**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

A blue and white logo

Description automatically generated with low confidence

**ĐỒ ÁN MÃ HOÁ ỨNG DỤNG VÀ AN NINH THÔNG TIN**

**ĐỀ TÀI: TÀI CHÍNH NGÂN HÀNG KẾT HỢP VỚI CHATGPT**

**19120616 - Mã Chấn Phong**

**19120641 - Nguyễn Đức Phát Tài**

**19120649 - Phạm Ngọc Tân**

**GIÁO VIÊN HƯỚNG DẪN**

PGS.TS Nguyễn Đình Thúc

Mục Lục

[I. Lời nói đầu. 3](#_Toc135006422)

[II. Giới thiệu. 4](#_Toc135006423)

[III. Yêu cầu kỹ thuật 5](#_Toc135006424)

[1. Thông tin ứng dụng 5](#_Toc135006425)

[2. Phương pháp kỹ thuật 5](#_Toc135006426)

[3. Bảo vệ source code 7](#_Toc135006434)

[IV. Yêu cầu dữ liệu 8](#_Toc135006435)

[1. Thông tin 8](#_Toc135006436)

[2. Nguồn dữ liệu 9](#_Toc135006437)

[3. Thông tin dữ liệu thu thập 9](#_Toc135006438)

[V. Màn hình giao diện 10](#_Toc135006439)

[1. Đăng ký 10](#_Toc135006440)

[2. Đăng nhập 11](#_Toc135006443)

[3. Chat 12](#_Toc135006444)

[VI. Mô hình hoạt động 17](#_Toc135006450)

[1. Luồng hoạt động 17](#_Toc135006451)

[2. Đặc tả yêu cầu 17](#_Toc135006452)

[VII. Kế hoạch thực hiện 19](#_Toc135006456)

[1. Kế hoạch 19](#_Toc135006457)

[2. Phân Công 20](#_Toc135006458)

# **Lời nói đầu.**

Trong những năm gần đây, trí tuệ nhân tạo (AI) đã trở thành xu hướng công nghệ hot nhất với sự phát triển mạnh mẽ và những ứng dụng đa dạng. Trong đó, dịch vụ chatbot đã trở nên phổ biến và đem lại nhiều tiện ích cho người dùng. Chatbot là một hình thức trí tuệ nhân tạo được ứng dụng để hiểu và tương tác với người dùng bằng ngôn ngữ tự nhiên.

Trong tháng 11 năm 2022, một dịch vụ chatbot mới mang tên ChatGPT (Chat Generative Pre-training Transformer) đã chính thức ra mắt và thu hút được gần 10 triệu người dùng chỉ sau 40 ngày. Điều này cho thấy sự quan tâm và nhu cầu của người dùng đối ứng dụng của trí tuệ nhân tạo trong xu thế mới.

ChatGPT được phát triển bởi công ty OpenAI, với khả năng xử lý ngôn ngữ tự nhiên và đưa ra các câu trả lời phù hợp với từng câu hỏi của người dùng. Với khả năng học tập và cải tiến liên tục, ChatGPT có thể trở thành một trợ lý thông minh cho nhiều lĩnh vực, đặc biệt là trong lĩnh vực tài chính ngân hàng.

Do đó, đồ án ứng dụng ChatGPT vào lĩnh vực tài chính ngân hàng đã được triển khai với mục tiêu giúp người dùng tiếp cận thông tin về báo cáo tài chính và các dịch vụ của ngân hàng một cách dễ dàng và thuận tiện. Với tính năng giải đáp câu hỏi và cung cấp thông tin, ChatGPT sẽ giúp người dùng tiết kiệm thời gian và công sức khi tìm kiếm thông tin.

Ngoài ra, ứng dụng này cũng cho phép người dùng truy xuất thông tin về báo cáo tài chính cụ thể của các ngân hàng tại Việt Nam. Việc này sẽ giúp cho người dùng có thể nắm rõ hơn về hoạt động kinh doanh của ngân hàng, đánh giá được tính cạnh tranh và đưa ra quyết định đầu tư thông minh.

# **Giới thiệu.**

* Đề tài: Tài chính ngân hàng chatbot
* Tên đề tài: FBC – finance Bank Chat
* Thành viên:
  + 19120616 – Mã Chấn Phong
  + 19120641 – Nguyễn Đức Phát Tài
  + 19120649 – Phạm Ngọc Tân
* Mục tiêu đề tài:
  + Xây dụng ứng dụng ChatGPT để truy vấn thông tin từ cơ sở dữ liệu (database)
  + Xây dựng ứng dụng cho phép người dùng nhập vào ngôn ngữ tự nhiên và trả về là biểu đồ, câu trả lời phù hợp
  + Xây dựng ứng dụng có độ bảo mật cao, bảo vệ thông tin người dùng
  + Xây dựng ứng dụng web

# **Yêu cầu kỹ thuật**

## **Thông tin ứng dụng**

* Ngôn ngữ: Python, Javascript, Html/Css
* Framework: Django, Reactjs
* Database: Postgresql
* Work manage: jira, Git, Bitbucket
* Server: Azure, AWS EC2
* Nguồn dữ liệu:
  + Fireant: <https://fireant.vn/dashboard>
  + Vietstock: <https://vietstock.vn/>
  + Cafef: <https://cafef.vn/>

## **Phương pháp kỹ thuật**

### **Xác thực API và uỷ quyền**

* Tiêu chuẩn: json web token (JWT)
* Thời gian tồn tại: 60 phút
* Lợi ích: xác thực người dùng thông qua access key
* Thông tin:
  + Nhận khoá bí mật (access key) từ server thông qua tên đăng nhập và mật khẩu
  + Client ký tên bằng access key và gửi các API requests về server
  + Server xác thực người dùng và trả về kết quả tương ứng
* Ý tưởng:
  + Cho phép một số API requests có định danh người dùng
  + Cho phép một số API requests chỉ có admin mới được sử dụng

### **Hệ mã hoá bất đối xứng RSA**

* + Độ dài : 2048 bit
  + Thời gian tồn tại: 30 phút
  + Lợi ích: bảo vệ – gây khó khăn cho những ý định tấn công, lấy cắp thông tin
  + Thông tin:
    - Mỗi user là một cặp khoá riêng biệt
    - Người dùng chưa định danh sẽ sử dụng cặp khoá chung
    - Mỗi cặp khoá có thời gian sống là 30 phút
  + Ý tưởng:
    - Mã hoá thông tin đăng nhập: tên đăng nhập, mật khẩu
    - Mã hoá thông tin đăng ký: tên đăng nhập, mật khẩu, email
    - Mã hoá thông tin nhắn người dùng: tin nhắn, các thông tin cấu hình

### **Google reCaptcha**

* + Version: v3
  + Lợi ích: tránh bot automation đăng nhập hoặc qua các nền tảng call API
  + Thông tin:
  + Sử dụng google key public ở client để lấy serect token thông qua API của google
  + Gửi thông tin token về server
  + Server xác thực bằng token và google key serect thông qua API của google
  + Ý tưởng:
    - Sử dụng google captcha ở bước đăng nhập

### **Làm nhiễu**

* Lợi ý: bảo vệ dữ liệu thực
* Thông tin:
  + - Làm nhiễu thông tin
    - Bảo vệ thông tin người dùng
    - Tránh trường hợp có ý định xấu khi thông tin bị rò rỉ
* Ý tưởng:
  + - Làm nhiễu số tiền trong câu hỏi người dùng
    - Làm nhiễu thông tin về số liệu ở database khi trả về

