**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC VINH**

**NGUYỄN THỊ TÂM**

**CÔNG NGHỆ BLOCKCHAIN, HỢP ĐỒNG THÔNG MINH VÀ ỨNG DỤNG TRONG QUẢN LÝ THUÊ NHÀ**

**LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN**

**NGHỆ AN, 6/2020**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC VINH**

**NGUYỄN THỊ TÂM**

**CÔNG NGHỆ BLOCKCHAIN, HỢP ĐỒNG THÔNG MINH VÀ ỨNG DỤNG TRONG QUẢN LÝ THUÊ NHÀ**

Chuyên ngành: CÔNG NGHỆ THÔNG TIN

Mã số: 848.02.01

**LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN**

Người hướng dẫn khoa học: TS. Lê Văn Minh

**NGHỆ AN, 6/2020**

**LỜI CẢM ƠN**

  Để hoàn thành luận văn này, tôi xin được tỏ lòng biết ơn và gửi lời cám ơn chân thành đến TS. Lê Văn Minh, người trực tiếp hướng dẫn luận văn, đã tận tình chỉ bảo và hướng dẫn tôi định hướng nghiên cứu, tiếp cận vấn đề, tìm kiếm tài liệu, giải quyết vấn đề… từ đó tôi mới có thể hoàn thành luận văn cao học của mình.

Ngoài ra, trong quá trình học tập, nghiên cứu và hoàn thành luận văn tôi còn nhận được nhiều sự quan tâm, góp ý, hỗ trợ quý báu của quý thầy cô, đồng nghiệp, bạn bè và người thân. Tôi xin bày tỏ lòng biết ơn sâu sắc đến:

Cha mẹ và những người thân trong gia đình đã hỗ trợ, tạo điều kiện thuận lợi cho tôi trong suốt thời gian qua và đặc biệt trong thời gian tôi theo học khóa thạc sĩ tại trường Đại học Vinh

Quý thầy cô Viện Kỹ thuật và Công nghệ và quý thầy cô Phòng đào tạo Sau đại học – trường Đại học Vinh đã truyền đạt cho tôi những kiến thức bổ ích trong suốt hai năm học vừa qua

Ban giám hiệu cùng toàn thể thầy/cô và các em học sinh thân yêu của trường PTTH Thái Hòa đã tạo điều kiện, giúp đỡ và động viên tôi trong suốt hai năm học vừa qua

Các bạn học viên Cao học K26 Thái Hòa, những người đã đồng lòng, đoàn kết cùng nhau học tập và nghiên cứu để có thành quả như ngày hôm nay.

*Nghệ An, ngày 6 tháng 6 năm 2020*

**Tác giả**

**Nguyễn Thị Tâm**

**LỜI CAM ĐOAN**

Tôi xin cam đoan luận văn này là kết quả tìm hiểu và nghiên cứu của bản thân, có sự hỗ trợ của Thầy hướng dẫn và những người tôi đã cảm ơn. Các kết quả nghiên cứu trong đề tài này là trung thực, các nội dung trích dẫn rõ ràng nằm trong danh mục tài liệu tham khảo và chưa được công bố.

*Nghệ An, ngày 6 tháng 6 năm 2020*

**Học viên**

**Nguyễn Thị Tâm**

**MỤC LỤC**

[DANH MỤC CÁC TỪ VIẾT TẮT 1](#_Toc42258597)

[DANH MỤC CÁC HÌNH 2](#_Toc42258598)

[MỞ ĐẦU 4](#_Toc42258599)

[1. Sự cần thiết của vấn đề nghiên cứu 4](#_Toc42258600)

[2. Mục tiêu nghiên cứu 6](#_Toc42258601)

[3. Đối tượng và phạm vi nghiên cứu 6](#_Toc42258602)

[4. Kết cấu của luận văn 6](#_Toc42258603)

[CHƯƠNG 1. TỔNG QUAN VỀ CÔNG NGHỆ BLOCKCHAIN 7](#_Toc42258604)

[1.1 Khái niệm blockchain 7](#_Toc42258605)

[1.2 Đặc điểm và nguyên lý hoạt động của blockchain 9](#_Toc42258606)

[1.2.1. Đặc điểm 9](#_Toc42258607)

[1.2.2. Nguyên lý hoạt động của blockchain 10](#_Toc42258608)

[1.3 Ứng dụng Blockchain 17](#_Toc42258609)

[1.3.1 Ứng dụng của blockchain trong thương mại điện tử 19](#_Toc42258610)

[1.3.2 Ứng dụng của blockchain trong dịch vụ tài chính, ngân hàng 19](#_Toc42258611)

[1.3.3 Ứng dụng của Blockchain trong chuỗi cung ứng 21](#_Toc42258612)

[1.3.4 Ứng dụng của blockchain trong nông nghiệp 22](#_Toc42258613)

[1.3.5 Ứng dụng của blockchain trong giáo dục, y tế 22](#_Toc42258614)

[1.3.6. Ứng dụng của Blockchain trong Internet of Things (IoT) 22](#_Toc42258615)

[1.4 Tương lai của Blockchain 23](#_Toc42258616)

[1.5 Kết luận chương 25](#_Toc42258617)

[CHƯƠNG 2. HỢP ĐỒNG THÔNG MINH VÀ ETHEREUM 27](#_Toc42258618)

[2.1 Hợp đồng thông minh 27](#_Toc42258619)

[2.1.1 Khái niệm hợp đồng thông minh. 27](#_Toc42258620)

[2.1.2 Lợi ích của hợp đồng thông minh 30](#_Toc42258621)

[1.2.3 Ưu điểm nhược điểm của hợp đồng thông minh 31](#_Toc42258622)

[2.2 Ethereum 32](#_Toc42258623)

[2.2.1 Các khái niệm cơ bản 32](#_Toc42258624)

[2.2.2 Tài khoản 33](#_Toc42258625)

[2.2.3 Giao dịch 34](#_Toc42258626)

[2.3 Hoạt động của hợp đồng thông minh trên nền tảng Ethereum 35](#_Toc42258627)

[2.3.1 Các yêu cầu hệ thống 35](#_Toc42258628)

[2.3.2 Mô hình hoạt động hợp đồng thông minh 36](#_Toc42258629)

[2.3.3 Mô hình thiết kế 38](#_Toc42258630)

[2.4 Kết luận chương 40](#_Toc42258631)

[CHƯƠNG 3. ỨNG DỤNG HỢP ĐỒNG THÔNG MINH TRONG QUẢN LÝ THUÊ NHÀ. 41](#_Toc42258632)

[3.1. Mô hình quản lý thuê nhà 41](#_Toc42258633)

[3.2. Hợp đồng 42](#_Toc42258634)

[3.3 Cài đặt thử nghiệm. 42](#_Toc42258635)

[3.4 Kết luận chương. 50](#_Toc42258636)

[KẾT LUẬN 52](#_Toc42258637)

[TÀI LIỆU THAM KHẢO 53](#_Toc42258638)

# DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Giải nghĩa** |
|  | DAO | Decentralized Application organization |
|  | Dapps | Decentralized applications |
|  | EOA | Externally owned account |
|  | EVM | Ethereum virtual environment |
|  | GUI | Graphic user interface |
|  | IDE | Integrated development environment |
|  | IoT | Internet of Things |
|  | P2P | Peer-to-peer |
|  | POW | Proof of work |
|  | POS | Proof of stake |
|  | Testnet | Testing network |

# DANH MỤC CÁC HÌNH VÀ BẢNG

[Hình 1.1. Mô hình bài toán các vị tướng Byzantine 7](#_Toc44939455)

[Hình 1.2. Kiến trúc Blockchain. 8](#_Toc44939456)

[Hình 1.3. Mô hình phân quyền 10](#_Toc44939457)

[Hình 1.4. Mô hình kết nối của blockchain [10],[5]. 11](#_Toc44939458)

[Hình 1.5. Cấu trúc một khối trong chuỗi. 12](#_Toc44939459)

[Hình 1.6. Mô hình chuỗi blockchain. 13](#_Toc44939460)

[Bảng 1.1. Chữ ký số và mã hóa [12]. 14](#_Toc44939461)

[Hình 1.7. Mô hình giao dịch của Blockchain [6]. 14](#_Toc44939462)

[Hình 1.8. Mô hình kết nối các giao dịch của blockchain [6]. 15](#_Toc44939463)

[Hình 1.9. Cấu trúc rẽ nhánh của blockchain [17]. 16](#_Toc44939464)

[Hình 1.10. Cơ chế giá trị băm 17](#_Toc44939465)

[Hình 1.11. Ứng dụng blockchain cho tài chính thương mại. 21](#_Toc44939466)

[Hình 2.1. Mô hình tiền mã hóa và hợp đồng thông minh. 37](#_Toc44939467)

[Hình 2.2. Tạo lập hợp đồng thông minh. 39](#_Toc44939468)

[Hình 2.3. Thực hiện hợp đồng thông minh. 39](#_Toc44939469)

[Hình 2.4. Kiểm tra hợp đồng. 40](#_Toc44939470)

[Hình 3.1. Cấu trúc chủ hộ và tham số. 42](#_Toc44939471)

[Hình 3.2. Cấu trúc người thuê nhà và nhận xét. 43](#_Toc44939472)

[Hình 3.3. Cấu trúc chu kỳ và tham số. 43](#_Toc44939473)

[Hình 3.4. Hàm khởi tạo của hợp đồng thông minh. 44](#_Toc44939474)

[Hình 3.5. Hàm kích hoạt cư dân mới. 44](#_Toc44939475)

[Hình 3.6. Hàm đưa khách hàng ra khỏi danh sách thuê nhà. 45](#_Toc44939476)

[Hình 3.7. Hàm trừ tiền vào số dư tài khoản khách thuê. 45](#_Toc44939477)

[Hình 3.8. Hàm trừ tiền từ số dư tài khoản của chủ sở hữu. 46](#_Toc44939478)

[Hình 3.9. Hàm thay đổi nhiệm vụ cho khách thuê. 46](#_Toc44939479)

[Hình 3.10. Hàm thiết lập lại nhiệm vụ cho khách thuê. 47](#_Toc44939480)

[Hình 3.11. Hàm thiết lập lại phàn nàn cho mỗi vòng. 47](#_Toc44939481)

[Hình 3.12. Biên dịch hợp đồng. 48](#_Toc44939482)

[Hình 3.13. Ký xác thực để triển khai hợp đồng. 48](#_Toc44939483)

[Hình 3.14. Triển khai hợp đồng. 49](#_Toc44939484)

[Hình 3.15. Kết quả triển khai hợp đồng thể hiện trong Ganache. 49](#_Toc44939485)

[Hình 3.16. Tương tác với hợp đồng. 50](#_Toc44939486)

[Hình 3.17. Các hàm cơ bản của hợp đồng thông minh. 50](#_Toc44939487)

# MỞ ĐẦU

## 1. Sự cần thiết của vấn đề nghiên cứu

Những năm gần đây, Blockchain và các ứng dụng của nó nổi lên như một xu thế công nghệ của tương lai. Công nghệ blockchain nhận được sự quan tâm của nhiều các nhà đầu tư và các doanh nghiệp trên thế giới, blockchain đã và đang được ứng dụng trong nhiều ngành công nghiệp khác nhau, đặc biệt trong lĩnh vực tài chính.

Tính đến thời điểm hiện tại thì hợp đồng thông minh có thể được coi là ứng dụng được sử dụng nhiều nhất của công nghệ blockchain.

Khái niệm hợp đồng thông minh được giới thiệu bởi Nick Szabo, Ông là một nhà khoa học máy tính và một học giả pháp lý, ông kết hợp hai thứ đó lại vào năm 1994, và đã khai sinh ra khái niệm về smart contract (hợp đồng thông minh) mà chúng ta đang thấy trên tính năng của Ethereum.

Ông đi đến kết luận rằng bất kỳ sổ cái phi tập trung nào cũng có thể được sử dụng làm hợp đồng tự thực hiện (self-executable contracts), sau này được gọi là Hợp đồng thông minh (smart contracts). Các hợp đồng kỹ thuật số này có thể được chuyển đổi thành mã máy và được phép chạy trên blockchain. [Ethereum](https://en.wikipedia.org/wiki/Ethereum) (ETH) hay còn được gọi là Bitcoin 2.0 là một nền tảng điện toán phân tán khối chuỗi chạy trên công nghệ 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](https://blogtienao.com/ether-trong-ethereum-la-gi/).

Mặc dù ý tưởng về các hợp đồng thông minh đã xuất hiện từ rất lâu nhưng thế giới mà chúng ta đang sống hiện tại vẫn dựa trên hợp đồng trên giấy rất nhiều. Ngay cả khi hợp đồng kỹ thuật số được sử dụng thì sự tham gia của bên thứ ba trung gian cũng có thể dẫn đến các vấn đề bảo mật hoặc các hoạt động gian lận cùng với sự gia tăng chi phí giao dịch. Tuy nhiên nhờ sự ra đời của blockchain - cho phép tất cả các thực thể trong mạng tương tác với nhau phi tập trung => loại bỏ sự tham gia của bên thứ ba trung gian. Blockchain chính là công nghệ cho phép chúng ta lưu trữ dự liệu trên một sổ cái phân tán. Các dữ liệu của hồ sơ và giao dịch được cập nhật theo thời gian thực cho tất cả các bên trong mạng, đảm bảo tính minh bạch và toàn vẹn dữ liệu.

* Các thỏa thuận hợp đồng truyền thống, chẳng hạn như các thỏa thuận được tạo ra bởi một chuyên gia pháp lý, chủ yếu dựa trên giấy và dựa nhiều vào các bên thứ ba để thực thi. Thực thi bên thứ ba không chỉ rất tốn thời gian, mà còn rất mơ hồ. Nếu mọi thứ đi lệch hướng, các bên tham gia hợp đồng thường phải dựa vào hệ thống tư pháp công cộng để khắc phục tình hình, điều này có thể rất tốn kém và mất thời gian.
* Hợp đồng thông minh, thường được tạo bởi các lập trình viên máy tính thông qua sự trợ giúp của các công cụ phát triển hợp đồng thông minh, hoàn toàn bằng kỹ thuật số và được viết bằng các ngôn ngữ mã lập trình như Solidity , C ++, Go, Python, Java. Mã này xác định các quy tắc và kết quả theo cùng một cách mà một văn bản pháp lý truyền thống sẽ nêu rõ nghĩa vụ, lợi ích và hình phạt có thể do một trong hai bên trong các trường hợp khác nhau. Mã này sau đó có thể được tự động thực thi và thi hành bởi một hệ thống sổ cái phân tán .

Nhờ các tính năng của mình, hợp đồng thông minh có thể được áp dụng trong các ngành và lĩnh vực khác nhau như các giao dịch mua bán, cho thuê, các giao dịch thương mại điện tử, bất động sản và quản lý tài sản, v.v.

Hợp đồng thông minh có thể đem lại những lợi ích đáng kinh ngạc nếu chúng được áp dụng trong cuộc sống hàng ngày, thay thế cho các hợp đồng truyền thống. Chúng cung cấp một giải pháp tiện lợi và an toàn cho dù thứ tài sản bạn cần trao đổi có thể là bất động sản, tiền tệ hoặc cổ phần,... Việc loại bỏ sự tham dự của bên thứ ba cũng là một đặc điểm hấp dẫn để áp dụng hợp đồng thông minh vào cuộc sống hàng ngày.

Tại hội thảo quốc tế về ứng dụng blockchain, Ông Vương Quang Long, CEO của TomoChain – startup phát biểu: “Nhà nước và các doanh nghiệp Việt Nam có thể ứng dụng blockchain vào các lĩnh vực cụ thể như y tế (quản lý hồ sơ bệnh án), quản lý dữ liệu công dân, chuỗi cung ứng sản phẩm, nông nghiệp (truy xuất nguồn gốc thực phẩm), phát hành cổ phiếu, giao dịch chuyển tiền…Các ứng dụng phi tập trung giúp tự động hóa những quy trình thông qua ‘smart contract’- hợp đồng thông minh, tăng cường khả năng minh bạch, tin cậy”[[1]](#footnote-1).

Như vậy, chúng ta nhận thấy sự cần thiết cũng như cơ hội và thách thức khi nghiên cứu và đưa ra các giải pháp ứng dụng blockchain đặc biệt là ứng dụng hợp đồng thông minh vào cuộc sống. Hiện nay, nội dung đó đang trở thành chủ đề nóng thu hút nhiều tổ chức, nhà nghiên cứu và cộng đồng tham gia.

## 2. Mục tiêu nghiên cứu

Nghiên cứu tìm hiểu về công nghệ blockchain, Hợp đồng thông minh, Ethereum và triển khai thử nghiệm cho quản lý thuê nhà.

## 3. Đối tượng và phạm vi nghiên cứu

Phạm vi và đối tượng nghiên cứu chính của luận văn bao gồm:

- Công nghệ blockchain

- Mô hình hợp đồng thông minh

- Triển khai hợp đồng thông minh trong Ethereum.

## 4. Kết cấu của luận văn

Cấu trúc luận văn bao gồm phần mở đầu và ba chương:

Mở đầu: Giới thiệu tổng quan, ngắn gọn về luận văn, mô tả sự cần thiết và mục tiêu nghiên cứu.

