

**TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ MÔN BLOCK CHAIN VÀ CÔNG NGHỆ
SỔ CÁI PHÂN TÁN**

ĐỀ TÀI : BLOCKCHAIN - SOLIDITY

Người hướng dẫn: **GV Phạm Thái Kỳ Trung**

Người thực hiện: **PREANN MESA– 52000909**

Lớp : 20050201

Khoá : 24

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023

**TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ MÔN BLOCK CHAIN VÀ CÔNG NGHỆ
SỔ CÁI PHÂN TÁN**

ĐỀ TÀI : BLOCKCHAIN - SOLIDITY

Người hướng dẫn: **GV Phạm Thái Kỳ Trung**

Người thực hiện: **PREANN MESA– 52000909**

Lớp : 20050201

Khoá : 24

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023

LỜI CẢM ƠN

Lời nói đầu tiên, em xin gửi lời cảm ơn chân thành nhất đến toàn bộ quý thầy cô Trường Đại học Tôn Đức Thắng, quý thầy cô Khoa Công nghệ thông tin đã dạy dỗ, và truyền đạt những kiến thức quý báu cũng như đã tạo mọi điều kiện thuận lợi nhất để em được tiếp cận và hoàn thành môn block chain và công nghệ sổ cái phân tán.

Với thời gian và trình độ còn hạn chế, bài báo cáo không thể tránh khỏi những thiếu sót. Kính mong quý thầy chỉ bảo và đóng góp ý kiến để bài báo cáo của em được hoàn thiện hơn. Đó sẽ là hành trang quý giá để em có thể hoàn thiện về kỹ năng và kiến thức liên quan đến những vấn đề sau này.

Lời cuối cùng, em xin kính chúc quý thầy thật nhiều sức khỏe, thành công, hạnh phúc, và luôn giữ mãi sự nhiệt huyết để có thể giúp thêm thật nhiều thế hệ sinh viên Trường Đại Học Tôn Đức Thắng có nhiều sự tự tin và vững kiến thức với môn block chain và công nghệ sổ cái phân tán. Ngọn lửa của môn học sẽ ngày càng được lan tỏa rộng rãi nhiều hơn!

ĐỒ ÁN ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Em xin cam đoan đây là sản phẩm báo cáo của riêng em và được sự hướng dẫn của GV Phạm Thái Kỳ Trung ;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình. Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày 17 tháng 01 năm 2023

Tác giả

(ký tên và ghi rõ họ tên)

Preann Mesa

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

Phần xác nhận của GV hướng dẫn

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

Phần đánh giá của GV chấm bài

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

TÓM TẮT

Bài làm gồm có 3 chương như sau:

- Chương 1 Tìm hiểu tổng quan về blockchain
- Chương 2 tìm hiểu về phiên bản của blockchain
- Chương 3 tìm hiểu về Smart contract và Solidity

MỤC LỤC

LỜI CẢM ƠN	i
PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN	iii
TÓM TẮT	iv
MỤC LỤC	1
DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ	4
CHƯƠNG 1 – TỔNG QUAN VỀ BLOCK CHAIN	5
1.1 Mục đích đề tài.....	5
1.2 Khái niệm về Blockchain.....	5
1.2 Các đặc tính của block chain	6
1.2.1 Cơ sở dữ liệu phân tán (phi tập trung).....	6
1.2.2 Tính bền vững và tăng cường bảo mật	6
1.2.3 Xác thực dữ liệu.....	7
1.2.4 Tính minh bạch.....	8
1.2.5 Tính bất biến.....	8
1.3 Nguyên lý hoạt động của blockchain.....	8
1.4 Ứng dụng thực tiễn của công nghệ Blockchain trong cuộc sống	9
CHƯƠNG 2 – PHIÊN BẢN BLOCKCHAIN.....	11
2.1 Blockchain 1.0 (Tiền tệ).....	11
2.1.1 Các hoạt động của blockchain 1.0	11
2.1.2 Đặc điểm của blockchain 1.0	12
2.2 Blockchain 2.0 (Smart contract)	13
2.2.1 Cách hoạt động của blockchain 2.0	13
2.2.2 Đặc điểm của blockchain 2.0	16
2.3 Blockchain 3.0 (Ứng dụng phi tập trung Dapp)	16
2.3.1 Cách đặc điểm của blockchain 3.0 (Dapp)	17
2.4 Blockchain 4.0 (Ứng dụng thực tiễn).....	18

2.4.1 Cách đặc điểm của blockchain 4.0.....	19
2.5 Các loại của blockchain	20
CHƯƠNG 3 – SMART CONTRACT & SOLIDITY	22
3.1 Khái niệm smart contract	22
3.2 Cách hoạt động của smart contract	22
3.3 Lợi ích của smart contract.....	24
3.4 Ưu điểm và nhược điểm của smart contract	24
3.4.1 Ưu điểm	24
3.4.1 Nhược điểm.....	25
3.5 Ứng dụng của hợp đồng thông minh trong thực tiễn	25
3.6 Solidity	26
3.6.1 Khái niệm Solidity	26
3.6.2 Contracts	26
3.6.3 Sử dụng Metamask triển khai Smart contract trong Solidity.....	27

DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

CÁC CHỮ VIẾT TẮT

Dapps Decentralized Applications

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

DANH MỤC HÌNH

Hình 1: Chuỗi khối.....	5
Hình 2: Mô hình sổ cái phân tán của block chain.....	6
Hình 3: Liên kết block.....	7
Hình 4: Thuật toán mã hóa blockchain	8
Hình 5: Bitcoins	11
Hình 6: Smart contract	13
Hình 7: Cách hoạt động của Smart contract	15
Hình 8: Phân biệt app và Dapp	17
Hình 9: Ứng dụng blockchain.....	19
Hình 10: Bảng so sánh private và public blockchain.....	21
Hình 11: Smart Contract	22
Hình 12: Cơ chế hoạt động của smart contract	23
Hình 13: Ứng dụng thực tế của hợp đồng thông minh	26
Hình 14: Code ví dụ về contract	27
Hình 15: MetaMask Extension.....	28
Hình 16: MetaMask wallet.....	28
Hình 17: Custom Network	29
Hình 18: Add a network manually	30
Hình 19: Tạo ví và kết nối network thành công.....	31
Hình 20: Tạo File HelloSolidity.sol	32
Hình 21: Sét Environment Deploy	33
Hình 22: Xác nhận đã triển khai	34
Hình 23: Contract Deployment	35
Hình 24: Kết quả code sau khi deployed contracts	36

CHƯƠNG 1 – TỔNG QUAN VỀ BLOCK CHAIN

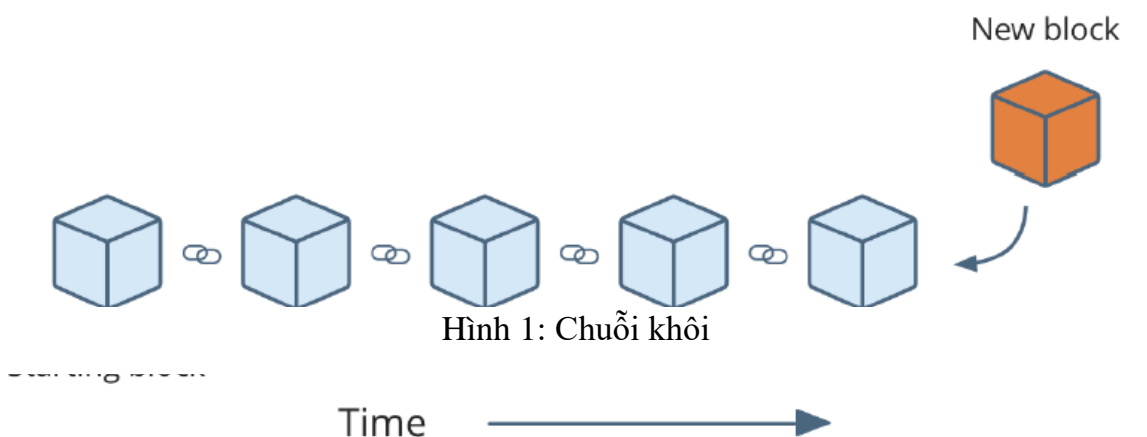
1.1 Mục đích đề tài

- Tìm hiểu về blockchain
- Tìm hiểu cụ thể Block Chain 1.0, 2.0 , các ứng dụng của nó và lịch sử ra đời
- Tìm hiểu smart contract và solidity

1.2 Khái niệm về Blockchain

Blockchain là một công nghệ lưu trữ và truyền thông tin phi tập trung, có tính bảo mật cao và khả năng xác thực dữ liệu một cách đáng tin cậy. Nó được sử dụng để tạo ra một hệ thống ghi chúng ta gọi là "khối" (block) để lưu trữ thông tin và giao dịch. Mỗi khối sẽ chứa thông tin về các giao dịch và một mã hash duy nhất, dựa trên thông tin của khối trước đó. Các khối này được liên kết với nhau thông qua mã hash, tạo thành một chuỗi liên tiếp gọi là blockchain.

