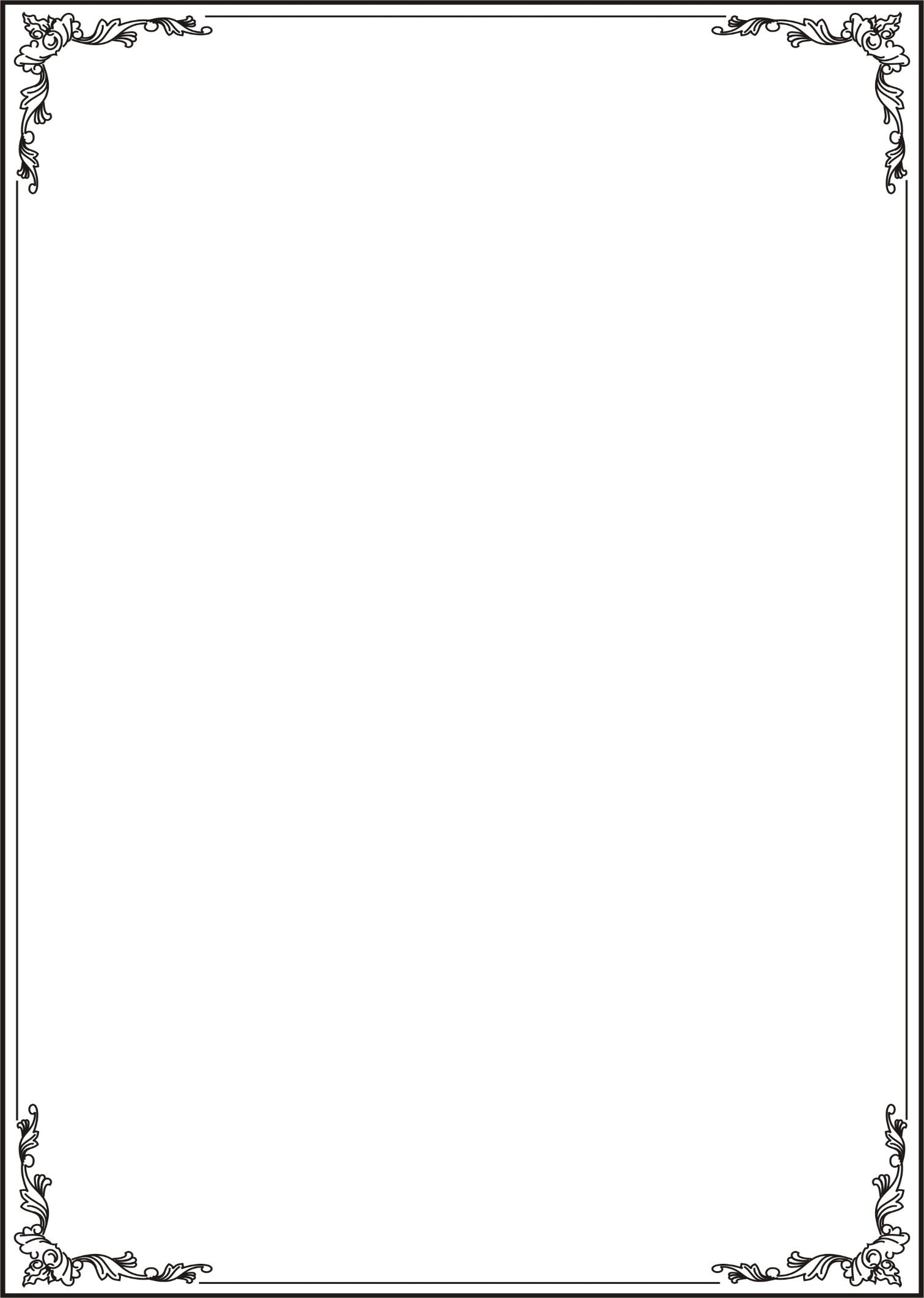
TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI



KHOA CÔNG NGHỆ THÔNG TIN

~~~\*\*\*\*\*\*\*\*\*~~~

**ĐỒ ÁN TỐT NGHIỆP**

**Đề tài**

Xây dựng Website ứng dụng công nghệ Blockchain vào quản lý chuỗi cung ứng - truy suất nguồn gốc hàng hoá

Giảng viên hướng dẫn : Bùi Ngọc Dũng

Sinh viên thực hiện : Nguyễn Duy Khánh

Mã sinh viên : 211202428

Lớp : Công Nghệ Thông Tin 2

Khóa : 62

Hà Nội, tháng 06 năm 2025

1

1

# **LỜI CẢM ƠN**

Trước hết, tôi xin gửi lời cảm ơn chân thành đến Trường Đại học Giao Thông Vận Tải và Khoa Công Nghệ Thông Tin đã cho tôi cơ hội tham gia vào chương trình đào tạo và hoàn thiện đồ án tốt nghiệp " Xây dựng Website ứng dụng công nghệ Blockchain vào quản lý chuỗi cung ứng, truy suất nguồn gốc hàng hoá. ". Đặc biệt, tôi xin gửi lời cảm ơn sâu sắc đến Ths. Bùi Ngọc Dũng, người đã làm hướng dẫn viên tận tâm và đồng hành cùng tôi trong suốt quá trình nghiên cứu và phát triển đồ án này.

Tôi muốn bày tỏ lòng biết ơn đến gia đình và bạn bè của tôi vì sự động viên và hỗ trợ không ngừng suốt thời gian tôi dành cho việc nghiên cứu và hoàn thiện đồ án này. Sự ủng hộ và tình yêu thương của họ đã truyền động lực và giúp tôi vượt qua những thử thách trong quá trình hoàn thành dự án này. Tôi cũng muốn gửi lời cảm ơn đến các giảng viên, bạn bè và đồng nghiệp đã cùng tôi chia sẻ kiến thức, kinh nghiệm và ý kiến quan trọng. Những đóng góp và những cuộc thảo luận hữu ích đã giúp tôi cải thiện dự án và đảm bảo tính đầy đủ và chất lượng của trang web ứng dụng công nghệ Blockchain vào quản lý chuỗi cung ứng, truy suất nguồn gốc hàng hoá.

Cuối cùng, tôi muốn gửi lời cảm ơn đến tất cả những người đã sử dụng trang web quản lý trang trại trong quá trình thử nghiệm. Phản hồi và đề xuất của các bạn đã cung cấp thông tin quý giá để tôi có thể cải thiện và tối ưu hoá trang web. Một lần nữa, tôi xin chân thành cảm ơn tất cả mọi người đã đóng góp và hỗ trợ trong quá trình hoàn thiện đồ án tốt nghiệp này.

Tôi xin chân thành cảm ơn.

# **MỤC LỤC**

[LỜI CẢM ƠN 1](#_Toc7244)

[MỤC LỤC 2](#_Toc19142)

[DANH MỤC VÀ CÁC TỪ VIẾT TẮT 4](#_Toc21969)

[DANH MỤC BẢNG BIỂU 5](#_Toc759)

[DANH MỤC HÌNH ẢNH 6](#_Toc7074)

[GIỚI THIỆU 8](#_Toc4216)

[CHƯƠNG 1. KHẢO SÁT NGHIỆP VỤ BÀI TOÁN ỨNG DỤNG CÔNG NGHỆ BLOCHCHAIN VÀO QUẢN LÝ CHUỖI CUNG ỨNG, TRUY SUẤT NGUỒN GỐC HÀNG HOÁ 9](#_Toc22501)

[1.1. Mở đầu 9](#_Toc10372)

[1.2. Thực trang trong quản lý chuỗi cung ứng và truy suất nguồn gốc hàng hoá 9](#_Toc14313)

[1.3. Khảo sát nghiệp vụ 10](#_Toc25636)

[a. Kết quả khảo sát 10](#_Toc30114)

[b. Kết quả khảo sát 10](#_Toc20041)

[1.4. So sánh các hình thức quản lý chuỗi cung ứng truy suất nguồn gốc hàng hoá khác 12](#_Toc28133)

[1.4.1. Hình thức quản lý truyền thống 12](#_Toc24461)

[1.4.2. Hình thức quản lý qua Web 2.0 12](#_Toc29075)

[1.5. Công nghệ sử dụng 16](#_Toc15671)

[1.5.1. Next.js 16](#_Toc28952)

[a. Giới thiệu 16](#_Toc32059)

[b. Mục đích sử dụng 16](#_Toc23786)

[1.5.2. MeshJS và Cbor 16](#_Toc32582)

[a. Giới thiệu 16](#_Toc10983)

[b. Mục đích sử dụng 16](#_Toc11030)

[1.5.3. Aiken và Plutus 16](#_Toc12229)

[a. Giới thiệu 16](#_Toc9904)

[b. Mục đích sử dụng 16](#_Toc13561)

[1.5.4. Postgresql và Prisma 17](#_Toc27444)

[a. Giới thiệu 17](#_Toc14001)

[b. Mục đích sử dụng 17](#_Toc5470)

[1.6. Kết luận 17](#_Toc21216)

[c. Giới thiệu 17](#_Toc30448)

[d. Mục đích sử dụng 17](#_Toc31084)

[CHƯƠNG 2. PHÂN TÍCH THIẾT KẾ HỢP ĐỒNG THÔNG MINH CỦA ỨNG DỤNG 18](#_Toc22687)

[2.1. Công nghệ áp dụng 18](#_Toc12027)

[a. Khái niệm 18](#_Toc6204)

[b. Luồng sử lý dữ liệu 19](#_Toc32496)

[2.2. Thiết kế các điều kiện của hợp đồng thông minh 19](#_Toc27936)

[2.1.1. Hợp đồng thông minh để tạo sản phẩm 20](#_Toc24218)

[2.1.2. Hợp đồng thông minh để cập nhật thông tin của sản phẩm 21](#_Toc11576)

[2.3. Phân tích các luồng xử lý dữ liệu của hợp đồng thông minh 22](#_Toc4780)

[2.3.1. Chức năng tạo sản phẩm 23](#_Toc32537)

[2.3.2. Chức năng cập nhật sản phẩm 26](#_Toc29028)

[2.3.3. Chức năng xoá sản phẩm 29](#_Toc2563)

[2.4. Kiểm thử các trường hợp có thể xảy ra của hợp đồng thông minh 32](#_Toc28437)

[2.4.1. Kiểm thử chức năng thêm sản phẩm 32](#_Toc31428)

[2.4.2. Kiểm thử chức năng cập nhật sản phẩm 35](#_Toc4086)

[2.4.3. Kiểm thử chức năng xóa sản phẩm 39](#_Toc11472)

[CHƯƠNG 3. PHÂN TÍCH THIẾT KẾ TRANG WEB ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN VÀO QUẢN LÝ CHUỖI CUNG ỨNG TRUY SUẤT NGUỒN GỐC HÀNG HOÁ 41](#_Toc29021)

[3.1. Thiết kế use case 41](#_Toc275)

[3.1.1. Use case tổng quát 41](#_Toc28109)

[3.1.2. Use case kết nối ví 41](#_Toc30781)

[3.1.3. Use case quản lý dịch vụ 42](#_Toc14978)

[3.1.4. Use case quản lý bộ sưu tập 43](#_Toc5282)

[3.1.5. Use case quản lý sản phẩm 44](#_Toc4710)

[3.1.6. Use case truy xuất nguồn gốc sản phẩm 44](#_Toc26593)

[3.2. Thiết kế cơ sở dữ liệu 47](#_Toc24971)

[3.2.1. Mô hình liên kết cơ sở dữ liệu 47](#_Toc4843)

[3.2.2. Chi tiết các bảng 48](#_Toc15779)

[a. Bảng user - Người dùng 48](#_Toc29476)

[b. Bảng wallet nonce - Xác thực ví 48](#_Toc6927)

[c. Bảng collection - Bộ sưu tập 48](#_Toc19897)

[d. Bảng metadata - Metadata của Product 49](#_Toc27505)

[e. Bảng media - Tài nguyên Media 49](#_Toc4692)

[f. Bảng product - Sản phẩm 50](#_Toc31222)

[g. Bảng document - Tài liệu liên quan 50](#_Toc22751)

[h. Bảng product process - Quy trình sản xuất 51](#_Toc15016)

[i. Bảng certification - Chứng nhận sản phẩm 51](#_Toc6645)

[j. Bảng feedback - Đánh giá sản phẩm 52](#_Toc11651)

[k. Bảng supplier - Nhà cung cấp 52](#_Toc24617)

[l. Bảng raw material - Nguyên liệu thô 53](#_Toc15155)

[m. Bảng service plan - Gói dịch vụ 53](#_Toc24664)

[n. Bảng subscription - Đăng kí dịch vụ 54](#_Toc24723)

[o. Bảng payment - Thanh toán 54](#_Toc6547)

[p. Bảng warehouse - Kho lưu trữ 55](#_Toc26480)

[q. Bảng warehouse storage - Lưu trữ hàng hóa 55](#_Toc24943)

[CHƯƠNG 4. CÀI ĐẶT VÀ THỰC NGHIỆM WEBSITE ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN VÀO QUẢN LÝ CHUỖI CUNG ỨNG TRUY SUẤT NGUỒN GỐC HÀNG HOÁ 56](#_Toc7711)

[4.1. Giao diện kết nối ví 56](#_Toc10169)

*[Hinh 4.1 Đăng nhập - Kết nối Ví](#_Toc19673)* [56](#_Toc19673)

[KẾT LUẬN VÀ KIẾN NGHỊ 58](#_Toc21727)

[Kết luận: 58](#_Toc24328)

[Kiến nghị: 58](#_Toc143)

[DANH MỤC TÀI LIỆU THAM KHẢO 59](#_Toc10213)

[Tiếng Việt: 59](#_Toc27223)

[Tiếng Anh: 59](#_Toc9492)

# **DANH MỤC VÀ CÁC TỪ VIẾT TẮT**

|  |  |
| --- | --- |
| **Viết tắt** | **Ý nghĩa** |
| QL&TS  NFT  Token  Smart Contract  UtxO  Datum  Redeemer  Parameters | Quản lý và truy suất  Non Fungible Token là một loại đơn vị dữ liệu trên Blockchain không thể thay thế. Đại diện cho một tài sản số độc nhất vô nhị.  Token là một đơn vị giá trị được phát hành và giao dịch trên các nền tảng phi tập trung.  Smart Contract là các chương trình chạy trên Blockchain, tự động thực hiện, kiểm soát và ghi lại những sự kiện, hành động có liên quan đến nhau về mặt pháp lý dựa theo những điều khoản của hợp đồng hoặc thoả thuận.  UTxO là viết tắt của **Unspent Transaction Output**, nghĩa là **đầu ra giao dịch chưa được sử dụng**. Đây là một khái niệm quan trọng trong các blockchain sử dụng mô hình **UTxO**, như **Bitcoin** hoặc **Cardano**.  **Datum** là một phần dữ liệu **được đính kèm** vào một **UTxO**, giúp **lưu trữ trạng thái** cho smart contract trong mô hình **EUTxO**.  **Redeemer** là **dữ liệu** được **người dùng cung cấp khi tiêu thụ (spend)** một UTxO có gắn validator script, giúp **chỉ định hành động hoặc lựa chọn cụ thể** mà họ đang thực hiện.  **Parameters** là các giá trị **được truyền vào tại thời điểm khởi tạo (deploy)** smart contract (validator), dùng để **cấu hình trước** cho contract — và không thể thay đổi sau đó. |
|  |  |

# **DANH MỤC BẢNG BIỂU**

[Bảng 1. 1 Câu hỏi khảo sát vận hành trang trại 11](#_Toc136218516)

[Bảng 1. 2 Kết quả khảo sát vận hành trang trại 12](#_Toc136218517)

[Bảng 1. 3 Câu hỏi khảo sát nhu cầu sử dụng trang web quản lý trang trại 14](#_Toc136218518)

[Bảng 1. 4 Kết quả khảo sát nhu cầu sử dụng trang web quản lý trang trại 14](#_Toc136218519)

[Bảng 1. 1 Câu hỏi khảo sát vận hành trang trại 11](#_Toc136218516)

[Bảng 1. 2 Kết quả khảo sát vận hành trang trại 12](#_Toc136218517)

[Bảng 1. 3 Câu hỏi khảo sát nhu cầu sử dụng trang web quản lý trang trại 14](#_Toc136218518)

[Bảng 1. 4 Kết quả khảo sát nhu cầu sử dụng trang web quản lý trang trại 14](#_Toc136218519)

# **DANH MỤC HÌNH ẢNH**

[Bảng 1. 1 Câu hỏi khảo sát vận hành trang trại 11](#_Toc136218516)

[Bảng 1. 2 Kết quả khảo sát vận hành trang trại 12](#_Toc136218517)

[Bảng 1. 3 Câu hỏi khảo sát nhu cầu sử dụng trang web quản lý trang trại 14](#_Toc136218518)

[Bảng 1. 4 Kết quả khảo sát nhu cầu sử dụng trang web quản lý trang trại 14](#_Toc136218519)

# **GIỚI THIỆU**

Trong thời đại toàn cầu hoá và sự phát triển không ngừng của công nghệ thông tin, việc quản lý chuỗi cung ứng và đảm bảo tính minh bạch trong quá trình sản xuất, phân phối hàng hoá ngày càng trở nên quan trọng. Sự phức tạp của các chuỗi cung ứng hiện đại đòi hỏi các doanh nghiệp phải đổi mới và áp dụng những giải pháp công nghệ tiên tiến nhằm tăng cường hiệu quả vận hành, giảm thiểu rủi ro và đáp ứng nhu cầu ngày càng cao của người tiêu dùng về nguồn gốc và chất lượng sản phẩm. Tuy nhiên, các phương pháp quản lý truyền thống đang bộc lộ nhiều hạn chế, đặc biệt là trong việc kiểm soát thông tin và đảm bảo tính minh bạch trong toàn bộ quy trình. Gian lận thương mại, hàng giả, và sự thiếu minh bạch trong sản xuất, vận chuyển đã trở thành những vấn đề nhức nhối, ảnh hưởng đến uy tín của doanh nghiệp và quyền lợi của người tiêu dùng.

