TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

Phát triển ứng dụng ví tiền điện tử tích hợp NFT và DeFi

ĐẶNG TÙNG LÂM
lam.dt183936@sis.hust.edu.vn

Ngành: Công Nghệ Thông Tin

Giảng viên hướng dẫn: TS. Nguyễn Đức Anh

Chữ kí GVHD

Khoa: Khoa học máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 12/2024

LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành nhất đến gia đình – nguồn động lực lớn lao luôn ở bên cạnh, ủng hộ và đồng hành cùng em trong suốt hành trình thực hiện đồ án tốt nghiệp.

Em cũng vô cùng biết ơn thầy cô, đặc biệt là giảng viên hướng dẫn, vì những chỉ dẫn tận tình, góp ý quý báu đã giúp em hoàn thiện đồ án này.

Bên cạnh đó, em muốn cảm ơn bạn bè – những người đã chia sẻ kiến thức, động viên và sát cánh trong suốt quãng thời gian học tập và nghiên cứu.

Cuối cùng, em trân trọng chính nỗ lực của bản thân vì đã kiên trì, chăm chỉ và quyết tâm vượt qua những thử thách để đạt được kết quả tốt nhất.

Đồ án này là thành quả của sự đồng hành và cố gắng không ngừng, em xin cảm ơn tất cả!

TÓM TẮT NỘI DUNG ĐỒ ÁN

Trong thời đại blockchain phát triển mạnh mẽ, ví điện tử dành cho tiền mã hóa (crypto wallet) đã trở thành một công cụ không thể thiếu, hỗ trợ người dùng lưu trữ, quản lý và giao dịch tài sản kỹ thuật số. Tuy nhiên, sự phổ biến của ví điện tử cũng đi kèm với những thách thức lớn, bao gồm bảo mật tài sản, trải nghiệm người dùng phức tạp, và khả năng tương thích với nhiều loại token khác nhau. Các giải pháp hiện tại như MetaMask, Trust Wallet đã cung cấp nhiều tính năng hữu ích nhưng vẫn tồn tại hạn chế, như giao diện khó sử dụng đối với người mới, chi phí giao dịch cao, hoặc nguy cơ bị tấn công.

Trong đồ án này, em lựa chọn hướng phát triển một ví điện tử tập trung vào bảo mật cao, giao diện thân thiện với người dùng và hỗ trợ đa nền tảng. Lý do lựa chọn hướng này là để giải quyết bài toán về tính an toàn và tính tiện dụng, đồng thời cung cấp một giải pháp tối ưu hơn trong quản lý tài sản số cho cả người dùng mới lẫn người dùng có kinh nghiệm.

Giải pháp được đề xuất bao gồm việc xây dựng một ví điện tử phi tập trung, sử dụng công nghệ xác thực đa lớp (MFA), mã hóa khóa cá nhân tiên tiến, và tích hợp với các blockchain phổ biến như Ethereum, Binance Smart Chain. Ví cũng hỗ trợ chuyển đổi token dễ dàng thông qua tích hợp các giao thức DeFi như Uniswap hoặc PancakeSwap.

Đóng góp chính của đồ án là một hệ thống ví điện tử crypto toàn diện, cung cấp trải nghiệm mượt mà và bảo mật cao. Kết quả thử nghiệm cho thấy ví hoạt động ổn định, tốc độ xử lý nhanh và bảo vệ dữ liệu hiệu quả. Giải pháp này không chỉ hỗ trợ giao dịch crypto an toàn mà còn mở ra cơ hội áp dụng rộng rãi trong lĩnh vực tài chính phi tập trung (DeFi).