### **Limit throllte**

* Lợi ích: tránh bị tấn công ddos
* Thông tin:
  + - Giới hạn số lần gọi API requests từ client
    - Chặn nếu số lần gọi API requests lớn trong một thời gian nhất định
* Ý tưởng:
  + - Giới hạn số lần gọi API đăng nhập: 3 lần/giờ
    - Giới hạn số lần gọi API có yêu cầu định danh người dùng: 30 lần/phút
    - Giới hạn số lần gọi API không cần định danh người dùng: 50 lần/phút

### **CORS Headers**

* Lợi ích: chỉ cho phép truy từ từ các domain nhất định
* Thông tin:
  + Thông tin cho server biết về domain thực hiện hành động này trên các API requests
* Ý tưởng:
  + Chỉ cho phép domain của mình hoặc domain local được phép call api trên giao diện
  + Không cho mở iframe trên các trang web khác

### **HTTPS**

* Lợi ích: giao thức được tích hợp thêm chứng chỉ bảo mật từ HTTPS với mục đích để mã hóa các thông tin giao tiếp làm tăng tính bảo mật.
* Thông tin:
  + Sử dụng domain được cung cấp
  + Install certificate from <https://sslforfree.com/>
* Ý tưởng:
  + Deploy backend server to https <https://fbc-api.lodilangthang.com>
  + Deploy frontend to https <https://fbc-chat.lodilangthang.com>

## **Bảo vệ source code**

* Lợi ích:
  + Tránh key bị lộ trên các công vụ quản lý source code: bitbucket
* Nếu bị lộ source thì vẫn bảo vệ các key bí mật
* Thông tin:
* Sử dụng biến các biến môi trường để lưu trữ các key đặc biệt
* Lưu trữ key ở file .env
* Bỏ .env vào .gitignore

# **Yêu cầu dữ liệu**

## **Thông tin**

* Mã chứng khoán: 27 (mã chứng ngân hàng Việt Nam)

|  |  |  |
| --- | --- | --- |
| STT | Mã | Tên |
| 1 | ABB | Ngân hàng TMCP An Bình |
| 2 | ACB | Ngân hàng TMCP Á Châu |
| 3 | AGR | Ngân hàng TMCP Đông Á |
| 4 | BID | Ngân hàng TMCP Đầu tư và Phát triển Việt Nam |
| 5 | BVB | Ngân hàng TMCP Bảo Việt |
| 6 | CTG | Ngân hàng TMCP Công Thương Việt Nam (VietinBank) |
| 7 | EIB | Ngân hàng TMCP Xuất Nhập Khẩu Việt Nam (Eximbank) |
| 8 | HDB | Ngân hàng TMCP Phát triển Tp. Hồ Chí Minh (HDBank) |
| 9 | KLB | Ngân hàng TMCP Kiên Long |
| 10 | LPB | Ngân hàng TMCP Liên Việt Post (LienVietPostBank) |
| 11 | MBB | Ngân hàng TMCP Quân đội (MB Bank) |
| 12 | MSB | Ngân hàng TMCP Hàng Hải Việt Nam (Maritime Bank) |
| 13 | NAB | Ngân hàng TMCP Nam Á |
| 14 | NVB | Ngân hàng TMCP Quốc Dân (National Citizen Bank) |
| 15 | OCB | Ngân hàng TMCP Phương Đông (OCB) |
| 16 | PGB | Ngân hàng TMCP Xăng dầu Petrolimex (PGBank) |
| 17 | SCB | Ngân hàng TMCP Sài Gòn (SaigonBank) |
| 18 | SGB | Ngân hàng TMCP Sài Gòn Công Thương (Saigonbank - CT) |
| 19 | SHB | Ngân hàng TMCP Sài Gòn - Hà Nội (SHB) |
| 20 | SSB | Ngân hàng TMCP Sài Gòn thương tín (Sacombank) |
| 21 | STB | Ngân hàng TMCP Sài Gòn thương Tín chi nhánh Tp. Hồ Chí Minh (Sacombank) |
| 22 | TCB | Ngân hàng TMCP Kỹ Thương Việt Nam (Techcombank) |
| 23 | TPB | Ngân hàng TMCP Tiên Phong (TPBank) |
| 24 | VAB | Ngân hàng TMCP Việt Á |
| 25 | VPB | Ngân hàng TMCP Việt Nam Thịnh Vượng (VPBank) |
| 26 | VCB | Ngân hàng TMCP Ngoại Thương Việt Nam (Vietcombank) |
| 27 | VIB | Ngân hàng TMCP Quốc tế (VIB) |

## **Nguồn dữ liệu**

* Nhà cung cấp: 3
  + Fireant: <https://fireant.vn/dashboard>
  + Vietstock: <https://vietstock.vn/>
  + Cafef: <https://cafef.vn/>