Chương 1: Tổng quan về công nghệ Blockchain

Chương 2: Hợp đồng thông minh và Ethereum

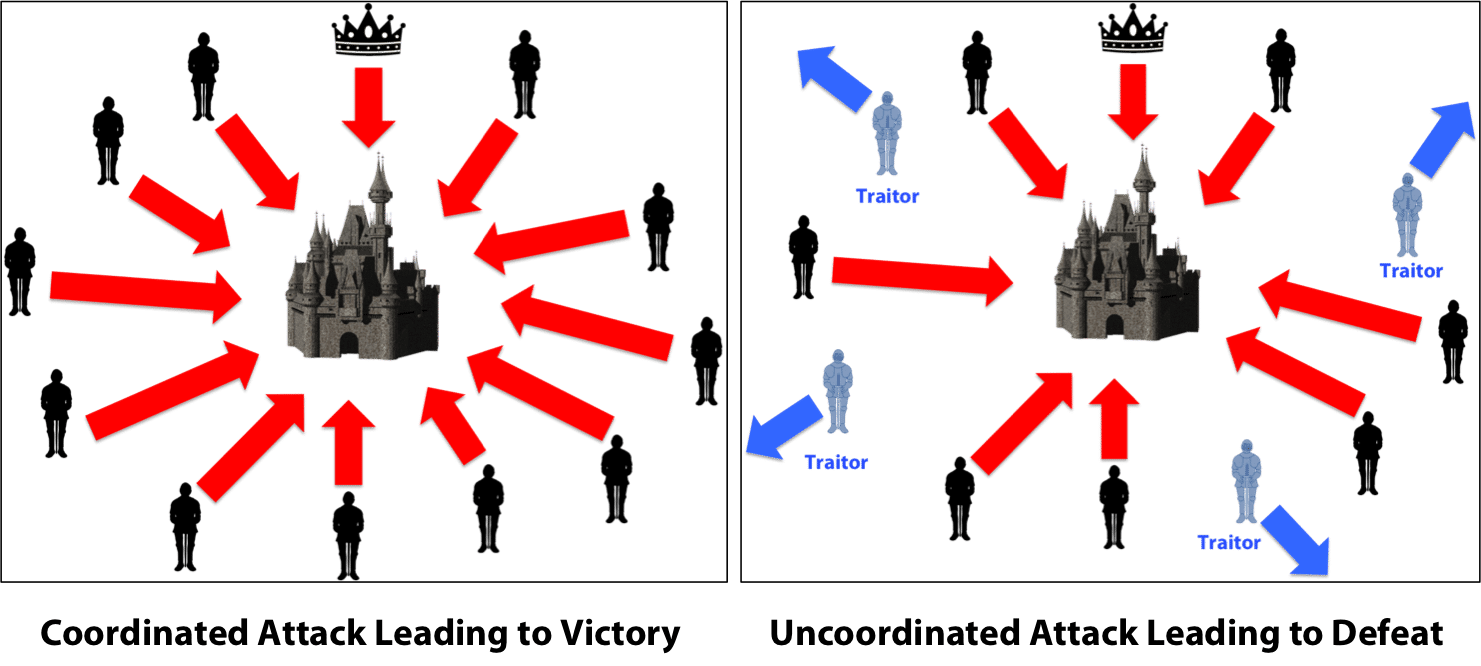
Chương 3: Ứng dụng hợp đồng thông minh trong quản lý thuê nhà.

# CHƯƠNG 1. TỔNG QUAN VỀ CÔNG NGHỆ BLOCKCHAIN

## 1.1 Khái niệm blockchain

Ý tưởng ra đời Blockchain bắt nguồn từ bài toán Các vị tướng Byzantine (Byzantine Generals) trong ngành khoa học máy tính và xử lý đường truyền tin cậy trong một hệ thống phân cấp.

Nội dung bài toán mô tả: Một đạo quân đi chiếm thành và các vị tướng nằm ở nhiều vị trí khác nhau. Trong đó có N tướng trung thành muốn chiếm thành và M tuớng phản bội muốn rút binh, một tướng phản bội truyền tin cho một nhóm là tấn công và truyền tin cho nhóm khác là rút binh. Vậy làm sao để các tướng có thể nhất quán thông tin và cùng nhau chiếm thành? Chỉ cần một sơ xuất trong việc truyền tin có thể khiến cả đạo quân có thể bị tiêu diệt.



Hình 1.1. Mô hình bài toán các vị tướng Byzantine

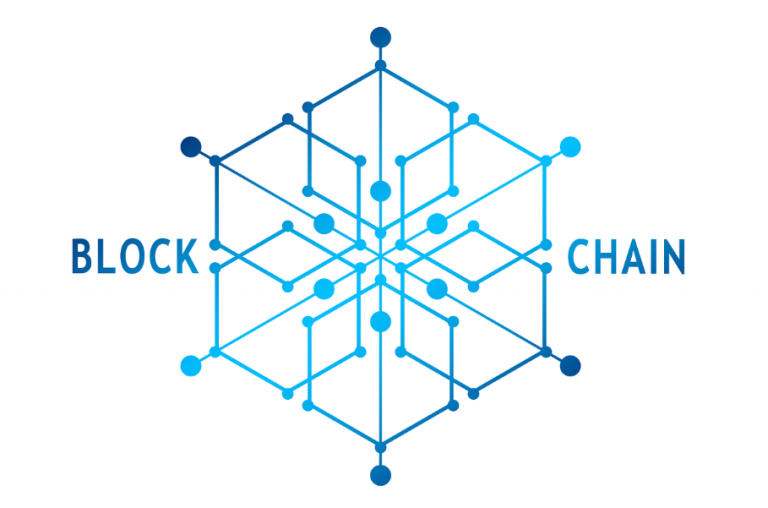
Nếu đồng loạt tấn công vào thành thì sẽ chiến thắng, bằng không tất cả sẽ bị tiêu diệt.

Bài toán Các vị tướng Byzantine này vẫn chưa ai có thể đưa ra lời giải. Do đó chúng ta cần phải có một bên thứ ba để xây dựng lòng tin. Ví dụ như trong bài toán trên, cần có một bên thứ ba đứng ra làm thoả thuận để các tướng lĩnh ký tên vào, nếu vị tướng nào làm trái thoả thuận sẽ bị trừng phạt. Bên thứ ba đảm bảo cho việc chiếm thành của các vị tướng là đồng loạt, bởi vì các tướng có thể không tin nhau nhưng bắt buộc phải tin tưởng tuyệt đối vào bên thứ ba này.

Đây là ý tưởng mở đầu cho một hệ thống Blockchain có thể giúp các vị tướng tin tưởng nhau hơn.

**Khái niệm Blockchain**

Theo các chuyên gia, Blockchain bao gồm các khối chứa các thông tin về thời gian khởi tạo và liên kết với các khối trước, việc truyền tải thông tin được thực hiện qua các khối kết nối với nhau và mở rộng theo thời gian.



Hình 1.2. Kiến trúc Blockchain.

**Blockchain** chính là công nghệ cho phép chúng ta lưu trữ dữ liệu trên một sổ cái phân tán. Các dữ liệu của hồ sơ và giao dịch được cập nhật theo thời gian thực cho tất cả các bên trong mạng, đảm bảo tính minh bạch và toàn vẹn dữ liệu.

Kiến trúc của Blockchain có thể chống lại sự thay đổi không nhất quán dữ liệu. Thông tin trong Blockchain chỉ có thể thay đổi hoặc bổ sung thêm khi có sự đồng thuận của quá nửa số nút tham gia trong hệ thống. Trong tình huống xấu nhất nếu một phần của hệ thống Blockchain bị hỏng, các máy tính và nút còn lại sẽ tiếp tục hoạt động để bảo vệ thông tin.

## 1.2 Đặc điểm và nguyên lý hoạt động của blockchain

### 1.2.1. Đặc điểm

Blockchain được ứng dụng giống như một cuốn sổ cái cho tất cả các giao dịch. Một số đặc trưng cơ bản của Blockchain có thể kể đến như:

• Dữ liệu không bị mất: dữ liệu blockchain được lưu trữ trên nhiều thiết bị của một mạng lưới gồm nhiều node phân tán, hệ thống và dữ liệu có khả năng chống lại lỗi kỹ thuật và các cuộc tấn công.

Mỗi node trong mạng có khả năng sao chép và lưu trữ một bản sao của cơ sở dữ liệu nên dữ liệu sẽ không bị mất mà được bảo toàn.

• Tính ổn định: các khối không thể bị đảo ngược, có nghĩa là dữ liệu đã được ghi vào blockchain, thì đồng nghĩa với việc loại bỏ hoặc thay đổi là vô cùng khó khăn. Chính điều này đã khiến blockchain trở thành công nghệ phù hợp cho các lĩnh vực lưu trữ hồ sơ tài chính hoặc các giao dịch, dữ liệu được ghi lại vĩnh viễn trên một sổ cái phân tán và công khai.

• Hệ thống không gửi niềm tin vào bên thứ ba: Hiện nay trong hầu hết các phương thức thanh toán truyền thống, các giao dịch sẽ được bảo chứng bởi một bên trung gian ví dụ như ngân hàng, công ty thẻ tín dụng… nhưng khi sử dụng công nghệ Blockchain sẽ loại bỏ quá trình trung gian này thông qua việc các nút phân tán xác minh các giao dịch.

Hệ thống blockchain thì sẽ loại bỏ tối đa được rủi ro từ việc tin tưởng vào một tổ chức duy nhất và giảm chi phí chung và chi phí giao dịch bằng cách loại bỏ các bên trung gian hoặc bên thứ ba.

• Tính minh bạch và không thể thay đổi: tất cả các dữ liệu lưu trữ trên blockchain có thể được xem xét công khai bởi các bên, tạo sự minh bạch. Các giao dịch là bất biến nghĩa là chúng không thể bị thay đổi hoặc bị xóa đi.

• Thực hiện các giao dịch nhanh hơn: các giao dịch liên ngân hàng có thể mất thời gian hàng giờ thậm chí là ngày để thực hiện xong. Nhưng với giao dịch Blockchain thì có thể giảm xuống đơn vị phút, hoặc giây và được xử lý 24/7.

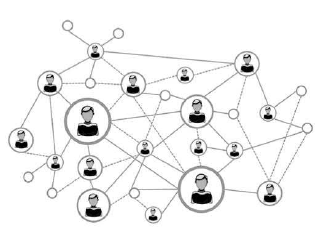
• Tiết kiệm chi phí: Tiết kiệm chi phí nhờ việc cắt giảm được các quy trình xác minh không cần thiết, giảm thiểu các lỗi và giảm tải việc lưu trữ bằng giấy truyền thống.

### 1.2.2. Nguyên lý hoạt động của blockchain

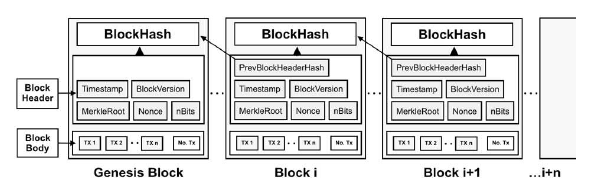
Cơ sở dữ liệu phân tán

Nền tảng của công nghệ Blockchain là cơ sở dữ liệu phân tán, được tạo thành bởi chuỗi các khối (Blockchain).

Thực chất Blockchain là một cơ sở dữ liệu chứa thông tin được quản lý đồng thời bởi nhiều người tham gia hệ thống, thay vì một cơ quan riêng lẻ như nhà nước hay ngân hàng trung ương. Thông tin mới cần được toàn bộ các thành viên trong mạng lưới chấp nhận trước khi được thêm vào cơ sở dữ liệu. Hệ thống phân quyền ngang hàng của một mạng blockchain được mô tả như hình 1.3.



Hình 1.3. Mô hình phân quyền

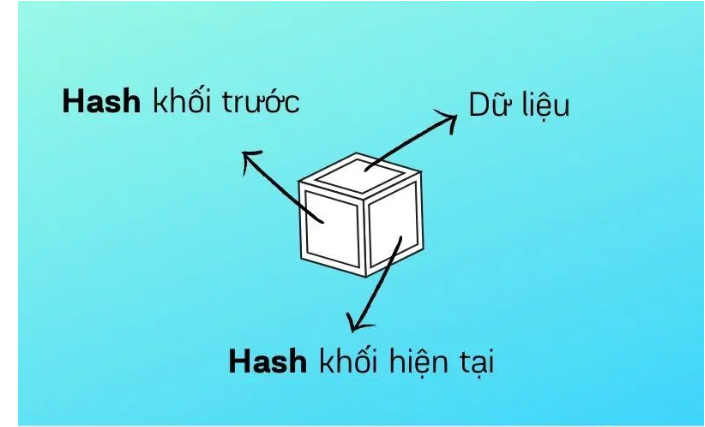
Người dùng tương tác với blockchain thông qua các máy khách được cài đặt trên các nút đại diện cho các máy tính thuộc nhiều loại khác nhau [5]. Do kiến trúc hệ thống không tập trung nên các nút có thể tham gia hoặc rời khỏi mạng bất kỳ lúc nào mà không làm ảnh hưởng đến các nút khác và các giao dịch đang xử lý [7]. Blockchain theo nghĩa đen bao gồm một chuỗi các khối, như được minh họa trong hình 1.3. Mỗi khối chứa một lượng dữ liệu nhất định, một số giao dịch trong một khoảng thời gian nhất định, được quy định trong giao thức hệ thống [8]. Như vậy, các block giống như là các thùng chứa của các giao dịch bao gồm các gói dữ liệu có thể nhận dạng lưu trữ các tham số và kết quả của các lời gọi hàm [9]. Các block kết nối với nhau bằng cách thêm thông tin mật mã của khối gốc (khối đã xác nhận trước đó) vào khối mới [10],[5]. Từ đó, việc xác nhận các giao dịch có thể được thực hiện từ "khối gốc" chứa các giao dịch ban đầu trong hệ thống [6].

Hình 1.4. Mô hình kết nối của blockchain [10],[5].

Sau khi hoàn chỉnh blockchain tạo thành một sổ cái và được phân phối công khai trên toàn mạng [10]. Một trong những hạn chế của blockchain liên quan đến khả năng mở rộng phạm vi. Khi thêm vào một block mới hệ thống sẽ yêu cầu toàn bộ bản sao có trong mỗi nút dẫn đến thách thức về không gian để thực hiện nhiệm vụ song song và ngăn chặn tạo ảnh của cơ sở dữ liệu [6]. Ngược lại, sẽ làm tăng thông lượng và khả năng mở rộng của hệ thống nếu chúng ta chỉ sử dụng một phần sao chép phân tán trong các cơ sở dữ liệu [11]. Từ những hạn chế trên dẫn đến hệ thống blockchain không đáp ứng được các yêu cầu giao dịch của các ứng dụng hiện đại như xử lý thanh toán tiền hay email. Ví dụ, hệ thống Bitcoin chỉ có khả năng xử lý 7 giao dịch trên mỗi giây trong khi các hệ thống xử lý thanh toán tập trung như Visa trung bình 2000 giao dịch trên mỗi giây, có thể đạt giá trị cao nhất là 56000 giao dịch trên mỗi giây [11]. Tuy nhiên, gần đây đã xuất hiện một số giải pháp đầy triển vọng. Dự án Coco của Microsoft Azure có thể đạt được tốc độ cao tới 600 giao dịch trên mỗi giây bằng cách thiết lập môi trường thực thi đáng tin cậy trong các mạng blockchain hiện có như Ethereum hoặc Hyperledger [12].

Thông tin trong mỗi khối riêng lẻ bao gồm các trường tạo thành khối băm. Ví dụ như phiên bản khối, giá trị băm header của khối trước, gốc cây merkle, nhãn thời gian, nBits và nonce. Trong đó phiên bản khối sẽ quyết định tập hợp các quy tắc xác thực cho khối theo sau. Giá trị băm header của khối trước đó sẽ trỏ đến chính khối ấy. Gốc cây merkle biểu thị cho giá trị băm của tất cả các giao dịch trong khối. Kỹ thuật này được áp dụng để tối ưu hóa việc xác minh các giao dịch với số lượng lớn. Nhãn thời gian cho biết thời gian hiện tại chính xác đến giây theo thời gian quốc tế. NBits là giá trị ngưỡng của một khối hợp lệ và trường nonce là một giá trị ngẫu nhiên được thêm vào khối, cả hai đều không nhất thiết phải có, tùy thuộc vào cơ chế đồng thuận được áp dụng [5].

Cấu trúc mỗi khối của Blockchain



Hình 1.5. Cấu trúc một khối trong chuỗi.

Mỗi khối (block) sẽ lưu trữ gồm 3 phần:

* Dữ liệu
* Giá trị băm của khối hiện tại
* Giá trị băm của khối trước

**Dữ liệu**

Dữ liệu sẽ tùy thuộc vào từng loại Blockchain. Chẳng hạn như blockchain của Bitcoin sẽ chứa dữ liệu giao dịch. Dữ liệu giao dịch gồm: Thông tin người gửi, nhận và số lượng coin được gửi.

**Giá trị băm của khối hiện tại**

Giá trị băm của khối hiện tại như một đặt điểm để nhận dạng. Nó là duy nhất và không trùng nhau giống như vân tay của chúng ta.

**Giá trị băm của khối trước**

Nhờ giá trị băm này mà các khối (block) liên kết tạo ra một chuỗi (chain). Tuy nhiên khối đầu tiên sẽ không được liên kết với bất cứ khối nào. Vì nó được tạo ra đầu tiên.

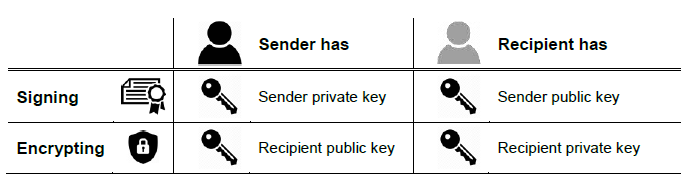
Khối đầu tiên này được gọi là Genesis block dịch ra tiếng Việt là “Khối nguyên thủy”.

A close up of a sign

Description automatically generated

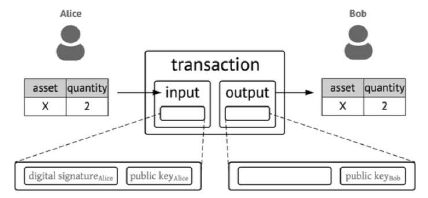
Hình 1.6. Mô hình chuỗi blockchain.