Trong bối cảnh đó, công nghệ Blockchain đã nổi lên như một giải pháp đầy tiềm năng, mang lại những cải tiến đột phá trong việc quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hoá. Với đặc tính phi tập trung, tính minh bạch, khả năng bảo mật cao và dữ liệu không thể thay đổi sau khi được ghi nhận, Blockchain giúp các bên tham gia dễ dàng giám sát và xác thực thông tin về sản phẩm từ khâu sản xuất, lưu trữ, vận chuyển, đến tay người tiêu dùng cuối cùng. Ứng dụng Blockchain không chỉ giúp hạn chế rủi ro gian lận và hàng giả mà còn tối ưu hoá quy trình vận hành, giảm thiểu chi phí quản lý và nâng cao hiệu quả hoạt động của doanh nghiệp. Đặc biệt, trong bối cảnh các tiêu chuẩn quốc tế về an toàn và chất lượng ngày càng được siết chặt, Blockchain đóng vai trò quan trọng trong việc hỗ trợ doanh nghiệp tuân thủ các quy định pháp lý, đồng thời tăng cường uy tín và khả năng cạnh tranh trên thị trường quốc tế.

Xuất phát từ thực tế đó, đề tài "Ứng dụng công nghệ Blockchain trong quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hoá" được thực hiện nhằm mục tiêu nghiên cứu và đề xuất các giải pháp ứng dụng Blockchain vào quản lý chuỗi cung ứng. Đề tài sẽ tập trung vào việc đánh giá tiềm năng và hiệu quả của công nghệ này trong việc tăng cường tính minh bạch, nâng cao hiệu quả quản lý và đảm bảo an toàn thông tin trong suốt quá trình vận hành của doanh nghiệp. Thông qua nghiên cứu này, chúng tôi kỳ vọng sẽ xây dựng một hệ thống quản lý chuỗi cung ứng dựa trên nền tảng Blockchain, mang lại giải pháp thực tiễn và hiệu quả cho doanh nghiệp trong việc giám sát, kiểm soát và truy xuất nguồn gốc sản phẩm. Đồng thời, đề tài cũng hướng đến việc thúc đẩy quá trình chuyển đổi số trong lĩnh vực quản lý chuỗi cung ứng, góp phần tạo dựng một môi trường kinh doanh công bằng, minh bạch và bền vững trong thời kỳ công nghiệp 4.0.

# **CHƯƠNG 1. KHẢO SÁT NGHIỆP VỤ BÀI TOÁN ỨNG DỤNG CÔNG NGHỆ BLOCHCHAIN VÀO QUẢN LÝ CHUỖI CUNG ỨNG, TRUY SUẤT NGUỒN GỐC HÀNG HOÁ**

## Mở đầu

Sự phát triển của công nghệ Blockchain đã mở ra nhiều cơ hội mới trong việc tối ưu hoá quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hoá. Công nghệ này mang lại tính minh bạch, bảo mật và hiệu quả cao hơn trong việc theo dõi và xác minh nguồn gốc sản phẩm từ khâu sản xuất đến tay người tiêu dùng.

Khảo sát nghiệp vụ này được thực hiện với mục tiêu nghiên cứu, đánh giá và tìm hiểu sâu hơn về bài toán ứng dụng Blockchain trong quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hoá. Chúng tôi muốn xác định những yêu cầu và nhu cầu của các doanh nghiệp, nhà sản xuất và các bên liên quan trong việc sử dụng Blockchain, đồng thời tìm hiểu về những thách thức và vấn đề mà họ đang gặp phải.

Phạm vi của khảo sát bao gồm:

* Khảo sát quy trình chuỗi cung ứng: Chúng tôi sẽ tìm hiểu về cách vận hành của chuỗi cung ứng, các khâu sản xuất, vận chuyển, lưu trữ và phân phối hàng hóa.
* Xác định yêu cầu và nhu cầu sử dụng: Chúng tôi sẽ nghiên cứu và phân tích những yêu cầu cụ thể mà các doanh nghiệp đặt ra khi ứng dụng Blockchain vào quản lý chuỗi cung ứng. Điều này có thể bao gồm việc theo dõi nguồn gốc hàng hóa, quản lý dữ liệu minh bạch, giảm thiểu gian lận và tự động hóa quy trình thông qua hợp đồng thông minh (Smart Contract).
* Đánh giá thách thức và vấn đề hiện tại: Chúng tôi sẽ tìm hiểu những thách thức và vấn đề mà các doanh nghiệp đang gặp phải khi triển khai công nghệ Blockchain vào chuỗi cung ứng. Những vấn đề có thể liên quan đến chi phí đầu tư, khả năng mở rộng, tích hợp với hệ thống hiện có, tính bảo mật và tốc độ giao dịch.
* Tìm hiểu tiềm năng và lợi ích: Chúng tôi sẽ nghiên cứu các lợi ích mà Blockchain có thể mang lại, bao gồm nâng cao độ tin cậy và minh bạch trong chuỗi cung ứng, giảm chi phí vận hành, tối ưu hóa quy trình kiểm tra và xác thực hàng hóa.

Mục tiêu cuối cùng của khảo sát nghiệp vụ này là đề xuất các giải pháp và khung phát triển hợp lý cho việc ứng dụng Blockchain vào quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hoá, giúp các doanh nghiệp nâng cao hiệu quả hoạt động, tăng tính cạnh tranh và đáp ứng các yêu cầu ngày càng cao của thị trường.

## Thực trang trong quản lý chuỗi cung ứng và truy suất nguồn gốc hàng hoá

Hiện nay, việc quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hóa đang gặp phải nhiều thách thức, bao gồm:

* Quy trình quản lý thủ công: Nhiều doanh nghiệp vẫn sử dụng phương pháp ghi chép thủ công hoặc hệ thống không đồng bộ, dẫn đến khó khăn trong việc theo dõi và xác minh thông tin hàng hóa.
* Thiếu minh bạch và dễ bị giả mạo: Hàng giả, hàng nhái và gian lận trong chuỗi cung ứng là vấn đề nghiêm trọng, gây mất niềm tin cho người tiêu dùng và đối tác kinh doanh.
* Hạn chế trong chia sẻ dữ liệu: Việc chia sẻ dữ liệu giữa các bên trong chuỗi cung ứng còn nhiều hạn chế, thiếu sự đồng bộ và dễ xảy ra sai sót.
* Khó khăn trong tuân thủ quy định: Các doanh nghiệp phải đáp ứng nhiều tiêu chuẩn và quy định khác nhau về xuất xứ, an toàn thực phẩm, môi trường, nhưng việc quản lý và chứng minh tuân thủ còn phức tạp.
* Tốc độ xử lý và truy xuất thông tin chậm: Hệ thống truyền thống thường mất nhiều thời gian để truy xuất thông tin sản phẩm từ nhà sản xuất đến điểm bán hàng.

## Khảo sát nghiệp vụ

### Kết quả khảo sát

|  |  |
| --- | --- |
| **Câu 1:** Xin vui lòng giới thiệu về doanh nghiệp của ông/bà, bao gồm lĩnh vực hoạt động và quy mô. | **Trả lời:** |
| **Câu 2:** Doanh nghiệp hiện đang quản lý chuỗi cung ứng theo phương thức nào? | **Trả lời:** |
| **Câu 3:** Những khó khăn lớn nhất trong việc quản lý chuỗi cung ứng của doanh nghiệp là gì? | **Trả lời:** |
| **Câu 4:** Hiện tại, doanh nghiệp có yêu cầu truy xuất nguồn gốc sản phẩm không? | **Trả lời:** |
| **Câu 5:** Doanh nghiệp đang sử dụng phương pháp nào để lưu trữ thông tin truy xuất nguồn gốc? | **Trả lời:** |
| **Câu 6:** Những thông tin nào doanh nghiệp đang theo dõi trong hệ thống truy xuất nguồn gốc? | **Trả lời:** |
| **Câu 7:** Doanh nghiệp có gặp khó khăn khi chia sẻ dữ liệu chuỗi cung ứng với đối tác không? | **Trả lời:** |
| **Câu 8:** Doanh nghiệp có từng tìm hiểu về blockchain trong quản lý chuỗi cung ứng chưa? | **Trả lời:** |
| **Câu 9:** Blockchain có thể giúp ích gì cho doanh nghiệp của ông/bà? | **Trả lời:** |
| **Câu 10**: Những rào cản nào khiến doanh nghiệp chưa ứng dụng blockchain? | **Trả lời:** |
| **Câu 11:** Nếu có giải pháp blockchain phù hợp, doanh nghiệp có sẵn sàng triển khai không? | **Trả lời:** |

### Kết quả khảo sát

|  |  |
| --- | --- |
| **Câu 1:** Xin vui lòng giới thiệu về doanh nghiệp của ông/bà, bao gồm lĩnh vực hoạt động và quy mô. | **Trả lời:** Doanh nghiệp chúng tôi hoạt động trong lĩnh vực phân phối thực phẩm hữu cơ với mạng lưới gồm 50 nhà cung cấp và hơn 200 điểm bán lẻ trên toàn quốc. |
| **Câu 2:** Doanh nghiệp hiện đang quản lý chuỗi cung ứng theo phương thức nào? | **Trả lời:** Hiện tại, chúng tôi sử dụng hệ thống ERP kết hợp với ghi chép truyền thống để theo dõi hàng hóa. |
| **Câu 3:** Những khó khăn lớn nhất trong việc quản lý chuỗi cung ứng của doanh nghiệp là gì? | **Trả lời:** Thiếu minh bạch trong dữ liệu giữa các bên. Khó kiểm soát hàng giả, hàng nhái trên thị trường. Mất nhiều thời gian để xác minh nguồn gốc sản phẩm khi có khiếu nại từ khách hàng. |
| **Câu 4:** Hiện tại, doanh nghiệp có yêu cầu truy xuất nguồn gốc sản phẩm không? | **Trả lời:** Có. Khách hàng ngày càng quan tâm đến xuất xứ và chất lượng sản phẩm, đặc biệt là thực phẩm hữu cơ. |
| **Câu 5:** Doanh nghiệp đang sử dụng phương pháp nào để lưu trữ thông tin truy xuất nguồn gốc? | **Trả lời:** Mã QR Code trên bao bì sản phẩm. Ghi chép trong hệ thống nội bộ (không chia sẻ dữ liệu với đối tác). |
| **Câu 6:** Những thông tin nào doanh nghiệp đang theo dõi trong hệ thống truy xuất nguồn gốc? | **Trả lời:** Nguồn gốc nguyên liệu (nhà cung cấp, khu vực sản xuất). Quy trình kiểm định chất lượng trước khi phân phối. Hành trình vận chuyển từ nhà sản xuất đến cửa hàng. |
| **Câu 7:** Doanh nghiệp có gặp khó khăn khi chia sẻ dữ liệu chuỗi cung ứng với đối tác không? | **Trả lời:** Có. Dữ liệu hiện tại chủ yếu được quản lý riêng lẻ bởi từng công ty, gây khó khăn khi đối chiếu thông tin giữa các bên. |
| **Câu 8:** Doanh nghiệp có từng tìm hiểu về blockchain trong quản lý chuỗi cung ứng chưa? | **Trả lời:** Chúng tôi đã tìm hiểu nhưng chưa triển khai, vì còn lo ngại về chi phí và tính khả thi. |
| **Câu 9:** Blockchain có thể giúp ích gì cho doanh nghiệp của ông/bà? | **Trả lời:** Minh bạch hóa thông tin giữa các bên trong chuỗi cung ứng. Chống giả mạo dữ liệu, giúp bảo vệ thương hiệu trước vấn nạn hàng giả. Tăng niềm tin của khách hàng bằng hệ thống truy xuất nguồn gốc minh bạch. |
| **Câu 10:** Những rào cản nào khiến doanh nghiệp chưa ứng dụng blockchain? | **Trả lời:** Chi phí đầu tư ban đầu cao. Nhân sự chưa đủ kiến thức về blockchain. Chưa có quy định pháp lý rõ ràng về truy xuất nguồn gốc trên blockchain. |
| **Câu 11:** Nếu có giải pháp blockchain phù hợp, doanh nghiệp có sẵn sàng triển khai không? | **Trả lời:** Có, nếu chi phí hợp lý và dễ tích hợp với hệ thống hiện có. |

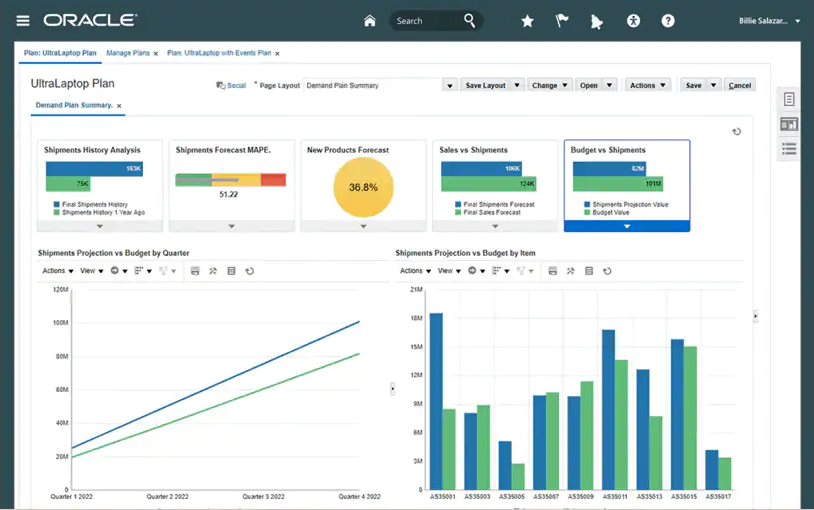
## So sánh các hình thức quản lý chuỗi cung ứng truy suất nguồn gốc hàng hoá khác

### Hình thức quản lý truyền thống

* Ghi chép thủ công: Doanh nghiệp sử dụng sổ sách hoặc hệ thống nội bộ để ghi lại thông tin về nguồn gốc, vận chuyển, lưu kho và phân phối hàng hoá. Việc này dễ dẫn đến sai sót, mất dữ liệu và khó kiểm tra khi cần.
* Giao tiếp qua trung gian: Dữ liệu thường được truyền đạt thông qua nhiều bên trung gian (như nhà cung cấp, đơn vị vận chuyển, nhà phân phối), dẫn đến chậm trễ và thiếu tính minh bạch.
* Lưu trữ dữ liệu phân tán: Mỗi bên trong chuỗi cung ứng có hệ thống quản lý riêng, gây khó khăn khi đồng bộ và xác minh thông tin.
* Rủi ro gian lận và giả mạo: Do dữ liệu không được bảo vệ và xác thực chặt chẽ, nguy cơ hàng giả, gian lận hoặc thay đổi thông tin trong chuỗi cung ứng là rất cao.
* Chi phí cao và khó mở rộng: Các hệ thống truyền thống thường yêu cầu nhiều nhân lực, thời gian để kiểm tra, xác nhận dữ liệu và tuân thủ quy định pháp lý.

### Hình thức quản lý qua Web 2.0

#### Oracle Supply Chain Management (SCM)



Hình 1.1 Hình ảnh Web Oracle Supply Chain Management

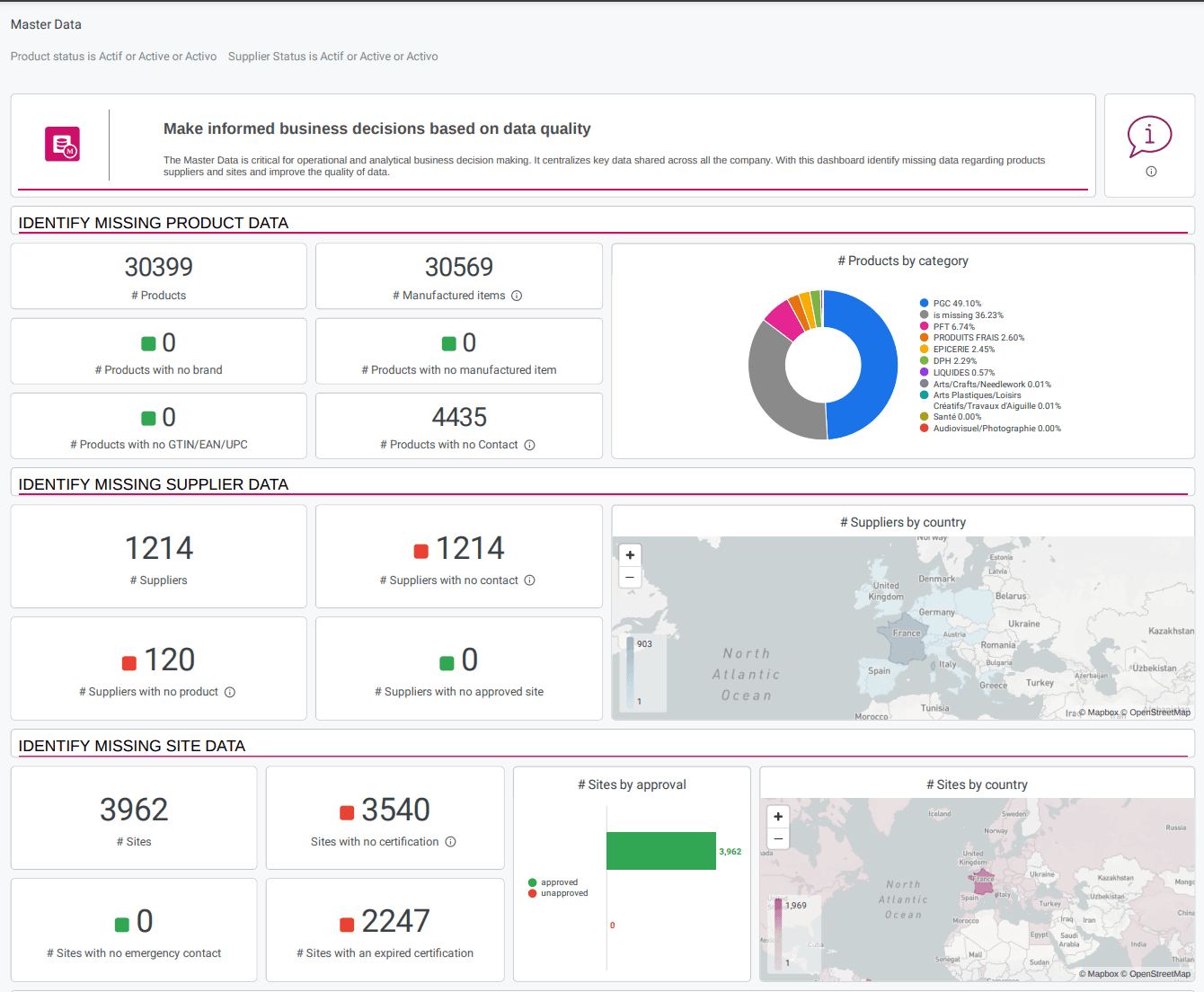
Ưu điểm:

* Tích hợp toàn diện: Oracle SCM Cloud cung cấp một giải pháp toàn diện cho quản lý chuỗi cung ứng, bao gồm lập kế hoạch, quản lý hàng tồn kho, logistics, mua sắm và sản xuất.