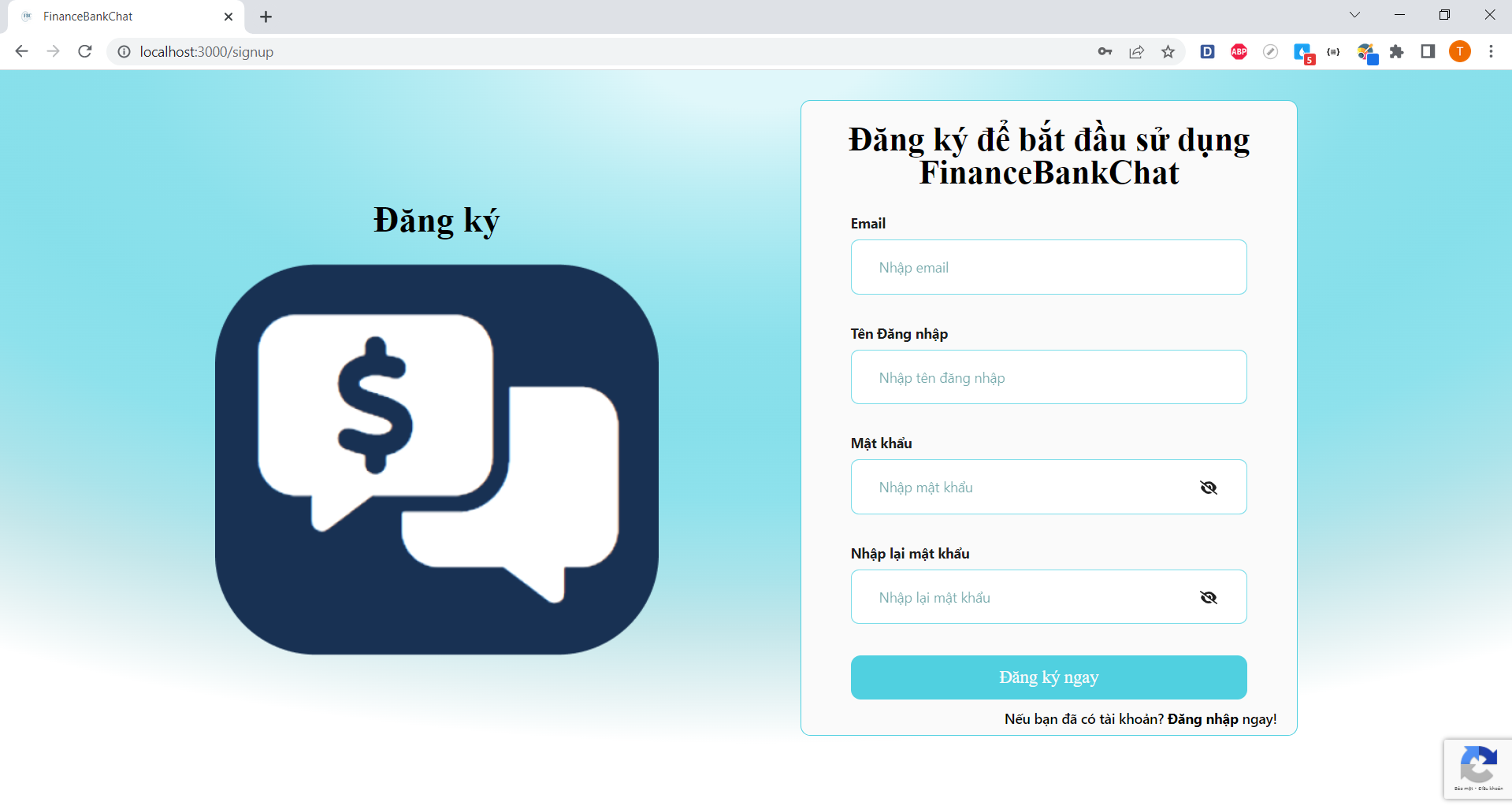
## **Thông tin dữ liệu thu thập**

* + Thông tin tài sản:
    - Tiền mặt, vàng bạc
    - Tiền gửi tại ngân hàng nhà nước
    - Cho vay các tổ chức tín dụng
    - Cho vay khách hàng
    - Tổng tài sản
  + Thông tin nợ:
    - Nợ xấu
    - Dư nợ
  + Thông tin thu nhập:
    - Lãi thuần
    - Lợi nhuận thuế
    - Lợi nhuận từ hoạt động dịch vụ
    - Lợi nhuận từ hoạt động khác
    - Lợi nhuận sau thuế

