**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**



**CÁC HỆ QUẢN TRỊ CƠ SỞ DỮ LIỆU**

*Đề tài*

**hợp đồng thông minh**

GVHD: Th.S PHẠM ĐỨC THÀNH

SVTH: TRƯƠNG TẤN DŨNG 16DH110449

HUỲNH NGỌC VY 16DH110448

LÊ ANH SONG 16DH110901

**TP. Hồ Chí Minh, Tháng 07 Năm 2020**

**MỤC LỤC**

[DANH MỤC CÁC BẢNG BIỂU 4](#_Toc42532856)

[DANH MỤC CÁC HÌNH VẼ 5](#_Toc42532857)

[CHƯƠNG 1: GIỚI THIỆU ĐỀ TÀI 7](#_Toc42532858)

[**1.1. Sơ lược về đề tài: 7**](#_Toc42532859)

[**1.2. Khảo sát ứng dụng: 7**](#_Toc42532860)

[**1.3. Nội dung đề tài 9**](#_Toc42532861)

[**1.4. Chức năng của chương trình 9**](#_Toc42532862)

[**1.5. Bố cục đề tài 9**](#_Toc42532863)

[CHƯƠNG 2: CÔNG NGHỆ LIÊN QUAN 10](#_Toc42532864)

[**2.1. Sơ lược về Blockchain: 10**](#_Toc42532865)

[**2.1.1. Blockchain là gì ? 10**](#_Toc42532866)

[**2.1.2. Ưu điểm và nhược điểm: 11**](#_Toc42532867)

[**2.1.3. Hình thức hoạt động của Blockchain: 11**](#_Toc42532868)

[**2.1.4. Đặc điểm của công nghệ Blockchain: 12**](#_Toc42532869)

[**2.1.5. Các loại và phiên bản của Blockchain hiện nay: 12**](#_Toc42532870)

[**2.1.6. Tương lai của công nghệ Blockchain: 13**](#_Toc42532871)

[**2.2. Smart Contract (Hợp đồng thông minh) là gì? 13**](#_Toc42532872)

[**2.3. Tiền kỹ thuật số là gì? 14**](#_Toc42532873)

[**2.4. Giới thiệu về Testnet: 14**](#_Toc42532874)

[**2.5. Ngôn ngữ Solidity: 15**](#_Toc42532875)

[**2.6. Giới thiệu về Ethereum: 16**](#_Toc42532876)

[**2.7. Giới thiệu về Infura: 17**](#_Toc42532877)

[CHƯƠNG 3: PHÂN TÍCH THIẾT KẾ 18](#_Toc42532878)

[**3.1. Phân tích 18**](#_Toc42532879)

[**3.1.1. Sơ đồ phân cấp chức năng: 18**](#_Toc42532880)

[**3.1.2. Chức năng hệ thống 19**](#_Toc42532881)

[**3.1.3. Sơ đồ Use Case: 19**](#_Toc42532882)

[**3.2. Thiết kế 20**](#_Toc42532885)

[**3.2.1. Thiết kế giao diện 20**](#_Toc42532886)

[**3.2.2. Cơ sở dữ liệu 28**](#_Toc42532887)

[**3.2.3. Thiết kế xử lý 32**](#_Toc42532888)

[CHƯƠNG 4: KẾT LUẬN 37](#_Toc42532889)

[**4.1. Kết quả đã đạt được 37**](#_Toc42532890)

[**4.1.1. Giao diện đăng nhập: 37**](#_Toc42532891)

[**4.1.2. Giao diện danh sach mạng thử nghiệm: 37**](#_Toc42532892)

[**4.1.3. Giao diện khôi phục mật khẩu: 38**](#_Toc42532893)

[**4.1.4. Giao diện chính của ví: 38**](#_Toc42532894)

[**4.1.5. Giao diện danh sách tài khoản: 39**](#_Toc42532895)

[**4.1.6. Giao diện lịch sử giao dịch: 39**](#_Toc42532896)

[**4.1.7. Giao diện chi tiết tài khoản 1: 40**](#_Toc42532897)

[**4.1.8. Giao diện chi tiết tài khoản 2: 40**](#_Toc42532898)

[**4.1.9. Giao diện ký gửi Ether: 41**](#_Toc42532899)

[**4.1.10. Giao diện chuyển khoản: 41**](#_Toc42532900)

[**4.1.11. Giao diện tạo tài khoản mới: 42**](#_Toc42532901)

[**4.1.12. Giao diện import tài khoản mới: 42**](#_Toc42532902)

[**4.1.13. Giao diện thêm sản phẩm (Chi tiết): 43**](#_Toc42532903)

[**4.1.14. Giao diện thêm sản phẩm (Dữ liệu): 43**](#_Toc42532904)

[**4.1.15. Giao diện thêm sản phẩm (Lựa chọn hình thức): 44**](#_Toc42532905)

[**4.1.16. Giao diện danh sách sản phẩm: 44**](#_Toc42532906)

[**4.1.17. Giao diện mua sản phẩm: 45**](#_Toc42532907)

[**4.1.18. Giao diện chi tiết giao dịch (Chi tiết): 46**](#_Toc42532908)

[**4.1.19. Giao diện chi tiết giao dịch (Dữ liệu) 47**](#_Toc42532909)

[**4.1.20. Giao diện chi tiết giao dịch (Trang thái): 47**](#_Toc42532910)

[**4.1.21. Giao diện bản hợp đồng thông minh: 48**](#_Toc42532911)

[**4.2. Hạn chế: 48**](#_Toc42532912)

[**4.3. Hướng phát triển: 49**](#_Toc42532913)

[TÀI LIỆU THAM KHẢO 50](#_Toc42532914)

# **DANH MỤC CÁC BẢNG BIỂU**

[Bảng 1-3.2.1b: Bảng mô tả các thao tác xử lý trên giao diện đăng nhập. 21](#_Toc43195053)

[Bảng 2-3.2.1c: Bảng mô tả các thao tác xử lí trên giao diện tài khoản. 22](#_Toc43195054)

[Bảng 3-3.2.1d: Bảng mô tả các thao tác xử lí trên giao diện chi tiết tài khoản. 23](#_Toc43195055)

[Bảng 4-3.2.1e: Bảng mô tả các thao tác xử lí trên giao diện danh sách tài khoản. 24](#_Toc43195056)

[Bảng 5-3.2.1f: Bảng mô tả các thao tác xử lí trên giao diện import tài khoản. 25](#_Toc43195057)

[Bảng 6-3.2.1g: Bảng mô tả các thao tác xử lí trên giao diện tạo tài khoản. 26](#_Toc43195058)

[Bảng 7-3.2.1h: Bảng mô tả các thao tác xử lí trên giao diện đăng nhập. 27](#_Toc43195059)

[Bảng 8-3.2.2b: Bảng mô tả cơ sở dữ liệu của bảng Product. 29](#_Toc43195060)

[Bảng 9-3.2.2c: Bảng mô tả cơ sở dữ liệu của bảng ProductCreated. 29](#_Toc43195061)

[Bảng 10-3.2.2d: Bảng mô tả cơ sở dữ liệu của bảng ProductPurchased. 30](#_Toc43195062)

[Bảng 11-3.2.3a: Bảng mô tả danh sách các biến cố. 31](#_Toc43195063)

# **DANH MỤC CÁC HÌNH VẼ**

[Hình 1-1.1: Blockchain 6](#_Toc43581249)

[Hình 2-1.2: Bitproperty 8](#_Toc43581250)

[Hình 3-1.2: Deedcoin 8](#_Toc43581251)

[Hình 4-1.2: Ubitquity 9](#_Toc43581252)

[Hình 5-2.1.2: Cấu trúc chuỗi khối 10](#_Toc43581253)

[Hình 6-2.2.1: Đồng tiền kỹ thuật số 14](#_Toc43581254)

[Hình 7-2.2.4: Ngôn ngữ Solidity 15](#_Toc43581255)

[Hình 8-2.2.5: Nền tảng Ethereum 16](#_Toc43581256)

[Hình 9-2.2.6: Infura 17](#_Toc43581257)

[Hình 10-3.1.1: Sơ đồ phân cấp chức năng. 18](#_Toc43581258)

[Hình 11-3.1.3: Use Case Seller. 19](#_Toc43581259)

[Hình 12-3.1.3: Use Case Buyer. 20](#_Toc43581260)

[Hình 13-3.2.1a: Sitemap 20](#_Toc43581261)

[Hình 14-3.2.1b: Đăng nhập ví. 21](#_Toc43581262)

[Hình 15-3.2.1c: Giao diện tài khoản . 22](#_Toc43581263)

[Hình 16-3.2.1d: Chi tiết tài khoản. 23](#_Toc43581264)

[Hình 17-3.2.1e: Danh sách tài khoản. 24](#_Toc43581265)

[Hình 18-3.2.1f: Import tài khoản. 25](#_Toc43581266)

[Hình 19-3.2.1g: Tạo tài khoản. 26](#_Toc43581267)

[Hình 20-3.2.1h: Giao diện trang chủ. 27](#_Toc43581268)

[Hình 21-3.2.2a: Sơ đồ lớp 28](#_Toc43581269)

[Hình 22-3.2.2a: Sequence Diagram 29](#_Toc43581270)

[Hình 23-3.2.3b: Sơ đồ đăng nhập. 33](#_Toc43581271)

[Hình 24-3.2.3c: Sơ đồ khôi phục tài khoản. 33](#_Toc43581272)

[Hình 25-3.2.3d: Sơ đồ thêm tài khoản. 33](#_Toc43581273)

[Hình 26-3.2.3e: Sơ đồ mạng thử nghiệm. 34](#_Toc43581274)

[Hình 27-3.2.3f: Sơ đồ ký gửi/nạp tiền. 34](#_Toc43581275)

[Hình 28-3.2.3g: Sơ đồ gửi tiền. 34](#_Toc43581276)

[Hình 29-3.2.3h: Sơ đồ thêm tokens. 35](#_Toc43581277)

[Hình 30-3.2.3i: Sơ đồ đăng xuất. 35](#_Toc43581278)

[Hình 31-3.4.3: Sơ đồ import tài khoản. 35](#_Toc43581279)

[Hình 32-3.4.3: Sơ đồ tạo tài khoản. 36](#_Toc43581280)

[Hình 33-3.4.4: Sơ đồ thêm sản phẩm. 36](#_Toc43581281)

[Hình 34-4.1.1: Giao diện đăng nhập. 37](#_Toc43581282)

[Hình 35-4.1.2: Giao diện danh sách mạng thử nghiệm. 37](#_Toc43581283)

[Hình 36-4.1.3: Giao diện khôi phục mật khẩu. 38](#_Toc43581284)

[Hình 37-4.1.4: Giao diện chính của ví. 38](#_Toc43581285)

[Hình 38-4.1.5: Giao diện danh sách tài khoản. 39](#_Toc43581286)

[Hình 39-4.1.6: Giao diện lịch sử giao dịch. 39](#_Toc43581287)