Việc băm dữ liệu kết hợp với nhãn thời gian được thực hiện trong phần lõi của giao thức giúp cho các giao dịch của blockchain an toàn và chống giả mạo [14], [6]. Trong mật mã, hàm băm là hàm toán học một chiều ánh xạ đầu vào dữ liệu chiều dài tùy ý thành các chuỗi bit có kích thước cố định và từ đó đầu vào ban đầu không thể đảo ngược [15]. Giá trị hàm băm này đại diện cho nội dung chính xác của tệp gốc có thể được kiểm tra bằng cách chạy hàm băm trên tệp gốc [14]. Như vậy, giá trị băm có thể được xem như là dấu vân tay của tệp dữ liệu.



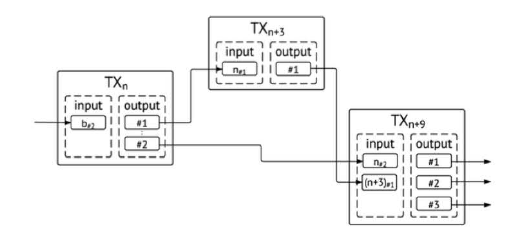
Bảng 1.1. Chữ ký số và mã hóa [12].

Dữ liệu truyền đi sẽ bao gồm giá trị băm của bản tin và khóa. Hình 1.4 minh họa các giao dịch trong hệ thống blockchain.



Hình 1.7. Mô hình giao dịch của Blockchain [6].

Các giao dịch trong blockchain thường được gắn với một chi phí được chỉ định, được biểu thị bằng các thẻ bài. Các thẻ bài này dùng để cấp quyền truy cập cho các ứng dụng và hoạt động như các khóa giám sát các giao dịch kỹ thuật số [14]. Một giao dịch trong mạng blockchain sẽ bao gồm giá trị băm của mã định danh giao dịch và danh sách các đầu vào và đầu ra [10]. Để có thể thông báo số dư của thẻ bài cho mỗi nút, sổ cái blockchain sẽ lưu trữ toàn bộ lịch sử giao dịch của hệ thống đồng thời xác minh giao dịch thông qua các liên kết của chúng đến các giao dịch trước đó [6]. Đầu ra của một giao dịch có thể được tham chiếu bởi một giao dịch khác hoặc không. Nếu có thì đầu ra của giao dịch được gọi là đã dùng, nếu không thì được gọi là đầu ra giao dịch chưa thanh toán [10]. Đầu vào của giao dịch phải được sử dụng để hoàn tất giao dịch và mỗi đầu vào chỉ có thể được sử dụng một lần [16]. Hình 1.5 biểu diễn sơ đồ của các giao dịch blockchain. Trong đó, chuỗi giao dịch theo dõi cách thức sở hữu thẻ bài và thông báo thay đổi còn blockchain theo dõi thứ tự các giao dịch hợp lệ.



Hình 1.8. Mô hình kết nối các giao dịch của blockchain [6].

Các giao dịch đã hoàn thành được nhóm thành các khối và được phát trong mạng. Các giao dịch được ghi trong một khối được coi là xác nhận, trong khi phần còn lại của các giao dịch được thực hiện trong mạng vẫn chưa được xác nhận hoặc chưa sắp thứ tự. Việc thêm một khối vào Blockchain được gọi là khai phá - một tiến trình được phân phối và có thể được thực hiện bởi các nút của mạng theo giao thức được áp dụng. Tính toàn vẹn của mạng blockchain phụ thuộc vào quy trình khai phá, nên ‘phần thưởng’ thường được sử dụng để đảm bảo rằng một số lượng lớn các nút tham gia vào tiến trình, từ đó phân tán xác nhận của các khối và ngăn ngừa tập trung quyền lực và sự ảnh hưởng [16], [ 5].

Có những tình huống hai khối khác nhau có thể được chọn vào mạng blockchain cùng một lúc. Điều này dẫn đến một phân nhánh của Blockchain như thể hiện trong hình 1.6. Vấn đề này có thể được giải quyết bằng cách thêm các khối sau vào ngã ba dài nhất được biết đến liên quan đến số tiền cao nhất của kết quả đạt được hoặc giá trị cho đến hiện thời. Việc thiết kế cơ chế đồng thuận tốt sẽ ngăn chặn được tình huống một nút nào đó có thể xác nhận khối nhiều lần trong một hàng hoặc nhiều khối được xác thực cùng một lúc. Hơn nữa, trong mỗi khối có chứa giá trị băm của khối cha mẹ nên việc khai thác “sớm” các khối bị ngăn chặn. Cuối cùng, chỉ có một ngã ba tồn tại và mạng đạt được sự đồng thuận về nội dung của sổ cái dựa trên nhánh dài hơn, làm mất hiệu lực của nhánh còn lại và giao dịch của nó được thực hiện [6], [16], [10].

A close up of a logo

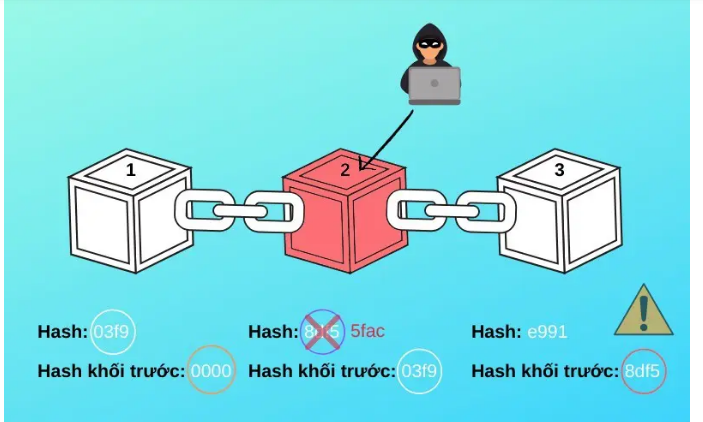
Description automatically generated

Hình 1.9. Cấu trúc rẽ nhánh của blockchain [17].

Đảm bảo tính toàn vẹn dữ liệu trên Blockchain

• Cơ chế giá trị băm: nếu sửa đổi được dữ liệu của một khối thì giá trị băm của khối đó sẽ bị thay đổi. Các khối phía sau khối đó cũng sẽ bị sửa đổi và trở nên không hợp lệ. Bởi vì lúc này giá trị băm của khối trước không giống với khối bị sửa đổi, hình 1.10. Cách duy nhất để sửa đổi dữ liệu của một khối là phải làm cho tất cả các khối phía sau nó trở nên hợp lệ.

• Cơ chế đồng thuận: để làm cho block hợp lệ thì bạn phải can thiệp vào các khối và thay đổi Hash một lúc. Nhưng vì máy tính ngày có thể tính toán rất nhanh. Mỗi giây, chúng có thể tính toán hằng trăm ngàn Hash. Điều này ảnh hưởng đến độ bảo bật. Lúc này, nhờ vào cơ chế đồng thuần sẽ quyết định ai là người sẽ thêm block mới. Mục dích để để chuỗi không bị ghi đè. Từ đó đảm bảo tính toàn vẹn và bảo mật.



Hình 1.10. Cơ chế giá trị băm

• Mạng ngang hàng (P2P Network)

Các blockchain sử dụng kiến trúc mạng ngang hàng thay vì một trung tâm quản lí. Điều này có nghĩa là ai cũng có thể tham gia vào mạng. Mỗi người trong mạng lưới đóng vai tro như một nút (node). Họ sẽ nhận một bản copy đầy đủ của blockchain. Sử dụng bản copy này để xác nhận mọi thứ đúng theo trình tự.

Tất cả các nút tạo sự đồng thuận. Nếu sự đồng thuận này lớn hơn 50% tức là khối đã hợp lệ và đươc thêm vào chuỗi khối.

Mạng ngang hàng kết hợp cùng sự đồng thuận tạo thành một lớp bảo vệ tránh các hoạt động gây hại.

## 1.3 Ứng dụng Blockchain

Hiện nay, Blockchain được chia thành 3 phiên bản:

• 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.

Ứng dụng được biết đến và thảo luận nhiều nhất về công nghệ Blockchain chính là đồng tiền điện tử Bitcoin. Hiện nay đồng tiền điện tử này có thể được sử dụng để trao đổi các sản phẩm và dịch vụ, giống như đồng đô la Mỹ (USD), Euro (EUR), đồng nhân dân tệ Trung Quốc (CNY) và các loại tiền tệ của các quốc gia khác. Do vậy chúng ta sẽ tạm lấy đồng tiền này làm đại diện để nói về nguyên lý hoạt động của công nghệ Blockchain.

“Bitcoin thực sự là ứng dụng đầu tiên của công nghệ blockchain cho phép chúng ta có thể gửi một tài sản dạng điện tử số thông qua mạng internet tới một người dùng khác trên mạng Internet, bên cạnh đó giao dịch này được đảm bảo an toàn và bảo mật, mọi người đều biết rằng việc chuyển tiền này đã diễn ra và không ai có thể xen vào và can thiệp hay sửa đổi quá trình này,” theo Marc Andreessen.

• 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 2.0 là thuật ngữ diễn tả chức năng mới của Blockchain đang tồn tại hiện nay so với mã nguồn nguyên thủy. Nền tảng Ethereum đã hiện thực hóa việc thiết lập và vận hành các ứng dụng phi tập trung và hợp đồng thông minh trên Blockchain.

Các ứng dụng phi tập trung và hợp đồng thông minh xây dựng trên mạng lưới Ethereum hoặc các Blockchain hiện thời khác có sử dụng các thẻ thay vì tiền kỹ thuật số đang là xu thế mới phát triển mạnh mẽ.

• 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.

Như đã đề cập ở trên Blockchain được ứng dụng lần đầu tiên vào Bitcoin và sau này nó được sử dụng rộng rãi trong lĩnh vực tiền điện tử (Cryptocurrency), nhưng hiện tại Blockchain đã được ứng dụng trong hầu hết các ngành công nghiệp khác nhau. Tiếp theo, chúng ta xem xét một vài ví dụ thiết thực về ứng dụng của công nghệ blockchain trong thực tế.

### 1.3.1 Ứng dụng của blockchain trong thương mại điện tử

• Warranteer: Là một ứng dụng blockchain cho phép người tiêu dùng dễ dàng truy cập thông tin về sản phẩm họ đã mua và nhận hỗ trợ dịch vụ trong trường hợp có trục trặc sản phẩm.

• Blockpoint: Là một ứng dụng đơn giản hóa việc tạo ra các hệ thống thanh toán và chấp nhận ví điện tử, chương trình khách hàng thân thiết, thẻ quà tặng và các chức năng khác.

• Loyyal: Được hỗ trợ bởi công nghệ blockchain và hợp đồng thông minh, nền tảng dịch vụ khách hàng thân thiết và tích điểm thưởng này tạo ra nhiều chương trình tùy chỉnh hơn, cho phép khách hàng tích điểm thưởng từ nhiều thương hiệu khác nhau.

### 1.3.2 Ứng dụng của blockchain trong dịch vụ tài chính, ngân hàng

• Bitcoin Atom: Là một nhánh mới của Bitcoin cho phép trao đổi tiền mã hóa dễ dàng mà không tốn phí giao dịch và không thể bị tấn công khi giao dịch, khiến Bitcoin thực sự được phân cấp lại. Công nghệ này dựa trên các hoán đổi nguyên tử (atomic swaps) – được xem là một công cụ vô giá để trao đổi các đồng tiền mã hóa và không cần phải có một bên thứ ba đáng tin cậy. Nhưng hiện tại, việc áp dụng rộng rãi các giao dịch hoán đổi nguyên tử đã bị ngăn chặn vì chúng đòi hỏi phải có kỹ năng kỹ thuật cao; Bitcoin Atom có thể giải quyết vấn đề này một phần nào đó.

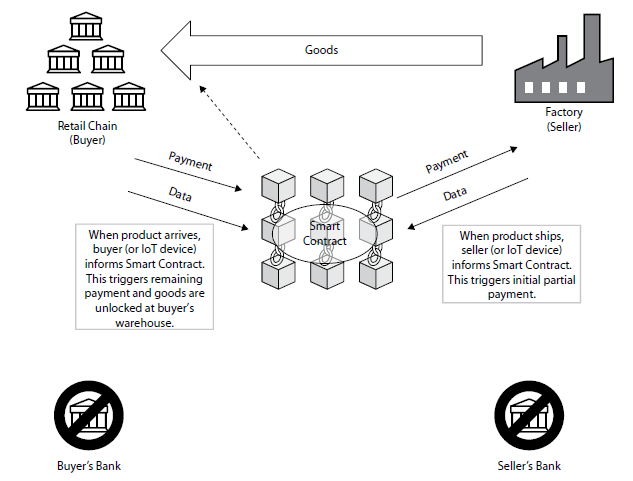
• Aeternity: Là một nền tảng blockchain có khả năng mở rộng cao này có thể được sử dụng cho bất kỳ ứng dụng nào yêu cầu tốc độ giao dịch cao, bao gồm các hợp đồng thông minh được tạo ra từ các thanh toán chuỗi, nano và vi mô.

• Ripple: Ripple nhắm đến việc trở thành một nhà cung cấp giải pháp thanh toán toàn cầu bằng cách kết nối ngân hàng, nhà cung cấp dịch vụ thanh toán, doanh nghiệp và các giao dịch tài sản kỹ thuật số, cho phép giải quyết ngay tức thì, theo nhu cầu trên toàn cầu

• Securrency: Đây là một nền tảng giao dịch tiền mã hóa và một vài loại tài sản, bao gồm cả những tài sản không hoán đổi thành tiền mặt, được trao đổi thông qua token của Securrency. Dự án cho phép tiền mã hóa được giao dịch bên ngoài các giao dịch chuyên dụng của chúng.

• ABRA: Là một ứng dụng toàn cầu và ví tiền mã hóa cho phép bạn mua, đầu tư và trữ 20 loại tiền mã hóa, bao gồm Bitcoin, ethereum, litecoin…

Tài chính thương mại đề cập đến các giao dịch tài chính, cả trong nước và quốc tế, liên quan đến tài chính thương mại có thể thu được và thương mại toàn cầu. Tài chính thương mại là hệ thống cốt lõi cho tất cả các hoạt động kinh doanh, buôn bán phạm vi toàn cầu. Trong đó hệ thống ngân hàng đóng vai trò quan trọng, đặc biệt là các ngân hàng cấp 1. Bởi vậy, nếu chậm trễ trong việc ứng dụng công nghệ và sử dụng các quy trình thủ công sẽ dẫn đến sự gián đoạn trong kinh doanh và sự thiếu minh bạch khiến cánh cửa mở ra cho tội phạm tài chính. Chuỗi cung ứng từ nhiều bên rất phức tạp, thiếu niềm tin, do đó tiến trình thực hiện rất chậm chạp và cần đến bên thứ ba như ngân hàng hay trung tâm thanh toán để tạo độ tin cậy cho phép chuỗi cung ứng thương mại được thực hiện. Hình 1.11 thể hiện một giải pháp để cung cấp tài chính chuỗi.



Hình 1.11. Ứng dụng blockchain cho tài chính thương mại.

Giải pháp cho vấn đề trên là dùng một hợp đồng thông minh lưu giữ tất cả các thông tin cần thiết, nội dung sẽ được cập nhật ngay lập tức và có thể xem được bởi tất cả các thành viên trên mạng. Hợp đồng thông minh có thể dùng để tự động hóa việc chuyển quyền sở hữu sang hàng hóa và tiền. Việc tự động hóa và xác thực mạng giúp loại bỏ sự cần thiết có mặt mang tính pháp lý của bên thứ ba, giúp hợp lý hóa toàn bộ quy trình và giảm chi phí.

### 1.3.3 Ứng dụng của Blockchain trong chuỗi cung ứng

Người tiêu dùng ngày càng muốn biết rằng có bao nhiêu phần trăm sự thật trong những tuyên bố về tiêu chuẩn sản phẩm của các công ty. Blockchain cung cấp cách thức xác nhận dễ dàng rằng những sản phẩm chúng ta mua là chính hãng hay không.

Tính minh bạch đi kèm với dấu thời gian (thông tin về ngày tháng, vị trí) dựa trên Blockchain, ví dụ đối với viên kim cương các thông tin trên sẽ tương ứng với mỗi sản phẩm.

Ở nước Anh có thể kiểm tra nguồn gốc xuất xứ của những mặt hàng tiêu dùng thông qua chuỗi cung ứng. Sử dụng Ethereum Blockchain, dự án thí điểm kiểm tra chất lượng đảm bảo rằng cá được bán trong các nhà hàng Sushi của Nhật đã được các nhà cung cấp cá ở Indonesia khai thác hiệu quả.

### 1.3.4 Ứng dụng của blockchain trong nông nghiệp

• Food industry: Là ứng dụng Blockchain có thể cải thiện tính minh bạch và hiệu quả trong việc tìm ra những loại thực phẩm có thể bị ô nhiễm và ở đâu trong suốt chuỗi cung ứng.

• OriginTrail: Là một nền tảng blockchain cho phép người tiêu dùng biết hàng hóa thực phẩm mà họ mua đến từ đâu và cách chúng được sản xuất.

### 1.3.5 Ứng dụng của blockchain trong giáo dục, y tế

• MedRec: Để cung cấp cho bất kỳ nhà cung cấp dịch vụ y tế truy cập an toàn vào hồ sơ của bệnh nhân, MedRec sử dụng blockchain để tiết kiệm thời gian, tiền bạc và các quy trình lặp lại trong việc tiến hành thủ tục giữa các cơ sở và nhà cung cấp khác nhau. Bệnh nhân cũng có thể truy cập vào hồ sơ y tế của họ để nghiên cứu các đơn vị cung cấp dịch vụ y tế.

