dữ liệu giao dịch. Ưu điểm, nhược điểm của blockchain.

Cấu trúc Blockchain gồm các block ghép nối với nhau tạo thành chuỗi khối(blockchain). Hình dưới là biểu diễn về cấu trúc dữ liệu của Blockchain:



* Ưu điểm:
* Đảm bảo tính bảo mật cao, được thiết kế để chống lại việc thay đổi của dữ liệu. Một khi dữ liệu đã được cập nhật trong mạng thì sẽ rất khó có thể thay đổi được nó. Ngay cả khi một phần của hệ thống blockchain sụp đổ, những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin.
* Nhược điểm:
* Tấn công 51%, một cuộc tấn công xảy ra nếu có một đơn vị kiểm soát hơn 50 % sức mạnh băm của mạng lưới. Điều này sẽ cho phép đơn vị đó phá vỡ mạng lưới bằng cách cố ý ngăn chặn hoặc sửa đổi việc đặt các giao dịch.
* Việc sửa đổi dữ liệu cực kỳ khó khăn: một khi dữ liệu được đưa vào Blockchain thì rất khó có thể thay đổi. Đó vừa là ưu điểm vừa là nhược điểm của Blockchain.
* Sự bất tiện của private key: mỗi tài khoản Blockchain sẽ được cấp khóa chung(chia sẻ) và khóa riêng(cần giữ bí mật). Cá nhân dùng khóa riêng truy cập vào tài khoản của mình, nếu quên khóa riêng này thì tài khoản họ sẽ bị mất mà không làm được gì.
* Không hiệu quả: Các blockchain, đặc biệt là các loại đang sử dụng thuật toán đồng thuận Proof of Work, là rất kém hiệu quả. Vì khi thực hiện đào có tính cạnh tranh cao và cứ sau mười phút lại có một người chiến thắng nên công sức các thợ mỏ khác sẽ bị lãng phí.

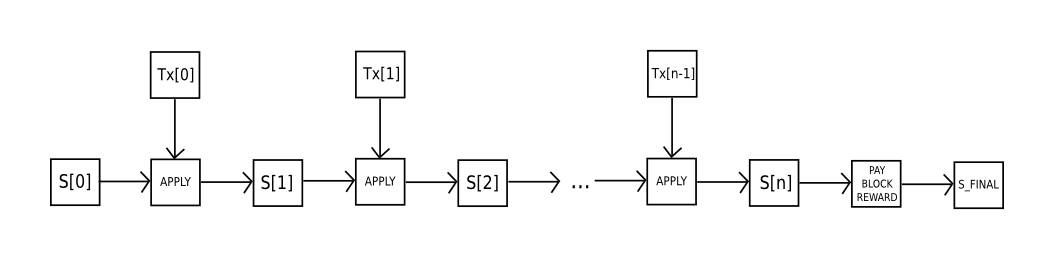
# 2. Ethereum và Smart contract trên Ethereum.

## 2.1 Ethereum và các khái niệm cơ bản.

Ethereum là nền tảng điện toán phân tán chuỗi khối chạy trên công nghệ blockchain, thông qua việc sử dụng chức năng Hợp đồng thông minh (Smart Contract), tạo thuận lợi cho các thỏa thuận hơp đồng trực tuyến.

Các khái niệm cơ bản:

* “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 xác nhận các giao dịch trong mạng. Quá trình này gọi là đào mỏ, do quá trình này tiêu thụ điện năng đó là phí tiền bạc, và vì vậy thợ mỏ được trả một phần thưởng cho mỗi khối họ khai thác( trả bằng ether).
* Ether: Tiền mã hóa được giao dịch trong mạng lưới Ethereum được gọi là ether. Được sử dụng để trả phí giao dịch và dịch vụ tính toán trên mạng Ethereum.
* Gas: Gas là một đơn vị được sử dụng để đo lường mức chi phí tính toán (computationally 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, mà bạn không thể sở hữu hay tích trữ nó. Nó đơn giản đo đạc mức tiêu hao của các phép tính toán mà hệ thống phải chịu nếu thực hiện giao dịch. Để có thể trả chi phí gas, bạn chỉ cần them ether vào tài khoản của bạn.
* Máy ảo Ethereum: Là máy chủ toàn cầu mà mọi người có thể sử dụng một chi phí nhỏ, có thể trả bằng ether.
* Máy ảo: Trong ngữ cảnh 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 máy tính khác. Việc mô phỏng này trên EVM sử dụng cả phần cứng và phần mềm, mỗi nút trong mạng có thể chạy bất cứ hệ điều hành nào.
* Vai trò của EVM: EVM tạo ra môi trường để chạy các chương trình bất kỳ (được gọi là các hợp đồng thông minh) được viết bằng ngôn ngữ Solidity. Các chương trình viết bằng Solidity có khả năng thực hiện tất cả các nhiệm vụ có thể thực hiện được bằng máy tính. Khi một hợp đồng được triển khai bằng việc tải từ một nút trong mạng, các bản sao của hợp đồng sẽ được phát tán ra các nút khác. Khi có yêu cầu chạy hợp đồng, các nút mạng sẽ chạy một cách độc lập với cùng một mã của hợp đồng.
* Tài khoản Ethereum: Mỗi tài khoản Ethereum được đại diện bởi 20 ký tự. Các thông số được lưu trong dữ liệu trạng thái của Ethereum cho mỗi trạng thái: Số nonce (để đảm bảo rằng mỗi giao dịch chỉ được xử lý một lần), số dự tài khoản, Mã nguồn hợp đồng, Phần lưu trữ của tài khoản.
* 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, Tài khoản nhận tin nhắn, Số lượng ether để truyền tải cùng thông điệp, 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).
* Giao dịch: Là gói dữ liệu mà bao 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, Giá trị GasPrice (đại diện cho khoản phí mà người gửi trả cho mỗi bước tính toán).
* Chuỗi khối và đào mỏ:



*Hình minh họa thuật toán xác nhận khối cơ bản trong Ethereum*

Chuỗi khối trong Ethereum có nhiều điểm tương tự với Bitcoin, tuy nhiên có một số khác biệt như sau: Khối Ethereum chứa một bản sao của cả danh sách giao dịch và trạng thái gần nhất. Bên cạnh đó, số khối và độ khó cũng được lưu trữ trong khối. Thuật toán xác nhận khối cơ bản trong Ethereum như sau:

* Kiểm tra tham chiếu khối trước đó tồn tại và hợp lệ không.
* Kiểm tra dấu thời gian (timestamp) của khối lớn hơn dấu thời gian của khối được tham chiếu đó và nhỏ hơn 15 phút trong tương lai.
* Kiểm tra số khối, độ khó, gốc giao dịch, gốc cha chú và giới hạn gas là hợp lệ không. Kiểm tra xem chứng minh công việc (proof of work) trên khối là hợp lệ không.
* Đặt s[0] là trạng thái cuối của khối trước đó.
* Đặt TX là danh sách giao dịch khối, với n là giao dịch. Đối với tất cả i từ 0…n-1, đặt S[i+1] = APPLY(S[i], TX[i]). Nếu bất kỳ ứng dụng nào trả về lỗi hoặc nếu tổng lượng gas tiêu thụ trong khối cho đến thời điểm này vượt quá GASLIMIT thì trả lại lỗi. (APPLY là một hàm thay đổi trạng thái S khi có giao dịch).
* Đặt S\_FINAL là S[n], nhưng có thêm phần thưởng cho thợ mỏ.
* Kiểm tra gốc cây Merkle của trạng thái S\_FINAL có bằng với gốc trạng thái cuối cùng được cung cấp trong tiêu đề khối không. Nếu có, khối này là hợp lệ, nếu không nó không hợp lệ.
* Solidity: Là ngôn ngữ lập trình sử dụng để viết các chương trình thông minh, thứ mà sẽ được chạy trên EVM.
* Ứng dụng phi tập trung (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 các 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 nói khi bắt đầu hoạt động. Các tokens này cần thiết cho việc sử dụng các ứng dụng và bất kỳ đóng góp nào từ người dung sẽ được thưởng bằng các khoản thanh toán trong các tokens của ứng dụng. Ứng dụng có thể thích ứng các giao thức của nó để đáp ứng với các cải tiến đề xuất và phản hồi thị trường nhưng tất cả thay đổi phải được quyết định bởi sự đồng thuận của người sử dụng. DApp có giá trị và có khả năng sẽ phá vỡ một số ngành công nghiệp.
* Sự đồng thuận về việc chấp nhận khối: Trên một mạng ngang hàng, mọi dữ liệu ở các nút cục bộ đều có thể bị thay đổi tùy ý bởi người sở hữu nút đó và khi thực hiện nhân bản sẽ có các xung đột và ta khó có thể xác định đâu mới là chuỗi khối đúng. Vì vậy, để đảm bảo sự tin cậy của mạng cũng như chuỗi khối, ta phải có cơ chế để làm sao tất cả các nút mạng đều đồng thuận khối thêm vào chuỗi đó là khối hợp lệ và sẽ phát hiện ra các hành vi phá hoại mạng bằng cách đưa ra các khối giả.

