LỜI NÓI ĐẦU

Vài năm trở lại đây, sự bùng nổ mạnh mẽ của các đồng tiền ảo Bitcoin (BTC), đồng Etherium (ETH), đồng Lifecoin (LTC)... và sự tăng giá lên tới hàng trăm lần của nhiều đồng tiền ảo trong năm 2017 đã khiến thị trường tiền ảo trở thành thị trường đầu tư hấp dẫn và sinh lời cao, thu hút mạnh sự quan tâm của giới đầu tư, đầu cơ, quỹ đầu tư lớn, các nhà đầu tư cá nhân.

Điểm qua một vài con số có thể thấy, tính đến cuối năm 2017, Bitcoin tăng giá khoảng gần 20 lần, đồng ETH tăng 120 lần và hàng trăm đồng coins khác cũng tăng giá rất nhiều lần trong một thời gian ngắn.

Thị trường tiền ảo có đặc điểm thu hút các nhà đầu tư, đó là tăng nhanh, tăng nhiều (có thể tăng 50-100 lần/ngày), tăng không có công thức và cũng rất khó dự đoán. Ngược lại, đà giảm sâu thì giảm cũng xuống rất nhanh, có thể giá trị của nhà đầu tư nhìn thấy thị trường này thực sự màu mỡ để đầu tư và sinh lời nhanh, bởi nguyên tắc rủi ro cao thì lợi nhuận cao. Nên nhiều ứng dụng phần mềm đã được lập ra nhằm để đào, mua bán, trao đổi, quản lý nhằm tăng lợi nhuận và tránh rủi ro. Vì vậy, em đã chọn đề tài “Xây dựng ứng dụng Bitcoin Wallet trên nền tảng Android và IOS” với mục đích nghiên cứu, tìm hiểu về ứng dụng phần mềm.

Nội dung báo cáo gồm 3 chương:

**Chương 1:** Giới thiệu tổng quan

**Chương 2**: Phân tích và thiết kế hệ thống

**Chương 3:** Xây dựng ứng dụng

**Kết luận và hướng nghiên cứu trong tương lai**

**LỜI CẢM ƠN**

Để có được thành quả học tập như ngày hôm nay, ngoài sự nỗ lực phấn đấu không ngừng của bản thân thì một phần không nhỏ đóng góp nên thành công ấy là sự sự hướng dẫn, dạy dỗ của các thầy cô trong khoa Công nghệ thông tin nói riêng và trường Đại học Điện Lực nói chung trong suốt gần năm năm em học tập và nghiên cứu tại trường.

Em xin gửi lời cảm ơn chân thành đến thầy Th.S Ngô Ngọc Thành – giảng viên khoa Công nghệ thông tin, trường Đại học Điện Lực đã định hướng, hướng dẫn và chỉ bảo tận tình trong quá trình em làm báo cáo tốt nghiệp này. Em xin chúc thầy và gia đình luôn luôn mạnh khoẻ, hạnh phúc.

Cuối cùng, em xin được cảm ơn đến gia đình, bạn bè đã động viên, đóng góp ý kiến và giúp đỡ em trong quá trình học tập, nghiên cứu và hoàn thành đồ án tốt nghiệp này. Tuy nhiên, do thời gian và trình độ có hạn nên báo cáo không thể tránh khỏi những thiếu sót. Chính vì vậy, em rất mong có được sự góp ý từ các thầy cô để em đạt được kết quả tốt nhất.

Em xin chân thành cảm ơn!

Sinh viên thực hiện

Trần Thị Diệu Ninh

DANH MỤC CÁC HÌNH ẢNH

[Hình 1.1 Logo Bitcoin 13](#_Toc27556188)

[Hình 1.2 Logo Ethereum 13](#_Toc27556190)

[Hình 1.3 Tạo entropy và mã hoá thành cụm từ trợ nhớ 16](#_Toc27556195)

[Hình 1.4 Từ cụm trợ nhớ đến hạt giống 17](#_Toc27556196)

[Hình 1.5 Tạo khoá chính và mã chuỗi từ một hạt giống gốc 19](#_Toc27556199)

[Hình 1.6 Mở rộng khoá bí mật mẹ để tạo khoá bí mật con 20](#_Toc27556201)

[Hình 1.7 Mở rộng khoá công khai mẹ để tạo ra khoá công khai con 22](#_Toc27556203)

[Hình 2.1 Usecase tổng quát 24](#_Toc27556210)

[Hình 2.2 Biểu đồ phân rã Usecase create wallet 24](#_Toc27556213)

[Hình 2.3 Biểu đồ phân rã Usecase delete wallet 25](#_Toc27556215)

[Hình 2.4 Biểu đồ phân rã Usecase import wallet 25](#_Toc27556217)

[Hình 2.5 Biểu đồ phân rã Usecase deposit 25](#_Toc27556219)

[Hình 2.6 Biểu đồ phân rã Usecase withdraw 25](#_Toc27556221)

[Hình 2.7 Biểu đồ phân rã Usecase exchange 26](#_Toc27556223)

[Hình 2.8 Biểu đồ phân rã Usecase helps 26](#_Toc27556225)

[Hình 2.9 Biểu đồ phân rã Usecase withdraw 26](#_Toc27556227)

[Hình 2.10 Biểu đồ hoạt động create wallet 28](#_Toc27556233)

[Hình 2.11 Biểu đồ trình tự create wallet 29](#_Toc27556234)

[Hình 2.12 Biểu đồ hoạt động import wallet 30](#_Toc27556237)

[Hình 2.13 Biểu đồ trình tự import wallet 30](#_Toc27556238)

[Hình 2.14 Biểu đồ hoạt động delete wallet 31](#_Toc27556241)

[Hình 2.15 Biểu đồ trình tự delete wallet 31](#_Toc27556242)

[Hình 2.16 Biểu đồ hoạt động withdraw 32](#_Toc27556245)

[Hình 2.17 Biểu đồ trình tự withdraw 33](#_Toc27556246)

[Hình 2.18 Biểu đồ hoạt động deposit 34](#_Toc27556249)

[Hình 2.19 Biểu đồ trình tự deposit 34](#_Toc27556250)

[Hình 2.20 Biểu đồ hoạt động exchange 35](#_Toc27556253)

[Hình 2.21 Biểu đồ trình tự exchange 36](#_Toc27556254)

[Hình 2.22 Biểu đồ hoạt động helps 37](#_Toc27556257)

[Hình 2.23 Biểu đồ trình tự helps 37](#_Toc27556258)

[Hình 2.24 Biểu đồ hoạt động Thay đổi thông tin cá nhân 38](#_Toc27556261)

[Hình 2.25 Biểu đồ trình tự Thay đổi thông tin cá nhân 39](#_Toc27556262)

[Hình 3.1 Màn hình home 40](#_Toc27556271)

[Hình 3.2 Màn hình Send 41](#_Toc27556273)

[Hình 3.3 Màn hình Receive 42](#_Toc27556275)

[Hình 3.4 Màn hình Exchange 43](#_Toc27556277)

[Hình 3.5 Màn hình Helps 44](#_Toc27556279)

[Hình 3.6 Màn hình Settings 45](#_Toc27556281)

[Hình 3.7 Màn hình History 46](#_Toc27556283)

DANH MỤC CÁC BẢNG

[Bảng 2.1 Mô tả Usecase của hệ thống 26](#_Toc27556229)

[Bảng 2.2 Mô tả Usecase create wallet 27](#_Toc27556232)

[Bảng 2.3 Mô tả Usecase import wallet 28](#_Toc27556236)

[Bảng 2.4 Mô tả Usecase delete wallet 30](#_Toc27556240)

[Bảng 2.5 Mô tả Usecase withdraw 31](#_Toc27556244)

[Bảng 2.6 Mô tả Usecase deposit 32](#_Toc27556248)

[Bảng 2.7 Mô tả Usecase exchange 34](#_Toc27556252)

[Bảng 2.8 Mô tả Usecase helps 35](#_Toc27556256)

[Bảng 2.9 Mô tả Usecase thay đổi thông tin cá nhân 37](#_Toc27556260)

DANH MỤC CÁC KÝ HIỆU

|  |  |  |  |
| --- | --- | --- | --- |
| **PHẦN TỬ MÔ HÌNH** | | **KÝ HIỆU** | **Ý NGHĨA** |
| **Biểu đồ USE CASE** | | | |
| Tác nhân  (Actor) | | a | Một người / nhóm người hoặc một thiết bị hoặc hệ thống tác động hoặc thao tác đến chương trình. |
| Use-case  (“Ca” sử dụng) | | uc | Biểu diễn một chức năng xác định của hệ thống |
| Mối quan hệ giữa các use case | |  | Use case này sử dụng lại chức năng của use case kia |
|  | Use case này mở rộng từ use case kia bằng cách thêm chức năng cụ thể |
|  | Use case này kế thừa các chức năng từ use case kia |
| **Biểu đồ LỚP** | | | |
| Lớp  (Class) | | class1 | Biểu diễn tên lớp, thuộc tính, và phương thức của lớp đó |
| Quan hệ kiểu kết hợp | |  | Biểu diễn quan hệ giữa hai lớp độc lập, có liên quan đến nhau |
| Quan hệ hợp thành | |  | Biểu diễn quan hệ bộ phận – tổng thể |
| Quan hệ phụ thuộc | |  | Các lớp phụ thuộc lẫn nhau trong hoạt động của hệ thống |
| **Biểu đồ TRẠNG THÁI** | | | |
| Trạng thái | |  | Biểu diễn trạng thái của đối tượng trong vòng đời của đối tượng đó |
| Trạng thái khởi đầu | |  | Khởi đầu vòng đời của đối tượng đó |
| Trạng thái kết thúc | |  | Kết thúc vòng đời của đối tượng |
| Chuyển tiếp  (transition) | |  | Chuyển từ trạng thái này sang trạng thái khác |
| **Biểu đồ TUẦN TỰ** | | | |
| Procedure  (Phương thức) | | s | Là một phương thức của B mà đối tượng A gọi thực hiện. |
| Message  (Thông điệp) | | m | Là một thông báo mà B gửi cho A. |
| **Biểu đồ HOẠT ĐỘNG** | | | |
| Hoạt động |  | | Mô tả hoạt động gồm tên hoạt động và đặc tả của nó |
| Trạng thái khởi đầu |  | |  |
| Trạng thái kết thúc |  | |  |
| Thanh đồng bộ ngang |  | | Mô tả thanh đồng bộ ngang |
| Chuyển tiếp |  | |  |
| Quyết định |  | | Mô tả một lựa chọn điều kiện |
| Các luồng | Phân tách các lớp đối tượng khác nhau trong biểu đồ hoạt động | | Phân cách nhau bởi một đường kẻ dọc từ trên xuống dưới biểu đồ |
| **Biểu đồ THÀNH PHẦN** | | | |
| Thành phần | |  | Mô tả một thành phần của biểu đồ, mỗi thành phần có thể chứa nhiều lớp hoặc nhiều chương trình con |
| Mối quan hệ phụ thuộc giữa các thành phần | |  | Mỗi quan hệ giữa các thành phần(nếu có) |
| **Biểu đồ TRIỂN KHAI** | | | |
| Các node  (các thiết bị) |  | | Biểu diễn các thành phần không có bộ vi xử lý |
| Các bộ xử lý |  | | Biểu diễn các thành phần có bộ vi xử lý |
| Liên kết truyền thông TCP/IP |  | | Giao thức truyền thông TCP/IP thông qua kết nói mạng LAN |

# 

# CHƯƠNG 1. GIỚI THIỆU TỔNG QUAN

* 1. **Các đồng tiền ảo nổi tiếng**

Hiện nay trên thế giới có hơn 2000 đồng tiền ảo khác nhau. Và Bitcoin, Ethereum vẫn là hai đồng tiền điện tử dẫn đầu thị trường tiền ảo.

