**UNIVERSITY OF INFORMATION TECHNOLOGY**

**VIETNAM NATIONAL UNIVERSITY HCM CITY**

**HOẠCH ĐỊNH NGUỒN LỰC DOANH NGHIỆP**

**BÁO CÁO ĐỒ ÁN THỰC HÀNH BLOCKCHAIN**

**Lớp: IS336.M21.TMCL**

**Giáo viên hướng dẫn : Thầy Đỗ Duy Thanh**

**Sinh viên thực hiện :**

**TP. Hồ Chí Minh, ngày 08 tháng 07 năm 2022**

**🙟·🙝**

**LỜI CẢM ƠN**

Đầu tiên, nhóm xin gửi lời cảm ơn chân thành đến thầy Đỗ Duy Thanh (Giảng viên môn Hoạch định nguồn lực doanh nghiệp) đã giúp cho nhóm có những kiến thức cơ bản làm nền tảng để thực hiện đề tài này.

Thầy đã trực tiếp hướng dẫn tận tình, sửa chữa và đóng góp nhiều ý kiến quý báu giúp nhóm hoàn thành tốt báo cáo môn học của mình. Trong thời gian một học kỳ thực hiện đề tài, nhóm đã vận dụng những kiến thức nền tảng đã tích lũy đồng thời kết hợp với việc học hỏi và nghiên cứu những kiến thức mới. Từ đó, nhóm vận dụng tối đa những gì đã thu thập được để hoàn thành một báo cáo đồ án tốt nhất.

Tuy nhiên, trong quá trình thực hiện, nhóm không tránh khỏi những thiếu sót. Chính vì vậy, nhóm rất mong nhận được những sự góp ý từ phía thầy nhằm hoàn thiện những kiến thức mà nhóm đã học tập và là hành trang để nhóm thực hiện tiếp các đề tài khác trong tương lai.

Xin chân thành cảm ơn thầy!

**TP. Hồ Chí Minh, ngày 08/07/2022**

**Nhóm sinh viên thực hiện**

**MỤC LỤC**

[I. Blockchain căn bản 4](#_Toc108169512)

[1. Sự ra đời và phát triển của blockchain: 4](#_Toc108169513)

[1.1. Sự ra đời của blockchain 4](#_Toc108169514)

[1.2. Các phiên bản của blockchain 5](#_Toc108169515)

[2. Blockchain là gì? 6](#_Toc108169516)

[2.1. Định nghĩa blockchain 6](#_Toc108169517)

[2.2. Công nghệ tạo ra blockchain 6](#_Toc108169518)

[2.3. Phân loại blockchain 6](#_Toc108169519)

[2.4 Các đặc điểm của blockchain 7](#_Toc108169520)

[3. Các loại node trong blockchain 7](#_Toc108169521)

[3.1. Light Nodes 8](#_Toc108169522)

[3.2. Full and Super Nodes 9](#_Toc108169523)

[3.3. Mining Nodes 11](#_Toc108169524)

[4. Mempool 11](#_Toc108169525)

[4.1. Mempool là gì? 11](#_Toc108169526)

[4.2. Mối quan hệ giữa Mempool, Full Node và Miner Node trong mạng Bitcoin 12](#_Toc108169527)

[4.3. Tầm quan trọng và hạn chế của kiến trúc Mempool 12](#_Toc108169528)

[5. Cơ chế đồng thuận trong blockchain 13](#_Toc108169529)

[5.1. Proof of Work (PoW) – Minh chứng công việc 13](#_Toc108169530)

[5.2. Proof of Stake (PoS) – Minh chứng cổ phần 13](#_Toc108169531)

[6. Ví tiền mã hóa 14](#_Toc108169532)

[II. Tìm hiểu khái niệm Smart Contract: Smart contract là gì? 15](#_Toc108169533)

[1. Smart Contract khác gì với hợp đồng truyền thống? 15](#_Toc108169534)

[2. Smart contract hoạt động như nào? 16](#_Toc108169535)

[3. Chu trình thực thi Smart Contract? 18](#_Toc108169536)

[4. Ứng dụng của Smart Contract 21](#_Toc108169537)

[5. Ưu điểm và nhược điểm của Smart Contract: 26](#_Toc108169538)

[5.1 Ưu điểm 26](#_Toc108169539)

[5.2 Nhược điểm 27](#_Toc108169540)

[III. Ứng dụng Blockchain trong truy xuất nguồn gốc sữa 28](#_Toc108169541)

[1. Mô tả bài toán 28](#_Toc108169542)

[1.1 Thực trạng chuỗi cung ứng sữa truyền thống 28](#_Toc108169543)

[1.2 Các vấn đề trong truy xuất nguồn gốc sữa 29](#_Toc108169544)

[2. Mô hình truy xuất nguồn gốc dựa trên Blockchain: 29](#_Toc108169545)

[2.1 Triển khai mô hình truy xuất nguồn gốc sữa tươi Mộc Châu 29](#_Toc108169546)

[2.2 Quy trình sản xuất sữa Mộc Châu 30](#_Toc108169547)

[2.3 Xây dựng website truy xuất 32](#_Toc108169548)

[2.4 Ưu điểm 52](#_Toc108169549)

[2.5 Kết quả đạt được 52](#_Toc108169550)

[IV.Tham khảo: 53](#_Toc108169551)

# I. Blockchain căn bản

## Sự ra đời và phát triển của blockchain:

### Sự ra đời của blockchain

Blockchain lần đầu tiên được phát minh và thiết kế bới Satoshi Nakamoto vào năm 2008 và được hiện thực hóa vào năm sau đó như là một phần cốt lõi của Bitcoin, khi công nghệ blockchain đóng vai trò như là một cuốn sổ cái cho tất cả các giao dịch. Qua việc sử dụng mạng lưới ngang hàng và một hệ thống dữ liệu phân cấp, Bitcoin blockchain được quản lý tự động. Việc phát minh ra blockchain cho Bitcoin đã làm cho nó trở thành loại tiền tệ kỹ thuật số đầu tiên giải quyết được vấn đề double spending (chi tiêu gian lận khi 1 lượng tiền được dùng 2 lần). Công nghệ này của Bitcoin đã trở thành nguồn cảm hứng cho một loạt các ứng dụng khác.

Blockchain được đảm bảo nhờ cách thiết kế sử dụng hệ thống tính toán phân cấp với khả năng chịu lỗi byzantine cao. Nhờ thế nên Blockchain có thể đạt được sự đồng thuận phân cấp. Vì vậy Blockchain phù hợp để ghi lại những sự kiện, hồ sơ y tế, xử lý giao dịch, công chứng, danh tính và chứng minh nguồn gốc. Việc này có tiềm năng giúp xóa bỏ các hậu quả lớn khi dữ liệu bị thay đổi trong bối cảnh thương mại toàn cầu.

### Các phiên bản của blockchain

Diagram

Description automatically generated

Hiện nay, Blockchain có 4 phiên bản như sau:

* Công nghệ Blockchain 1.0: Cryptocurrency
  + Việc triển khai DLT (distributed ledger technology) đã dẫn đến ứng dụng đầu tiên và nó là: Cryptocurrency (tiền mã hóa). Điều này cho phép các giao dịch tài chính dựa trên công nghệ này. Nó sử dụng trong tiền tệ và thanh toán. Bitcoin là ví dụ nổi bật nhất trong phân khúc này.
* Công nghệ Blockchain 2.0: Smart Contract
  + Smart Contract (hợp đồng thông minh), các chương trình máy tính “sống” trong chuỗi blockchain. Chúng là các chương trình máy tính miễn phí thực thi tự động và kiểm tra các điều kiện được xác định trước đó như hỗ trợ, xác minh. Nó được sử dụng để thay thế cho các hợp đồng truyền thống.
* Công nghệ Blockchain 3.0: Dapps
  + Dapps là tên viết tắt của ứng dụng phi tập trung. Nó có code backend chạy trên mạng peer-to-peer. DApp có thể có code ví dụ về frontend Blockchain và giao diện người dùng được viết bằng bất kỳ ngôn ngữ nào có thể call đến phần backend của nó, giống như ứng dụng truyền thống.
* Công nghệ Blockchain 4.0: Blockchain For industry
  + Mục tiêu của Blockchain 4.0 là giải quyết toàn bộ vấn đề của ba thế hệ trước. Nó giải thích các chiến lược và phương pháp giúp công nghệ blockchain sẵn sàng đáp ứng nhu cầu kinh doanh. Các doanh nghiệp sẵn sàng áp dụng công nghệ blockchain, nhưng chúng ta cần một blockchain an toàn hơn và mạnh mẽ hơn.

## Blockchain là gì?

### Định nghĩa blockchain

Blockchain là một công nghệ cho phép truyền tải dữ liệu một cách an toàn dựa vào hệ thống mã hoá vô cùng phức tạp, tương tự cuốn sổ cái kế toán của một công ty, nơi mà tiền mặt được giám sát chặt chẽ. Trong trường hợp này Blockchain là một cuốn sổ cái kế toán hoạt động trong lĩnh vực kỹ thuật số. Blockchain sở hữu tính năng vô cùng đặc biệt đó là việc truyền tải dữ liệu không đòi hỏi một trung gian để xác nhận thông tin.

Hệ thống Blockchain tồn tại rất nhiều nút độc lập có khả năng xác thực thông tin mà không đòi hỏi “dấu hiệu của niềm tin”. Thông tin trong Blockchain không thể bị thay đổi và chỉ được bổ sung thêm khi có sự đồng thuận của tất cả các nút trong hệ thống. Đây là một hệ thống bảo mật an toàn cao trước khả năng bị đánh cắp dữ liệu. Ngay cả khi một phần của hệ thống Blockchain sụp đổ, những máy tính và các nút khác sẽ tiếp tục bảo vệ thông tin và giữ cho mạng lưới tiếp tục hoạt động.