[Hình 40-4.1.7: Giao diện chi tiết tài khoản 1. 40](#_Toc43581288)

[Hình 41-4.1.8: Giao diện chi tiết tài khoản 2. 40](#_Toc43581289)

[Hình 42-4.1.9: Giao diện ký gửi Ether 41](#_Toc43581290)

[Hình 43-4.1.10: Giao diện chuyển khoản. 41](#_Toc43581291)

[Hình 44-4.1.11: Giao diện tạo tài khoản mới. 42](#_Toc43581292)

[Hình 45-4.1.12: Giao diện import tài khoản mới. 42](#_Toc43581293)

[Hình 46-4.1.13: Giao diện thêm sản phẩm (Chi tiết). 43](#_Toc43581294)

[Hình 47-4.1.14: Giao diện thêm sản phẩm (Dữ liệu). 43](#_Toc43581295)

[Hình 48-4.1.15: Giao diện thêm sản phẩm (Lựa chọn hình thức). 44](#_Toc43581296)

[Hình 49-4.1.16: Giao diện danh sách sản phẩm. 44](#_Toc43581297)

[Hình 50-4.1.17: Giao diện mua sản phẩm (Chi tiết). 45](#_Toc43581298)

[Hình 51-4.1.18: Giao diện mua sản phẩm (Dữ liệu). 45](#_Toc43581299)

[Hình 52-4.1.19: Giao diện mua sản phẩm (Lựa chọn hình thức). 46](#_Toc43581300)

[Hình 53-4.1.20: Giao diện chi tiết giao dịch (Chi tiết). 46](#_Toc43581301)

[Hình 54-4.1.21: Giao diện chi tiết giao dịch (Dữ liệu). 47](#_Toc43581302)

[Hình 55-4.1.22: Giao diện chi tiết giao dịch (Trạng thái). 47](#_Toc43581303)

[Hình 56-4.1.23: Giao diện bản hợp đồng thông minh. 48](#_Toc43581304)

# **CHƯƠNG 1: GIỚI THIỆU ĐỀ TÀI**

* 1. **Sơ lược về đề tài:**

Blockchain là công nghệ dù đã ra đời từ lâu nhưng những năm gần đây Blockchain mới được rất nhiều công ty tìm hiểu và đi theo hướng áp dụng kỹ thuật công nghệ này vào doanh nghiệp của mình. Blockchain có những công nghệ rất nổi bật như: Ví điện tử để lưu trữ các đồng tiền kỹ thuật số, bản hợp đồng thông minh (Smart Contracts),..



*Hình 1-1.1: Blockchain*

* 1. **Khảo sát ứng dụng:**

Ứng dụng hữu ích đầu tiên được biết đến rộng rãi từ công nghệ Blockchain có lẽ là Bitcoin và tiền mã hóa, nhưng bây giờ có lẽ đã tiến xa hơn nhiều. Blockchain giờ đây đang cách mạng hóa hầu hết các ngành công nghiệp. Dưới đây là một vài ví dụ thiết thực về công nghệ Blockchain:

* **Hợp đồng thông minh:**



*Hình 2-1.2: Bitproperty*

**BitProperty:** Sử dụng Blockchain và hợp đồng thông minh, BitProperty cho phép bất cứ ai ở bất cứ nơi nào trên thế giới (trừ Mỹ và Nhật Bản, do các vấn đề về pháp lý) đều có thể đầu tư vào bất động sản.



*Hình 3-1.2: Deedcoin*

**Deedcoin:** Thay vì một khoản hoa hồng 6% trong ngành bất động sản, với Deedcoin, mức phí chỉ là 1% và kỳ vọng vào cách mới cho người mua và bán nhà kết nối với các đại lý bất động sản chấp nhận mức hoa hồng thấp hơn.



*Hình 4-1.2: Ubitquity*

**Ubitquity:** Nền tảng Blockchain phần mềm như dịch vụ (Saas) này cung cấp trải nghiệm người dùng đơn giản hơn để ghi lại thông tin bất động sản một cách an toàn nhằm đảm bảo hồ sơ rõ ràng về quyền sở hữu.

* 1. **Nội dung đề tài**

**Xây dựng trình duyệt web quản lý sản phẩm kết nối với hợp đồng thông minh (Smart Contracts) bằng ngôn ngữ Solidity, sau đó đưa lên Blockchain để mã hóa và Blockchain sẽ hỗ trợ giao dịch theo hợp đồng.**

* 1. **Chức năng của chương trình**

**Mục tiêu của bài báo này muốn giới thiệu tới mọi người về cách thức hoạt động của một bản hợp đồng thông minh. Qua đó bài báo cáo về của nhóm chúng tôi có những chức nằng hoạt động sau:**

* **Tạo ra một trang website đơn giản để soạn thảo hợp đồng buôn bán sản phẩm với đối tác.**
* **Liên kết mọi giao dịch mua bán sản phẩm thông qua ví ảo MetaMask.**
* **Bản hợp đồng sau khi được tạo sẽ được deploy lên Testnet.**
* **Chạy được trên nền tảng Remix IDE.**
  1. **Bố cục đề tài**
* Chương 1: Giới thiệu đề tài.
* Chương 2: Công nghệ liên quan.
* Chương 3: Phân tích thiết kế.
* Chương 4: Kết luận.

# **CHƯƠNG 2: CÔNG NGHỆ LIÊN QUAN**

* 1. **Sơ lược về Blockchain:**

Nhiều người từng cho rằng công nghệ Blockchain là công nghệ tạo ra những đồng tiền ảo điển hình nhất là đồng Bitcoin, nhưng thật sự không phải như vậy Blockchain còn tạo ra những thứ vĩ đại hơn thế.

Blockchain có tiềm năng sẽ thay đổi tất cả mọi thứ, mọi người có thể không thực sự hiểu Blockchain là gì nhưng nó chắc chắn sẽ thay đổi cuộc sống của chúng ta.

* + 1. **Blockchain là gì ?**

**Blockchain** hay còn được biết đến như cuốn sổ cái, là một cơ sở dữ liệu phân cấp lưu trữ thông tin được liên kết với nhau bằng mã hóa.

Các khối thông tin này hoạt động độc lập và chúng có thể mở rộng theo thời gian. Và điều đặc biệt là chúng được quản lý bởi những người tham gia vào hệ thống chứ không qua bất kỳ đơn vị trung gian nào.

Nghĩa là một khối thông tin khi ghi vào hệ thống lưu trữ Blockchain thì không có cách nào thay đổi được. Chỉ có thể bổ sung thêm khi đạt được sự đồng thuận của tất cả mọi người tham gia mạng. Nó là hệ thống ngang hàng **Peer to Peer** loại bỏ tất cả mọi khâu trung gian, làm tăng cường an ninh, sự minh bạch và ổn định cũng như giảm thiểu chi phí và lỗi do con người gây ra. Và khối thông tin được nhắc đến ở đây chính là những cuộc trao đổi, giao dịch xảy ra trong thực tế cuộc sống.

Công nghệ Blockchain đã tạo ra xương sống cho một loại hình Internet mới khi cho phép phân phối các thông tin kỹ thuật số nhưng không được sao chép.

Ảnh có chứa đối tượng, đồng hồ

Mô tả được tạo tự động

*Hình 5-2.1.2: Cấu trúc chuỗi khối*

* + 1. **Ưu điểm và nhược điểm:**

1. **Ưu điểm:**
   * Dữ liệu không bị mất.
   * Không thể chỉnh sửa và xóa đi nên có tính ổn định cao.
   * Không cần bên trung gian hay còn gọi là bên thứ ba để giao dịch.
   * Dữ liệu chất lượng cao, dữ liệu liên tục được cập nhật và phổ biến rộng rãi.
   * Tính minh bạch và không thể thay đổi.
   * Các giao dịch nhanh hơn.
   * Giao dịch xuyên biên giới.
   * Tiết kiệm chi phí.
2. **Nhược điểm:**
   * Blockchain sẽ luôn chậm hơn so với các cơ sở dữ liệu tập trung.
   * Vấn đề tích hợp sửa đổi dữ liệu khó khăn.
   * Mức độ tiêu thụ năng lượng lớn.
   * Tốn nhiều chi phí đầu tư ban đầu.
   * Cuộc tấn công 51% (Nhưng rất khó để làm điều này).
   * Sự bất tiện của khóa riêng (Người dùng sử dụng khóa riêng để truy cập vào tiền quỹ và khi mất khóa riêng tiền sẽ bị mất và không thể làm gì khác).
     1. **Hình thức hoạt động của Blockchain:**

* Có 4 yếu tố để khối thông tin được thêm vào Blockchain:
  + Phải có giao dịch.
  + Giao dịch phải được xác minh.
  + Giao dịch phải được lưu trữ trong block.
  + Block phải được hash (Hàm chuyển đổi một giá trị sang giá trị khác, block chỉ có thể được thêm vào Blockchain khi nhận được hash).
    1. **Đặc điểm của công nghệ Blockchain:**
  + **Một cơ sở dữ liệu phân tán:** Cơ sở dữ liệu Blockchain được lưu trữ một cách công khai, dễ kiểm chứng. Không có một phiên bản tập trung nào của cơ sở dữ liệu này tồn tại, Blockchain được lưu trữ bởi hàng triệu máy tính cùng lúc.
  + **Không thể làm giả, không thể bị phá hủy các chuỗi Blockchain**: theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu.
  + **Bất biến và không thay đổi**: Dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.
  + **Bảo mật: Công nghệ mã hóa với cặp khóa private - public.** Các thông tin, dữ liệu trong Blockchain được an toàn tuyệt đối.
  + **Minh bạch:** Ai cũng có thể theo dõi dữ liệu Blockchain và xem toàn bộ lịch sử trên địa chỉ đó.
  + **Hợp đồng thông minh - Smart Contract:** là hợp đồng kỹ thuật số được nhúng đoạn mã code “if this then that” cho phép chúng tự thực thi mà không cần bên thứ ba.
    1. **Các loại và phiên bản của Blockchain hiện nay:**
* Blockchain có 3 loại: Public, Private, Permissoned.
* Blockchain có 4 phiên bản:
  + Blockchain 1.0: Tiền tệ và thanh toán.
  + Blockchain 2.0: Tài chính và thị trường.
  + Blockchain 3.0: Thiết kế và giám sát hoạt động.
  + Blockchain 4.0: Gồm các lĩnh vực liên quan tới cách mạng công nghiệp 4.0 (AI, IoT, Big Data,…).
    1. **Tương lai của công nghệ Blockchain:**

Nói một cách ngắn gọn thì Blockchain đang giống như Internet đã trải qua cuộc khủng hoảng mạnh mẽ ở năm 1999 và không chịu ngừng ở đó Internet đã không biến mất mà nó vẫn tiếp tục hoàn thiện mình và định hình toàn bộ ngành công nghiệp cho tới bây giờ. Blockchain cũng giống như Internet ở phiên bản thứ 2 được thể hiện qua:

* + Các chuyên gia đồng ý và khẳng định rằng blockchain có tiềm năng thay đổi hầu hết mọi thứ.
  + Những công ty lớn vẫn đang đầu tư rất mạnh và đang thử nghiệm, ứng dụng Blockchain trong nhiều lĩnh vực khác nhau và đã thu được các phản hồi tích cực.
  + Hiện chưa có cơ sở hạ tầng Blockchain ở cấp độ toàn cầu hay quốc tế nhưng nó vẫn thu hút được rất nhiều người thí điểm.
  + Mọi người không thực sự hiểu Blockchain là gì nhưng nó chắc chắn sẽ thay đổi cuộc sống của chúng ta.
  1. **Smart Contract (Hợp đồng thông minh) là gì?**

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

* 1. **Tiền kỹ thuật số là gì?**

**Tiền kỹ thuật số**(Digital Currency) là một dạng tiền tệ chỉ có sẵn ở dạng kỹ thuật số hoặc điện tử, và không ở dạng vật lý.