* + 1. **Đồng Bitcoin (BTC)**

Bitcoin (ký hiệu BTC, XBT) là một loại tiền mã hoá, được phát minh bởi Satoshi Nakamoto dưới dạng phần mềm mã nguồn mở từ năm 2009. Bitcoin có thể được trao đổi trực tiếp bằng thiết bị kết nối Internet mà không cần thông qua một tổ chức tài chính trung gian nào.



*Hình 1.1 Logo Bitcoin*

* + 1. **Đồng Ethereum (ETH)**

Ethereum (ETH) hay còn gọi là Bitcoin 2.0 là một nền tảng điện toán phân tán khối chuỗi chạy trên công nghệ blockchain, thông qua việc sử dụng chức năng hợp đồng thông minh (smart contract). Tiền ảo Ethereum có thể thực hiện các giao dịch, hợp đồng mạng ngang hàng thông qua đơn vị tiền ảo là Ether. Không những thế ETH còn được đánh giá là một nền tảng ứng dụng hữu ịch và tự tạo ra hệ tài chính phân tán của riêng mình. Ethereum được giới thiệu vào cuối năm 2013 bởi một chuyên viên nghiên cứu về lập trình tiền ảo có tên Vitalik Buterin.



*Hình 1.2 Logo Ethereum*

* 1. **Ví Bitcoin**

Từ “ví” dùng để nói chỉ một số yếu tố khác nhau trong bitcoin. Ở mức khái quát, ví là ứng dụng đóng vai trò giao diện người dùng chính. Ví kiểm soát quyền truy cập tiền của người dùng, quản lý các khoá và địa chỉ, theo dõi số dư, tạo và ký các giao dịch. Ở góc độ hẹp hơn, từ góc nhìn của một lập trình viên, từ “ví” chỉ cấu trúc dữ liệu dùng để lưu trữ và quản lý các khoá của người dùng.

* + 1. **Tổng quan về công nghệ ví**

Một sự nhầm lẫn khái niệm thường gặp về bitcoin là ví bitcoin chứa bitcoin. Trên thực tế, ví chỉ chứa khoá. Các “coin” (tiền) được ghi lại vào blockchain trên mạng bitcoin. Người dùng kiểm soát tiền của mình trên mạng lưới bằng cách dùng khoá trong ví để ký các giao dịch. Ở một góc độ nào đó, có thể hiểu ví bitcoin là một chùm chìa khoá.

Có hai loại ví chính, được phân biệt bằng mối liên hệ giữa các khoá chứa trong ví.

Loại đầu tiên là ví bất định, trong đó mỗi khoá được tạo ra độc lập từ một số ngẫu nhiên. Các khoá này không liên quan đến nhau. Loại ví này còn được gọi là ví JBOK, viết tắt của cụm từ “Just a Bunch Of Keys” (chỉ là một đống khoá).

Loại thứ hai là ví tất định, trong đó tất cả các khoá đều được tạo ra từ một khoá chính duy nhất (master key), hay còn gọi là hạt giống (seed). Tất cả các khoá trong loại ví này đều liên quan đến nhau và có thể được tạo lại nếu có hạt giống gốc. Có một số cách tạo khoá khác nhau được dùng trong các ví tất định, trong đó cách phổ biến nhất là sử dụng một cấu trúc dạng cây gọi là ví tất định phân cấp (hierarchical deterministic), hay ví HD. Các ví tất định được khởi tạo từ một hạt giống. Để chúng dễ sử dụng hơn, các hạt giống được mã hoá thành từ tiếng Anh, còn được gọi là các từ mật mã trợ nhớ.

* + 1. **Chi tiết về công nghệ ví**

Chúng ta sẽ khám phá chi tiết từng chuẩn quan trọng của ngành đang được nhiều ví bitcoin áp dụng.

* + - 1. **Cụm từ mã trợ nhớ (BIP-39)**

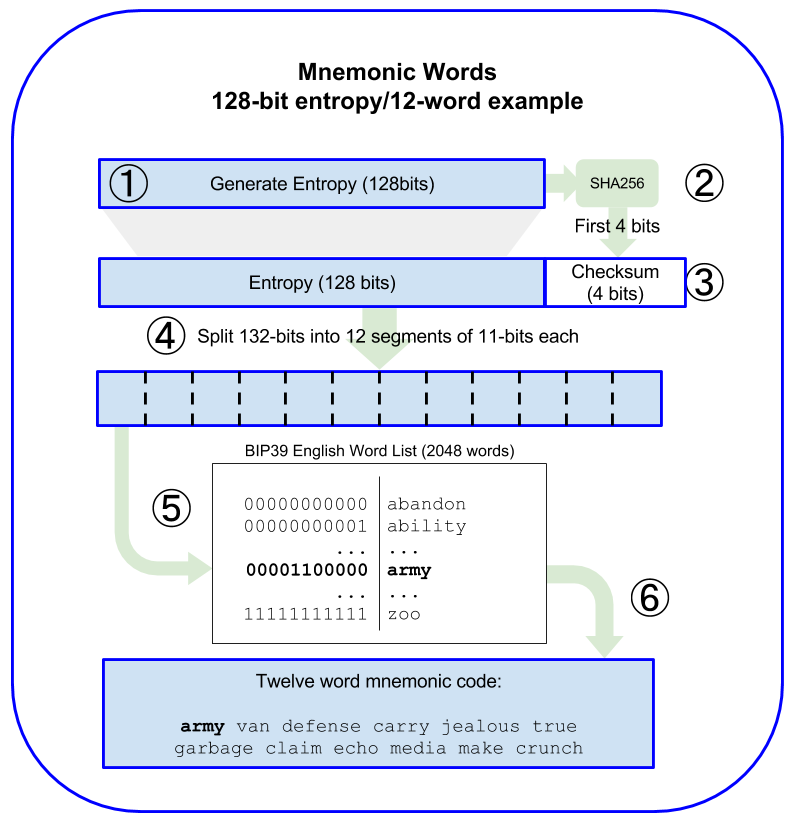
Cụm từ mã trợ nhớ là chuỗi từ tượng trưng cho (mã hoá) một số ngẫu nhiên được dùng làm hạt giống để tạo ví tất định. Chỉ cần chuỗi từ này là có thể tạo lại hạt giống đó, rồi từ hạt giống đó tạo lại ví với tất cả các khoá đã được tạo ra. Khi lần đầu tạo ví, ứng dụng ví cài đặt các ví tất định với cụm từ trợ nhớ sẽ hiển thị cho người dùng một chuỗi 12 đến 24 từ. Chuỗi từ này chính là bản sao lưu của ví và có thể dùng nó để khôi phục cũng như tạo lại tất cả các khoá trong cùng ứng dụng ví hoặc trong bất cứ ứng dụng ví tương thích nào. Các từ trợ nhớ giúp người dùng sao lưu ví dễ dàng hơn bởi chúng dễ đọc và dễ sao chép chính xác hơn so với một chuỗi ngẫu nhiên các con số. Các mã trợ nhớ được định nghĩa trong BIP-39 (<https://github.com/bitcoin/bips)>. Lưu ý, BIP-39 là một bản thực thi của một chuẩn mã trợ nhớ. Ngoài ra còn có một chuẩn khác trước BIP-39 với một tập hợp từ khác, được ví Electrum sử dụng. BIP-39 do công ty phát triển ví phần cứng Trezor đề xuất và không tương thích với bản thực thi của Electrum. Tuy nhiên, hiện nay BIP-39 đã nhận được sự ủng hộ rộng lớn trong ngành thông qua hàng chục bản thực thi tương thích lẫn nhau, do đó nên coi nó là chuẩn mặc định của ngành.

BIP-39 quy định quá trình tạo mã trợ nhớ và hạt giống (được miêu tả thành 9 bước ở đây). Để rõ ràng hơn, quá trình này được chia thành 2 phần: các bước từ 1 đến 6 được liệt kê trong mục “Tạo các từ trợ nhớ” và các bước từ 7 đến 9 được liệt kê trong mục “Từ cụm trợ nhớ đến hạt giống”.

**Tạo các từ trợ nhớ**

Ví tự động tạo ra các từ trợ nhớ thông qua quá trình chuẩn hoá được định nghĩa trong BIP-39. Từ điểm khởi đầu là một nguồn entropy, ví bổ sung một mã checksum, sau đó ánh xạ entropy này đến một danh sách các từ:

1. Tạo một chuỗi ngẫu nhiên (một entropy) 128 đến 256 bit.
2. Tạo một checksum của chuỗi ngẫu nhiênn trên bằng cách lấy các bit đầu tiên (độ dài entropy chia cho 32) của mã băm SHA256 của nó.
3. Thêm checksum này vào cuối chuỗi ngẫu nhiên.
4. Chia chuỗi này thành các đoạn 11 bit.
5. Ánh xạ từng giá trị 11 bit này thành 1 từ trong một từ điển cho trước gồm 2048 từ.
6. Mã trợ nhớ chính là chuỗi từ này.



