**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐÔNG Á**

**……\*\*\*.…..**



**BÁO CÁO CUỐI MÔN**

**MÔN: ĐỒ ÁN CHUYÊN NGÀNH BLOCKCHAIN**

GVHD : TS. Đỗ Sính

Lớp : ST19A1B

Thành viên : Đỗ Thiên Giang

Hoàng Đình Tuấn

Lê Quang Mẫn

*Đà Nẵng, 2023*

# LỜI CẢM ƠN

Lời đầu tiên em xin chân thành cảm ơn thầy Đỗ Sính đã tạo điều kiện thuận lợi cho em trong quá trình, thời gian thực hiện bài báo cáo.Thầy đã trực tiếp hướng dẫn, chỉ bảo, giúp em khắc phục những khó khăn, thiếu sót để có thể hoàn thành các phần trong đồ án.

Mặc dù đã cố gắng với tất cả nỗ lực của bản thân để hoàn thiện bài báo cáo, nhưng năng lực và kinh nghiệm còn hạn chế nên đồ án không thể tránh khỏi những thiếu sót. Kính mong nhận được sự đóng góp ý kiến từ phía Thầy để em có thể nâng cao kiến thức của bản thân, hoàn thiện đồ án được tốt hơn.

Em xin chân thành cảm ơn!

MỤC LỤC

[LỜI CẢM ƠN 2](#_Toc128214070)

[TỔNG QUAN ĐỀ TÀI 5](#_Toc128214071)

[I. Bối cảnh và lý do thực hiện đề tài 5](#_Toc128214072)

[II. Mục tiêu đề tài 5](#_Toc128214073)

[III. Đối tượng nghiên cứu 5](#_Toc128214074)

[IV. Phương pháp triển khai đề tài 5](#_Toc128214075)

[V. Nội dung của báo cáo 5](#_Toc128214076)

[VI. Dự kiến kết quả 6](#_Toc128214077)

[LÝ THUYẾT 7](#_Toc128214078)

[I. Truffle 7](#_Toc128214079)

[II. Smart Contract Develepment 7](#_Toc128214080)

[III. ERC20 7](#_Toc128214081)

[1. Khái niệm 7](#_Toc128214082)

[2. Ưu và nhược điểm 8](#_Toc128214083)

[3. Các chức năng 8](#_Toc128214084)

[4. Những loại hình Token ERC20: 8](#_Toc128214085)

[I. KYC & Token 9](#_Toc128214086)

[1. KYC là gì 9](#_Toc128214087)

[2. Tầm quan trọng của KYC? 9](#_Toc128214088)

[3. Tại sao KYC ngày càng quan trọng trong Crypto? 9](#_Toc128214089)

[IV. GIẢI THÍCH CODE 10](#_Toc128214090)

[1. Khởi tạo dự án 10](#_Toc128214091)

[2. MyToken.sol 10](#_Toc128214092)

[3. MyTokenSale.sol 11](#_Toc128214093)

[4. KycContract.sol 11](#_Toc128214094)

[5. Crowdsale.sol 12](#_Toc128214095)

[6. 2\_deploy\_my\_token.js 13](#_Toc128214096)

[7. MyToken.test.js 13](#_Toc128214097)

[8. MyTokenSale.test.js 14](#_Toc128214098)

[KẾT LUẬN 16](#_Toc128214099)

[I. Kết quả đạt được 16](#_Toc128214100)

[II. Hạn Chế 16](#_Toc128214101)

[III. Hướng Phát triển 16](#_Toc128214102)

[TÀI LIỆU THAM KHẢO 16](#_Toc128214103)