* Khả năng mở rộng linh hoạt: Là một nền tảng đám mây, Oracle SCM Cloud có thể dễ dàng mở rộng để phù hợp với quy mô doanh nghiệp từ nhỏ đến lớn mà không cần đầu tư nhiều vào hạ tầng.
* Tự động hoá và tối ưu hoá: Hệ thống giúp tự động hoá nhiều quy trình trong chuỗi cung ứng, giảm thiểu sai sót thủ công và tối ưu hoá hiệu suất vận hành.
* Phân tích dữ liệu mạnh mẽ: Oracle SCM Cloud sử dụng AI và phân tích dữ liệu để cung cấp thông tin chuyên sâu giúp cải thiện ra quyết định.
* Tích hợp tốt với các hệ thống khác: Có thể kết nối với ERP, CRM và các công cụ khác để đảm bảo luồng thông tin xuyên suốt.
* Bảo mật cao: Dữ liệu được lưu trữ trên nền tảng đám mây với các tiêu chuẩn bảo mật nghiêm ngặt của Oracle.

Nhược điểm:

* Chi phí cao: Oracle SCM Cloud là một giải pháp mạnh mẽ nhưng đi kèm với chi phí triển khai và vận hành không hề rẻ, có thể là rào cản đối với các doanh nghiệp nhỏ.
* Yêu cầu kỹ năng kỹ thuật: Việc triển khai và quản lý hệ thống có thể phức tạp, đòi hỏi đội ngũ IT có kinh nghiệm.
* Phụ thuộc vào kết nối internet: Vì là một nền tảng đám mây, hệ thống yêu cầu kết nối internet ổn định để hoạt động hiệu quả.
* Tuỳ chỉnh hạn chế: So với các giải pháp tùy chỉnh theo nhu cầu doanh nghiệp, Oracle SCM Cloud có thể gặp một số hạn chế trong việc tùy chỉnh sâu.

#### Quản lý qua TraceOne



Hình 1.2. Hình ảnh quản lý qua TraceOne

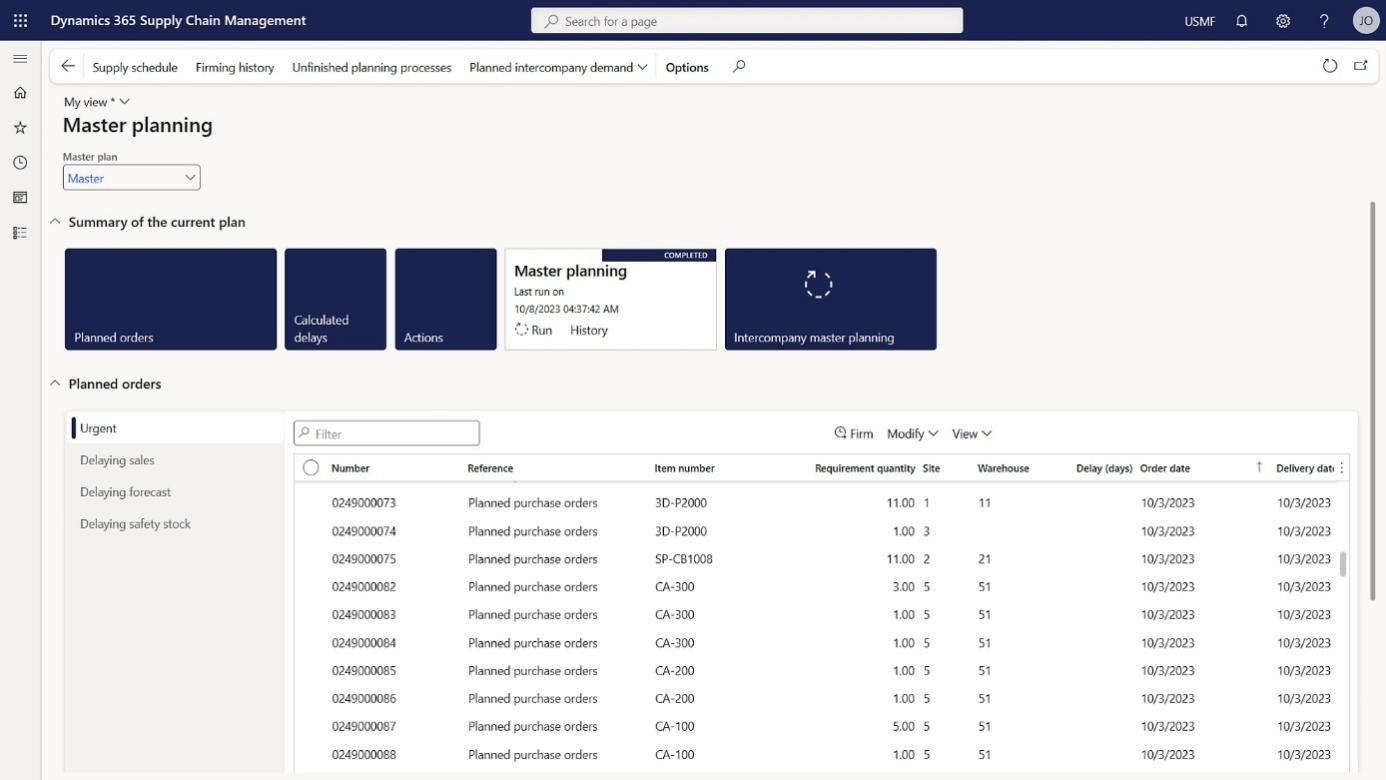
Ưu điểm:

* Minh bạch và truy xuất nguồn gốc: Trace One cung cấp khả năng theo dõi và truy xuất nguồn gốc sản phẩm từ nguyên liệu đầu vào đến thành phẩm, giúp nâng cao độ tin cậy và tuân thủ quy định.
* Cải thiện quản lý nhà cung cấp: Hệ thống giúp doanh nghiệp quản lý mối quan hệ với nhà cung cấp hiệu quả hơn, đảm bảo chất lượng và tính nhất quán của nguyên vật liệu.
* Hỗ trợ tuân thủ quy định: Trace One giúp doanh nghiệp đáp ứng các tiêu chuẩn an toàn thực phẩm, kiểm định chất lượng và các quy định pháp lý khác.
* Tự động hóa quy trình: Hệ thống giảm bớt công việc thủ công trong việc theo dõi dữ liệu sản phẩm, giúp tiết kiệm thời gian và giảm thiểu sai sót.
* Giao diện trực quan và dễ sử dụng: Người dùng có thể dễ dàng truy cập và quản lý thông tin qua nền tảng Trace One mà không cần quá nhiều kiến thức kỹ thuật.
* Cải thiện hiệu suất chuỗi cung ứng: Nhờ vào việc chia sẻ thông tin minh bạch, các bên liên quan trong chuỗi cung ứng có thể phối hợp tốt hơn, tối ưu hóa thời gian giao hàng và quản lý hàng tồn kho.

Hạn chế:

* Chi phí sử dụng cao: Trace One có thể có chi phí đăng ký và vận hành cao, đặc biệt đối với các doanh nghiệp vừa và nhỏ.
* Phụ thuộc vào nền tảng đám mây: Hệ thống hoạt động trực tuyến, nên cần có kết nối internet ổn định để đảm bảo hiệu suất làm việc.
* Khả năng tùy chỉnh hạn chế: Mặc dù hỗ trợ nhiều tính năng, nhưng một số doanh nghiệp có nhu cầu đặc thù có thể gặp khó khăn trong việc tùy chỉnh hệ thống theo yêu cầu riêng.
* Yêu cầu đào tạo ban đầu: Người dùng cần được đào tạo để tận dụng hết các tính năng của Trace One, điều này có thể mất thời gian và nguồn lực ban đầu.

#### Quản lý qua Microsoft Dynamics 365 Supply Chain Management



Hình 1.3. Hình ảnh quản lý Microsoft Dynamics 365 Supply Chain Management

Ưu điểm:

* Tích hợp toàn diện: Hệ thống kết nối dễ dàng với các giải pháp khác của Microsoft như Azure, Power BI, Office 365, giúp quản lý chuỗi cung ứng hiệu quả và thống nhất.
* Tự động hoá và tối ưu hoá quy trình: Công nghệ AI và IoT (Internet of Thing) giúp tự động hoá các hoạt động quản lý kho, sản xuất và vận chuyển, giảm sai sót và tối ưu năng suất.
* Dự báo nhu cầu chính xác: Sử dụng AI và phân tích dữ liệu để dự đoán nhu cầu hàng hoá, giúp doanh nghiệp chuẩn bị hàng tồn kho hợp lý và tránh tình trạng thiếu hụt hoặc dư thừa.
* Quản lý kho thông minh: Hỗ trợ theo dõi hàng tồn kho theo thời gian thực, giúp nâng cao độ chính xác và hiệu suất vận hành kho.
* Khả năng mở rộng cao: Phù hợp cho cả doanh nghiệp vừa và lớn, có thể dễ dàng mở rộng tính năng và quy mô sử dụng khi cần thiết.
* Tuân thủ quy định và bảo mật: Được xây dựng trên nền tảng đám mây Microsoft Azure, đảm bảo tuân thủ các tiêu chuẩn bảo mật và quy định quốc tế về dữ liệu.

Hạn chế:

* Chi phí cao: Hệ thống có chi phí triển khai và bảo trì khá lớn, không phù hợp với các doanh nghiệp nhỏ hoặc startup.
* Yêu cầu đào tạo chuyên sâu: Nhân sự cần được đào tạo bài bản để sử dụng tối ưu các tính năng nâng cao của hệ thống.
* Cấu hình phức tạp: Quá trình triển khai và tùy chỉnh có thể mất nhiều thời gian do hệ thống có nhiều tính năng phức tạp.
* Phụ thuộc vào đám mây: Dù cung cấp nhiều lợi ích, nhưng việc vận hành trên nền tảng đám mây cũng đòi hỏi kết nối internet ổn định để đảm bảo hiệu suất.

## Công nghệ sử dụng

### Next.js

1. **Giới thiệu**

Next.js là một framework React mạnh mẽ, được phát triển bởi Vercel, giúp xây dựng các ứng dụng web hiện đại với khả năng render phía server (SSR - Server-Side Rendering) và tạo trang tĩnh (SSG - Static Site Generation). Next.js hỗ trợ tối ưu hóa SEO, tự động chia nhỏ mã (code-splitting), và có hệ thống routing linh hoạt.

1. **Mục đích sử dụng**

Next.js được sử dụng để phát triển các ứng dụng web nhanh chóng, hiệu quả, hỗ trợ cả client-side rendering (CSR), server-side rendering (SSR) và static site generation (SSG). Nó đặc biệt hữu ích cho các website có yêu cầu cao về SEO, hiệu năng và trải nghiệm người dùng.

### MeshJS và Cbor

1. **Giới thiệu**

**MeshJS** là một thư viện JavaScript giúp tương tác với blockchain Cardano một cách dễ dàng. Nó cung cấp các công cụ để tạo, ký và gửi giao dịch, cũng như truy xuất dữ liệu từ blockchain một cách hiệu quả. MeshJS đặc biệt hữu ích cho các nhà phát triển DApp trên Cardano. **CBOR (Concise Binary Object Representation)** là một định dạng dữ liệu nhị phân được thiết kế để nhỏ gọn và hiệu quả, thường được sử dụng trong Blockchain để mã hoá giao dịch và dữ liệu. Trên Cardano, CBOR được sử dụng để biểu diễn các giao dịch nhằm giảm kích thước và tối ưu hóa hiệu suất.

1. **Mục đích sử dụng**

**MeshJS** được sử dụng để xây dựng các ứng dụng phi tập trung (DApp) trên Cardano, hỗ trợ quản lý ví, ký giao dịch, và tương tác với smart contracts. **CBOR** giúp tối ưu hóa việc lưu trữ và truyền tải dữ liệu trong các giao dịch blockchain, giúp giảm chi phí và cải thiện hiệu suất mạng.

### Aiken và Plutus

1. **Giới thiệu**

**Aiken** là một ngôn ngữ lập trình và bộ công cụ dành cho hợp đồng thông minh trên blockchain Cardano. Nó được thiết kế để tối ưu hóa hiệu suất, độ an toàn và đơn giản hóa quá trình phát triển hợp đồng thông minh so với Plutus. **Plutus** là ngôn ngữ lập trình hợp đồng thông minh chính thức của Cardano, dựa trên Haskell. Nó cung cấp các công cụ mạnh mẽ để viết, kiểm tra và triển khai hợp đồng thông minh trên mạng Cardano.

1. **Mục đích sử dụng**

**Aiken** giúp các nhà phát triển viết hợp đồng thông minh dễ dàng hơn, với cú pháp đơn giản và hiệu suất cao hơn.**Plutus** cung cấp khả năng lập trình mạnh mẽ và linh hoạt, cho phép tạo ra các hợp đồng thông minh phức tạp với mức độ bảo mật cao.

### Postgresql và Prisma

1. Giới thiệu

**PostgreSQL** là một hệ quản trị cơ sở dữ liệu quan hệ (RDBMS) mã nguồn mở, mạnh mẽ và có khả năng mở rộng cao. Nó hỗ trợ các tính năng tiên tiến như giao dịch ACID, truy vấn SQL linh hoạt, và mở rộng thông qua các extension. **Prisma** là một ORM (Object-Relational Mapping) hiện đại, hỗ trợ TypeScript và JavaScript, giúp đơn giản hóa việc làm việc với cơ sở dữ liệu như PostgreSQL, MySQL, và SQLite. Prisma cung cấp các công cụ mạnh mẽ để thao tác dữ liệu với cách tiếp cận trực quan và an toàn.

### Mục đích sử dụng

**PostgreSQL** được sử dụng để lưu trữ dữ liệu an toàn, hỗ trợ truy vấn phức tạp và tối ưu hóa hiệu suất trong các hệ thống web. **Prisma** giúp lập trình viên dễ dàng quản lý và truy vấn dữ liệu với PostgreSQL, cung cấp các API mạnh mẽ để xử lý dữ liệu một cách hiệu quả và an toàn.

## Kết luận

### Giới thiệu

**Aiken** là một ngôn ngữ lập trình và bộ công cụ dành cho hợp đồng thông minh trên blockchain Cardano. Nó được thiết kế để tối ưu hóa hiệu suất, độ an toàn và đơn giản hóa quá trình phát triển hợp đồng thông minh so với Plutus. **Plutus** là ngôn ngữ lập trình hợp đồng thông minh chính thức của Cardano, dựa trên Haskell. Nó cung cấp các công cụ mạnh mẽ để viết, kiểm tra và triển khai hợp đồng thông minh trên mạng Cardano.

### Mục đích sử dụng

**Aiken** giúp các nhà phát triển viết hợp đồng thông minh dễ dàng hơn, với cú pháp đơn giản và hiệu suất cao hơn.**Plutus** cung cấp khả năng lập trình mạnh mẽ và linh hoạt, cho phép tạo ra các hợp đồng thông minh phức tạp với mức độ bảo mật cao.

Dựa trên khảo sát nghiệp vụ về quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hóa, chúng tôi nhận thấy một số vấn đề quan trọng sau:

* Hiện tại, việc theo dõi và xác minh nguồn gốc hàng hóa vẫn gặp nhiều khó khăn do quy trình quản lý truyền thống còn rời rạc, thiếu minh bạch và dễ bị sai sót.
* Cần có một giải pháp hiện đại giúp cải thiện tính minh bạch, giảm gian lận và nâng cao độ tin cậy trong chuỗi cung ứng.
* Doanh nghiệp cần một hệ thống có khả năng lưu trữ và truy xuất dữ liệu một cách an toàn, không thể thay đổi, nhằm đảm bảo chất lượng và xuất xứ hàng hóa.