### Công nghệ tạo ra blockchain

* Blockchain được hình thành bởi sự kết hợp của 3 loại công nghệ: Mật mã học, Mạng ngang hàng và Lý thuyết trò chơi.
* Mật mã học: Public key và hàm Hash function được sử dụng để đảm bảo tính minh bạch, toàn vẹn và riêng tư.
* Mạng ngang hàng: Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ bản sao ứng dụng.
* Lý thuyết trò chơi: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (giao thức PoW, PoS,…) và được thúc đẩy bởi động lực kinh tế.

### Phân loại blockchain

- Public Blockchain: Dữ liệu trên Blockchain được công khai để mỗi người có thể theo dõi được dữ liệu nếu họ muốn.

- Private Blockchain: Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy.

- Permissioned Blockchain (hay còn gọi là Consortium): đây là sự kết hợp giữa Public và Private Blockchain.

### 2.4 Các đặc điểm của blockchain

Blockchain là công nghệ lưu trữ và truyền tải thông tin bằng các khối (block) được liên kết với nhau. Cụ thể, blockchain là một mạng lưới gồm nhiều block và mỗi block lưu trữ những thông tin về thời gian khởi tạo và được liên kết với các khối trước đó. Đặc biệt, các thông tin dữ liệu trên các block là không thể thay đổi, nó chỉ có thể được cập nhật và bổ sung thêm. Về cơ bản, blockchain là một chuỗi các máy tính mà tất cả phải chấp thuận thao tác trước khi nó có thể được thực hiện, mỗi block ra đời hay được chỉnh sửa thông tin đều phải có sự xác nhận của các máy tính tham gia hệ thống. Blockchain ở thời điểm hiện tại, đã cho thấy ở nó có các ưu điểm hơn hẳn những công nghệ khác đang được sử dụng, cụ thể:

*- Tính hiệu quả:* công nghệ blockchain giúp nâng cao hiệu quả giao dịch giữa các bên bằng việc loại bỏ sự có mặt của các bên trung gian, các bên tin cậy thứ ba. Các dữ liệu trong blockchain được xác thực tự động thông qua cơ chế đồng thuận theo thời gian thực (real-time). Blockchain có thể tăng tốc độ giao dịch/thanh toán giữa các bên khi thỏa thuận giữa các bên được tự động mã hóa và lưu trữ dưới dạng các hợp đồng thông minh (smart contract) và được các thực thể khác (cá nhân hoặc tổ chức) xác thực theo cơ chế tự động.

*- Tính phi tập trung:* sự kết hợp của nhiều thực thể (hệ thống máy tính) kết nối thành mạng lưới tạo ra một chuỗi dữ liệu dài vô tận. Mỗi thực thể của mạng lưới đều có thể tạo ra khối mới và quyền xác nhận các giao dịch. Đây là mô hình “mã nguồn mở”, không có cơ quan trung ương hoặc một bên duy nhất theo dõi hoặc ủy quyền cho bất kỳ thay đổi nào trong chuỗi. Nó giúp loại bỏ sự can thiệp và tập trung quyền lực vào một cơ quan trung ương, giúp loại bỏ chi phí tổ chức và hoạt động của các cơ quan này trong các hệ thống truyền thống hiện tại.

*- Tính minh bạch:* khi một block mới được tạo ra và xác nhận, nó sẽ tồn tại vĩnh viễn. Suốt trong thời gian tồn tại, tất cả các bên đều có thể dễ dàng xem nội dung block cũng như những giao dịch gắn liền với nó theo thời gian thực. Một bản ghi công khai với đầy đủ nội dung được tạo ra với mỗi giao dịch có tính chất vĩnh viễn, công khai với toàn bộ thành viên của mạng lưới sẽ giúp giảm thiểu (thậm chí có thể nói hoàn toàn không có) bất kỳ hoạt động gian lận nào.

*- Tính bền vững và bảo mật cao:* blockchain có tính năng bảo mật tốt hơn bởi vì sẽ không có bất kỳ một khe hở nào có thể được tận dụng để đánh sập hệ thống, thậm chí là đối với các hệ thống tài chính có nguy cơ tiềm ẩn cao nhất. Bởi vì hệ thống blockchain được bảo mật bởi rất nhiều máy tính khác nhau được gọi là các nút mạng (nodes) và chúng sẽ đảm bảo việc xác nhận cho những giao dịch trong hệ thống.

## Các loại node trong blockchain

Bất kỳ thiết bị nào được kết nối với blockchain đều có thể được phân loại là một node. Ví dụ: máy chủ, máy tính, máy tính xách tay, ví trực tuyến hoặc máy tính để bàn và điện thoại di động.

Blockchain càng có nhiều node, nó càng trở nên phi tập trung hơn và do đó trở nên linh hoạt trước các mối đe dọa như sự cố hệ thống hoặc mất điện.

Vai trò chính của Node :

* Kiểm tra tính hợp lệ của một khối (block) mới.
* Lưu trữ một khối vào blockchain.
* Cập nhật các node khác trong mạng blockchain để đảm bảo rằng thông tin trên các node khác đều là mới nhất.

### Light Nodes

Các light node có mục đích tương tự như các node đầy đủ, tuy nhiên thay vì lưu trữ toàn bộ lịch sử giao dịch của một blockchain thì chúng chỉ giữ một phần của lịch sử giao dịch như tiêu đề của các khối, từ đó có thể truy vấn tính hợp lệ của các giao dịch trước đó. Tiêu đề khối là một bản tóm tắt của một khối, bao gồm thông tin liên kết với khối trước đó. Thông tin lưu trữ trong tiêu đề bao gồm: dấu thời gian tại thời điểm tạo khối, và số nonce.

Ảnh có chứa văn bản, ký hiệu, đường cao tốc

Mô tả được tạo tự động

Như hình trên, các light node sẽ được kết nối với full node ( thường được gọi là node cha của chúng). Các light node phải dựa vào full node để xác minh tính hợp lệ của dữ liệu. Các light node giúp phần mở rộng và phân cấp mạng lưới blockchain, bởi vì lưu trử và xử lý dữ liệu ít hơn các node đầy đủ nên chúng cần ít tài nguyên hơn để duy trì và chạy. Ví dụ về light node : máy tính để bàn, ví blockchain.

### Full and Super Nodes

Một full node nắm giữ tất cả thông tin được lưu giữ trên một blockchain và hoạt động như một máy chủ cốt lõi trên các mạng blockchain phi tập trung. Mỗi khối trong một blockchain được xác minh, xác thực và lưu trữ bởi tất cả các full node trong mạng.

Ảnh có chứa văn bản, ngoài trời

Mô tả được tạo tự động

Mỗi node đầy đủ sẽ lưu trữ một bản sao của tất cả các giao dịch blockchain. Vì thế chúng đòi hỏi dung lượng lưu trữ và năng lượng tính toán cao. Các full node nắm giữ một vai trò rất quan trọng trong mạng blockchain. Bởi vì chúng quyết định đến tính bảo mật và hợp lệ của mạng blockchain đó. Vì thế vai trò của nó khác với các loại node khác bao gồm:

* Xác thực chữ ký trong mỗi khối giao dịch: Khi một khối mới được thêm vào blockchain, full node sẽ dùng khóa công khai của người gửi giao dịch để kiểm tra tính hợp lệ của giao dịch. Quá trình này gọi là xác thực chữ ký điện tử.
* Người thực thi quyết định chính của các quy tắc đồng thuận: Các node đầy đủ có quyền và sự ảnh hưởng đến việc từ chối các khối mới. Sau khi được các node khác xác thực, full node có thể từ chối khối mới này bởi vì một trong những lý do như : Định dạng khối không đúng, hoặc khối này đã được khai thác.

Các node đầy đủ thường được điều hành bởi các tình nguyện viên hoặc các bên liên quan. Và việc chạy các node đầy đủ này cụ thể là trên mạng bitcoin thì sẽ không nhận được phần thưởng cho việc xác thực giao dịch.

### Mining Nodes

Các node khai thác là các node tạo ra các khối cho blockchain. Giống như chúng ta thường nghe đến "thợ đào bitcoin", thì các thợ đào đang chạy loại node mining.

Vai trò của các node này là thực hiện tính toán để tìm ra một số nonce đáp ứng yêu cầu của blockchain đó. Node đầu tiên tìm ra được số nonce này, sẽ gửi kết quả của nó cho các full node xác thực và full node sẽ thêm block mới này blockchain. Việc tìm ra số nonce này sẽ tiêu tốn tài nguyên và năng lượng, vì vậy các node mining này sẽ nhận được một phần thưởng cho việc tạo ra khối mới.

Các node khai thác chỉ chịu trách nhiệm tạo ra các khối chứ chúng không chịu trách nhiệm về việc duy trì hoặc tính hợp lệ của các khối trong tương lai ( không giống như các full node).

Shape

Description automatically generated

## Mempool

### Mempool là gì?

Mempool là từ viết tắt của "memory" (bộ nhớ) và "pool" (bể). Đây là một cách để Bitcoin lưu lại những giao dịch chưa được xác nhận trước khi xác nhận chúng trên chuỗi khối.

Đây cũng là nơi các giao dịch chờ cho đến khi các Miner Node sắp xếp chúng vào block tiếp theo. Mỗi Node duy trì nhóm bộ nhớ của riêng mình và mỗi Node có dung lượng riêng để lưu trữ các giao dịch chưa được xác nhận. Khi một giao dịch được xử lý, nó sẽ bị xóa khỏi Mempool.

### Mối quan hệ giữa Mempool, Full Node và Miner Node trong mạng Bitcoin

Mọi Full Node của mạng Bitcoin đều có quyền truy cập vào Mempool, lưu trữ tất cả các giao dịch cũng như các block của Blockchain Bitcoin. Mục tiêu của các Full Node là xác thực các giao dịch theo các quy tắc của giao thức Bitcoin.

Các Full Node sẽ chạy một loạt kiểm tra để đảm bảo rằng giao dịch hợp lệ như xác minh rằng chữ ký là chính xác, đầu ra không vượt quá đầu vào và tiền chưa được chi tiêu. Nếu không đáp ứng các điều kiện này, nó sẽ bị từ chối.