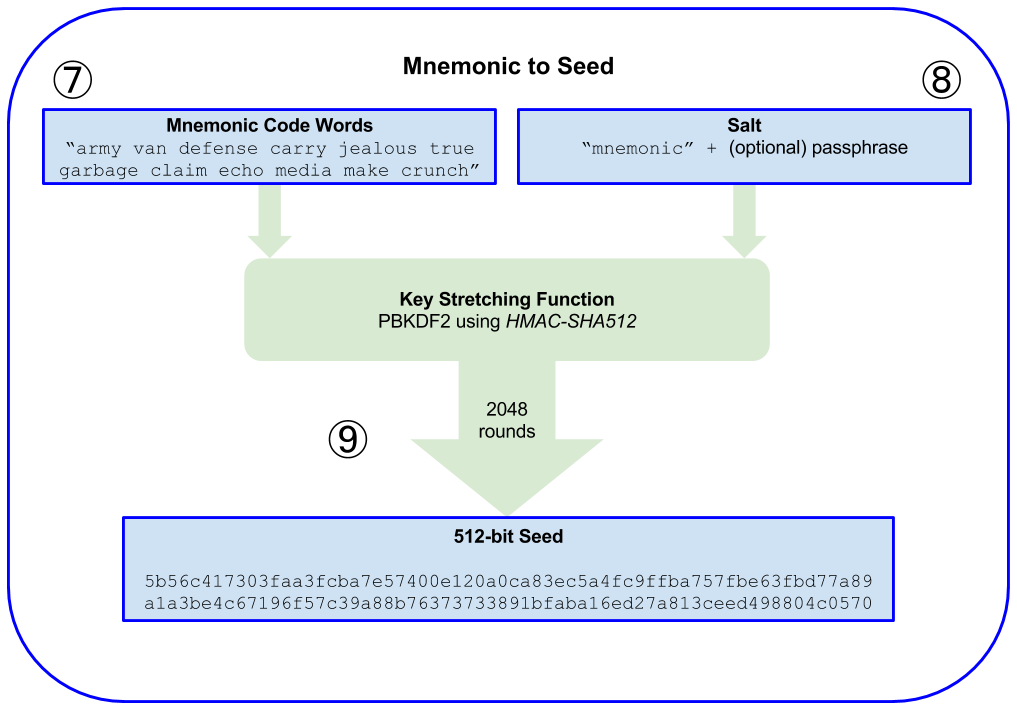
*Hình 1.3 Tạo entropy và mã hoá thành cụm từ trợ nhớ*

**Từ cụm trợ nhớ đến hạt giống**

Các từ trợ nhớ này đại diện cho entropy có độ dài từ 128 đến 256 bit. Sau đó, dùng entropy này để tạo một hạt giống dài hơn (512 bit) bằng hàm kéo dài khoá PBKDF2. Tiếp đến, dùng hạt giống tạo được để xây dựng một ví tất định rồi tạo các khoá của nó.

Hàm kéo dài nhận hai tham số: cụm từ trợ nhớ và một hạt muối (salt). Mục đích của hạt muối trong hàm khéo dài khoá là nhằm gây khó khăn cho việc xây dựng một bảng tìm kiếm để thực hiện một cuộc tấn công vét cạn. Trong chuẩn BIP-39, hạt muối còn có một mục đích khác – nó cho phép tạo ra một passphrase đóng vai trò một lớp bảo vệ tăng cường để bảo vệ hạt giống. Quá trình được mô tả trong các bước từ 7 đến 9 tiếp tục quá trình đã được mô tả trước đó ở phần “Tạo các từ trợ nhớ”.

1. Tham số đầu tiên cho hàm kéo dài khoá PBKDF2 là cụm trợ nhớ tạo ra ở bước 6.
2. Tham số thứ hai cho hàm kéo dài khoá PBKDF2 là một hạt muối. Hạt muối bao gồm một hằng số dạng chuỗi “mnemonic” được nối với một chuỗi passphrase tuỳ chọn do người dùng cung cấp.
3. PBKDF2 kéo dài các tham số cụm trợ nhớ và hạt muối bằng việc băm 2048 lần với thuật toán HMAC-SHA512, tạo ra kết quả cuối cùng là một giá trị 512 bit. Giá trị 512 bit này chính là hạt giống.



*Hình 1.4 Từ cụm trợ nhớ đến hạt giống*

# 1.2.2.2 Passphrase tuỳ chọn trong BIP-39

Chuẩn BIP-39 cho phép sử dụng một passphrase tuỳ chọn trong quá trình tạo hạt giống. Nếu không dùng passphrase, cụm trợ nhớ sẽ được kéo dài bằng một hạt muối chứa chuỗi không đổi “mnemonic”, tạo ra một hạt giống 512 bit từ bất kỳ cụm trợ nhớ nào cho trước. Nếu dùng passphrase, hàm kéo dài khoá sẽ tạo ra một hạt giống khác từ cùng một cụm trợ nhớ trên. Trên thực tế, với một cụm trợ nhớ cho trước, mỗi passphrase tiềm năng sẽ cho ra một hạt giống khác nhau. Về cơ bản, không có passphrase “sai”. Tất cả các passphrase đều hợp lệ và tạo ra các hạt giống khác nhau, từ đó hình thành nên một tập khổng lồ các ví chưa khởi tạo khả thi. Tập các ví khả thi này lớn (2^512) đến lỗi khả năng thực hiện một cuộc tấn công giải mã vét cạn hay vô tình đoán đúng ví đang được sử dụng là bất khả thi.

Passphrase tuỳ chọn này tạo ra 2 tính năng quan trọng:

* Một lớp bảo mật thứ hai (một thứ được nhớ) khiến cho một cụm trợ nhớ trở nên vô dụng nếu nó chỉ đi một mình. Lớp bảo mật này đóng vai trò bảo vệ các bản sao cụm trợ nhớ khỏi nguy cơ bị trộm.
* Một hình thức từ chối hợp lý hay “ví cưỡng ép”, trong đó sử dụng một passphrase dẫn đến một ví chứa ít tiền hơn nhằm đánh lạc hướng kẻ tấn công khỏi ví thật chứa phần lớn lượng tiền.

Tuy nhiên, cần phải lưu ý rằng việc dùng passphrase cũng mang lại rủi ro mất mát:

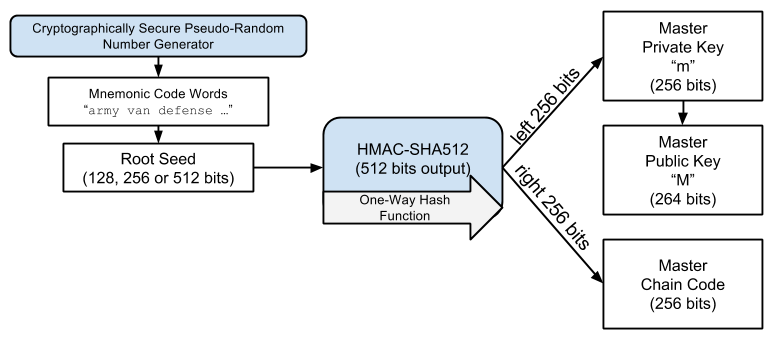
* Nếu chủ sở hữu ví bị mất khả năng (do thương tật, ốm đau…) hoặc qua đời và không ai biết passphrase, hạt giống sẽ trở nên vô dụng và toàn bộ tiền lưu trong ví đó sẽ bị mất vĩnh viễn.
* Ngược lại, nếu chủ sở hữu cất bản sao lưu passphrase ở cùng chỗ với hạt giống, nó sẽ vô hiệu hoá mục đích của lớp bảo vệ thứ hai.

Tuy passphrase rất hữu dụng, song chỉ nên dùng chúng kết hợp với một quy trình sao lưu và hồi phục được lên kế hoạch cẩn thận, trong đó tính đến cả khả năng chủ sở hữu qua đời và cho phép người thân trong gia đình có thể khôi phục lại tài sản tiền mã hoá.

* + - 1. **Tạo ví HD từ hạt giống**

Các ví HD được tạo ra từ một hạt giống gốc đơn lẻ là một số ngẫu nhiên 128, 256 hoặc 512 bit. Thường gặp nhất là các hạt giống được tạo ra từ một cụm trợ nhớ như đã trình bày chi tiết ở phần trước.

Mọi khoá trong ví HD đều được tạo ra từ hạt giống gốc này, vì vậy có thể tạo lại toàn bộ ví HD từ hạt giống đó trong bất kỳ ví HD tương thích nào. Vì thế có thể dễ dàng sao lưu, khôi phục và xuất nhập các ví HD vốn chứa hàng ngàn, thậm chí hàng triệu khoá với một thao tác đơn giản di chuyển cụm trợ nhớ đã tạo ra các hạt giống gốc.



*Hình 1.5 Tạo khoá chính và mã chuỗi từ một hạt giống gốc*

Hạt giống gốc là đầu vào cho thuật toán HMAC-SHA512 và mã băm kết quả được dùng để tạo ra một khoá bí mật chính (m) và một mã chuỗi chính (c).

Sau đó, khoá bí mật chính (m) tạo ra một khoá công khai chính tương ứng (M) thông qua phép nhân đường công elliptic m\*G.

Mã chuỗi (c) được dùng để tạo entropy trong hàm tạo khoá con từ khoá mẹ.

