**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**BÁO CÁO BÀI TẬP LỚN**

**Môn học: Mật mã học nâng cao**

**ĐỀ TÀI:**

**ỨNG DỤNG BLOCKCHAIN**

**TRONG SMART CONTRACT**

**Giảng viên : TS. Đỗ Xuân Chợ**

**Nhóm môn học : Nhóm 02**

**Nhóm bài tập : Nhóm 04**

**Các thành viên : Nguyễn Tuấn Thành - B19DCAT179**

**Phạm Ngọc Hiếu - B19DCAT071**

**Nguyễn Hải Long - B19DCAT115**

**Nguyễn Văn Khải - B19DCAT103**

**Hà Nội, 10/2022**

**MỞ ĐẦU**

Xu hướng Blockchain là một trong những chủ đề được quan tâm nhất trong lĩnh vực công nghệ và hứa hẹn nhiều thay đổi trong các ngành nghề, lĩnh vực. Về cơ bản Blockchain là một biến thể phân tán và mã hoá của cơ sở dữ lệu có thể giải quyết các vấn đề khác nhau lên quan tới bảo mật dữ liệu trực tuyển. Trong khi nhiều người chỉ biết đến Blockchain với những cái tên như đồng tiền điện tử Bitcoin, tuy nhiên nó còn có nhiều công dụng khác như: quản lỹ chuỗi cung ứng, bảo vệ quyền sở hữu tài sản, danh tính, thực hiện các hợp đồng thông minh kỹ thuật số…

Smart Contract (hay Hợp đồng thông minh) là các chương trình chạy trên blockchain. Hợp đồng thông minh cũng giống như một hợp đồng kỹ thuật số bị bắt buộc thực hiện bởi một bộ quy tắc cụ thể. Các quy tắc này do bộ mã máy tính xác định trước mà tất cả các nút (node) trong mạng đều phải sao chép và thực thi các quy tắc đó.

Nắm bắt được xu hướng đang đi lên này, nhóm 04 chúng em xin được chọn chủ đề về ứng dụng Blockchain trong Smart Contract là “ **Lottery Smart Contract**” làm đề tài của nhóm.

**MỤC LỤC**

**[MỞ ĐẦU 1](#_Toc18564)**

**[CHƯƠNG 1: BLOCKCHAIN 4](#_Toc18592)**

**[1.1. Định nghĩa Blockchain 4](#_Toc18384)**

**[1.2. Công dụng Blockchain 4](#_Toc20775)**

**[1.3. Đặc điểm Blockchain 5](#_Toc20506)**

**[1.4. Các thành phần chính 5](#_Toc13132)**

**[1.5. Cách thức hoạt động 6](#_Toc5833)**

**[1.6. Ứng dụng Blockchain 7](#_Toc32136)**

**[CHƯƠNG 2: SMART CONTRACT 10](#_Toc11354)**

**[2.1. Smart Contract 10](#_Toc29352)**

***[2.1.1. Lịch sử hình thành](#_Toc29598)* [10](#_Toc29598)**

***[2.1.2. Khái niệm và mục đích](#_Toc20619)* [10](#_Toc20619)**

***[2.1.3. Yêu cầu để tạo ra Smart Contract](#_Toc18439)* [11](#_Toc18439)**

***[2.1.4. Hoạt động của Smart Contract](#_Toc28095)* [12](#_Toc28095)**

***[2.1.5. Lợi ích của Smart Contract](#_Toc29503)* [13](#_Toc29503)**

***[2.1.6. Ưu-nhược điểm của Smart Contract](#_Toc27958)* [13](#_Toc27958)**

***[2.1.7. Ứng dụng của Smart Contract](#_Toc21664)* [14](#_Toc21664)**

**[2.2. Mạng Ethereum 15](#_Toc99)**

***[2.2.1. Khái niệm về mạng Ethereum](#_Toc29000)* [15](#_Toc29000)**

***[2.2.2. Lịch sử hình thành](#_Toc13182)* [15](#_Toc13182)**

***[2.2.3. Cách hoạt động](#_Toc6616)* [16](#_Toc6616)**

***[2.2.4. Các bộ quy tắc triển khai mạng lưới token của Ethereum](#_Toc23755)* [17](#_Toc23755)**

***[2.2.5. Ứng dụng của Ethereum](#_Toc31518)* [17](#_Toc31518)**

**[CHƯƠNG 3: LOTTERY SMART CONTRACT 19](#_Toc20235)**

**[3.1. Mô tả đề tài 19](#_Toc22854)**

**[3.2. Ưu điểm so với truyền thống 19](#_Toc12417)**

**[3.3. Sơ đồ hoạt động 19](#_Toc28987)**

**[3.4. Phát triển đề tài 19](#_Toc9020)**

**[KẾT LUẬN 21](#_Toc6750)**

**[TÀI LIỆU THAM KHẢO 22](#_Toc4220)**

**DANH MỤC CÁC HÌNH ẢNH**

|  |  |  |
| --- | --- | --- |
| **TT Hình** | **Nội dung** | **Trang** |
| Hình 2.1. | So sánh giữa hợp đồng truyền thống và hợp đồng thông minh | 11 |
| Hình 2.2. | Cách hoạt động của smart contract | 13 |
| Hình 2.3. | Cách hoạt động của Ethereum | 16 |
| Hình 3.1. | Sơ đồ hoạt động hệ thống | 19 |
| Hình 3.2. | Hàm getRandomNumber() | 19 |
| Hình 3.3. | Hàm payWinner() | 20 |

**CHƯƠNG 1: BLOCKCHAIN**

* 1. **Định nghĩa Blockchain**

Công nghệ Blockchain là một cơ chế cơ sở dữ liệu tiên tiến cho phép chia sẻ thông tin minh bạch trong một mạng lưới kinh doanh. Cơ sở dữ liệu chuỗi khối lưu trữ dữ liệu trong các khối được liên kết với nhau trong một chuỗi. Dữ liệu có sự nhất quán theo trình tự thời gian vì chúng ta không thể xóa hoặc sửa đổi chuỗi mà không có sự đồng thuận từ mạng lưới.