# TỔNG QUAN ĐỀ TÀI

## Bối cảnh và lý do thực hiện đề tài

Trong thực tế, Internet đã trở thành trình điều khiển của nền kinh tế. Sự xuất hiện của Internet và các mạng cục bộ đã giúp cho việc trao đổi thông tin trở nên nhanh chóng, dễ dàng hơn. Email cho phép chúng ta nhận hay gửi thư ngay trên máy tính của mình, E-business cho phép thực hiện giao dịch, buôn bán trên mạng,… Cũng giống như Internet, blockchain xuất phát như một trào lưu với đồng tiền ảo Bitcoin.Từ những rủi ro từ an ninh mạng nên các tổ chức tài chính cần những công nghệ mới, ví dụ như nền tảng của đồng tiền số Bitcoin, chính là Blockchain, được kì vọng không chỉ nhằm cắt giảm chi phí ngân hàng mà còn đảm bảo tính an toàn và xa hơn nữa thậm chí cách mạng hóa các giải pháp bảo mật.Nên em chọn đề tài này để tìm hiểu rõ hơn về BlockChain để cung cấp một cách nhìn tổng quan về công nghệ Blockchain..

## Mục tiêu đề tài

Đề tài nhằm tìm hiểu được cách về cách hoạt động của Token trong blockchain và khi giao dịch thì ta bán lun Token đó.

## Đối tượng nghiên cứu

* Ngôn ngữ lập trình JavaScript
* Công cụ hỗ trợ Ganache, Truffle
* Công việc tạo ra Token
* Kiểm tra và đưa vào sử dụng

## Phương pháp triển khai đề tài

* + Tìm hiểu BlockChain
  + Thiết kế và xây dựng Token trong BlockChain

## Nội dung của báo cáo

* Cơ sở lý thuyết
* Giải thích code

## Dự kiến kết quả

* Hiểu được quy trình tạo ra Token
* Biết và hiểu về Token trong BlockChain
* Tạo ra Token, kiểm tra và đưa vào sử dụng

# LÝ THUYẾT

## Truffle

1. **Truffle trong blockchain là gì ?**

* Truffle là một framework của lập trình Ethereum, cho phép tạo test environment, viết test cho contract và nhiều thứ khác nữa.

1. **Ethereum là gì?**

* Ethereum (ETH) là một loại cryptocurrency được xây dựng vào năm 2013 bởi Vitalik Buterin, thường được gọi là Bitcoin 2.0. Đây không chỉ là một đồng tiền tệ mà nó còn là nền tảng tạo ra nhiều ứng dụng khác thông qua ngôn ngữ lập trình của mình.
* Nó hoạt động trên một Blockchain tương tự như Bitcoin, chúng ta có thể khai thác ETH thông qua đơn vị tiền tệ Ether.
* Ethereum còn là một nền tảng ứng dụng hữu ích và đã tạo ra được một hệ sinh thái tài chính phân tán cho riêng mình.

## Smart Contract Develepment

1. **Smart Contract Development là gì**

* Smart Contract là một chương trình máy tính hoặc một giao thức giao dịch nhằm mục đích tự động thực hiện, kiểm soát hoặc ghi lại các sự kiện và hành động có liên quan về mặt pháp lý theo các điều khoản của hợp đồng hoặc thỏa thuận. Các mục tiêu của hợp đồng thông minh là giảm nhu cầu về các trung gian đáng tin cậy, trọng tài và chi phí thực thi, tổn thất do gian lận, cũng như giảm các ngoại lệ độc hại và ngẫu nhiên.

## ERC20

## Khái niệm

* ERC20 là chuẩn token Ethereum được sử dụng phổ biến nhất hiện nay. Có thể nói hầu như bất kỳ dự án ICO nào cũng được sử dụng token chuẩn ERC20.
* ERC-20 (Ethereum Request for Comments 20), được đề xuất bởi Fabian Vogelsteller vào tháng 11 năm 2015, là Tiêu chuẩn mã thông báo triển khai API cho mã thông báo trong Hợp đồng thông minh.

## Ưu và nhược điểm

1. *Ưu điểm*

* Tính Fungible: Các Token riêng lẻ có thể hoán đổi cho nhau, không làm hỏng đi mục đích sử dụng làm tiền tệ của chúng.
* Tính linh hoạt: Các ERC20 token có khả năng tùy biến cao và có thể được điều chỉnh cho phù hợp với nhiều ứng dụng khác nhau.
* Tính phổ biến: Sự phổ biến của ERC20 trong không gian Crypto là một lý do rất thuyết phục để sử dụng làm một tiêu chuẩn chung. Có sự hỗ trợ của các nhà phát triển và tài liệu nên rất phong phú.