• MedicalChain: Là công ty trong lĩnh vực chăm sóc sức khỏe đầu tiên sử dụng công nghệ blockchain để tạo thuận lợi trong việc lưu trữ và sử dụng hồ sơ y tế điện tử để cung cấp trải nghiệm y học từ xa (telemedicine) hoàn chỉnh. Họ là các bác sĩ thực tế trong hệ thống chăm sóc sức khỏe của Anh và muốn thay đổi hệ thống này từ bên trong.

### 1.3.6. Ứng dụng của Blockchain trong Internet of Things (IoT)

Một trong những ứng dụng của IoT là việc quản lý mạng lưới kiểm soát của một số loại thiết bị điện tử, ví dụ như nhiệt độ không khí trong nhà kho. Hợp đồng thông minh có thể tự động hóa việc quản lý hệ thống này từ xa. Một sự kết hợp của phần mềm, cảm biến và mạng sẽ tạo điều kiện trao đổi dữ liệu giữa các đối tượng và cơ chế vận hành. Kết quả làm tăng hiệu quả làm việc của hệ thống và cắt giảm chi phí theo dõi.

Các nhà sản xuất lớn nhất trong lĩnh vực sản xuất, công nghệ và viễn thông đều đang tranh giành ngôi vị thống trị của IoT, ví dụ Samsung, IBM, AT&T. Việc mở rộng cơ sở hạ tầng hiện có được kiểm soát bởi con người bằng ứng dụng IoT sẽ thực hiện nhiệm vụ từ dự đoán các bộ phận cơ khí đến thống kê dữ liệu và quản lý hệ thống tự động trên quy mô lớn.

## 1.4 Tương lai của Blockchain

Tại hội thảo “Blockchain: Tương lai khả thi cho quản lý tài chính” do đại học RMIT Việt Nam, Trung tâm Sáng tạo Công nghệ Blockchain RMIT (RMIT Blockchain Innovation Hub) và CPA Úc tổ chức ngày 1/8 tại Hà Nội, tiến sĩ Chris Berg đến từ Đại học RMIT Úc nhận định: Trong bối cảnh cuộc cách mạng công nghiệp 4.0 hiện nay, Blockchain đang ngày càng được biết đến là công nghệ có tiềm năng ứng dụng lớn trên thế giới cũng như tại Việt Nam.

Blockchain đang được xem là một trong những phát kiến mang tính đột phá, là một trong những công nghệ tác động mạnh mẽ nhất được phát triển trong những năm gần đây.

Với những đặc tính ưu việt như tính bảo mật cao và không thể tẩy xóa, giới công nghệ đánh giá Blockchain sẽ được ứng dụng trong nhiều lĩnh vực như công nghệ tài chính, ngân hàng, công nghiệp sản xuất, dịch vụ, chuỗi cung ứng, giáo dục. Ngoài ra, Blockchain còn được ứng dụng trong các cơ quan chính phủ để quản lý dữ liệu về dân cư, phương tiện giao thông.

Lấy ví dụ cụ thể với lĩnh vực tài chính ngân hàng, công nghệ Blockchain cho phép quản lý dữ liệu, tài sản và đảm bảo an toàn trong giao dịch.

Công nghệ Blockchain với thuật toán phức tạp, bảo mật cao, cho phép vô hiệu hóa việc can thiệp sửa đổi dữ liệu, giúp làm giảm phần lớn khả năng xảy ra sai sót khi đối chiếu các thông tin phức tạp từ nhiều nguồn khác nhau. Blockchain cũng loại bỏ yêu cầu sử dụng của một tổ chức trung gian (bên thứ 3), góp phần đẩy nhanh tốc độ thanh toán, giảm chi phí trong các giao dịch.

Vì những lợi ích đó, công nghệ này đang được đẩy mạnh ứng dụng trong giao dịch liên ngân hàng, giúp đảm bảo an toàn ở mức cao hơn so với phương thức giao dịch truyền thống. “Blockchain là một trong những động lực của cuộc cách mạng công nghiệp 4.0 hiện nay. Trong cuộc cách mạng công nghiệp 4.0, Blockchain cũng là nền tảng để ứng dụng trí tuệ nhân tạo, các công nghệ tự động hóa, dữ liệu lớn.”, tiến sĩ Chris Berg nhấn mạnh tại hội thảo.

Cũng theo tiến sĩ Chris, công nghệ Blockchain xuất hiện trên thế giới khoảng 10 năm nay, tuy có nhiều ứng dụng hiệu quả nhưng đến nay thực tế công nghệ này vẫn đang ở trong giai đoạn đầu tiên ứng dụng và tiếp tục được hoàn thiện.

Dù vậy theo đánh giá của chuyên gia đến từ đại học RMIT, sự phát triển của Blockchain cũng chính là cơ hội cho Việt Nam tìm hiểu, khai thác và ứng dụng vào thực tế các lĩnh vực để tạo ra những bước tiến nhảy vọt, đặc biệt trong phát triển ngành sản xuất, tài chính. Do tiềm năng ứng dụng trong ngành tài chính rất lớn, Việt Nam có thể bắt tay vào nghiên cứu công nghệ Blockchain để tạo ra những bước tiến nhảy vọt trong tương lai.

Theo đánh giá của tiến sĩ Chris Berg, các doanh nghiệp tại Việt Nam cũng đang quan tâm lớn đến công nghệ Blockchain ở cấp độ tối ưu hóa chuỗi cung ứng như ứng dụng để theo dõi luồng hàng xuất – nhập, giao dịch thương mại quốc tế vv.

Công nghệ Blockchain có những thiết kế, mục đích sử dụng khác nhau cho từng ngành, lĩnh vực, vấn đề đặt ra là phải tối ưu việc ứng dụng. Việt Nam tuy phát triển sau nhiều nước trong ứng dụng Blockchain nhưng có thể học hỏi những kinh nghiệm từ các quốc gia đã phát triển hơn và áp dụng vào thực tế.

Ngoài ra công nghệ Blockchain sở hữu những tính năng bảo mật cao, có thể ngăn ngừa rủi ro về an ninh mạng tốt hơn nhiều các công nghệ cũ trước sự tấn công của hacker.

Cũng theo chia sẻ của tiến sĩ Chris Berg, thời gian qua đại học RMIT đã có nhiều nghiên cứu, tìm hiểu về tác động của Blockchain đối với hoạt động của chính phủ, cộng đồng doanh nghiệp… nhằm đồng hành cùng doanh nghiệp, chính phủ, các ngành kinh tế để phát huy những lợi thế cũng như tìm hiểu mặt trái của Blockchain trong ứng dụng.

Năm 2018, đại học RMIT đã ra mắt khóa học ngắn hạn đầu tiên trong chương trình đại học của Australia về chiến lược Blockchain tại cơ sở Melbourne, nhằm bắt kịp xu hướng đào tạo Blockchain – một ngành đang nổi và ngày càng khẳng định vị thế quan trọng.

## 1.5 Kết luận chương

Nội dung chương này đã khái quát hóa các nét cơ bản của công nghệ blockchain bao gồm khái niệm, cơ sở dữ liệu phân tán, giao thức, cơ chế đồng thuận, giao dịch và các ứng dụng của blockchain. Hiểu một cách đơn giản blockchain là một cơ sở dữ liệu phân tán lưu trữ thông tin trong các khối, thông tin được kết nối với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và kết nối tới khối trước đó kèm theo mã thời gian và dữ liệu giao dịch. Kiến trúc của blockchain chống lại việc thay đổi của dữ liệu cho nên một khi dữ liệu đã được mạng blockchain chấp nhận thì sẽ không có cách nào thay đổi được.

Blockchain sẽ tiếp tục làm thay đổi ngành công nghiệp dịch vụ vì những lợi ích và tính năng mà nó có thể đem đến như: thông lượng nhanh hơn, giảm chi phí, ít xảy ra sai sót, minh bạch, tính tin cậy, đơn giản và truy xuất nguồn gốc. Từ các ưu điểm đó các ứng dụng của blockchain không chỉ giới hạn trong lĩnh vực tiền điện tử mà còn xa hơn nữa như hợp đồng thông minh. Nội dung chương tiếp theo chúng ta sẽ nghiên cứu về hợp đồng thông minh và môi trường triển khai Ethereum.

# CHƯƠNG 2. HỢP ĐỒNG THÔNG MINH VÀ ETHEREUM

Hợp đồng thông minh là thế hệ thứ hai của blockchain, sau tiền điện tử. Hợp đồng thông minh được thực hiện bằng cách tính toán trên mạng dựa trên các điều kiện đã được thỏa thuận trước về giao dịch và cũng có thể dựa vào các biến bên ngoài trong các giao dịch mà nhà xuất khẩu và nhập khẩu cùng với các ngân hàng hoặc bên trung gian khác hỗ trợ tài chính. Ethereum là nền tảng giúp hiện thực hóa việc thiết lập và vận hành các ứng dụng không tập trung và hợp đồng thông minh trên Blockchain.

## 2.1 Hợp đồng thông minh

### 2.1.1 Khái niệm hợp đồng thông minh.

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 thoả thuận giữa các bên trong hợp đồng (trong hệ thống các máy tính) nhờ sự hỗ trợ của công nghệ Blockchain. Toàn bộ hoạt động của hợp đồng thông minh được thực hiện một cách tự động và không có sự can thiệp từ bên ngoài, hay thông qua một bên thứ ba trung gian. Những giao dịch được thực hiện bằng các hợp đồng thông minh rất minh bạch, có thể dễ dàng truy xuất được và không thể bị can thiệp hoặc đảo chiều. Các điều khoản trong hợp đồng thông minh tương đương với một hợp đồng có pháp lý và được ghi lại dưới ngôn ngữ của lập trình.

Hợp đồng thông minh so sánh với hợp đồng truyền thống:

- Các thỏa thuận hợp đồng truyền thống: thỏa thuận được tạo ra bởi một chuyên gia pháp lý, chủ yếu dựa trên giấy và dựa nhiều vào các bên thứ ba để thực thi. Thực thi bên thứ ba không chỉ rất tốn thời gian, mà còn rất mơ hồ. Nếu mọi thứ đi lệch hướng, các bên tham gia hợp đồng thường phải dựa vào hệ thống tư pháp công cộng để khắc phục tình hình, điều này có thể rất tốn kém và mất thời gian.

- Hợp đồng thông minh, thường được tạo bởi các lập trình viên máy tính thông qua sự trợ giúp của các công cụ phát triển hợp đồng thông minh, hoàn toàn bằng kỹ thuật số và được viết bằng các ngôn ngữ mã lập trình như Solidity , C ++, Go, Python, Java. Mã này xác định các quy tắc và kết quả theo cùng một cách mà một văn bản pháp lý truyền thống sẽ nêu rõ nghĩa vụ, lợi ích và hình phạt có thể do một trong hai bên trong các trường hợp khác nhau. Mã này sau đó có thể được tự động thực thi và thi hành bởi một hệ thống sổ cái phân tán

Theo Szabo, các hợp đồng cần phải có một vài yếu tố khác biệt để được xác định là hợp đồng thực sự thông minh. Những đặc tính này là khả năng hiển thị, năng lực thực thi trực tuyến, tính xác thực và quyền riêng tư. Khả năng hiển thị có nghĩa là những người tham gia hợp đồng sẽ có thể nhìn thấy hiệu suất của các điều khoản khác trong hợp đồng hoặc có thể chứng minh quá trình thực hiện các điều khoản của riêng họ cho những người tham gia khác. Nó cũng đề cập đến khả năng hiển thị của các hành động được thực hiện bởi logic trong hợp đồng. Khả năng thực thi trực tuyến liên quan đến việc đảm bảo rằng các điều khoản của hợp đồng đang được thực hiện. Các biện pháp có thể được phân loại thành các biện pháp chủ động và bị động. Biện pháp chủ động tìm cách làm cho về mặt kỹ thuật không thể vi phạm các điều khoản hoặc cho phép một trong hai bên bỏ hợp đồng nếu có vi phạm hợp đồng ở một phần khác. Các biện pháp bị động ngăn chặn hành vi độc hại thông qua danh tiếng, nhưng cũng bằng cách thu hồi tài sản tiềm năng sau khi vi phạm hợp đồng. Hợp đồng thông minh cũng cần phải được kiểm tra hoặc có thể kiểm toán được nếu có xung đột xảy ra. Cuối cùng, hợp đồng thông minh đảm bảo riêng tư nhất nếu có thể, nghĩa là tính năng kiểm soát dữ liệu liên quan đến hợp đồng thông minh chỉ nên có sẵn cho người tham gia nếu cần thiết.

Chúng ta có thể nhận thấy rằng từ các mục tiêu của hợp đồng thông minh được đề cập như khả năng hiển thị, khả năng thực thi trực tuyến, kiểm chứng và quyền riêng tư sẽ dẫn đến hai hướng riêng biệt. Quyền riêng tư đang tạo ra sự kiểm soát đối với các hợp đồng, làm giảm đi sự cởi mở với bên ngoài. Ngược lại, có ba mục tiêu khác là khả năng hiển thị, khả năng thực thi và kiểm chứng đối với những người yêu cầu quyền truy cập vào dữ liệu hợp đồng phải được trao cho người tham gia hoặc kiểm toán viên. Do đó, thiết kế phải tối ưu để có ít thông tin và sự kiểm soát nhất để cung cấp cho các bên ở ngoài mà khả năng xác minh, giám sát và thi hành vẫn khả dụng. Năm 1997, trước khi có sự tiến bộ của công nghệ blockchain trong các mô hình tính toán an toàn của nhiều bên thì giải pháp của Szabo đối với vấn đề tối ưu hóa là tin tưởng vào bên thứ ba - bên trung gian, ví dụ như kiểm toán viên được xem là giải pháp [31].

Nền tảng Ethereum bao gồm một Blockchain tổng quát và một máy ảo (Ethereum Virtual Machine, EVM) để triển khai các hợp đồng thông minh. Do môi trường chỉ tồn tại trên blockchain dưới dạng máy ảo nên các hợp đồng thông minh được độc lập hoàn toàn khỏi mạng, hệ thống tệp hoặc các quy trình khác trên các node máy. Một ngôn ngữ cấp cao có cấu trúc Turing hoàn chỉnh được tạo ra để viết hợp đồng thông minh trên Ethereum.

Hiện nay, ngôn ngữ Solidity đã trở thành tiêu chuẩn cho các nền tảng khác có khả năng triển khai hợp đồng thông minh. Cú pháp của Solidity tương tự như JavaScript nhưng được viết theo một phong cách hoàn toàn khác. Sau khi một hợp đồng đã được xây dựng bằng Solidity nó được biên dịch thành mã byte EVM và sau đó được thực thi tại một địa chỉ Ethereum cụ thể. Tuy nhiên, để triển khai và tương tác với các hợp đồng thông minh trên Ethereum thì thư viện RPC JavaScript đặc biệt được sử dụng cùng với API web.3. Bởi vì lập trình hợp đồng thông minh bắt đầu với Ethereum và Solidity cho nên đây vẫn là một chủ đề đang được phát triển. Ngôn ngữ Solidity có một số đặc trưng đã biết và một danh mục các thay đổi sắp tới, tức là mã được viết bây giờ có thể không đầy đủ chức năng so với bản cập nhật tiếp theo.

Trong thực tế, có một vài mẫu hệ thống tốt nhất về lập trình dành riêng cho phát triển hợp đồng thông minh, tuy nhiên sau thời gian ngắn thì Solidity đã được sử dụng. Có hai yếu tố chính cần cân nhắc thêm về bảo mật để phát triển hợp đồng thông minh; Hợp đồng tin cậy là có khả năng xử lý quyền sở hữu các mã thông báo, vật phẩm hoặc quyền có giá trị đối với một thứ gì đó; việc triển khai hợp đồng thông minh xảy ra trên một blockchain, có nghĩa là tất cả những người tham gia có thể quan sát hợp đồng và mã nguồn của nó. Các nguyên tắc an toàn đã được thu thập trong thời gian khá ngắn mà đã được Solidity sử dụng là:

**Kiểm soát lỗi**: số lượng mã thông báo lưu trữ trong hợp đồng thông minh nên được giới hạn vì nếu mã nguồn, nền tảng hoặc trình biên dịch có chứa lỗi thì mã thông báo có thể bị kẹt trong hợp đồng.

**Modul hóa**: Hợp đồng thông minh được xây dựng càng nhỏ và đơn giản càng tốt. Kích thước các biến cục bộ và độ dài của các hàm nên có giới hạn để giữ cho các hợp đồng càng dễ đọc càng tốt. Càng nhiều modul hợp đồng thì càng dễ dàng cải thiện một hệ thống hợp đồng thông minh.

**Kiểm tra**: Các hàm quan trọng sẽ được kiểm tra điều kiện tiên quyết ở bước đầu tiên của thuật toán. Sau đó, các biến thay đổi trạng thái sẽ được thực hiện. Cuối cùng là tương tác với các hợp đồng khác sẽ xảy ra.

### 2.1.2 Lợi ích của hợp đồng thông minh

**Tự động hóa**: Quy trình thực hiện là tự động. Bạn chính là người tạo ra hợp đồng, không cần phải đến môi giới, trung gia hay bên thứ 3 nào, nên giảm thiểu nguy cơ lừa đảo do bên thứ 3 gây nên.

**Không bị thất lạc**: Hợp đồng của bạn được mã hóa trên một cuốn sổ cái chung, không thể bị mất hay thất lạc đi đâu được. Với Blockchain, tất cả những người bạn đều có lưu trữ lại tài liệu của bạn.

**An toàn**: Tài liệu, hợp đồng của bạn được bảo mật rất tốt, không có ai hay một hacker có thể tấn công và lấy nó đi.

**Nhanh chóng**: Hợp đồng thông minh sử dụng các ngôn ngữ lập trình, code phần mềm để tự động hóa các điều khoản, nhằm tiết kiệm thời gian nhất cho người dùng.