Do đó, ta có thể sử dụng công nghệ chuỗi khối để tạo một sổ cái không thể chỉnh sửa hay biến đổi để theo dõi các đơn đặt hàng, khoản thanh toán, tài khoản và những giao dịch khác. Hệ thống có những cơ chế tích hợp để ngăn chặn các mục nhập giao dịch trái phép và tạo ra sự nhất quán trong chế độ xem chung của các giao dịch này.

* 1. **Công dụng Blockchain**

Blockchain được dùng để lưu trữ thông tin trong các khối thông tin được liên kết với nhau. Nó được quản lý bởi tất cả mọi người tham gia hệ thống.

Thay vì một bên thứ 3 riêng lẻ như nhà nước hay ngân hàng trung ương. Đồng thời cho phép truyền tải dữ liệu một cách an toàn bằng một hệ thống mã hóa phức tạp, và được mở rộng theo thời gian.

Hơn nữa, công nghệ này được tạo ra để chống lại sự thay đổi dữ liệu trong hệ thống. Nó cũng có một tính năng rất đặc biệt đó là việc truyền tải dữ liệu không đòi hỏi một trung gian nào để xác nhận thông tin.

Bởi vì trong hệ thống Blockchain tồn tại rất nhiều nút hoạt động độc lập có khả năng xác thực các thông tin trong hệ thống mà không đòi hỏi “dấu hiệu của niềm tin”.

Thông tin khi được nhập vào trong chuỗi khối blockchain thì sẽ không thể thay đổi và chỉ được bổ sung thêm khi có sự chấp thuận của tất cả mọi người trong hệ thống.

Đây là một hệ thống đảm bảo sự an toàn rất cao cho các dữ liệu trước các nguy cơ bị đánh cắp.

Nhất là các dữ liệu nhạy cảm như tài khoản ngân hàng online, tài khoản thẻ thanh toán… Ngay cả khi nếu một phần của hệ thống blockchain bị tấn công, thì các phần khác không bị ảnh hưởng và vẫn tiếp tục hoạt động để bảo vệ thông tin.

* 1. **Đặc điểm Blockchain**

Công nghệ Blockchain có các đặc điểm chính sau:

* *Phi tập trung:*

Tính phi tập trung trong Blockchain là chỉ việc chuyển quyền kiểm soát và ra quyết định từ một thực thể tập trung (cá nhân, tổ chức hoặc nhóm) sang một mạng lưới phân tán. Các mạng lưới chuỗi khối phi tập trung sử dụng tính minh bạch để giảm nhu cầu phải có sự tin tưởng giữa những người tham gia. Các mạng lưới này cũng ngăn cản những người tham gia sử dụng quyền hạn hoặc quyền kiểm soát lên lẫn nhau theo những cách làm suy yếu chức năng của mạng lưới.

* *Bất biến:*

Bất biến có nghĩa là một cái gì đó không thể thay đổi hay biến đổi được. Không người tham gia nào có thể làm giả giao dịch sau khi ai đó đã ghi lại giao dịch này vào sổ cái được chia sẻ. Nếu bản ghi giao dịch có lỗi, người chơi phải thêm giao dịch mới để bù trừ cho lỗi và cả hai giao dịch đều được hiển thị trong mạng lưới.

* *Đồng thuận:*

Một hệ thống chuỗi khối thiết lập các quy tắc về sự đồng thuận của người tham gia cho phép ghi lại các giao dịch. Người chơi chỉ có thể ghi lại các giao dịch mới khi đa số người tham gia mạng lưới đồng thuận.

* 1. **Các thành phần chính**

Kiến trúc Blockchain có các thành phần chính sau:

* *Sổ cái phân tán:*

Sổ cái phân tán là cơ sở dữ liệu dùng chung trong mạng lưới lưu trữ các giao dịch, chẳng hạn như một tệp dùng chung mà mọi người trong nhóm có thể chỉnh sửa. Trong hầu hết các trình chỉnh sửa văn bản dùng chung, bất kỳ ai có quyền chỉnh sửa đều có thể xóa toàn bộ tệp. Tuy nhiên, công nghệ sổ cái phân tán có các quy tắc nghiêm ngặt về người có thể chỉnh sửa và cách chỉnh sửa. Chúng ta không thể xóa các mục nhập sau khi chúng đã được ghi lại.

* *Hợp đồng thông minh:*

Các công ty sử dụng hợp đồng thông minh để tự quản lý các hợp đồng kinh doanh mà không cần bên thứ ba hỗ trợ. Đây là các chương trình được lưu trữ trên hệ thống tự động chạy khi đáp ứng các điều kiện đã định sẵn. Chúng chạy kiểm tra điều kiện “nếu-thì” để các giao dịch có thể được hoàn thành một cách đáng tin cậy. Ví dụ: một công ty kho vận có thể thiết lập một hợp đồng thông minh tự động thanh toán khi hàng hóa đến cảng.

* *Mật mã hóa khóa công khai:*

Mật mã hóa khóa công khai là một tính năng bảo mật để xác định những người tham gia duy nhất trong mạng lưới Blockchain. Cơ chế này tạo ra hai bộ mã khóa cho các thành viên trong mạng lưới. Một mã khóa là mã khóa công khai cho mọi người trong mạng lưới dùng chung. Mã khóa còn lại là mã khóa riêng tư duy nhất của mỗi thành viên. Mã khóa riêng tư và công khai hoạt động cùng nhau để mở khóa dữ liệu trong sổ cái.