Nếu một giao dịch vi phạm các quy tắc (ví dụ: chữ ký không hợp lệ), giao dịch đó sẽ không được chuyển tiếp đến các Node khác. Tuy nhiên, một khi giao dịch được xác minh theo các quy tắc hợp lệ, nó sẽ được thêm vào Bitcoin Mempool.

Khi các giao dịch chưa được xử lý đã ở mempool, các Miner Node sẽ là người chọn và sắp sếp chúng vào block tiếp theo của Bitcoin. Các Miner sẽ lựa chọn dựa trên tiêu chí là phí giao dịch, giao dịch nào trả phí cao nhất sẽ được ưu tiên xử lý trước.

### Tầm quan trọng và hạn chế của kiến trúc Mempool

Trong kiến trúc của Bitcoin và các blockchain tương tự, mọi giao dịch đều phải đi qua Mempool trước khi được thêm vào các block mới trên blockchain. Trong thời gian lưu lượng truy cập cao và tắc nghẽn, Mempool thu thập và lưu trữ các giao dịch cho đến khi các Miner Node có thể thêm chúng vào các block mới.

Tuy nhiên, Mempool cũng đem đến những ảnh hưởng lớn đến quyền lợi người dùng (MEV). MEV (Miner Extractable Value) có thể hiểu là lợi nhuận mà Miner Node kiếm được nhờ việc lợi dụng quyền hạn của mình.

Miner Node không cần xử lý giao dịch theo thời gian người dùng đưa lệnh on-chain mà họ có thể ưu tiên những giao dịch trả mức phí cao hơn hoặc các lệnh có lợi cho mình. Hai tác hại phổ biến của MEV là:

Bot giao dịch chênh lệch giá của những bên thứ ba.

Exchange front-running bot, các bot này có thể giám sát những giao dịch lớn đang chờ được xử lý trên mempool và tận dụng chúng để kiếm lời.

## Cơ chế đồng thuận trong blockchain

Về bản chất, blockchains là cơ sở dữ liệu phân tán được thiết kế để ghi lại, giao tiếp và giao dịch thông tin mà không cần cơ quan trung ương. Hầu hết các blockchain được xây dựng trên một mạng lưới các nút riêng lẻ phân tán hoạt động cùng nhau để cung cấp các giao dịch diễn ra trên mạng mà tất cả chúng đều chia sẻ. Do đó, mọi mạng lưới blockchain cần phải có một cơ chế giúp đảm bảo tất cả các nút của nó được đồng bộ hóa với nhau và thống nhất về các giao dịch nào là hợp pháp và nên được thêm vào blockchain.

Hệ thống phi tập trung này để xác định trạng thái thực sự của blockchain được gọi là Cơ Chế Đồng Thuận. Ngoài việc đảm bảo các hoạt động cốt lõi của một blockchain, các cơ chế đồng thuận có thể tác động trực tiếp đến các thông số tài chính và bảo mật của mạng mà chúng làm nền tảng.

Hầu hết các blockchains đều có ba thuộc tính cần thiết: Khả Năng Mở Rộng, Phân Quyền Và Bảo Mật – mà các nhà phát triển phải tìm cách mã hóa thành DNA thuật toán của mạng. Ba ưu tiên cạnh tranh đã được mệnh danh là “ Blockchain Trilemma ” bởi Vitalik Buterin, đồng sáng lập của Ethereum . Nhiệm vụ thiết kế và triển khai một mô hình quản trị mạng phi tập trung hiệu quả cân bằng cả ba thuộc tính này là một thách thức không có hồi kết.

Do đó, các mạng khác nhau đã đưa ra các cơ chế đồng thuận blockchain khác nhau phù hợp nhất với các ưu tiên chiến lược của họ. Dưới đây là các loại đồng thuận blockchain phổ biến nhất ngoài Proof of Work (PoW) và Proof of Stake (PoS) .

### Proof of Work (PoW) – Minh chứng công việc

Bằng chứng công việc (POW) là một thuật toán đồng thuận phổ biến được sử dụng bởi các mạng tiền điện tử phổ biến nhất như Bitcoin và Litecoin. Nó yêu cầu một nút người tham gia để chứng minh rằng công việc được thực hiện và gửi bởi họ đủ điều kiện để họ nhận được quyền thêm giao dịch mới vào blockchain.

Tuy nhiên, toàn bộ cơ chế khai thác này của Bitcoin cần mức tiêu thụ năng lượng cao và thời gian xử lý lâu hơn.

### Proof of Stake (PoS) – Minh chứng cổ phần

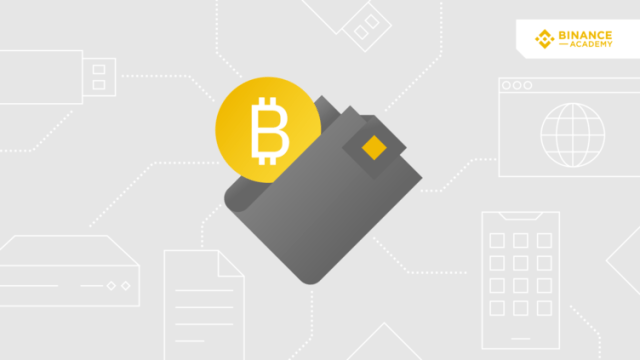
Bằng chứng cổ phần (POS) là một thuật toán đồng thuận phổ biến khác phát triển như một giải pháp thay thế tiêu thụ năng lượng thấp, chi phí thấp cho thuật toán POW. Nó liên quan đến việc phân bổ trách nhiệm trong việc duy trì sổ cái công khai cho một nút người tham gia tương ứng với số lượng mã thông báo tiền ảo do nó nắm giữ.

Tuy nhiên, điều này đi kèm với một nhược điểm là nó thúc đẩy tiết kiệm tiền điện tử, thay vì chi tiêu.

## Ví tiền mã hóa

Ví tiền mã hóa là một công cụ (phần mềm hoặc phần cứng) mà bạn có thể sử dụng để tương tác với mạng [blockchain.](https://academy.binance.com/vi/articles/how-does-blockchain-work)

Ví tiền mã hóa không thực sự lưu trữ tiền mã hóa. Thực tế, nó là một ứng dụng cung cấp các công cụ cần thiết để tương tác với một blockchain. Nói cách khác, các ví này có thể tạo ra thông tin cần thiết để gửi và nhận tiền mã hoá, thông qua các giao dịch trên blockchain. Một trong những thông tin cần thiết đó bao gồm một hoặc nhiều cặp [khóa công khai và riêng tư](https://academy.binance.com/vi/articles/what-is-public-key-cryptography).



Khóa cá nhân (private key) là bằng chứng sở hữu cung cấp quyền truy cập vào tiền mã hoá và Khóa công khai (Public Key) dùng để định danh tài khoản và có thể được tìm kiếm bằng blockchain

Tiền mã hóa không bao giờ thực sự rời khỏi blockchain, chúng chỉ được chuyển từ ví này sang ví khác.

# Tìm hiểu khái niệm Smart Contract: Smart contract là gì?

Smart Contract (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.

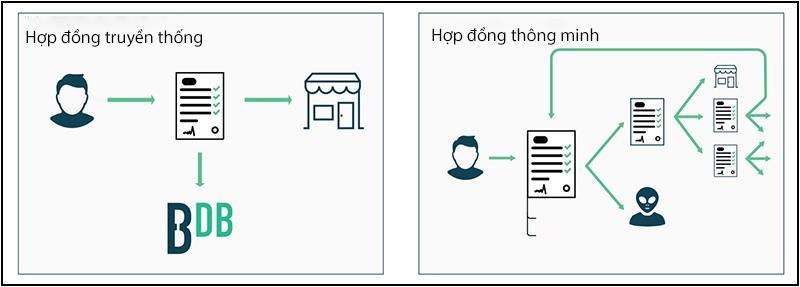
Về bản chất, Smart Contract chỉ là một đoạn mã chạy trên một hệ thống phân tán (blockchain), cho phép tạo ra các giao thức Permissionless (tức là không cần trao quyền). Điều đó có nghĩa là:

* 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.

## Smart Contract khác gì với hợp đồng truyền thống?

|  |  |  |
| --- | --- | --- |
|  | **Hợp đồng thông minh** | **Hợp đồng truyền thống** |
| **Giao kết** | Được giao kết bằng phương tiện điện tử và sẽ có chữ ký điện tử. | Giao kết bằng phương tiện “giấy tờ”, “vật chất” và ký tay sau khi các bên gặp và trao đổi với nhau. |
| **Tạo bởi** | Hợp đồng thông minh tạo ra bởi hệ thống máy tính ngôn ngữ lập trình, các điều khoản quy định được đưa ra và không chịu sự can thiệp bởi của con người.  => Giúp thực thi hợp đồng một cách công minh và chính xác. | Tạo bởi các chuyên gia pháp lý, họ dựa vào các tài liệu, văn bản quy định và cần bên thứ ba giúp thực thi.  => Mất nhiều thời gian và chi phí, nhất là trong trường hợp xảy ra sự cố phải chỉnh sửa lại hợp đồng. |
| **Lưu trữ** | Lưu trữ trực tiếp trên các nền tảng số. => Không lo thất lạc, hư hỏng. | Lưu trữ hợp đồng giấy như thông thường. |

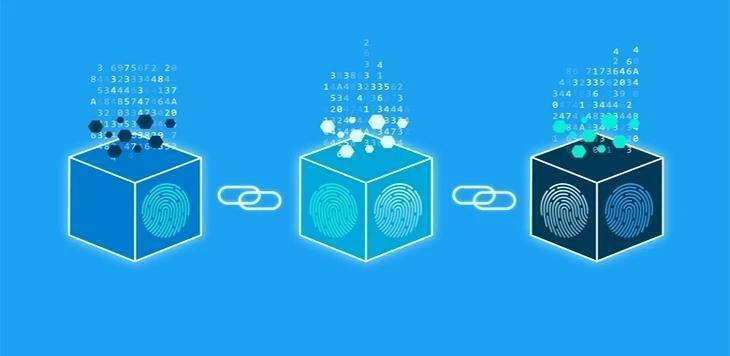


## Smart contract hoạt động như nào?

Smart Contract chỉ tự động thực hiện khi những điều khoản đã được lập trình sẵn từ trước. Đầu tiên, các điều khoản trong hợp đồng sẽ được viết bằng ngôn ngữ lập trình, rồi được mã hóa và chuyển vào một block thuộc Blockchain. Sau đó, hợp đồng thông minh được phân phối và sao chép lại bằng các node đang hoạt động tại nền tảng đó.