**Tiết kiệm chi phí**: hợp đồng thông minh sẽ giúp bạn tiết kiệm chi phí nhờ đã bỏ khâu trung gian thứ 3.

**Chính xác**: Tránh được các lỗi mà con người hay mắc phải khi viết giấy tờ thông thường.

### 1.2.3 Ưu điểm nhược điểm của hợp đồng thông minh

**Ưu điểm của hợp đồng thông minh**

• Ứng dụng được nhiều vào trong cuộc sống hàng ngày, một số lĩnh vực đã được triển khai hợp đồng thông minh chẳng hạn như: Ngân hàng, tiền điện tử, bầu cử,…

• Tự do: Không bị bất kì một cá nhân hay doanh nghiệp nào thao túng hay quản lý.

• An toàn minh bạch

**Nhược điểm của hợp đồng thông minh**

• Pháp lý: Nếu xảy ra một vấn đề gì thì bạn sẽ không được nhà nước hay cơ quan có thẩm quyền bảo vệ do các nước hiện nay chưa có chính sách để khai thác, quản lý hợp đồng thông minh.

• Chi phí triển khai: Cần chi trả cho hệ thống cơ sở hạ tầng, máy tính, và các lập trình viên giỏi để họ triển khai.

• Rủi ro từ internet: bản chất hợp đồng thông minh rất an toàn nhưng nếu bạn để lộ một số thông tin nhạy cảm hoặc bị các hacker khai thác các thông tin đó thì chắc chắn sẽ gặp những trường hợp rắc rối.

## 2.2 Ethereum

### 2.2.1 Các khái niệm cơ bản

Ethereum là một nền tảng blockchain được gọi là Hợp Đồng Thông Minh, cung cấp hệ thống máy ảo EVM (Ethereum Virtual Machine) và sử dụng đơn vị tiền tệ gọi là Ether trong hệ thống.

Ethereum (ETH) là:

• Một nền tảng (platform) chạy trên nền tảng công nghệ Blockchain

• Hỗ trợ hợp đồng thông minh (smart contract)

• Mạng lưới sử dụng tiền mã hoá 2.0

• Sử dụng blockchain riêng

• Có dự định chuyển từ sử dụng Proof of Work (Ethash) sang Proof of Stake (Casper)

• Có thể viết chương trình kiểu model Turing Complete chạy trên nền giao thức P2P

Về cơ bản, Blockchain của Ethereum cũng như các Blockchain khác. Được cấu thành bởi mạng lưới các máy tính hay còn gọi là Nodes.

Để tham gia vào mạng lưới, các nodes cần cài đặt phần mềm Ethereum Client như Geth, Parity ...v.v. Khi cài đặt Ethereum Client, đồng nghĩa với việc các nodes sẽ phải chạy một chương trình máy ảo EVM. EVM sẽ chịu trách nhiệm thực thi các chương trình hợp đồng thông minh.

Khi các nhà phát triển muốn xây dựng ứng dụng phi tập trung trên Ethereum, họ cần phải triển khai smart contract thông qua ngôn ngữ lập trình Solidity.

Để kích hoạt việc thực thi các hoạt động như smart contract, lệnh giao dịch... mạng lưới cần đến một lượng phí gọi là “Gas". Phí “Gas” trong mạng Ethereum sẽ được thanh toán bằng đồng tiền kỹ thuật số gọi là Ether (Ξ hay ETH).

Khi giao dịch được thực thi, đây là lúc cần đến việc xác nhận giao dịch đó có hợp lệ hay không. Trong mạng của Ethereum, thành phần đảm nhiệm việc xác nhận giao dịch này có tên - Miner Node. Để mạng lưới vận hành độc lập, nhất quán các miner nodes phải tuân theo luật đồng thuận - Consensus (hay còn gọi là cơ chế đồng thuận).

Ethereum sử dụng luật đồng thuận có tên - Proof of Work (PoW) hay còn gọi là bằng chứng công việc. Tức là các miner nodes phải chứng minh được công việc họ đã hoàn thành và thông báo đến toàn mạng lưới. Sau đó, các miner nodes khác trong mạng lưới sẽ xác nhận xem bằng chứng này là có hợp lệ hay không.

Công việc ở đây có thể là:

• Tạo ra block mới bằng cách tìm ra lời giải thông qua thuật toán - Ethash.

• Xác nhận giao dịch trên mạng lưới.

Khi bằng chứng được thông qua, dữ liệu giao dịch sẽ được ghi vào Blockchain của Ethereum và không thể thay đổi.

### 2.2.2 Tài khoản

Tài khoản là một đối tượng lưu trữ trạng thái của số dư tài khoản người dùng hoặc của hợp đồng.Tài khoản đầu tiên được gọi là tài khoản thuộc sở hữu bên ngoài (EOA), vì tài khoản này thuộc về một thực thể bên ngoài và được kiểm soát bởi một khóa riêng. Nó có thể gửi tin nhắn bằng cách tạo và ký các giao dịch với khóa riêng của nó.

Tài khoản thứ hai được gọi là tài khoản hợp đồng và trạng thái của nó được kiểm soát bởi hợp đồng mã. Khi một tài khoản hợp đồng nhận được một tin nhắn, mã của nó được thực thi. Nó cũng có thể gửi nhắn tin cho các hợp đồng khác hoặc tạo hợp đồng mới.

EVM không phân biệt giữa 2 loại tài khoản. Mỗi tài khoản có một lưu trữ khóa-giá trị được gọi là lưu trữ và số dư màu trắng có thể được thay đổi bằng cách gửi giao dịch bao gồm ether.

### 2.2.3 Giao dịch

Giao dịch là gói dữ liệu được ký bởi một bên ngoài sở hữu tài khoản. Nó chứa người gửi giao dịch, người nhận giao dịch, lượng ether được gửi, trường dữ liệu tùy chọn, giới hạn gas và trường giá gas. Một tin nhắn giống như một giao dịch được gửi từ hợp đồng này sang hợp đồng khác hợp đồng. Nó hoạt động tương tự như một cuộc gọi chức năng thông thường trong các ngôn ngữ lập trình khác.

Mỗi khi mã đang chạy của một tài khoản hợp đồng thực thi mã opp cuộc gọi, một tin nhắn được tạo và gửi đến hợp đồng người nhận hoặc tài khoản thuộc sở hữu bên ngoài. Cả hai hành động và cuộc gọi, có thể được sử dụng để tạo hợp đồng mới, để gọi các chức năng của hợp đồng hoặc để chuyển ether sang hợp đồng hoặc tài khoản thuộc sở hữu bên ngoài.

Ether là mã thông báo tiền tệ được Ethereum sử dụng để thanh toán phí giao dịch. Devel các opers phải cung cấp ether khi họ triển khai mã hợp đồng cho blockchain và người dùng phải chi tiêu hoặc đốt ether khi họ thực hiện giao dịch trên hợp đồng. Ether có thể trao đổi với các loại tiền tệ fiat khác thông qua các trao đổi tiền điện tử khác nhau.

Ether có thể được chia thành các đơn vị nhỏ hơn, nhỏ nhất trong số chúng được gọi là wei. Một ether bằng 10 18 trắng.

Gas được sử dụng để thanh toán phí giao dịch bằng Ethereum. Gas không phải là tiền tệ, mà là đơn vị định giá nội bộ tách rời giá thị trường của ether từ chi phí chuyển đổi hành động. 1 đơn vị khí đại diện cho giá cho hoạt động đơn giản nhất được thực hiện trên EVM. Giá cho một đơn vị gas, giá gas, có thể được điều chỉnh linh hoạt để thích ứng đến các giá trị dao động của tiền tệ ether. Giá khí có thể được xác định bởi người khởi tạo của một giao dịch và người khai thác quyết định xem họ có muốn bao gồm các giao dịch trong khối hay không.

Giới hạn khí hoặc giá trị bắt đầu của giao dịch xác định có bao nhiêu bước tính toán một giao dịch được phép thực hiện. Càng nhiều dòng mã hợp đồng thực thi và Càng sử dụng nhiều bộ nhớ và lưu trữ, giới hạn gas của nhu cầu giao dịch ban đầu càng cao Phí giao dịch và giới hạn gas giúp ngăn chặn việc thực thi mã bị lỗi, như vô hạn các vòng lặp và chúng giúp tiết kiệm tài nguyên tính toán trên mạng. Vì vậy, giới hạn khí không khuyến khích các cuộc tấn công từ chối dịch vụ tiềm năng trên mạng.

## 2.3 Hoạt động của hợp đồng thông minh trên nền tảng Ethereum

### 2.3.1 Các yêu cầu hệ thống

Một hợp đồng thông minh bao gồm những yếu tố sau:

• Chủ thể hợp đồng: hợp đồng thông minh phải được 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 vào hợp đồng thông minh đều phải đồng ý triển khai bằng chữ kĩ điện tử của họ.

• Điều khoản hợp đồng: điều khoản trong hợp đồng thông minh có dạng là một chuỗi các hoạt động. Và các bên tham gia hợp đồng đều phải ký chấp nhận nó.

• Nền tảng phân quyền: hợp đồng thông minh 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.

Bitcoin đã đặt ra những nền tảng cơ bản cho việc thiết lập hợp đồng thông minh trên Blockchain hay gọi tắt là “Smart Contract Blockchain”. Tuy nhiên, nó vẫn chưa thể thỏa mãn mọi yêu cầu về thiết lập và thực thi hợp đồng thông minh.

- Bitcoin được tạo ra như một loại tiền tệ và được lưu trữ như một tài sản có giá trị

- Ethereum là nền tảng giao dịch của một hợp đồng thông minh, là bộ giao thức cho phép tạo và thực thi hợp đồng thông minh.

- Ethereum được thiết kế rõ ràng để tạo điều kiện cho các hợp đồng thông minh Turing-complete và các ứng dụng phi tập trung trên mạng của nó.

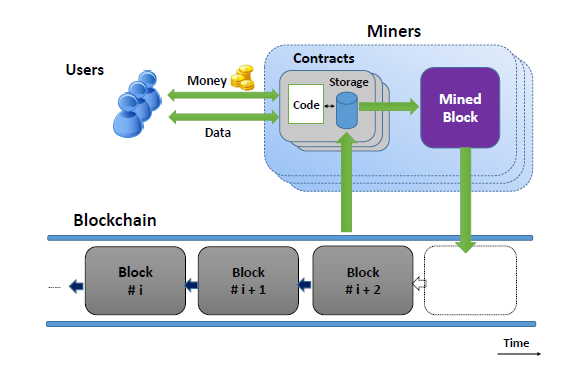
Chỉ đến khi Ethereum và Smart Contract Ethereum xuất hiện thì ý tưởng hợp đồng thông minh mới được phổ biến đến cho mọi người dùng, cung cấp cho ta thêm một phương thức mới để thiết lập hợp đồng.

Chúng ta thấy đặc tính kỹ thuật gần nhất với hợp đồng thông minh là Bitcoin. Tuy nhiên, Bitcoin có một hệ thống kịch bản thô sơ, không thân thiện với người dùng. Đã tốn một nguồn lực lớn trong cả lĩnh vực nghiên cứu và trong công nghiệp để thiết kế các ứng dụng hợp đồng thông minh khác nhau bằng cách trang bị thêm cho ngôn ngữ kịch bản của Bitcoin [3, 31].

Bởi vì các giới hạn cơ bản về biểu diễn trong ngôn ngữ kịch bản của Bitcoin cho nên việc trang bị thêm cho ngôn ngữ không những tốn thời gian mà có thể dẫn đến việc triển khai tốn kém hơn về số lượng vòng hoặc chi phí trên toàn bộ chuỗi. Nếu so sánh các tác vụ tương tự thì sẽ dễ cài đặt và hiệu quả hơn nếu chúng được lập trình trên một ngôn ngữ hợp đồng thông minh tổng quát (Ethereum [23] là ngôn ngữ đầu tiên).

### 2.3.2 Mô hình hoạt động hợp đồng thông minh

Hợp đồng thông minh là một chương trình máy tính chạy trên Blockchain, tức là các hoạt động được thực hiện bởi sự động thuận của tất cả các node. Hợp đồng thông minh bao gồm mã chương trình, tệp lưu trữ và số dư tài khoản. Bất kỳ ai cũng có thể tạo hợp đồng bằng cách đăng một giao dịch lên Blockchain. Mã chương trình của hợp đồng là cố định, không thể thay đổi khi hợp đồng được tạo ra. Như được hiển thị trong hình tệp lưu trữ của hợp đồng được lưu trữ trên Blockchain công khai. Logic chương trình hợp đồng được thực hiện bởi mạng lưới các “thợ mỏ”, những người sẽ đạt được sự đồng thuận về kết quả của quá trình thực hiện và cập nhật vào Blockchain tương ứng. Mã của hợp đồng được thực thi bất cứ khi nào nhận được tin nhắn từ người dùng hoặc từ hợp đồng khác. Trong khi thực thi mã hợp đồng có thể đọc hoặc ghi vào tệp lưu trữ dữ liệu của nó. Hợp đồng có thể nhận tiền vào số dư tài khoản của mình hoặc gửi tiền cho các hợp đồng hoặc người dùng khác.



Hình 2.1. Mô hình tiền mã hóa và hợp đồng thông minh.

Chúng ta thường quan niệm rằng hợp đồng là một bên thứ ba đặc biệt "đáng tin cậy". Tuy nhiên, bên thứ ba này chỉ được tin cậy về tính chính xác và tính sẵn sàng chứ không phải về quyền riêng tư. Bởi vì, toàn bộ trạng thái của hợp đồng sẽ hiện hữu công khai.

Mã của hợp đồng sẽ được gọi bất cứ khi nào nó nhận được giao dịch từ người dùng. Một hợp đồng có thể thực thi tại nhiều điểm, đối với ngôn ngữ Serpent của Ethereum thì mỗi điểm đầu vào được định nghĩa như một hàm. Trong nội dung của giao dịch sẽ chỉ rõ điểm đầu vào, từ đó mã của hợp đồng sẽ được gọi. Do vậy, các giao dịch hoạt động như là các lời gọi hàm trong các ngôn ngữ lập trình thông thường. Sau khi hợp đồng xử lý một tin nhắn mà nó nhận được thì có thể chuyển trả lại giá trị cho người gửi.

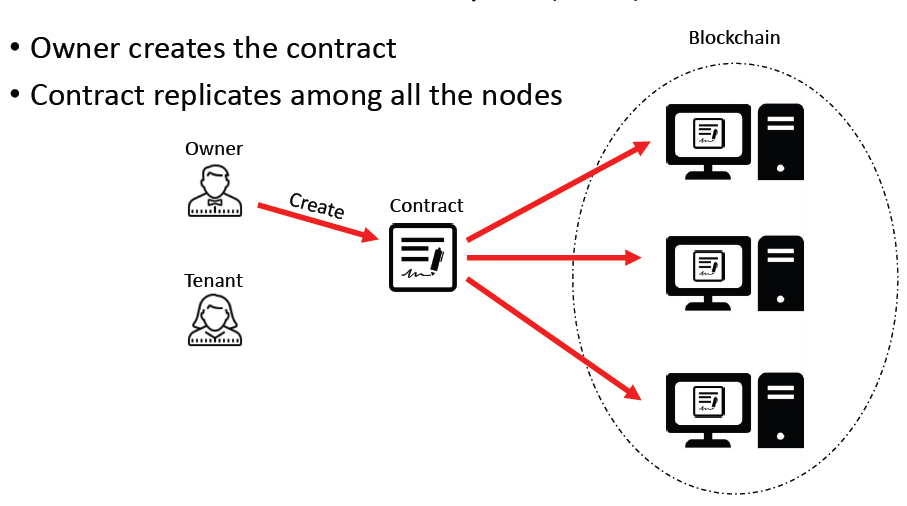
Trong Ethereum sử dụng khái niệm “gas” để ngăn chặn sự tiêu thụ quá mức tài nguyên. Người dùng tạo ra giao dịch phải chi tiền để mua gas. Bất cứ câu lệnh nào của chương trình đều tiêu thụ một lượng gas nhất định. Nếu hết gas trước khi giao dịch đạt đến điểm dừng thì nó được coi là một ngoại lệ và trạng thái được hoàn nguyên như thể chưa có giao dịch, nhưng Ether được sử dụng để mua gas không được hoàn trả. Khi một hợp đồng thông minh thực hiện việc gửi tin nhắn từ người này cho người khác, bên gửi có thể chuyển một phần gas của mình cho bên nhận. Nếu bên nhận hết gas hệ thống sẽ điều khiển trả lại cho bên gửi và bên gửi có thể sử dụng gas còn lại của mình để xử lý ngoại lệ và các bước tiếp theo.

Nội dung nghiên cứu tiếp theo về cách sử dụng ngôn ngữ Solidity của Ethereum để minh họa cho lập trình hợp đồng thông minh, các nguyên lý và quy trình này có thể áp dụng chung cho các loại tiền điện tử và hệ thống hợp đồng thông minh khác. Do đó, chỉ sử dụng một số thuật ngữ đặc tả Ethereum cần thiết trong các ví dụ ở phần tiếp theo. Ví dụ tiền tệ tích hợp của Ethereum gọi là Ether và Ether có thể được chia thành các đơn vị tiền tệ nhỏ hơn như “wei”.