# **Màn hình giao diện**

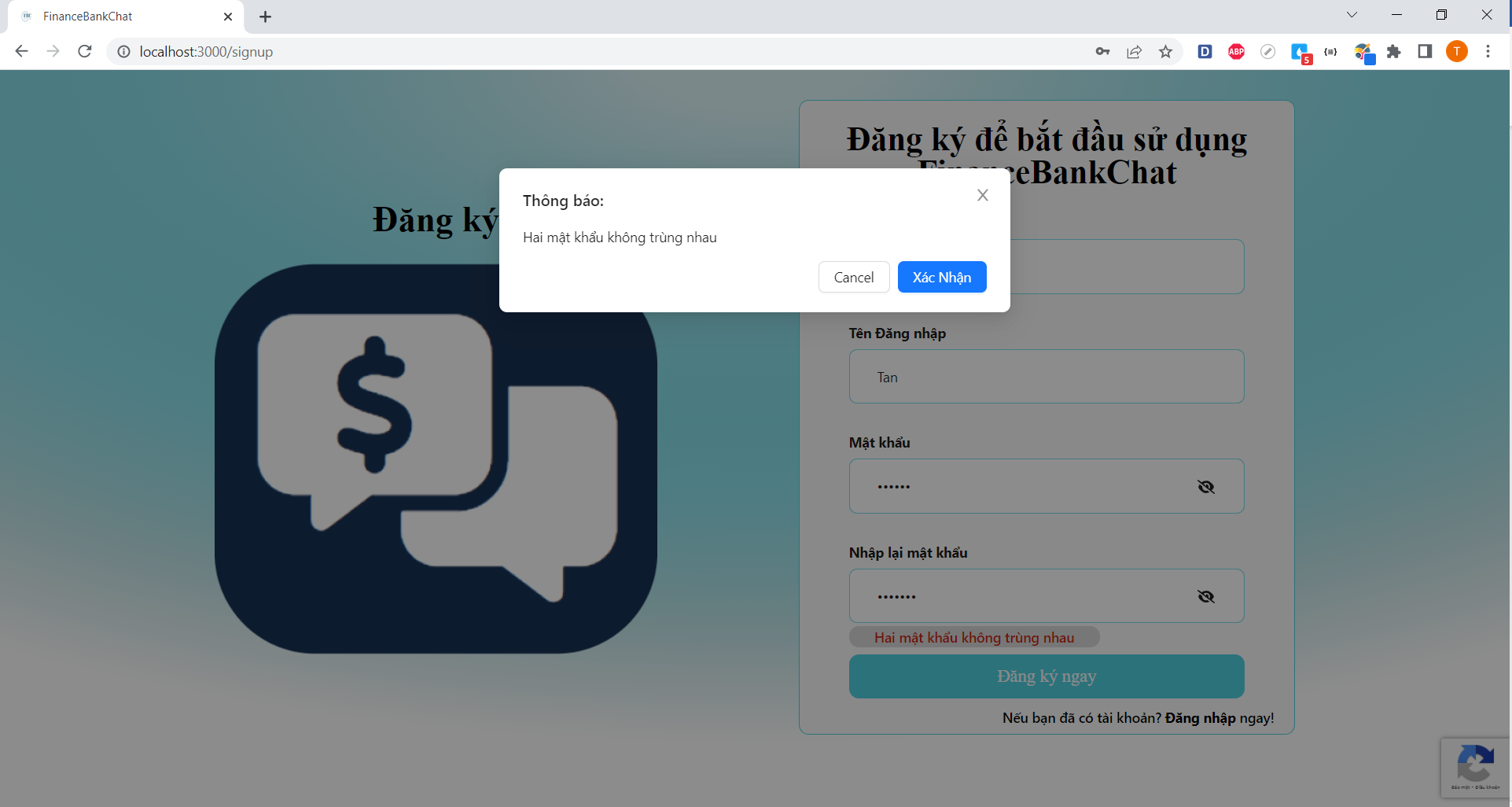
## **Đăng ký**

### **Đăng ký**



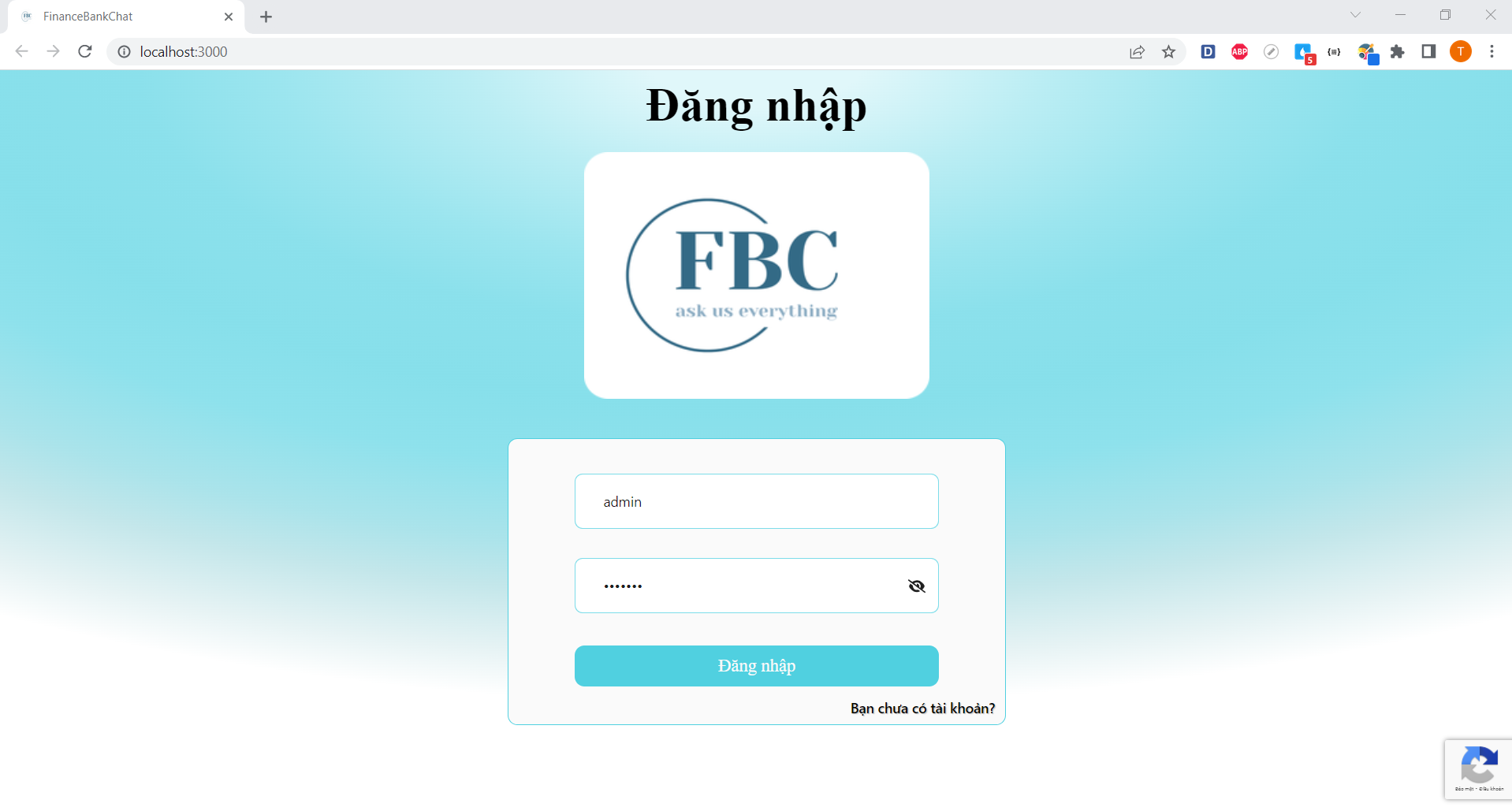
### **Đăng ký lỗi**

* Lỗi gmail
* Lỗi user tồn tại
* Lỗi 2 mật khẩu không trùng khớp với nhau

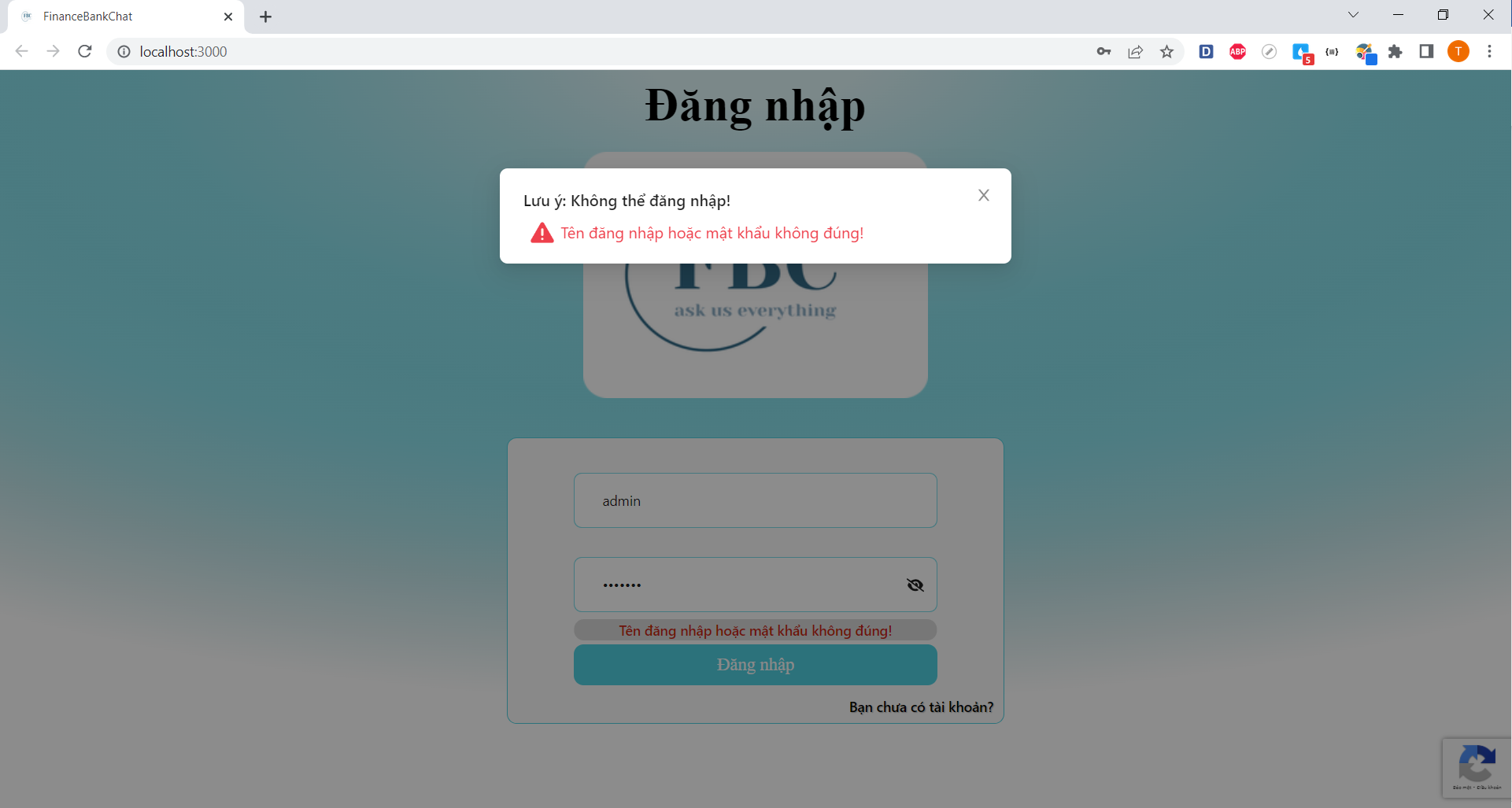


## **Đăng nhập**

Sau khi đăng ký thành công sẽ chuyển đến màn hình đăng nhập



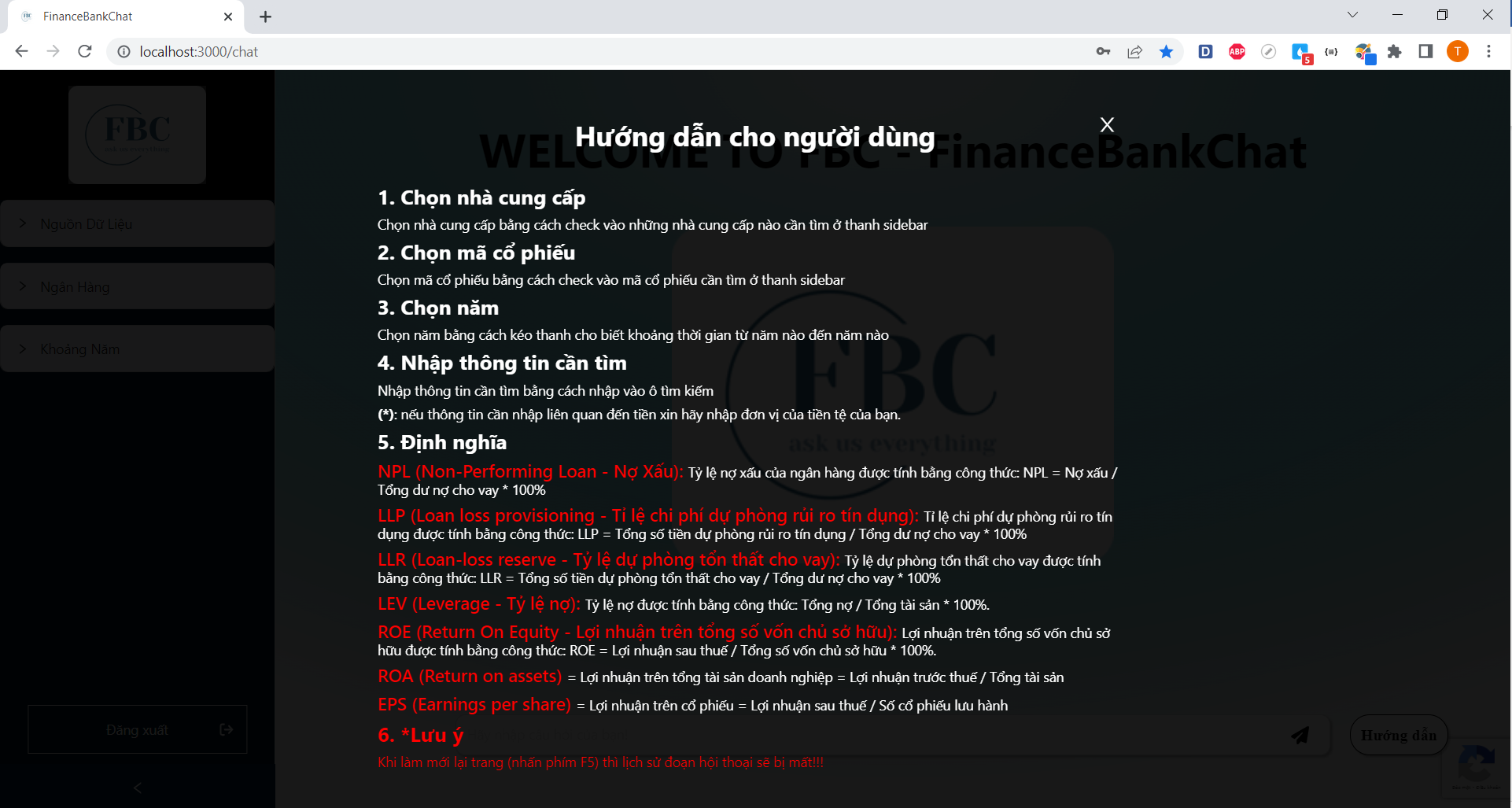