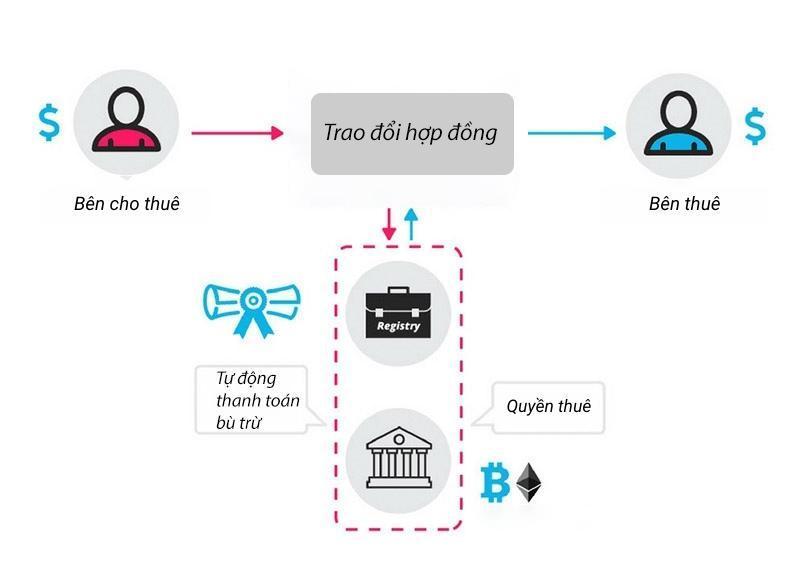
Sau khicó lệnh triển khai thì hợp đồng sẽ được triển khai theo đúng như điều khoản định sẵn**.** Đồng thời, Smart Contract cũng sẽ tự động kiểm tra quá trình thực hiện những cam kết, điều khoản được nêu trong hợp đồng.

Vì hệ thống hoạt động dựa trên câu lệnh “**If - Then**” và hàng trăm người giám sát nên sẽ không xảy ra lỗi sai trong quá trình giao nhận.



*Ví dụ:*

Bạn dự định thuê căn phòng, bạn đã trả tiền thuê qua Blockchain. Biên nhận trả tiền sẽ được ghi nhận vào hợp đồng thông minh. Trong hợp đồng quy định đầu tháng sau bạn sẽ nhận mật mã căn hộ. Tuy nhiên nếu đến thời điểm đó, bạn vẫn chưa nhận được. Hợp đồng thông minh sẽ tự động hoàn tiền lại cho bạn, bạn không cần liên lạc bên thuê nhà để lấy tiền thuê. Mọi thứ sẽ được diễn ra theo đúng quy trình, quy định của hợp đồng.



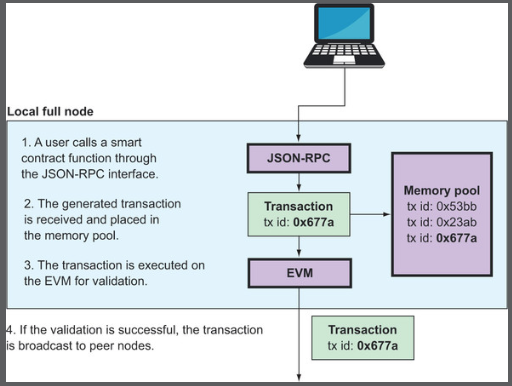
## Chu trình thực thi Smart Contract?

Bước 1: Người dùng gọi một hàm hợp đồng thông minh thông qua JSON-RPC interface.

Bước 2: Giao dịch phát ra được nhận và đặt nó vào memory pool

Bước 3: Thực hiện giao dịch trên EVM để xác thực

Bước 4: Nếu xác thực thành công, nút sẽ phát hành giao dịch tới các node ngang hàng khác. Nếu xác thực không thành công, nút sẽ không truyền giao dịch đi nữa.

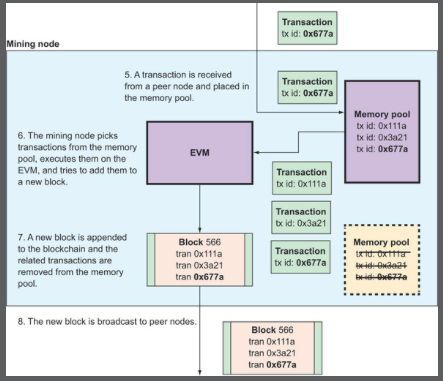


Bước 5: Mining node đặt giao dịch nhận được từ một nút ngang hàng trong memory pool.

Bước 6: Mining node chọn các giao dịch từ memory pool, thực hiện chúng trên EVM và cố gắng thêm chúng vào một block mới

Bước 7: Nếu block đã tạo được thêm thành công vào blockchain, nút khai thác sẽ xóa các giao dịch liên quan khỏi memory pool

Bước 8: Block mới sẽ được phát hành đến các node ngang hàng khác trong mạng.

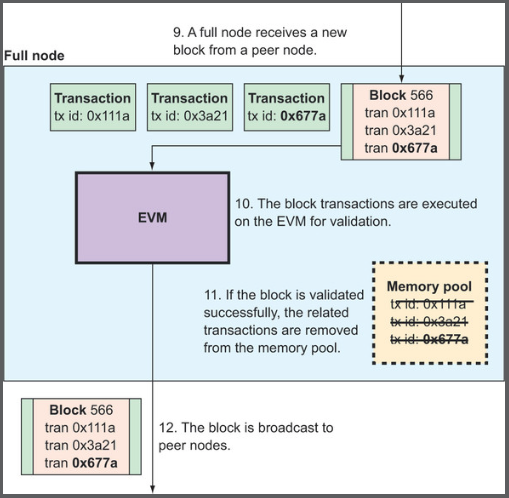


Bước 9: Full node nhận block mới từ một node ngang hàng.

Bước 10: Full node thực hiện tất cả các giao dịch của block trên EVM để xác thực.

Bước 11: Full node xóa tất cả các giao dịch được liên kết khỏi memory pool nếu block đã được xác thực thành công.

Bước 12: Full node phát hành block tới các node ngang hàng khác

****

## Ứng dụng của Smart Contract

Theo ông Jerry Cuomo, phó chủ tịch về công nghệ Blockchain của công ty IBM, tin rằng Smart Contract – hợp đồng thông minh có thể sử dụng trong nhiều trường hợp, từ dịch vụ tài chính, chăm sóc sức khỏe đến bảo hiểm. Dưới đây là một số ví dụ về các ứng dụng của nó:

* Sử dụng cho các cuộc Bầu cử
* Sử dụng cho các nhà quản lý
* Dịch vụ y tế
* Logistics (Chuỗi cung ứng)

Với vai trò quan trọng trong thương mại quốc tế, hoạt động logistics đối mặt với nhiều co hội chuyển mình cũng như thách thức trong cuộc cách mạng công nghiệp 4.0. Thực trạng hiện nay khi mà nguy co quá tải trong các tài liệu của hồ so giao dịch khi hàng hóa đi qua hàng trăm cảng biển truớc khi đến đuợc noi yêu cầu, nhu cầu về sự minh bạch thông tin trong giao dịch, thông tin về hàng hóa, nhiều khâu trong chuỗi giá trị logistics bị ràng buộc quy trình thủ công do co quan quản lý bắt buộc, các công ty phải thuờng xuyên dựa vào huớng dẫn nhập dữ liệu và tài liệu trên giấy để tuân thủ quy trình hải quan. Những việc này khiến cho việc theo dõi nguồn gốc hàng hóa và trạng thái của lô hàng là khó khăn. Tất cả những điều trên đặt cho lĩnh vực này cần có một sự thay đổi tất yếu. Do đó, với những tác động tích cực mà blockchain mang lại, ngành logistics kỳ vọng sẽ có một sự đột phá lớn trong tuông lai gần.

Các tác động khả quan mà blockchain kỳ vọng đem lại cho ngành logistics như sau:

**Logistics nhanh hơn và tỉnh gọn hơn trong thương mại toàn cầu:**

Logistics đuợc xem là huyết mạch của thế giới hiện đại, với khoảng 90% thuong mại thế giới đuợc thực hiện bởi ngành vận tải quốc tế mỗi năm.

Hiện nay, logistics toàn cầu vẫn liên quan đến rất nhiều giấy tờ, do đó tốn kém về thời gian và tiền bạc. Quy trình vận chuyển đuờng dài này bao gồm rất nhiều thủ tục giấy tờ liên kết với nhau. Ngoài ra, tài liệu vận chuyển bằng giấy nhu vận đon (Bill of Lading) có nguy co bị mất, giả mạo và gian lận (Popper & Lohr, 2017).

Blockchain có thể giúp giảm bớt nhiều sự tương tác trong logistics thương mại toàn cầu, bao gồm cả quản lý vận tải, theo dõi dấu vết và tài chính. Cụ thể, blockchain có thể giúp tối uu hóa chi phí và thời gian liên kết với tài liệu thương mại và quản lý hành chính đối với các lô hàng.