Ảnh có chứa bàn, khác nhau, đầy đủ, nhiều

Mô tả được tạo tự động

*Hình 6-2.2.1: Đồng tiền kỹ thuật số*

* 1. **Giới thiệu về Testnet:**

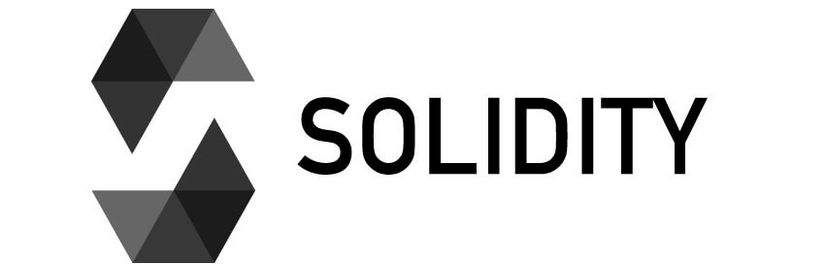
1. **Testnet là gì?**

* Testnet là một cơ chế để các lập trình viên thử nghiệm các tính năng của phần mềm trước khi áp dụng vào một loại tiền điện tử nhất định mà không sợ xảy ra bất kỳ sai sót nào.
* Cơ chế Testnet cũng giống như [Mainnet](https://bitcoinvietnamnews.com/mainnet-la-gi" \t "_blank), bao gồm một Blockchain, một mạng lưới các node, thợ mỏ, người dùng. Tất cả phục vụ cho việc thử nghiệm hệ thống.
* Bạn có thể đánh giá được loại tiền điện tử thông qua việc sử dụng mạng lưới Testnet.

1. **Tầm quan trọng của Testnet:**

* **Phát triển liên tục:** Công nghệ chuỗi khối Blockchain vẫn đang trong giai đoạn sơ khai và cần một lượng lớn các thử nghiệm và phát triển để dần tiến tới việc được cho phép sử dụng và chính thống. Môi trường của testnet được tạo ra để phục vụ cho điều này.
* **An toàn cho mainnet:** Testnet cho phép người kiểm tra và nhà phát triển ứng dụng thử nghiệm các tính năng và chức năng của giao thức trong một môi trường riêng biệt mà không phải lo lắng về việc phá vỡ chuỗi khối chính. Thực hiện các thử nghiệm trên mainnet là điều không thể thực hiện vì các tương tác phức tạp giữa các thành phần trong giao thức có thể làm tổn hại mạng hoặc phá vỡ chuỗi chính.
* **Thử nghiệm miễn phí:** Sẽ rất tốn kém cho các nhà phát triển để kiểm tra các tính năng ứng dụng hoặc chạy thử nghiệm trên mainnet, vì họ sẽ cần mua số lượng lớn các đồng tiền điện tử với giá trị thực. Testnets cung cấp một nền tảng thử nghiệm cho các nhà phát triển, những người muốn tạo ra các ứng dụng trên Blockchain hoặc thử nghiệm các chức năng nhất định mà không cần trả phí.
  1. **Ngôn ngữ Solidity**:

**Solidity** là ngôn ngữ lập trình high-level dùng để cài đặt hợp đồng thông minh (smart contract). Nó là một ngôn ngữ hướng đối tượng được thiết kế dành riêng cho Ethereum Virtual Machine. Solidity khá giống Javascript, hiện tại là ngôn ngữ phổ biến nhất cho lĩnh vực này.



*Hình 7-2.2.4: Ngôn ngữ Solidity*

* 1. **Giới thiệu về Ethereum:**
* **Ethereum (ETH) là:**
* Một nền tảng (platform) chạy trên nền tảng công nghệ Blockchain.
* Hỗ trợ hợp đồng thông minh (smart contract).
* Mạng lưới sử dụng tiền mã hoá 2.0.
* Sử dụng blockchain riêng.
* Có dự định chuyển từ sử dụng Proof of Work (Ethash) sang Proof of Stake (Casper).
* Có thể viết chương trình kiểu model Turing Complete chạy trên nền giao thức P2P.

Ảnh có chứa cửa sổ, sáng

Mô tả được tạo tự động

*Hình 8-2.2.5: Nền tảng Ethereum*

* 1. **Giới thiệu về Infura:**

**Infura** là một cơ sở hạ tầng rất quan trọng trên Blockchain Ethereum. Đây là một công cụ dành cho nhà phát triển, Infura dễ sử dụng, cung cấp quyền truy cập an toàn, đáng tin cậy và có thể mở rộng để truy cập Ethereum blockchain và IPFS. Hãy để các nhà phát triển tập trung vào việc phát triển DApps hơn là giải quyết những rắc rối của cơ sở hạ tầng.



*Hình 9-2.2.6: Infura*

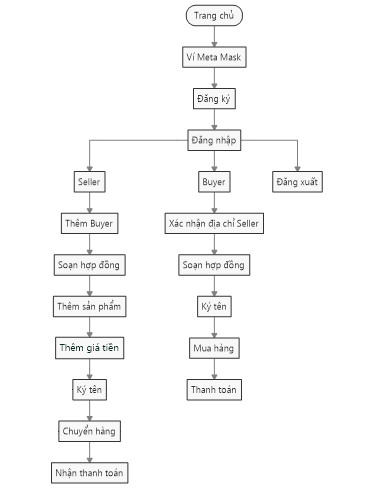
Từ góc nhìn chuyên nghiệp, Infura là một sản phẩm IaaS (Cơ sở hạ tầng như một dịch vụ “Infrastructure as a Service”) được thiết kế để giảm các rào cản truy cập dữ liệu của Ethereum.

Nói chung, Infura là một nền tảng cho phép DApp của bạn nhanh chóng truy cập vào Ethereum mà không cần phải chạy các nút Ethereum cục bộ. Đồng thời nó cũng miễn phí.

Infura sẽ là một phần rất quan trọng trong hệ sinh thái ETC.

# **CHƯƠNG 3: PHÂN TÍCH THIẾT KẾ**

* 1. **Phân tích**
     1. **Sơ đồ phân cấp chức năng:**

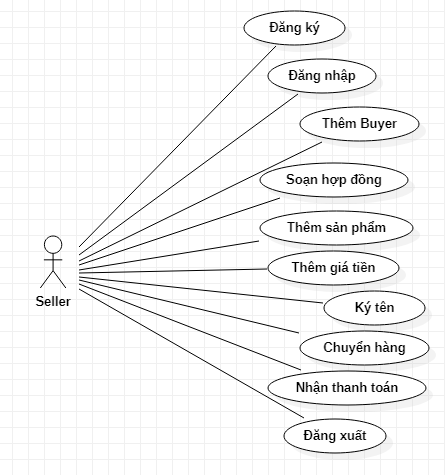


*Hình 10-3.1.1: Sơ đồ phân cấp chức năng.*

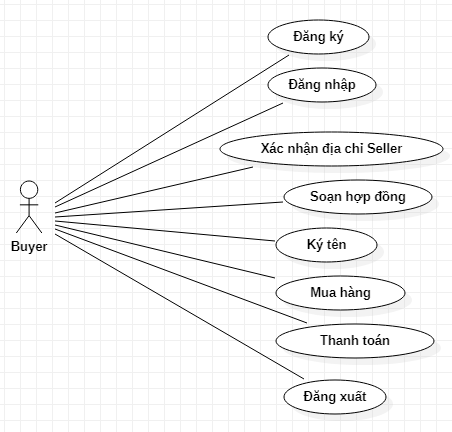
* + 1. **Chức năng hệ thống**

Gồm 2 phần: Front-end và Back-end.

* Front-end:
  + Thiết lập trình duyệt web kết nối với blockchain.
  + Đăng nhập, đăng ký thông qua liên kết với ví ảo.
  + Soạn thảo hợp đồng.
  + Danh sách sản phẩm.
  + Bán sản phẩm.
  + Mua sản phẩm.
* Back-end:
  + Thêm sản phẩm.
  + Thêm giá tiền.
    1. **Sơ đồ Use Case:**

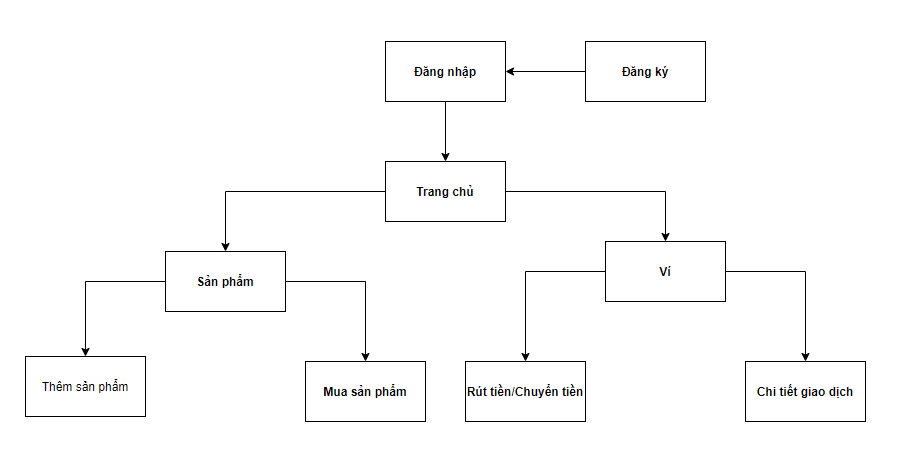


*Hình 11-3.1.3: Use Case Seller.*



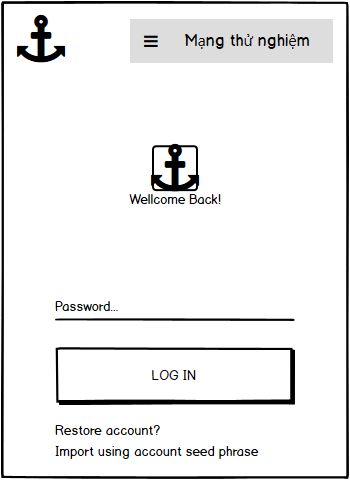
*Hình 12-3.1.3: Use Case Buyer.*

* 3. **Thiết kế**
     1. **Thiết kế giao diện**
     2. **Sơ đồ màn hình**



*Hình 13-3.2.1a: Sitemap*

* + 1. **Giao diện đăng nhập:**



*Hình 14-3.2.1b: Đăng nhập ví.*

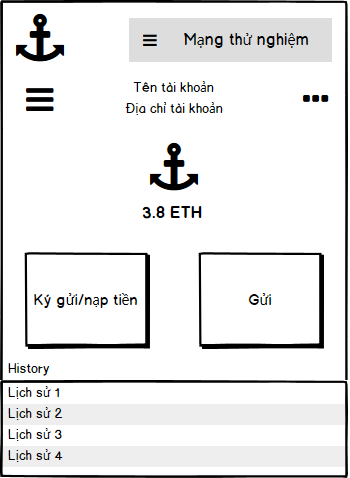
* **Các thao tác xử lí trên giao diện:**

Đây là giao diện MetaMask được chạy trên trình duyệt Chorme dưới dạng tiện ích mở rộng. Muốn tạo tài khoản cần vào địa chỉ <https://metamask.io/> để tải trình duyệt về và làm theo hướng dẫn để tạo.