* Nhu cầu về một nền tảng có thể tự động hóa quy trình giám sát, cập nhật thông tin theo thời gian thực và cung cấp dữ liệu chính xác cho các bên liên quan ngày càng tăng.
* Việc tuân thủ các tiêu chuẩn và quy định về an toàn thực phẩm, môi trường và chất lượng sản phẩm là yếu tố quan trọng, đòi hỏi một hệ thống có thể hỗ trợ giám sát và báo cáo một cách hiệu quả.

Dựa trên những nhu cầu trên, ứng dụng công nghệ Blockchain vào quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hóa có thể là một giải pháp tối ưu. Công nghệ này giúp đảm bảo dữ liệu minh bạch, bảo mật và dễ dàng truy xuất, giúp các doanh nghiệp nâng cao khả năng quản lý, tối ưu hóa chuỗi cung ứng và xây dựng lòng tin với khách hàng.

# **CHƯƠNG 2. PHÂN TÍCH THIẾT KẾ HỢP ĐỒNG THÔNG MINH CỦA ỨNG DỤNG**

## 2.1. Công nghệ áp dụng

### a. Khái niệm

CIP-68 là một tiêu chuẩn trên blockchain Cardano nhằm mở rộng khả năng lưu trữ và cập nhật metadata của các tài sản như NFT và token một cách linh hoạt hơn. Khác với CIP-25, nơi metadata được lưu trữ cố định trong transaction metadata, CIP-68 sử dụng **datum** để chứa metadata, cho phép cập nhật và kiểm tra thông tin thông qua smart contract. Điều này giúp metadata có thể thay đổi mà không làm thay đổi chính tài sản gốc, đồng thời bảo đảm tính minh bạch và khả năng xác minh thông tin trên blockchain.

CIP-68 sử dụng hai loại token chính để quản lý dữ liệu:

* **Reference NFT (Label 100):** Chứa metadata trong datum và có thể được kiểm soát bởi smart contract, cho phép cập nhật và truy vấn thông tin.
* **User Token:** Đại diện cho tài sản mà người dùng sở hữu, nhưng không chứa metadata.

Việc tách biệt metadata và tài sản gốc giúp đảm bảo rằng thông tin có thể được cập nhật một cách an toàn và dễ dàng, đồng thời giữ nguyên lịch sử và nguồn gốc của tài sản trên blockchain.

### b. Luồng sử lý dữ liệu

Quá trình sử dụng và cập nhật dữ liệu theo CIP-68 bắt đầu với việc tạo một **Reference NFT (Label 100)**, kèm theo metadata được lưu trữ trong datum và một **User Token** đại diện cho tài sản mà người dùng sở hữu nhưng không chứa metadata. Smart contract sẽ kiểm soát **Reference NFT** để đảm bảo rằng metadata không bị sửa đổi sai quy tắc, giúp bảo vệ tính toàn vẹn của dữ liệu. Khi người dùng hoặc hệ thống cần kiểm tra thông tin về tài sản, họ chỉ cần truy vấn datum của **Reference NFT** trên blockchain, từ đó xác minh nguồn gốc sản phẩm, theo dõi trạng thái hoặc hiển thị thông tin trong ứng dụng.

Khi metadata cần cập nhật (ví dụ: cập nhật trạng thái của sản phẩm trong chuỗi cung ứng), một giao dịch mới sẽ được thực hiện để thay thế datum của **Reference NFT** mà không ảnh hưởng đến chính tài sản gốc. Các smart contract có thể đặt ra quy tắc kiểm soát chặt chẽ, chẳng hạn như chỉ cho phép nhà sản xuất hoặc bên được ủy quyền có quyền thay đổi metadata. Đồng thời, khi **User Token** được chuyển từ người này sang người khác, **Reference NFT** vẫn giữ nguyên metadata của mình, giúp bảo vệ thông tin về nguồn gốc và lịch sử của tài sản mà không làm thay đổi dữ liệu quan trọng. Cuối cùng, bất kỳ ai cũng có thể xác minh thông tin metadata thông qua việc tra cứu **Reference NFT** trên blockchain, giúp đảm bảo tính minh bạch và chống giả mạo. Smart contract cũng có thể tự động kiểm tra tính hợp lệ của metadata, từ chối giao dịch nếu dữ liệu không đúng hoặc không hợp lệ, góp phần bảo vệ quy trình và bảo đảm chất lượng.

## 2.2. Thiết kế các điều kiện của hợp đồng thông minh

Thiết kế hợp đồng thông minh để đáp ứng nhu cầu của người dùng phải dựa trên những phát hiện thu thập được thông qua khảo sát, đảm bảo tích hợp các tính năng cần thiết và giải quyết trực tiếp các yêu cầu đã xác định. Trong trường hợp ứng dụng quản lý ứng dụng quản lý chuỗi cung ứng truy suất nguồn gốc hàng hóa thông qua Blockchain trên hệ sinh thái Cardano, khảo sát người dùng đã chỉ ra rằng các tính năng quan trọng như Mint (tạo sản phẩm mới), Burn (xóa các tài sản không dùng đến hoặc đã được sử dụng) và Update (cập nhật siêu dữ liệu hoặc thông tin liên quan đến sản phẩm) là cần thiết để phục vụ tốt hơn các nhu cầu thực tế. Do đó, ứng dụng sẽ được xây dựng với các tính năng này, giúp người dùng không chỉ dễ dàng tạo phẩm mà còn quản lý và chỉnh sửa chúng một cách linh hoạt, đáp ứng các trường hợp sử dụng cụ thể và cải thiện trải nghiệm tổng thể dễ dang kiếm soát và truy suất nguồn gốc một cách dễ dàng kiểm soát. Với các yêu cầu trên, hai hợp đồng thông minh (Mint và Store) được tạo ra để giúp đáp ứng các yêu cầu của sản phẩm.

### 2.1.1. Hợp đồng thông minh để tạo sản phẩm

Hợp đồng đúc tài sản trong CIP 68 đảm bảo việc tạo ra các tài sản duy nhất bằng cách tách Tài sản tham chiếu và Tài sản người dùng để tăng cường bảo mật, minh bạch và khả năng mở rộng. Trong hợp đồng này, có các đầu vào và đầu ra cụ thể như Tham số, Dữ liệu và Người đổi thưởng được trình bày như sau.

Tham số (Parameters):

* Địa chỉ phí nền tảng: Đây là địa chỉ ví mà người dùng sẽ phải gửi tiền để trả phí bảo trì nền tảng khi thực hiện giao dịch trên nền tảng. Địa chỉ này thường được sử dụng để thu phí nền tảng khi người dùng tương tác với hợp đồng thông minh hoặc thực hiện các hoạt động như tạo, cập nhật hoặc xoá sản phẩm.
* Phí nền tảng: Phí này là số tiền tối thiểu mà người dùng cần phải trả cho sàn giao dịch mỗi khi thực hiện giao dịch. Phí này được sử dụng để duy trì hoạt động của nền tảng, bảo mật giao dịch và đảm bảo tính ổn định trong hệ sinh thái. Phí này có thể được tính theo phần trăm hoặc một số tiền cố định, tuỳ thuộc vào các điều khoản của sàn giao dịch.
* Địa chỉ lưu trữ: Đây là địa chỉ lưu trữ các mã thông báo tham chiếu trong sản phẩm được đúc theo CIP-68. Tất cả sản phẩm tham chiếu của người dùng sẽ được lưu trữ tại địa chỉ này, giúp đảm bảo tính toàn vẹn và bảo mật của các mã thông báo. Địa chỉ lưu trữ này cũng giúp người dùng và hệ thống kiểm tra trạng thái và siêu dữ liệu của Tài sản khi cần thiết và hỗ trợ cập nhật và quản lý thông tin của các Tài sản này.

Dữ liệu được lưu (Datum): Không có dữ liệu

Điều kiện chuộc lại sản phẩm: Trình xác thực này được chia thành 2 trình xác thực cụ thể làm điều kiện để thực hiện 2 chức năng chính: Tạo và xóa sản phẩm trên Blockchain Cardano.

Điều kiện để tạo sản phẩm trên hợp đồng:

* Được ký bởi tác giả: Khi người dùng tạo một sản phẩm, dữ liệu trình xác thực trong hồ sơ chứa trường tác giả và người dùng phải cung cấp chữ ký để xác định rằng đây là tác giả đã đúc tài sản. Điều kiện này được đáp ứng bằng cách so sánh chữ ký đã nhập với dữ liệu trình xác thực trong hồ sơ.
* Kiểm tra phí nền tảng: Kiểm tra đầu ra giao dịch để đảm bảo rằng có tồn tại UTxO chứa phí tối thiểu của sàn giao dịch và được gửi đến địa chỉ sàn giao dịch được chỉ định trong các tham số.
* Kiểm tra siêu dữ liệu định dạng: Kiểm tra đầu ra giao dịch để đảm bảo rằng có tồn tại UTxO chứa phí tối thiểu của sàn giao dịch và được gửi đến địa chỉ sàn giao dịch được chỉ định trong các tham số.
* Số lượng giao dịch đầu ra: số lượng đầu ra UTxO bằng bốn trong đó một UTxO cho địa chỉ phí nền tảng, một UTxO cho địa chỉ xác thực cửa hàng chứa tài sản tham chiếu và 2 địa chỉ người nhận UTxO trong đó 1 UTxO chứa tài sản của người dùng.
* Kiểm tra địa chỉ cửa hàng: Kiểm tra xem tham chiếu tài sản được gửi đến một địa chỉ có phải là địa chỉ xác thực cửa hàng hay không.

Điều kiện để xóa sản phẩm trên hợp đồng:

* Được ký bởi tác giả: Khi người dùng thực hiện ghi tài sản, dữ liệu xác thực lưu trữ sẽ chứa trường tác giả và người dùng phải cung cấp chữ ký để xác định rằng đây là tác giả đã thực hiện giao dịch ghi tài sản. Điều kiện này được triển khai bằng cách so sánh chữ ký đã nhập với dữ liệu xác thực lưu trữ.
* Số lượng giao dịch đầu ra: Giao dịch đầu ra là 2 (1 UTxO của địa chỉ trao đổi và 1 UTxO của địa chỉ người nhận).
* Kiểm tra phí nền tảng: Kiểm tra xem số lượng ADA được gửi đến sàn giao dịch có lớn hơn hoặc bằng số lượng ADA được chỉ định trong các tham số xác thực hay không.
* Kiểm tra số lượng: Kiểm tra xem số lượng mã thông báo người dùng mà người gửi muốn ghi có hợp lệ và không vượt quá số lượng họ sở hữu hay không.
* Kiểm tra ADA được đính kèm: Kiểm tra xem ADA được đính kèm với mã thông báo tham chiếu sẽ đi đến đâu (đến ví mà người dùng hiện đang sở hữu).
* Kiểm tra số lượng đốt: Tác giả sẽ đốt cả hai tài sản (Mã thông báo người dùng, Mã thông báo tham chiếu) với số lượng đã cho.

### 2.1.2. Hợp đồng thông minh để cập nhật thông tin của sản phẩm

Sau khi tài sản được đúc thành công trong cơ chế CIP-68, Tài sản tham chiếu được gửi đến Store Validator để lưu trữ. Đây là một bước quan trọng trong quy trình, vì Store Validator hoạt động như một "hộp an toàn" lưu trữ siêu dữ liệu bất biến của tài sản, đảm bảo rằng nó luôn có sẵn để tham chiếu bất cứ khi nào cần. Store Validator không chỉ lưu trữ Tài sản tham chiếu mà còn hoạt động như một công cụ để thực hiện cập nhật siêu dữ liệu cho tài sản thông qua cơ chế.

Tham số (Parameter):

* Địa chỉ phí nền tảng: Đây là địa chỉ ví mà người dùng sẽ phải gửi tiền để trả phí bảo trì nền tảng khi thực hiện giao dịch trên nền tảng. Địa chỉ này thường được sử dụng để thu phí nền tảng khi người dùng tương tác với hợp đồng thông minh hoặc thực hiện các hoạt động như đúc, đốt, cập nhật hoặc xóa tài sản.
* Phí nền tảng: Phí này là số tiền tối thiểu mà người dùng cần phải trả cho sàn giao dịch mỗi khi thực hiện giao dịch. Phí này được sử dụng để duy trì hoạt động của nền tảng, bảo mật giao dịch và đảm bảo tính ổn định trong hệ sinh thái. Phí này có thể được tính theo tỷ lệ phần trăm hoặc một số tiền cố định, tùy thuộc vào các điều khoản của sàn giao dịch.

Dữ liệu được lưu trữ (Datum): Dưới đây là mô tả chi tiết về các trường siêu dữ liệu được xác định trong dữ liệu đính kèm vào UTxO được gửi đến trình xác thực cửa hàng:

* Tên: Trường này lưu trữ tên của tài sản. Đây là tên mà người dùng sẽ thấy khi truy cập thông tin của tài sản đó. Ví dụ: "CIP 68 Generator", v.v.
* Hình ảnh: Trường này chứa URL hoặc địa chỉ lưu trữ của hình ảnh đại diện cho tài sản. Đây là hình ảnh mà người dùng sẽ thấy khi xem hoặc tương tác với NFT. Hình ảnh có thể là hình ảnh, hình minh họa, biểu tượng hoặc thậm chí là video đại diện cho NFT.
* Loại phương tiện: Trường này lưu trữ loại hình ảnh hoặc phương tiện có trong trường hình ảnh. Các giá trị của trường này có thể bao gồm các định dạng hình ảnh (png, jpg, gif) hoặc định dạng video/âm thanh (mp4, mp3, v.v.). Trường này giúp hệ thống nhận dạng và xử lý đúng loại dữ liệu khi người dùng tương tác với NFT.
* Tác giả: Trường này lưu trữ địa chỉ của người tạo (hoặc nhà xuất bản) tài sản. Ngoài việc là thông tin về người tạo ra tài sản, trường này còn đóng vai trò quan trọng trong việc kiểm tra quyền sử dụng và sở hữu tài sản. Điều này đảm bảo rằng người dùng chỉ có thể sử dụng hoặc phân phối tài sản mà họ sở hữu hoặc đã được cấp phép.

Điều kiện chuộc lại sản phẩm (Redeemer): Trong trình xác thực này, có 2 trình xác thực cụ thể làm điều kiện để thực hiện 2 chức năng chính: Cập nhật và Xóa (Tham gia vào quá trình Đốt) tài sản.

Cập nhật:

* Được ký bởi tác giả: Khi người dùng cập nhật tài sản, có một trường tác giả trong dữ liệu trình xác thực lưu trữ. Đồng thời, người dùng cũng phải cung cấp chữ ký để cập nhật các trường trong dữ liệu để thay đổi siêu dữ liệu của tài sản.
* Số lượng giao dịch đầu ra: Kiểm tra đầu ra giao dịch có số lượng là 3 (1 UTxO được gửi đến trình xác thực lưu trữ, 1 UTxO được gửi đến địa chỉ trao đổi và UTxO là địa chỉ của tác giả).
* Kiểm tra địa chỉ lưu trữ: Kiểm tra xem mã thông báo tham chiếu được sử dụng để thay đổi siêu dữ liệu có tồn tại và được gửi đến địa chỉ của trình xác thực lưu trữ hay không.
* Kiểm tra siêu dữ liệu định dạng: Kiểm tra xem các trường được chỉ định như tên, hình ảnh, loại phương tiện và tác giả có tồn tại trong dữ liệu trình xác thực lưu trữ (hay còn gọi là siêu dữ liệu tài sản) hay không. Các trường này là bắt buộc. Không thể thay đổi giá trị tác giả.
* Kiểm tra phí nền tảng: Kiểm tra đầu ra giao dịch để xem UTxO có chứa phí trao đổi tối thiểu và được gửi đến địa chỉ trao đổi được chỉ định trong các tham số hay không.
* Kiểm tra mã thông báo tham chiếu: Kiểm tra tài sản tham chiếu để cập nhật siêu dữ liệu có trong đầu ra giao dịch.