Để nâng cao sự hiệu quả trong vận tải đường biển, Maersk và IBM đã bắt đầu một liên doanh để thiết lập một hệ thống blockchain toàn cầu để số hóa luồng công việc thương mại và theo dõi lô hàng. Hệ thống cho phép các bên liên quan trong chuỗi cung ứng xem quá trình hàng hóa trong chuỗi, biết được hàng hóa đang được vận chuyển đến đâu. Các bên liên quan có thể thấy được trạng thái của các chứng từ hải quan, có thể xem được vận đơn và các dữ liệu khác. Blockchain giúp đảm bảo sự an toàn cho dữ liệu và kho lưu trữ giả mạo cho các tài liệu này

Accenture - Công ty cung cấp dịch vụ và tư vấn công nghệ, là một trong những công ty tư vấn lớn nhất thế giới, đang phát triển một hệ thống blockchain tập trung vào việc thay thế vận đon truyền thống. Ở đây, một mạng kết nối tất cả các bên trong chuỗi cung ứng và cho phép giao dịch trực tiếp, loại bỏ việc dựa vào các bên trung gian. Và kết quả của điều này sẽ thúc đẩy giảm chi phí trong chuỗi cung ứng cho các bên liên quan, bao gồm chủ hàng, người nhận hàng, người vận chuyển, người giao nhận, cảng, cơ quan hải quan, ngân hàng và công ty bảo hiểm.

**Cải thiện tính minh bạch của chuỗi cung ứng**

Trong điều kiện kinh tế phát triển như hiện nay, niềm tin của người tiêu dùng lại là mối quan tâm đặc biệt của nhiều công ty. Do đó, nhiều dự án sử dụng blockchain nhằm cải thiện tính minh bạch của chuỗi cung ứng. Dữ liệu về hàng hóa về cách chúng được tạo ra, chúng đến từ đâu và cách chúng được quản lý được lưu trữ trên hệ thống blockchain. Điều đặc biệt là các thông tin này là vĩnh viễn và chia sẻ. Vì thế những người tham gia họ không thể sửa đổi thông tin, các thông tin được đảm bảo an toàn và bảo mật. Các công ty họ có thể sử dụng những thông tin này làm bằng chứng cho tính hợp pháp của sản phẩm của mình.

Minh họa cho điều này, năm 2017, Walmart, IBM và Đại học Tsinghua (Trung Quốc) đã thí điểm việc sử dụng blockchain để theo dõi các mặt hàng thực phẩm, bao gồm thịt lợn ở Trung Quốc và xoài ở Mỹ, khi chúng di chuyển qua chuỗi cung ứng để cất giữ trên kệ. Thử nghiệm của Walmart cho thấy áp dụng blockchain giảm thời gian cần để theo dõi một gói xoài từ trang trại đến cửa hàng từ ngày hoặc tuần đến hai giây.

Walmart cùng với các đối tác đã thử nghiệm co chế tại chỗ để xác định và khắc phục việc bảo quản thực phẩm không đúng cách trong suốt quá trình từ trang trại đến cửa hàng. Những cảm biến đuợc gắn liền với sản phẩm và Walmart cam kết các dữ liệu này đuợc dựa trên blockchain. Bridget van Kralingen, phó chủ tịch cấp cao của IBM cho biết rằng Blockchain giữ lời hứa đáng kinh ngạc trong việc cung cấp sự minh bạch cần thiết để giúp thúc đẩy an toàn thực phẩm trên toàn bộ chuỗi cung ứng.

**Truy xuất nguồn gốc và xác định sản phẩm giả mạo**

Hiện nay, vấn nạn thực phẩm bẩn tràn lan và an toàn vệ sinh thực phẩm đang là vấn đề nhức nhối của du luận toàn cầu. Tuy nhiên, nỗi hoang mang của nguời tiêu dùng đó là sự bất cân xứng về thông tin, khi mà họ không thể biết đuợc sản phẩm họ đang sử dụng có thật sự là sản phẩm tốt hay không. Và khi có chuyện xảy ra nhu ngộ độc thực phẩm,... thì lại khó tìm ra đuợc nguyên nhân xuất phát từ khâu nào trong chuỗi hoạt động từ nguyên liệu cho đến thành phẩm.

Nhằm theo dõi nguồn gốc của các mặt hàng thực phẩm, Walmart đã hợp tác với IBM vào năm 2016, blockchain đuợc sử dụng để theo dõi sự chuyển động của các mặt hàng này. Truớc tiên, Walmart và IBM theo dõi kỹ thuật số cả chuyển động trong nuớc; cụ thể là thịt lợn từ các trang trại nhỏ của Trung Quốc đến các cửa hàng Trung Quốc và theo dõi chuyện động quốc tế - sản xuất từ Mỹ La tinh đến các cửa hàng ở Hoa Kỳ (Popper & Lohr, 2017). Trong hệ thống blockchain, các dữ liệu nhu nguồn gốc trang trại, số lô, nhà máy và dữ liệu quá trình chế biến, ngày hết hạn và chi tiết vận chuyển đuợc viết chi tiết và thể hiện cho tất cả thành viên trong hệ thống mạng đuợc biết. Với bệnh liên quan đến thức ăn khi bùng phát thì hệ thống cho phép Walmart theo dõi nguồn gốc chỉ trong vài giây.

Ngoài nỗi lo về nguồn gốc sản phẩm tốt xấu thì một nỗi lo của nguời tiêu dùng hiện nay đó là sản phẩm giả. Khi mà trình độ khoa học công nghệ tăng lên thì mặt trái của nó là khả năng làm giả sản phẩm ngày càng trở nên tinh vi và rất khó để nguời tiêu dùng có thể nhận biết đuợc. Để giảm thiểu mối lo này, công nghệ blockchain thông qua việc thiết lập sự minh bạch trong chuỗi cung ứng từ nhà sản xuất đến nguời bán hàng và cuối cùng thì thông tin đó sẽ đến nguời tiêu dùng, thì sẽ giúp họ xác định đuợc sản phẩm giả mạo. Đối với những nguời bệnh nhân, thông tin xác thực trong chuỗi này càng hiệu quả khi tránh nguy co nhận phải thuốc giả, vì nó rất nguy hiểm. Thông qua mã vạch hoặc công nghệ Identification (ID) tự động mà những người bệnh nhân có thể được trao quyền để kiểm tra xem họ có nhận được thuốc thực sự (Mackey & Nayyar, 2017).

Tự động hóa quy trình thương mại trong logistics với hợp đồng thông minh

Một trong những công ty đầu tiên ứng dụng hợp đồng thông minh trong logistics đó là ShipChain. ShipChain thiết lập hệ thống theo dõi trên toàn bộ chuỗi cung ứng, từ thời điểm hàng rời khỏi nhà máy, cánh đồng hay trang trại để phân phối hoàn chỉnh đến khách hàng. Shipchain thống nhất việc theo dõi lô hàng trên blockchain Ethereum, sử dụng hợp đồng thông minh. Hợp đồng ShipChain được thực hiện trên Ethereum có thể được sử dụng bởi bất cứ ai để thiết lập một ký quỹ vận chuyển. Khi lô hàng được hoàn thành và xác nhận, hợp đồng được lưu trữ trên blockchain chính. ShipChain chủ yếu sẽ là một thị trường mở, noi các chủ hàng và hãng vận tải có thể kết nối và tiến hành kinh doanh hiệu quả hơn và có tính minh bạch cao hon. Tuy nhiên, cũng sẽ có nền tảng web ShipChain, cho phép đặt chỗ và quản lý các lô hàng sử dụng nhiều nhà cung cấp dịch vụ và phưong thức vận tải khác nhau (Hamilton, 2018).

Dự án 300 Cubits đã ra đời, đây là dự án áp dụng công nghệ blockchain đế xây dựng một nền tảng phi tập trung, trong đó thông tin về chuyến tàu, tình trạng đặt chỗ, tình trạng hàng hóa... đều được công khai với cả khách hàng và công ty vận tải. Khi một lệnh đặt tàu được thực hiện, blockchain sẽ sinh ra một hợp đồng thông minh, yêu cầu hai bên phải đặt cọc một khoản tiền bằng token chứa container vận chuyển công nghiệp (token TEU). Bên công ty tàu sẽ được bồi thường TEU nếu khách hàng không mang hàng đến giao, và ngược lại khách hàng cũng sẽ nhận được TEU nếu hàng hóa của họ bị bỏ lại do lỗi của bên cho thuê tàu. Tất nhiên số tiền đặt cọc sẽ chảy lại về túi của cả hai nếu hợp đồng được tuân thủ hoàn toàn (Nami.today, 2018).

**Một lợi ích khác của hợp đồng thông minh trong logistics nữa được thể hiện trong các điều kiện thanh toán cho người bán.**

Cụ thể, các lợi ích đó như sau:

- Mô hình hóa thư tín dụng (Letter of Credits - L/C) như một hợp đồng thông minh có nghĩa là tuân thủ điều kiện và ngăn ngừa sự mơ hồ trong giải thích các điều kiện của L/C.

- Giảm thời gian và chi phí sửa đổi L/C: L/C có thể được phát hành và sửa đổi ngay lập tức và kỹ thuật số.

- Cho phép phát hiện sớm sự khác biệt về thông tin: Các bên liên quan có thể nhìn vào quy trình L/C và có thể giải quyết sự khác biệt nhanh hon.