Các thông tin trong blockchain được lưu trữ và phân tán trên nhiều nút (node) trong mạng. Mỗi nút có một bản sao của toàn bộ blockchain, giúp đảm bảo tính toàn vẹn



và không thể thay đổi dữ liệu. Khi có một giao dịch mới được thêm vào, thông tin này sẽ được gửi đến toàn bộ mạng và các nút sẽ thực hiện xác minh và cập nhật blockchain.

Quá trình này được thực hiện bởi các thuật toán mã hóa và các quy tắc xác định trước được gọi là giao thức của blockchain.

Một điều khác biệt của blockchain so với các công nghệ khác là thông tin **không nằm tập trung ở một máy chủ** nào cả, cũng không ai kiểm soát được nó, mọi thông tin sẽ được sao lưu trên nhiều máy chủ khác nhau. Thiết kế của mạng lưới này giúp chống lại sự thay đổi của dữ liệu và quản lý dưới mạng lưới phi tập trung. Ngay cả khi một phần của hệ thống blockchain sụp đổ thì các nút khác vẫn sẽ tiếp tục lưu trữ và giữ cho mạng lưới hoạt động bình thường.

1.2 Các đặc tính của block chain

1.2.1 Cơ sở dữ liệu phân tán (phi tập trung)

Phi tập trung: Blockchain không được kiểm soát bởi một tổ chức hay cá nhân duy nhất mà được lưu trữ và quản lý trên nhiều nút trong mạng. Điều này đảm bảo rằng không có bên thứ ba nào có thể thay đổi dữ liệu hoặc kiểm soát hệ thống.

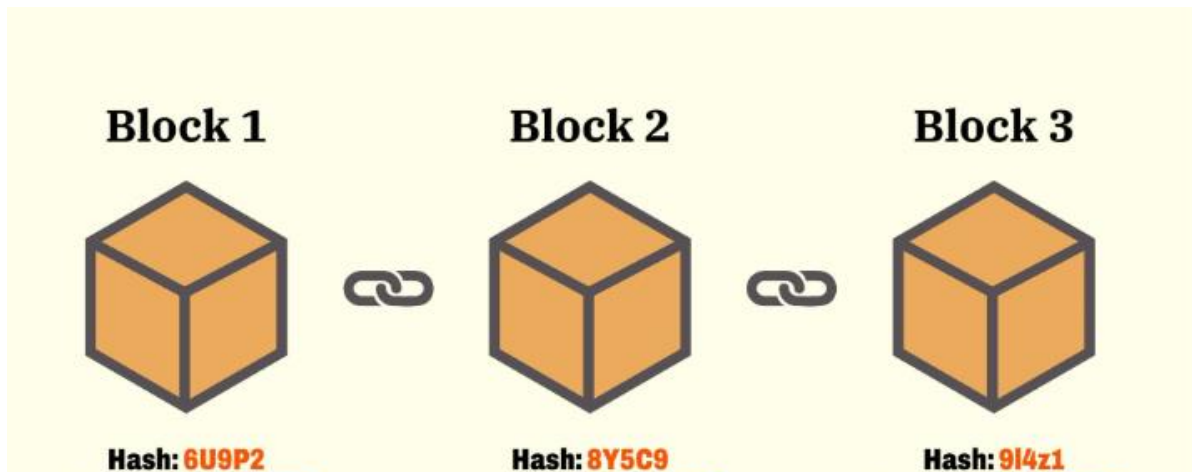


Hình 2: Mô hình sổ cái phân tán của block chain

1.2.2 Tính bền vững và tăng cường bảo mật

Bảo mật: Dữ liệu trong blockchain được mã hóa và được xác thực bằng các thuật toán mã hóa mạnh mẽ. Mỗi khối trong chuỗi được liên kết với khối trước đó thông qua mã hash, tạo thành một chuỗi không thể thay đổi. Điều này đảm bảo tính toàn vẹn và an toàn của dữ liệu.

Những người khai thác chuỗi này sẽ sử dụng phần mềm chuyên dụng để giải



Hình 3: Liên kết block

quyết các vấn đề liên quan đến số học vô cùng phức tạp, khi muốn tìm ra một nonce tạo ra một hàm băm được chấp nhận. Bởi, mỗi nonce chỉ có 32bit trong khi mỗi hàm băm là 256bit, nên có khoảng bốn tỷ tổ hợp nonce và hàm băm cần phải được tìm kiếm trước khi tìm ra “nonce vàng” để khối của họ được thêm vào chuỗi.

Ngoài ra, nếu có bất kỳ sự thay đổi nào đó ở một khối thì tất cả các khối ở sau đều bị ảnh hưởng vì khối sau liên kết với khối trước bằng mã băm.

Dựa vào điều đó có thể xảy ra các cuộc tấn công hệ thống bằng cách thay đổi các khối đến khối cuối cùng tuy nhiên chỉ là có thể nhưng thực tế nó lại không thể.

1.2.3 Xác thực dữ liệu

Mỗi giao dịch trong blockchain được xác thực bởi các nút trong mạng. Quá trình này đảm bảo rằng chỉ những giao dịch hợp lệ mới được thêm vào blockchain. Điều này giúp ngăn chặn các hành vi gian lận và đảm bảo tính chính xác của dữ liệu.

1.2.4 Tính minh bạch

Các block được nối tiếp nhau tạo thành chuỗi, một khi một block đã được cập nhật, bạn sẽ không thể xóa thông tin trong đó đi. Blockchain hoạt động dựa trên nguyên tắc ghi chép phổ biến trong tài chính là không được phép xóa bỏ dữ liệu đã cập nhật, thay vào đó cập nhật thêm các block mới, với nội dung cần chỉnh sửa và tên tuổi của người chỉnh sửa. Điều này vừa giúp rõ ràng thông tin lẫn sự toàn vẹn của các dữ liệu đã được tạo. Blockchain minh bạch để mỗi người có thể theo dõi dữ liệu nếu họ muốn.

1.2.5 Tính bất biến

Một khi dữ liệu được đưa vào một khối thì sẽ được mã hóa bằng thuật toán mã hóa băm kết hợp RSA security (mã hóa bất đối xứng) đảm bảo rằng dữ liệu không thể sửa đổi.

Do tính chất liên kết của các khối và mã hash, một khi một khối đã được thêm vào blockchain, nó không thể bị thay đổi hoặc xóa. Điều này đảm bảo tính lịch sử và không thể giả mạo dữ liệu.



Hình 4: Thuật toán mã hóa blockchain

1.3 Nguyên lý hoạt động của blockchain

- Tạo khối (Block creation): Mỗi giao dịch mới trong hệ thống được gom nhóm thành một khối. Khối này chứa các thông tin về giao dịch cùng với một mã hash duy nhất,

được tạo ra dựa trên nội dung của khối trước đó. Mã hash này đóng vai trò như một "dấu vân tay" duy nhất của khối.

- **Xác minh (Verification):** Sau khi một khối mới được tạo, các nút trong mạng sẽ xác minh tính hợp lệ của các giao dịch trong khối. Quá trình xác minh này thường được thực hiện bằng cách kiểm tra chữ ký số và sử dụng các thuật toán mã hóa. Nếu giao dịch được xác minh là hợp lệ, khối sẽ được chấp nhận và thêm vào blockchain.
- **Liên kết khối (Linking blocks):** Sau khi một khối mới được chấp nhận, nó sẽ được liên kết với khối trước đó bằng cách sử dụng mã hash. Mã hash của khối mới sẽ được lưu trong khối tiếp theo, tạo thành một chuỗi liên tiếp các khối, gọi là blockchain. Quá trình này làm cho blockchain trở nên không thể thay đổi vì bất kỳ thay đổi nào trong một khối cũng sẽ làm thay đổi mã hash của nó, ảnh hưởng đến toàn bộ chuỗi.
- **Xác thực phân tán (Decentralized validation):** Blockchain được lưu trữ và quản lý trên nhiều nút trong mạng. Mỗi nút có một bản sao của toàn bộ blockchain. Khi một giao dịch mới được thêm vào, thông tin sẽ được gửi đến tất cả các nút trong mạng để xác minh tính hợp lệ. Điều này đảm bảo tính xác thực phân tán và ngăn chặn các hành vi gian lận.
- **Cơ chế khai thác (Consensus mechanism):** Blockchain sử dụng cơ chế khai thác để quyết định nút nào được phép thêm một khối mới vào blockchain. Có nhiều cơ chế khai thác khác nhau, như Proof of Work (PoW) hoặc Proof of Stake (PoS), nhằm đảm bảo tính công bằng và ngăn chặn các cuộc tấn công từ các bên xấu.