* *Ví dụ:* John và Jill là hai thành viên trong mạng lưới. John ghi lại một giao dịch được mã hóa bằng mã khóa riêng tư của anh ấy. Jill có thể giải mã giao dịch này bằng mã khóa công khai của cô ấy. Bằng cách này, Jill tin chắc rằng John đã thực hiện giao dịch. Mã khóa công khai của Jill sẽ không hoạt động nếu mã khóa riêng tư của John bị làm giả.
  1. **Cách thức hoạt động**

***Bước 1:*** *Ghi lại giao dịch*

Một giao dịch Blockchain cho thấy sự lưu động của các tài sản vật lý hoặc kỹ thuật số từ bên này đến bên khác trong mạng lưới Blockchain. Giao dịch được ghi lại dưới dạng một khối dữ liệu và có thể bao gồm các thông tin chi tiết như sau:

* Giao dịch gồm những ai tham gia?
* Điều gì đã xảy ra trong quá trình giao dịch?
* Giao dịch xảy ra khi nào?
* Giao dịch xảy ra ở đâu?
* Giao dịch xảy ra vì lý do gì?
* Phần tài sản được trao đổi là bao nhiêu?
* Có bao nhiêu điều kiện tiên quyết đã được đáp ứng trong quá trình giao dịch?

***Bước 2:*** *Đạt được sự đồng thuận*

Hầu hết những người tham gia trên mạng lưới Blockchain phân tán phải đồng ý rằng giao dịch được ghi lại là hợp lệ. Tùy thuộc vào loại mạng lưới, các quy tắc thỏa thuận có thể khác nhau nhưng thường được thiết lập khi bắt đầu mạng lưới.

***Bước 3:*** *Liên kết các khối*

Khi những người tham gia đã đạt được sự đồng thuận, các giao dịch trên chuỗi khối sẽ được viết vào khối, tương đương với trang giấy trong một cuốn sổ cái. Cùng với các giao dịch, một hàm băm mật mã cũng được thêm vào khối mới. Hàm băm đóng vai trò như một chuỗi liên kết các khối với nhau. Nếu nội dung của khối bị cố ý hoặc vô ý sửa đổi, giá trị băm sẽ thay đổi, mang đến một cách thức để phát hiện dữ liệu bị làm giả.

Do đó, các khối và chuỗi được liên kết an toàn và chúng ta không thể chỉnh sửa chúng. Mỗi khối được thêm lại tăng cường cho quá trình xác minh khối trước đó và do đó tăng cường cho toàn bộ chuỗi khối. Điều này giống như xếp chồng các khối gỗ để tạo thành một tòa tháp. Chúng ta chỉ có thể xếp khối lên trên, và nếu bạn rút một khối ở giữa tháp thì cả tháp sẽ đổ sụp.

***Bước 4:*** *Chia sẻ sổ cái*

Hệ thống phân phối bản sao mới nhất của sổ cái trung tâm cho toàn bộ người tham gia.

* 1. **Ứng dụng Blockchain**

Blockchain là một công nghệ mới nổi đang được các ngành khác nhau áp dụng theo cách thức sáng tạo. Dưới đây là mô tả một số trường hợp sử dụng trong các ngành khác nhau:

* *Năng lượng*

Các công ty năng lượng sử dụng công nghệ chuỗi khối để tạo ra các nền tảng giao dịch năng lượng ngang hàng và hợp lý hóa việc tiếp cận năng lượng tái tạo. Chẳng hạn, hãy xem xét những trường hợp sử dụng sau:

* Các công ty năng lượng dựa trên chuỗi khối đã tạo ra một nền tảng giao dịch để các cá nhân mua bán điện. Chủ nhà có các tấm pin mặt trời sử dụng nền tảng này để bán năng lượng mặt trời dư thừa của họ cho những người hàng xóm. Quá trình này phần lớn là được tự động hóa: đồng hồ đo thông minh tạo ra các giao dịch và chuỗi khối ghi lại những giao dịch này.
* Với các sáng kiến huy động vốn cộng đồng dựa trên chuỗi khối, người dùng có thể tài trợ và sở hữu các tấm pin mặt trời trong những cộng đồng không có khả năng tiếp cận nguồn năng lượng. Các nhà tài trợ cũng có thể nhận được tiền thuê từ các cộng đồng này sau khi đã xây dựng các tấm pin mặt trời.
* *Tài chính*

Các hệ thống tài chính truyền thống, như ngân hàng và sàn giao dịch chứng khoán, sử dụng các dịch vụ chuỗi khối để quản lý các khoản thanh toán trực tuyến, tài khoản và giao dịch thị trường.

Ví dụ: Singapore Exchange Limited, một tổng công ty về đầu tư cung cấp các dịch vụ giao dịch tài chính trên khắp châu Á, sử dụng công nghệ chuỗi khối để xây dựng một tài khoản thanh toán liên ngân hàng hiệu quả hơn. Bằng cách áp dụng chuỗi khối, họ đã giải quyết được nhiều thách thức, bao gồm xử lý hàng loạt và đối soát thủ công hàng nghìn giao dịch tài chính.

* *Truyền thông và giải trí*

Các công ty trong lĩnh vực truyền thông và giải trí sử dụng hệ thống chuỗi khối để quản lý dữ liệu bản quyền. Xác minh bản quyền là rất quan trọng để các nghệ sĩ nhận được thù lao công bằng. Cần nhiều giao dịch để ghi lại việc bán hoặc chuyển giao nội dung bản quyền. Sony Music Entertainment Japan sử dụng các dịch vụ chuỗi khối để quản lý quyền kỹ thuật số hiệu quả hơn. Họ đã sử dụng thành công chiến lược chuỗi khối để cải thiện năng suất và giảm chi phí xử lý bản quyền.

* *Bán lẻ*

Các công ty bán lẻ sử dụng chuỗi khối để theo dõi sự lưu động của hàng hóa giữa nhà cung cấp và người mua.

Ví dụ: công ty bán lẻ Amazon đã nộp bằng sáng chế cho một hệ thống công nghệ sổ cái phân tán sẽ sử dụng công nghệ chuỗi khối để xác minh rằng tất cả hàng hóa được bán trên nền tảng đều đáng tin cậy. Người bán trên Amazon có thể lập bản đồ chuỗi cung ứng toàn cầu của họ bằng cách cho phép những người tham gia như nhà sản xuất, người giao hàng, nhà phân phối, người dùng cuối và người dùng thứ cấp thêm sự kiện vào sổ cái sau khi đăng ký với cơ quan cấp chứng nhận.