Bảng 1*-3.2.1b: Bảng mô tả các thao tác x*ử lý *trên giao diện đăng nhập.*

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 1 | Đăng nhập. | Khi người dùng click chuột vào nút Log in. |
| 2 | Khôi phục tài khoản. | Khi người dùng click chuột vào Restore account. |
| 3 | Thêm tài khoản. | Khi người dùng click chuột vào Import using account seed phrase. |
| 4 | Mạng thử nghiệm. | Khi người dùng click chuột vào Mạng lưới thử nghiệm. |

* + 1. **Giao diện tài khoản:**



*Hình 15-3.2.1c: Giao diện tài khoản .*

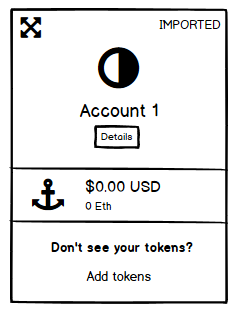
* Các thao tác xử lí trên giao diện:

Khi đã đăng nhập thành công thì giao diện chính của ví sẽ như thế này. ETH ở đây là đồng tiền mã hóa trong mạng lưới Ethereum. History là danh sách lịch sử giao dịch khi bạn gửi tiền, nhận tiền hoặc hoàn tất một bản hợp đồng thông minh.

Bảng 2*-3.2.1c: Bảng mô tả các thao tác xử lí trên giao diện tài khoản.*

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 5 | Ký gửi/nạp tiền vào tài khoản. | Khi người dùng click chuột vào Ký gửi/nạp tiền. |
| 6 | Gửi tiền vào tài khoản khác. | Khi người dùng click chuột vào Gửi. |

* + 1. **Giao diện chi tiết tài khoản:**



*Hình 16-3.2.1d: Chi tiết tài khoản.*

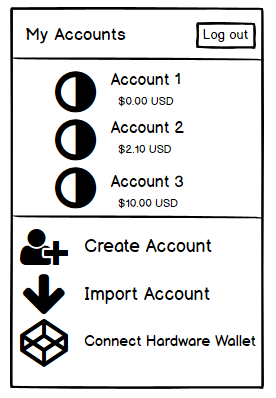
* **Các thao tác xử lí trên giao diện:**

Đây là giao diện chi tiết tài khoản, cho phép người dùng có thể theo dõi thông tin giao dịch, mã khóa cá nhân và đổi tên tài khoản.

Bảng 3*-3.2.1d: Bảng mô tả các thao tác xử lí trên giao diện chi tiết tài khoản.*

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 7 | Thêm tokens. | Khi người dùng click chuột vào Add tokens. |

* + 1. **Giao diện danh sách tài khoản:**



*Hình 17-3.2.1e: Danh sách tài khoản.*

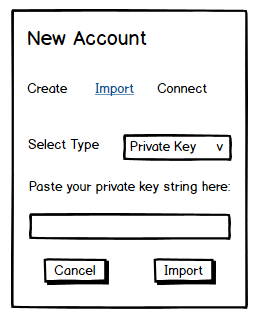
* **Các thao tác xử lí trên giao diện:**

Button “Create Account”: Có chức năng tạo một account mới ngay trong ví của bạn, button “Import Account”: Có chức năng cũng gần giống Create Account nhưng bạn cần có một dãy khóa cá nhân (Private Key), button “Connect Hardware Wallet”: Giúp kết nối MetaMask với các liên kết hỗ trợ.

*Bảng 4-3.2.1e: Bảng mô tả các thao tác xử lí trên giao diện danh sách tài khoản.*

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 8 | Đăng xuất. | Khi người dùng click chuột vào Log out. |

* + 1. **Giao diện import tài khoản:**



*Hình 18-3.2.1f: Import tài khoản.*

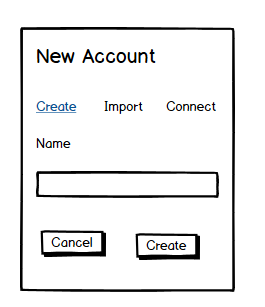
* **Các thao tác xử lí trên giao diện:**

Bạn cần dán đoạn mã cá nhân (Private Key) vào trong textbox rồi bấm button “Import” để thêm tài khoản mới vào trong ví của bạn.

*Bảng 5-3.2.1f: Bảng mô tả các thao tác xử lí trên giao diện import tài khoản.*

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 9 | Import tài khoản. | Khi người dùng click chuột vào Import. |

* + 1. **Giao diện tạo tài khoản:**



*Hình 19-3.2.1g: Tạo tài khoản.*

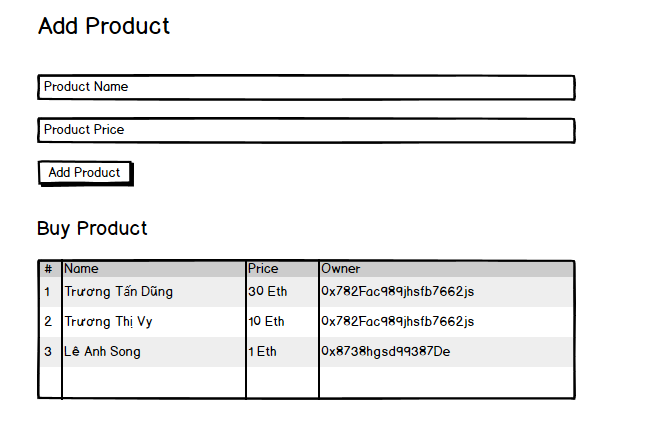
* + **Các thao tác xử lí trên giao diện:**

Bạn nhập tên tài khoản cần tạo (Được trùng) nhưng khác id sau đó bấm button “Create” để tạo tài khoản mới vào trong ví của bạn.

*Bảng 6-3.2.1g: Bảng mô tả các thao tác xử lí trên giao diện tạo tài khoản.*

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 10 | Tạo tài khoản. | Khi người dùng click chuột vào Create. |

1. **Giao diện trang chủ:**



*Hình 20-3.2.1h: Giao diện trang chủ.*

* **Các thao tác xử lí trên giao diện:**

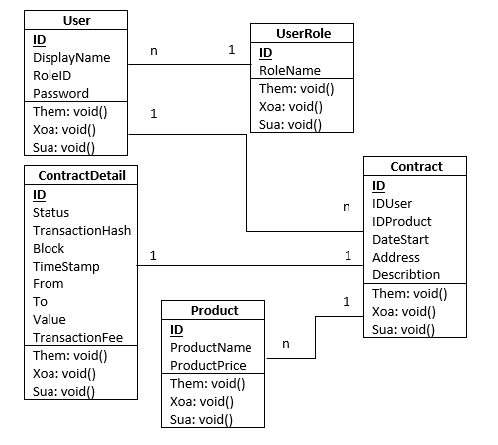
Textbox “Product Name”: Điền tên sản phẩm cần bán, textbox “Product Price”: Điền giá tiền cần bán theo dạng tiền ảo, sau khi điền đầy đủ thông tin bấm button “Add Product” sau đó sẽ ra giao diện ví MetaMask để bắt đầu thanh toán trả phí để deploy lên local Blockchain. Hoàn tất sản phẩm vừa nhập sẽ được add vào danh sách sản phẩm phía dưới.

*Bảng 7-3.2.1h: Bảng mô tả các thao tác xử lí trên giao diện đăng nhập.*

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 11 | Thêm sản phẩm. | Khi người dùng click chuột vào Add Product. |

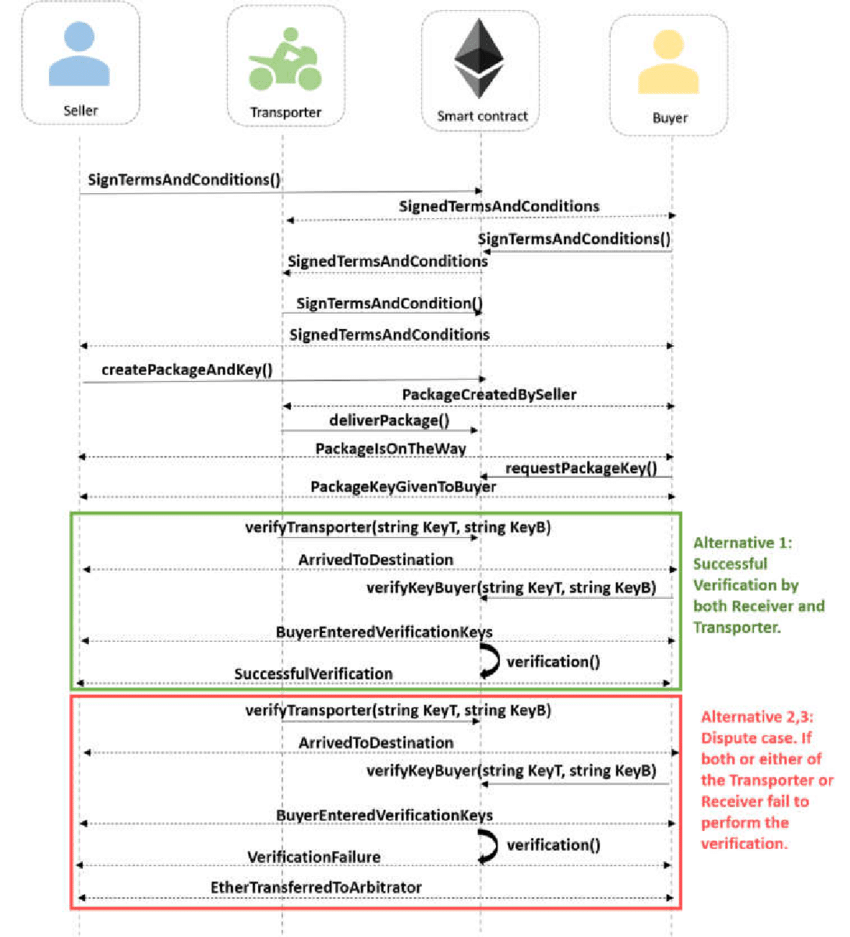
## Cơ sở dữ liệu

1. **Class Diagram:**



*Hình 21-3.2.2a: Sơ đồ lớp*

1. **Sequence Diagram:**

****

*Hình 22-3.2.2a: Sequence Diagram*

1. **Mô tả Table Product:**

Chứa thông tin mã sản phẩm, tên sản phẩm, giá tiền sản phẩm, địa chỉ đăng bán sản phẩm, trạng thái.