Tổng hợp lại, nguyên lý hoạt động của blockchain bao gồm việc tạo khối, xác minh tính hợp lệ, liên kết khối thành chuỗi, xác thực phân tán và cơ chế khai thác. Quá trình này đảm bảo tính bảo mật, minh bạch và không thể thay đổi của dữ liệu trong blockchain.

1.4 Ứng dụng thực tiễn của công nghệ Blockchain trong cuộc sống

Một số ngành công nghiệp mà công nghệ Blockchain có thể tác động đến như:

- Công nghệ ô tô Automotive (Automotive)
- Chế tạo (Manufacturing)
- Công nghệ, truyền thông và viễn thông (Tech, media & Telecommunications)
- Dịch vụ tài chính (Financial Services)
- Nghệ thuật & Giải trí (Art & Recreation)
- Chăm sóc sức khỏe (Healthcare)
- Bảo hiểm (Insurance)
- Bán lẻ (Retail)
- Khu vực công (Public Sector)
- Bất động sản (Property)
- Nông nghiệp (Agricultural)
- Khai thác (Mining)
- Vận tải và Logistics (Transport & Logistics)
- Công trình hạ tầng kỹ thuật (Utility)

Hiện nay có rất nhiều công ty và tập đoàn lớn đang xây dựng mạng lưới của riêng mình bằng công nghệ Blockchain. Chắc chắn rằng Blockchain sẽ tạo nên một cuộc cách mạng trong vài năm tới ở Việt Nam và đóng vai trò ngày càng lớn trong việc thay đổi thế giới CNTT.

CHƯƠNG 2 – PHIÊN BẢN BLOCKCHAIN

2.1 Blockchain 1.0 (Tiền tệ)

Blockchain 1.0, còn được gọi là "Blockchain tiền tệ", tập trung vào việc tạo ra và quản lý tiền tệ số (cryptocurrency) như Bitcoin. Đây là phiên bản đầu tiên của blockchain và được phát triển để giải quyết vấn đề về sự tin cậy và an toàn trong việc thực hiện các giao dịch tài chính trực tuyến mà không cần sự can thiệp của các bên thứ ba.

Năm 2005, người ta cho ra đời ý tưởng về việc tạo ra một loại tiền điện tử. Sở cái Blockchain ra đời như một phương tiện hỗ trợ hoạt động của loại tiền này. Nói cách khác, Bitcoin, loại crypto đầu tiên cũng chính là ứng dụng đầu tiên của Blockchain.



Hình 5: Bitcoins

2.1.1 Các hoạt động của blockchain 1.0

Cụ thể khi khách hàng muốn sử dụng Bitcoin để thanh toán dịch vụ hay hàng hóa, người dùng sẽ ra lệnh ghi chép và xác nhận giao dịch. Giao dịch sẽ được ghi lại một cách công khai thành những khối block được xếp vào chuỗi, và được xác nhận bởi những

người sử dụng Bitcoin khác. Trung bình cứ 10 phút, một khối block mới được tạo ra thông qua việc "đào" Bitcoin.

Tức là, dựa vào giao thức của Bitcoin, cơ sở dữ liệu Blockchain được chia sẻ cho tất cả các máy tính tham gia vào hệ thống này. Mỗi máy tính sẽ có một bản sao chép của Blockchain có chứa dữ liệu ghi chép lại và là bằng chứng cho việc một giao dịch được hoàn tất.

2.1.2 Đặc điểm của blockchain 1.0

Các đặc điểm của Blockchain 1.0 (tiền tệ) bao gồm:

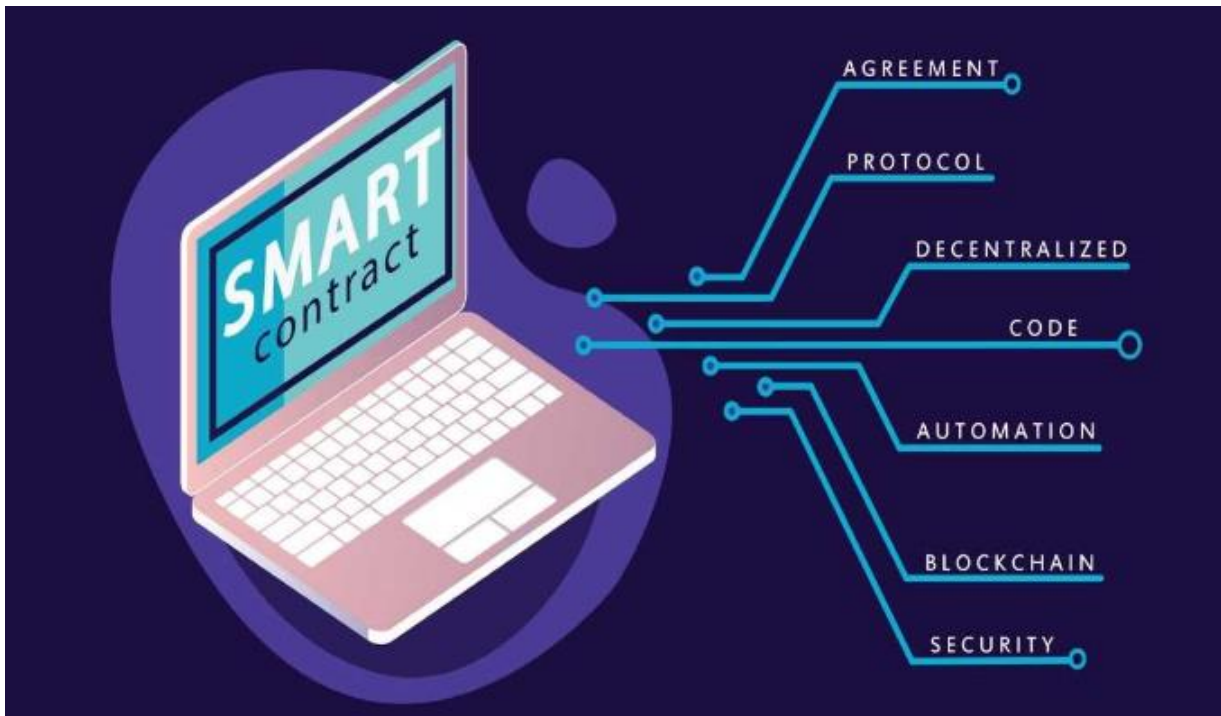
- **Cryptocurrency:** Blockchain 1.0 tạo ra các loại tiền tệ số như Bitcoin, Litecoin, hay Ethereum. Các giao dịch tài chính được thực hiện trên blockchain này sử dụng các đồng tiền số này, thay vì tiền tệ truyền thống.
- **Phi tập trung:** Blockchain 1.0 loại bỏ sự phụ thuộc vào các bên thứ ba như ngân hàng hay tổ chức tài chính truyền thống. Thay vào đó, blockchain được quản lý và duy trì bởi một mạng phân tán các nút, mỗi nút có một bản sao của toàn bộ blockchain.
- **Xác minh phân tán:** Mỗi giao dịch trên blockchain 1.0 được xác minh bởi các nút trong mạng. Quá trình xác minh này đảm bảo tính hợp lệ và chính xác của các giao dịch.
- **Mã hóa và bảo mật:** Blockchain 1.0 sử dụng các thuật toán mã hóa mạnh mẽ để bảo vệ tính riêng tư và an toàn của người dùng. Mỗi giao dịch được mã hóa và xác minh bằng chữ ký số.
- **Tính minh bạch:** Mọi giao dịch trên blockchain công cộng đều là công khai và có thể được xem và kiểm tra bởi tất cả mọi người. Điều này tạo ra tính minh bạch và tin tưởng trong hệ thống.

Blockchain 1.0 đã mở ra một cách tiếp cận mới trong lĩnh vực tài chính và tiền tệ. Nó đã cung cấp một nền tảng an toàn và tin cậy cho việc thực hiện các giao dịch tài chính trực tuyến mà không cần sự can thiệp của các bên trung gian.

2.2 Blockchain 2.0 (Smart contract)

Blockchain 2.0, hay còn được gọi là "Blockchain thông minh" hoặc "Blockchain hợp đồng thông minh", tập trung vào việc triển khai và thực thi các hợp đồng thông minh trên nền tảng blockchain. Blockchain 2.0 mở rộng khái niệm của blockchain 1.0 bằng cách tích hợp các hợp đồng thông minh, cho phép các giao dịch tự động và không cần sự can thiệp của bên thứ ba.

Blockchain đã thoát khỏi sự hạn hẹp bằng cách vượt ra khỏi lĩnh vực crypto mà tiến đến với Smart Contract. Công nghệ này có tác dụng bảo vệ các hợp đồng thông minh dưới sự can thiệp của những người có mục đích không tốt. Khi làm việc trên loại hợp đồng này, người sử dụng sẽ không cần tiêu tốn chi phí vào việc xác thực, vận hành và chống gian lận.