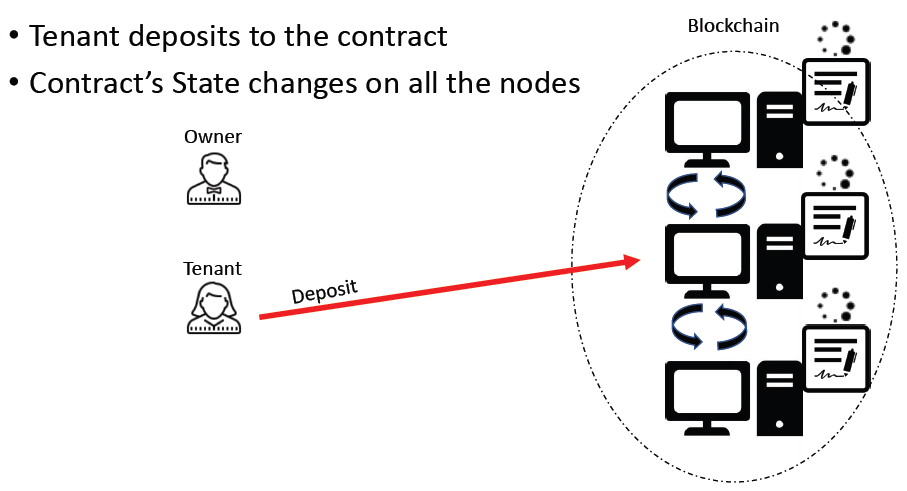
### 2.3.3 Mô hình thiết kế

Tiền điện tử là cơ sở nền tảng xây dựng nên hợp đồng thông minh. Tiền điện tử là một hệ thống phân tán, các tương tác với tiền ảo thực hiện trong một sổ cái chia sẻ chung. Người dùng có thể chuyển tiền và tương tác với hợp đồng thông minh bằng cách công bố các tin nhắn đã ký gọi là giao dịch lên mạng tiền điện tử. Mạng ở đây bao gồm các node (hay còn gọi là thợ khai phá) truyền thông tin, lưu trữ dữ liệu và cập nhật dữ liệu bằng cách sử dụng các giao dịch.

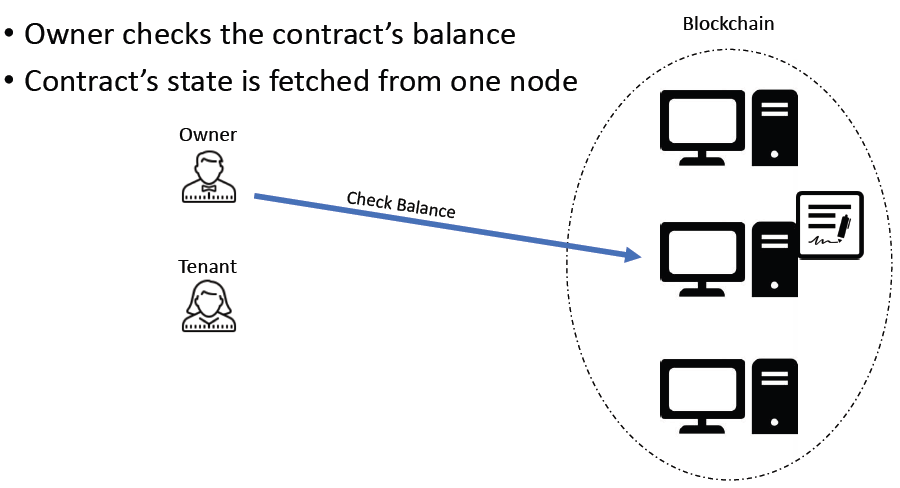
Các bước thực hiện tạo lập, triển khai và kiểm tra hợp đồng thông minh bao gồm:



Hình 2.2. Tạo lập hợp đồng thông minh.



Hình 2.3. Thực hiện hợp đồng thông minh.



Hình 2.4. Kiểm tra hợp đồng.

## 2.4 Kết luận chương

Trong chương này chúng ta đã được biết đến hợp đồng thông minh với những nét phác thảo cơ bản bao gồm khái niệm, mô hình hoạt động, mô hình triển khai. Hợp đồng thông minh có thể nhận hoặc thực hiện các giao dịch từ bất kỳ địa chỉ nào (giao dịch có thể bị từ chối hoặc yêu cầu các đối số đặc biệt để hoạt động) và đó có thể hoạt động như một thỏa thuận bất biến. Mục đích của các hợp đồng thông minh là tự động thực hiện như một "giao thức giao dịch được vi tính hóa thực hiện các điều khoản của hợp đồng" và được đặt ra bởi nhà mật mã học Nick Szabo. Mục đích chính của hợp đồng thông minh là kết hợp giữa thông tin được đưa vào và kiến trúc hệ thống sao cho việc vi phạm chúng là tốn kém hoặc không thể.

Ethereum là một nền tảng điện toán phân tán sử dụng blockchain để lưu trữ không chỉ trạng thái của tài khoản người dùng, mà còn có mã chương trình và trạng thái liên quan của nó. Nó cho phép việc thực thi phân tán mã tùy ý và cung cấp một nền tảng phù hợp cho thiết bị phát triển hợp đồng thông minh, đặc biệt Ethereum được thiết kế phù hợp cho bất cứ ai viết hợp đồng thông minh và các ứng dụng phi tập trung. Giống như một số ngôn ngữ kịch bản có thể được biên dịch thành mã byte và thực thi trên Máy ảo Ethereum (EVM).

# CHƯƠNG 3. ỨNG DỤNG HỢP ĐỒNG THÔNG MINH TRONG QUẢN LÝ THUÊ NHÀ.

Nội dung chương này chúng tôi trình bày một ứng dụng đơn giản của hợp đồng thông minh triển khai trong Ethereum: ứng dụng hợp đồng thông minh trong quản lý thuê nhà.

## 3.1. Mô hình quản lý thuê nhà

Mô hình quản lý thuê nhà ở đây được giả định như một chung cư mini hoặc ký túc xá tự nguyện của sinh viên. Mô hình này dành cho các ông chủ muốn kinh doanh về nhà ở (theo dạng cho thuê) và khách hàng là những người khá bận rộn như đang đi học hoặc thời gian đầu đi làm sau khi ra trường. Tòa nhà cho thuê được thiết kế với không gian riêng dành cho từng cá nhân và khu vực dành chung cho cộng đồng cư dân thuê nhà (sảnh chung, phòng khách, phòng bếp, phòng tập gym, …). Giả sử có N người thuê mỗi người một phòng, có D phòng/khu vực dùng chung và mỗi phòng dùng chung phải ở trạng thái sạch sẽ trong R ngày. Tổng quát, chúng ta có thể phát biểu là có N người và D nhiệm vụ cho mỗi chu kỳ R ngày.

Chủ sở hữu không muốn giải quyết khiếu nại và xung đột giữa cư dân liên quan đến chất lượng sạch sẽ của các phòng/khu vực dùng chung. Hơn nữa, chủ sở hữu không muốn thêm nhiệm vụ giám sát trạng thái của các khu vực dùng chung. Thay vào đó, chủ sở hữu có thể xây dựng hợp đồng, hợp thức hóa hợp đồng thành hợp đồng thông minh bằng ngôn ngữ Solidity triển khai nó lên Ethereum. Chủ sở hữu sẽ định kỳ gửi một thông báo đến hợp đồng thông minh như lời nhắc chu kỳ mới. Nếu sự kiện đặc biệt xảy ra, chẳng hạn như có cư dân mới được đăng ký, chủ sở hữu sẽ thực hiện các hành động bổ sung.

## 3.2. Hợp đồng

Một người mới đăng ký ở sẽ gửi khoản tiền B cho chủ sở hữu căn hộ. Chủ sở hữu không thể ăn cắp tiền gửi. Tuy nhiên, tiền gửi có thể được khóa và mở khóa bởi chủ sở hữu. Cư dân chỉ có thể truy cập tiền gửi đang mở khóa.

Phân công nhiệm vụ được thay đổi trên mỗi chu kỳ - mỗi người sẽ có nhiệm vụ khác nhau ở vòng tiếp theo. Phân công sẽ thực hiện xoay vòng đối với các cư dân đăng ký ổn định ở đây. Những người mới có thể được lưu trú và trả phòng trong tương lai nên các nghĩa vụ có thể được thêm vào hoặc xóa đi Nếu cần thiết, chủ sở hữu có thể cài đặt lại trạng thái mặc định.

Nếu một số cư dân không hài lòng với sự sạch sẽ của phòng sử dụng chung, anh ta hoặc cô ta có thể khiếu nại một lần cho một vòng. Một khiếu nại có giá trị chi phí theo quy định. Giá trị có thể được thay đổi bởi chủ sở hữu cho vòng tiếp theo. Khi vòng hiện tại kết thúc, tất cả các nhiệm vụ được kiểm tra. Nếu có một nhiệm vụ mà ít nhất 50% cư dân đã khiếu nại thì chi phí tích lũy của tất cả các khiếu nại chuyển nhượng sẽ được trừ vào số dư tiền gửi của cư dân chịu trách nhiệm về nhiệm vụ. Nếu có một số khiếu nại không đủ số lượng (dưới 50%) thì số dư tích lũy được hạch toán vào tài khoản riêng của chủ sở hữu.

## 3.3 Cài đặt thử nghiệm.

Mô hình hợp đồng phân tích ở mục 3.2 được triển khai trong Solidity với các cấu trúc cơ bản sau:

\*) Cấu trúc chủ hộ và chủ hợp đồng:

A screenshot of a cell phone

Description automatically generated

Hình 3.1. Cấu trúc chủ hộ và tham số.

Trong đoạn mã Hình 3.1 chủ sở hữu được quản lý với hai trường là địa chỉ và số dư. Trường địa chỉ để thực thi các giao dịch trong hợp đồng thông minh và trường số dư là số tiền của chủ sở hữu để thực hiện các giao dịch. Cấu trúc tham số dùng để khởi tạo tiền gửi của các bên liên quan khi tham gia thực hiện vòng (chu kỳ) trong tòa nhà.

\*) Cấu trúc cư dân và các phàn nàn:

A screenshot of a cell phone

Description automatically generated

Hình 3.2. Cấu trúc người thuê nhà và nhận xét.

Mỗi cư dân cư trú tại nhà cho thuê phải đóng một khoản tiền vào để thực hiện nghĩa vụ của hợp đồng thông minh (Hình 3.2). Số tiền này không bị rút bởi chủ sở hữu hay người thuê nhà mà được phân chia thực hiện bởi hợp đồng thông minh. Cấu trúc phàn nàn bao gồm số dư và số lượng phàn nàn từ các cư dân dùng để phân xử việc thực thi nhiệm vụ.

\*) Cấu trúc tham số và chu kỳ:

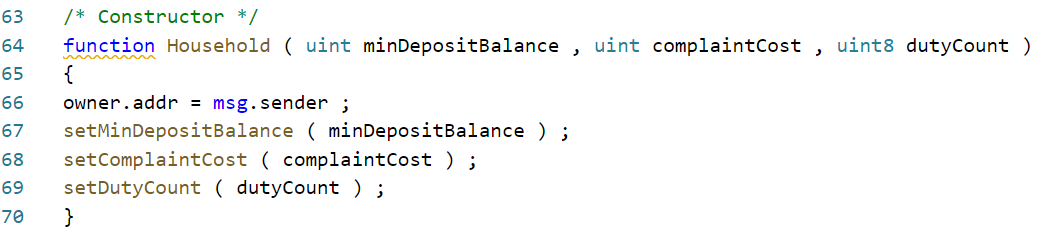
A screenshot of a cell phone

Description automatically generated

Hình 3.3. Cấu trúc chu kỳ và tham số.

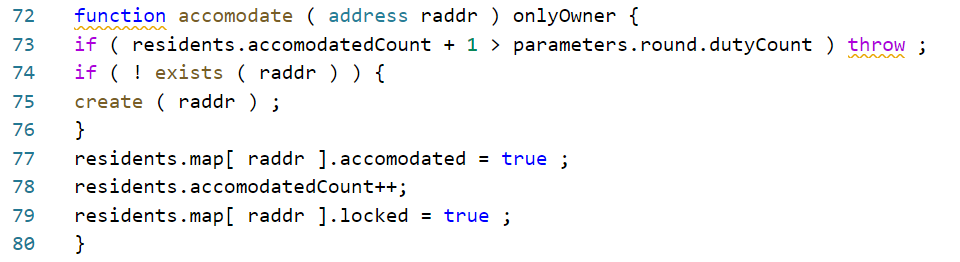
Trong hình 3.3, cấu trúc tham số vòng bao gồm giá trị phàn nàn và số lượng nhiệm vụ của vòng đó. Trong mỗi vòng sẽ ánh xạ nhiệm vụ đến các cư dân, nhiệm vụ đến phàn nàn và cư dân đến phàn nàn.

Hàm khởi tạo của hợp đồng thông minh sẽ nhận giá trị khởi tạo từ thông báo được gửi từ chủ sở hữu gồm lượng tiền gửi tối thiểu, giá của phàn nàn và số lượng nhiệm vụ, như đoạn mã trong hình 3.4.



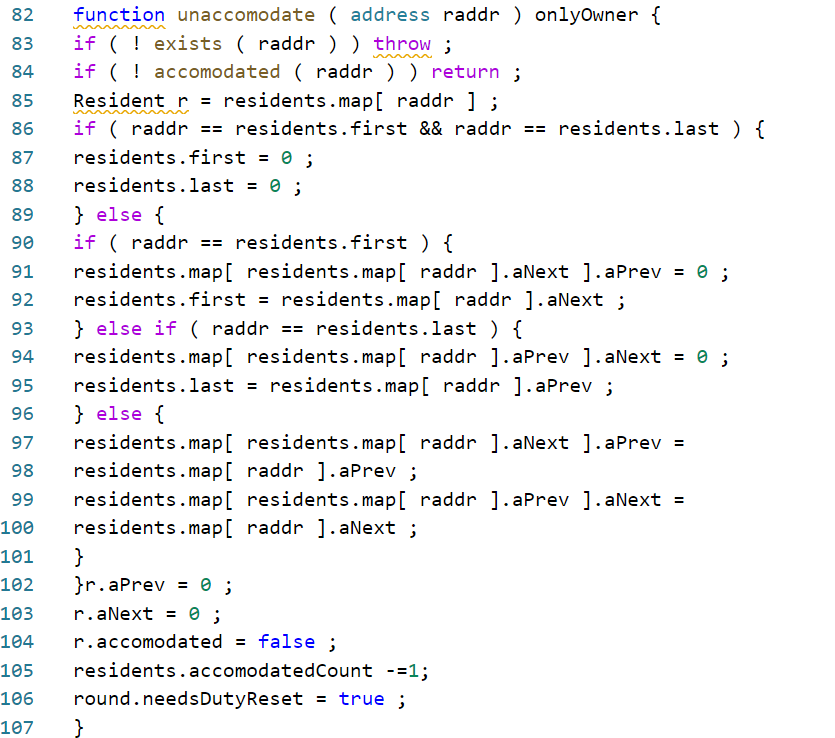
Hình 3.4. Hàm khởi tạo của hợp đồng thông minh.

Đối với mỗi khách thuê mới sẽ được chủ sở hữu chấp nhận cho thuê bởi hàm như trong hình 3.5.



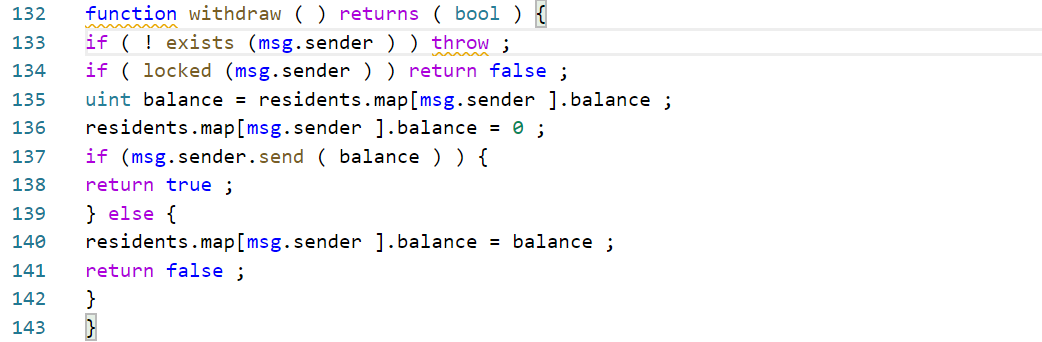
Hình 3.5. Hàm kích hoạt cư dân mới.

Trong trường hợp khách trả phòng ở và chuyển đi thì chủ sở hữu dùng hàm giải quyết như trong hình 3.6.



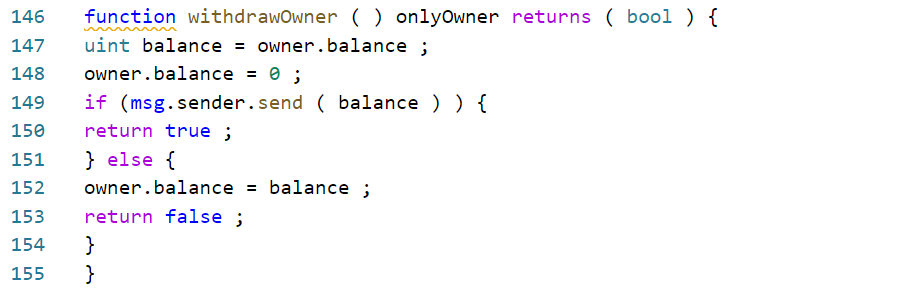
Hình 3.6. Hàm đưa khách hàng ra khỏi danh sách thuê nhà.

Trong trường hợp khách thuê chịu trách nhiệm về một nhiệm vụ nào đó bị hơn 50% khách thuê phàn nàn thì số tiền sẽ được tự động trừ trong tài khoản của người đó như trong hình 3.7.