* + - 1. **Tạo khoá bí mật con**

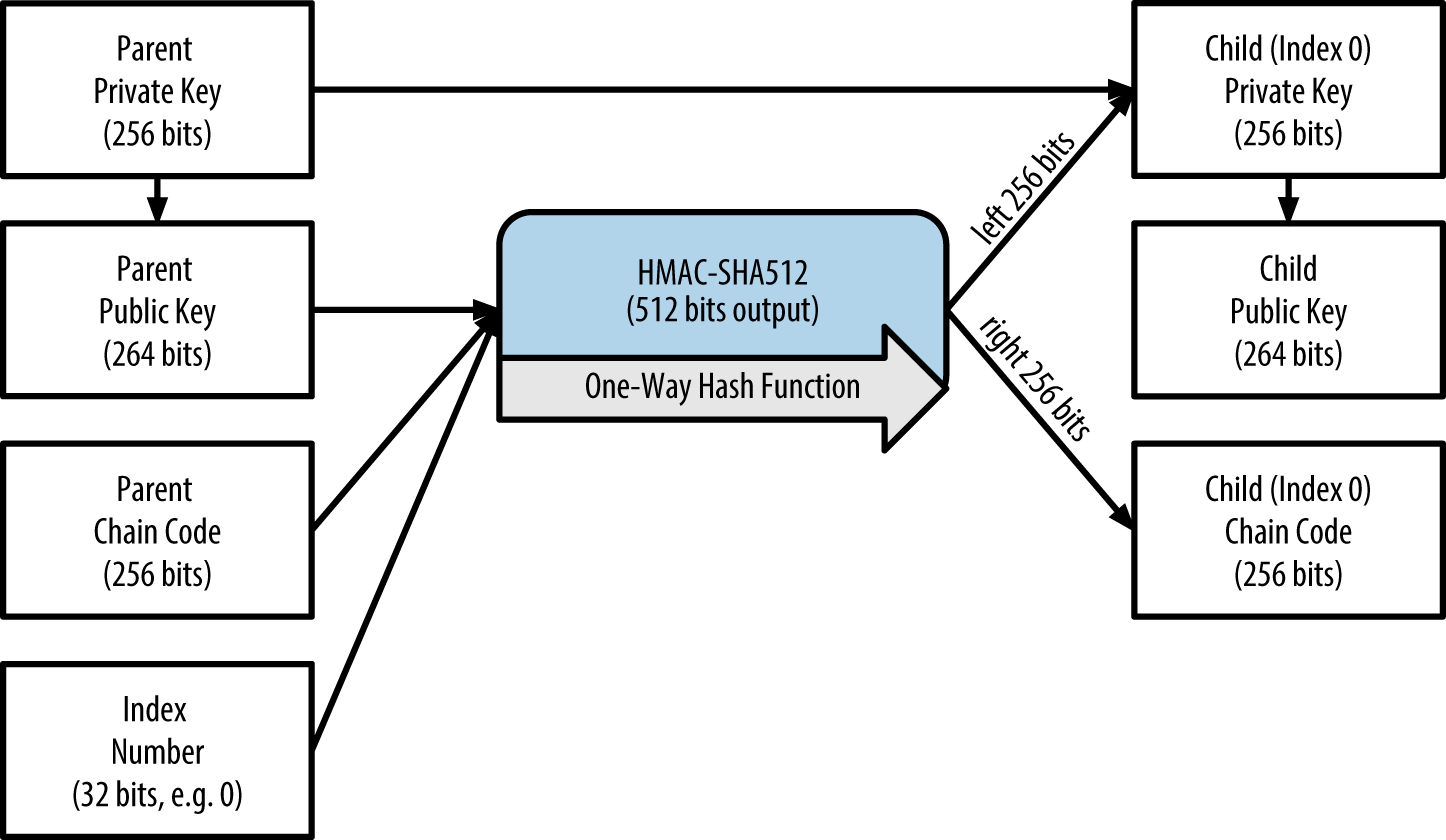
Ví HD sử dụng hàm tạo khoá con (child key derivation – CKD) để tạo ra các khoá con từ các khoá mẹ. Các hàm tạo khoá con dựa trên một hàm băm một chiều kết hợp với:

* Một khoá bí mật hoặc công khai mẹ (khoá ECDSA không nén)
* Một hạt giống gọi là một mã chuỗi (256 bit)
* Một số thứ tự (32 bit)

Mã chuỗi được dùng để đưa dữ liệu ngẫu nhiên tất định vào quá trình này, do đó nếu chỉ biết số thứ tự và một khoá con là chưa đủ để suy ra các khoá con khác. Việc biết một khoá con không làm cho việc tìm kiếm các khoá ngang hàng với nó trở nên khả thi, nếu như không biết mã chuỗi. Hạt giống mã chuỗi đầu tiên (tại gốc của cây) được tạo ra từ hạt giống, trong khi các mã chuỗi con về sau lại được tạo ra từ mã chuỗi mẹ.

Ba thành phần này (khoá mẹ, mã chuỗi và số thứ tự) được kết hợp lại với nhau rồi băm để tạo ra các khoá con như sau.

Kết hợp khoá công khai mẹ, mã chuỗi và số thứ tự với nhau rồi băm bằng thuật toán HMAC-SHA512 để tạo ra một mã băm 512 bit. Chia mã băm 512 bit này thành hai nửa 256 bit. Nửa 256 bit bên phải của mã băm trở thành mã chuỗi của khoá con. Nửa 256 bit bên trái được thêm vào khoá bí mật mẹ để tạo khoá bí mật con.



*Hình 1.6 Mở rộng khoá bí mật mẹ để tạo khoá bí mật con*

Việc thay đổi số thứ tự cho phép ta mở rộng khoá mẹ và tạo ra các khoá con khác thành chuỗi. Ví dụ, Con 0, Con 1, Con 2,… Mỗi khoá mẹ có thể có tới 2.147.483 647 (2^31) khoá con (2^31 là một nửa của toàn dải khả dụng 2^32).

Lặp lại quá trình này ở một tầng thấp hơn của cây, mỗi khoá con khi đó lại trở thành một khoá mẹ và tạo ra các con của nó, cứ thế tiếp diễn thành vô số thế hệ.

**Sử dụng các khoá con được tạo ra**

Khoá bí mật con và khoá bất định (ngẫu nhiên) không có gì khác nhau. Bởi hàm tạo khoá là hàm một chiều, nên không thể dùng khoá con để tìm khoá mẹ, cũng không thể dùng khoá con để tìm các anh em (khoá ngang hàng) của nó. Nếu có khoá con thứ n, bạn không thể tìm anh em của nó như khoá con thứ n-1 hay n+1, hay bất cứ khoá con nào trong chuỗi. Chỉ khoá mẹ và mã chuỗi mới có thể tạo ra tất cả các khoá con. Nếu không có mã chuỗi của khoá con, cũng không thể dùng khoá con để tạo ra bất kỳ khoá cháu nào. Bạn cần phải có cả khoá bí mật con và mã chuỗi của khoá con đó mới có thể bắt đầu một nhánh mới và tạo ra các khoá cháu.

Vậy chỉ mình khoá bí mật con thì có thể làm được gì? Có thể dùng nó để tạo ra một khoá công khai và một địa chỉ bitcoin. Sau đó có thể dùng nó để ký các giao dịch và chi tiêu các khoản tiền được gửi đến địa chỉ đó.

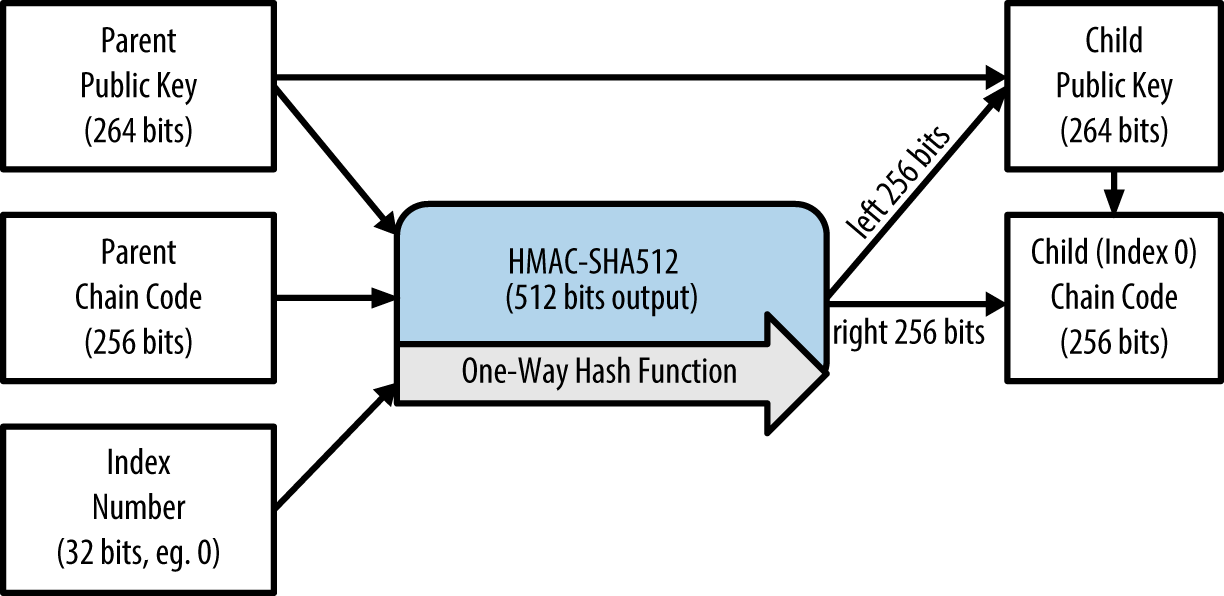
* + - 1. **Tạo khoá công khai con**

Như đã đề cập ở trên, một đặc tính rất hữu dụng của ví HD là khả năng tạo khoá công khai con từ khoá công khai mẹ mà không cần phải có khoá bí mật. Đặc tính này mang đến hai cách tạo khoá công khai con: hoặc là tạo từ khoá bí mật con, hoặc tạo trực tiếp từ khoá công khai mẹ.

Vì thế, có thể dùng khoá công khai mở rộng để tạo ra tất cả các khoá công khai (và chỉ khoá công khai mà thôi) trong nhánh đó của cấu trúc ví HD.

Có thể dùng lối tắt này để tạo ra các dạng triển khai chỉ dùng khoá công khai rất an toàn, trong đó một máy chủ hay ứng dụng có một bản sao của một khoá công khai mở rộng nhưng không hề có khoá bí mật nào. Dạng triển khai này có thể tạo ra vô số khoá công khai và địa chỉ bitcoin, nhưng không thể chi tiêu bất kì khoản tiền nào được gửi đến những địa chỉ ấy. Trong khi đó, trên một máy chủ khác an toàn hơn, khoá bí mật mở rộng có thể tạo ra tất cả các khoá bí mật tương ứng để ký các giao dịch và chi tiêu các khoản tiền đó.