**CHƯƠNG 2: SMART CONTRACT**

* 1. **Smart Contract**
     1. ***Lịch sử hình thành***

Smart Contract (hợp đồng thông minh) được hình thành ý tưởng lần đầu tiên bởi Nick Szabo - sinh viên tốt nghiệp Đại học Washington vào năm 1994.

Szabo giải thích rằng ông sử dụng từ "thông minh" vì các hợp đồng này có thể thực hiện các bước được lập trình sẵn mà các hợp đồng giấy không thể thực hiện được.

Ông cũng cảnh báo rằng việc sử dụng thuật ngữ "Smart Contract (hợp đồng thông minh)" không ngụ ý việc sử dụng trí tuệ nhân tạo, các hợp đồng này không thể phân tích và xác định các yêu cầu chủ quan hơn của một hợp đồng.

* + 1. ***Khái niệm và mục đích***

Smart Contract là các chương trình chạy trên blockchain. Hợp đồng thông minh cũng giống như một hợp đồng kỹ thuật số bị bắt buộc thực hiện bởi một bộ quy tắc cụ thể. Các quy tắc này do bộ mã máy tính xác định trước mà tất cả các nút (node) trong mạng đều phải sao chép và thực thi các quy tắc đó.

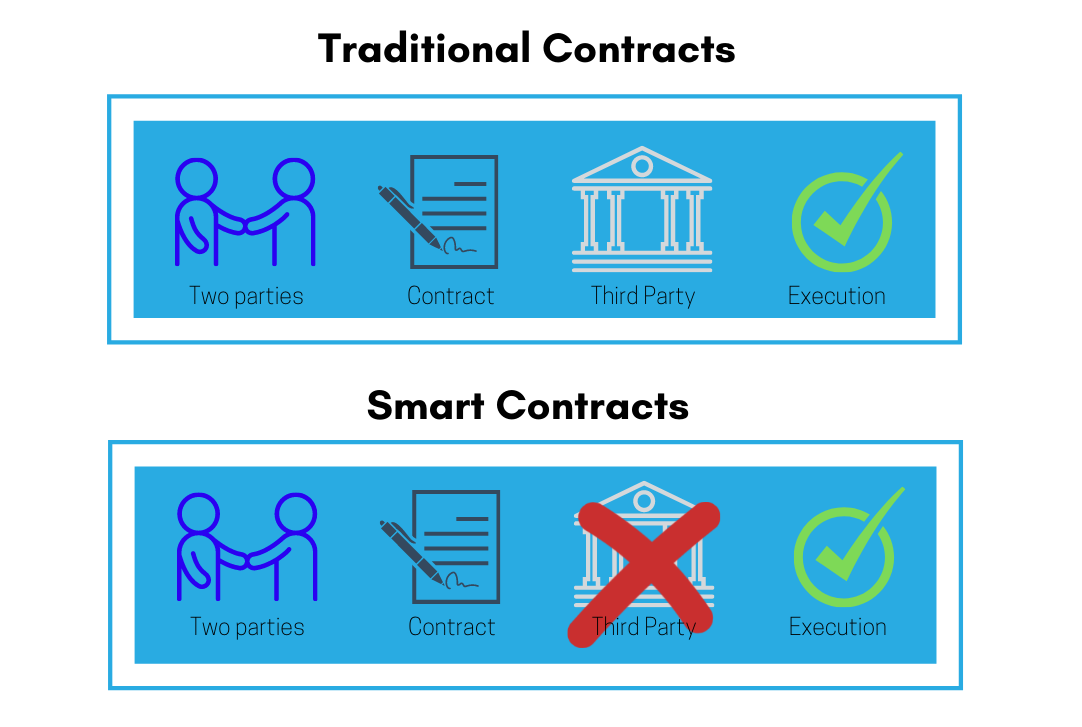
Về bản chất, Smart Contract chỉ là một đoạn mã chạy trên một hệ thống phân tán, cho phép tạo ra các giao thức Permissionless (tức là không cần trao quyền). Điều đó có nghĩa là:

* Hai bên trong hợp đồng có thể đưa ra các cam kết thông qua blockchain mà không cần phải biết về danh tính hay tin tưởng lẫn nhau.
* Họ có thể đảm bảo rằng nếu các điều kiện của hợp đồng không được thỏa mãn, hợp đồng sẽ không được thực thi.

Ngoài ra, việc sử dụng hợp đồng thông minh loại bỏ nhu cầu đối với các bên trung gian, giúp giảm đáng kể chi phí hoạt động

Nói chung, mục đích chính của smart contract là đơn giản hóa các giao dịch kinh doanh giữa các bên bằng cách loại bỏ các bên trung gian liên quan đến các quy trình kinh doanh truyền thống. Các hợp đồng này nhằm mục đích giảm sự chậm trễ thanh toán, rủi ro có sai sót và sự phức tạp của một hợp đồng thông thường mà không ảnh hưởng đến tính xác thực và uy tín.

Lợi thế đặc biệt chính là cho phép thực hiện các giao dịch đáng tin cậy mà không cần trung gian.



**Hình 2.1. So sánh giữa hợp đồng truyền thống và hợp đồng thông minh**

* + 1. ***Yêu cầu để tạo ra Smart Contract***

Trong Smart Contract cần chứa các thông tin sau:

* Chủ thể của hợp đồng: Chúng ta cần xác định các chủ thể trong hợp đồng là ai. Những chủ thể này cần phải có định danh và được liệt kê đầy đủ trong smart contract.
* Chữ kí số của các bên liên quan: Để hợp đồng có tính hợp lệ và cho phép nó có thể can thiệp được vào các tài nguyên liên quan của các chủ thể thì bên trong hợp đồng cần chứa các chữ ký số xác nhận của các bên liên quan. Tất cả các bên tham gia vào Smart Contract đều phải đồng ý triển khai thỏa thuận bằng các khóa cá nhân (chữ kí điện tử) của họ.
* Các điều khoản hợp đồng: Các điều khoản trong Smart Contract quy định các hành động thực thi của nó. Các điều khoản được mô tả là một chuỗi các hoạt động. Và các bên tham gia hợp đồng đều phải ký chấp nhận nó.