Xóa:

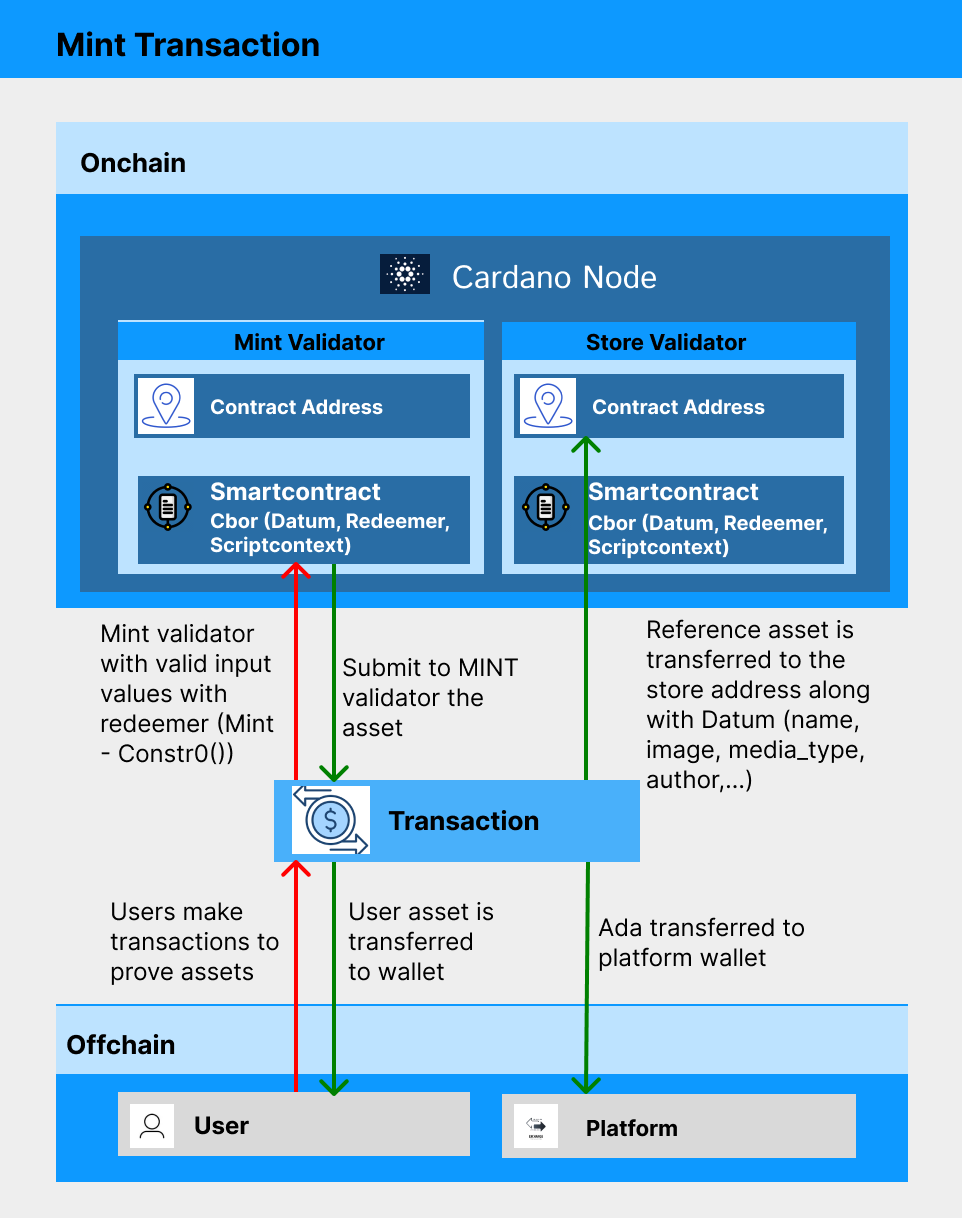
* Được ký bởi tác giả: Khi người dùng xóa một tài sản, dữ liệu xác thực lưu trữ sẽ chứa trường tác giả và người dùng phải cung cấp chữ ký để xác định rằng đây là tác giả đã thực hiện giao dịch đúc tài sản. Điều kiện này được đáp ứng bằng cách so sánh chữ ký đã nhập với dữ liệu xác thực lưu trữ.
* Kiểm tra phí nền tảng: Kiểm tra đầu ra giao dịch để đảm bảo rằng có tồn tại một UTxO chứa phí nền tảng tối thiểu và được gửi đến địa chỉ nền tảng được chỉ định trong các tham số.
* Đầu ra giao dịch số lượng: Đầu ra giao dịch có số lượng là 2 (1 UTxO của địa chỉ nền tảng, 1 UTxO của tác giả).

## 2.3. Phân tích các luồng xử lý dữ liệu của hợp đồng thông minh

Với các điều kiện được xác định trước, hợp đồng thông minh được cấu trúc thành ba chức năng cốt lõi nhằm quản lý toàn diện vòng đời của một đơn vị hàng hóa trong chuỗi cung ứng. Mỗi chức năng — **Mint**, **Burn** và **Update** — được thiết kế để đảm bảo rằng mỗi bước trong quá trình di chuyển và xử lý hàng hoá đều được ghi nhận một cách minh bạch, không thể chỉnh sửa, đồng thời hỗ trợ đầy đủ các yêu cầu về **truy xuất nguồn gốc** trong môi trường blockchain. Việc tuân thủ tiêu chuẩn **CIP-68** cho phép tách biệt metadata tĩnh và động, nhờ đó tăng tính linh hoạt trong việc cập nhật thông tin mà không làm thay đổi mã định danh của hàng hóa.

### 2.3.1. Chức năng tạo sản phẩm

Quá trình **đúc tài sản** là một phần quan trọng của tiêu chuẩn **CIP-68**, được thiết kế nhằm đảm bảo rằng mỗi tài sản được tạo ra đều phản ánh một nhu cầu thực tế và tuân thủ nghiêm ngặt các chính sách đã được thiết lập trong quá trình phát triển hợp đồng thông minh. Trong bối cảnh **quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hóa**, quá trình này giữ vai trò như điểm khởi đầu của chu trình theo dõi sản phẩm từ khi được sản xuất cho đến khi tới tay người tiêu dùng cuối cùng. Thay vì chỉ tạo ra tài sản một cách tuỳ tiện, hệ thống yêu cầu **xác minh trước nhu cầu đúc**, từ đó đảm bảo rằng mỗi NFT đại diện cho một đơn vị sản phẩm, lô hàng hoặc tài sản cụ thể trong chuỗi cung ứng. Nhờ áp dụng tiêu chuẩn **CIP-68**, tài sản số có thể được cấu trúc với **metadata tĩnh** (chứa thông tin không thay đổi như mã sản phẩm, nhà sản xuất, ngày sản xuất...) và **metadata động** (phản ánh các thông tin có thể thay đổi trong quá trình vận chuyển như vị trí, tình trạng, kiểm định chất lượng...).

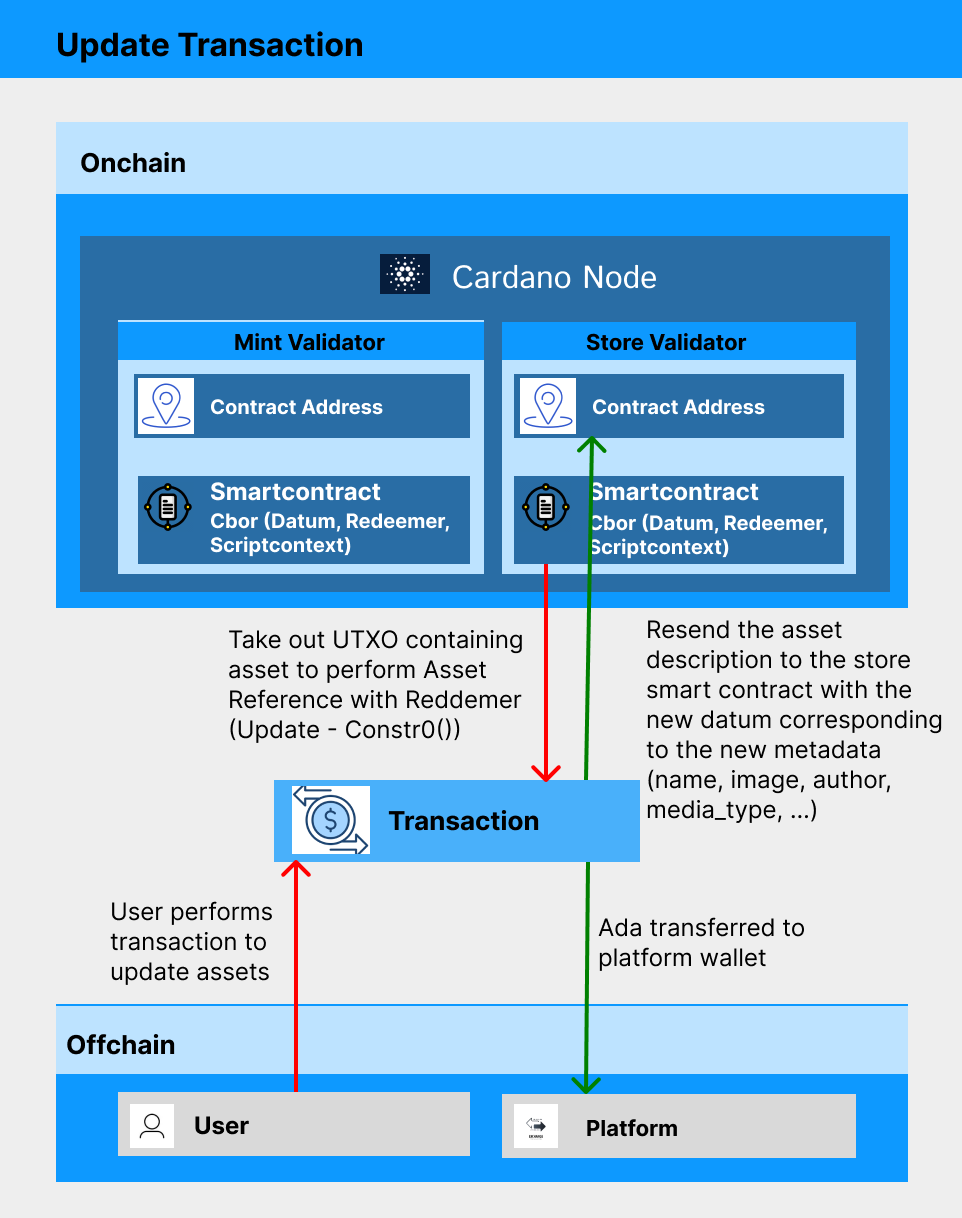


Trong hệ thống ứng dụng công nghệ blockchain để **quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hóa**, quá trình đúc tài sản không chỉ đơn giản là hành động tạo ra một NFT, mà là một phần trong chuỗi hoạt động có tổ chức,mang tính hệ thống cao. Mỗi bước được thiết kế nhằm đảm bảo sự minh bạch, an toàn, xác thực và dễ dàng kiểm tra lại thông tin trong suốt vòng đời sản phẩm – từ khâu sản xuất, vận chuyển đến tay người tiêu dùng cuối.

|  |  |  |
| --- | --- | --- |
| Bước | Tên bước | Mô tả chi tiết |
| 1 | Khởi tạo điều kiện – Thiết lập nền tảng xác thực | Người dùng, bao gồm nhà sản xuất, đơn vị kiểm định hoặc nhà phân phối, khởi động quá trình bằng cách truy cập vào nền tảng blockchain (qua dApp hoặc hệ thống quản lý chuỗi cung ứng). Trong bước này, họ cần:  - **Kết nối ví cá nhân** với nền tảng để hệ thống có thể xác minh danh tính và kiểm tra điều kiện đúc tài sản.  - **Xác thực danh tính:** Hệ thống đảm bảo người thực hiện có quyền tạo tài sản trên chuỗi cho lô hàng tương ứng, thông qua xác minh ví và quyền truy cập.  - **Kiểm tra điều kiện ví:** Bao gồm việc kiểm tra số dư trong ví có đủ để thanh toán phí mạng và chi phí đúc tài sản (ví dụ: lượng ADA cần thiết trong mạng Cardano).  Chỉ khi cả hai điều kiện trên được đảm bảo, giao dịch đúc tài sản mới được cho phép, ngăn chặn nguy cơ thao túng hoặc gian lận. Đây là nền tảng đảm bảo độ tin cậy cho toàn bộ chuỗi cung ứng. |
| 2 | Tạo tài sản – Xây dựng định danh số cho hàng hóa | Sau khi điều kiện được xác nhận, hệ thống tiến hành **đúc tài sản** trên blockchain theo tiêu chuẩn CIP-68. Có hai loại tài sản được tạo ra:  **(a) User Asset** – là định danh số đại diện cho chính sản phẩm vật lý. Tuỳ thuộc vào tính chất sản phẩm: • **NFT (Non-Fungible Token):** Dành cho hàng hóa độc nhất như máy móc, thiết bị điện tử, linh kiện chuyên biệt, hay hàng thủ công mỹ nghệ. • **FT (Fungible Token):** Phù hợp với sản phẩm sản xuất hàng loạt như thực phẩm đóng gói, đồ uống, hàng tiêu dùng. → Tài sản này thuộc sở hữu của người dùng và có thể luân chuyển trong hệ thống như sản phẩm vật lý.  **(b) Reference NFT** – đây là NFT đặc biệt dùng để chứa **metadata** (siêu dữ liệu) của sản phẩm: • Bao gồm thông tin như nơi sản xuất, thành phần, điều kiện bảo quản, tình trạng kiểm định, lịch sử vận chuyển,... • Được **khóa tại một địa chỉ có Plutus Script**, giúp hỗ trợ logic cập nhật metadata khi cần thiết mà không ảnh hưởng đến quyền sở hữu.  Việc chia metadata và asset riêng biệt giúp dễ dàng cập nhật, kiểm tra và minh bạch hóa dữ liệu. |
| 3 | Gửi và phân phối tài sản – Xác lập quyền sở hữu và lưu trữ thông tin | Sau khi đúc xong, hệ thống thực hiện **phân phối tài sản** đến các địa chỉ tương ứng:  **• User Asset:** - Được gửi đến ví người dùng tương ứng (ví dụ như nhà sản xuất, đơn vị vận chuyển hoặc đại lý phân phối). - Tài sản này có thể được chuyển tiếp, giao dịch hoặc theo dõi trong toàn bộ chuỗi cung ứng, giống như sự di chuyển thực tế của sản phẩm.  **• Reference NFT:** - Được chuyển đến **Store Validator** – một địa chỉ có smart contract dùng để xác minh và lưu trữ metadata của sản phẩm. - Mọi thay đổi về metadata (ví dụ thay đổi vị trí, trạng thái, hoặc điều kiện vận chuyển) đều sẽ thông qua smart contract để đảm bảo tính minh bạch và bảo mật.  **• Chi phí đúc và xử lý giao dịch:** - Một lượng ADA cũng được gửi kèm theo giao dịch để phục vụ cho chi phí đúc tài sản và phí xử lý mạng.  Nhờ vậy, sản phẩm trong chuỗi cung ứng giờ đây có thể được truy xuất nguồn gốc một cách chính xác và không thể chỉnh sửa tùy tiện, tạo niềm tin cho toàn bộ các bên liên quan. |

### 2.3.2. Chức năng cập nhật sản phẩm

Việc cập nhật siêu dữ liệu (metadata) là một bước quan trọng nhằm đảm bảo rằng thông tin liên quan đến tài sản – như tình trạng sản phẩm, lịch sử kiểm định, hoặc vị trí hiện tại – luôn **được duy trì chính xác, minh bạch và kịp thời**. Trong tiêu chuẩn CIP-68, việc này được thực hiện một cách có tổ chức thông qua hợp đồng thông minh, bảo vệ tính bất biến của dữ liệu lịch sử đồng thời cho phép cập nhật khi cần thiết.

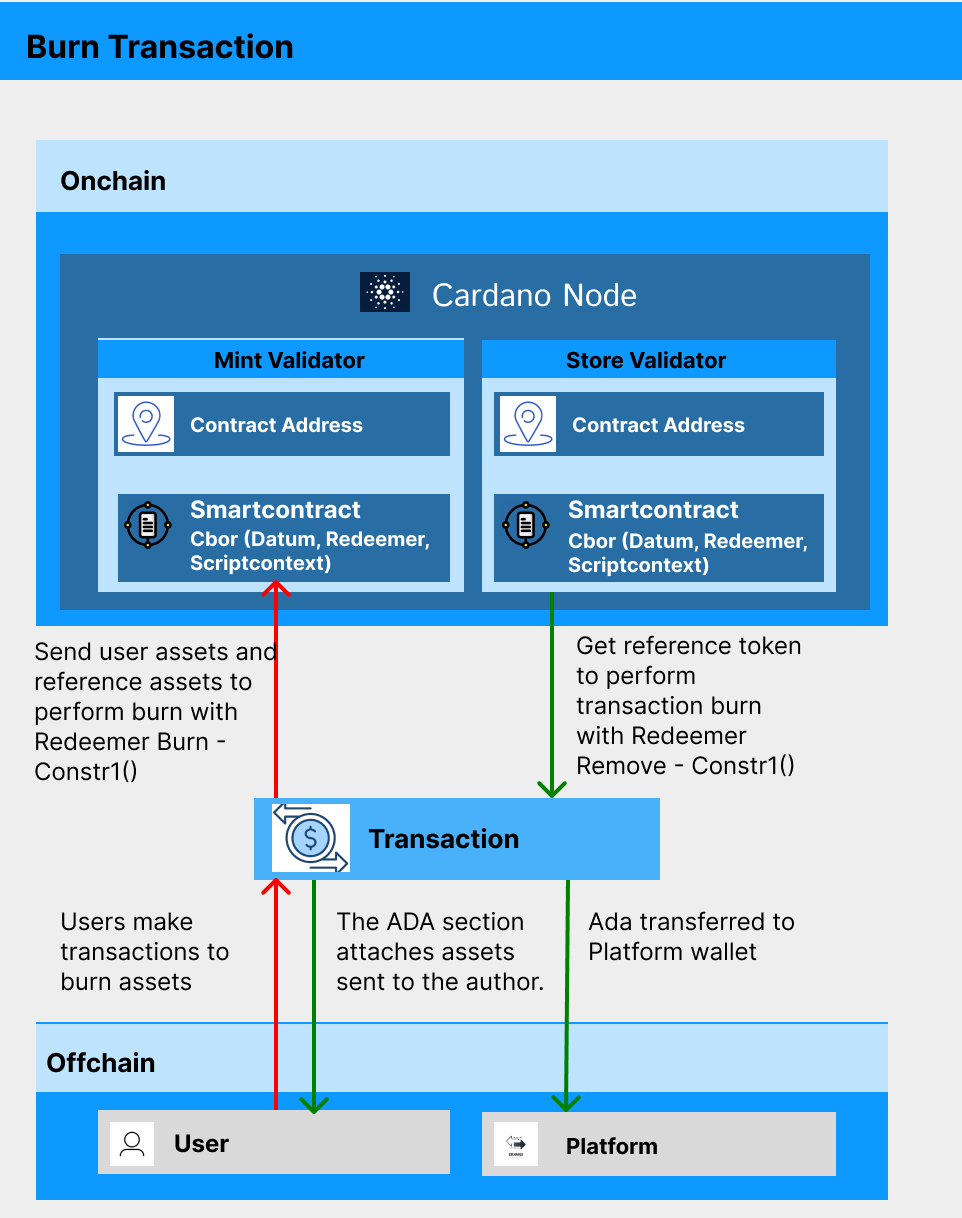


Quy trình cập nhật siêu dữ liệu tài sản trong chuỗi cung ứng sẽ được thực hiện qua các bước rõ ràng và có tính xác minh cao để đảm bảo tính chính xác và bảo mật của dữ liệu. Các thay đổi trong thông tin sản phẩm sẽ được ghi nhận trên blockchain, giúp mỗi sản phẩm có một lịch sử minh bạch mà không thể thay đổi hoặc làm giả.