Nói về cơ chế đồng thuận thì hiện nay cơ hai cơ chế phổ biến là chứng nhận công việc (Proof of Work) và chứng nhận cổ phần (Proof of Stake). Ngoài ra còn mô hình chứng nhận thẩm quyền (Proof of Authority).

* POW: POW là một trong các cách để xác định sự đồng thuận của cộng đồng. Ở mô hình hay giải thuật này, để thêm mới một khối và blockchain đồi hỏi phải thực hiện các hàm tính toán rất phức tạp để tạo nên một giá trị băm hợp lệ (khó để tạo ra nhưng rất dễ dàng để xác định nó hợp lệ). Việc giải mã này ngoài việc cần những cấu hình mạnh còn tiêu tốn rất rất nhiều điện năng và gây nguy hại đến môi trường. Cộng đồng sẽ công nhận khối anh tạo ra dựa vào lượng công việc anh đã thực hiện được.

Một yếu tố đặc trưng của mô hình này đó là sự xuất hiện của các khối dư thừa (orphan block) do có nhiều người tham gia cùng tạo nên một khối nên sẽ có trường hợp hai người tạo ra hai khối đều hợp lệ nhưng ta chỉ có thể chọn khối đến trước và khối kia (tốn rất nhiều năng lượng tạo ra) bị lãng phí và bỏ đi. Những đặc trưng kể trên phần nào nói lên nhược điểm của giải thuật mà phần lớn các đồng tiền ảo đang sử dụng.

Khi độ khó để tạo ra một khối càng ngày càng tăng lên, việc đào ra một khối của các thợ mỏ ngày càng thấp và họ bắt đầu thua lỗ,một số sẽ quyết định từ bỏ hoặc tham gia vào các bể đào (mining pool). Việc này tạo ra các cỗ máy tập trung (trái với các tính chất phân tán mà mô hình mong muốn). Và còn một vấn đề hệ quả nữa là tấn công 51% (51% attack) sẽ được nên ở sau.

Nhưng nó phổ biến có nguyên nhân của nó. Giá trị sử dụng của nó là khi một đồng tiền ảo mới được phát hành, lượng tiền chưa được nhiều. Hầu hết các đồng tiền ảo sẽ chọn mô hình này để gia tăng lượng tiền mà vẫn kiểm soát được phần nào lạm phát của nó (điều mà ETH đã làm), tiền chỉ được tạo ra không hề dễ dàng.

* POS: Khi mà POW bộc lộ rõ các yếu điểm thì là lúc các mô hình và các giải thuật khác được đề xuất, trong đó có POS. Thực tế thì POS đã được áp dụng ở một số đồng tiền ảo, tiên phong trong đó là PeerCoin và Ethereum sẽ là cái tên tiếp theo áp dụng mô hình này.

Mô hình POS thay vì công nhận công việc của anh bằng sức lực anh bỏ ra (chi cho phần cứng và năng lượng) thì lại công nhận bằng nó bằng cổ phần hay số tiền mà anh đặt cọc vào mỗi khối người đó sinh ra. Và giờ đây, mỗi khối không phải là cuộc chạy đua xem ai giải mã được chính xác và nhanh nhất (có thể gây lãng phí với các khối thừa) mà việc tạo khối được chỉ định cho người nào góp cổ phần nhiều nhất vì hệ thống tự động hiểu rằng nếu anh góp vào nhiều tiền như vậy thì anh cũng sẽ có đủ khả năng tính toán để tạo ra khối mới. Và một điều quan trọng nữa là sẽ không còn tồn tại việc thưởng ETH theo mỗi khối đào được mà chỉ trả cho người tạo khối một khoản tiền vì đã thực hiện giao dịch (transaction fee).