Đăng nhập lỗi



## **Chat**

Sau khi đăng nhập thành công sẽ chuyển vào giao diện chat

### **Mục hướng dẫn**



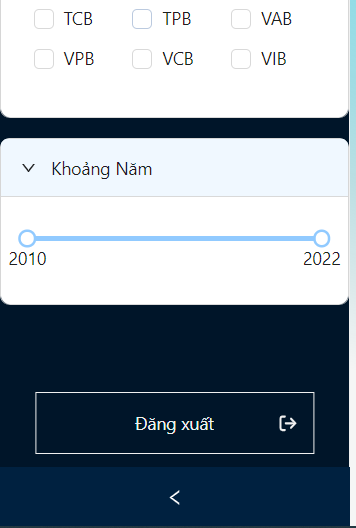
### **Giao diện chat**

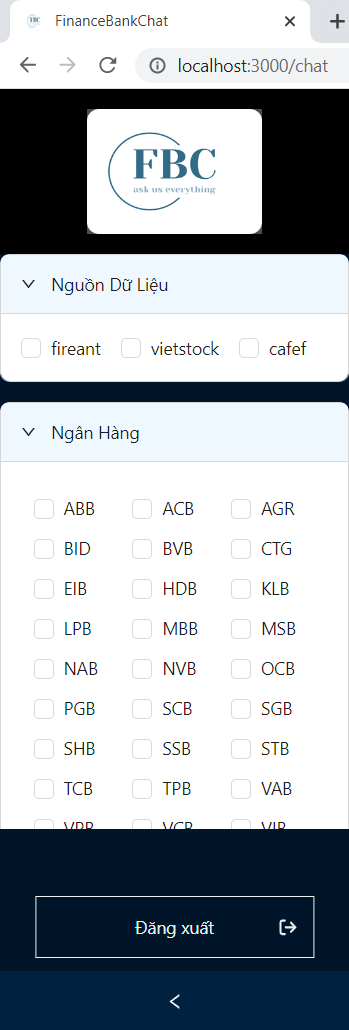




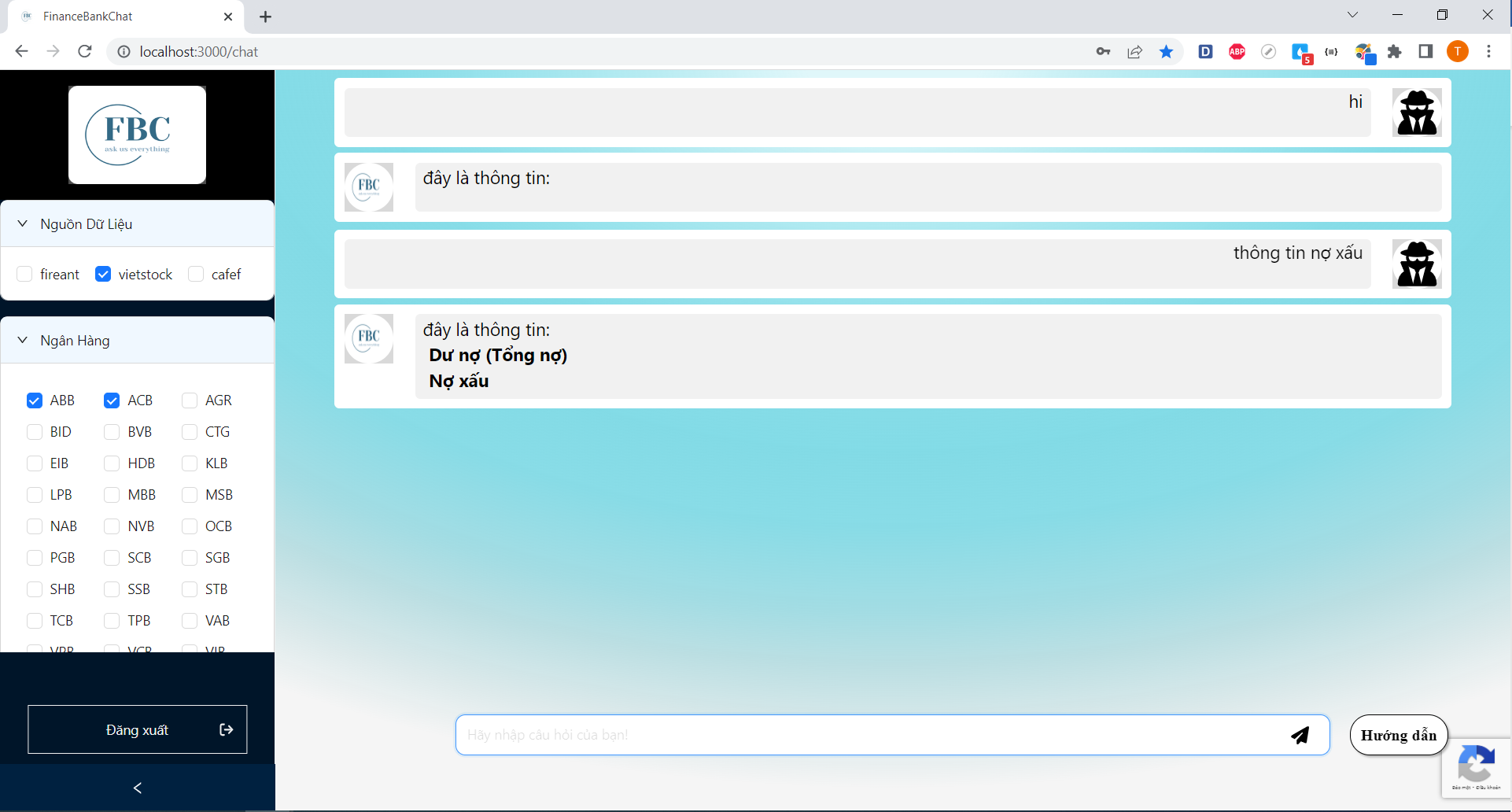
### **Template**

* Nguồn dữ liệu
* Ngân hàng
* Khoảng năm

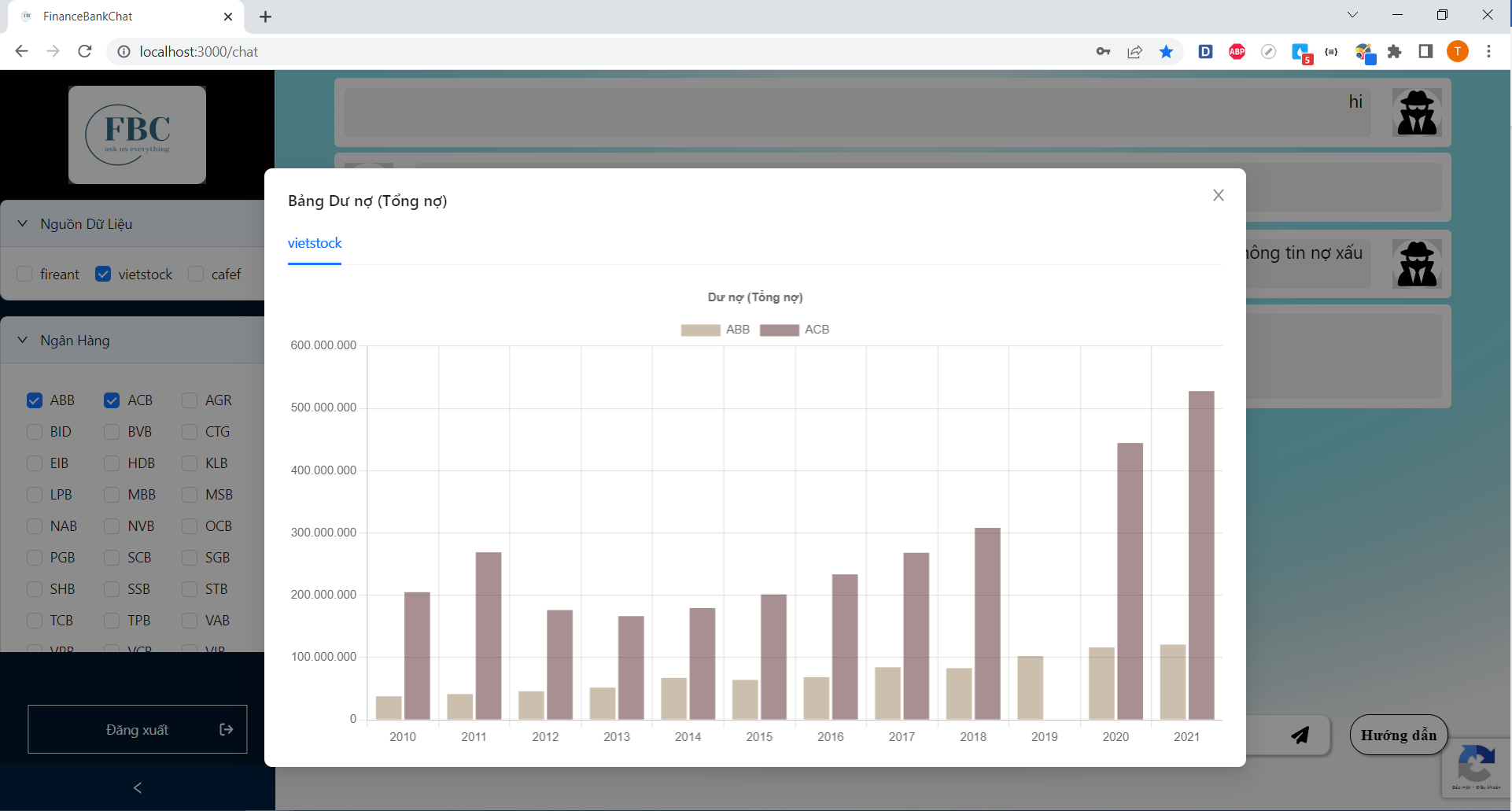




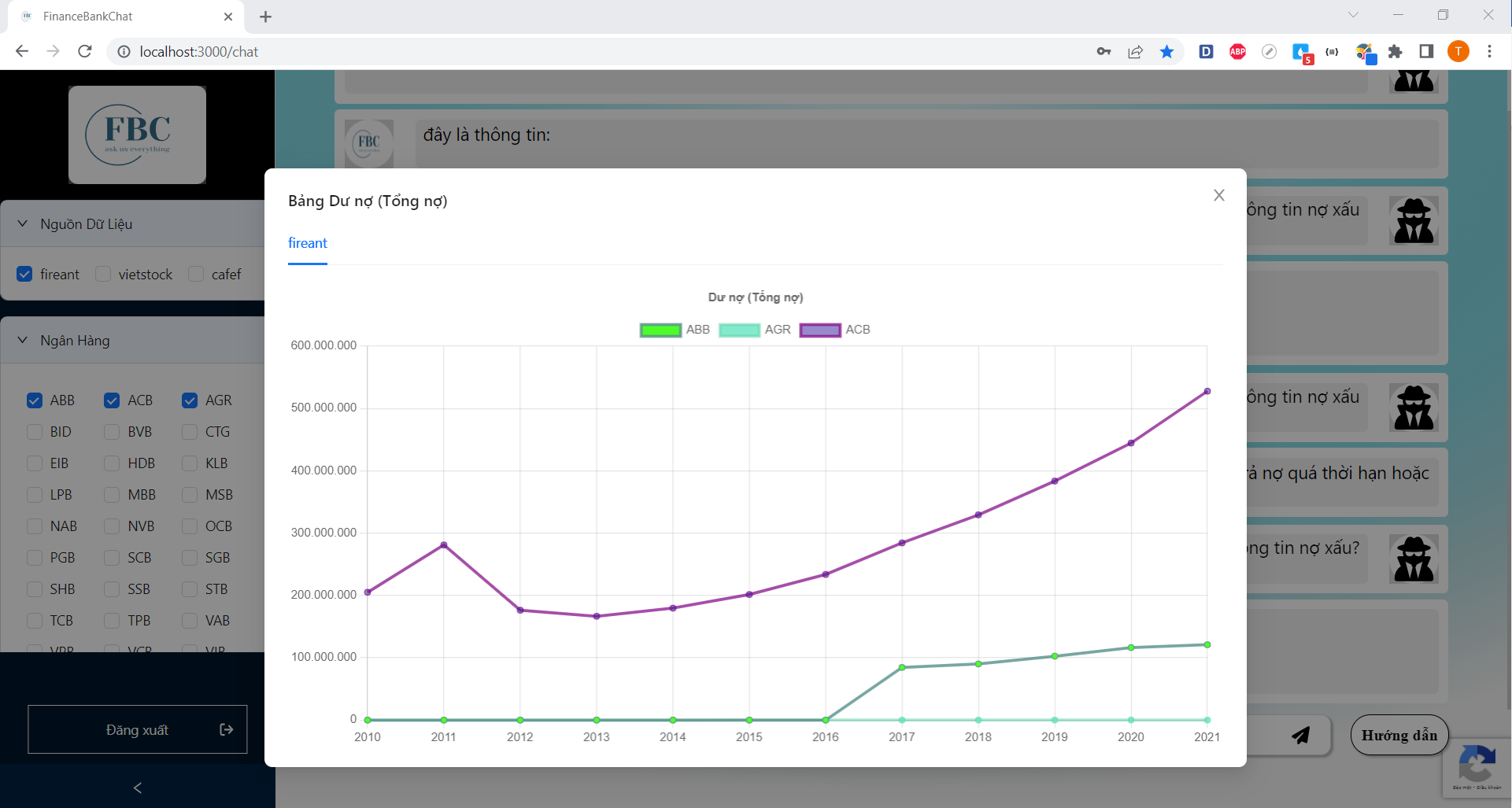