Các đối tượng tác động của hợp đồng: Chẳng hạn như số tiền chuyển giữa các tài khoản, các tài sản được số hóa khác như nhà đất, bảo hiểm... Tùy từng ứng dụng sẽ có các đối tượng khác nhau.

Các thông tin này sẽ được cụ thể hóa trong hợp đồng và được biên dịch thành các mã thực thi sau đó gửi lên blockchain. Hợp đồng hợp lệ, có đầy đủ các thông tin sẽ được phê duyệt và đưa vào các khối. Hợp đồng sẽ được thực hiện khi có các hành vi kích hoạt (thực hiện qua các giao dịch) nhằm thay đổi trạng thái của blockchain. Khi hành vi kích hoạt diễn ra, các smart contract được cấp khả năng truy cập đến tài nguyên liệt kê trong hợp đồng để có thể tự động khóa hay mở khóa chúng và tạo ra các thay đổi trạng thái tương ứng lên các tài nguyên này trên blockchain. Sự thay đổi sẽ diễn ra tự động tại mọi nút của mạng lưới và hợp đồng được thực thi.

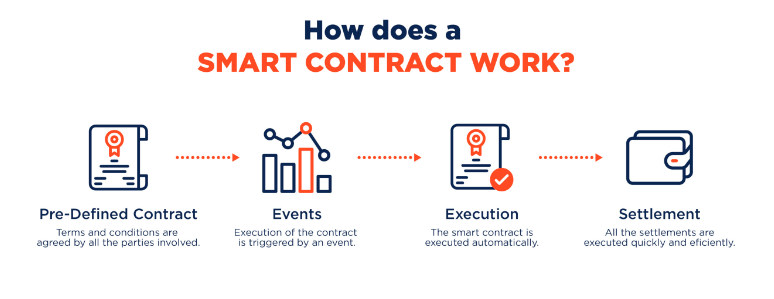
* + 1. ***Hoạt động của Smart Contract***

Hợp đồng thông minh có cơ chế hoạt động như một chương trình nhất định, thực thi yêu cầu, tác vụ cụ thể ứng với từng điều kiện riêng biệt trong một số trường hợp. Vì thế, câu lệnh trong hợp đồng thông minh thường sẽ được viết ở dạng “nếu…thì…”.

Mặc dù tên gọi là vậy, tuy nhiên trên thực tế, đây không phải là một hợp đồng pháp lý và cũng không “thông minh”. Đơn thuần chỉ là các đoạn mã chạy trên một hệ thống phân tán (blockchain) được lập trình sẵn.

Hợp đồng thông minh sẽ chịu sự kiểm soát của máy tính và EOA(externally owned account) là do người dùng kiểm soát (EOA là tài khoản người sở hữu, chứa 2 cặp khóa public và private key. Public key đc xem là đia chỉ ví để nhận tiền còn Private key để xem là mã để truy cập ví).

Hợp đồng thông minh được tiến hành thông qua các giao dịch blockchain khi và chỉ khi được kích hoạt bởi một EOA (hoặc các hợp đồng thông minh khác) yêu cầu. Dĩ nhiên, phía kích hoạt đầu tiên luôn là EOA (người dùng).



**Hình 2.2. Cách hoạt động của smart contract**

* + 1. ***Lợi ích của Smart Contract***
* *Tự động hóa*: Các quá trình thực hiện hợp đồng đều là cơ chế tự động hóa. Người dùng chính là người tạo hợp đồng, điều này sẽ xóa bỏ các lo lắng về việc phụ thuộc vào môi giới, luật sư hay bất kì bên thứ ba nào khác.
* *Không bị thất lạc*: Chính vì tất cả dữ liệu đều được mã hóa trên một cuốn sổ cái chung, nên việc thất lạc là điều rất khó. Điều này cũng sẽ thuận tiện hơn trong việc tìm kiếm hay xem lại, người dùng có thể nắm giữ và kiểm soát một cách hiệu quả.
* *An toàn*: Bạn sẽ hạn chế được sự tấn công của hacker khi được blockchain đảm bản an toàn cho tài liệu.
* *Tốc độ*: Nhờ vào việc sử dụng các ngôn ngữ lập trình, code phần mềm để tự động hóa các điều khoản, thế nên hợp đồng thông minh có thể tiết kiệm được rất nhiều thời gian cho những việc không cần thiết.
* *Tiết kiệm:* Hợp đồng thông minh cũng tiết kiệm cho bạn một khoản ngân sách lớn vì đã xóa bỏ các khâu trung gian.
* *Chính xác*: Vì đã lập trình trên máy móc, việc hạn chế các lỗi mắc phải như trên giấy tờ là điều dễ hiểu.
  + 1. ***Ưu-nhược điểm của Smart Contract***

1. *Ưu điểm*

* *Tự do*: không chịu sự quản lý của bất kỳ một cơ quan nào và không thông qua bên thứ ba.
* *Phân tán*: hợp đồng thông minh được sao chép và phân phối trong mạng lưới phi tập trung. Đây cũng là một tiện ích khi so với các hình thức tập trung.
* *Tất định*: hợp đồng thông minh chỉ thực hiện những lệnh đã được thiết lập khi thỏa điều kiện. Đồng thời, kết quả sẽ không phân biệt người thực hiện, đảm bảo tính công bằng.
* *Tự động*: cơ chế tự động hóa đa dạng các loại tác vụ. Nếu như không được kích hoạt, hợp đồng thông minh sẽ duy trì trạng thái “không hoạt động” và cũng sẽ không thực hiện bất kỳ hoạt động nào.
* *Không thể sửa đổi*: một khi đã triển khai, không ai có thể thay đổi hợp đồng thông minh. Điều này sẽ rất hữu ích trong việc chống giả mạo.
* *Không cần dựa trên sự tin cậy*: vì tất cả đều được công nghệ hóa, thế nên ngay cả khi hai bên chưa có niềm tin với nhau vẫn có thể sử dụng hợp đồng thông minh để hợp tác. Công nghệ blockchain sẽ bảo đảm tính chính xác của dữ liệu.
* *Minh bạch*: mặc dù bất kỳ ai cũng đều có thể xem được dựa trên nền tảng công khai, thế nhưng không một ai có thể thay đổi mã nguồn của hợp đồng thông minh.