|  |  |  |
| --- | --- | --- |
| Bước | Tên bước | Mô tả chi tiết |
| 1 | Tạo Giao Dịch Cập Nhật (Update Transaction) | Đây là bước khởi đầu khi muốn thay đổi thông tin liên quan đến sản phẩm đã được ghi nhận trước đó trên blockchain.   🔸 **Thông tin có thể cập nhật:**  • Tình trạng sản phẩm (đã kiểm định, đang vận chuyển, bảo quản ra sao, v.v.) • Thông tin vận chuyển (tên người giao, địa điểm nhận) • Ngày sản xuất và ngày hết hạn (rất quan trọng với thực phẩm, dược phẩm)  🔸 **Cấu trúc giao dịch:** • **Chi tiêu UTxO cũ**: Giao dịch sử dụng UTxO chứa tài sản gốc (Legacy Asset) có metadata cũ. • **Tạo UTxO mới**: Sinh ra UTxO mới chứa metadata đã được cập nhật, đính kèm Datum mới. • **Sử dụng Redeemer**: Được truyền vào để chỉ định mục đích cập nhật, giúp validator xác minh logic cập nhật. |
| 2 | Gửi Reference Asset đến Store Validator | Sau khi tạo giao dịch, UTxO chứa Reference Asset được chuyển đến địa chỉ của **Store Validator** (hợp đồng thông minh chịu trách nhiệm lưu trữ).  **Tác vụ thực hiện:** • Xác minh sự hợp lệ giữa metadata cũ và mới. • So sánh sự thay đổi để đảm bảo không có dữ liệu sai lệch, giả mạo. • Bảo vệ dữ liệu khỏi bị chỉnh sửa ngoài hợp lệ.  **Vai trò:** Store Validator là nơi bảo đảm các cập nhật tuân theo chính sách và tiêu chuẩn định sẵn. |
| 3 | Xác Nhận & Ghi Nhận Trên Blockchain | Khi hợp đồng thông minh kiểm tra thấy tất cả điều kiện đã đúng (chữ ký, redeemer, logic...), giao dịch sẽ được xác nhận và ghi nhận vĩnh viễn trên blockchain.  **Hành động tiếp theo:** • Ghi lại metadata mới thành bản ghi bất biến. • Cập nhật trạng thái sản phẩm, vị trí, người phụ trách, thông tin kiểm định,...  **Tính minh bạch:** Mọi dữ liệu cập nhật được ghi công khai, không thể chỉnh sửa sau khi đã ghi. Tạo điều kiện cho truy xuất nguồn gốc đáng tin cậy. |
| 4 | Hiển Thị Thông Tin Mới Cho Người Dùng | Sau khi quá trình ghi nhận hoàn tất:  **Hệ thống hiển thị:** • Người dùng truy cập giao diện quản lý chuỗi cung ứng sẽ thấy thông tin mới về sản phẩm. • Bao gồm: nguồn gốc sản phẩm, tình trạng hiện tại, hành trình vận chuyển. **Lợi ích:** • Nhà sản xuất, đơn vị vận chuyển và người tiêu dùng có thể kiểm chứng tính xác thực. • Tăng độ tin cậy, giảm gian lận trong chuỗi cung ứng. **Giao diện minh bạch – truy xuất mọi lúc, mọi nơi.** |

### 2.3.3. Chức năng xoá sản phẩm

Quy trình **Burning Asset** trong cơ chế CIP-68 được thiết kế để đảm bảo tính minh bạch, chính xác và an toàn khi một tài sản không còn cần thiết và cần phải loại bỏ khỏi hệ thống. Mục tiêu của quy trình này là đảm bảo rằng tài sản đã bị "đốt" không thể được sử dụng, chuyển nhượng, hay giao dịch trong bất kỳ tình huống nào, đồng thời giữ cho hệ thống blockchain sạch sẽ và hiệu quả.



|  |  |  |
| --- | --- | --- |
| Bước | Tên bước | Mô tả chi tiết |
| 1 | Tạo giao dịch để đốt tài sản | - Quy trình bắt đầu khi người dùng có nhu cầu loại bỏ một tài sản nhất định ra khỏi blockchain Cardano theo chuẩn CIP-68.  **Hành động chính:** • Người dùng truy cập vào hệ thống ứng dụng hoặc nền tảng hỗ trợ giao dịch đốt tài sản. • Chọn tài sản muốn đốt (NFT/FT/tài sản khác). • Hệ thống yêu cầu chọn hai UTxO:   ◦ **UTxO tài sản chính**: chứa tài sản người dùng muốn đốt.   ◦ **UTxO tài sản tham chiếu**: là UTxO chứa thông tin metadata, chính sách đốt, hoặc script liên quan đến quá trình xác thực.  **Kết quả:** Giao dịch đốt được tạo và sẵn sàng gửi đến blockchain. |
| 2 | Thực hiện xác thực giao dịch thông qua Mint Validator | - Giao dịch đốt khi gửi lên blockchain sẽ được xử lý bởi smart contract được gọi là **Mint Validator** – thành phần có nhiệm vụ đảm bảo rằng mọi điều kiện đốt tài sản đều được tuân thủ nghiêm ngặt.  **Hành động kiểm tra bao gồm:** • **Tính hợp lệ của tài sản**:   ◦ Tài sản không bị khóa trong các giao dịch khác.   ◦ Token vẫn đang tồn tại trên blockchain. • **Xác minh quyền sở hữu**:   ◦ Địa chỉ ký giao dịch chính là chủ sở hữu tài sản.   ◦ Tài khoản đã được cấp quyền đốt theo quy tắc của CIP-68 (thường là có chữ ký hợp lệ hoặc có trong danh sách được phép). • **Kiểm tra chính sách đốt:**   ◦ Validator sẽ kiểm tra rằng chính sách đốt được định nghĩa trong minting policy script có được thỏa mãn hay không (ví dụ: có thể yêu cầu đúng chữ ký, hoặc số lượng token bị đốt là một số cụ thể).  **Kết quả:** Nếu tất cả điều kiện được đáp ứng, giao dịch sẽ được đưa vào block và xử lý. |
| 3 | Xử lý tài sản sau khi đốt thành công | - Khi giao dịch đã được xác nhận trên blockchain, hệ thống sẽ tiến hành xử lý kết quả của việc đốt tài sản.  **Chi tiết hành động:** • **Hủy token**:   ◦ Tài sản sẽ bị xóa khỏi hệ thống blockchain, không thể truy cập, sử dụng hoặc phục hồi.   ◦ Tất cả metadata (nếu có) liên quan đến token cũng sẽ bị huỷ hoặc cập nhật lại trạng thái. • **Hoàn trả giá trị còn lại**:   ◦ Nếu có ADA hoặc token khác trong UTxO tham chiếu, chúng sẽ được hoàn trả lại cho người gửi giao dịch như một phần thưởng.   ◦ Đây thường là phần tài sản còn sót lại sau khi token bị đốt. • **Khấu trừ phí nền tảng**:   ◦ Một phần nhỏ ADA được trích ra làm phí để duy trì hạ tầng smart contract, validator, và hệ thống vận hành. Khoản phí này có thể cố định hoặc tính theo tỷ lệ cấu hình. |
| 4 | Cập nhật hệ thống và xác nhận đốt thành công | - Sau khi giao dịch được xác nhận hoàn tất, hệ thống và blockchain sẽ ghi nhận đầy đủ thông tin về việc tài sản đã bị đốt.  **Chi tiết hành động:** • **Ghi nhận on-chain**:   ◦ Tình trạng mới của tài sản được cập nhật trên blockchain. Thường là tài sản sẽ biến mất hoàn toàn, hoặc được gắn trạng thái "burned". • **Cập nhật các thông tin liên quan**:   ◦ Nếu token có metadata được lưu trong datum hoặc trong IPFS, hệ thống sẽ cập nhật để phản ánh rằng tài sản không còn tồn tại. • **Giao diện người dùng**:   ◦ Người dùng sẽ được hiển thị thông báo "Burn successful", cùng số ADA (nếu có) được hoàn trả.  **Kết quả cuối cùng:** Tài sản bị đốt được ghi nhận là đã bị huỷ vĩnh viễn. Không còn tồn tại bất kỳ bản sao nào có thể sử dụng lại. |

## 2.4. Kiểm thử các trường hợp có thể xảy ra của hợp đồng thông minh

### 2.4.1. Kiểm thử chức năng thêm sản phẩm

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Tên | Mô tả | Các bước thực hiện | Kết quả mong đợi | Kết quả |
| 1 | Tạo sản phẩm với dữ liệu được định sẵn | Đúc tài sàn với số lượng mong muốn và metadata có đủ các trường theo quy định. | 1. Vào trong thư mục contract trong file test với function mint. 2. Nhập các thông tin của một NFT của các trường mặc định như asset\_name, medata (name, image, media\_type, author), quantity.  3. Chạy câu lệnh 'npm run test' trên terminal | Giao dịch được thực hiện thành công chạy không bị lỗi và txHash được hiển thị trên terminal. và người chủ sở hữu có thể nhận Asset với số lượng và metadata được định nghĩa. | Passed |
| 2 | Thiếu các dữ liệu bắt buộc | Đúc tài sản nhưng các trường mặc định trong metadata (name, image, media\_type, author) không tồn tại. | 1. Vào trong thư mục contract file tests với function mint. 2. Để các trường metadata trống. 3. Chạy câu lệnh 'npm run test' trên terminal để xem kết quả. | Giao dịch xuất hiện lỗi ' Tx evaluation failed' giao dịch không build được và bị hủy. | Passed |
| 3 | Dữ liệu không hợp lệ | Đúc tài sản với metadata được định nghĩa nhưng các key (name, image, media\_type) đều tồn tại nhưng giá trị của các trường bị khuyển một phần hoặc toàn bộ. | 1. Vào thư mục contract file tests với function mint. 2. Định nghĩa medata đủ các trường truy nhiên trường name bị trống value hoặc các trường bị thiếu value hoặc bị trống hoàn toàn. 3. Chạy câu lệnh npm run test trên terminal để kiểm tra kết quả. | Xuất hiện lỗi với 'Tx evaluation failed' với id là '8f8df621-42de-44f1-98d5-dd9fc401a57b' giao dịch bị build lỗi và giao dịch bị hủy. | Passed |
| 4 | Dữ liệu được đưa lên sai địa chỉ của người tạo | Đúc tài sản với các metadata được định nghĩa đẩy đủ cả về kay và value tuy nhiên author address bị trống hoặc bị sai địa chỉ. | 1. Vào thư mục contract/tests sau đó vào file cip68.test.ts 2. Định nghĩa metadata đẩy đủ tuy nhiên phần địa chỉ của author address bị chuyển thành 'addr\_test1qq9my6zszlwfssdwv9au60ln8q3e79cn7l2nmz6u042fqzgdntvngdeudrnmxezylymnyt6nw33s3565vepdzjsn4rsqanrclv' và người kí với địa chỉ làm author là 'addr\_test1qqk6p73fh30uq7ag89hya9cq0f2llugj68vp9xvs9cpjc20xug5mjfdyw5uy9wvs7w8xfw6wj8q84lht979j824l7drsfcjud7'. 3. Chạy câu lệnh 'npm run test' trên terminal để kiểm tra kêt quả. | Xuất hiện lỗi với ' Tx evaluation failed' với id là '34c042bb-a912-403c-bf38-dd7b7ffdecb7' build bị lỗi và giao dịch bị hủy. | Passed |
| 5 | Phí giao dịch nhỏ hơn yêu cầu | Đúc tài sản với phí giao dịch nhỏ hơn số tiền quy định được đưa vào trong prameters của validator. | 1. Vào trong thư mục contract trong file test với function mint. 2. Gửi cho địa chỉ của sàn với số lương là 0.9ADA trong khi đó số lượng parameter truyền vào là 1ADA. 3. Chạy câu lệnh 'npm run test' trên terminal để xem kết quả. | Xuất hiện lỗi trên giao diện terminal là 'txBuildResult error: JsValue("Value 900000 less than the minimum UTXO value 969750")' toàn bộ giao dịch không thể build được giao dịch bị hủy. | Passed |
| 6 | Địa chỉ sàn sai | Đúc tài sản với phí giao dịch đúng với params. tuy nhiên bị sai địa chỉ của sàn được định nghĩa trong params. | 1. Vào thư mục contract với file test function mint. 2. Gửi cho địa chỉ khác vơi địa chỉ là "addr\_test1qqkyms8pahasv43q6mrthgs3f5f8jr7mguddkg27r0lryuwz4njvq57qjdqw22wuaqu4tkppsmnlf0wcg430skm5lvdqxm2d7r" trong khi đó địa chỉ của sản là "addr\_test1qzwu6jcqk8f96fxq02pvq2h4a927ggn35f2gzdklfte4kwx0sd5zdvsat2chsyyjxkjxcg6uz2y46avd46mzqdgdy3dsckqxs4" 3. Chạy câu lênh 'npm run test' trên terminal để xem kết quả. | Xuất hiện lỗi Tx evaluation failed trên màn hình terminal, toàn bộ giao dịch không thể build được giao dịch bị hủy. | Passed |
| 7 | Địa chỉ store sai | Người tạo Token gửi sai địa chỉ của store address được đưa vào params. | 1. Vào thư mục contract/tests và function mint. 2. Địa chỉ store address gửi bị sai là một địa chỉ khác. 3. Chạy câu lệnh 'npm run test' và xem kết quả. | Xuất hiện lỗi 'Tx evaluation failed' trên terminal, Giao dịch không thể build được giao dịch và bị hủy. | Passed |
| 8 | Sai prefix Token (CIP100) | Người tạo gửi Token với prefix\_100 (CIP100) | 1. Vào thư mục contract/tests và function mint. 2. gửi vào địa chỉ của hợp đồng thông minh với token có prefix là 200 khác prefix 200. 3. Chạy câu lệnh 'npm run test' và xem kết quả, | Xuất hiện lỗi ' Tx evaluation failed' với id là '3ec61063-2c57-4494-9e7e-5d7ab38b28b4' giao dịch không thể build và bị hủy. | Passed |
| 9 | Thiếu UTXO output cần thiết | Đầu ra các UTxO bị thiếu phần gửi cho hợp đồng thông minh store address hoặc gửi cho phí sàn bị thiếu | 1. Vào thư mục contract/test và function mint. 2. Gửi thực hiên không gửi cho địa chỉ của store address và exchange address. 3. Chạy câu lệnh 'npm run test' và xem kết quả. | Xuất hiện lỗi ' Tx evaluation failed' với id là '3ec61063-2c57-4494-9e7e-5d7ab38b28b4' giao dịch không thể build và bị hủy. | Passed |

### 2.4.2. Kiểm thử chức năng cập nhật sản phẩm

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Tên | Mô tả | Các bước thực hiện | Kết quả mong đợi | Kết quả |
| 1 | Cập nhật sản phẩm thành công | Cập nhật tài sản thành công. Phí sàn được huyển cho địa chỉ sàn. Tài sản được cập nhật thành công. | 1. Vào thư mục contract/test và function update.  2. Thực hiện copy txHash vừa mint hoặc từ những lần update trước đó vào trong txHash params.  3. Sau đó thực hiện thay đổi các trường trong metadata thêm bớt tùy thích tuy nhiên các trường mặc định phải được điền đầy đủ đồng thời các author không được sửa.  4. Chạy câu lệnh 'npm run test'và xem kết quả update trên terminal | Chạy không bị lỗi và transaction hash được in ra màn hình trong giao dịch được gửi phí sàn cho địa chỉ của exchange fee, địa chỉ của store address | Passed |
| 2 | Thiếu metadata bắt buộc | Trong metadata thay dổi trường author hoặc không có trường author. | 1. Vào trong tư mục contract/test và function update  2. Thực hiện copy txhash vừa mint hoặc từ những lần update trước đó vào trong txHash Pasrams của function update  3. Nhập các metadata tuy nhiên trường author để trống hoặc không tồn tại hoặc bị sai địa chỉ của author hiện tại.  4. Chạy câu lệnh npm run test và kiểm tra kết quả trên terminal. | Xuất hiện lỗi ' Tx evaluation failed' với id là '3ec61063-2c57-4494-9e7e-5d7ab38b28b4' giao dịch không thể build và bị hủy. | Passed |