Sinh viên thực hiện

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....5
1.1 Đặt vấn đề.....5
1.2 Mục tiêu và phạm vi đề tài.....5
1.3 Định hướng giải pháp.....6
1.4 Bố cục đồ án.....6
CHƯƠNG 2. KHẢO SÁT VÀ PHÂN TÍCH YÊU CẦU.....7
2.1 Khảo sát hiện trạng.....7
2.2 Tổng quan chức năng.....9
2.2.1 Biểu đồ use case tổng quát.....9
2.3 Đặc tả chức năng.....19
2.3.1 Đặc tả use case "Tạo ví mới".....19
2.3.2 Đặc tả use case "Khôi phục ví".....19
2.3.3 Đặc tả use case "Đăng nhập".....19
2.3.4 Đặc tả use case "Đăng xuất".....19
2.3.5 Đặc tả use case "Tạo danh bạ".....19
2.3.6 Đặc tả use case "Thêm danh mục tài sản".....19
2.3.7 Đặc tả use case "Send".....19
2.3.8 Đặc tả use case "Receive".....19
2.3.9 Đặc tả use case "Swap/Exchange".....19
2.3.10 Đặc tả use case "Connect Dapps".....19
2.3.11 Đặc tả use case "Quản lý NFTs".....19
2.3.12 Đặc tả use case "ICO Token".....19
2.4 Yêu cầu phi chức năng.....28
CHƯƠNG 3. CÔNG NGHỆ SỬ DỤNG.....30
3.1 TypeScript.....30
3.2 Flutter.....31
3.3 MySQL.....32
CHƯƠNG 4. THIẾT KẾ, TRIỂN KHAI VÀ ĐÁNH GIÁ HỆ THỐNG.....34
4.1 Thiết kế kiến trúc.....34
4.1.1 Lựa chọn kiến trúc phần mềm.....34
4.1.2 Thiết kế tổng quan.....35
4.1.3 Thiết kế chi tiết gói.....37
4.2 Thiết kế chi tiết.....39
4.2.1 Thiết kế giao diện.....39
4.2.2 Thiết kế lớp.....41
4.2.3 Thiết kế cơ sở dữ liệu.....56
4.3 Xây dựng ứng dụng.....63
4.3.1 Thư viện và công cụ sử dụng.....63
4.3.2 Kết quả đạt được.....64

4.3.3 Minh hoạ các chức năng chính..... 64
4.4 Kiểm thử..... 67
4.5 Triển khai..... 69
CHƯƠNG 5. CÁC GIẢI PHÁP VÀ ĐÓNG GÓP NỔI BẬT.....72
CHƯƠNG 6. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN.....76
6.1 Kết luận..... 76
6.2 Hướng phát triển..... 76

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

1.1 Đặt vấn đề

Trong những năm gần đây, sự phát triển vượt bậc của công nghệ blockchain và tài chính phi tập trung (DeFi) đã tạo ra một cuộc cách mạng trong việc quản lý tài sản kỹ thuật số. Cùng với đó, tiền mã hóa (cryptocurrency) đang ngày càng phổ biến và được chấp nhận rộng rãi trên toàn cầu như một hình thức thanh toán, đầu tư và lưu trữ giá trị. Tuy nhiên, việc quản lý và giao dịch các tài sản kỹ thuật số này đang đặt ra nhiều thách thức lớn cho người dùng, đặc biệt là về bảo mật, sự tiện lợi, và khả năng tương thích với các hệ thống tài chính hiện có.

Hiện tại, các ví điện tử dành cho tiền mã hóa, như MetaMask hay Trust Wallet, đã cung cấp các công cụ cơ bản để người dùng quản lý tài sản. Tuy nhiên, số lượng các vụ tấn công mạng, mất mát tài sản do lỗ hổng bảo mật, và sự phức tạp trong quá trình sử dụng vẫn là những rào cản lớn đối với cả người dùng mới và người dùng có kinh nghiệm. Đồng thời, nhu cầu kết nối các ví điện tử với nhiều blockchain khác nhau và tích hợp các giao thức tài chính phi tập trung ngày càng gia tăng, tạo ra một bài toán đòi hỏi sự cải tiến mạnh mẽ về công nghệ.

Nếu bài toán về bảo mật, trải nghiệm người dùng và khả năng tương thích của ví điện tử được giải quyết, điều này sẽ mang lại lợi ích to lớn cho người dùng cá nhân, các doanh nghiệp hoạt động trong lĩnh vực blockchain, cũng như hệ sinh thái DeFi nói chung. Không chỉ giúp người dùng yên tâm hơn khi lưu trữ và giao dịch tài sản kỹ thuật số, một hệ thống ví điện tử hiệu quả còn góp phần thúc đẩy sự phát triển của các ứng dụng blockchain trong nhiều lĩnh vực khác, từ thương mại điện tử đến tài chính và đầu tư.