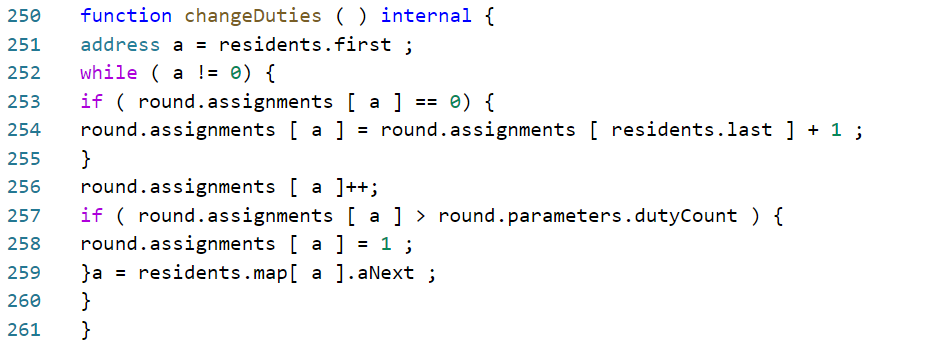
Hình 3.7. Hàm trừ tiền vào số dư tài khoản khách thuê.

Ngược lại nếu số lượng phàn nàn nhỏ hơn 50% số khách thuê nhà thì số tiền sẽ được trừ từ số dư tài khoản của chủ sở hữu, như trong hình 3.8.



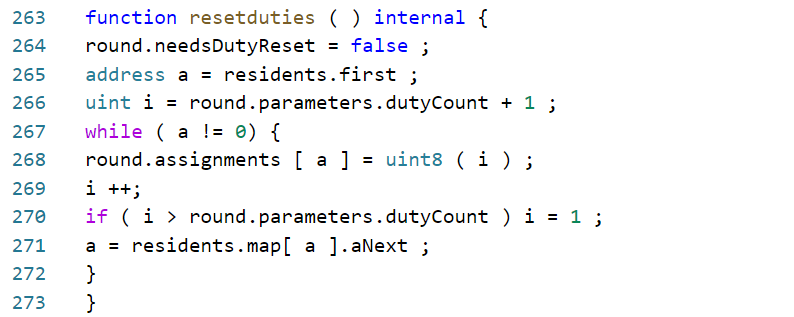
Hình 3.8. Hàm trừ tiền từ số dư tài khoản của chủ sở hữu.

Việc thay đổi nhiệm vụ cho các khách thuê được thực hiện bởi hàm như trong hình 3.9.

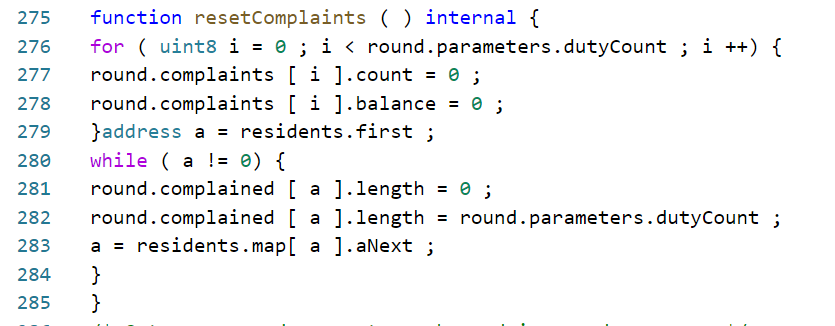


Hình 3.9. Hàm thay đổi nhiệm vụ cho khách thuê.

Kết thúc mỗi vòng thì các nhiệm vụ và phàn nàn sẽ được thiết lập lại như trong hình 3.10 và 3.11.



Hình 3.10. Hàm thiết lập lại nhiệm vụ cho khách thuê.



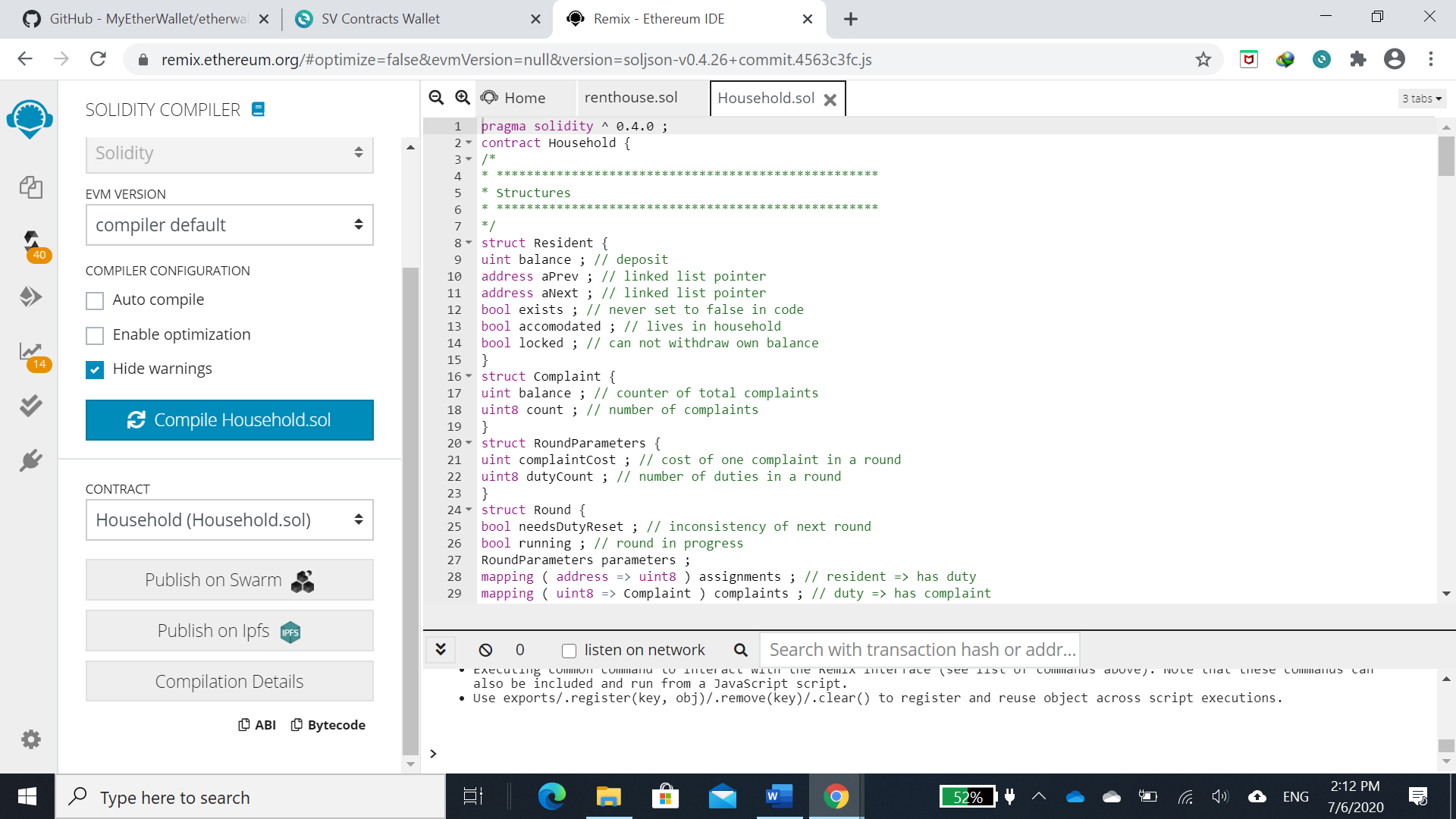
Hình 3.11. Hàm thiết lập lại phàn nàn cho mỗi vòng.

Hợp đồng thông minh được triển khai từ hai tài khoản khởi tạo bao gồm:

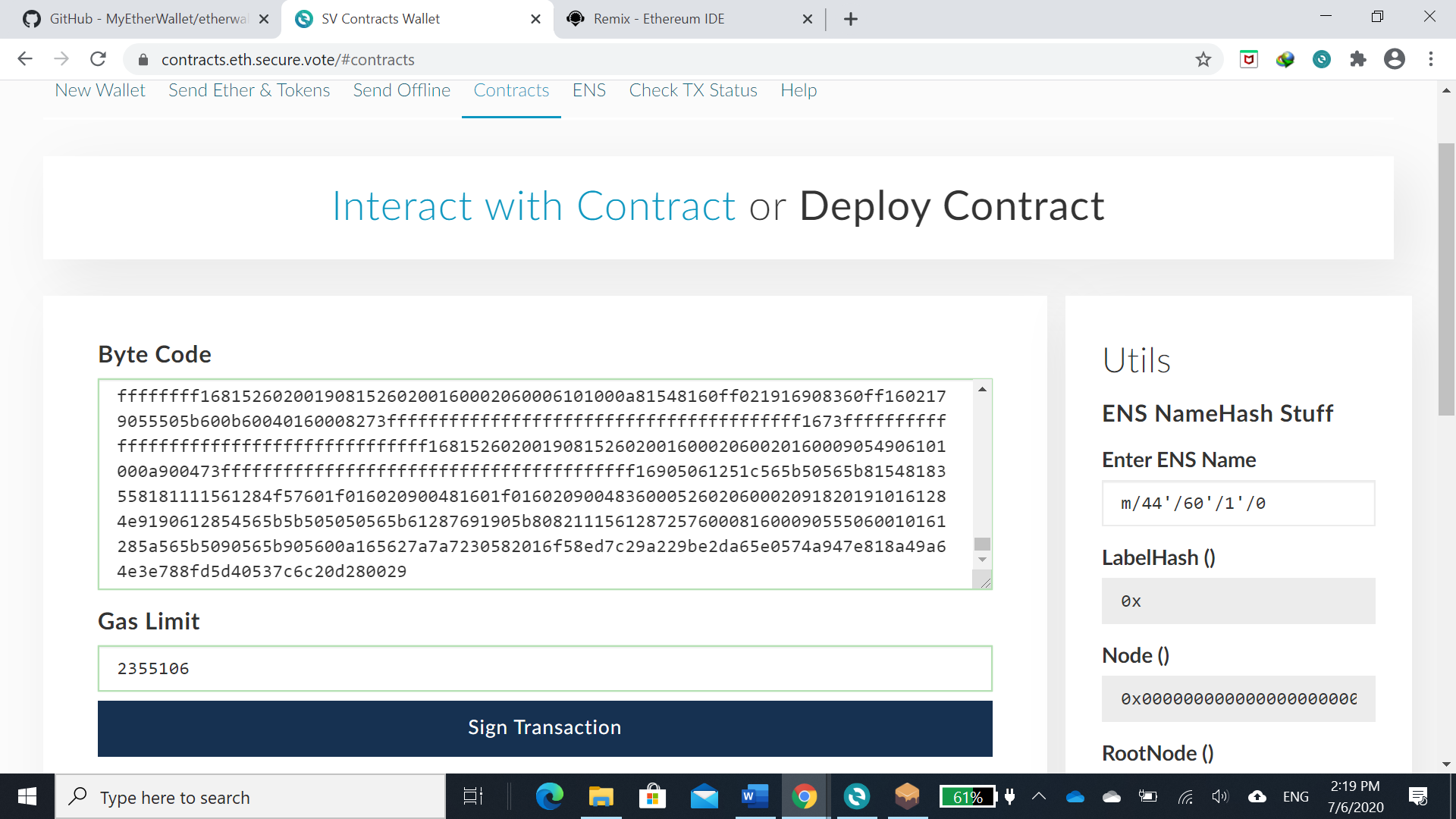
- 0x8e4D863D07Aa969aa997B56EF8ee0535E31C550F

- 0x79BA2e023905485D572e46d935387D01476e228F

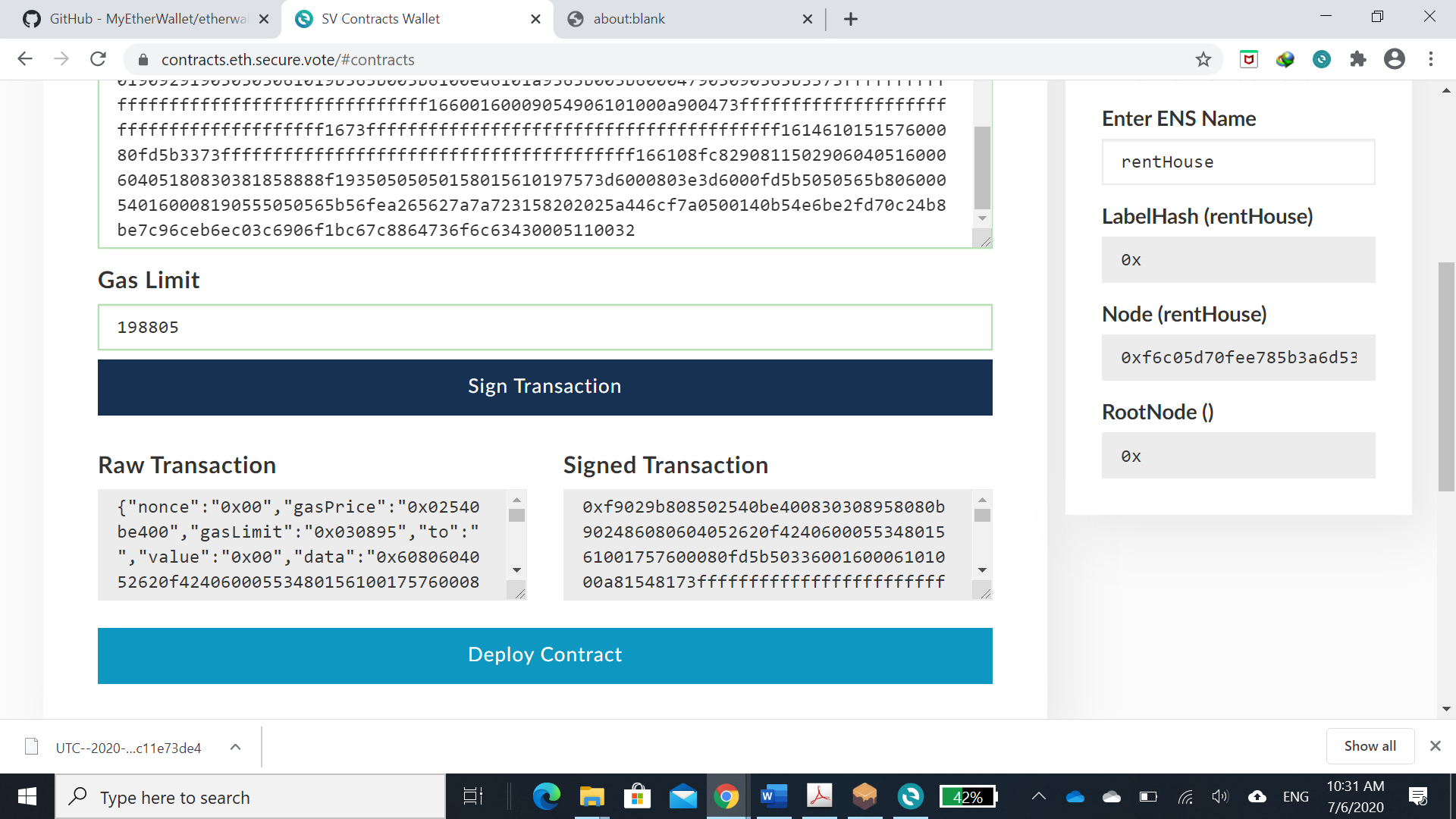
Quá trình triển khai trên remix.ethereum.org với trình biên dịch solidity như trong hình vẽ 3.12- 3.17.



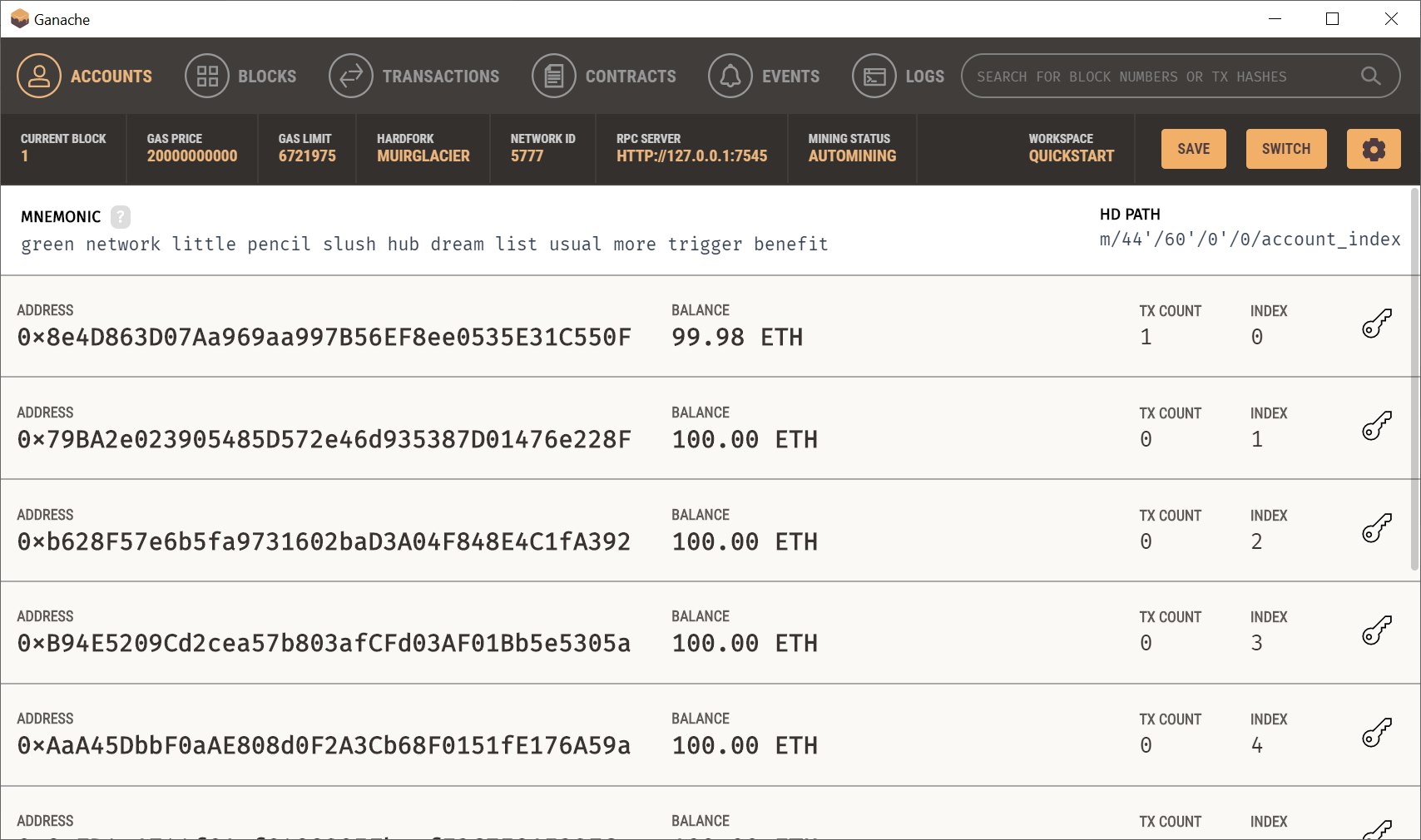
Hình 3.12. Biên dịch hợp đồng.