Một ứng dụng phổ biến của giải pháp này là cài đặt khoá công khai mở rộng trên một máy chủ nền web đóng vai trò một ứng dụng thương mại điện tử. Máy chủ nền web này có thể dùng hàm tạo khoá công khai để tạo ra một địa chỉ bitcoin mới cho mỗi giao dịch (ví dụ cho một giỏ hàng của khách). Máy chủ nền web này không có bất kỳ khoá bí mật nào nên không sợ trộm cắp. Nếu không có ví HD, cách duy nhất để thực hiện điều này là tạo sẵn hàng nghìn địa chỉ bitcoin trên một máy chủ an toàn riêng biệt và nạp sẵn chúng vào máy chủ thương mại điện tử. Đây là một phương án rất rắc rối và đòi hỏi phải bảo trì thường xuyên để đảm bảo rằng máy chủ thương mại điện tử không bị “hết” khoá.



*Hình 1.7 Mở rộng khoá công khai mẹ để tạo ra khoá công khai con*

Một ứng dụng phổ biến khác của giải pháp này là lưu trữ lạnh và các ví phần cứng. Trong trường hợp này, có thể lưu khoá bí mật mở rộng vào ví giấy hay thiết bị phần cứng (thí dụ như ví phần cứng Trezor), trong khi có thể lưu khoá công khai mở rộng trên mạng trực tuyến. Người dùng có thể tạo ra các địa chỉ “nhận” tuỳ ý, trong khi các khoá bí mật vẫn được cất giữ an toàn ngoại tuyến. Để chi tiêu tiền, người dùng có thể sử dụng khoá bí mật mở rộng trên một phần mềm ký giao dịch bitcoin ngoại tuyến hoặc ký giao dịch trên một thiết bị vi phần cứng (ví dụ như Trezor).

* 1. **Bài toán**

Bài toán ở đây là làm thế nào để xây dựng được một ứng dụng ví Bitcoin theo những thông tin có được ở trên.

* 1. **Nội dung đề tài**
* **Lý thuyết**
* Tìm hiểu về các đồng tiền ảo, ví bitcoin
* Tìm hiểu ngôn ngữ Javascript và React-native framework
* **Thực hành**
* Phân tích thiết kế hệ thống
* Xây dựng các chức năng của ứng dụng: create, import, delete wallet, exchange…
  1. **Kết luận chương 1**

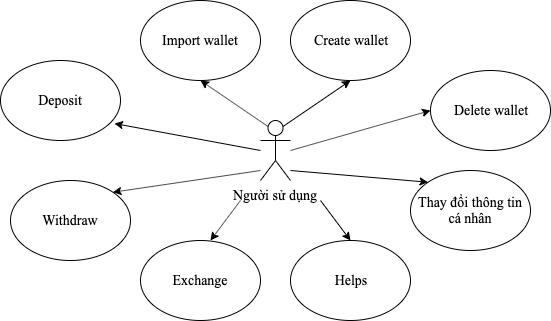
Chương 1 đã nêu được các thông tin cơ bản về một số coin nổi tiếng, ví bitcoin và các thông tin liên quan. Từ đó, chúng ta có thể hiểu rõ hơn về mục đích xây dựng ứng dụng ví bitcoin và kiến thức nền để phân tích chi tiết hơn về cách hoạt động trong chương 2.

# 

# CHƯƠNG 2. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

# 2.1 Biểu đồ Usecase

# 2.1.1 Biểu đồ Usecase tổng quát

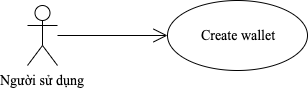


Hình 2. Usecase tổng quát

Qua biểu đồ Usecase tổng quát, ta có thể nhìn thấy được khái quát các chức năng chính của hệ thống như create wallet, delete wallet, import wallet, deposit, withdraw, exchange, helps, thay đổi thông tin cá nhân dưới sự tác động của tác nhân tham gia hệ thống là người sử dụng.

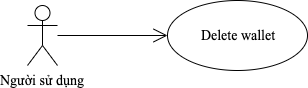
# 2.1.2 Biểu đồ phân rã Usecase

# 2.1.2.1 Chức năng “Create wallet”



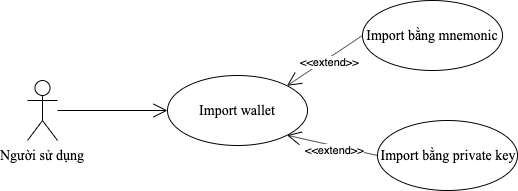
Hình 2. Biểu đồ phân rã Usecase create wallet

# 2.1.2.2 Chức năng “Delete wallet”



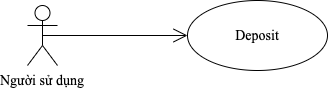
Hình 2.3 Biểu đồ phân rã Usecase delete wallet

# 2.1.2.3 Chức năng “Import wallet”

****

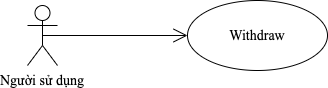
Hình 2.4 Biểu đồ phân rã Usecase import wallet

# 2.1.2.4 Chức năng “Deposit”



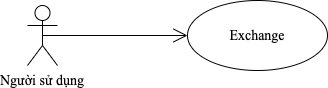
Hình 2.5 Biểu đồ phân rã Usecase deposit

# 2.1.2.5. Chức năng “Withdraw”



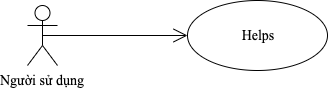
Hình 2.6 Biểu đồ phân rã Usecase withdraw

# 2.1.2.6. Chức năng “Exchange”



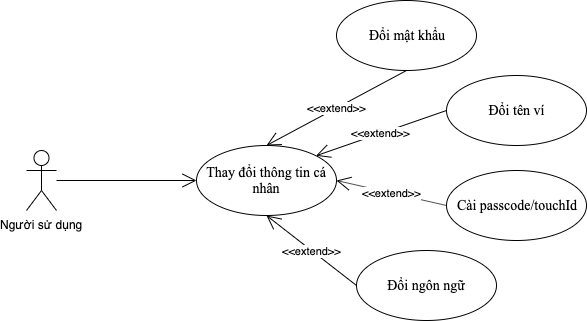
Hình 2.7 Biểu đồ phân rã Usecase exchange

# 2.1.2.7 Chức năng “Helps”



Hình 2.8 Biểu đồ phân rã Usecase helps

# 2.1.2.8. Chức năng “Thay đổi thông tin cá nhân”



Hình 2.9 Biểu đồ phân rã Usecase withdraw

# 2.1.3 Các tác nhân chính tham gia hệ thống

Ví Bitcoin có một tác nhân chính: Người sử dụng.

Dựa vào tác nhân đã xác định, bảng mô tả Usecase của hệ thống được xây dựng như sau:

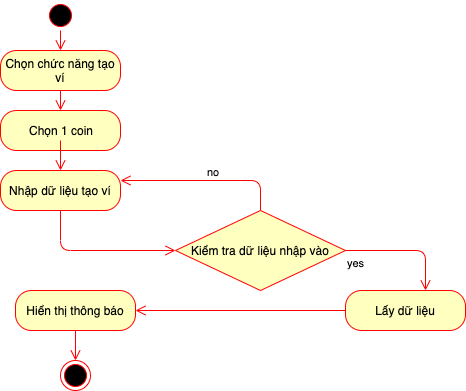
Bảng 2. Mô tả Usecase của hệ thống

|  |  |  |
| --- | --- | --- |
| **Tác nhân** | **Ca sử dụng** | **Mô tả** |
| Người sử dụng | Create wallet | Tạo ví với tên và mật khẩu, mật khẩu ví sẽ dùng để sinh ra Private Key |
| Delete wallet | Người dùng phải backup thông tin ví trước khi xóa ví hoàn toàn. |
| Import wallet | Thêm ví bằng Private Key hoặc chuỗi Mnemonic |
| Withdraw | Người sử dụng gửi một lượng coin đến một địa chỉ ví khác |
| Deposit | Người sử dụng nhận coin về ví thông qua địa chỉ của ví coin |
| Exchange | Là chức năng đổi tiền tại ví từ đồng coin này sang đồng coin khác với mức phí quy định. |
| Helps | Người dùng có thể gửi thắc mắc hoặc ý kiến đóng góp cho ví |
| Thay đổi thông tin cá nhân | Thay đổi các thông tin về tên ví, mật khẩu, passcode, ngôn ngữ |

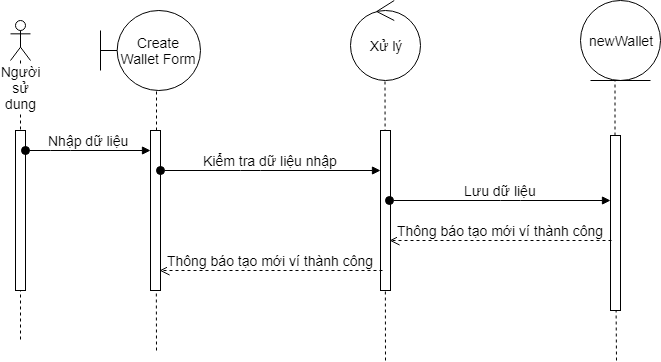
* 1. **Đặc tả và hiện thực hóa Usecase**
     1. **Usecase “Create wallet”**

Bảng 2.2 Mô tả Usecase create wallet

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Create wallet | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Không có | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn chức năng tạo ví |  |
| 2 |  | Hiển thị danh sách coin |
| 3 | Chọn 1 coin |  |
| 4 |  | Hiện thị form tạo ví |
| 5 | Nhập dữ liệu, nhấn tạo ví |  |
| 6 |  | Kiểm tra dữ liệu, hiển thị  thông báo |