Do đó, vấn đề này mang tính cấp thiết và có ý nghĩa quan trọng không chỉ trong việc đáp ứng nhu cầu của người dùng hiện tại mà còn mở ra những cơ hội lớn cho tương lai của tài chính số.

1.2 Mục tiêu và phạm vi đề tài

Với sự bùng nổ của thị trường tiền mã hóa và công nghệ blockchain, nhu cầu về các hệ thống ví điện tử an toàn, tiện lợi và tương thích cao ngày càng gia tăng. Các sản phẩm hiện tại như MetaMask, Trust Wallet, và Coinbase Wallet đã đạt được nhiều thành công nhất định trong việc cung cấp công cụ quản lý và giao dịch tài sản số. Tuy nhiên, qua phân tích, có thể nhận thấy rằng các ví này vẫn còn nhiều hạn chế đáng kể.

Thứ nhất, vấn đề bảo mật vẫn luôn là mối lo ngại hàng đầu. Các vụ tấn công phishing, lộ khóa cá nhân, và khai thác lỗ hổng trong các dApp liên tục xảy ra, gây tổn thất lớn cho người dùng. Thứ hai, các sản phẩm hiện nay thường có giao diện và quy trình sử dụng khá phức tạp, tạo ra rào cản đối với người mới tiếp cận tiền mã hóa. Cuối cùng, khả năng tương thích của các ví này vẫn chưa toàn diện, đặc biệt trong việc hỗ trợ giao dịch liên chuỗi (cross-chain) hoặc tích hợp với nhiều blockchain và dApp khác nhau.

Trên cơ sở các phân tích trên, mục tiêu của đề tài này là phát triển một hệ thống ví điện tử mới nhằm:

- Tăng cường bảo mật: Sử dụng công nghệ xác thực đa lớp (MFA) và mã hóa tiên tiến để bảo vệ tài sản và thông tin của người dùng.

- Cải thiện trải nghiệm người dùng: Tạo giao diện thân thiện, quy trình sử dụng đơn giản và hiệu quả, phù hợp với cả người dùng mới và người dùng có kinh nghiệm.
- Tăng khả năng tương thích: Hỗ trợ đa chuỗi (multi-chain), giao dịch liên chuỗi (cross-chain), và tích hợp dễ dàng với các dApp trên nhiều blockchain khác nhau.

Phạm vi đề tài tập trung vào việc xây dựng một hệ thống ví điện tử đáp ứng các nhu cầu trên, thử nghiệm trong môi trường blockchain phổ biến như Ethereum và Binance Smart Chain. Hệ thống sẽ cung cấp các chức năng chính như lưu trữ, giao dịch tài sản, quản lý khóa cá nhân, và hỗ trợ tích hợp các giao thức DeFi.

Đề tài này không chỉ nhằm giải quyết các hạn chế hiện tại của các ví điện tử mà còn hướng đến việc tạo ra một sản phẩm đột phá, góp phần thúc đẩy ứng dụng công nghệ blockchain vào thực tiễn.

1.3 Định hướng giải pháp

Để giải quyết các vấn đề về bảo mật, trải nghiệm người dùng và khả năng tương thích trong hệ thống ví điện tử tiền mã hóa, đồ án định hướng phát triển dựa trên các công nghệ hiện đại như xác thực đa lớp (MFA), mã hóa bất đối xứng (RSA/ECC), và tích hợp các giao thức DeFi như Uniswap hoặc PancakeSwap. Hệ thống sẽ được xây dựng theo mô hình phi tập trung (decentralized) nhằm đảm bảo tính minh bạch và an toàn. Giải pháp được đề xuất là thiết kế một ví điện tử phi tập trung với các tính năng chính như lưu trữ và quản lý tài sản số, thực hiện giao dịch nhanh chóng, và hỗ trợ giao dịch liên chuỗi (cross-chain). Công nghệ blockchain sẽ được áp dụng để đảm bảo dữ liệu không thể bị giả mạo, cùng với giao diện người dùng thân thiện để người dùng dễ dàng thao tác. Đóng góp chính của đồ án là một hệ thống ví điện tử với các tính năng vượt trội như bảo mật cao nhờ mã hóa tiên tiến và xác thực đa lớp, giao diện thân thiện giúp nâng cao trải nghiệm người dùng, và khả năng tương thích rộng rãi với nhiều blockchain và dApp. Kết quả đạt được là một hệ thống ví điện tử hoạt động ổn định, an toàn, dễ sử dụng và có tiềm năng ứng dụng thực tiễn trong các lĩnh vực liên quan đến tài chính phi tập trung và blockchain.