1. *Nhược điểm*

* Khả năng mở rộng còn kém: Hiện tại, việc mở rộng quy mô của Ethereum đang diễn ra không tốt, việc cố gắng gửi một giao dịch vào thời gian cao điểm dễ dẫn đến phí cao và sự chậm trễ.
* Nguy cơ lừa đảo cao, dễ bị mạo danh: Token ERC20 được tạo ra rất đơn giản có nghĩa là bất kỳ ai cũng có thể làm điều đó, dù với mục đích tốt hay xấu nên điều này dễ khiến cho nhiều kẻ gian lợi dụng nhằm tạo ra các Token không có giá trị, mạo danh để lừa đảo nhiều nhà đầu tư khá

## Các chức năng

* Chuyển mã thông báo từ tài khoản này sang tài khoản khác
* Lấy số dư mã thông báo hiện tại của tài khoản
* Nhận tổng nguồn cung mã thông báo có sẵn trên mạng
* Phê duyệt liệu một lượng mã thông báo từ tài khoản có thể được sử dụng bởi tài khoản bên thứ ba hay không

## Những loại hình Token ERC20:

1. *Stablecoin:*

* Stablecoin là loại tiền mã hóa được thiết kế với mục đích giảm thiểu tối đa sự ảnh hưởng của sự biến động giá (volatility) bằng cách cố định vào một tài sản ổn định hơn như tiền thật (fiat money), hàng hoá (vàng, bạc…), hoặc có thể là một tiền mã hóa khác.

1. Token tiện ích

* Trong Token ERC20 thì Token tiện ích là phổ biến và được phát hành nhiều nhất, việc phát hành Token tương đối dễ dàng. Token tiện ích giống như chương trình ưu đãi mà bên phát triển dành cho khách hàng.

1. Token chứng khoán

* Token chứng khoán sẽ đại diện cho trái phiếu, phiếu các loại hình tài sản vật lý. Loại hình Token này gần tương tự như một loại cổ phần trong doanh nghiệp hoặc đối với một loại hình tài sản nào đó.

## KYC & Token

## KYC là gì

* KYC (Know Your Customer) là quy trình xác minh danh tính mà các nhà cung cấp dịch vụ tài chính phải thực hiện để biết khách hàng của họ. Điều này là một phần của nỗ lực Chống Rửa tiền / Chống Tài trợ cho Khủng bố (AML / CFT) và tội phạm tài chính, cũng như nâng cao khả năng thẩm định của khách hàng.

## Tầm quan trọng của KYC?

* KYC làm giảm nguy cơ hoạt động của tội phạm tài chính
* KYC giúp xây dựng niềm tin với khách hàng
* KYC giúp ổn định thị trường tiền điện tử
* KYC đảm bảo các sàn giao dịch tuân thủ quy định pháp luật

## Tại sao KYC ngày càng quan trọng trong Crypto?

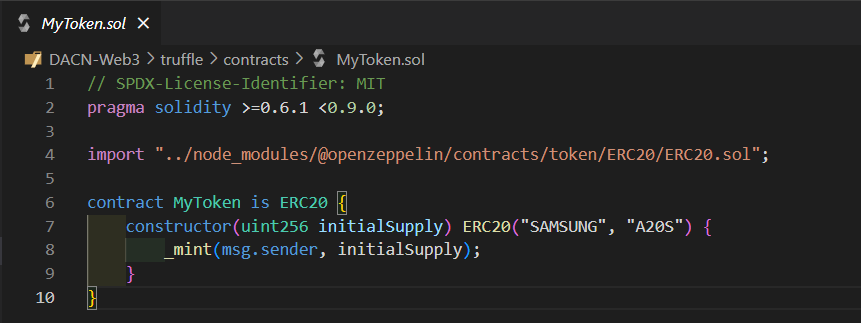
* Giao dịch ctypto được tiếp sức từ nhu cầu công chúng và các sàn giao dịch đưa ra các dịch vụ. Một số sàn giao dịch được đặt ở thiên đường thuế và các địa điểm nước ngoài, giúp họ thoải mái tiến hành các giao dịch mà không bị các quy định hạn chế.
* Việc thiếu sự tuân thủ quy định trên khắp thế giới cho phép các cá nhân bỏ qua quy định AML và tham gia rửa tiền điện tử. Theo Arachnys, một công ty AML RightSource, xấp xỉ $3.8 tỉ được rửa thông qua Bitcoin và giao dịch crypto năm 2019. Hình mẫu này đang tăng trưởng và có khả năng tăng hơn nữa nếu các quy định như KYC crypto không được đặt đúng chổ.
* Theo đó, KYC ngày càng trở nên quan trọng vì nó tạo ra cơ hội nhận diện tội phạm. Đây là lý do tai sao KYC xuất hiện trên bản tin .