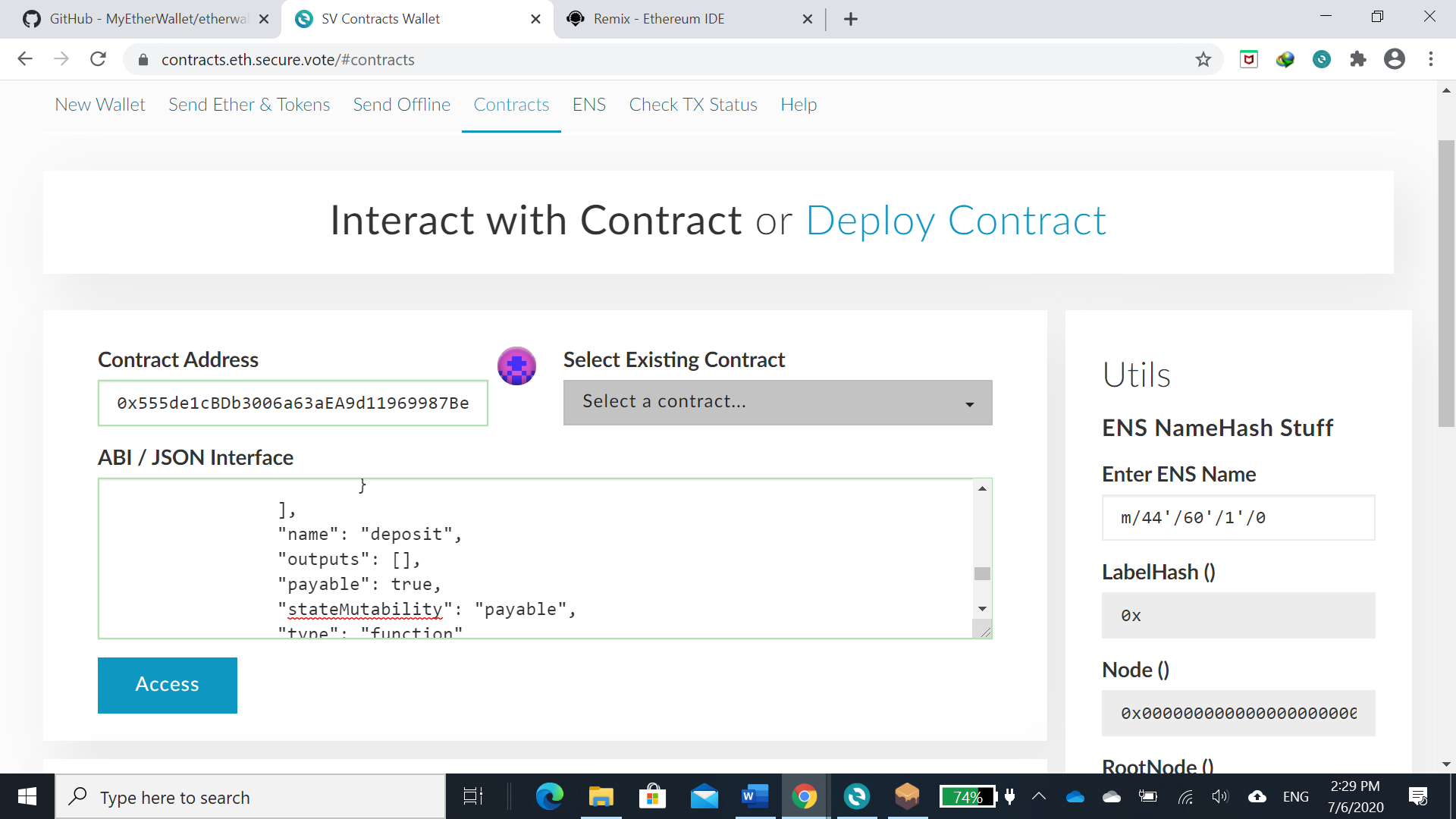
Hình 3.13. Ký xác thực để triển khai hợp đồng.



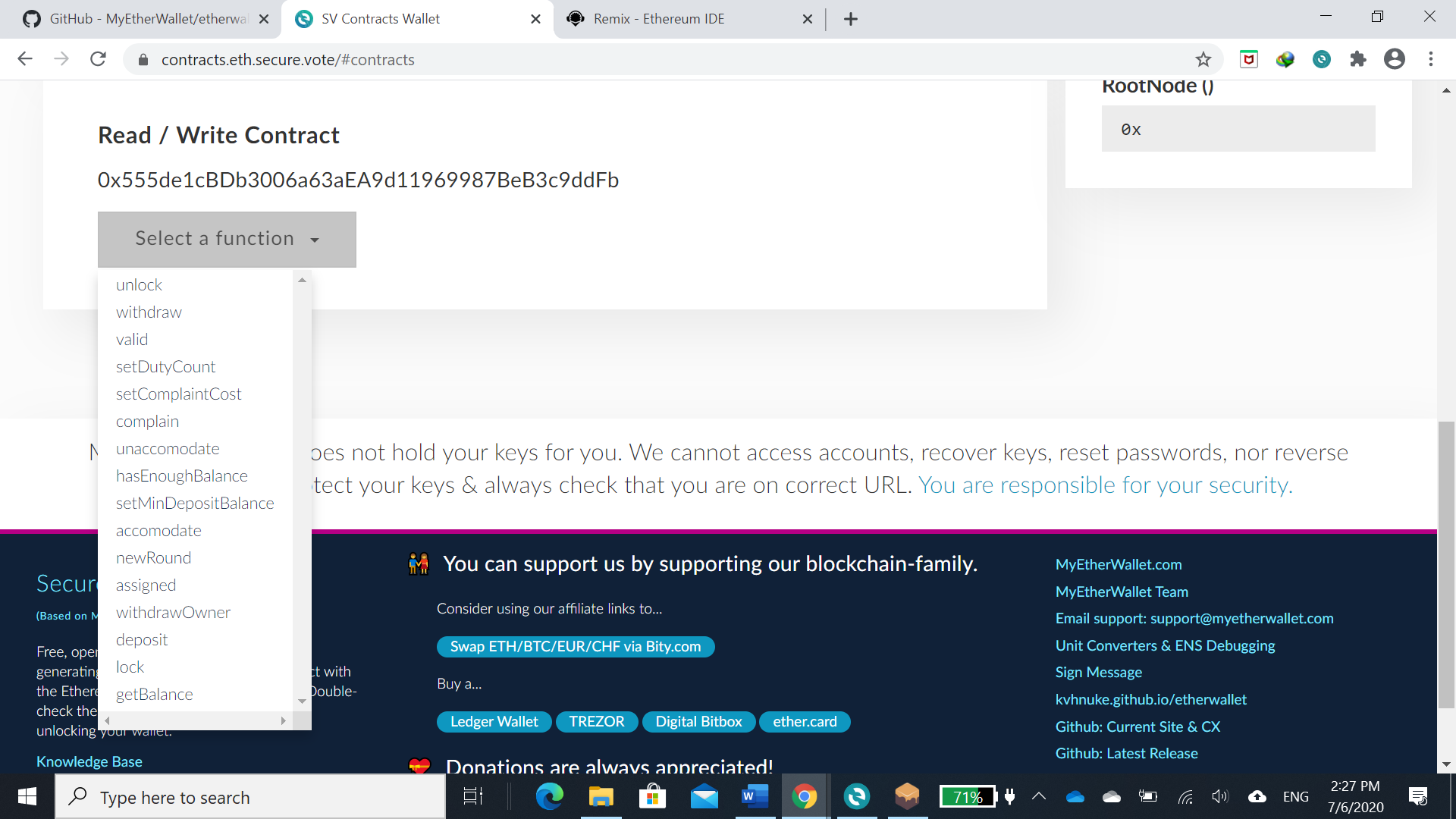
Hình 3.14. Triển khai hợp đồng.



Hình 3.15. Kết quả triển khai hợp đồng thể hiện trong Ganache.



Hình 3.16. Tương tác với hợp đồng.



Hình 3.17. Các hàm cơ bản của hợp đồng thông minh.

## 3.4 Kết luận chương.

Nội dung chương này đã thực hiện triển khai hợp đồng thông minh đơn giản, có thể xem như là một CaseStudy của chương 1 và 2. Trong công nghệ phần mềm, để thiết kế và xây dựng phần mềm, rất khó để xác định chính xác các yêu cầu chức năng và tạo ra phần mềm tương ứng. Trong thực tế, một hợp đồng được thiết lập các yêu cầu chức năng và hợp đồng thông minh là việc thực hiện tương ứng.

Một hợp đồng không rõ ràng có thể được giải thích khác nhau bởi một hoặc nhiều người. Một giải thích hoặc yêu cầu vô lý có thể được bỏ qua bằng trực giác, giải thích thuyết phục có thể được lựa chọn bởi những người có thẩm quyền hoặc theo quy trình bỏ phiếu. Ví dụ: hợp đồng quản lý thuê nhà có nội dung sau:

Tuy nhiên, tiền gửi tiền gửi có thể bị khóa và mở khóa bởi chủ sở hữu. Cư dân chỉ có thể truy cập tiền gửi mở khóa.

Có ít nhất hai cách giải thích. Điều đầu tiên là mỗi cư dân có thể truy cập vào từng khoản tiền gửi được mở khóa của mỗi cư dân. Giải thích thứ hai là mỗi cư dân chỉ có thể truy cập tiền gửi riêng nếu tiền gửi được mở khóa. Tuy nhiên, cái đầu tiên là vô lý và sẽ bị bỏ qua bằng trực giác.

Nếu một tình huống vô lý được xác định là một phần của hợp đồng thông minh hoặc tình huống vô lý xảy ra như một trạng thái của hợp đồng, hợp đồng thông minh xác định ý nghĩa chính xác và những hành động sửa chữa có thể được thực hiện.

# KẾT LUẬN

Blockchain đã trở thành một chủ đề “hot” thu hút sự quan tâm của dư luận xã hội, các tổ chức và các nhà nghiên cứu trong những năm gần đây. Ứng dụng của công nghệ blockchain, đặc biệt là ứng dụng hợp đồng thông minh đã giải quyết được những khó khăn, vướng mắc trong một số lĩnh vực của xã hội. Trong tương lai gần với xu thế chung của sự phát triển xã hội mỗi chúng ta sẽ phải tương tác với các hệ thống có ứng dụng blockchain và ứng dụng hợp đồng thông minh vào cuộc sống, do đó tác giả đã chọn nội dung luận văn nghiên cứu bao gồm:

- Công nghệ blockchain.

- Hợp đồng thông minh hay thế hệ thứ hai của blockchain.

- Ethereum và ứng dụng hợp đồng thông minh vào các lĩnh vực kinh doanh buôn bán, cho thuê… cụ thể trường hợp quản lý thuê nhà là một minh họa.

Trong khuôn khổ nội dung của một luận văn cao học ngành Công nghệ thông tin, tác giả nỗ lực để đạt được những kết quả có tính ứng dụng cao. Tuy nhiên do thời gian có hạn tác giả mong muốn nhận được sự hỗ trợ từ các thầy/cô và bạn cùng lớp để luận văn đạt được chất lượng cao.

# TÀI LIỆU THAM KHẢO

**Tài liệu Tiếng Việt**

1. Nguyễn Đình Thông, *Blockchain và ứng dụng thực tế của nó,* Tạp chí Bitcoint, 02/2018.
2. Forbes Magazine, *30 ứng dụng thiết thực của công nghệ blockchain trong đời sống.* Forbes VietNam , 05/2018.

**Tài liệu Tiếng Anh**

1. Satoshi Nakamoto (Retrieved 2016).*Bitcoin: A Peer-to-Peer Electronic Cash System.*http://bitcoin.org/bitcoin.pdf.
2. Vitalik Buterin (Retrieved 2016). *White Paper.URL: https://github.com/ethereum/wiki/wiki/White-Paper*.
3. Zheng, Xie, Dai, Wang (2017).*“Blockchain Challenges and Opportunities: A Survey”***.** International Journal of Web and Grid Services, Inc Press.
4. Christidis, Devetsikiotis (2016). *“Blockchains and Smart Contracts for the Internet of Things”*. IEEE VOLUME 4.
5. Greenspan (2016). *“MultiChain Private Blockchain—White Paper”*, URL:

http://www.multichain.com/white-paper.

1. Beck, Stenum Czepluch, Lollike, Malone (2016). *“Blockchain – The gateway to trust-free cryptographic transactions”*, 24th European Conference on Information Systems (ECIS), Istanbul, Turkey.
2. Weber, Xu, Riveret, Governatori, Ponomarev, Mendling (2016). *“Untrusted Business Process Monitoring and Execution Using Blockchain”*, Business Process Management the series Lecture Notes in Computer Science, Vol. 9850.
3. Schauermann, Tschorsch (2016). *“Bitcoin and beyond – A technical survey on decentralized digital currencies”*. IEEE Communications Surveys & Tutorials 18.
4. McConaghy, Marques, Müller, De Jonghe, McConaghy, McMullen, Henderson, Bellemare, Granzotto (2017). *“BigchainDB: A Scalable Blockchain Database”*. URL: <https://www.bigchaindb.com/whitepaper/> bigchaindb-whitepaper.pdf.
5. Microsoft (2017). “*The Coco Framework: Technical Overview”*. URL: https://github.com/Azure/coco-framework/blob/master/docs/Coco% 20Framework%20whitepaper.pdf
6. Encyclopaedia Britannica (2016). *“Protocol”*, URL:

https://global. britannica.com/technology/protocol-computer-science.

1. Swan (2015). *Blockchain: Blueprint for a new economy*, O'Reilly Media, Inc.".
2. Al-Kuwari, Davenport, Bradford (2010). *“Cryptographic hash functions: recent design trends and security notions”*, 6th China International Conference on Information Security and Cryptology. Science Press of China, pp. 133-150.
3. Herrera-Joancomartí, Pérez-Solá (2016). *“Privacy in Bitcoin Transactions: New Challenges From Blockchain Scalability Solutions”*, Modeling Decisions for Artificial Intelligence the series Lecture Notes in Computer Science, Vol. 9880, pp. 26-44.
4. Bitcoin Glossary (2017). *Hard-Fork, Hard-Forking Change*, URL: https://bitcoin.org/en/glossary/hard-fork.
5. Oraclize (2017). *White Paper.* URL: http://docs.oraclize.it/#overview.
6. Consensys (2017). *“A Visit to the Oracle”*. URL: https://media.consensys.net/a-visit-to-the-oracle-de9097d38b2f.
7. TreasuryToday (2017), *The future of trade finance?* URL*:* http://treasurytoday.com/2016/11/the-future-of-trade-finance-ttti.
8. Astri (2017). *White paper on distributed ledger technology*. URL: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical infrastructure/ Whitepaper\_On\_Distributed\_Ledger\_ Technology.pdf.
9. EBA (2016). *Applying cryptotechnologies to trade finance,* Information paper EBA Working Group on Electronic Alternative Payments. URL: https://www.abe-eba.eu/downloads/knowledge-and-research/EBA\_May2016\_eAPWG\_Applying\_cryptotechnologies\_ to\_Trade\_Finance.pdf.
10. McKinsey Global Institute, McKinsey & Company (2017). URL: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies.
11. Jeff Colemen. (2016), *Where is the private key for a contract stored?* URL: http://ethereum.stackexchange.com/a/1993.
12. Jimkberry (2016). *What is the ethereum transaction data structure*? url:
13. http://ethereum.stackexchange.com/a/2097.
14. Ethereum community. *Account Types, Gas, and Transactions*. url:

http://ethdocs.org/en/latest/contracts-and-transactions/

account - types - gas - and - transactions . html.

1. Ethereum. *Solidity in Depth*. url: http://solidity.readthedocs.

io/en/latest/solidity-in-depth.html.

1. Phil Daian (2016). *Analysis of theDAOexploit*.

url: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit

1. Ethereum Foundation. *Decentralized Autonomous Organization*.

url: https://www.ethereum.org/dao.

1. Szabo (1994). *Smart contracts*. URL: http://virtualschool. edu/mon/Economics/ SmartContracts.html
2. Szabo (1997). Formalizing and securing relationships on public networks. URL: http://ojphi.org/ojs/index. php/fm/article/view/
3. Griggs (2015). URL: http://iang.org/papers/intersection\_ ricardian\_smart.html
4. Vasek, Moore (2015). *There’s no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams*, International conference on financial cryptography and data security (pp. 44–61).

1. Hội thảo quốc tế: Thời điểm thú vị cho ứng dụng Blockchain tại Việt Nam, ngày 7-8/3/2018, TP HCM, Việt Nam. [↑](#footnote-ref-1)