1.4 Bố cục đồ án

Phần còn lại của báo cáo đồ án tốt nghiệp này được tổ chức như sau.

Chương 2 trình bày quá trình khảo sát thị trường và xác định các yêu cầu đối với ứng dụng ví điện tử. Nội dung bao gồm việc thu thập ý kiến từ người dùng để hiểu rõ nhu cầu sử dụng ví điện tử. Các yêu cầu chức năng và phi chức năng của hệ thống sẽ được liệt kê chi tiết, như yêu cầu về giao diện thân thiện, tốc độ xử lý nhanh, và tính bảo mật cao. Ngoài ra, chương này cũng phân tích các ứng dụng ví điện tử hiện có trên thị trường để tìm hiểu ưu và nhược điểm của chúng, từ đó đề xuất các điểm cải tiến.

Chương 3 tập trung giới thiệu các công nghệ chính được áp dụng để phát triển ứng dụng ví điện tử. Các công nghệ được chọn bao gồm ngôn ngữ lập trình (như Typescript), framework phát triển ứng dụng di động (như Flutter), và cơ sở dữ liệu (như MySQL). Ngoài ra, chương này sẽ phân tích chi tiết các công nghệ liên quan đến bảo mật, như mã hóa dữ liệu, xác thực hai yếu tố (2FA), và giao thức HTTPS. Mỗi công nghệ được chọn đều sẽ được đánh giá dựa trên tính phù hợp, hiệu suất, và khả năng mở rộng để đáp ứng các yêu cầu của hệ thống.

Chương 4 mô tả chi tiết quá trình thiết kế hệ thống ứng dụng ví điện tử từ giai đoạn đầu đến khi triển khai. Phần đầu của chương sẽ trình bày kiến trúc tổng thể của hệ thống, bao gồm mô hình MVC và các thành phần chính như backend, frontend, và cơ sở dữ liệu. Tiếp theo, sơ đồ thiết kế chi tiết như sơ đồ lớp (UML) và biểu đồ thực thể liên kết(ERD) . Chương này cũng bao gồm thiết kế giao diện người dùng với các màn hình chính như trang đăng nhập, nạp/rút tiền, và lịch sử giao dịch. Phần triển khai sẽ trình bày chi tiết quy trình xây dựng hệ thống, từ việc thiết lập môi trường phát triển, coding, đến kiểm thử và triển khai trên môi trường thực tế.

Chương 5 tập trung vào các giải pháp kỹ thuật và các đóng góp nổi bật được thực hiện trong đồ án. Hệ thống cũng được tối ưu hóa về hiệu năng với việc sử dụng caching để tăng tốc độ xử lý giao dịch. Các biện pháp bảo mật mạnh mẽ, như mã hóa đầu cuối và xác thực sinh trắc học, sẽ được nhấn mạnh để đảm bảo an toàn cho người dùng.

Chương cuối cùng sẽ tổng hợp các kết quả đạt được của đồ án và đánh giá hiệu quả của ứng dụng ví điện tử. Ưu điểm nổi bật của hệ thống như tính tiện lợi, độ bảo mật cao, và khả năng mở rộng sẽ được tóm lược. Đồng thời, các hướng phát triển trong tương lai sẽ được đề xuất, bao gồm mở rộng hỗ trợ nhiều blockchain hơn, tích hợp thêm các DApp và dịch vụ phi tập trung, cùng với việc tối ưu hóa hiệu suất để đảm bảo ứng dụng hoạt động mượt mà trên nhiều nền tảng và thiết bị.