Các cụm từ như “đầu tháng” và “ngày sau” được thay thế bằng phạm vi ngày và giờ để chỉ định rõ ngày được phép giao hàng, giao hàng, thanh toán,... Thông qua hợp đồng thông minh, mỗi điều kiện có thể được đánh giá dựa trên các tài liệu do nhà xuất khẩu gửi, loại bỏ sự mơ hồ của người nhập khẩu một cách hiệu quả

## Ưu điểm và nhược điểm của Smart Contract:

### Ưu điểm

* Ứng dụng của Smart Contractcó thể sử dụng được trong nhiều lĩnh vực trong tương lai, hiện tại một số lĩnh vực đã triển khai smart contract bao gồm: Tiền điện tử, logistic, ngân hàng, bất động sản thậm chí là việc bầu cử.
* **Tự do:** Không bị một cơ quan nào quản lý
* **Phân tán.** Hợp đồng thông minh được sao chép và phân phối trong tất cả các nút của mạng Ethereum. Đây là một điểm khác biệt so với các giải pháp khác dựa trên các máy chủ tập trung.
* **Tất định.** Hợp đồng thông minh chỉ thực hiện các hành động mà chúng được thiết kế để thực hiện trong trường hợp các điều kiện được thỏa mãn. Bên cạnh đó, các kết quả của hợp đồng thông minh không đổi dù người thực hiện là ai.
* **Tự động.** Hợp đồng thông minh có thể tự động hóa tất cả các loại tác vụ, nó hoạt động như một chương trình tự thực hiện. Tuy nhiên, trong hầu hết các trường hợp, nếu hợp đồng thông minh không được kích hoạt, nó sẽ duy trì trạng thái “không hoạt động” và sẽ không thực hiện bất kỳ hành động nào.
* **Không thể sửa đổi.** Không thể sửa đổi hợp đồng thông minh sau khi triển khai. Chỉ có thể “xóa” chúng nếu chức năng này đã được thêm vào từ trước. Do đó, có thể nói rằng hợp đồng thông minh giống như một mã chống giả mạo.
* **Có thể tùy chỉnh.** Trước khi triển khai, hợp đồng thông minh có thể được mã hóa theo nhiều cách khác nhau. Vì vậy, chúng có thể được sử dụng để tạo ra nhiều loại ứng dụng phi tập trung (Dapp). Điều này là bởi Ethereum là một blockchain có thể được sử dụng để giải quyết bất kỳ vấn đề tính toán nào (Turing complete)
* **Không cần dựa trên sự tin cậy**. Hai hoặc nhiều bên của hợp đồng có thể tương tác thông qua hợp đồng thông minh mà không cần biết hoặc tin tưởng lẫn nhau. Ngoài ra, công nghệ blockchain đảm bảo tính chính xác của dữ liệu.
* **Minh bạch**. Vì các hợp đồng thông minh dựa trên một blockchain công khai, không ai có thể thay đổi mã nguồn của chúng, mặc dù bất kỳ ai cũng có thể xem được.

### Nhược điểm

* **Tính pháp lý:** Bạn sẽ không được bảo vệ quyền lợi khi xảy ra lỗi phát sinh do pháp luật các nước hiện nay chưa có chính sách để khai thác, quản lý smart contract
* **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 của Smart Contract là 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.

# III. Ứng dụng Blockchain trong truy xuất nguồn gốc sữa

## 1. Mô tả bài toán

### Thực trạng chuỗi cung ứng sữa truyền thống

* Chuỗi cung ứng (SC) ngày nay rất phức tạp với nhiều loại sản phẩm chế biến khác nhau được chuyển qua nhiều bên tham gia.
* Sữa và các sản phẩm từ sữa có liên quan đến bệnh tật do thực phẩm trong nhiều thế kỷ nên chúng là những thực phẩm cần [được kiểm soát chặt chẽ](https://extension.psu.edu/dairy-food-processing-federal-regulations) nhất.
* Ngày càng xuất hiện nhiều hãng sữa chỉ đóng hộp đơn giản, không có nguồn gốc xuất xứ rõ ràng.
* Người tiêu dùng quan tâm nhiều hơn đến nguồn gốc nguyên liệu cũng như xuất xứ và sự an toàn của các sản phẩm sữa.
* Các sản phẩm sữa được sản xuất trực tiếp từ sữa tươi được ưu tiên hơn so với các sản phẩm sữa hoàn nguyên.
* Lượng sữa tươi trong nước có chất lượng cao, đáp ứng được tiêu chuẩn kỹ thuật đầu vào chỉ đạt khoảng 30%-35% nhu cầu
* Sữa tươi đạt chuẩn quốc tế, đặc biệt là sữa đạt chuẩn hữu cơ ở Việt Nam đến nay cung vẫn không đủ cầu.
* Kiểm soát được vùng nguyên liệu sữa trở thành vấn đề sống còn đối với các doanh nghiệp sản xuất sữa tại Việt Nam
* Một số kết quả khảo sát (Theo Ipsos Việt Nam)
  + 80% các  mẹ không tự tin khi chọn mua sữa bột cho con trong lần đầu tiên.
  + 66% không rõ về thế nào là tiêu chí làm nên sữa bột tốt.
  + 74% cho rằng thông tin trên bao bì chưa đủ để họ đánh giá chất lượng.
* 78% các bà mẹ cho rằng nếu được truy xuất nguồn gốc sữa họ sẽ an tâm hơn rất nhiều trong việc quyết định mua sữa bột cho con

### Các vấn đề trong truy xuất nguồn gốc sữa

* Khó theo dõi các sản phẩm khi nó nằm ngoài các nhà cung cấp trực tiếp. Người quản lý hàng tồn kho và những người ra quyết định khác thiếu thông tin liên quan đến vị trí, trạng thái... về sản phẩm, thành phần, và vật liệu.
* Gian lận thực phẩm và khó xác định các bên chịu trách nhiệm do hệ thống chuỗi cung ứng thực phẩm phức tạp.
* Các nhóm nông dân nhỏ lẻ khó kết nối với người thu mua ổn định và cũng khó đảm bảo chất lượng nguồn gốc nông sản.
* Thiếu hệ thống thông tin tập trung, minh bạch và cơ chế chia sẻ thông tin từ người sản xuất, nhà phân phối tới người tiêu dùng như thông tin về sản phẩm, nguồn gốc, chất lượng, thông tin về người sản xuất và nhà phân phối có chứng chỉ, thông tin truyền thông, giáo dục về sản phẩm an toàn, bổ dưỡng và bền vững đối với người tiêu dùng.
* Việc áp dụng công nghệ Blockchain vào quản trị chuỗi cung ứng sẽ giải quyết được những khó khăn nói trên, đem đến sản phẩm minh bạch, an toàn cho người tiêu dùng.

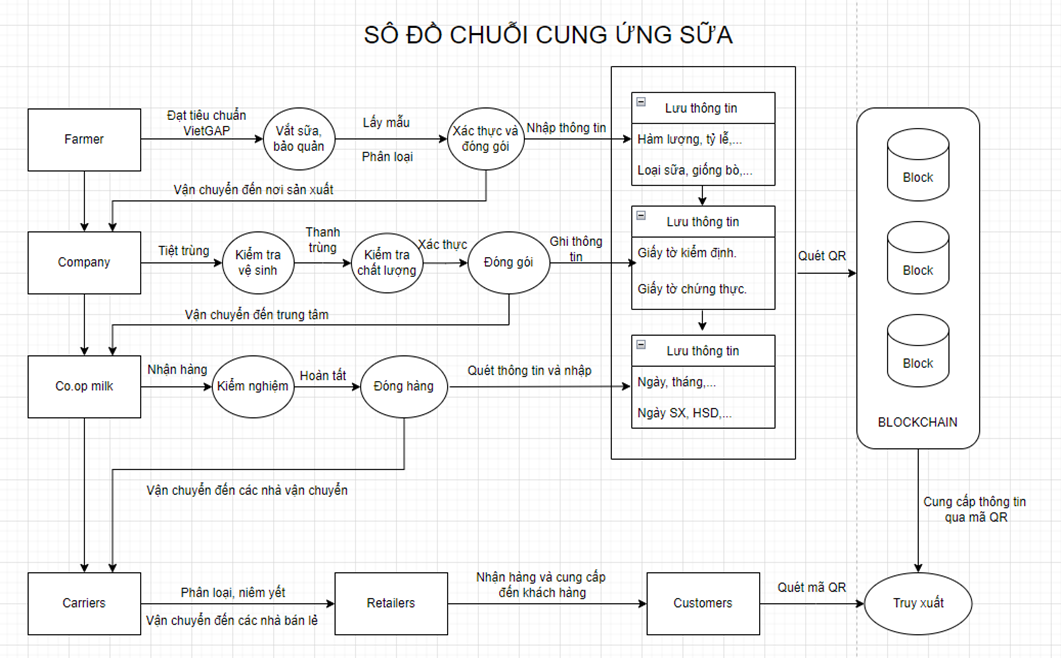
## 2. Mô hình truy xuất nguồn gốc dựa trên Blockchain

### Triển khai mô hình truy xuất nguồn gốc sữa tươi Mộc Châu

Sữa tươi Mộc Châu là một công ty sữa lâu năm với nhiều sản phẩm sữa trên thị trường như sữa tươi thanh trùng, sữa tươi tiệt trùng... Quy trình sản xuất sữa tươi Mộc Châu cũng trải qua rất nhiều quy trình, giai đoạn. Để sản phẩm được người tiêu dùng tin tưởng hơn - người tiêu dùng xem được chi tiết quy trình sản xuất và cũng để nhà cung cấp sản phẩm nắm được các quy trình sản xuất sữa qua các giai đoạn, được cơ quan nào kiểm tra chất lượng ? Nếu sản phẩm chưa đảm bảo chất lượng cũng nắm được chưa đảm bảo ở giai đoạn nào để có hướng xử lý phù hợp. Như vậy, rất cần thiết một hệ thống truy xuất nguồn gốc sữa tươi Mộc châu áp dụng công nghệ Blockchain.

Mô hình truy xuất nguồn gốc nông sản dựa trên Blockchain gồm có những bên tham gia:

1. Hộ nông dân, trang trại nuôi bò (Farmer)
2. Nhà máy sản xuất sữa (Company)
3. Trung tâm thu mua sữa tươi (Co.op milk)
4. Người phân phối (Carriers)
5. Đại lý, cửa hàng ()
6. Người tiêu dùng (customers)



### Quy trình sản xuất sữa Mộc Châu

**Quy trình chăn nuôi ( Trước khi đem về nhà máy )**

Trang trại chăn nuôi bò sữa phải đạt tiêu chuẩn VietGAP.