*Bảng 8-3.2.2b: Bảng mô tả cơ sở dữ liệu của bảng Product.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Độ dài** | **Not null** | **Diễn giải** |
| Id | Uint | 160 | Yes | Mã sản phẩm |
| Name | String | 100 | Yes | Tên sản phẩm |
| Price | Unit | 160 | Yes | Giá tiền sản phẩm |
| Owner | String | 100 | Yes | Address đăng bán sản phẩm |
| Purchased | bool |  | No | Trạng thái |

1. **Mô tả Table ProductCreated:**

Chứa thông tin mã sản phẩm bán, tên sản phẩm bán, giá tiền sản phẩm bán, Address đăng bán sản phẩm, trạng thái.

***Bảng 9-3.2.2c:*** *Bảng mô tả cơ sở dữ liệu của bảng ProductCreated.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Độ dài** | **Not null** | **Diễn giải** |
| Id | Uint | 160 | Yes | Mã sản phẩm bán |
| Name | String | 100 | Yes | Tên sản phẩm bán |
| Price | Unit | 160 | Yes | Giá tiền sản phẩm bán |
| Owner | String | 100 | Yes | Address đăng bán sản phẩm |
| Purchased | bool |  | No | Trạng thái (Còn hàng) |

1. **Mô tả Table ProductPurchased:**

Chứa thông tin mã sản phẩm mua, tên sản phẩm mua, giá tiền sản phẩm mua, địa chỉ mua sản phẩm, trạng thái.

*Bảng 10-3.2.2d: Bảng mô tả cơ sở dữ liệu của bảng ProductPurchased.*

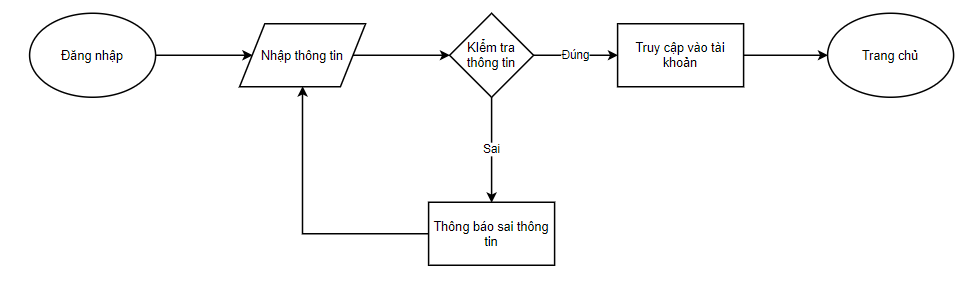
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Độ dài** | **Not null** | **Diễn giải** |
| Id | Uint | 160 | Yes | Mã sản phẩm mua |
| Name | String | 100 | Yes | Tên sản phẩm mua |
| Price | Unit | 160 | Yes | Giá tiền sản phẩm mua |
| Address payable | String | 100 | Yes | Address mua sản phẩm |
| Purchased | bool |  | No | Trạng thái (Đã mua) |

* + 1. **Thiết kế xử lý**
  1. **Danh sách các biến cố:**

*Bảng 11-3.2.3a: Bảng mô tả danh sách các biến cố.*

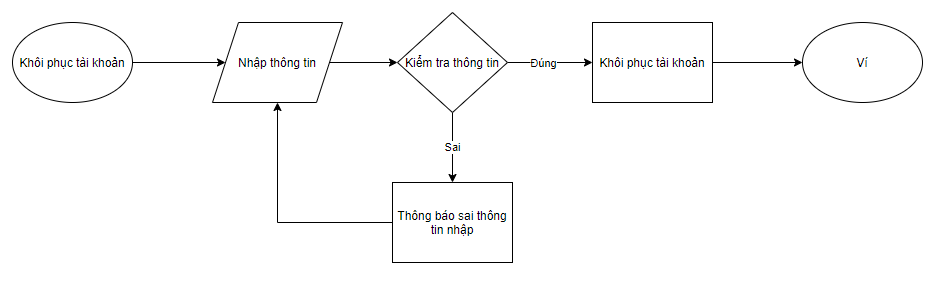
|  |  |  |
| --- | --- | --- |
| **STT** | **Tên biến cố** | **Ghi chú** |
| 1 | Đăng nhập. | Khi người dùng click chuột vào nút Log in. |
| 2 | Khôi phục tài khoản. | Khi người dùng click chuột vào Restore account. |
| 3 | Thêm tài khoản. | Khi người dùng click chuột vào Import using account seed phrase. |
| 4 | Mạng thử nghiệm. | Khi người dùng click chuột vào Mạng lưới thử nghiệm. |
| 5 | Ký gửi/nạp tiền vào tài khoản. | Khi người dùng click chuột vào Ký gửi/nạp tiền. |
| 6 | Gửi tiền vào tài khoản khác. | Khi người dùng click chuột vào Gửi. |
| 7 | Thêm tokens. | Khi người dùng click chuột vào Add tokens. |
| 8 | Đăng xuất. | Khi người dùng click chuột vào Log out. |
| 9 | Import tài khoản. | Khi người dùng click chuột vào Import. |
| 10 | Tạo tài khoản. | Khi người dùng click chuột vào Create Account. |
| 11 | Thêm sản phẩm. | Khi người dùng click chuột vào Add Product. |

* 1. **Biến cố 1: Đăng nhập**



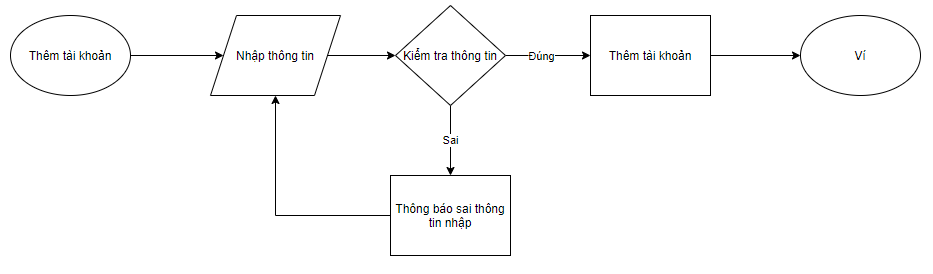
*Hình 23-3.2.3b: Sơ đồ đăng nhập.*

1. **Biến cố 2: Khôi phục tài khoản**



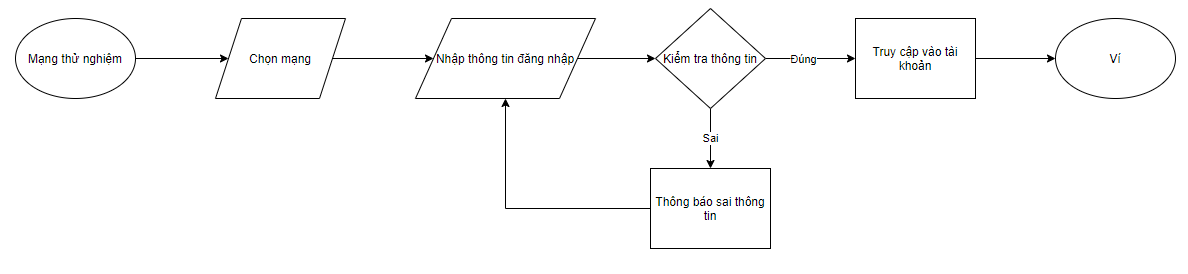
*Hình 24-3.2.3c: Sơ đồ khôi phục tài khoản.*

1. **Biến cố 3: Thêm tài khoản**



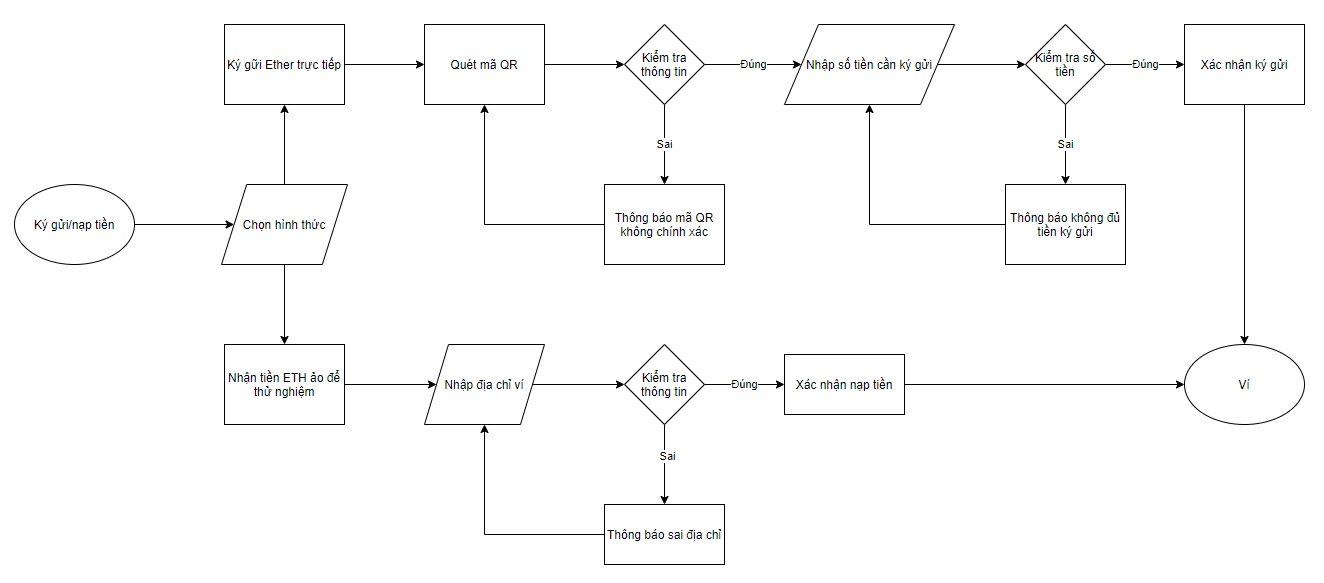
*Hình 25-3.2.3d: Sơ đồ thêm tài khoản.*

1. **Biến cố 4: Mạng thử ngiệm**



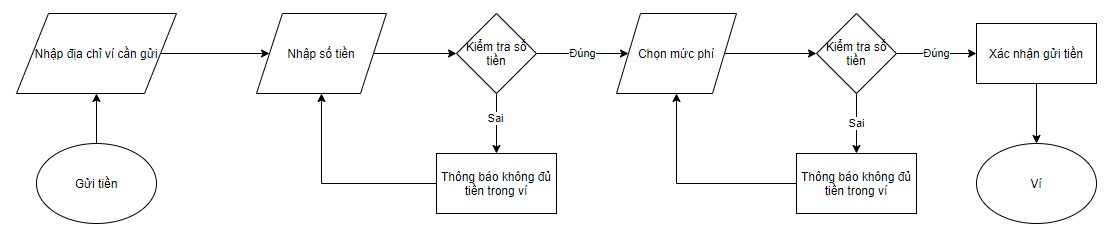
*Hình 26-3.2.3e: Sơ đồ mạng thử nghiệm.*