1. *Nhược điểm*

* *Tính pháp lý*: vì Smart Contract hiện chưa được pháp luật quy định, bảo hộ nên nếu có xảy ra lỗi phát sinh, người dùng sẽ không được bảo vệ quyền lợi .
* *Chi phí triển khai*: dù tiết kiệm được các khâu trung gian nhưng để tạo hợp đồng thông minh cần một số tiền để chi trả cho hệ thống cơ sở hạ tầng, máy tính và các lập trình viên có kinh nghiệm.
* *Rủi ro từ internet*: về cơ bản, hợp đồng thông minh sẽ vô cùng an toàn nếu như không để lộ thông tin nhạy cảm hay không để hacker tìm ra lỗ hổng. Bất kỳ chuyện gì liên quan đến internet đều sẽ gặp rủi ro chung là nguy cơ có thể bị hack.
  + 1. ***Ứng dụng của Smart Contract***

Một số ứng dụng hợp đồng thông minh có thể có là:

* *Supply Chain*: Các công ty logistics cần có thể sử dụng hợp đồng thông minh để cập nhật các nhà cung cấp và hàng tồn kho của họ dựa trên việc giao hàng.
* *Bất động sản:* Một hợp đồng thông minh giúp các giao dịch bất động sản bớt căng thẳng hơn. Người mua và người bán ký một hợp đồng thông minh sẽ chuyển quyền sở hữu tài sản cho người mua khi nhận được số tiền đã thỏa thuận.
* *Bảo hiểm*: Các hợp đồng bảo hiểm có thể được thay thế một phần bằng các hợp đồng thông minh. Bảo hiểm y tế có thể được giải ngân thông qua một hợp đồng thông minh khi nhận được xác nhận (Bằng chứng Công việc) của một cuộc phẫu thuật hoặc thủ tục sức khỏe. Bản thân Bằng chứng công việc có thể dựa trên một hệ thống blockchain, trong đó hồ sơ của mọi bệnh nhân được duy trì và các cơ quan chức năng nhất định có chìa khóa để truy cập dữ liệu.
* *Nhận dạng cá nhân*: Mọi cá nhân đều có thể giữ các bằng chứng nhận dạng của họ ở dạng kỹ thuật số và cấp quyền truy cập cho các cơ quan chức năng nếu cần. Điều này sẽ làm giảm đáng kể sự rắc rối của việc quản lý danh tính và làm cho quá trình KYC đơn giản và an toàn hơn.
  1. **Mạng Ethereum**
     1. ***Khái niệm về mạng Ethereum***

Ethereum là một nền tảng công nghệ blockchain mã nguồn mở, công khai và phân quyền mà cho phép chạy các ứng dụng phi tập trung trên nền tảng của mình. Mạng lưới Blockchain của Ethereum là hệ thống siêu máy với hàng trăm nghìn thiết bị được kết nối trên toàn cầu hoạt động để duy trì trạng thái điện toán của nó.

Ý tưởng lớn đằng sau dự án này là bất kỳ ai cũng có thể sử dụng mạng lưới phi tập trung mới để tạo và vận hành những ứng dụng cùng với đó không cần phải xin phép hay đăng ký với một bên thứ ba nào khác vì về bản chất sẽ không còn bên trung gian nào khác.