* POA: POA khá khác so với hai mô hình đồng thuận trước, trong khi hai mô hình trên vẫn giữ tính ẩn danh của tất cả những người tham gia và sự tin tưởng khó có thể đạt tới sự chắc chắn (tạm tin tưởng vào lượng công việc cũng như cổ phần) thì thay vào đó ta sẽ có các cơ quan được chứng thực một cách hợp pháp và công khai tham gia vào mạng như các thành viên kiểm chứng. Những cơ quan này sẽ sở hữu các tài khoản và các nút được coi là có thẩm quyền, các thành viên trong mạng có thể tin tưởng hoàn toàn họ và họ sẽ đóng vai trò chính trong việc kiểm tra các giao dịch và các khối có hợp lệ hay không.

Mạng theo mô hình này sẽ có một số lợi thế vượt trội so với hai mô hình kia như thời gian tạo khối tương đối ngắn, không lãng phí vì không cần phải đào, giúp cải thiện thời gian triển khai, kiểm thử và ngăn chặn các cuộc tấn công spam. Ethereum đã triển khai một mạng thử nghiệm triển khai mô hình này có tên là Kovan.

* Hợp đồng thông minh: sẽ nói rõ hơn phần sau

## 2.2 Hợp đồng thông minh (Smart contract).

### A. Khái niệm:

Smart Contract ( hợp đồng thông minh) là một giao thức quản lý hợp đồng đảm bảo tính nhanh gọn và minh bạch. Toàn bộ quá trình của Smart Contract là được thực hiện một cách tự động và không có sự can thiệp từ bên ngoài. Mục tiêu chính của Smart Contract là cho phép 2 bên không xác định danh tính có thể giao dịch hay là việc với nhau trên internet mà không cần thông qua trung gian.

Trong Smart Contract nêu rõ các điều khoản và hình phạt tương đương một hợp đồng truyền thống, tuy nhiên Smart Contract không cần sự can thiệp của con người, nên sẽ đảm bảo việc thực thi chính xác và khách quan nhất.

### B. Cách thức hợp đồng thông minh hoạt động.

Smart Contract hoạt động như một chương trình mà nó thực thi các tác vụ cụ thể trong trường hợp thỏa mãn các điều kiện nhất định. Một hệ thống Smart Contract thường tuân theo các câu lệnh “Nếu… thì...”. Thực ra hiểu đơn giản thì Smart Contract là một đoạn mã mà chạy trên một hệ thống phân tán (blockchain).

Đối với mạng Ethereum, các Smart Contract sẽ có trách nhiệm là thực thi và quản lý các hoạt động diễn ra trên blockchain khi những người dùng tương tác với nhau. Các địa chỉ không phải là địa chỉ của Smart Contract đều được gọi là các tài khoản độc lập. Nên có thể hiểu là SC do máy tính kiểm soát. còn các tài khoản độc lập thì do người dùng kiểm soát.

Smart Contract được triển khai thông qua giao dịch blockchain và chúng chỉ được kích hoạt khi một tài khoản độc lập ( hoặc các hợp đồng thông minh khác) triển khai chúng lên mạng.

Khi hợp đồng thông minh được triển khai thì tài sản và các điều khoản hợp đồng được mã hóa và chuyển vào một block của Blockchain, sau đó hợp đồng này được phân phối đến tất cả các node hoạt động trên nền tảng đó, tức là các hợp đồng thông minh này phi tập trung, không tập trung trên một máy chủ tập trung duy nhất mà phân tán và tự thực hiện trên các node mạng.

### C. Sự khác nhau hợp đồng thông minh và hợp đồng truyền thống.

* Hợp đồng truyền thống được tạo ra bởi các chuyên gia pháp lí để biên soạn và thi hành. Điều này rất mất thời gian và không minh bạch hoàn toàn. Khi có sự cố xảy ra thì phải dựa vào hệ thống pháp lí để giải quyết hợp đồng và điều này sẽ tốn các chi phí liên quan.
* Hợp đồng thông minh được tạo ra bởi hệ thống máy tính bằng ngôn ngữ lập trình. Trong đó nêu rõ các điều khoản và hình phạt tương đương với các hợp đồng truyền thống đưa ra. Nhưng hợp đồng thông minh không cần sự can thiệp của con người, do đó đảm bảo việc thực thi hợp đồng được chính xác và công minh nhất. Toàn bộ hợp đồng thông minh được thực hiện bởi hệ thống chuỗi khối phân tán.