Hình 6: Smart contract

2.2.1 Cách hoạt động của blockchain 2.0

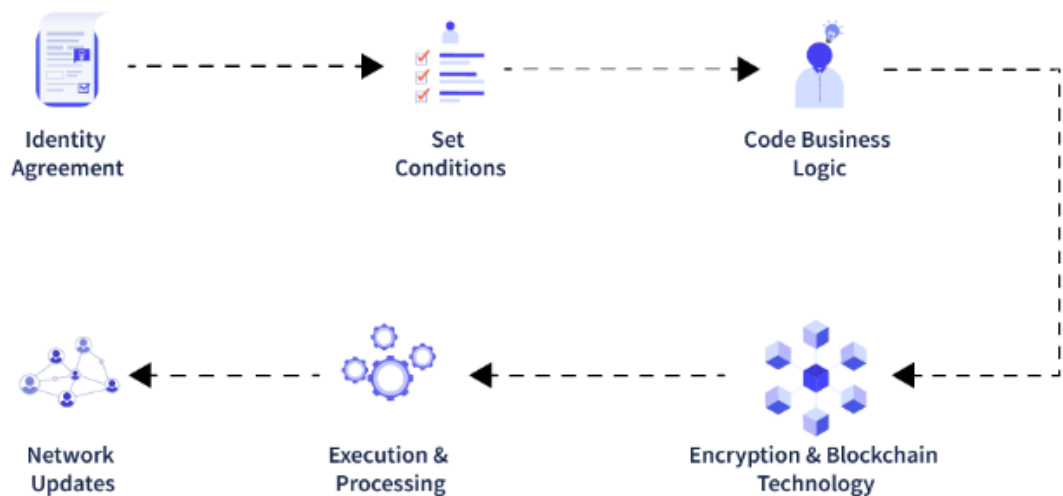
Hoạt động của blockchain 2.0 dựa trên việc triển khai và thực thi các hợp đồng thông minh trên nền tảng blockchain. Dưới đây là cách hoạt động của blockchain 2.0 smart contract:

- Triển khai hợp đồng thông minh: Đầu tiên, một hợp đồng thông minh được viết bằng một ngôn ngữ lập trình hỗ trợ trên nền tảng blockchain, chẳng hạn như Solidity trên Ethereum. Hợp đồng này chứa các điều khoản, điều kiện và tác vụ mà các bên trong giao dịch muốn thực hiện tự động.
- Gửi giao dịch: Người dùng muốn sử dụng hợp đồng thông minh sẽ tạo một giao dịch trên blockchain, chứa thông tin về hợp đồng và các tham số đầu vào. Giao dịch này được gửi đến mạng blockchain để được xác minh và thực thi.
- Xác minh giao dịch: Các nút trong mạng blockchain nhận được giao dịch và xác minh tính hợp lệ của nó. Điều này bao gồm kiểm tra chữ ký số, xác thực thông tin và kiểm tra điều kiện trong hợp đồng thông minh.
- Thực thi hợp đồng thông minh: Nếu giao dịch được xác minh là hợp lệ, các nút trong mạng sẽ thực hiện các tác vụ và điều kiện được định nghĩa trong hợp đồng thông minh. Các tác vụ này có thể bao gồm chuyển đổi tài sản, lưu trữ dữ liệu, tính toán hoặc thay đổi trạng thái của hợp đồng.
- Ghi vào blockchain: Sau khi hợp đồng thông minh được thực thi, kết quả và trạng thái mới của hợp đồng được ghi vào blockchain. Điều này đảm bảo rằng tất cả các bên trong mạng đồng thuận về trạng thái của hợp đồng và có thể kiểm tra và xác minh nó.
- Trả phí và thưởng: Để thực hiện các giao dịch và thực hiện hợp đồng thông minh, người gửi giao dịch phải trả một khoản phí nhỏ. Phí này được sử dụng để thưởng cho các nút tham gia vào quá trình xác minh và thực thi hợp đồng.

Tổng hợp lại, hoạt động của blockchain 2.0 smart contract bao gồm triển khai hợp đồng thông minh, gửi giao dịch, xác minh và thực thi hợp đồng, ghi vào blockchain và trả phí. Các hợp đồng thông minh giúp tự động hóa các giao dịch và loại bỏ sự phụ thuộc vào bên thứ ba, tăng tính minh bạch và độ tin cậy trong các quy trình kinh doanh và tài chính.

CoinDCX

How does a Smart Contract Work?



Hình 7: Cách hoạt động của Smart contract

Nguồn: CoinDCX

2.2.2 Đặc điểm của blockchain 2.0

Các đặc điểm của Blockchain 2.0 (Smart Contract) bao gồm:

- Hợp đồng thông minh (Smart Contract): Blockchain 2.0 cho phép việc tạo, triển khai và thực thi các hợp đồng thông minh trên nền tảng blockchain. Hợp đồng thông minh là các chương trình tự thực hiện và thực hiện các điều khoản hợp đồng một cách tự động khi các điều kiện đã được đáp ứng. Điều này giúp loại bỏ sự phụ thuộc vào các bên trung gian và tăng tính tự động hóa trong các giao dịch.
- Tính toán phân tán: Các hợp đồng thông minh trên blockchain 2.0 được thực thi trên một mạng phân tán các nút. Mỗi nút trong mạng thực hiện cùng một phiên bản của hợp đồng và xác minh tính hợp lệ của các giao dịch liên quan đến hợp đồng. Điều này tạo ra tính toán phân tán và đảm bảo tính công bằng và minh bạch trong việc thực hiện các hợp đồng.
- Tính năng Turing đầy đủ: Blockchain 2.0 hỗ trợ tính năng Turing đầy đủ trong hợp đồng thông minh. Điều này có nghĩa là hợp đồng thông minh có thể thực hiện bất kỳ loại tính toán phức tạp nào, tương tự như các ngôn ngữ lập trình thông thường. Điều này mở ra nhiều cơ hội sáng tạo và ứng dụng trong việc triển khai hợp đồng thông minh.
- Phí giao dịch: Các giao dịch liên quan đến hợp đồng thông minh trên blockchain 2.0 thường có một khoản phí nhỏ, được sử dụng để thưởng cho các nút tham gia vào việc xác minh và thực thi hợp đồng. Phí giao dịch này giúp ngăn chặn việc spam và đảm bảo tính bền vững của mạng.

Blockchain 2.0 mở ra một cách tiếp cận mới trong việc triển khai và thực thi các hợp đồng thông minh. Nó cho phép giao dịch tự động và không cần sự can thiệp của bên thứ ba, tăng tính tự động hóa và minh bạch trong các quy trình kinh doanh và tài chính.

2.3 Blockchain 3.0 (Ứng dụng phi tập trung Dapp)

Blockchain 3.0, hay còn được gọi là "Blockchain ứng dụng phi tập trung" hoặc "Blockchain phi tập trung ứng dụng" (Decentralized Applications - Dapps), tập trung vào việc phát triển và triển khai các ứng dụng phi tập trung trên nền tảng blockchain. Blockchain 3.0 mở rộng khái niệm của blockchain 2.0 bằng cách tập trung vào việc xây dựng các ứng dụng thực tế và tiện ích, không chỉ giới hạn trong lĩnh vực tài chính và quản lý hợp đồng.



Hình 8: Phân biệt app và Dapp

- **Mô hình website truyền thống:** Frontend → API → Database
- **Mô hình website Dapps:** Frontend → Smart Contract (ABI) → Blockchain