| 3 | Tác giả không kí gửi | Author không gửi chữ kí lên để xác nhận giao dịch. | 1. Vào trong thư mục contract/txbuilder trong function update thực hiện xóa bỏ đi phần chữ kí kèm theo.  2. Thực hiện copy TxHash từ lần update trươc đó vào trong params để thực hiện giao dịch  3. Thực hiện nhập các params và metadata đúng định dạng yêu cầu.  4. Chạy câu lệnh npm run test và kiểm tra kết quả. | Xuất hiện lỗi ' Tx evaluation failed' với id là '3ec61063-2c57-4494-9e7e-5d7ab38b28b4' giao dịch không thể build và bị hủy. | Passed |
| 4 | Metadata sai author address | Đúc tài sản với các metadata được định nghĩa đẩy đủ cả về kay và value tuy nhiên author address bị trống hoặc bị sai địa chỉ. | 1. Vào thư mục contract/tests sau đó vào file cip68.test.ts 2. Định nghĩa metadata đẩy đủ tuy nhiên phần địa chỉ của author address bị chuyển thành 'addr\_test1qq9my6zszlwfssdwv9au60ln8q3e79cn7l2nmz6u042fqzgdntvngdeudrnmxezylymnyt6nw33s3565vepdzjsn4rsqanrclv' và người kí với địa chỉ làm author là 'addr\_test1qqk6p73fh30uq7ag89hya9cq0f2llugj68vp9xvs9cpjc20xug5mjfdyw5uy9wvs7w8xfw6wj8q84lht979j824l7drsfcjud7'. 3. Chạy câu lệnh 'npm run test' trên terminal để kiểm tra kêt quả. | Xuất hiện lỗi với ' Tx evaluation failed' với id là '34c042bb-a912-403c-bf38-dd7b7ffdecb7' build bị lỗi và giao dịch bị hủy. | Passed |
| 5 | Phí giao dịch nhỏ hơn yêu cầu | Đúc tài sản với phí giao dịch nhỏ hơn số tiền quy định được đưa vào trong prameters của validator. | 1. Vào trong thư mục contract trong file test với function mint. 2. Gửi cho địa chỉ của sàn với số lương là 0.9ADA trong khi đó số lượng parameter truyền vào là 1ADA. 3. Chạy câu lệnh 'npm run test' trên terminal để xem kết quả. | Xuất hiện lỗi trên giao diện terminal là 'txBuildResult error: JsValue("Value 900000 less than the minimum UTXO value 969750")' toàn bộ giao dịch không thể build được giao dịch bị hủy. | Passed |
| 6 | Địa chỉ sàn sai | Đúc tài sản với phí giao dịch đúng với params. tuy nhiên bị sai địa chỉ của sàn được định nghĩa trong params. | 1. Vào thư mục contract với file test function mint. 2. Gửi cho địa chỉ khác vơi địa chỉ là "addr\_test1qqkyms8pahasv43q6mrthgs3f5f8jr7mguddkg27r0lryuwz4njvq57qjdqw22wuaqu4tkppsmnlf0wcg430skm5lvdqxm2d7r" trong khi đó địa chỉ của sản là "addr\_test1qzwu6jcqk8f96fxq02pvq2h4a927ggn35f2gzdklfte4kwx0sd5zdvsat2chsyyjxkjxcg6uz2y46avd46mzqdgdy3dsckqxs4" 3. Chạy câu lênh 'npm run test' trên terminal để xem kết quả. | Xuất hiện lỗi Tx evaluation failed trên màn hình terminal, toàn bộ giao dịch không thể build được giao dịch bị hủy. | Passed |
| 7 | Địa chỉ store sai | Người tạo Token gửi sai địa chỉ của store address được đưa vào params | 1. Vào thư mục contract/tests và function mint. 2. Địa chỉ store address gửi bị sai là một địa chỉ khác. 3. Chạy câu lệnh 'npm run test' và xem kết quả. | Xuất hiện lỗi 'Tx evaluation failed' trên terminal, Giao dịch không thể build được giao dịch và bị hủy. | Passed |
| 8 | Sai prefix Token (CIP100) | Người tạo gửi Token với prefix\_100 (CIP100) | 1. Vào thư mục contract/tests và function mint. 2. gửi vào địa chỉ của hợp đồng thông minh với token có prefix là 200 khác prefix 200. 3. Chạy câu lệnh 'npm run test' và xem kết quả, | Xuất hiện lỗi ' Tx evaluation failed' với id là '3ec61063-2c57-4494-9e7e-5d7ab38b28b4' giao dịch không thể build và bị hủy. | Passed |
| 9 | Sai điều kiện Redeemer | Đầu vào giao dịch lấy điều kiện của redeemer khác điều kiện của redeemer update | 1. Vào thư mục contract/script/txbuilder và function update của class CIP68Generator. 2.Thực hiện chuyển redeemer từ update thảnh redeemer remove. 3. Chạy câu lệnh "npm run test" và kiểm tra kết quả. | Xuất hiện lỗi "ScriptFailures" cùng với value "b8e7eabf-8821-4be1-9780-b68ed845e4b1" và in ra txHex của giao dịch. Giao dịch build lỗi và bị hủy. | Passed |

### 2.4.3. Kiểm thử chức năng xóa sản phẩm

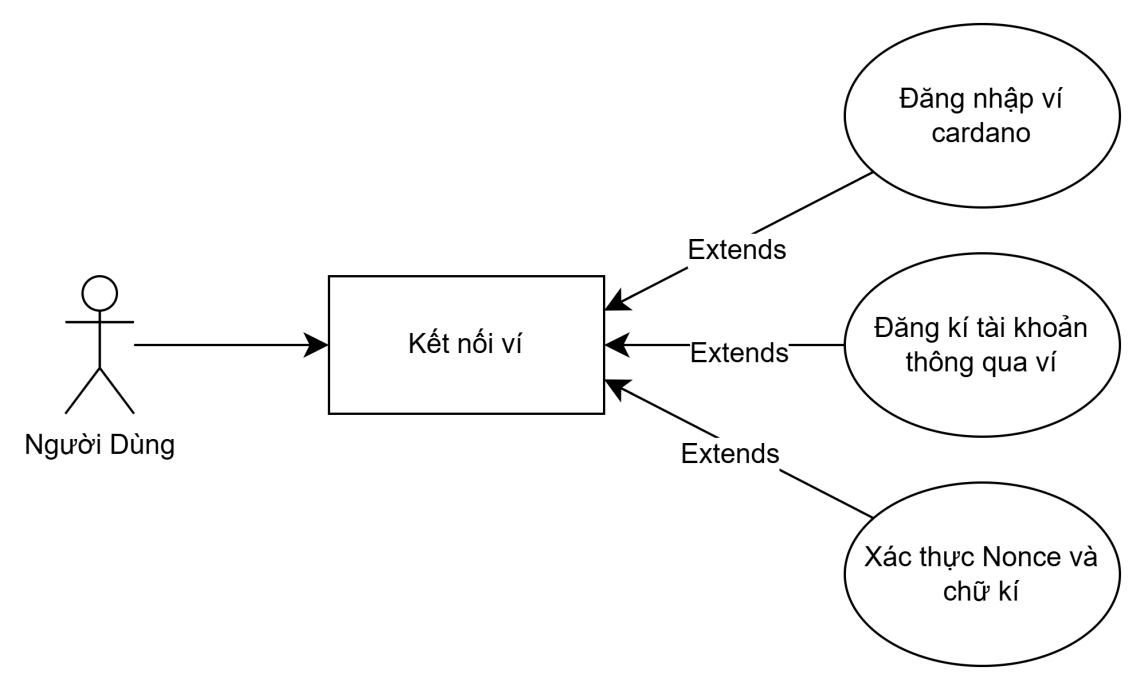
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Tên | Mô tả | Các bước thực hiện | Kết quả mong đợi | Kết quả |
| 1 | Xóa sản phẩm thành công | Khi Thực hiện Burn User Asset và Reference Asset và thực hiện gửi ada cho platform fee thành công | 1. Vào thư mục contract/tests/cip68.test.ts. 2. Thực hiện nhập asset name đã mint từ trước đó để thực hiện burn tài sàn. 3. Chạy câu lệnh "npm run test" và kiểm tra kết quả. | Xuất hiên txHash được in ra trên màn hình. Quá trình burn tà sản được thực hiện thành công. | Passed |
| 2 | Xóa sản phẩm nhưng thiếu các điều kiện đính kèm | Burn asset bị thiếu User Asset Hoặc Reference Asset Hoặc thiếu cả hai | 1. Vào thư mục contract/scripts/txbuilder/cip68.txbuilder.ts 2. Thực hiện nhập assetName đã mint từ trước để thực hiện kiểm tra. 3. Chạy câu lệnh "npm run test" và kiểm tra kết quả. | Xuất hiện lỗi "Tx evaluation failed" với Id là " 4b69e0c4-7110-403c-972e-cc4b14b987af" và in ra txHex của giao dịch. Quá trình Burn tài sản thất bại. | Passed |
| 3 | Parameters không được đúng so với ban đầu | Burn tài sản nhưng phần ada được gửi cho platform nhỏ hơn phần phí được định nghĩa trong params | 1. Vào trong thư mục contract trong file test với function burn. 2. Gửi cho địa chỉ của sàn với số lương là 0.9ADA trong khi đó số lượng parameter truyền vào là 1ADA. 3. Chạy câu lệnh 'npm run test' trên terminal để xem kết quả. | Xuất hiện lỗi trên giao diện terminal là 'txBuildResult error: JsValue("Value 900000 less than the minimum UTXO value 969750")' toàn bộ giao dịch không thể build được giao dịch bị hủy. | Passed |
| 4 | Tài sản bị gửi sai địa chỉ | Burn tài sản nhưng địa chỉ được gửi trong platform khác địa chỉ của phí sàn được định nghĩa trong params. | 1. Vào thư mục contract với file test funcion burn. 2. Thực hiện gửi Số ada được định kèm trong referece asset với địa chỉ khác địa chỉ của author address. 3. Chạy câu lệnh "npm run test" để kiểm tra kết quả. | Xuất hiện lỗi "Tx evaluation failed" với Id là " 4b69e0c4-7110-403c-972e-cc4b14b987af" và in ra txHex của giao dịch. Quá trình Burn tài sản thất bại. | Passed |
| 5 | Gửi tài sản đính kèm sai địa chỉ | Khi burn giao dịch số ada đính kèm reference asset được gửi cho một địa chỉ khác hoặc không được gửi cho người dùng. | 1. Vào thư mục contract với file test funcion burn. 2. Thực hiện gửi Số ada được định kèm trong referece asset với địa chỉ khác địa chỉ của author address. 3. Chạy câu lệnh "npm run test" để kiểm tra kết quả. | Xuất hiện lỗi "Tx evaluation failed" với Id là " 4b69e0c4-7110-403c-972e-cc4b14b987af" và in ra txHex của giao dịch. Quá trình Burn tài sản thất bại. | Passed |
| 6 | Thêm một đầu ra đính kèm bị sai | Với mặc định yêu cầu là 2 đầu ra. Thực hiện thêm một đầu ra mới gửi cho địa chỉ khác. | 1. Vào thư mục contract với file test funcion burn. 2. Thêm một hay nhiều đầu ra mới với địa chỉ và số ADA kèm theo. 3. Chạy câu lệnh "npm run test" để kiểm tra kết quả. | Xuất hiện lỗi "Tx evaluation failed" với Id là " 4b69e0c4-7110-403c-972e-cc4b14b987af" và in ra txHex của giao dịch. Quá trình Burn tài sản thất bại. | Passed |

# CHƯƠNG 3. PHÂN TÍCH THIẾT KẾ TRANG WEB ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN VÀO QUẢN LÝ CHUỖI CUNG ỨNG TRUY SUẤT NGUỒN GỐC HÀNG HOÁ

## 3.1. Thiết kế use case

### 3.1.1. Use case tổng quát

### 3.1.2. Use case kết nối ví



|  |  |
| --- | --- |
|  | **Nội dung** |
| Tên use case | Kết nối ví |
| Mô tả | Người dùng thực hiện đăng nhập bằng cách kết nối ví của mình để thực hiện sử dụng dịch vụ của ứng dụng. |
| Actor | Người dùng |
| Điều kiện kích hoạt | Trong môi trường Browser tồn tại các module của ví được cài trên máy, người dùng kết nối ví Blockchain Cardano (Eternl, Lace, …) để thực hiện kết nối vào trang web. |
| Tiền điều kiện | Người dùng đã tải ví và kích hoạt ví cho phép chúng có thể kết nối với mạng lưới blockchain cardano thông qua quyền truy cập của ví. |
| Hậu điều kiện | Người dùng kết nối ví thành công, hệ thống thực hiện xác minh bằng cách kí và ghi nhận thông tin. |
| Luồng sự kiện chính | * Người dùng truy cập trang web. * Trước hết là chọn mạng lưới để kết nối sau đó chọn lệnh kết nối ví. * Cửa sổ hiện lên yêu cầu người dùng cho phép kết nối ví với trang web. * Người dùng thực hiện kí mật khẩu mà đã thiết lập trong ví. * Hệ thống xác thực thông tin người dùng cho phép người dùng đăng nhập thành công. * Hiển thị trang thông tin dashboard với những sản phẩm mà người dùng đã tạo. |
| Luồng sự kiện phụ | * Người dùng chọn lệnh “Huỷ” use case dừng lại. * Nếu người dùng chọn sai mạng sẽ bị hủy đăng nhập * Người dùng nhập sai mật khẩu của ví thì sẽ phải nhập lại mật khẩu. |

### 3.1.3. Use case quản lý dịch vụ

|  |  |
| --- | --- |
|  | **Nội dung** |
| Tên use case | Quản lý dịch vụ |
| Mô tả | Người dùng xem, mua, gia hạn và kiểm tra trạng thái các gói dịch vụ có sẵn trong hệ thống bằng ví Cardano. |
| Actor | Người dùng |
| Điều kiện kích hoạt | Người dùng có nhu cầu sử dụng dịch vụ: xem, mua, gia hạn hoặc kiểm tra thời hạn dịch vụ. |
| Tiền điều kiện | Truy cập hệ thống, Kết nối ví Cardano (đối với các chức năng thanh toán/gia hạn). Đã đăng nhập (đối với các chức năng cá nhân hóa) |
| Hậu điều kiện | Người dùng có thể sử dụng các dịch vụ theo gói, kiểm tra thời hạn hoặc nhận thông báo khi gói sắp hết hạn. |
| Luồng sự kiện chính | 1. Người dùng truy cập trang “Dịch vụ” 2. Hệ thống hiển thị danh sách gói dịch vụ (tên, giá, tính năng) 3. Người dùng chọn một trong các hành động:  * **Xem chi tiết gói dịch vụ.** * **Mua gói dịch vụ**: kết nối ví → ký giao dịch ADA → hệ thống xác nhận * **Kiểm tra gói đang sử dụng**: truy cập “Dịch vụ của tôi” → hệ thống hiển thị thông tin còn hạn * **Gia hạn/nâng cấp**: chọn gói mới → thanh toán → cập nhật dịch vụ  1. Nếu gói sắp hết hạn, hệ thống tự động gửi thông báo (email/thông báo hệ thống). |
| Luồng sự kiện phụ | Nếu ví không đủ ADA → thông báo lỗi “Số dư không đủ”.  Nếu người dùng chưa đăng nhập → chuyển hướng tới trang đăng nhập |

### 3.1.4. Use case quản lý bộ sưu tập

|  |  |
| --- | --- |
|  | **Nội dung** |
| Tên use case | Quản lý bộ sưu tập |
| Mô tả | Người dùng tạo, cập nhật, xoá và liệt kê các bộ sưu tập là nguyên liệu để tạo các sản phẩm trong hệ thống |
| Actor | Người dùng |
| Điều kiện kích hoạt | Người dùng truy cập trang "Bộ sưu tập" và có nhu cầu quản lý bộ sưu tập của mình. |
| Tiền điều kiện | Người dùng đã kết nối và xác minh vào hệ thống. Còn thời hạn sử dụng dịch vụ (đối với chức năng tạo và cập nhật) |
| Hậu điều kiện | Bộ sưu tập được tạo mới, cập nhật, xoá hoặc hiển thị đúng theo quyền truy cập của người dùng. |
| Luồng sự kiện chính | 1. Người dùng truy cập trang “Bộ sưu tập của tôi” 2. Hệ thống hiển thị danh sách bộ sưu tập đã tạo 3. Người dùng chọn một trong các hành động:  * **Tạo mới**: nhập tên, mô tả, ảnh đại diện → gửi yêu cầu → hệ thống lưu và hiển thị * **Cập nhật**: chọn bộ sưu tập → sửa thông tin → xác nhận → hệ thống lưu thay đổi * **Xoá**: chọn bộ sưu tập → xác nhận xoá → hệ thống xoá và cập nhật danh sách  1. Kết quả được phản hồi ngay lập tức cho người dùng |
| Luồng sự kiện phụ | * Nếu người dùng không có quyền chỉnh sửa/xoá bộ sưu tập → hệ thống hiển thị thông báo lỗi. * Nếu chưa đăng nhập → chuyển hướng sang trang đăng nhập. * Nếu hết hạn dịch vụ → thông báo và yêu cầu gia hạn để tiếp tục sử dụng tính năng. |

### 3.1.5. Use case quản lý sản phẩm

|  |  |
| --- | --- |
|  | **Nội dung** |
| Tên use case | Quản lý sản phẩm |
| Mô tả | Người dùng quản lý quy trình đưa một sản phẩm thực tế lên blockchain thông qua NFT, bao gồm tạo mới sản phẩm, mint NFT, bổ sung metadata, tài liệu, nguyên liệu, quy trình sản xuất, chứng nhận và lưu kho. |
| Actor | Người dùng |
| Điều kiện kích hoạt | Người dùng truy cập tính năng tạo/mint sản phẩm NFT từ giao diện quản lý sản phẩm. |
| Tiền điều kiện | Người dùng đã đăng nhập hệ thống bằng ví Cardano. Tài khoản còn hạn dịch vụ (gói dịch vụ còn hiệu lực). Ví người dùng có đủ ADA để chi trả phí giao dịch. Người dùng có bộ sưu tập đã tạo để liên kết sản phẩm |
| Hậu điều kiện | Sản phẩm được mint thành NFT và lưu trữ trên blockchain. Metadata, tài liệu, nguyên liệu, chứng nhận và thông tin sản xuất được lưu lại. NFT được gắn với bộ sưu tập tương ứng. Sản phẩm NFT được đánh dấu là đã lưu kho. |