Khu chuồng trại rộng rãi, thoáng mát với hệ thống tiêu thoát nước hoàn thiện. Thức ăn cho bò ở đây được chế biến khá hiện đại, kết hợp giống cỏ kho Alfalfa nhập khẩu từ Mỹ với giống cỏ trong nước của các hộ chăn nuôi tự trồng, thân cây ngô được đem ủ men kỹ rồi mới đem cho bò ăn.

Sau khi thu mua sữa bò mới vắt ra ở nhiệt độ 35 - 37 độ C sẽ được chuyển xuống bảo quản ở nhiệt độ 2 - 4 độ C và kiểm tra nhanh độ tươi của sữa để phân loại.

Tiếp đó lấy mẫu của tất cả các bình sữa để kiểm tra các chỉ tiêu như: nhiệt độ, hàm lượng chất khô, chất béo, tỷ lệ vi sinh… trong sữa. Tất cả số sữa thu mua từ các hộ chăn nuôi sẽ được vận chuyển về nhà máy bằng xe chuyên dụng.

**Quy trình lấy sữa**

Sản lượng sữa tính theo chu kỳ vắt sữa 305 ngày, nếu bò có thời gian vắt sữa tự nhiên không đủ 180 ngày thì không được tính là một chu kỳ cho sữa.

Sản lượng sữa được xác định bằng cân điện tử hoặc cân bàn. Đơn vị tính sản lượng sữa là kilogram, độ chính xác của cân tới 0,1 kg.

Lượng sữa ngày kiểm tra phải được xác định đảm bảo đủ trong 24 h và phải vắt sữa đúng quy trình kỹ thuật.

Thời gian giữa các lần kiểm tra sản lượng sữa liên tiếp theo là 30 ngày.

**Quy trình chế biến sữa (Sau khi đem về nhà máy)**

Hiện công ty đã xây dựng được một dây chuyền sản xuất sữa tiệt trùng hiện đại và khép kín cùng với một hệ thống xử lý nước thải bằng phương pháp vi sinh và hóa học với công suất xử lý 300m2/ngày.

Mộc Châu Milk hiện có 2 nhà máy dây chuyền chế biến hiện đại từ tập đoàn Tetra Park với năng lực sản xuất hon 230 tấn sữa mỗi ngày cho ra các sản phẩm sữa sạch

**Quá trình thanh trùng sữa**

Quá trình thanh trùng phải được bảo đảm thực hiện liên tục. Có 2 cách thanh trùng: Một, đun sữa ở nhiệt độ thấp khoảng 63 độ C trong vòng 30 phút, sau đó để lạnh ngay. Hai, đun sữa ở nhiệt độ tương đối cao (85-90 độ C) trong thời gian ngắn từ 30 giây đến 1 phút rồi làm lạnh ngay.

Tuy nhiên, với phương pháp thanh trùng, sữa phải luôn được giữ lạnh từ 3- 5 độ C để đảm bảo chất lượng và an toàn cho sản phẩm. Sữa bò tươi thanh trùng khi mua về nên được để trong ngăn đá đến khi sản phẩm có thể đạt đến nhiệt độ 4 độ C thì có thể để xuống ngăn làm mát trong tủ lạnh để dùng dần trong khoảng 10 ngày.

Do sữa thanh trùng hoàn toàn dùng vật liệu là sữa tươi vắt từ bò sữa, nên hương vị ngon hơn sữa tiệt trùng. Nhưng cũng chính vì vậy nên việc tồn trữ và bảo quản sữa thanh trùng rất khó, đòi hỏi luôn phải được giữ lạnh. Do phải bảo quản lạnh thường xuyên để sản phẩm sữa không bị hỏng nên khi đưa ra thị trường, giá của sữa thanh trùng bao giờ cũng mắc hơn sữa tiệt trùng.

Sữa tươi thanh trùng thường bổ béo và thơm ngon hơn sữa tiệt trùng. Nguyên nhân là do sữa tươi thanh trùng được xử lý ở nhiệt độ thấp nên gần như giữ được toàn bộ các vitamin, khoáng chất quan trọng và mùi vị thơm ngon của sữa ban đầu.

**Quá trình tiệt trùng sữa**

Phương pháp tiệt khuẩn cực nhanh hay còn gọi là tiệt trùng tức là diệt khuẩn cực nhanh bằng cách cho sữa chảy thành màng mỏng ở nhiệt độ cực cao (135 – 150 độ C) trong một khoảng thời gian cực ngắn 3-15 giây, rồi làm lạnh ngay xuống ở 12,5 độ C. Công nghệ tiệt trùng còn được gọi là tiến trình xử lý nhiệt cho thực phẩm dạng lỏng như sữa ở nhiệt độ cực cao trong thời gian cực ngắn.

Công nghệ tiệt trùng, một trong những tiến bộ khoa học quan trọng nhất thế kỷ 20, giúp sản phẩm có thể được bảo quản mà không cần dùng đến hệ thống tồn trữ lạnh.

**Quy trình đóng gói và bảo quản**

Quy trình đóng gói phải đảm bảo vệ sinh từ các thiết bị đóng gói đến hộp đóng gói đều phải được kiểm tra vệ sinh.

### Xây dựng website truy xuất

Website được thiết kế trên nền tảng ứng dụng web - ASP.NET Web Application (.NET Framework). Website sử dụng ngôn ngữ C#, mô hình MVC ( Model – View – Controller) và sử dụng cơ sở dữ liệu SQL Server.

**Cơ sở dữ liệu website**

Cơ sở dữ liệu Website bao gồm 5 bảng:

- Bao gồm các bảng: VaiTro, NguoiDung, LoHang, SanPham, QuyTrinh.

- Các trường của các bảng và mối quan hệ giữa các bảng:

Diagram

Description automatically generated

*Hình 2.1: Cơ sở dữ liệu website*

**Quy trình hoạt động của Website**

Website truy xuất nguồn gốc sản xuất sữa tươi Mộc Châu bằng công nghệ Blockhchain có các đối tượng người dùng tham gia đó là:

- Quản trị viên

- Nhà sản xuất

- Cơ quan kiểm định

- Người tiêu dùng

Text

Description automatically generated

*Hình 2.2: Giao diện đăng nhập*

Khi bấm vào nút *Đăng nhập* Hàm **Dangnhap** trong controller **HomeController** sẽ được thực hiện:

Text

Description automatically generated

*Giao diện đăng nhập*

Tùy vào các tài khoản ứng với vai trò khác nhau sẽ chuyển đến trang giao diện tương ứng.

**Đối với quản trị viên**

Graphical user interface, text, application, chat or text message

Description automatically generated

*Giao diện hiển thị của quản trị viên*

Quản trị viên website có chức năng:

- Quản lý người dùng:

+ Thêm mới tài khoản cho nhà sản xuất.

+ Thêm mới tài khoản cho các cơ quan kiểm định.

+ Sửa, xóa các tài khoản khỏi hệ thống.

- Giao diện và hàm xem chi tiết, thêm, sửa, xóa người dùng:

+ Xem chi tiết người dùng

Graphical user interface, text, application, chat or text message

Description automatically generated

*Giao diện xem chi tiết người dùng*

Graphical user interface, text, application, email

Description automatically generated

*Hàm xem chi tiết người dùng*

+ Thêm mới người dùng

Graphical user interface, application

Description automatically generated

*Giao diện thêm mới người dùng*

Graphical user interface, text, application, email

Description automatically generated

*Hàm thêm mới người dùng*

+ Chỉnh sửa người dùng

Graphical user interface

Description automatically generated with medium confidence

*Giao diện chỉnh sửa người dùng*

Graphical user interface, text, application, email

Description automatically generated

*Hàm sửa thông tin người dùng*

+ Xóa người dùng người dùng

Graphical user interface, text, application, chat or text message, email

Description automatically generated

*Hình 2.11: Giao diện xóa người dùng*

Text, application

Description automatically generated

*Hình 2.12: Hàm xóa người dùng*

**Đối với nhà sản xuất**

Sau khi được Quản trị viên hệ thống cấp tài khoản, nhà sản xuất đăng nhập hệ thống bằng tài khoản được cấp. Hiển thị giao diện:

Graphical user interface, application

Description automatically generated

*Giao diện hiển thị của nhà sản xuất*

Nhà sản xuất có các chức năng:

- Quản lý lô hàng: Thêm mới, sửa, xóa các lô hàng. Bao gồm: Tên lô hàng, ngày sản xuất, ngày hết hạn lô hàng, ghi chú của lô hàng.

- Quản lý các sản phẩm: Thêm mới, sửa, xóa các sản phẩm . Bao gồm các thông tin : Tên sản phẩm, mô tả sản phẩm, hình ảnh của sản phẩm, lô hàng của sản phẩm.

- Quản lý các quy trình sản xuất sản phẩm : Thêm mới, sửa, xóa các quy trình. Bao gồm: Tên quy trình, mô tả quy trình, tệp tin chứng thực mô tả của quy trình, chọn cơ quan kiểm định của quy trình.

Graphical user interface, application

Description automatically generated

*Giao diện hiển thị các quy trình sản xuất*

- Tìm kiếm quy trình : Tìm kiếm các quy trình theo tên sản phẩm.

+ Khi nhà sản xuất nhập từ khóa vào ô input bấm vào nút *Tìm kiếm* hàm **Index** trong Controller **QuyTrinhsController** sẽ thực hiện. Tìm kiếm trong cơ sở dữ liệu các quy trình có tên sản phẩm là từ khóa đã nhập vào ô input và hiển thị trên website.

Graphical user interface, text, application

Description automatically generated

*Hàm tìm kiếm và hiển thị quy trình sản xuất*

**Đối với cơ quan kiểm định**

Sau khi được Quản trị viên hệ thống cấp cho tài khoản. Cơ quan kiểm định đăng nhập hệ thống bằng tài khoản được cấp. Cơ quan kiểm định chọn menu *Tạo chữ kí RSA* để tạo bộ khóa RSA.