1. **Biến cố 5: Ký gửi/nạp tiền vào tài khoản**



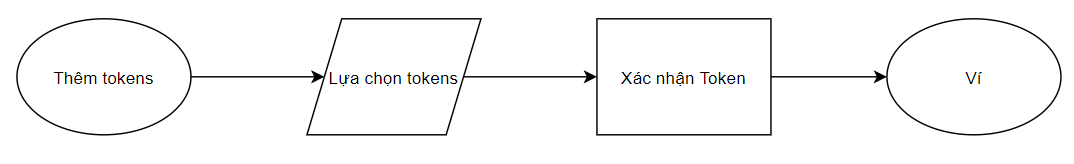
*Hình 27-3.2.3f: Sơ đồ ký gửi/nạp tiền.*

1. **Biến cố 6: Gửi tiền vào tài khoản khác**



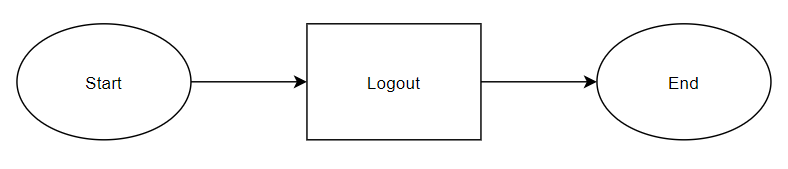
*Hình 28-3.2.3g: Sơ đồ gửi tiền.*

1. **Biến cố 7: Thêm Tokens**



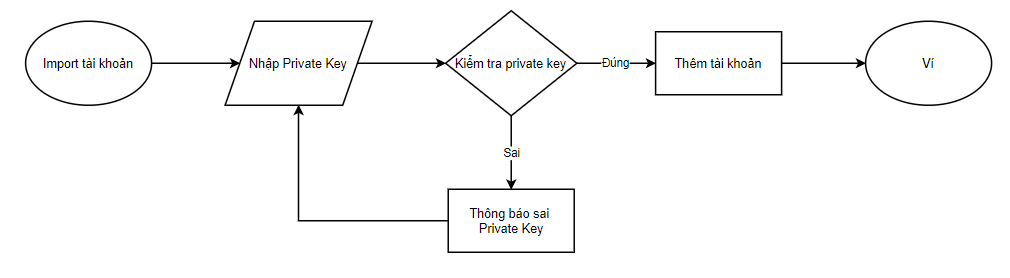
*Hình 29-3.2.3h: Sơ đồ thêm tokens.*

1. **Biến cố 8: Đăng xuất**



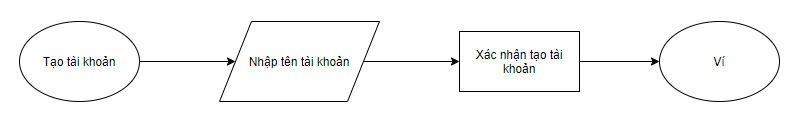
*Hình 30-3.2.3i: Sơ đồ đăng xuất.*

1. **Biến cố 9: Import tài khoản**



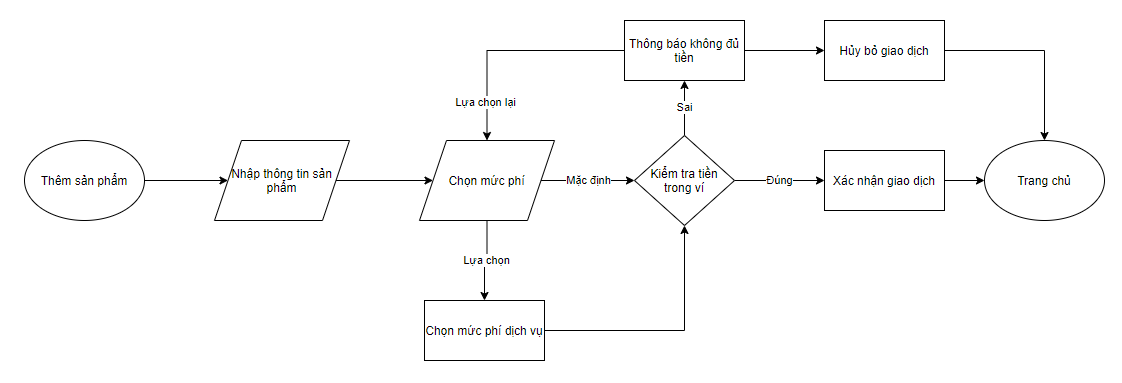
*Hình 31-3.4.3: Sơ đồ import tài khoản.*

1. **Biến cố 10: Tạo tài khoản**



*Hình 32-3.4.3: Sơ đồ tạo tài khoản.*

1. **Biến cố 11: Thêm sản phẩm**

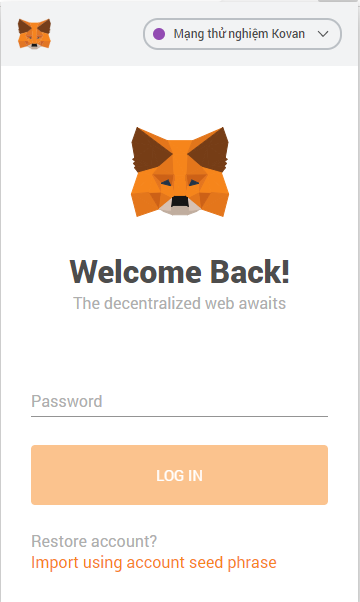


*Hình 33-3.4.4: Sơ đồ thêm sản phẩm.*

# **CHƯƠNG 4: KẾT LUẬN**

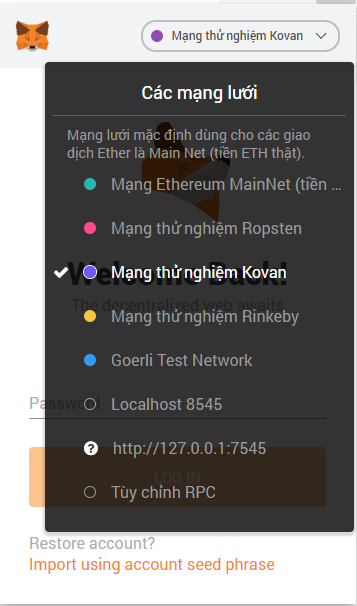
## 4.1. Kết quả đã đạt được

* + 1. Giao diện đăng nhập:



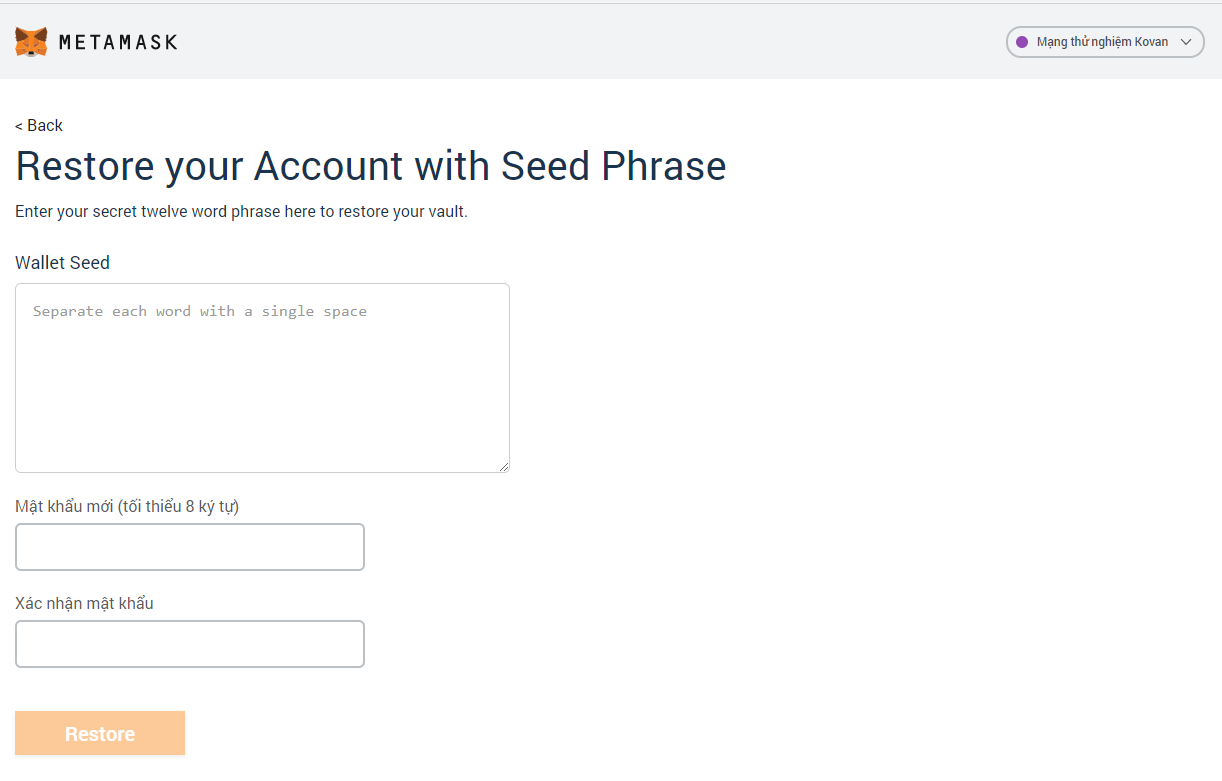
*Hình 34-4.1.1: Giao diện đăng nhập.*

* + 1. Giao diện danh sach mạng thử nghiệm:



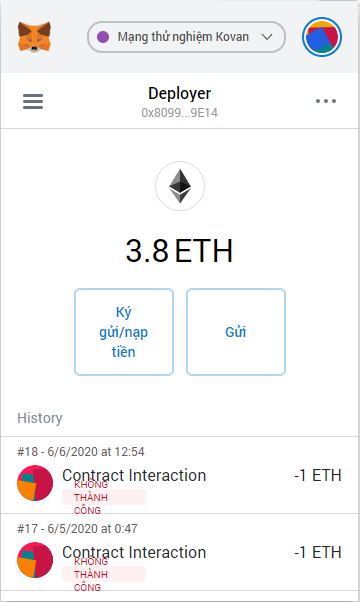
*Hình 35-4.1.2: Giao diện danh sách mạng thử nghiệm.*