### **Màn hình chat**



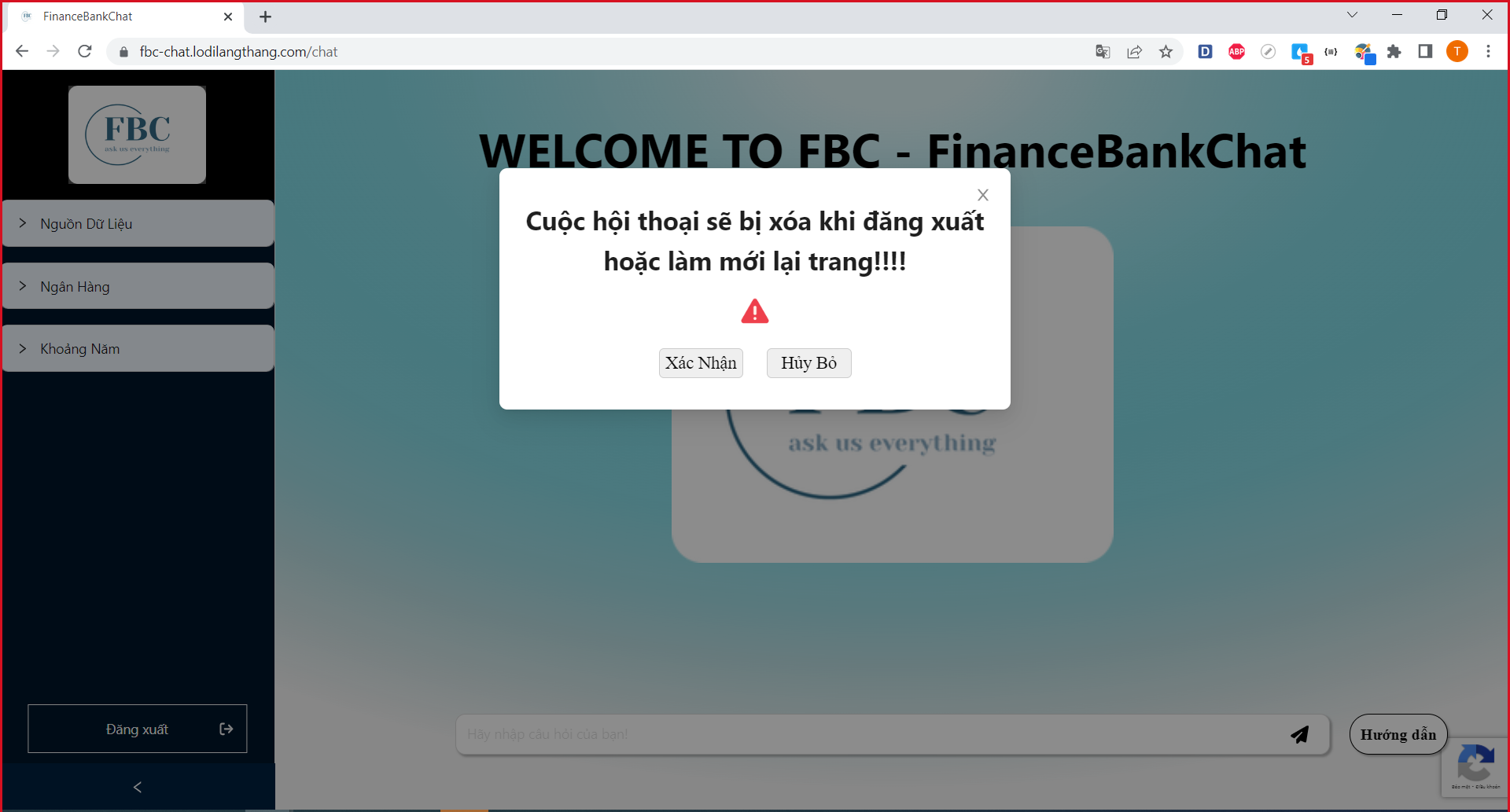
Click vào **Dư Nợ(Tổng nợ)** sẽ hiện biểu đồ



Khi số lượng ngân hàng được chọn 3 thì sẽ vẽ biểu đồ đường



### **Đăng xuất tài khoản**



# **Mô hình hoạt động**

## **Luồng hoạt động**

* Nhúng cấu trúc diagram database vào chatGPT
* Nhận API requests từ User (yêu cầu đăng nhập) -> Xử lý bảo mật thông tin