CHƯƠNG 2. KHẢO SÁT VÀ PHÂN TÍCH YÊU CẦU

2.1 Khảo sát hiện trạng

Để phát triển hệ thống ví điện tử tiền mã hóa, việc khảo sát và đánh giá các sản phẩm hiện có là bước quan trọng để xác định những ưu điểm và nhược điểm của các giải pháp hiện tại, từ đó rút ra những yêu cầu cần thiết cho phần mềm. Quá trình khảo sát hiện trạng được thực hiện thông qua ba nguồn chính: (i) Người dùng/khách hàng, (ii) Các hệ thống đã có, và (iii) Các ứng dụng tương tự.

(i) Khảo sát người dùng/khách hàng:
Khách hàng của ví điện tử tiền mã hóa thường có yêu cầu về tính bảo mật, dễ sử dụng và khả năng hỗ trợ nhiều loại tiền mã hóa. Họ mong muốn các hệ thống dễ dàng thao tác, nhanh chóng và an toàn khi thực hiện giao dịch. Một số yêu cầu nổi bật từ người dùng bao gồm: bảo mật cao (xác thực hai yếu tố, mã hóa), hỗ trợ đa blockchain (Ethereum, Binance Smart Chain, Polygon), và giao diện người dùng thân thiện.

(ii) Các hệ thống đã có:
Các ví điện tử phổ biến hiện nay như MetaMask, Trust Wallet, và Coinbase Wallet đã đạt được một số thành tựu nhất định trong việc quản lý và giao dịch tài sản mã hóa. Tuy nhiên, chúng vẫn còn tồn tại một số nhược điểm:

- MetaMask: Ưu điểm là dễ dàng tích hợp với các dApp, nhưng giao diện sử dụng khá phức tạp đối với người mới và thiếu tính bảo mật cao.
- Trust Wallet: Hỗ trợ nhiều blockchain và token, nhưng cũng gặp phải vấn đề về bảo mật và tốc độ giao dịch.
- Coinbase Wallet: Tính năng tích hợp giao dịch fiat (tiền pháp định) rất tiện lợi, nhưng chỉ hỗ trợ một số ít blockchain và thiếu tính phi tập trung.

(iii) Các ứng dụng tương tự:

Các giải pháp tương tự cũng chú trọng đến việc cải thiện tính bảo mật và trải nghiệm người dùng. Các hệ thống ví điện tử tiền mã hóa khác ngoài các sản phẩm lớn như MetaMask và Trust Wallet vẫn chưa phát triển đủ mạnh để cạnh tranh về bảo mật và tính năng. Một số ví khác như Exodus, Mycelium cũng gặp vấn đề trong việc hỗ trợ giao dịch liên chuỗi và bảo mật không cao.

Mô tả các tính năng phần mềm cần phát triển:
Dựa trên khảo sát hiện trạng, các tính năng cần phát triển cho hệ thống ví điện tử tiền mã hóa bao gồm:

- Bảo mật cao: Áp dụng các phương pháp xác thực đa lớp (MFA), mã hóa khóa cá nhân tiên tiến (RSA, ECC).
- Hỗ trợ đa blockchain: Cung cấp khả năng giao dịch trên nhiều blockchain phổ biến như Ethereum, Binance Smart Chain, Polygon, v.v.
- Giao diện người dùng thân thiện: Thiết kế giao diện đơn giản, dễ sử dụng, phù hợp với cả người dùng mới và có kinh nghiệm.
- Giao dịch liên chuỗi (cross-chain): Hỗ trợ giao dịch giữa các blockchain khác nhau, giúp tăng khả năng linh hoạt và tối ưu cho người dùng.

- Tích hợp DeFi và dApp: Tích hợp các giao thức tài chính phi tập trung (DeFi) và ứng dụng phi tập trung (dApp) vào ví điện tử để mở rộng tính năng và ứng dụng.

Việc phát triển các tính năng này sẽ giúp giải quyết những hạn chế của các hệ thống hiện tại và đáp ứng tốt hơn yêu cầu của người dùng.

2.2 Tổng quan chức năng

2.2.1 Biểu đồ use case tổng quát