****

Hình 2.10 Biểu đồ hoạt động create wallet

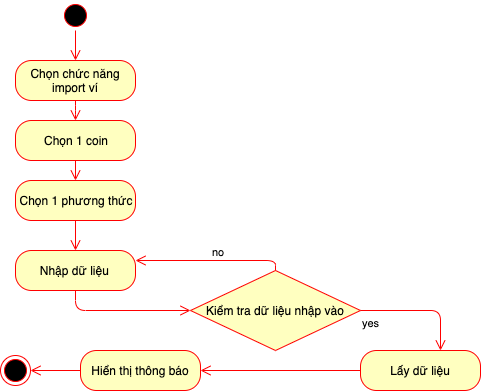
****

Hình 2.11 Biểu đồ trình tự create wallet

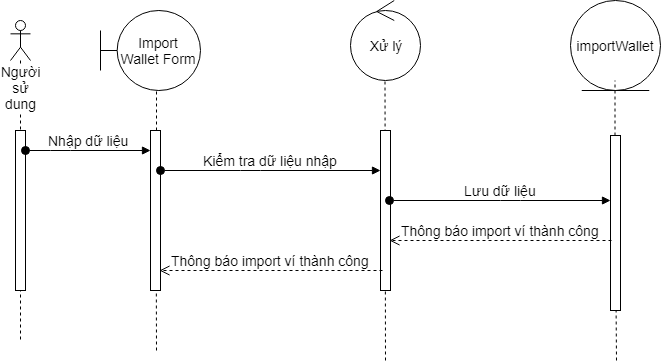
* + 1. **Usecase “Import wallet”**

Bảng 2.3 Mô tả Usecase import wallet

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Import wallet | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Không có | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn thêm ví |  |
| 2 |  | Hiển thị danh sách coin |
| 3 | Chọn 1 coin |  |
| 4 |  | Hiển thị danh sách phương thức thêm ví |
| 5 | Chọn 1 phương thức |  |
| 6 |  | Hiển thị form thêm ví |
| 7 | Nhập dữ liệu |  |
| 8 |  | Kiểm tra dữ liệu, hiển thị thông báo |



Hình 2.12 Biểu đồ hoạt động import wallet

****

Hình 2.13 Biểu đồ trình tự import wallet

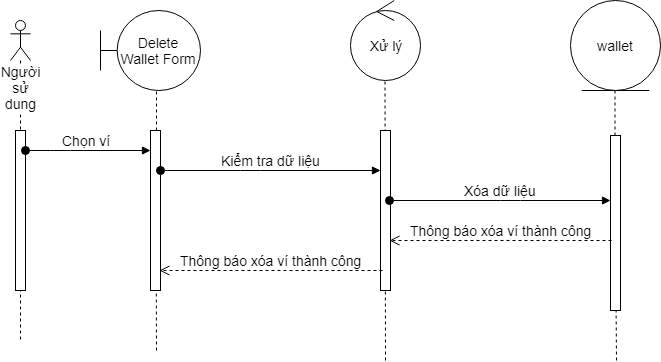
* + 1. **Usecase “Delete wallet”**

Bảng 2.4 Mô tả Usecase delete wallet

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Delete wallet | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Người dùng phải backup ví trước | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn chức năng xóa ví |  |
| 2 |  | Hiển thị thông báo |

****

Hình 2.14 Biểu đồ hoạt động delete wallet

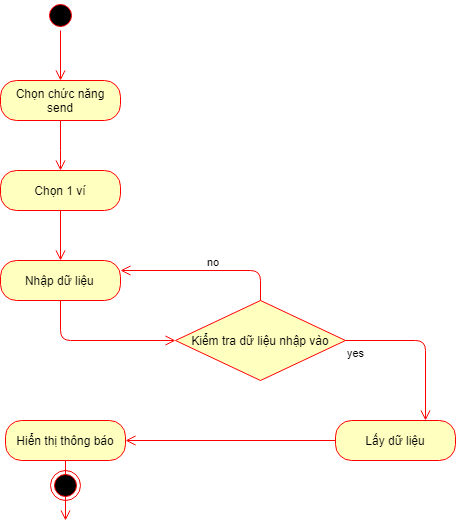
****

Hình 2.15 Biểu đồ trình tự delete wallet

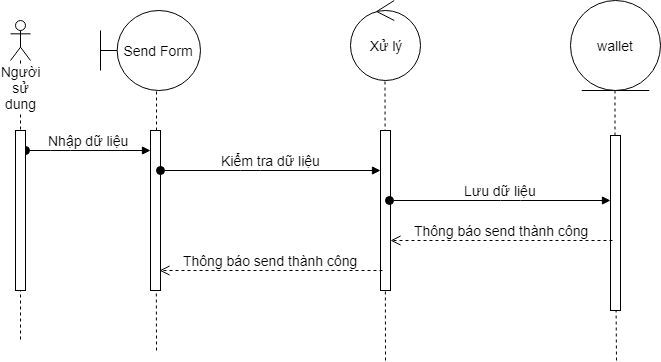
* + 1. **Usecase “Withdraw”**

Bảng 2.5 Mô tả Usecase withdraw

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Withdraw | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Số dư ví lớn hơn 0 | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn chức năng withdraw |  |
| 2 |  | Hiển thị form withdraw |
| 3 | Chọn ví |  |
| 4 | Nhập dữ liệu |  |
| 5 |  | Kiểm tra dữ liệu, hiển thị thông báo |

****

Hình 2.16 Biểu đồ hoạt động withdraw

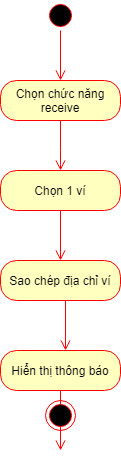
****

Hình 2.17 Biểu đồ trình tự withdraw

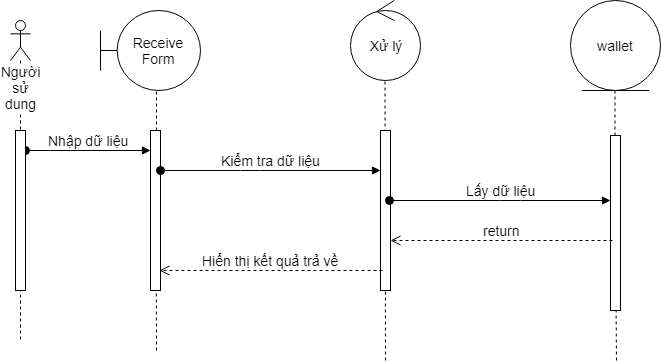
* + 1. **Usecase “Deposit”**

Bảng 2.6 Mô tả Usecase deposit

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Deposit | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Sau khi tạo ví hoặc Import ví thành công | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn chức năng Deposit |  |
| 2 |  | Hiển thị form Deposit |
| 3 | Chọn ví |  |
| 4 |  | Hiển thị địa chỉ ví,  mã QR của địa chỉ ví |
| 5 | Sao chép địa chỉ ví |  |
| 6 |  | Hiển thị thông báo |

****

Hình 2.18 Biểu đồ hoạt động deposit

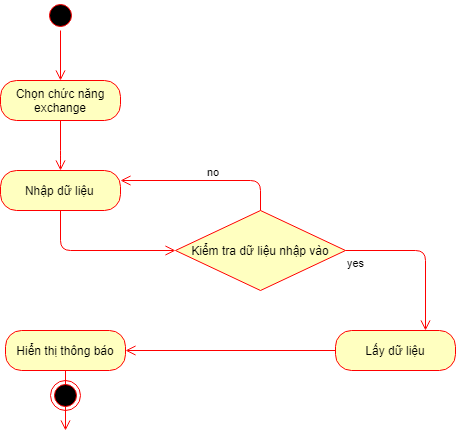
****

Hình 2.19 Biểu đồ trình tự deposit

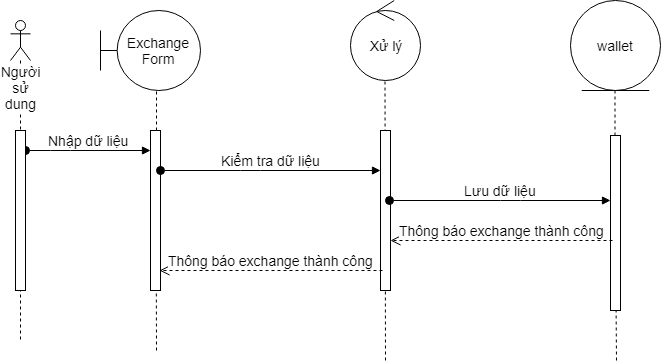
* + 1. **Usecase “Exchange”**

Bảng 2.7 Mô tả Usecase exchange

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Đổi coin (Exchange) | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Số dư của coin đổi lớn hơn 0 | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn chức năng Exchange |  |
| 2 |  | Hiển thị form Exchange |
| 3 | Nhập dữ liệu |  |
| 4 |  | Kiểm tra dữ liệu và  hiển thị thông báo |

****

Hình 2.20 Biểu đồ hoạt động exchange

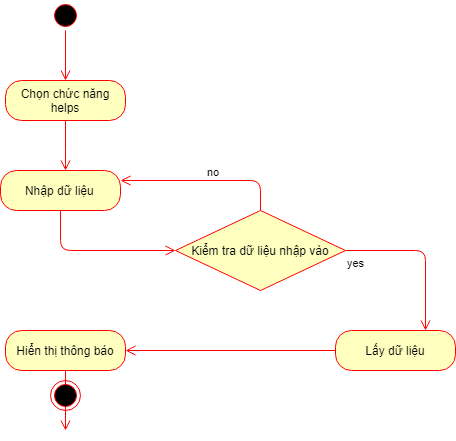
****

Hình 2.21 Biểu đồ trình tự exchange

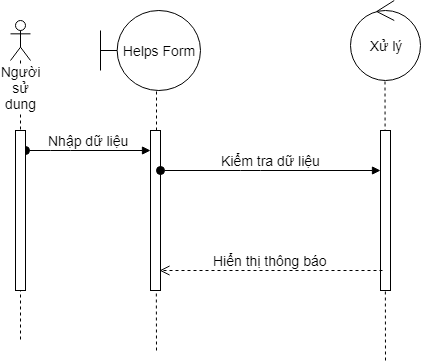
* + 1. **Usecase “Helps”**

Bảng 2.8 Mô tả Usecase helps

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Helps (Trợ giúp) | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Không có | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn chức năng Helps |  |
| 2 |  | Hiển thị form Helps |
| 3 | Nhập dữ liệu |  |
| 4 |  | Kiểm tra dữ liệu và  hiển thị thông báo |