2.3.1 Cách đặc điểm của blockchain 3.0 (Dapp)

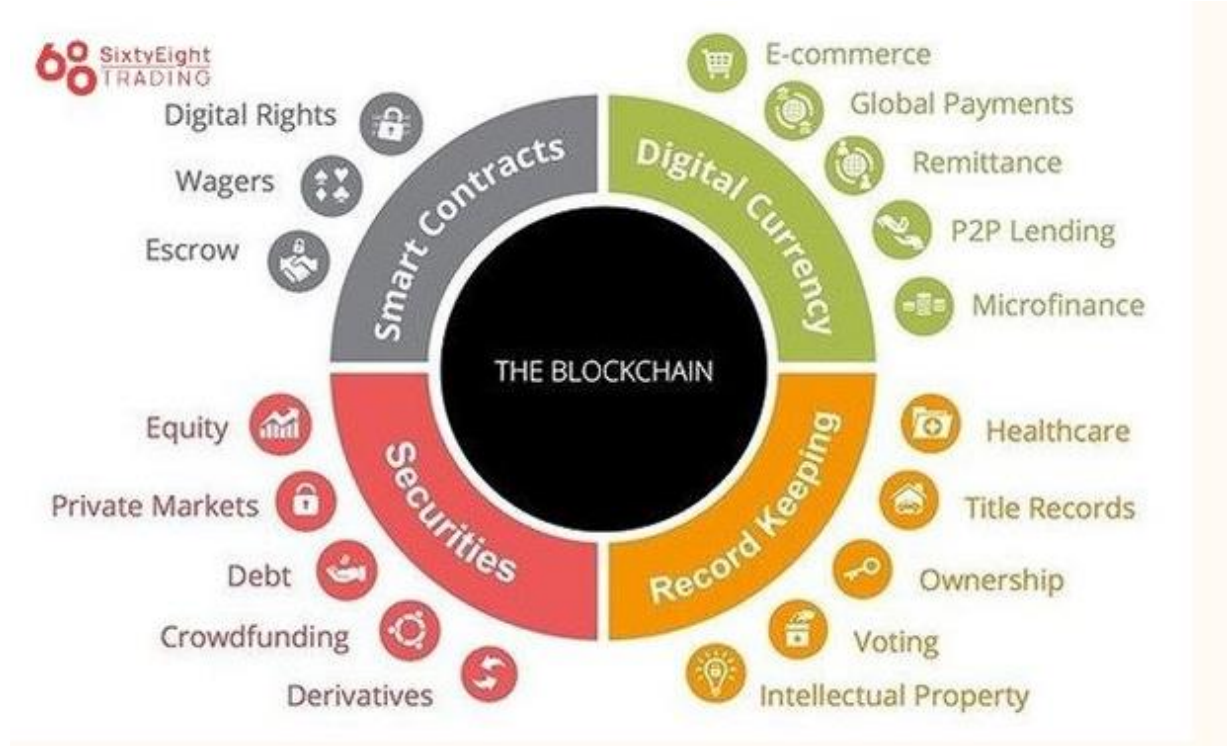
Các đặc điểm của Blockchain 3.0 (Ứng dụng phi tập trung Dapp) bao gồm:

- **Phi tập trung:** Blockchain 3.0 nhấn mạnh tính phi tập trung, trong đó dữ liệu và chức năng của ứng dụng được phân tán trên nhiều nút trong mạng blockchain. Điều này giúp loại bỏ sự phụ thuộc vào một bên thứ ba trung gian và tạo ra môi trường công bằng và minh bạch cho người dùng.

- Ứng dụng thực tế: Blockchain 3.0 tập trung vào việc phát triển các ứng dụng thực tế và tiện ích, không chỉ giới hạn trong lĩnh vực tài chính và quản lý hợp đồng. Các ứng dụng phi tập trung có thể bao gồm các lĩnh vực như bỏ phiếu phi tập trung, chuỗi cung ứng, quản lý danh tính, chia sẻ tài sản và nhiều lĩnh vực khác.
- Tiêu chuẩn giao thức: Blockchain 3.0 thường sử dụng các tiêu chuẩn giao thức mở, cho phép các ứng dụng phi tập trung tương tác và tương thích với nhau. Các tiêu chuẩn như ERC-20 trên Ethereum cho phép các dự án phát triển và triển khai các token tiêu chuẩn trên blockchain.
- Tính bảo mật và quyền riêng tư: Blockchain 3.0 quan tâm đến bảo mật và quyền riêng tư của người dùng. Các ứng dụng phi tập trung cung cấp cơ chế mã hóa và quản lý quyền riêng tư để đảm bảo rằng dữ liệu cá nhân và giao dịch được bảo vệ.
- Tính mở rộng: Blockchain 3.0 tập trung vào việc cải thiện khả năng mở rộng của nền tảng blockchain. Một số dự án ứng dụng phi tập trung sử dụng các giải pháp như sharding, sidechains và công nghệ hiệu suất cao để tăng tốc độ xử lý và khả năng mở rộng của mạng.

2.4 Blockchain 4.0 (Ứng dụng thực tiễn)

Blockchain của thời đại này không chỉ tập trung vào lĩnh vực tài chính mà còn trở thành một giải pháp cho các vấn đề cơ bản của đời sống. Blockchain có tác dụng hỗ trợ các doanh nghiệp xây dựng một quá trình làm việc xuyên nền tảng, chẳng hạn như chuỗi cung ứng, hệ thống xử lý đơn hàng tự động, thanh toán, thu thập dữ liệu Internet.



Hình 9: Ứng dụng blockchain

2.4.1 Cách đặc điểm của blockchain 4.0

Các đặc điểm của Blockchain 4.0 (Ứng dụng thực tiễn) bao gồm:

- Hiệu suất và mở rộng: Blockchain 4.0 tập trung vào việc cải thiện hiệu suất và khả năng mở rộng của công nghệ blockchain. Các phương pháp như sharding, sidechains, và công nghệ hiệu suất cao được áp dụng để tăng tốc độ xử lý và khả năng mở rộng của mạng.
- Tích hợp với hệ thống hiện có: Blockchain 4.0 hướng đến tích hợp với hệ thống hiện có và các nguồn dữ liệu bên ngoài. Điều này cho phép dữ liệu từ các nguồn khác nhau được gửi và nhận trên blockchain, tạo điều kiện cho việc xây dựng các ứng dụng và dịch vụ phức tạp hơn.









- Quyền riêng tư và bảo mật: Blockchain 4.0 đặc biệt quan tâm đến bảo mật và quyền riêng tư của người dùng. Các công nghệ mã hóa và chứng thực được áp dụng để bảo vệ dữ liệu và giao dịch trên blockchain.
- Tích hợp với trí tuệ nhân tạo và IoT: Blockchain 4.0 đưa công nghệ blockchain vào cuộc cách mạng kỹ thuật số tổng thể bằng cách tích hợp với trí tuệ nhân tạo (AI) và Internet of Things (IoT). Sự kết hợp này tạo ra những ứng dụng thông minh và tự động hơn, từ hệ thống quản lý tài sản đến các hệ thống xử lý giao dịch tự động.
- Tính sẵn sàng và ổn định: Blockchain 4.0 đặt trọng tâm vào tính sẵn sàng và ổn định của các ứng dụng và hệ thống blockchain. Việc phát triển công nghệ blockchain với sự thử nghiệm, kiểm tra và cải tiến liên tục giúp đảm bảo tính ổn định và khả năng đáp ứng của hệ thống.

2.5 Các loại của blockchain

Có ba loại chính của blockchain:

- Blockchain công cộng (Public Blockchain): Đây là loại blockchain mà bất kỳ ai cũng có thể tham gia và xem được toàn bộ thông tin. Mọi người có thể tạo và xác nhận các giao dịch, và thông tin được lưu trữ công khai trên mạng blockchain. Ví dụ nổi tiếng của blockchain công cộng là Bitcoin và Ethereum.
- Blockchain tư nhân (Private Blockchain): Đây là loại blockchain chỉ cho phép một nhóm nhất định của các thực thể tham gia, thường là các tổ chức, doanh nghiệp hoặc tổ chức chính phủ. Quyền truy cập và quyền kiểm soát dữ liệu được giới hạn cho những người tham gia được ủy quyền. Blockchain tư nhân thường được sử dụng để xây dựng các ứng dụng nội bộ và giải quyết các vấn đề liên quan đến quyền riêng tư và bảo mật.
- Blockchain konsortium (Consortium Blockchain): Đây là một dạng trung gian giữa blockchain công cộng và tư nhân. Trong loại blockchain này, một nhóm các tổ chức đồng ý cùng quản lý và vận hành mạng blockchain. Các thành viên của

mạng blockchain konsortium thường được xác thực và có quyền kiểm soát dữ liệu. Loại blockchain này thường được sử dụng trong các ngành công nghiệp hoặc lĩnh vực có nhiều tổ chức cần liên kết và chia sẻ thông tin.

THE COMPARISON TABLE		
	PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN
 Access	 Anyone	Single organization
Authority	Decentralized	Partially decentralized 
Transaction Speed	 Slow	Fast
Consensus	Permissionless	Permissioned 
Efficiency	 Low	High
Data Handling	Read and Write access for anyone	Read and write for a single organization 
Immutability	 Full	Partial

Hình 10: Bảng so sánh private và public blockchain

CHƯƠNG 3 – SMART CONTRACT & SOLIDITY

3.1 Khái niệm smart contract

Smart contract (hợp đồng thông minh) là một chương trình máy tính tự động hóa, được viết bằng mã nguồn và thực thi trên blockchain. Nó là một phần của công nghệ blockchain, cho phép thực hiện các giao dịch và thỏa thuận mà không cần sự can thiệp của bên thứ ba.

Smart contract hoạt động theo nguyên tắc "nếu... thì". Khi một điều kiện được đáp ứng, ví dụ như một số lượng tiền được chuyển đến, hợp đồng sẽ tự động thực hiện một hành động nào đó. Điều này giúp đảm bảo tính tự động, đáng tin cậy và không thể thay đổi của các giao dịch.