Graphical user interface

Description automatically generated

*Giao diện hiển thị của cơ quan kiểm định*

- Bấm nút vào *Tạo khóa tự động*: Hàm **TaoKhoa** trong controller **TaoKhoaRSAController** sẽ được thực hiện:

Graphical user interface, text, application

Description automatically generated

*Hàm tạo khóa RSA cho cơ quan kiểm định*

Graphical user interface, text, application

Description automatically generated

*Hàm khởi tạo và tạo bộ khóa RSA ngẫu nhiên*

- Sau khi tạo khóa thành công màn hình hiển thị khóa bí mật, cơ quan kiểm định copy và lưu lại khóa bí mật của mình vào file trong máy tính.

Graphical user interface, text, application, email

Description automatically generated

*Hiển thị khóa bí mật trên website*

- Cơ quan kiểm định vào menu *Quy trình chưa kí*. Hiển thị các quy trình chưa kí:

Graphical user interface, application

Description automatically generated

*Giao diện quy trình chưa kí*

- Bấm vào nút *Chi tiết* để hiển thị chi tiết quy trình :

Graphical user interface, application

Description automatically generated

*Giao diện xem chi tiết quy trình*

- Bấm vào nút *Xác thực quy trình*. Hiển thị giao diện nhập khóa bí mật để xác thực:

Graphical user interface, text, application, email

Description automatically generated

*Giao diện xác thực quy trình*

- Sau khi nhập đúng khóa bí mật và bấm vào nút *Xác thực ngay*. Hàm **KiemDinhQuyTrinh** trong **KiemDinhsController** được thực hiện:

+ Hàm **KiemDinhQuyTrinh** nhận vào tham số ID quy trình, Khóa bí mật.

+ Tìm trong cơ sở dữ liệu quy trình đang cần xác thực. Dùng FileStream đọc file ảnh tệp tin cần chứng thực được nhà sản xuất tải lên. Dùng hàm Băm sh256 băm file.

+ Sử dụng khóa bí mật kí lên file ảnh đã được băm. Lưu chữ kí vào cơ sở dữ liệu.

Text

Description automatically generated

*Hàm KiemDinhQuyTrinh*

Graphical user interface, text, application

Description automatically generated

*Hàm RSA\_Mahoa tính lũy thừa nhanh*

- Sau khi nhập đúng khóa bí mật và bấm *Xác thực ngay* thì sẽ hiển thị thông báo “Ký thành công”.

Graphical user interface, text, application, email

Description automatically generated

*Hiển thị thông báo trên website*

- Sau khi tất cả quy trình sản xuất của sản phẩm được kiểm định bởi các cơ quan kiểm định trạng thái quy trình sẽ chuyển thành “ Đã kiểm định”

Graphical user interface, application

Description automatically generated

*Quy trình đã được ký*

**Đối với người tiêu dùng**

**-** Truy cập trang chủ của website.

Graphical user interface, application

Description automatically generated

*Trang chủ website*

- Bấm vào chức năng Tìm kiếm sản phẩm. Hiển thị giao diện tìm kiếm sản phẩm.

Graphical user interface, application

Description automatically generated

*Giao diện tìm kiếm*

- Nhập tên sản phẩm bấm vào *Tìm kiếm. ­*Hàm **TimKiem** trong Controller **HomeController** được thực hiện.

Graphical user interface, text, application

Description automatically generated

*Hàm tìm kiếm sản phẩm*

- Tìm kiếm thành công website trả về view sản phẩm tương ứng:

Graphical user interface, application, Word

Description automatically generated

*Kết quả tìm kiếm*

**-** Bấm vào *Xem chi tiết.* Hàm **XemChiTiet** trong Controller **HomeController** được thực hiện.

+ Hàm **XemChiTiet** nhận vào tham số là ID sản phẩm.

+ Từ ID sản phẩm tìm ra tất cả các quy trình sản xuất ra sản phẩm đó. Xác thực lại chữ kí của các cơ quan kiểm định trên từng quy trình sản xuất xem đúng hay không ?

+ Sau đấy thông báo cho người dùng sản phẩm đã được kiểm định đầy đủ hay chưa?

+ Mô tả chi tiết từng quy trình cho biết quy trình do ai kiểm định. Và chữ kí trên quy trình đó.

Graphical user interface, text, application, email

Description automatically generated

*Hàm XemChiTiet sản phẩm*

- Nếu tất cả các quy trình sản xuất của sản phẩm được xác thực là đúng:

+ Sẽ hiển thị trạng thái của sản phẩm là : “ SẢN PHẨM ĐÃ ĐƯỢC KIỂM ĐỊNH ĐẦY ĐỦ ”.

+ Hiển thị đầy đủ mô tả quy trình sản xuất của sản phẩm và do cơ quan nào kiểm định.

Graphical user interface, text

Description automatically generated

*Sản phẩm đã được kiểm định*

- Nếu 1 trong các quy trình sản xuất của sản phẩm đã được cơ quan kiểm định ký kiểm định nhưng sau đó nhà sản xuất thay đổi thông tin mô tả quy trình:

+ Sẽ hiển thị trạng thái của sản phẩm là : SẢN PHẨM CHƯA ĐƯỢC KIỂM ĐỊNH ĐẦY ĐỦ.

+ Hiển thị chi tiết từng quy trình: quy trình nào đã được kiểm định – xác thực lại chữ kí là đúng và quy trình nào đã được kiểm định nhưng đã bị nhà sản xuất thay đổi thông tin .

Timeline

Description automatically generated with medium confidence

*Sản phẩm chưa được kiểm định*

+ Đối với Cơ quan kiểm định: Khi nhà sản xuất thay đổi thông tin tệp tin mô tả quy trình. Đăng nhập vào hệ thống vào menu ­*Quy trình bị sửa đổi* sẽ hiển thị các quy trình nhà sản xuất đã sữa đổi thông tin.

Graphical user interface, application

Description automatically generated

*Sản phẩm chưa được kiểm định*

- Cơ quan kiểm định bấm vào nút *Chi tiết* để xem lại chi tiết quy trình và thực hiện kí lại trên các quy trình bị sửa đổi.

### 2.4 Ưu điểm

* Giảm chi phí xác minh thông tin về các giao dịch trong quá khứ và chi phí kết nối mạng trong vận hành chuỗi cung ứng.
* SC với mức độ cao khả năng thích ứng, tính chủ động, độ tin cậy, khả năng đáp ứng và trách nhiệm giải trình.
* Cung cấp mức độ hiển thị dữ liệu cao.
* Một giao dịch được xác nhận bởi nhiều người tham gia vào một mạng lưới, vì vậy làm tăng tính minh bạch của SC và độ chính xác của dữ liệu giao dịch.

**2.3 Nhược điểm**

* Website giao diện đang còn chưa bắt mắt, cơ sở dữ liệu và các chức năng còn cần được hoàn thiện để web hoạt động tốt hơn.

### 2.5 Kết quả đạt được

* Nhóm đã xây dựng thành công website truy xuất nguồn gốc sản phẩm sữa tươi Mộc Châu dựa trên công nghệ Blockchain.
* Nhà sản xuất thêm được các sản phẩm khác nhau, lô hàng khác nhau và chọn cơ quan kiểm định phù hợp với quy trình sản xuất.
* Cơ quan kiểm định tự tạo bộ khóa RSA và khóa bí mật chỉ mình cơ quan kiểm định biết. Sử dụng khóa bí mật để ký lên các quy trình sản xuất.
* Sản phẩm sau khi các cơ quan kiểm định ký lên mô tả các quy trình sản xuất được hiển thị lên trang chủ và sẽ được xác thực lại chữ ký của các cơ quan kiểm định xem thông tin có đúng và có bị thay đổi không? Hiển thị chi tiết mô tả từng quy trình sản xuất.

### 2.6 Nội dung phân công việc

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TT** | **Nội dung công việc** | **Kết quả cần đạt được** | **Người thực hiện** | **Ghi chú** |
|
| 1 | Tìm hiểu quy trình sản xuất sữa Mộc Châu. | Bản báo cáo quy trình sản xuất sữa | Cả nhóm |  |
| 2 | Khảo sát, phân tích, xây dựng CSDL | CSDL về website truy xuất nguồn gốc sữa | Nguyễn Quốc Khánh |  |
| 3 | Tìm hiểu công cụ lập trình Visual Studio IDE, ngôn ngữ lập trình c#, mô hình MVC | Sử dụng thành thạo công cụ lập trình. | Cả nhóm |  |
| 4 | Xây dựng các chức năng chính của phần mềm, cài đặt chữ ký điện tử RSA | Các chức năng chính của phần mềm, hàm tạo chữ kí, mã hóa RSA | Nguyễn Quốc Khánh |  |
| 5 | Xây dựng giao diện cho website | Giao diện website | Võ Lâm Trường  Phạm Huy Hoàng |  |
| 6 | Hoàn thiện website | Website truy xuất nguồn gốc sữa Mộc Châu | Nguyễn Quốc Khánh  Võ Lâm Trường |  |
| 7 | Kiểm thử phần mềm | Báo cáo các lỗi mà phần mềm còn gặp phải | Cả nhóm |  |
| 8 | Viết báo cáo, hoàn thiện bài tập | Báo cáo hoàn thiện | Chu Ngọc Thắng  Phạm Huy Hoàng |  |

# IV.Tham khảo:

1. Báo cáo Hệ thống truy xuất nguồn gốc thực phẩm (sữa tươi tiệt trùng) (Võ Thị Mỹ Hà)
2. Báo cáo đồ án Truy xuất nguồn gốc nông sản blockchain (Đinh Hoàng Tùng, Dương Bảo Nam)
3. <https://dotnet.microsoft.com/en-us/learn/aspnet/hello-world-tutorial/intro>
4. Giáo trình Hoạch định nguồn lực doanh nghiệp (UIT)
5. https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rsacryptoserviceprovider?view=net-6.0