* + 1. **Giao diện khôi phục mật khẩu:**



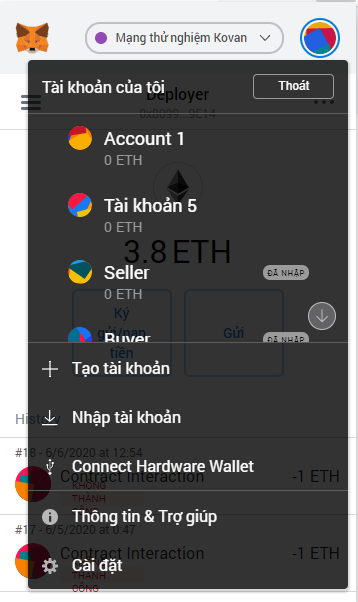
*Hình 36-4.1.3: Giao diện khôi phục mật khẩu.*

* + 1. Giao diện chính của ví:



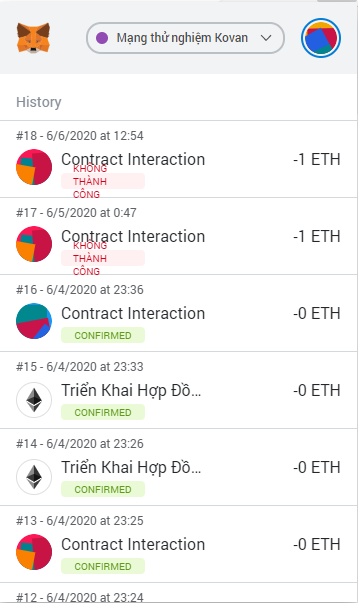
*Hình 37-4.1.4: Giao diện chính của ví.*

* + 1. Giao diện danh sách tài khoản:



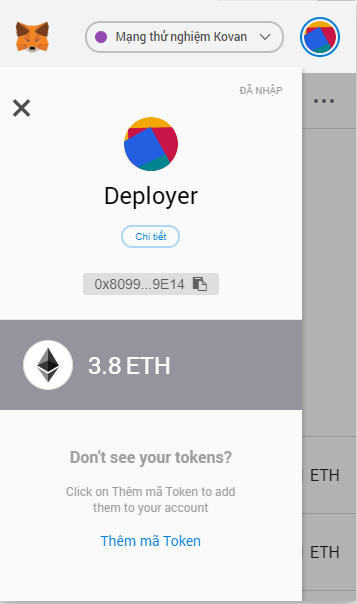
*Hình 38-4.1.5: Giao diện danh sách tài khoản.*

* + 1. **Giao diện lịch sử giao dịch:**



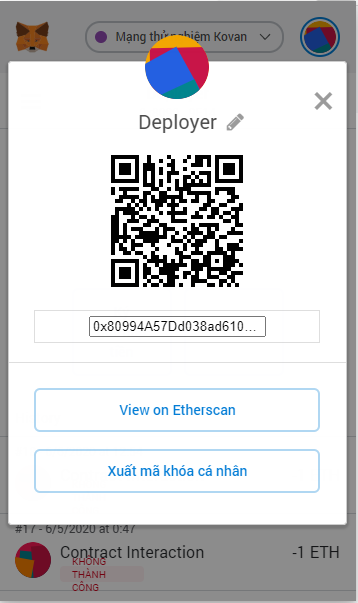
*Hình 39-4.1.6: Giao diện lịch sử giao dịch.*

* + 1. Giao diện chi tiết tài khoản 1:



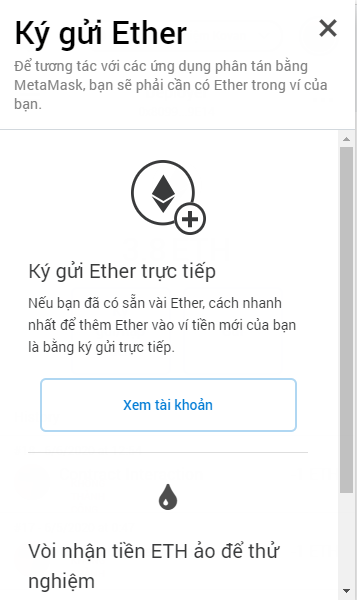
*Hình 40-4.1.7: Giao diện chi tiết tài khoản 1.*

* + 1. **Giao diện chi tiết tài khoản 2:**



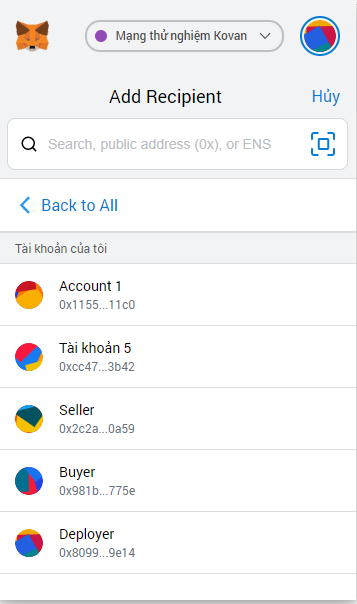
*Hình 41-4.1.8: Giao diện chi tiết tài khoản 2.*

* + 1. **Giao diện ký gửi Ether:**



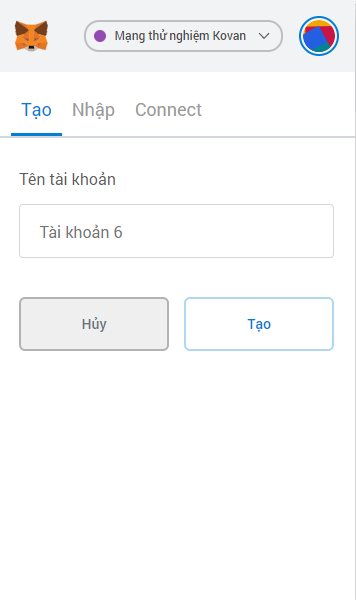
*Hình 42-4.1.9: Giao diện ký gửi Ether*

* + 1. **Giao diện chuyển khoản:**



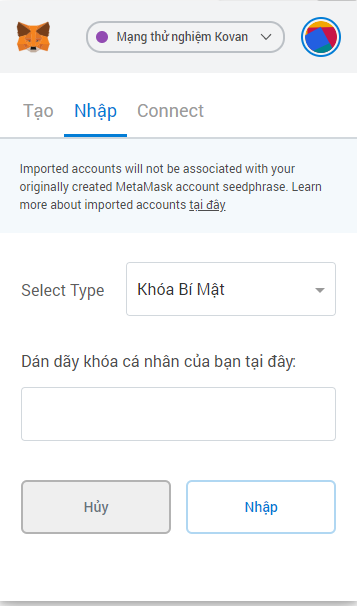
*Hình 43-4.1.10: Giao diện chuyển khoản.*

* + 1. **Giao diện tạo tài khoản mới:**



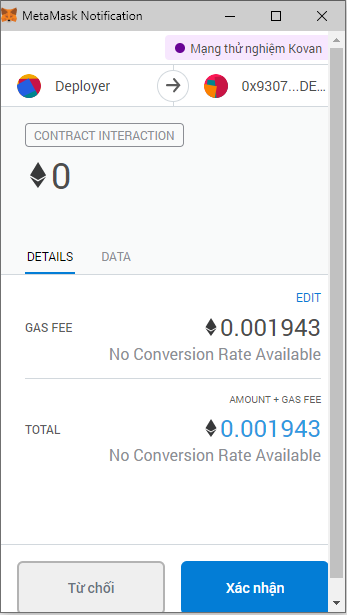
*Hình 44-4.1.11: Giao diện tạo tài khoản mới.*

* + 1. **Giao diện import tài khoản mới:**



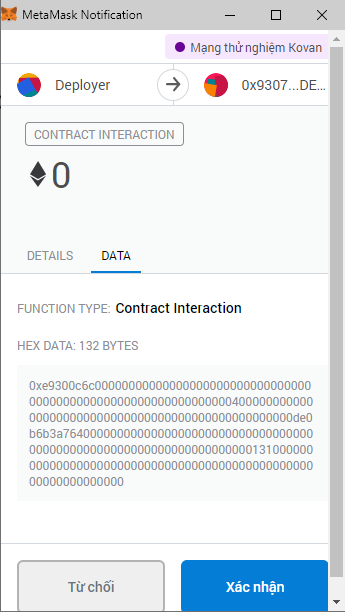
*Hình 45-4.1.12: Giao diện import tài khoản mới.*

* + 1. **Giao diện thêm sản phẩm (Chi tiết):**



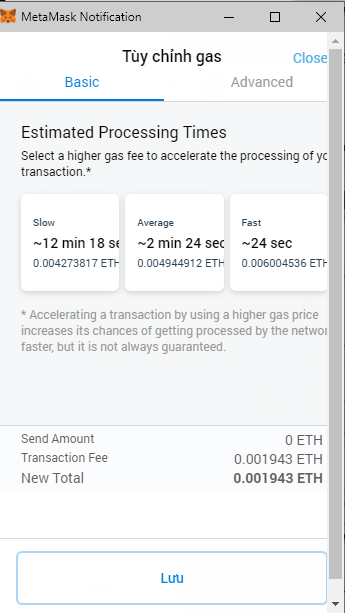
*Hình 46-4.1.13: Giao diện thêm sản phẩm (Chi tiết).*

* + 1. **Giao diện thêm sản phẩm (Dữ liệu):**



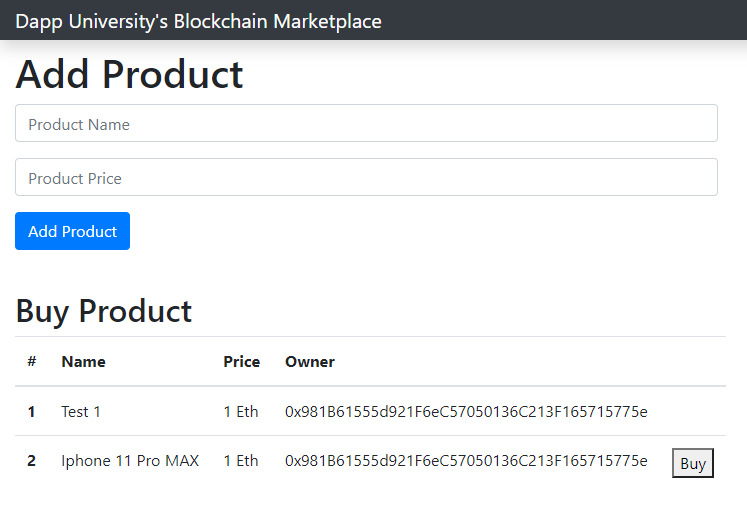
*Hình 47-4.1.14: Giao diện thêm sản phẩm (Dữ liệu).*