## GIẢI THÍCH CODE

## Khởi tạo dự án

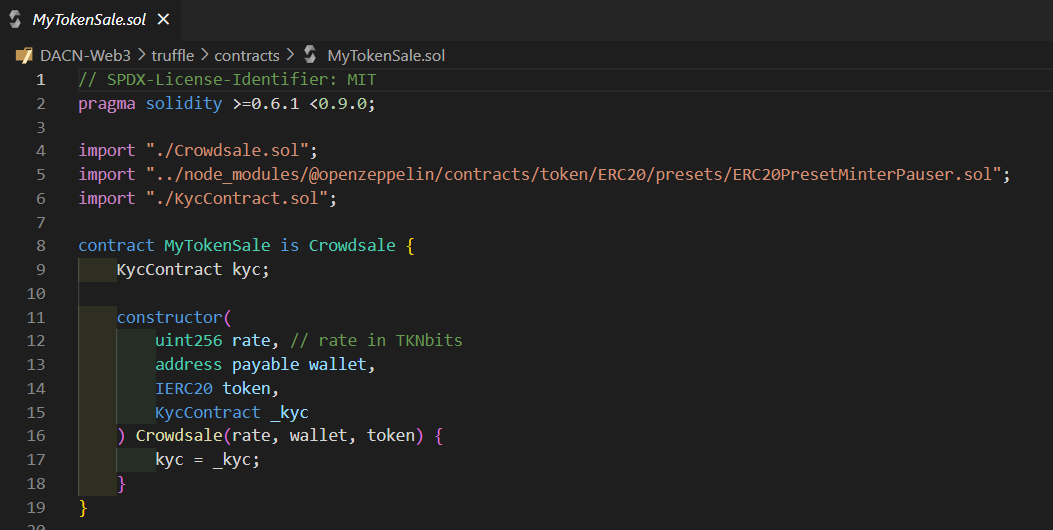
* Tạo folder dự án : *mkdir ten\_folder*
* Tạo cấu trúc dự án : *truffle unbox react*
* Cài thư viện contract : *npm install @openzeppelin/contracts*
* Cài thư viện chai : *npm install chai chai-bn chai-as-promised*
* Cài thư viện dotenv : *npm install --save dotenv*
* Kiểm tra : *truffle test*

## MyToken.sol

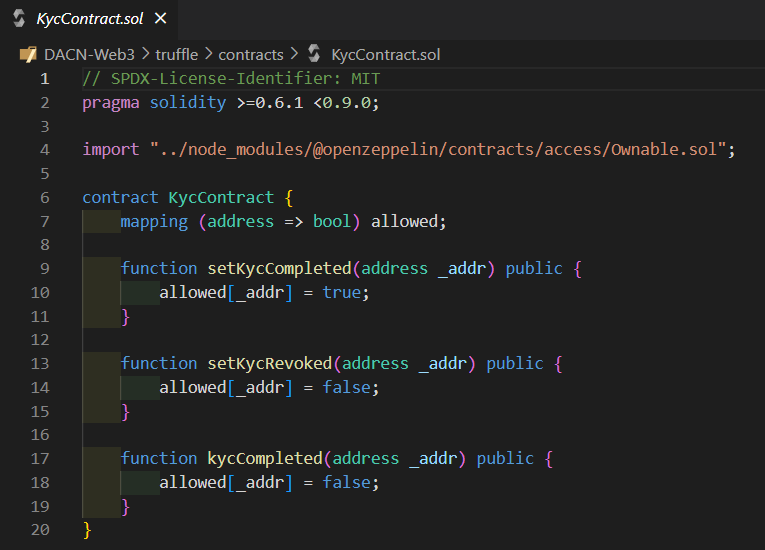


* Import ERC20
* Viết các câu lệnh như hình nhằm mục đích tạo ra 1 Token cho dự á
* Hợp đồng ERC20 mới có một hàm tạo với các đối số cho tên và biểu tượng của mã thông báo. Nó có tên "SamSung", ký hiệu là "A20S".