# 3. Triển khai Multi-Sig Wallet trên Ethereum.

## 3.1 Khái niệm và chức năng Multi-Sig Wallet.

Multi-Sig Wallet là Smart Contract dựa trên hợp đồng đa bên và được triển khai trên blockchain. Mục đích của ví multisig là tăng cường bảo mật bằng cách yêu cầu nhiều bên đồng ý về các giao dịch trước khi thực hiện.

Ví dụ, nếu bạn có ví đa chữ ký (multi-sig wallet) được cấu hình cho 3 trong số 5 chữ ký, điều này có nghĩa là đối với bất kỳ giao dịch nào được xử lý, bạn sẽ cần ít nhất ba trong năm chữ ký để phê duyệt trước khi giao dịch được xác nhận.

Multi-Sig Wallet giúp bảo vệ tiền của tổ chức một cách tốt nhất, có nhiều lý do nhưng quan trọng nhất là:

* Để ngăn chặn 1 người rút, hay là bị hack
* Tránh trường hợp tài sản bị đóng băng khi tài sản chỉ có 1 người kiểm soát.

Các thành viên ký lên ví chung sẽ có các địa chỉ khác nhau và các tài sản khác nhau riêng của họ. Họ deploy Smart Contract Multi-Sig Wallet và tương tác với ví đa chữ ký này bằng ví của họ.

## 3.2 Triển khai project Multi-Sig Wallet.

### 3.2.1 Các công cụ áp dụng.

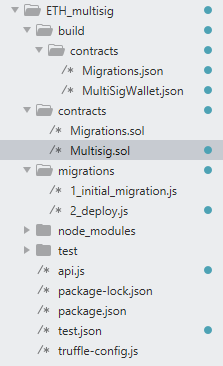
Truffle: là một framework của lập trình Ethereum, cho phép tạo test environment, viết test cho contract và nhiều thứ khác nữa. Ta sẽ thực hiện tạo project bằng truffle.

Ganache: Trước khi deploy ứng dụng blockchain của mình lên môi trường production, thì ta nên thực hiện test nó trên môi trường local. Ganache là một blockchain ảo, thiết lập 10 địa chỉ Ethereum mặc định, hoàn chỉnh với các private key, mỗi địa chỉ có sẵn 100 Ether. Khi kích hoạt Ganache thì ta sẽ có địa chỉ IP và cổng mặc định là localhost:7545 hoặc 127.0.0.1:7545 (đối với ứng dụng phiên bản UI).

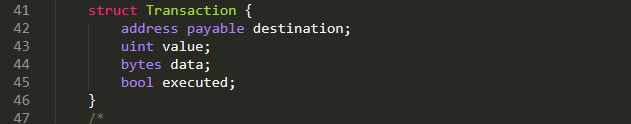
Thư viện Web3.js: Bộ thư viện web3.js giúp chúng ta kết nối và truy xuất vào mạng blockchain local hoặc mạng Ethereum. Là một thư viện trung gian với trách nhiệm giúp developer phát triển các ứng dụng client tương tác với blockchain Ethereum. Nó bao gồm tập hợp các thư viện cần thiết cho bạn thực hiện các hành động như gửi Ether từ tài khoản này sang tài khoản khác, đọc và ghi dữ liệu từ smart contract, tạo smart contract. Webe.js giao tiếp với blockchain Ethereum và Json RPC.

### 3.2.2 Xây dựng Multi-Sig Wallet Smart Contract.

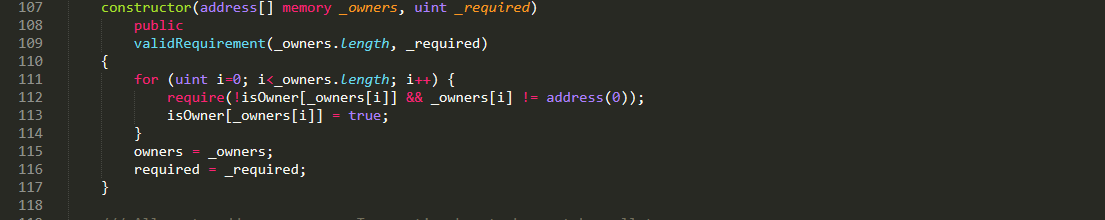
* Thành phần cơ bản cần có của Multi-Sig Wallet:
* Danh sách những người được phép
* Quy tắc để một sự kiện được thực hiện
* Cách submit một yêu cầu( gửi tiền, thay đổi danh sách người được phép, quy tắc,…)
* Các các yêu cầu được thực hiện
* Tạo project bằng Truffle, project ETH\_multisig có dạng:



* Thực hiện viết smart contract Multisig.sol
* Cấu trúc một transaction có dạng:



* Trong hợp đồng thông minh này sẽ có hàm constructor quy định những người được phép ký, các thành viên này ký lên 1 ví chung, ví của hợp đồng thông minh:



* Các function về gửi tiền, thêm danh sách người được phép ký vào ví chung, xóa một người trong danh sách đó, thay đổi quy tắc mà một sự kiện được thực hiện (tối thiểu bao nhiêu người confirm trong số những người được phép ký):



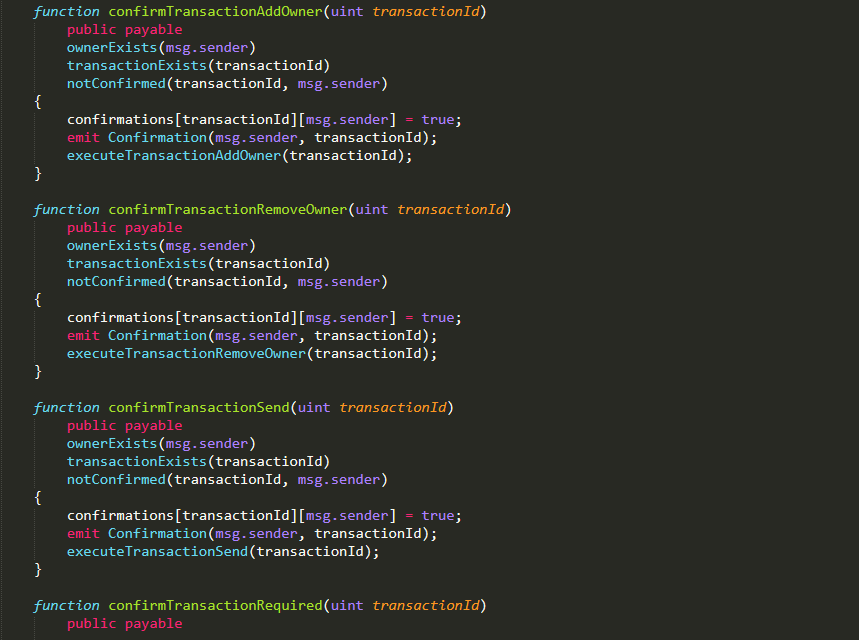


* Các function submit các Transaction với yêu cầu thêm người được phép, xóa người được phép, gửi tiền , thay đổi điều kiện để 1 sự việc xảy ra, …