* + 1. **Giao diện thêm sản phẩm (Lựa chọn hình thức):**



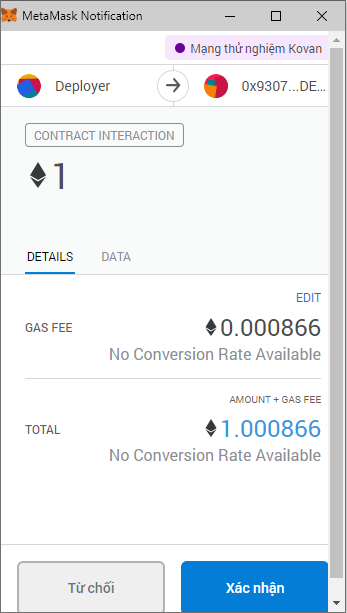
*Hình 48-4.1.15: Giao diện thêm sản phẩm (Lựa chọn hình thức).*

* + 1. **Giao diện danh sách sản phẩm:**



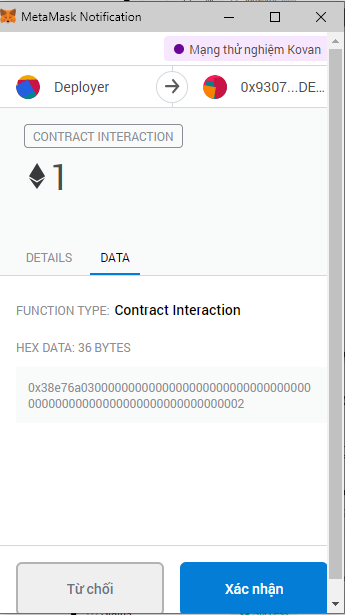
*Hình 49-4.1.16: Giao diện danh sách sản phẩm.*

* + 1. **Giao diện mua sản phẩm (Chi tiết):**



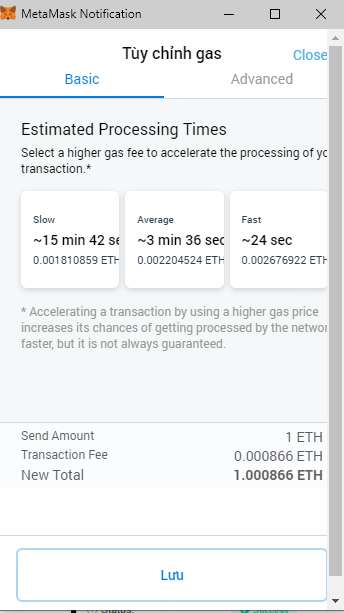
*Hình 50-4.1.17: Giao diện mua sản phẩm (Chi tiết).*

* + 1. **Giao diện mua sản phẩm (Dữ liệu):**



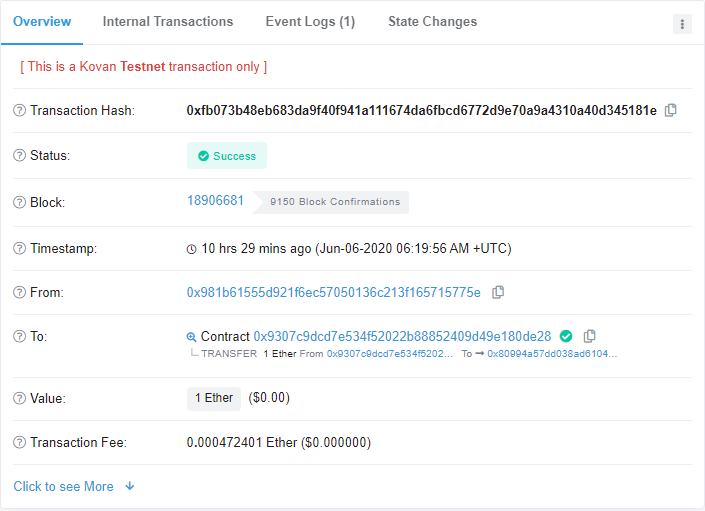
*Hình 51-4.1.18: Giao diện mua sản phẩm (Dữ liệu).*

* + 1. **Giao diện mua sản phẩm (Lựa chọn hình thức):**



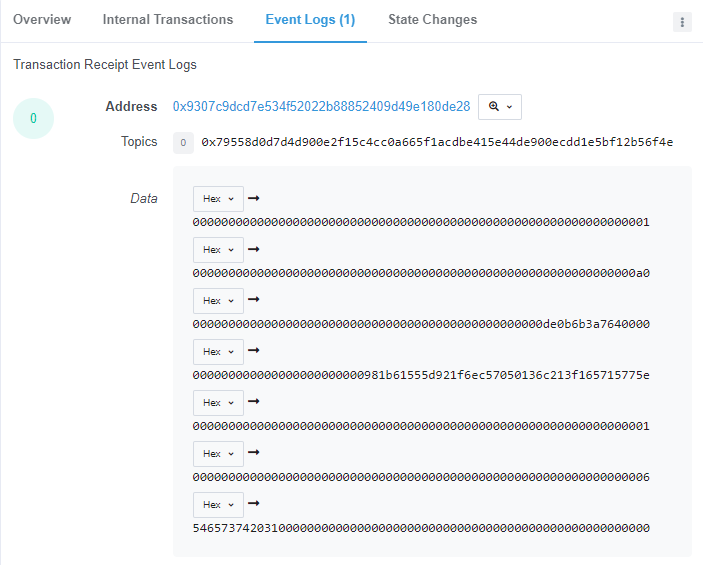
*Hình 52-4.1.19: Giao diện mua sản phẩm (Lựa chọn hình thức).*

* + 1. **Giao diện chi tiết giao dịch (Chi tiết):**



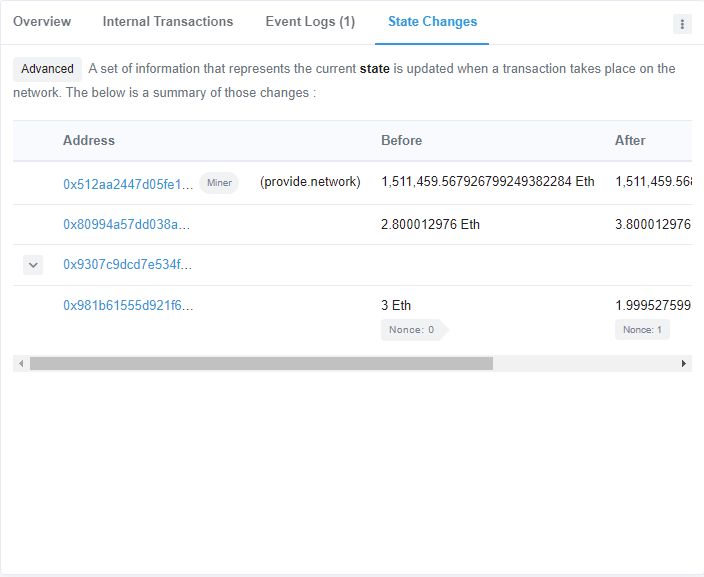
*Hình 53-4.1.20: Giao diện chi tiết giao dịch (Chi tiết).*

* + 1. **Giao diện chi tiết giao dịch (Dữ liệu)**



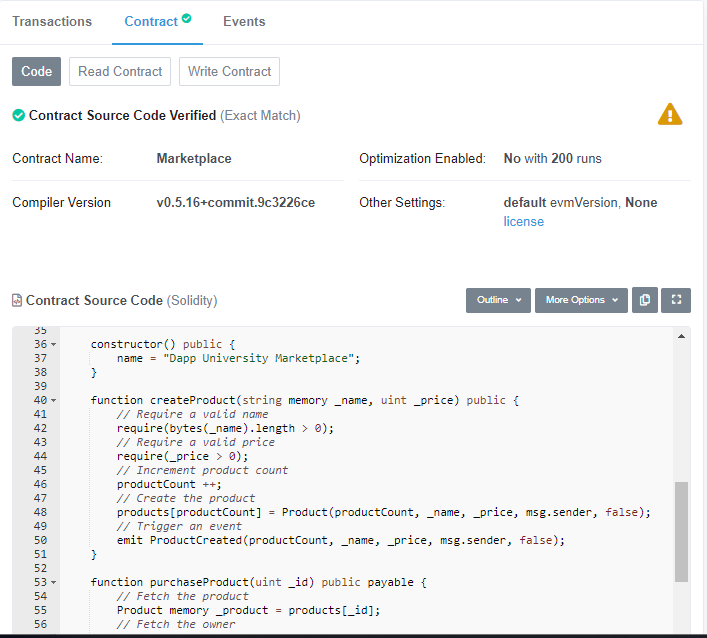
*Hình 54-4.1.21: Giao diện chi tiết giao dịch (Dữ liệu).*

* + 1. **Giao diện chi tiết giao dịch (Trang thái):**



*Hình 55-4.1.22: Giao diện chi tiết giao dịch (Trạng thái).*

* + 1. **Giao diện bản hợp đồng thông minh:**



*Hình 56-4.1.23: Giao diện bản hợp đồng thông minh.*

## Hạn chế:

* Chưa tạo riêng cho mình một ứng dụng ví để sử dụng cho bài báo cáo được mà còn phù thuộc vào ứng dụng có sẵn MetaMask.
* Giao diện trang web chưa được đầu tư và chỉn chu kỹ lưỡng.
* Trang web chưa được áp dụng real-time mà còn phải F5 lại.
* Chưa tạo ra không gian riêng biệt chỉ có 2 người dùng hoặc nhiều người dùng khi được mời vào bản hợp đồng.
* Còn phụ thuộc vào dữ liệu mẫu quá nhiều chưa thực sự hiểu rõ ngôn ngữ mới Solitity và hệ thống Blockchain,...

## Hướng phát triển:

* Hoàn thiện giao diện trang web quy mô hơn và dễ sử dụng hơn cho người dùng.
* Nghiên cứu và phát triển tạo ra một ứng dụng ví để thực hiện những cuộc giao dịch thông qua các đồng tiền kỹ thuật số và liên kết được với Blockchain.
* Xây dựng môi trường chỉ có 2 người hoặc nhiều người khi được người tạo bản hợp đồng mới thì mới được thực hiện và theo dõi thông tin giao dịch.

# **TÀI LIỆU THAM KHẢO**

[1] Cryptoassets - October 19, 2017 by Chris Burniske, Jack Tatar.

[2] The Blockchain Developer – July 23, 2019 by Elad Elrom.

[3] Mastering Ethereum: Building Smart Contracts and Dapps – November 13, 2018 by Andreas Antonopoulos.

[4] Solidity Programming Essentials: A beginner’s guide to buid smart contracts for Ethereum and blockchain – April 20, 2018 by Ritesh Modi.

[5] Smart Contracts: The Essential Guide to Using Blockchain Smart Contracts for Cryptocurrency Exchange – October 6, 2016 by Jeff Reed.

Website

[6] [Online] <https://blockchaindemo.io/>

[7] [Online] <https://bytesoft.vn/blockchain-la-gi>

[8] [Online] <https://academy.binace.com/vi/security/the-ultimate-guide-to-proof-of-keys-day>

[9] [Online] <https://arctouch.com/blog/how-to-develop-smart-contracts/>

[10][Online]https://www.dappuniversity.com/articles/how-to-buid-a-blcokchain app#preview