## MyTokenSale.sol

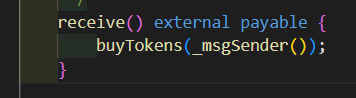


## KycContract.sol

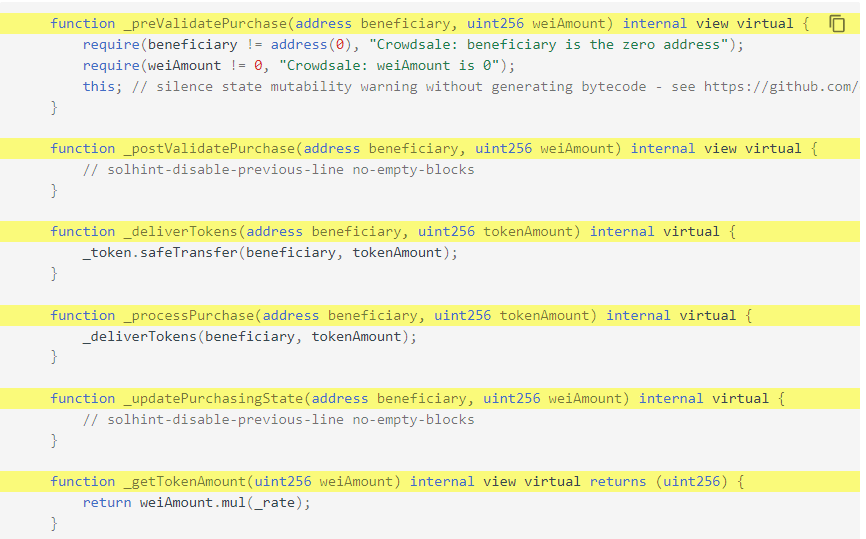


## Crowdsale.sol

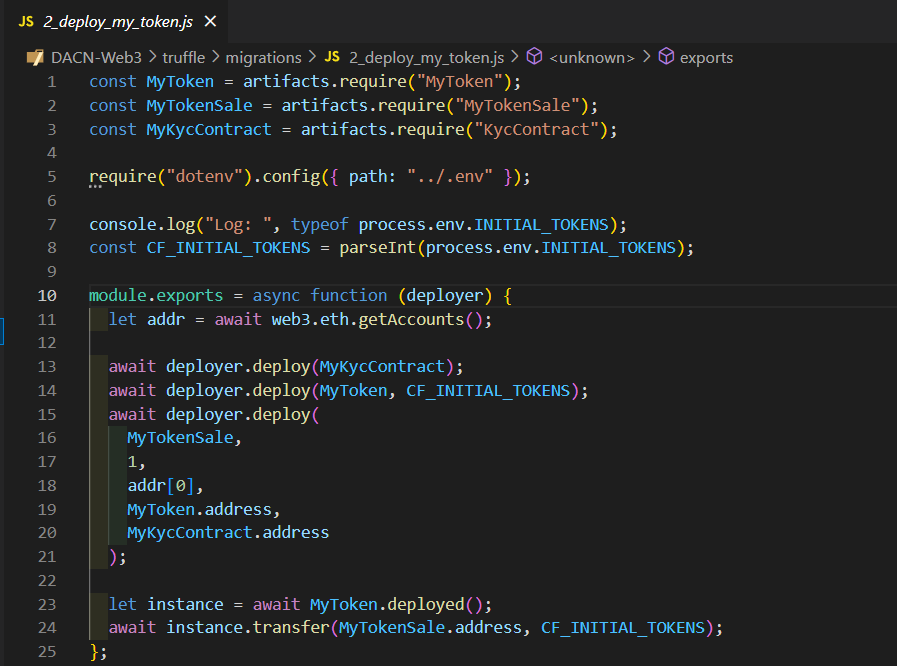
* Sao chép hợp đồng thông minh ra khỏi kho lưu trữ khác thay vì chỉ sử dụng nó, thì chúng tôi phải điều chỉnh các câu lệnh nhập
* Thay thế chức năng "fallback()" bằng chức năng này:



* Nếu bạn muốn ghi đè các chức năng trong Solidity 0.6 thì hợp đồng thông minh cơ sở phải xác định tất cả các chức năng là ảo để được ghi đè. Trong Crowdsale, chúng ta phải thêm từ khóa ảo vào các chức năng có khả năng bị ghi đè:

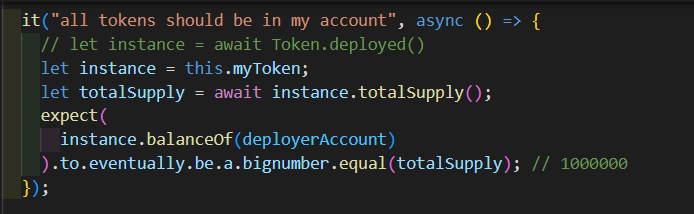


## 2\_deploy\_my\_token.js

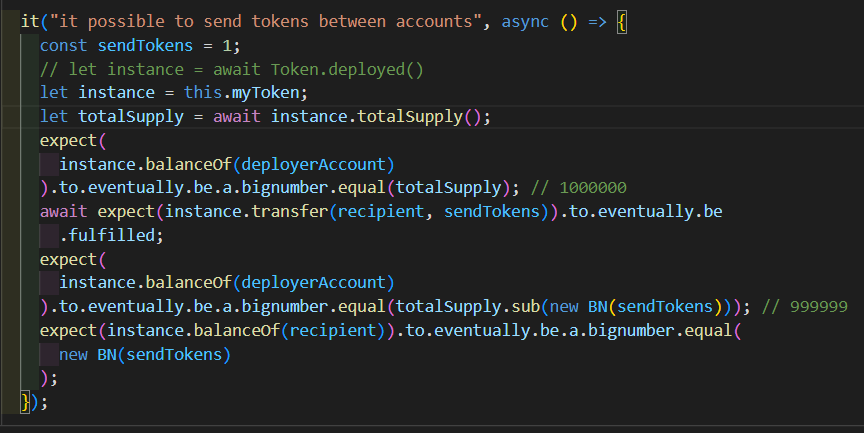


## MyToken.test.js

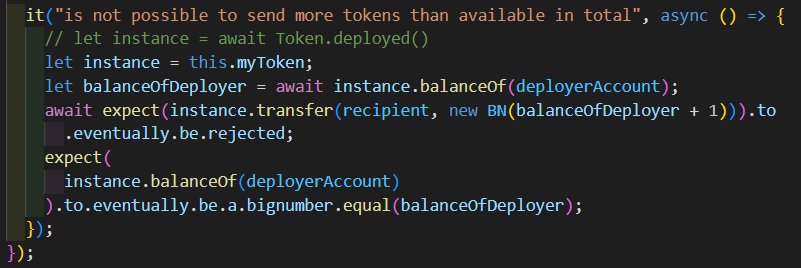
* Tất cả các mã thông báo phải có trong tài khoản của tôi
* Sau khi deloy thì nó sẽ trả về 1 mytoken và totalsupply trong dữ liệu để tôi có thể quản lý.



* Mục đính của đoạn code dưới là khi bán 1 sản phẩm cho người mua thì cũng đồng nghĩa ta bán lun mã Token đó lun để tránh trường hợp bị lợi dụng.

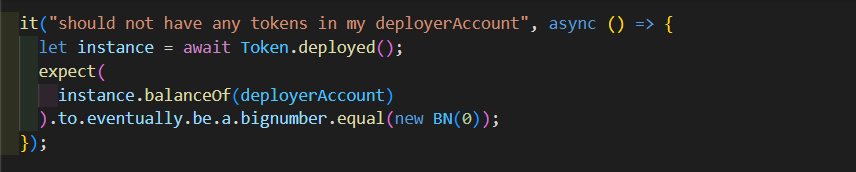


* Đoạn code dưới mô tả mỗi sản phẩm chỉ có 1 Token nhất định.