Hình 11: Smart Contract

3.2 Cách hoạt động của smart contract

Hợp đồng thông minh hoạt động bằng cách tuân theo quy tắc câu lệnh “Nếu/khi...thì...” đơn giản, được viết thành mã trên chuỗi khối.

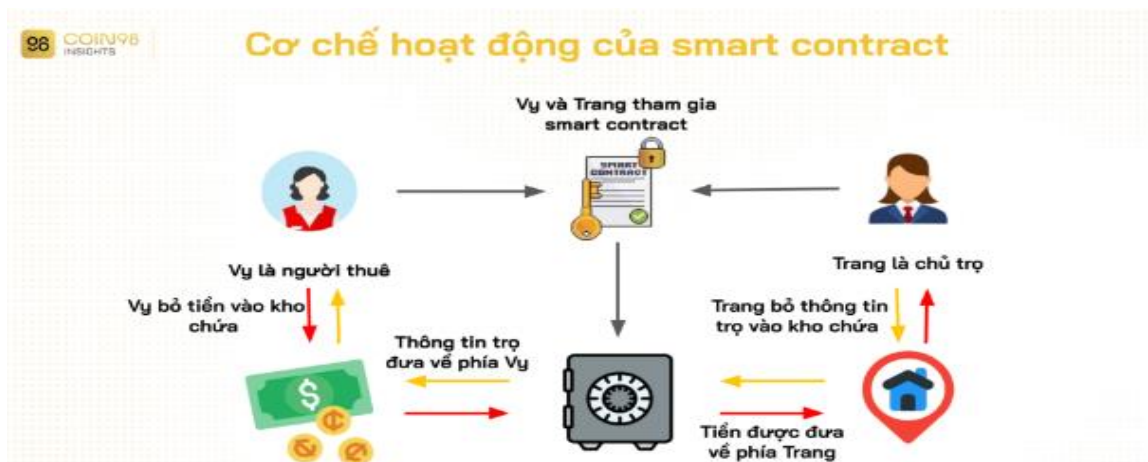
Một mạng máy tính thực hiện các hành động khi điều kiện xác định trước đó được đáp ứng và xác minh. Những hành động này bao gồm việc giải ngân cho người thích hợp, đăng ký phương tiện, gửi thông báo hoặc xuất vé,...

Sau đó, hợp đồng thông minh blockchain sẽ cập nhật khi giao dịch hoàn tất. Điều đó có nghĩa là giao dịch không thể thay đổi và chỉ những bên đã được cấp phép mới có quyền xem kết quả.

Trong một hợp đồng thông minh, có thể đặt ra nhiều quy định cần thiết để làm hài lòng những người tham gia và cam kết rằng nhiệm vụ sẽ được hoàn thành thỏa đáng.

Để thiết lập điều khoản, người tham gia phải xác định cách các giao dịch và dữ liệu của họ thể hiện trên blockchain, đồng ý về quy tắc “nếu/khi...thì...” chi phối những giao dịch đó, liệt kê tất cả trường hợp ngoại lệ có khả năng xảy ra và xác định khuôn khổ để giải quyết tranh chấp.

Sau đó, hợp đồng thông minh được lập trình bởi nhà phát triển. Hiện nay, cấu trúc của smart contract cũng phần nào được đơn giản hóa bởi nhiều tổ chức cung cấp dịch vụ blockchain cho doanh nghiệp tạo ra các mẫu, giao diện web và nhiều công cụ trực tuyến khác.



Hình 12: Cơ chế hoạt động của smart contract

3.3 Lợi ích của smart contract

Hợp đồng thông minh ngày càng trở nên phổ biến nhờ mang lại nhiều lợi ích:

- *Tốc độ, hiệu quả và độ chính xác:*

Khi một điều kiện đáp ứng đầy đủ, hợp đồng sẽ được thực hiện ngay lập tức. Hợp đồng thông minh là hợp đồng kỹ thuật số và hoàn toàn tự động, các bên tham gia không cần xử lý thủ tục giấy tờ, không mất thời gian điều chỉnh lỗi (thường xảy ra do soạn tài liệu theo cách thủ công).

- *Sự tin cậy và minh bạch*

Vì không có bên thứ ba liên quan và hồ sơ giao dịch được mã hóa, chia sẻ giữa những người tham gia nên thông tin không thể bị thay đổi vì lợi ích cá nhân.

- *Bảo vệ*

Hồ sơ giao dịch trên blockchain được mã hóa nên rất khó bị hack. Hơn nữa, vì mỗi bản ghi được kết nối với các bản ghi trước đó và tiếp theo trên sổ cái phân tán, tin tặc sẽ phải thay đổi toàn bộ chuỗi để thay đổi một bản ghi duy nhất.

- *Tiết kiệm*

Hợp đồng thông minh loại bỏ nhu cầu sử dụng bên thứ ba để xử lý giao dịch. Nhờ đó, những bên tham gia tiết kiệm chi phí liên quan, cũng như giảm lãng phí thời gian.

3.4 Ưu điểm và nhược điểm của smart contract

3.4.1 Ưu điểm

- Ứng dụng của hợp đồng thông minh có thể được sử dụng vào nhiều lĩnh vực khác nhau: Logistic, ngân hàng, bất động sản, bầu cử,...
- Tự do: Không nhận sự quản lý của bất kỳ một cơ quan nào.
- Giảm thiểu rủi ro đến từ bên thứ ba.

- An toàn và minh bạch.
- Tiết kiệm và nhanh chóng.

3.4.1 Nhược điểm

- Rủi ro từ Internet: Có thể bị tấn công hoặc khai thác bởi các hacker nếu để lộ những thông tin quan trọng.
- Không nhận được quyền pháp lý: Quyền lợi có thể không được bảo vệ vì chưa có chính sách.
- Yêu cầu cao về trình độ triển khai của các lập trình viên và hệ thống. Từ đó, chi phí để trả cho họ và cơ sở hạ tầng là không hề nhỏ.

3.5 Ứng dụng của hợp đồng thông minh trong thực tiễn

Một số ứng dụng của smart contract bao gồm:

- Giao dịch tài chính: Smart contract có thể được sử dụng để thực hiện các giao dịch tài chính tự động, chẳng hạn như chuyển tiền, thanh toán lãi suất, hoặc thực hiện các hợp đồng tương lai.
- Quản lý tài sản: Smart contract có thể được sử dụng để quản lý và giao dịch các tài sản kỹ thuật số, chẳng hạn như đất đai, bất động sản, hoặc các quyền sở hữu trí tuệ.
- Quản lý chuỗi cung ứng: Smart contract có thể được sử dụng để theo dõi và quản lý các giao dịch trong chuỗi cung ứng, giúp tăng tính minh bạch và hiệu quả.
- Bỏ phiếu và lưu trữ thông tin: Smart contract có thể được sử dụng để kiểm tra tính chính xác và bảo mật của quá trình bỏ phiếu hoặc lưu trữ thông tin quan trọng.



Hình 13: Ứng dụng thực tế của hợp đồng thông minh

3.6 Solidity

3.6.1 Khái niệm Solidity

Solidity là ngôn ngữ lập trình được sử dụng để viết smart contract trên nền tảng Ethereum. Nó được thiết kế để cung cấp các tính năng mạnh mẽ và linh hoạt để phát triển các ứng dụng phi tập trung (decentralized applications - DApps) trên blockchain Ethereum.

Solidity có cú pháp tương tự như ngôn ngữ lập trình JavaScript và được biên dịch thành mã bytecode để thực thi trên máy ảo Ethereum (EVM - Ethereum Virtual Machine). Ngôn ngữ này hỗ trợ các tính năng như kế thừa, kiểu dữ liệu tùy chỉnh, hợp đồng, sự kiện và quản lý tiền tệ.

3.6.2 Contracts

Mã của Solidity được đóng gói trong các hợp đồng. Một hợp đồng là khối xây dựng cơ bản của các ứng dụng Ethereum – tất cả các biến và chức năng thuộc về một hợp đồng, và đây là điểm khởi đầu của tất cả các dự án của bạn. VD về contract có tên HelloSolidity:

```

1  // Khai báo phiên bản Solidity
2  pragma solidity ^0.8.0;
3
4  // Khai báo contract
5  contract HelloSolidity {
6      // Khai báo biến lưu trữ thông điệp
7      string private message;
8
9      // Hàm khởi tạo, được thực thi khi contract được triển khai
10     constructor() {
11         message = "Hello Solidity!";
12     }
13
14     // Hàm trả về thông điệp
15     function getMessage() public view returns (string memory) {
16         return message;
17     }
18
19     // Hàm để thay đổi thông điệp
20     function setMessage(string memory newMessage) public {
21         message = newMessage;
22     }
23 }

```

Hình 14: Code ví dụ về contract

3.6.3 Sử dụng Metamask triển khai Smart contract trong Solidity

a. Remix IDE

Để viết và thực thi mã solidity, IDE phổ biến nhất được sử dụng là REMIX. <https://remix.ethereum.org/> hoặc có thể sử dụng Mist (trình duyệt Ethereum DApp).