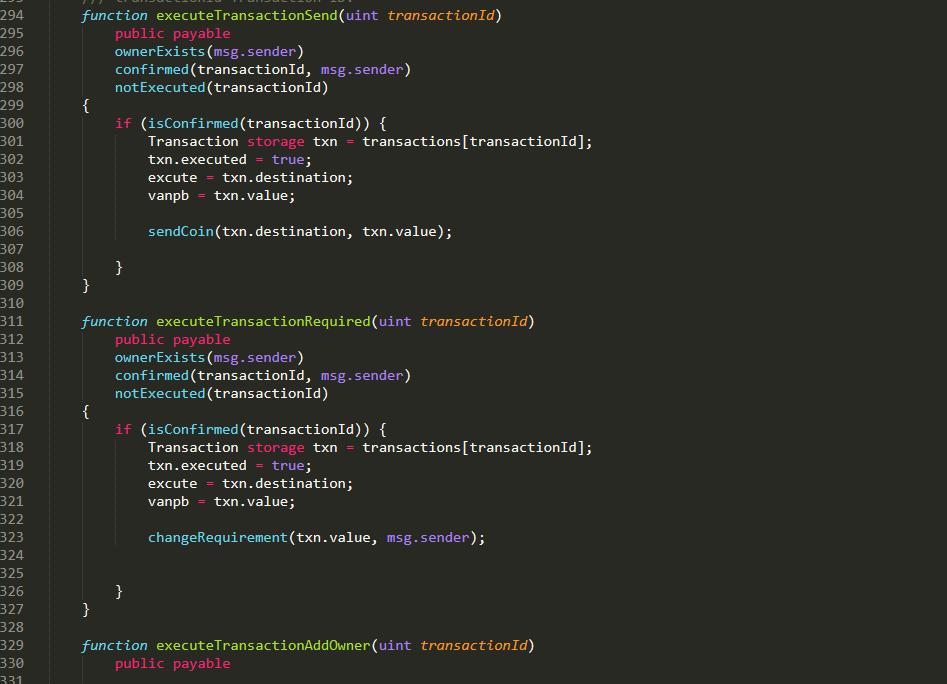


Chỉ những người ký lên ví mới được submit Transaction

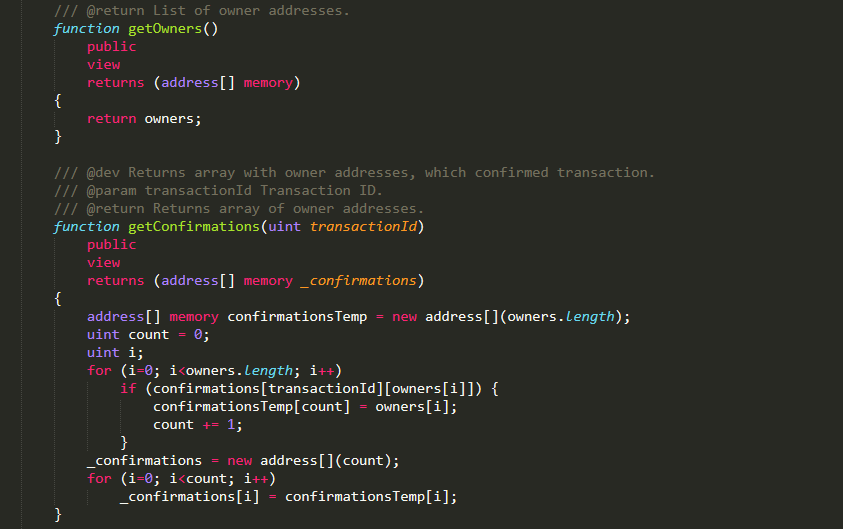
* Khi submit các transaction thì các thành phần trong những người ký lên ví sẽ thực hiện confirm:



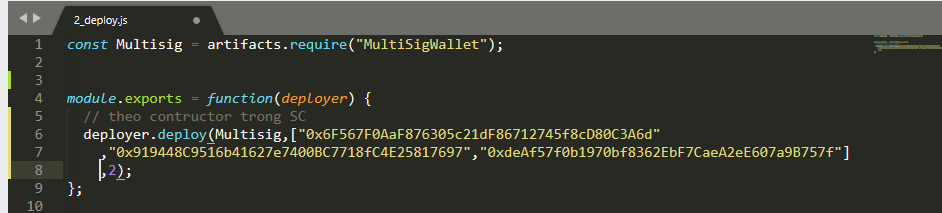
* Khi các transaction submit được số confirm đúng số lượng quy tắc đặt ra thì các yêu cầu được thực hiện bằng các hàm:



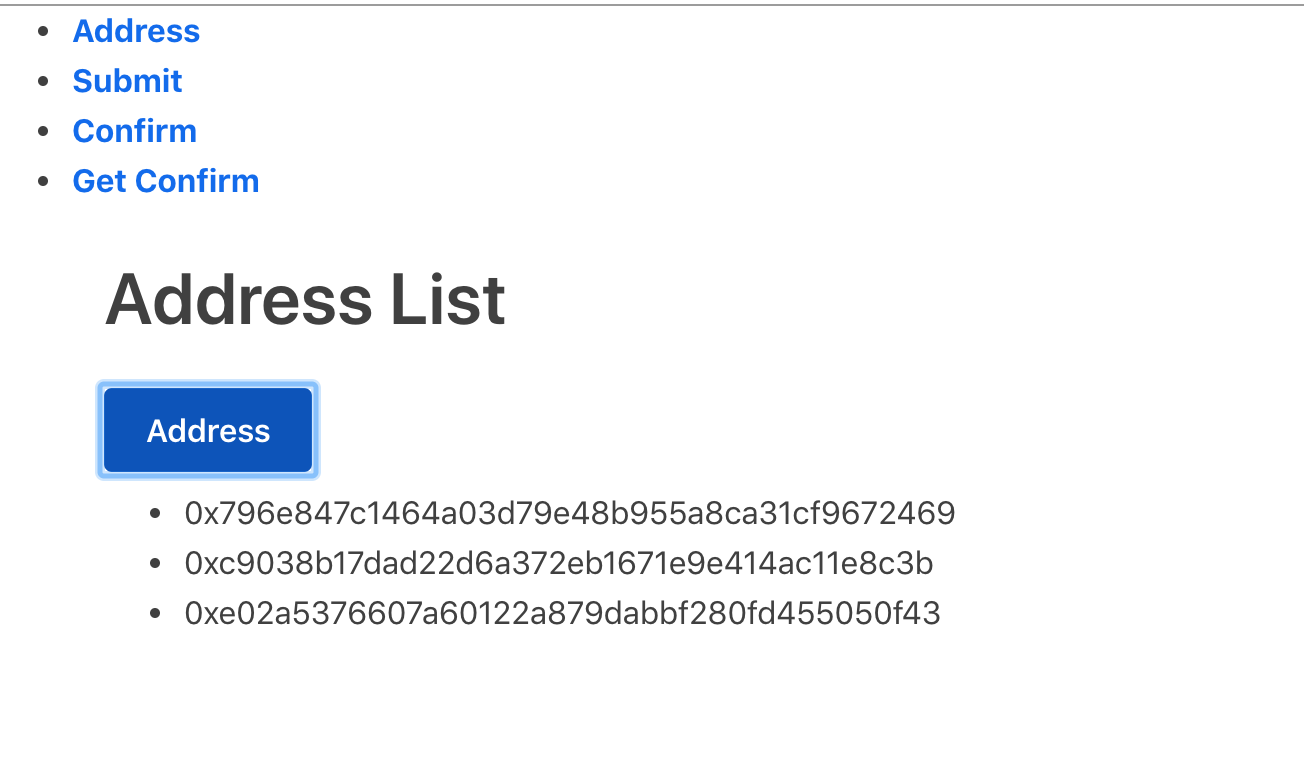
* Sau đó trong smart contract còn có các function để lấy danh sách những người ký lên ví, số lượng confirm để yêu cầu được thực hiện,…



* Tạo file 2\_deploy.js tại thư mục migrations để deploy smart contract Multisig.sol



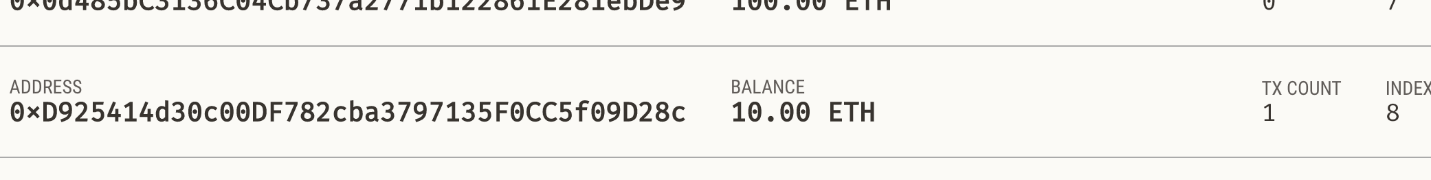
* Kết quả Demo: ta thực hiện demo khi deploy hợp đồng lên, gửi cho tài khoản hợp đồng thông minh 1 số lượng tài khoản, ví dụ khi một người được ký lên ví chung muốn thực hiện chuyển tiền từ ví này đến 1 tài khoản, họ submit yêu cầu và đợi đủ lượng confirm tối thiểu thì tiền tự động được chuyển đển tài khoản được yêu cầu.
* Danh sách các địa chỉ là thành viên của multisig:



* Address đầu tiên muốn chuyển tiền thực hiện submit (gửi 1 ETH):



* Địa chỉ đích có giá trị ETH ban đầu là:



* Address thứ 2 thực hiện confirm:



* Khi đó đủ số confirm thì smart contract tự động chuyển tiền, ETH của địa chỉ đích lúc này là:



* Chúng ta cũng có thể xem danh sách Address đã confirm

# Tài Liệu Tham Khảo

[1] ["Ethereum Yellow Paper"](https://github.com/truonganhhoang/int3507-2017/blob/master/Nhom%208%20Ethereum/yellowpaper.io), Gavin Wood

[2] [www.ethereum.org](http://www.ethereum.org)

[3] [www.blockchain.com](http://www.blockchain.com)

[4] "Blockchain", [www.wikipedia.org](http://www.wikipedia.org/)

[5] ["Introducing Ethereum and Solidity"](https://drive.google.com/file/d/0Bz_MvHBFauwkY1lFdThyQ0U1dE0/view), Chris Dannen

Và 1 số nguồn trên internet khác.