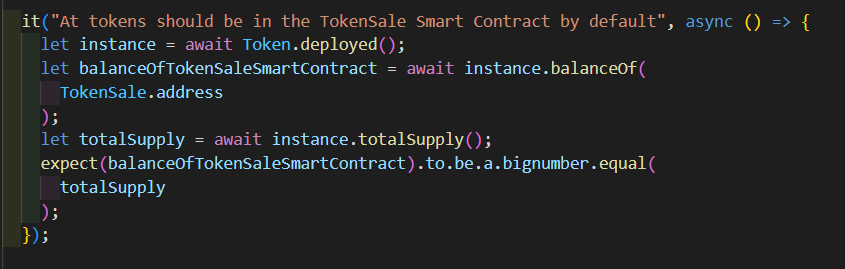


## MyTokenSale.test.js

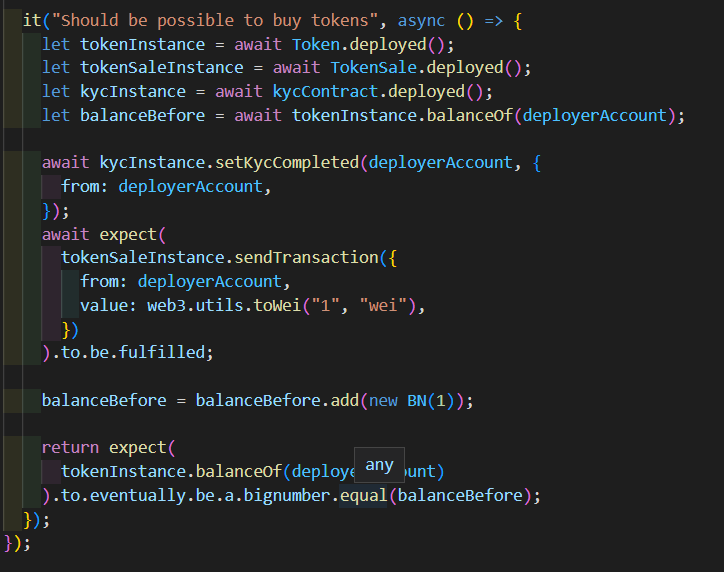
* Khi đã bán thì trong tài khoản người triển khai sẽ không còn lưu lại token đó mà Token sẽ lưu vào Contract trừ trường hợp bên mua không mua muốn mua nữa thì bên mình sẽ trả lại tiền.



* Tại các mã thông báo phải có trong Hợp đồng thông minh bán mã thông báo theo mặc định.



* Đoạn code dưới là chúng ta test mã Token có thể bán đi lun cùng với sản phẩm



# KẾT LUẬN

## Kết quả đạt được

* Hiểu và demo được quy trình tạo và bán mã Token trong BlockChain
* Biết và hiểu được ERC20 và KYC

## Hạn Chế

* Với những điều đã nghiên cứu và tìm hiểu về Token, KYC, ERC20 mặc dù đã hoàn thành, nhưng nó vẫn còn rất nhiều mặt hạn chế chương trình còn đơn giản, chưa đáp ứng được nhu cầu thiết thực và một số nội dung cần phải phân tích kỹ hơn, sâu hơn và tỉ mỉ hơn.
* Và trong thời gian tới thì em sẽ cố gắng khắc phục các hạn chế, những vân đề chưa được tốt, và bổ sung thêm những chức năng mới.

## Hướng Phát triển

* Bổ sung nhiều hơn các báo cáo, thống kê.
* Hoàn thành các chức năng và có thể bán mã Token cùng với sản phẩm

# TÀI LIỆU THAM KHẢO

Link Source Code :

* <https://github.com/DoThienGiang/DACN-ERC20TokenContract>

Link tham khảo:

* <https://docs.openzeppelin.com/contracts/4.x/erc20>
* <https://ethereum-blockchain-developer.com/2022-05-erc20-token/00-overview/>