Sau khi viết mã và biên dịch nó, chúng ta có thể triển khai nó theo 3 cách:

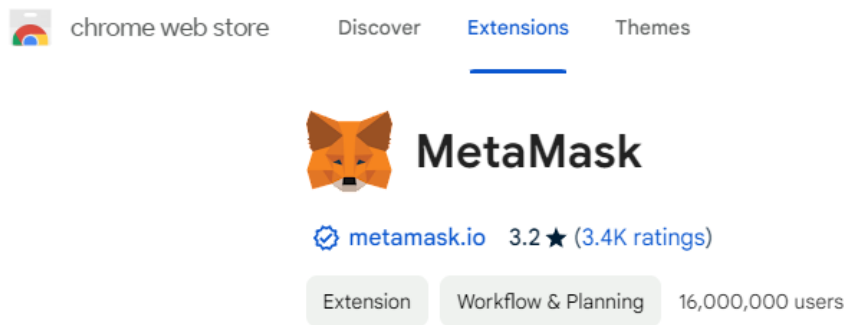
- JavaScriptVM
- Injected Provider Metamask

- Web3 Provider

Các bước dưới đây triển khai hợp đồng bằng cách sử dụng MetaMask dưới dạng Injected Provider MetaMask.

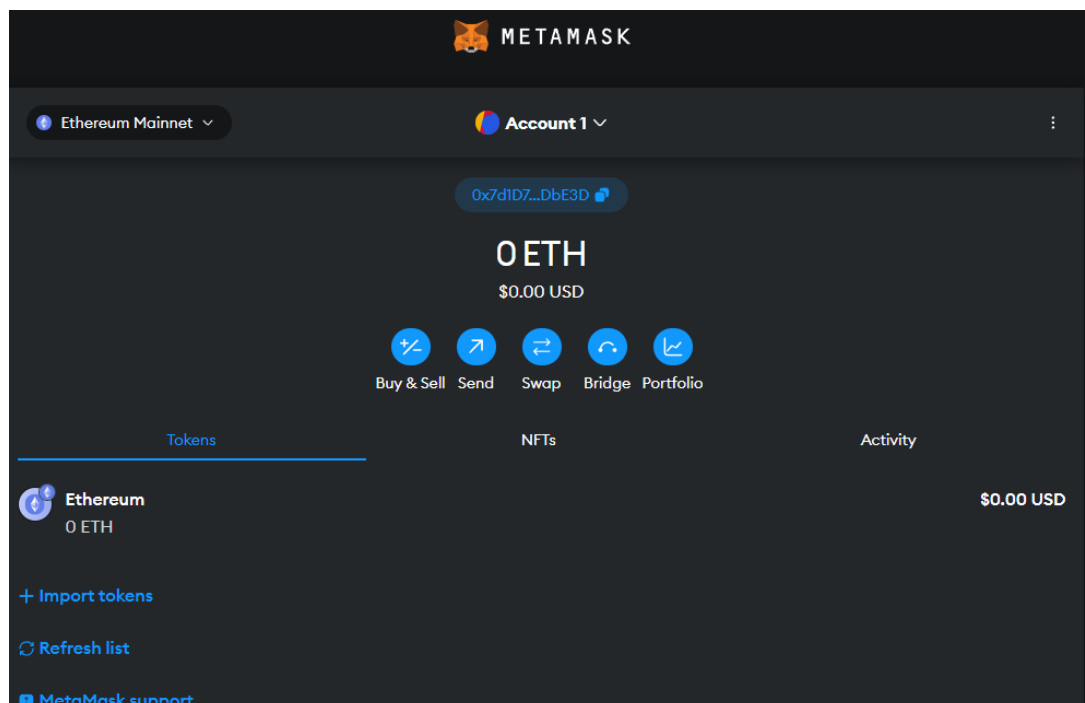
b. Cài đặt ví thử nghiệm MetaMask

- Tìm kiếm từ khóa “Metamask” trong Extension.



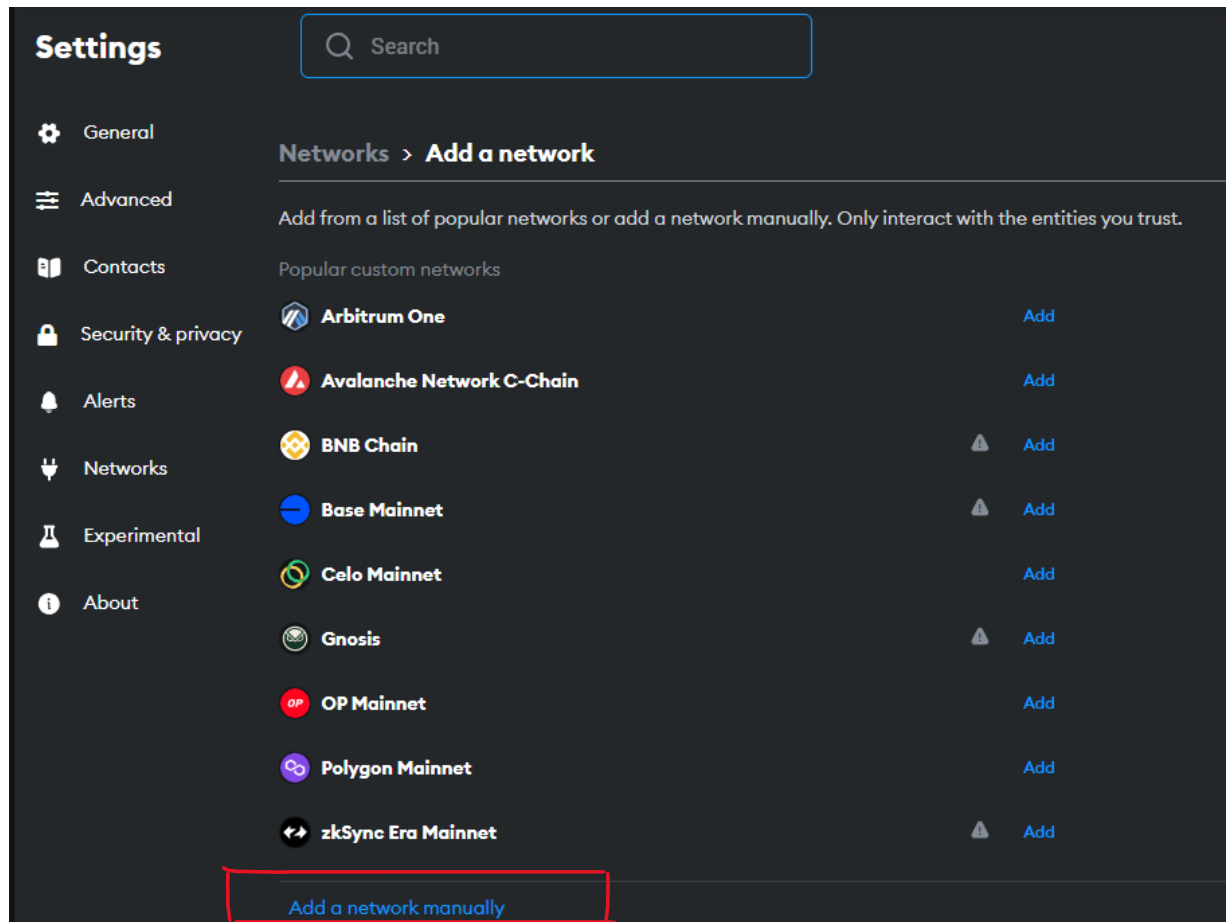
Hình 15:MetaMask Extension

- Tiếp theo là thiết lập ví trong MetaMask



Hình 16:MetaMask wallet

- Sau khi thiết lập ví thì kết nối mạng như sau:



Hình 17: Custom Network

- Add a network manually như sau:

Networks > Add a network > Add a network manually

i A malicious network provider can lie about the state of the blockchain and record your network activity. Only add custom networks you trust.