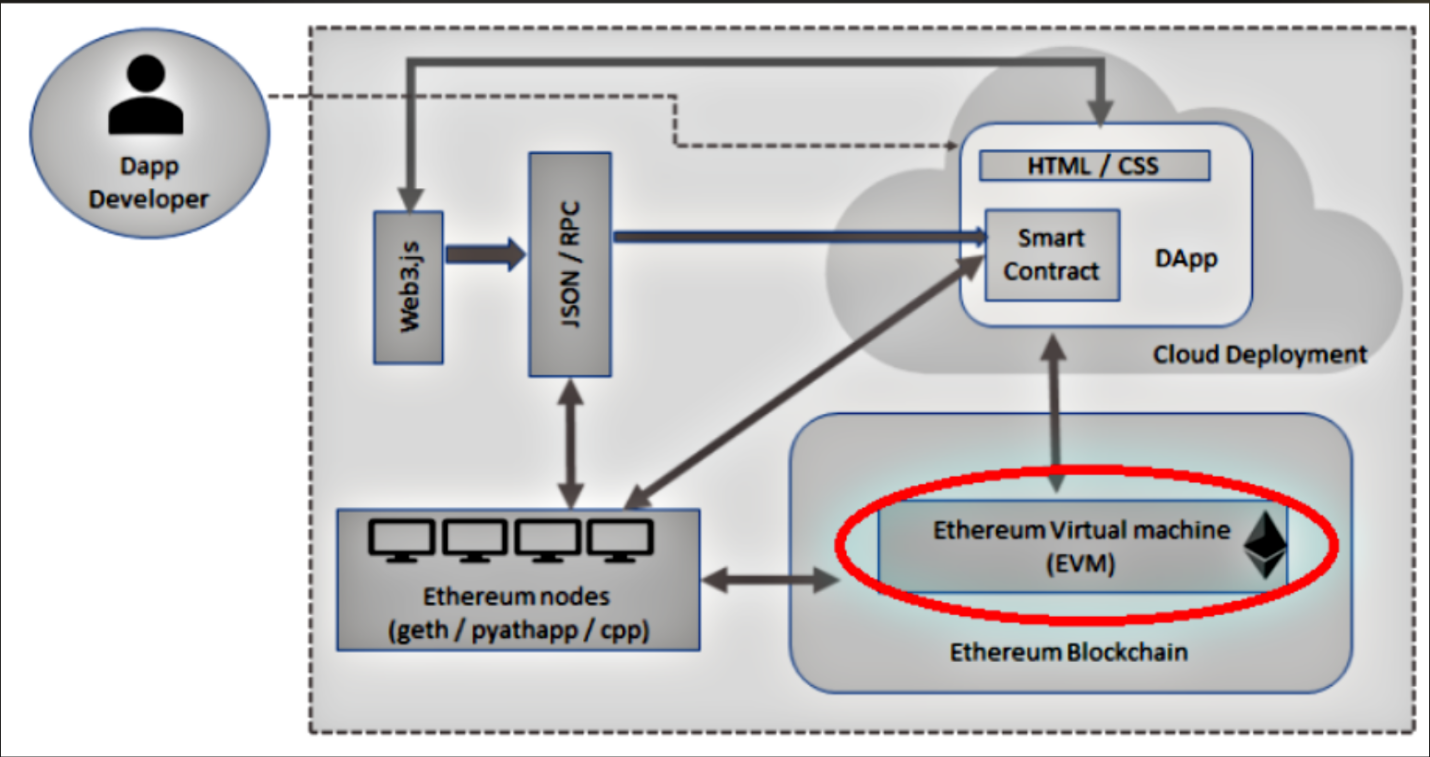
* + 1. ***Lịch sử hình thành***

Vitalik lần đầu chia sẻ bản Whitepaper phác thảo Ethereum vào tháng 11/2013 tuy nhiên đề xuất đã không được áp dụng nên ông tự mình nghiên cứu và hoàn thiện Whitepaper.

Mùa hè năm 2014, cộng sự của Vitalik là Gavin Wood công bố Yellowpaper cho Ethereum và Vitalik xác nhận Ethereum sẽ được phát triển tiếp tục bởi tổ chức Ethereum Foundation.

Tháng 6 năm 2015 một khối (block) đầu tiên của Ethereum được khai thác thành công, đánh dấu sự hình thành chính thức của Ethereum Blockchain.

* + 1. ***Cách hoạt động***



**Hình 2.3. Cách hoạt động của Ethereum**

Ethereum hoạt động bởi mạng lưới các máy tính gọi là Nodes, để tham gia vào mạng lưới này, các Nodes phải cài đặt phần mềm Ethereum Client. Sau khi cài đặt thì Nodes sẽ chạy chương trình ảo Ethereum Virtual Machine – EVM.

EVM chịu trách nhiệm thực hiện các hợp đồng thông minh, khi nhà phát triển muốn xây dựng DApps trên Ethereum, họ phải khai thác các hợp đồng thông qua ngôn ngữ lập trình Solidity.

Máy ảo EVM thực thi hoạt động như lệnh giao dịch, smart contract,… Mạng lưới cần đến một lượng phí gọi là Gas – phí thanh toán bằng đồng tiền kỹ thuật số gọi là Ether (ETH).

Khi giao dịch được thực thi, Miner Nodes sẽ xác nhận xem giao dịch đó có hợp lệ hay không. Ethereum sử dụng cơ chế Proof Of Word (PoW) để các Miner Nodes chứng minh công việc của họ đã hoàn thành và thông báo đến toàn mạng lưới. Sau đó các Miner Nodes khác sẽ xác nhận xem bằng chứng hợp lệ hay không.

Block mới được tạo ra bằng cách giải mã với thuật toán Ethash, sau đó xác nhận mạng lưới giao dịch khi PoW được thông qua, dữ liệu giao dịch ghi vào Blockchain của Ethereum và không thể thay đổi.

* + 1. ***Các bộ quy tắc triển khai mạng lưới token của Ethereum***

Ethereum Request For Comment là bộ các quy tắc (tiêu chuẩn) cần thiết để triển khai mạng lưới token trong Ethereum. Chúng đã được sửa đổi, nhận xét và chấp nhận bởi cộng đồng thông qua Ethereum Improvement Proposal. Dưới đây là 4 bộ quy tắc phổ biến:

* ERC20: Là bộ danh sách các quy tắc, quy định chung cho việc phát hành những token trên Ethereum giúp nhà phát triển có một chuẩn chung, triển khai hiệu quả các Fungible token.
* ERC721: Bộ tiêu chuẩn dành cho việc phát hành NFTs – Non-Fungible Token trên Ethereum. Theo đó, một NFT này không thể hoán đổi, thay thế bởi một NFT khác. Nhờ ERC721 mà nhà phát triển Ethereum đã xây dựng một hệ sinh thái mới Crypto Kitties – DApps nuôi mèo trên Ethereum.
* Tiêu chuẩn ERC777 – cải thiện các vấn đề của ERC20.
* ERC1155 – tiêu chuẩn dành cho các token gồm Non-Fungible và Fungible.
  + 1. ***Ứng dụng của Ethereum***
* *Ngân hàng - tài chính*:

Ethereum giúp phát hành chứng khoán kỹ thuật số trong khoảng thời gian ngắn hơn, với chi phí đơn vị thấp và mức độ tùy biến cao hơn. Vì vậy, các công cụ tài chính kỹ thuật số có thể được điều chỉnh theo nhu cầu của nhà đầu tư, mở rộng thị trường cho các nhà đầu tư, giảm chi phí cho các nhà phát hành và giảm rủi ro cho các đối tác.

* *Thương mại quốc tế và hàng hóa:*

Quy trình tài chính thương mại và trao đổi hàng hóa, đặc biệt là các giao dịch xuyên biên giới hiện yêu cầu rất nhiều thủ tục, giấy tờ hồ sơ kỹ thuật liên quan đến vận chuyển và các loại chứng nhận khác nhau. Hệ thống hiện hành nặng về hồ sơ giấy khiến các doanh nghiệp dễ bị lừa đảo, chịu nhiều rủi ro và phải đợi chờ thanh toán

* *Chuỗi cung ứng*:

Một cơ sở hạ tầng công nghệ thông tin ứng dụng công nghệ Blockchain sẽ hợp lý hóa quy trình công việc cho tất cả các bên, bất kể quy mô của mạng lưới kinh doanh. Ngoài ra, cơ sở hạ tầng dùng chung sẽ cung cấp cho kiểm toán viên tầm nhìn rõ hơn về các hoạt động của người tham gia cùng với chuỗi giá trị.