* Gọi API requets đến OPENAI để xử lý yêu cầu tạo các câu sql hoặc câu trả lời
* Nhận sql và truy vấn đến database
* Xử lý dữ liệu và gửi kết quả đến Client

## **Đặc tả yêu cầu**

### **Hoạt động tương tác**

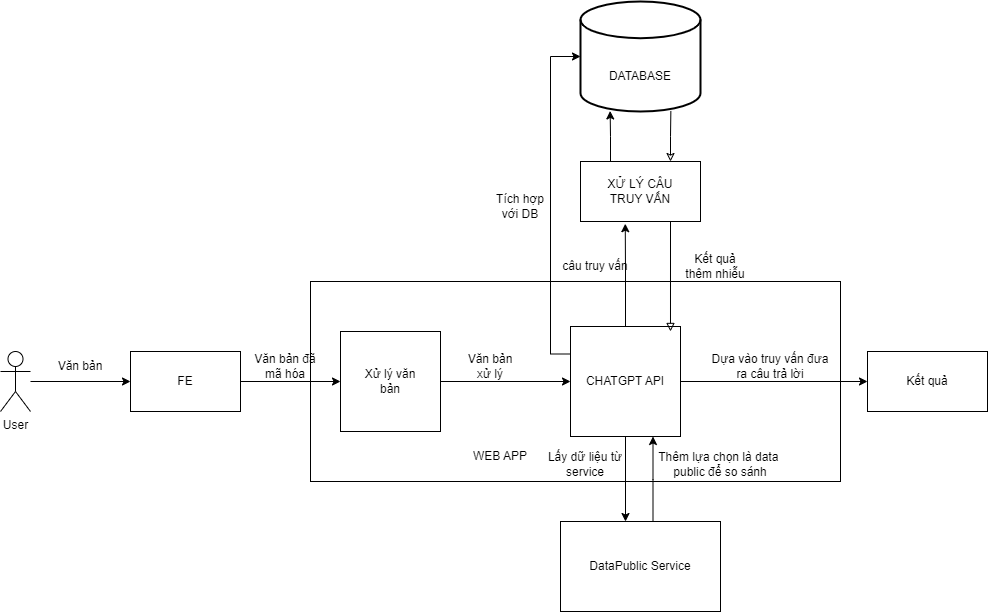
Dựa vào luồng hoạt động trên, Ứng dụng sẽ được thiết kế tập trung chủ yếu để cho người dùng hỏi về những câu hỏi về Tài chính của Ngân hàng hoặc nhiều ngân hàng gồm các đối tượng với chức năng sau:

|  |  |
| --- | --- |
| Đối tượng | Hoạt động |
| Người dùng | * Đăng nhập và đăng ký * Hỏi và tương tác trực tiếp những câu hỏi liên quan đến tài chính ngân hàng ở Việt Nam bằng ngôn ngữ tự nhiên * Đăng xuất sẽ xoá hết những câu hỏi đã hỏi |
| Mã ngân hàng | * Được lấy thông tin về báo cáo tài chính từ các trang web uy tín: fireant, vietstock, cafef * Lấy là lưu data vào database * Lấy lại toàn bộ dữ liệu tự động từ các trang web nhưng chỉ khi admin thực hiện điều này |
| ChatGPT/OpenAI | * Tích hợp database * Nhận câu hỏi theo template và trả lời * Model thực hiện: text-davinci-003 |

### **Hoạt động bảo mật**

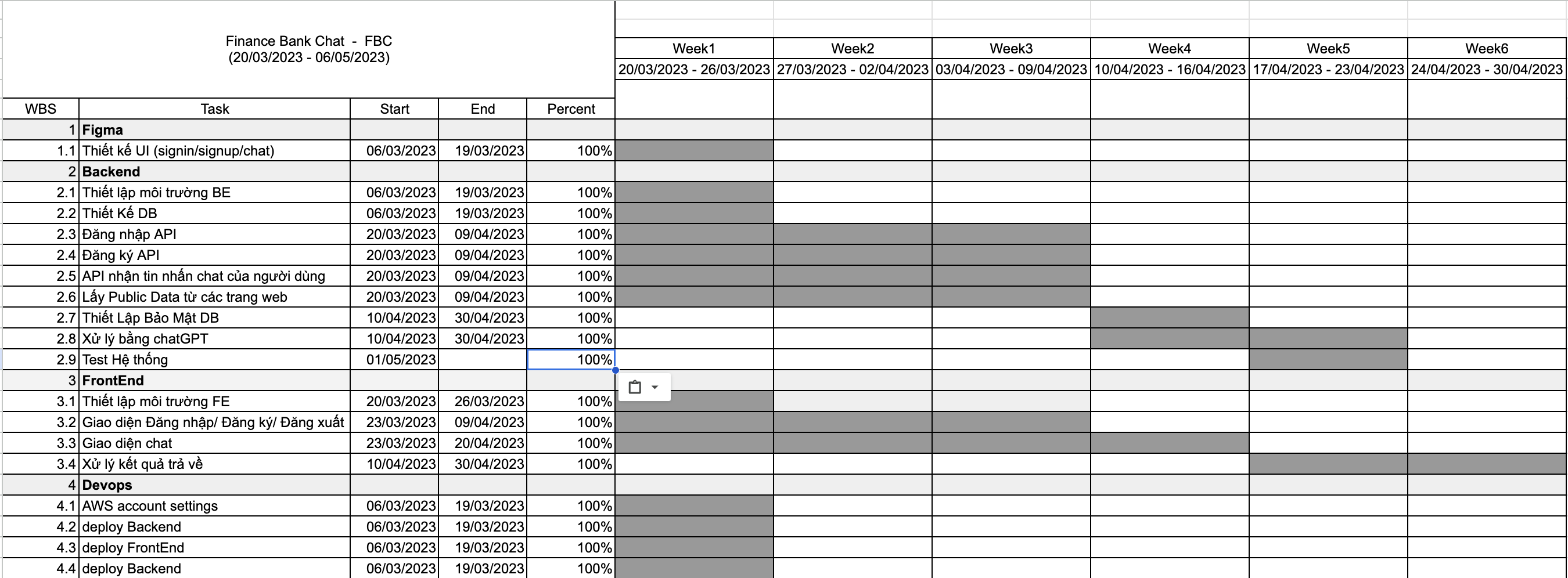
* Đăng nhập
* Mã hoá tên đăng nhập, mật khẩu
* Xác người robot – google captcha
* Xác thực và định danh người dùng
* Đăng ký:
* Mã hoá tên đăng nhập, mật khẩu, email
* Tương tác câu hỏi
* Mã hoá câu hỏi
* Mã hoá các thông tin cấu hình
* Làm nhiễu câu hỏi có số tiền cụ thể
* Bảo vệ database
* Làm nhiễu thông tin trả về
* Gọi API requests
* Giới hạn số lần gọi – limit throllte
* Xác thực người dùng thông qua json web token (JWT)
* Đình danh domain – CORS headers
* Sử dụng giao thức HTTPS

### **Tổng quan mô hình hoạt động**



# **Kế hoạch thực hiện**

## **Kế hoạch**



## **Phân Công**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Tính năng | Công việc | Thời gian | Phân công |
| 1 | Thiết kế UI | Thiết kế giao diện cho các màn hình : login, logout, sign up, chat | 6/3/2023-19/3/2023 | Tân |
| 2 | Deploy server và DB | Deploy DB và Server BE, FE | Phong |
| 3 | Thiết lập môi trường BE | Thiết lập source code BE và kết nối DB | Tài |
| 4 | Thiết lập môi trường FE | Thiết lập source code FE | Tân |
| 5 | Thiết Kế DB | Thiết kế DB của hệ thống | Tài |
| 6 | Đăng nhập | FE : code giao diện | 20/3/2023-9/4/2023 | Tân |
| 7 | BE : code API | Tài |
| 8 | Đăng ký | FE : code giao diện | Tân |
| 9 | BE : code API | Tài |
| 10 | API nhận tin nhấn chat của người dùng | Mã hóa luồng và giải mã luồng | Phong |
| 11 | Filter câu hỏi mang tính riêng tư | Phong |
| 12 | Làm nhiễu thông tin câu hỏi | Phong |
| 13 | Lấy Public Data từ các trang web | Nghiên cứu | Tài |
| 14 | viết các Data lấy thông tin thích hợp | Tài |
| 15 | Thiết Lập Bảo Mật | Viết Service DP cho Database dùng nhiễu laplace | 10/4/2023-1/5/2023 | Phong |
| 16 | Thiết lập bảo mật hệ thống | Tài |
| 17 | Xử lý bằng chatGPT | Tích hợp ChatGPT với Database | Phong |
| 18 | Dùng ChatGPT để chuyển văn bản thành câu truy vấn | Phong |
| 19 | Dùng ChatGPT để chuyển kết quả thành câu trả lời cho người dùng | Tài |
| 20 | Dùng ChatGPT trả lời kết quả dựa trên public Data | Tài |
| 21 | Dựa theo kết quả trả về hiển thị biểu đồ cho người dùng | Tân |
| 22 | Kiểm thử hệ thống | Kiểm thử giao diện | 2/5/2023- 15/05/2023 | Phong |
| 23 | Sửa các lỗi giao diện | Tân |
| 24 | Kiểm thử luồng hệ thống | Tân |
| 25 | Sửa các lỗi luồng hệ thống | Tài |
| 26 | Fix bug bảo mật hệ thống | Phong |