****

Hình 2.22 Biểu đồ hoạt động helps

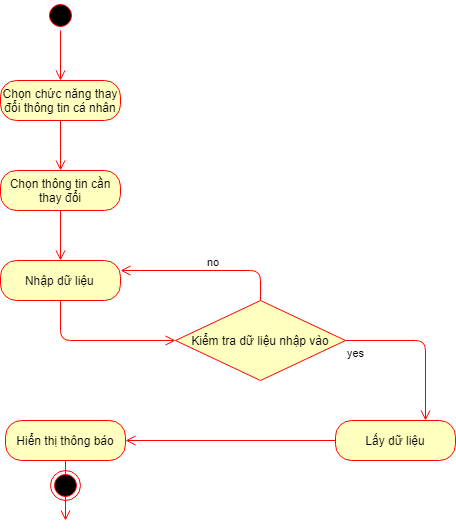
****

Hình 2.23 Biểu đồ trình tự helps

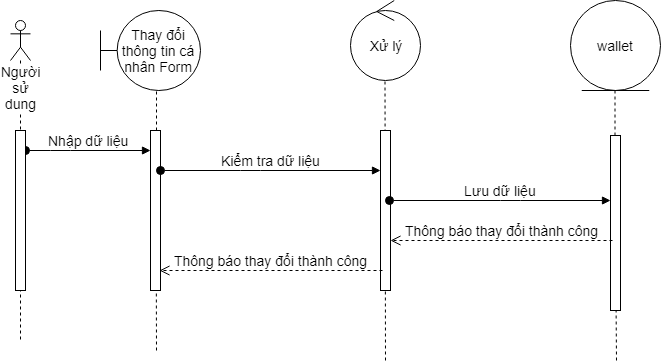
* + 1. **Usecase “Thay đổi thông tin cá nhân”**

Bảng 2.9 Mô tả Usecase thay đổi thông tin cá nhân

|  |  |  |  |
| --- | --- | --- | --- |
| Usecase | | Thay đổi thông tin cá nhân | |
| Tác nhân | | Người sử dụng | |
| Điều kiện | | Không có | |
|  | | **Tác nhân tác động** | **Hệ thống** |
| Luồng sự kiện | 1 | Chọn chức năng Thay đổi thông tin cá nhân |  |
| 2 |  | Hiển thị form thay đổi thông tin cá nhân |
| 3 | Chọn thông tin cần thay đổi |  |
| 4 | Nhập dữ liệu mới |  |
| 5 |  | Kiểm tra dữ liệu và hiển thị thông báo |

****

Hình 2.24 Biểu đồ hoạt động Thay đổi thông tin cá nhân

****

Hình 2.25 Biểu đồ trình tự Thay đổi thông tin cá nhân

* 1. **Biểu đồ lớp đối tượng (Class Diagram)**
  2. **Thiết kế dữ liệu**
  3. **Thiết kế gói**
  4. **Kết luận chương 2**

Chương 2 đã phân tích rõ yêu cầu và chức năng của ứng dụng ví bitcoin. Đồng thời đưa ra các biểu đồ thể hiện cụ thể từng chức năng sẽ hoạt động ra sao để người dùng nắm rõ.

# 

# CHƯƠNG 3: XÂY DỰNG ỨNG DỤNG

# 3.1. Công nghệ, công cụ và môi trường phát triển

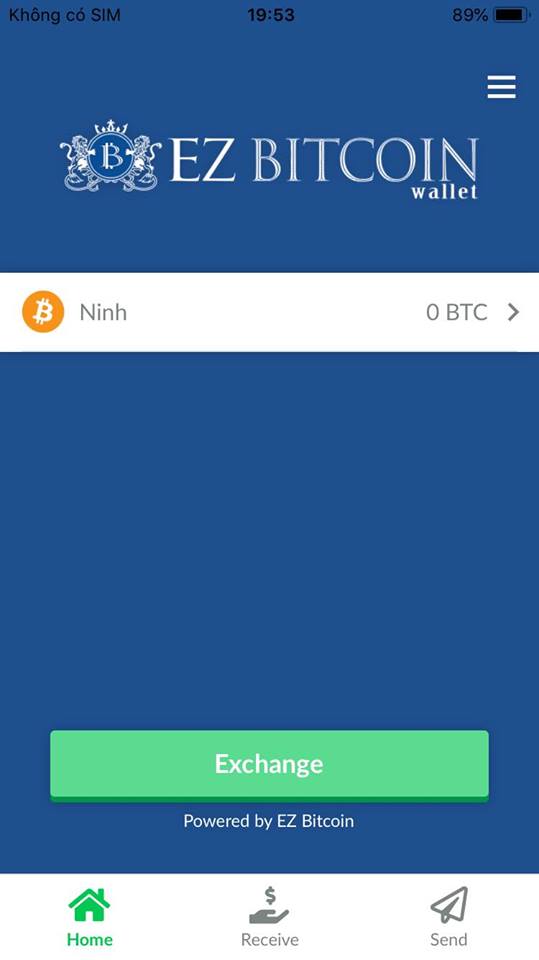
Ứng dụng Bitcoin Wallet lựa chọn xây dựng trên nền tảng React-native, ngôn ngữ lập trình JavaScript cho cả hai hệ điều hành Android và IOS, công cụ sử dụng Visual Studio Code, Android Studio, Xcode, môi trường phát triển di dộng.

# 3.2 Giao diện hệ thống

Dưới đây là một số màn hình của ứng dụng đã xây dựng.

# 3.2.1 Màn hình home

Khi mới truy cập ứng dụng, màn hình sẽ hiển thị danh sách ví với coin tương ứng hiện có của người dùng. Người dùng có thể vào xem chi tiết ví khi nhấn chọn một ví coin trong danh sách ví. Người dùng có thể sử dụng chức năng exchange khi nhấn chọn bút “Exchange” phía dưới màn hình. Người dùng có thể thực hiện deposit khi nhấn chọn tab “Receive” hay thực hiện withdraw khi nhấn chọn tab “Send” trên màn hình. Ngoài ra, người dùng có thể di chuyển đến màn hình cài đặt khi nhấn chọn icon menu phía trên góc phải của màn hình.

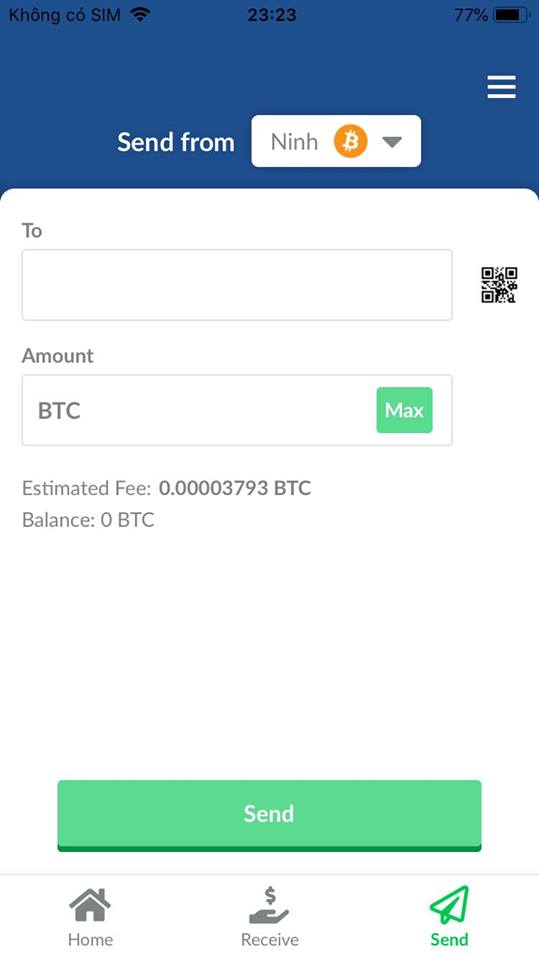
****

Hình 3.1 Màn hình home

# 3.2.2 Màn hình Send

Khi chọn tab “Send”, người dùng sẽ di chuyển đến màn withdraw. Để withdraw thành công, người dùng chọn ví coin withdraw tại combobox “Send from”, nhập địa chỉ gửi tại ô nhập “To” hoặc quét qr địa chỉ gửi khi nhấn chọn icon qrcode bên cạnh ô nhập, nhập số lượng coin tuỳ ý hoặc nhấn button “MAX” để nhập tối đa lượng coin trong ví. Sau khi nhập đầy đủ thông tin, mức fee phải chịu khi thực hiện withdraw sẽ được ước tính và số dư còn lại của ví. Người dùng nhấn nút “Send” để hoàn tất chức năng.

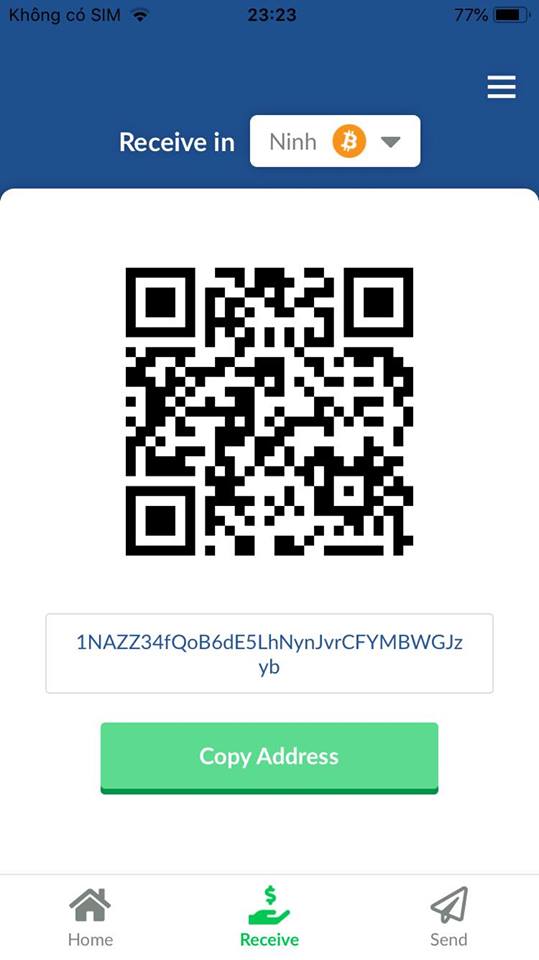
Tại màn hình withdraw, người dùng cũng có thể di chuyển đến màn hình cài đặt khi nhấn icon menu phía trên góc phải.

****

Hình 3.2 Màn hình Send

# 3.2.3. Màn hình Receive

Khi chọn tab “Receive”, người dùng sẽ di chuyển đến màn deposit. Người dùng có thể chọn ví muốn deposit tại combobox “Receive in”. Trên màn sẽ hiển thị chuỗi địa chỉ public của ví, mã qrcode của địa chỉ và nút “Coppy Address” để người dùng sao chép địa chỉ ví. Tại màn hình deposit, người dùng cũng có thể di chuyển đến màn hình cài đặt khi nhấn icon menu phía trên góc phải.