* *Bất động sản*:

Nền tảng Ethereum cung cấp một giải pháp thiết thực để tối ưu hóa các quy trình bất động sản hiện tại và loại bỏ các trung gian. Theo các nhà phân tích, một trong những điểm thú vị nhất Ethereum mang lại cho ngành bất động sản là token hóa. Tài sản kỹ thuật số có thể đại diện cho bất cứ tài sản gì, bao gồm cổ phần các tài sản trong thế giới thực như bất động sản, quỹ bất động sản, dòng doanh thu, quyền quản trị... Dựa trên khả năng token hóa tài sản thực, việc xử lý chứng khoán, quản lý trách nhiệm, xử lý tài liệu và kế toán chắc chắn sẽ thay đổi.

**CHƯƠNG 3: LOTTERY SMART CONTRACT**

* 1. **Mô tả đề tài**

Smart Contract Lottery được phát triển trên nền tảng Ethereum bằng ngôn ngữ Solidity. Lottery được xây dựng dựa trên trò chơi vòng quay may mắn. Luật chơi là các người chơi bỏ tiền vào hệ thống và hệ thống sẽ random chọn ra một người may mắn nhất được nhận tất cả số tiền trên.

* 1. **Ưu điểm so với truyền thống**

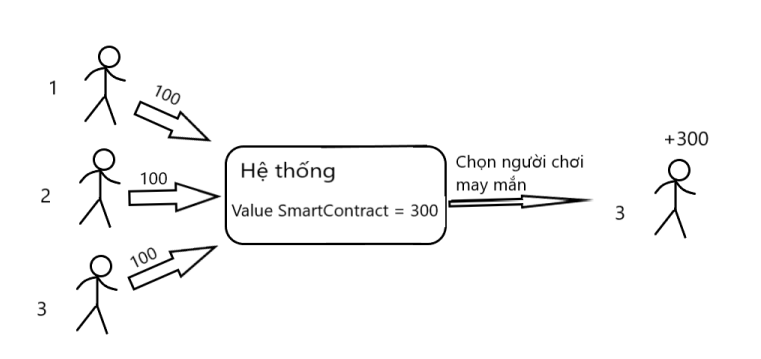
- Thuật toán chọn ra người may mắn được công khai.

- Giao dịch nhanh chóng và thuận tiện.

- Mọi thông tin giao dịch của người chơi đều được công khai minh bạch.

- Tiết kiệm được chi phí trung gian do không thông qua bên thứ 3.

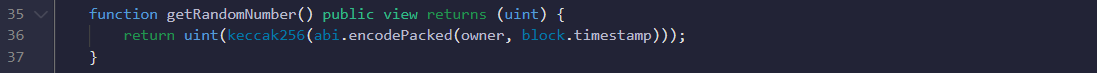
* 1. **Sơ đồ hoạt động**



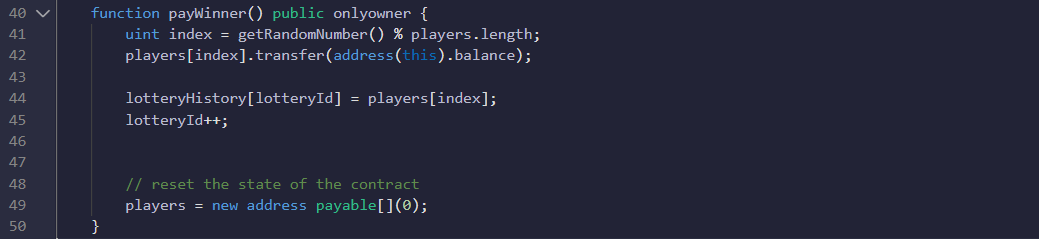
**Hình 3.1. Sơ đồ hoạt động hệ thống**

* 1. **Phát triển đề tài**

Dưới đây là các hàm chính được sử dụng trong Lottery Smart Contract



**Hình 3.2. Hàm getRandomNumber()**



**Hình 3.3. Hàm payWinner()**

Trong đó:

* *players:* mảng lưu địa chỉ người chơi.
* *index:* tạo ra từ chia dư của randomResult và số lượng người chơi.
* *players[index].transfer:* chuyển phí vào người thắng.

**KẾT LUẬN**

Trong bài báo cáo này, chúng em đã tìm hiểu về định nghĩa, cách hoạt động cũng như ứng dụng của Blockchain, Smart Contract và mạng Ethereum và triển khai đề tài Lottery ứng dụng dựa trên Smart Contract.

Do đề tài còn khá mới mẻ cũng như kiến thức và khả năng của nhóm chúng em còn nhiều hạn chế nên trong bài tập lớn này không tránh khỏi các sai sót. Nhóm em mong nhận được sự góp ý và điều chỉnh của thầy và các bạn để nội dung bài tập của nhóm em được hoàn thiện hơn. Nhóm em xin chân thành cảm ơn thầy!

**TÀI LIỆU THAM KHẢO**

1. History of Blockchain - Javapoint, 06/10/2022, từ <[https://www.javatpoint.com/](https://www.javatpoint.com/history-of-blockchain)

[history-of-blockchain](https://www.javatpoint.com/history-of-blockchain)>.

1. Smart Contract Trong Blockchain Và Cách Hoạt Động | Bybit Learn, 06/10/2022, từ <[https://learn.bybit.com/vi/blockchain/what-are-smart-contracts-in-blockchain](https://learn.bybit.com/vi/blockchain/what-are-smart-contracts-in-blockchain-how-do-they-work/)

[-how-do-they-work/](https://learn.bybit.com/vi/blockchain/what-are-smart-contracts-in-blockchain-how-do-they-work/)>

1. Ethereum Tutorial, 08/10/2022, từ <[https://www.tutorialspoint.com/ethereum/](https://www.tutorialspoint.com/ethereum/index.htm)

[index.htm](https://www.tutorialspoint.com/ethereum/index.htm)l>

1. PatrickAlphaC(2022), SmartContract Lottery, 06/10/2022, từ <[https://github.com/](https://github.com/PatrickAlphaC/smartcontract-lottery)

[PatrickAlphaC/smartcontract-lottery](https://github.com/PatrickAlphaC/smartcontract-lottery)>