| Luồng sự kiện chính | 1. Người dùng truy cập trang "Sản phẩm NFT" 2. Chọn tạo mới sản phẩm 3. Nhập thông tin:  * Metadata: tên, mô tả, hình ảnh đại diện * Tài liệu liên quan: PDF, ảnh * Nguyên liệu cấu thành sản phẩm * Quy trình sản xuất * Chứng nhận sản phẩm (nếu có)  1. Gửi yêu cầu mint → hệ thống chuẩn bị giao dịch  * Ví người dùng hiển thị yêu cầu ký giao dịch mint * Người dùng ký → hệ thống gửi giao dịch lên blockchain * Lưu lại transaction hash (txHash) và thông tin sản phẩm |
| Luồng sự kiện phụ | * **Ví không đủ ADA:** Hiển thị thông báo lỗi, gợi ý nạp thêm ADA. * **Ký giao dịch thất bại:** Cho phép thử lại hoặc hủy bỏ quá trình mint. * **Thông tin chưa đầy đủ:** Hệ thống yêu cầu nhập đủ các trường cần thiết trước khi cho phép mint. * **Lỗi khi upload tài liệu hoặc chứng nhận:** Hiển thị thông báo lỗi, yêu cầu người dùng tải lại file hợp lệ. |

### 3.1.6. Use case truy xuất nguồn gốc sản phẩm

|  |  |
| --- | --- |
|  | **Nội dung** |
| Tên use case | Truy suất nguồn gốc |
| Mô tả | Người dùng hoặc khách truy cập có thể xem chi tiết thông tin nguồn gốc của một sản phẩm đã được mint dưới dạng NFT: nguyên liệu, quy trình sản xuất, tài liệu liên quan, chứng nhận... |
| Actor | Người dùng, Khách truy cập (nếu sản phẩm công khai) |
| Điều kiện kích hoạt | Sản phẩm đã được mint thành NFT và lưu thông tin đầy đủ. Có địa chỉ token hoặc đường dẫn sản phẩm NFT. Sản phẩm được cấp quyền truy xuất công khai (hoặc người dùng là chủ sở hữu). |
| Tiền điều kiện | Người dùng đã đăng nhập hệ thống bằng ví Cardano. Tài khoản còn hạn dịch vụ (gói dịch vụ còn hiệu lực). |
| Hậu điều kiện | Người dùng xem được toàn bộ thông tin truy xuất nguồn gốc của sản phẩm NFT. Thông tin minh bạch, không thể chỉnh sửa sau khi mint giúp tăng độ tin cậy và xác thực. |
| Luồng sự kiện chính | 1. Người dùng truy cập trang "Sản phẩm NFT" 2. Chọn tạo mới sản phẩm 3. Nhập thông tin:  * Metadata: tên, mô tả, hình ảnh đại diện * Tài liệu liên quan: PDF, ảnh * Nguyên liệu cấu thành sản phẩm * Quy trình sản xuất * Chứng nhận sản phẩm (nếu có)  1. Gửi yêu cầu mint → hệ thống chuẩn bị giao dịch  * Ví người dùng hiển thị yêu cầu ký giao dịch mint * Người dùng ký → hệ thống gửi giao dịch lên blockchain * Lưu lại transaction hash (txHash) và thông tin sản phẩm |
| Luồng sự kiện phụ | * **Sản phẩm chưa mint hoặc bị xoá:** thông báo "Không tìm thấy thông tin sản phẩm." * **Thông tin metadata không đầy đủ / bị lỗi:** hiển thị cảnh báo và chỉ hiển thị phần có thể đọc được. * **Sản phẩm bị giới hạn truy cập:** thông báo "Bạn không có quyền xem chi tiết sản phẩm này." |

## 3.2. Thiết kế cơ sở dữ liệu

### 3.2.1. Mô hình liên kết cơ sở dữ liệu



### 3.2.2. Chi tiết các bảng

### Bảng user - Người dùng

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã user |
| 2 | Address | nvarchar(100) | Địa chỉ ví của người dùng |
| 3 | Created\_At | datetime | Thời gian người dùng được tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |

### Bảng wallet nonce - Xác thực ví

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh nonce |
| 2 | Address | nvarchar(100) | Địa chỉ ví gắn với nonce |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Nonce | Nvarchar(100) | Mã nonce dùng để xác thực người dùng (ví dụ trong đăng nhập ví). |

### Bảng collection - Bộ sưu tập

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | ID của bộ sưu tập |
| 2 | UserID | Nvarchar(100) | Id người tạo bộ sưu tập |
| 3 | Name | nvarchar(100) | Tên bộ sưu tập |
| 4 | Created\_At | datetime | Thời gian người dùng tạo |
| 5 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 6 | Description | Nvarchar(100) | Mô tả của bộ sưu tập |
| 5 | Thumbnail | Nvarchar(100) | Hình ảnh đại diện của bộ sưu tập |

### Bảng metadata - Metadata của Product

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh của metadata |
| 2 | CollectionID | nvarchar(100) | Mã của bộ sưu tập chứa metadata |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Content | Nvarchar(100) | Nội dung của metadata (có thể là json hoặc text |
| 6 | Assetname | Nvarchar(100) | Tên của Product |
| 7 | Reference | Mvarchar(100) | Danh sách các tham chiều liên quan |

### Bảng media - Tài nguyên Media

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh media |
| 2 | UserID | nvarchar(100) | Người tải media |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Name | Nvarchar(100) | Tên của media |
| 6 | Type | Nvarchar(100) | Loại media (image, video, pdf, …) |
| 7 | Url | NVarchar(100) | Đường dân file được định nghĩa trong IPFS |

### Bảng product - Sản phẩm

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh sản phẩm |
| 2 | UserID | nvarchar(100) | Người tạo sản phẩm |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | PolicyID | Nvarchar(100) | Mã chính sách tạo tài sản trên cardano |
| 6 | AssetName | Nvarchar(100) | Tên của sản phẩm |
| 7 | Name | Nvarchar(100) | Tên sản phẩm |
| 8 | TxHash | Nvarchar(100) | TxHash liên quan đến lịch sử sản phẩm trên Blockchain Cardano |

### Bảng document - Tài liệu liên quan

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh tài liệu |
| 2 | ProductID | nvarchar(100) | Liên kết sản phẩm |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Type | Nvarchar(100) | Loại tài liệu (hợp đồng, hướng dẫn, …) |
| 6 | Url | Nvarchar(100) | Đường dẫn file |
| 7 | Hash | Nvarchar(100) | Hash được lưu trên IPFS |

### Bảng product process - Quy trình sản xuất

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh process |
| 2 | ProductID | nvarchar(100) | Sản phẩm được sản xuất |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | StepName | Nvarchar(100) | Tên bước sản xuất |
| 6 | StartTime | Datetime | Thời gian bắt đầu |
| 7 | EndTime | Datetime | Thời gian kết thúc |
| 8 | Location | Nvarchar(100) | Vị trí thực hiện |

### Bảng certification - Chứng nhận sản phẩm

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh chứng nhận |
| 2 | ProductID | nvarchar(100) | Sản phẩm được chứng nhận |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | CertificateName | Nvarchar(100) | Tên chứng nhận |
| 6 | IssueDate | Datetime | Ngày cấp chứng nhận |
| 7 | ExpiryDate | Datetime | Ngày hết hạn của chứng nhận |
| 8 | CertificateHash | Nvarchar(100) | Mã hash xác minh chứng nhận |

### Bảng feedback - Đánh giá sản phẩm

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh feedback |
| 2 | UserID | nvarchar(100) | Người đánh giá |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | ProductID | Nvarchar(100) | Sản phẩm được đánh giá |
| 6 | Content | Nvarchar(100) | Nội dung đánh giá |
| 7 | Rating | Int | Điểm đánh giá (Sao) |

### Bảng supplier - Nhà cung cấp

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh nhà cung cấp |
| 2 | UserID | nvarchar(100) | Mã định danh người sở hữu |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Name | Nvarchar(100) | Tên nhà cung cấp |
| 6 | Location | Nvarchar(100) | Địa điểm hoạt động |
| 7 | GPS | Nvarchar(100) | Tọa độ GPS |
| 8 | ContactInfo | Nvarchar(100) | Thông tin liên hệ |

### Bảng raw material - Nguyên liệu thô

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | UserID | nvarchar(100) | Mã định danh nonce |
| 2 | SupplierID | nvarchar(100) | Mã đinh danh nhà cung cấp nguyên liệu |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Name | Nvarchar(100) | Tên nguyên liệu |
| 6 | Harvest | Datetime | Ngày thu hoạch |
| 7 | Quantity | Float | Số lượng nguyên liệu |

### Bảng service plan - Gói dịch vụ

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh của gói |
| 2 | Name | nvarchar(100) | Tên gói dịch vụ |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Description | Nvarchar(100) | Mô tả gói dịch vụ |
| 6 | Price | Float | Giá tiền |
| 7 | Duration | Int | Thời gian sử dụng (Ngày, Tháng, …) |

### Bảng subscription - Đăng kí dịch vụ

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | nvarchar(100) | Mã định danh đăng kí |
| 2 | UserID | nvarchar(100) | Người đăng kí |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Status | Nvarchar(100) | Trạng thái (active, expired, pending) |
| 6 | StartDate | Datetime | Thời gian bắt đầu |
| 7 | EndDate | Datetime | Thời gian kết thúc |

### Bảng payment - Thanh toán

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | ID | Nvarchar(100) | Mã định hanh của giao dịch |
| 2 | UserID | Nvarchar(100) | Mã định danh của người thanh toán |
| 3 | CreatedAt | datetime | Thời gian người dùng tạo |
| 4 | UpdatedAt | datetime | Thời gian người dùng cập nhật |
| 5 | SubcriptionID | Nvarchar(100) | Mã gắn với gói đăng kí nào |
| 6 | amount | Int | Số tiền đăng kí |
| 7 | Curency | Nvarchar(100) | Loại tiền chọn thanh toán (ADA, USD, …) |
| 8 | TxHash | Nvarchar(100) | Mã giao dịch trên blockchain |
| 9 | PaymentDate | Datetime | Ngày thanh toán |

### Bảng warehouse - Kho lưu trữ

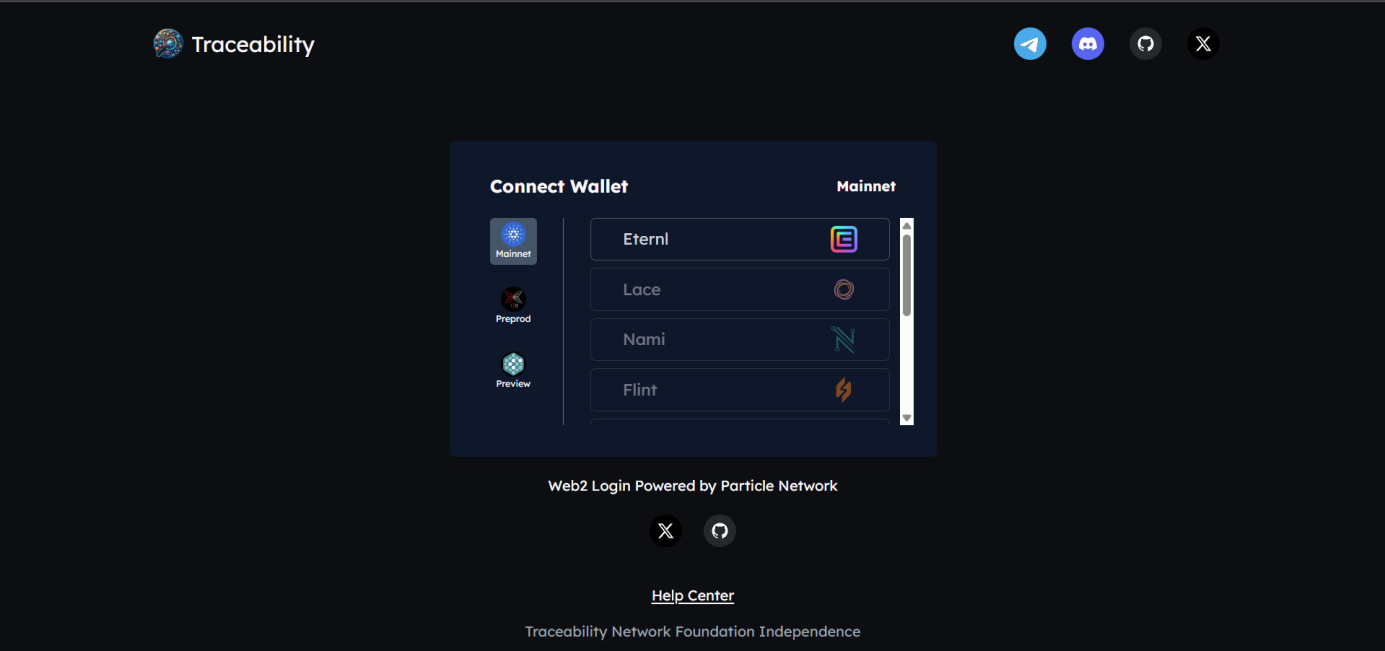
|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | Id | nvarchar(100) | Mã định danh kho |
| 2 | Name | nvarchar(100) | Tên kho |
| 3 | Created\_At | datetime | Thời gian người dùng tạo |
| 4 | Updated\_At | datetime | Thời gian người dùng cập nhật |
| 5 | Location | Nvarchar(100) | Vị trí, địa điểm của kho |
| 6 | Capacity | Nvarchar(100) | Sức chưa của kho(đơn vị tự chọn) |

### Bảng warehouse storage - Lưu trữ hàng hóa

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên cột** | **Kiểu dữ liệu** | **Mô tả** |
| 1 | Id | nvarchar(100) | Mã định danh lưu trữ |
| 2 | ProductId | nvarchar(100) | Mã của sản phẩm lưu trữ |
| 3 | WarehouseId | Nvarchar(100) | Mã định danh của kho lưu trữ |
| 4 | EntryTime | datetime | Thời điểm nhập kho |
| 5 | ExitTime | datetime | Thời điểm xuất kho |
| 6 | Conditions | Nvarchar(100) | Điều kiện bảo quản nhiệt độ ,độ ẩm,… |
| 7 | CreatedAt | datetime | Thời gian tạo bản ghi |
| 8 | UpdatedAt | datetime | Thời gian cập nhật bản ghi |

# **CHƯƠNG 4. CÀI ĐẶT VÀ THỰC NGHIỆM WEBSITE ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN VÀO QUẢN LÝ CHUỖI CUNG ỨNG TRUY SUẤT NGUỒN GỐC HÀNG HOÁ**

**4.1. Giao diện kết nối ví**



*Hinh 4.1 Đăng nhập - Kết nối Ví*

# KẾT LUẬN VÀ KIẾN NGHỊ

## Kết luận:

Việc ứng dụng công nghệ Blockchain vào quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hoá mang lại một bước tiến đột phá trong việc nâng cao tính minh bạch, độ tin cậy và hiệu quả trong chuỗi giá trị. Nhờ đặc tính bất biến, phân tán và minh bạch của Blockchain, mọi dữ liệu liên quan đến sản phẩm – từ nguyên liệu đầu vào, quá trình sản xuất, vận chuyển, lưu kho đến tay người tiêu dùng – đều được ghi lại và xác thực một cách an toàn. Điều này không chỉ giúp các doanh nghiệp kiểm soát tốt hơn quy trình sản xuất và phân phối mà còn gia tăng niềm tin nơi người tiêu dùng. Đồng thời, công nghệ Blockchain góp phần hỗ trợ đáp ứng các tiêu chuẩn quốc tế về truy xuất nguồn gốc, đặc biệt trong lĩnh vực nông nghiệp, thực phẩm, và dược phẩm.

## Kiến nghị:

Sau quá trình nghiên cứu và triển khai ứng dụng công nghệ Blockchain vào quản lý chuỗi cung ứng và truy xuất nguồn gốc hàng hoá, chúng tôi nhận thấy đây là một giải pháp hiệu quả và cần thiết trong bối cảnh hiện nay. Hệ thống giúp nâng cao tính minh bạch, đảm bảo độ tin cậy của thông tin sản phẩm và tăng cường khả năng kiểm soát trong toàn bộ chuỗi giá trị. Công nghệ Blockchain cho phép ghi lại mọi giao dịch, biến động hàng hoá một cách bất biến, minh bạch, hỗ trợ doanh nghiệp và người tiêu dùng dễ dàng truy xuất nguồn gốc thông qua mã QR hoặc mã định danh kỹ thuật số, đồng thời góp phần nâng cao năng lực xử lý sự cố và đáp ứng các yêu cầu tiêu chuẩn quốc tế về truy xuất. Để phát huy tối đa hiệu quả của hệ thống, chúng tôi kiến nghị tiếp tục phát triển và mở rộng các chức năng, tích hợp thêm các công nghệ tiên tiến như Trí tuệ nhân tạo (AI) và Internet of Things (IoT) nhằm tự động hoá quy trình, phân tích dữ liệu theo thời gian thực, và nâng cao hiệu suất vận hành. Ngoài ra, cần chú trọng đến việc đào tạo và hỗ trợ người dùng để đảm bảo khả năng vận hành hiệu quả, đồng thời áp dụng các biện pháp bảo mật hiện đại nhằm bảo vệ dữ liệu và quyền riêng tư. Việc duy trì cơ chế tiếp nhận phản hồi từ người dùng cũng đóng vai trò quan trọng trong việc hoàn thiện hệ thống, hướng đến một nền chuỗi cung ứng minh bạch, an toàn và bền vững.

# **DANH MỤC TÀI LIỆU THAM KHẢO**

**Tiếng Việt:**

**Tiếng Anh:**