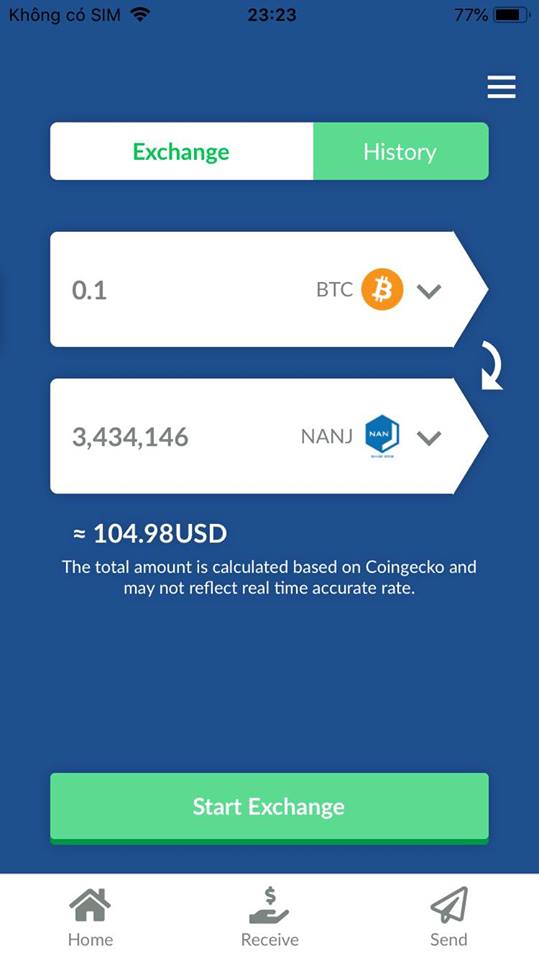
****

Hình 3.3 Màn hình Receive

### 

# 3.2.4. Màn hình Exchange

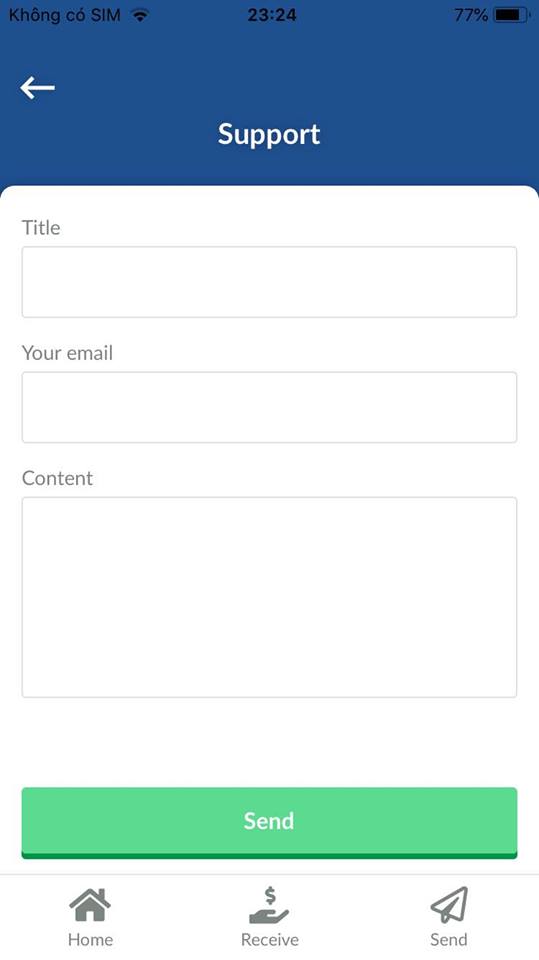
Tại màn hình exchange, người dùng cũng có thể xem thông tin lịch sử exchange khi nhấn chọn tab “History”. Tại tab “Exchange”, để thực hiện exchange thành công, yêu cầu người dùng chọn ví cần exchange, nhập số lượng exchange mong muốn. Khi nhập đầy đủ thông tin, ứng dụng sẽ tính toán quy đổi lượng exchange ra đơn vị USD tương ứng, người dùng nhấn nút “Exchange” để hoàn tất chức năng. Tại màn hình exchange, người dùng cũng có thể di chuyển đến màn hình cài đặt khi nhấn icon menu phía trên góc phải.

****

Hình 3.4 Màn hình Exchange

# 3.2.5 Màn hình Helps

Trong quá trình sử dụng ứng dụng, người dùng có bất cứ thắc mắc về ứng dụng hay góp ý để phát triển ứng dụng có thể gửi mail trực tiếp cho nhà phát triển thông qua chức năng “Helps” trong màn hình cài đặt. Người dùng nhập tiêu đề, địa chỉ mail của người dùng, nội dung muốn gửi vào các ô nhập tương ứng và nhấn “Send” để hoàn thành chức năng.

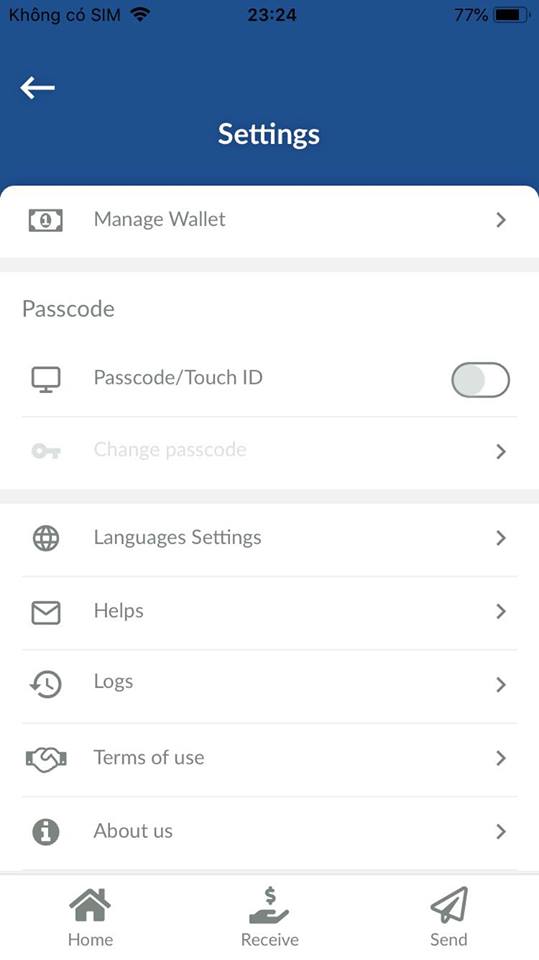
****

Hình 3.5 Màn hình Helps

### 

# 3.2.6 Màn hình Settings

Tại màn hình cài đặt, người dùng có thể cài đặt bảo vệ passcode/touchid, thay đổi ngôn ngữ ứng dụng, xem logs, term of use, about us, thay đổi thông tin ví.

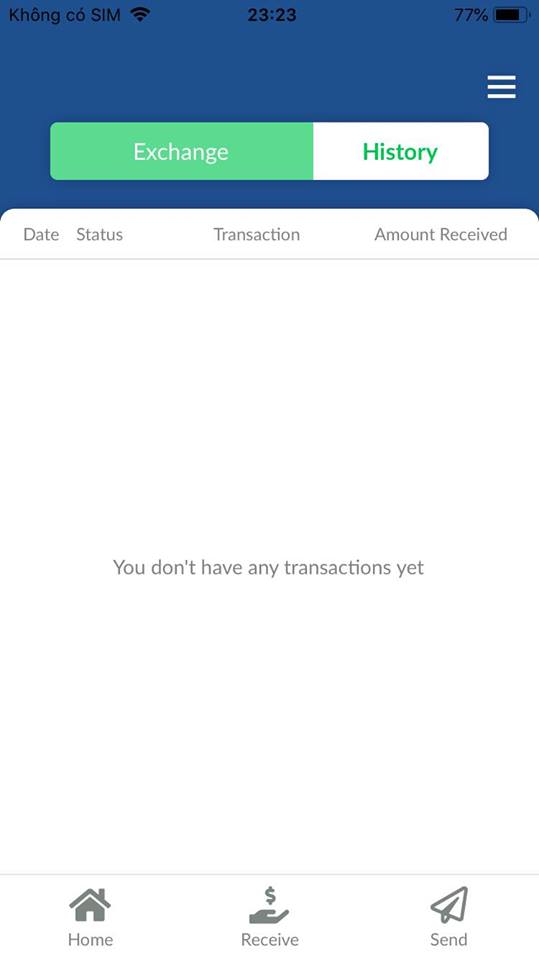


Hình 3.6 Màn hình Settings

### 

# 3.2.7 Màn hình History

Lịch sử các lần exchange của người dùng sẽ được lưu lại với các thông tin cụ thể: ngày tháng giao dịch, trạng thái giao dịch, mã hash giao dịch và số lượng coin trong giao dịch.

****

Hình 3.7 Màn hình History

# 

**3.3 Kết luận chương 3**

Chương 3 đã nêu được các công cụ để xây dựng nên ứng dụng ví, đồng thời cũng đưa ra được các hình ảnh trực quan của từng chức năng.

# KẾT LUẬN

Ứng dụng ví Bitcoin đã đáp ứng đầy đủ tính năng cần có của một ví tiền điện tử: deposit, withdraw, transaction history… Ngoài ra, ví còn tối ưu được các thao tác người dùng giúp trải nghiệm đơn giản, tiện lợi và an toàn hơn các ứng dụng ví khác.

**Kết luận và hướng nghiên cứu trong tương lai**

Những kết quả đạt được:

* Hiểu biết nhiều hơn về các kỹ thuật trong lập trình React-native.
* Phân thích thiết kế hướng đối tượng theo hướng chuyên nghiệp hơn.
* Hiểu biết hơn về nghiệp vụ ví Bitcoin.
* Nâng cao tinh thần tự học, tự nghiên cứu.
* Ứng dụng có giao diện dễ dùng, thẩm mỹ.
* Đáp ứng đầy đủ tính năng của một ví Bitcoin, tính bảo mật cao, cơ chế rõ ràng.

Hướng phát triển

* Thêm nhiều ngôn ngữ hỗ trợ
* Thêm nhiều coin
* Tăng các hình thức bảo mật mới