Network name

BNB Chain Testnet

New RPC URL

<https://data-seed-prebsc-1-s1.binance.org:8545/>

Chain ID **i**

97

Currency symbol

tBNB

Suggested ticker symbol: **tBNB**

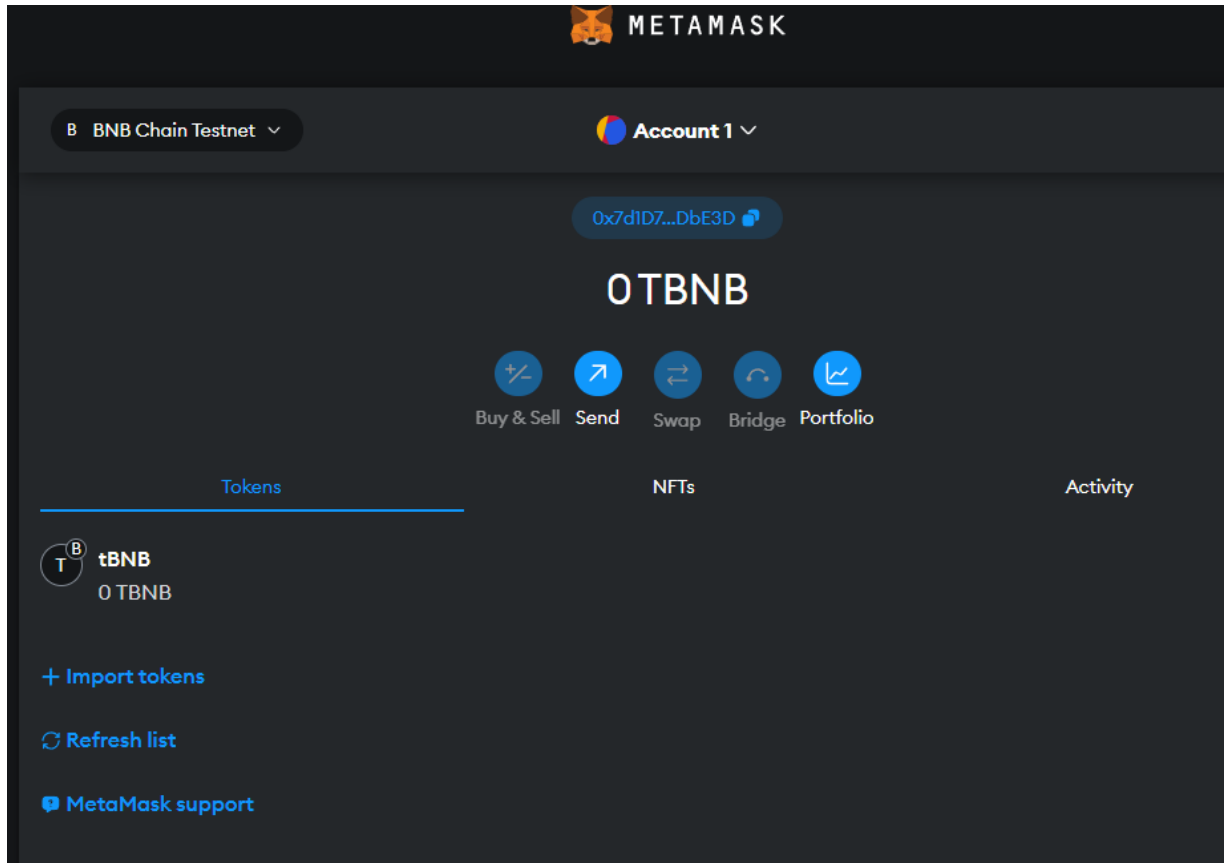
Block explorer URL (Optional)

<https://testnet.bscscan.com/>

Cancel Save

Hình 18: Add a network manually

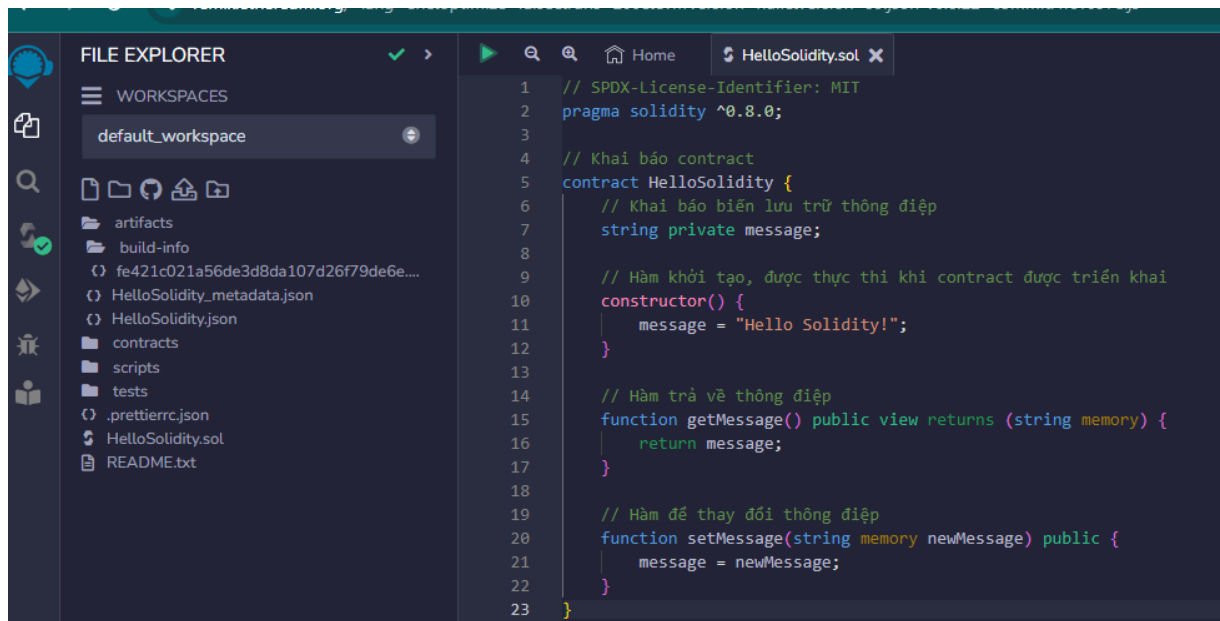
- Kết nối thành công



Hình 19: Tạo ví và kết nối network thành công

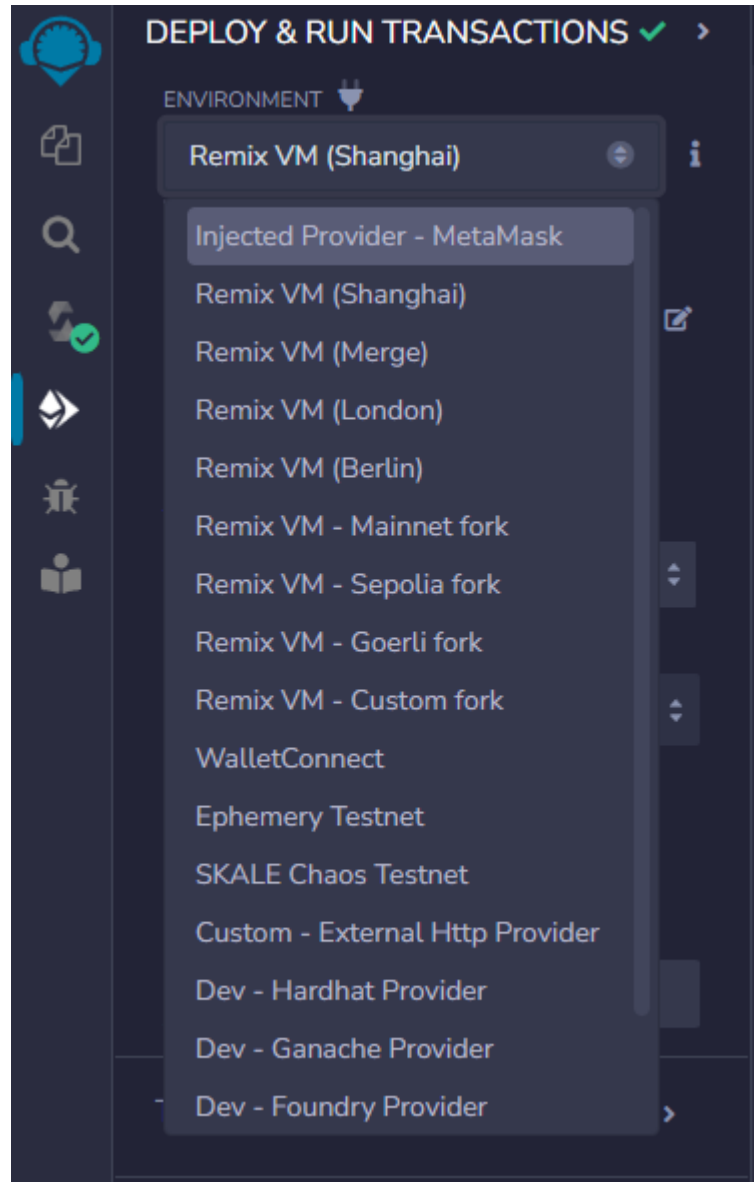
c. Cách triển khai contract

- Bước 1: Tạo new file.sol trong IDE Remix như sau:



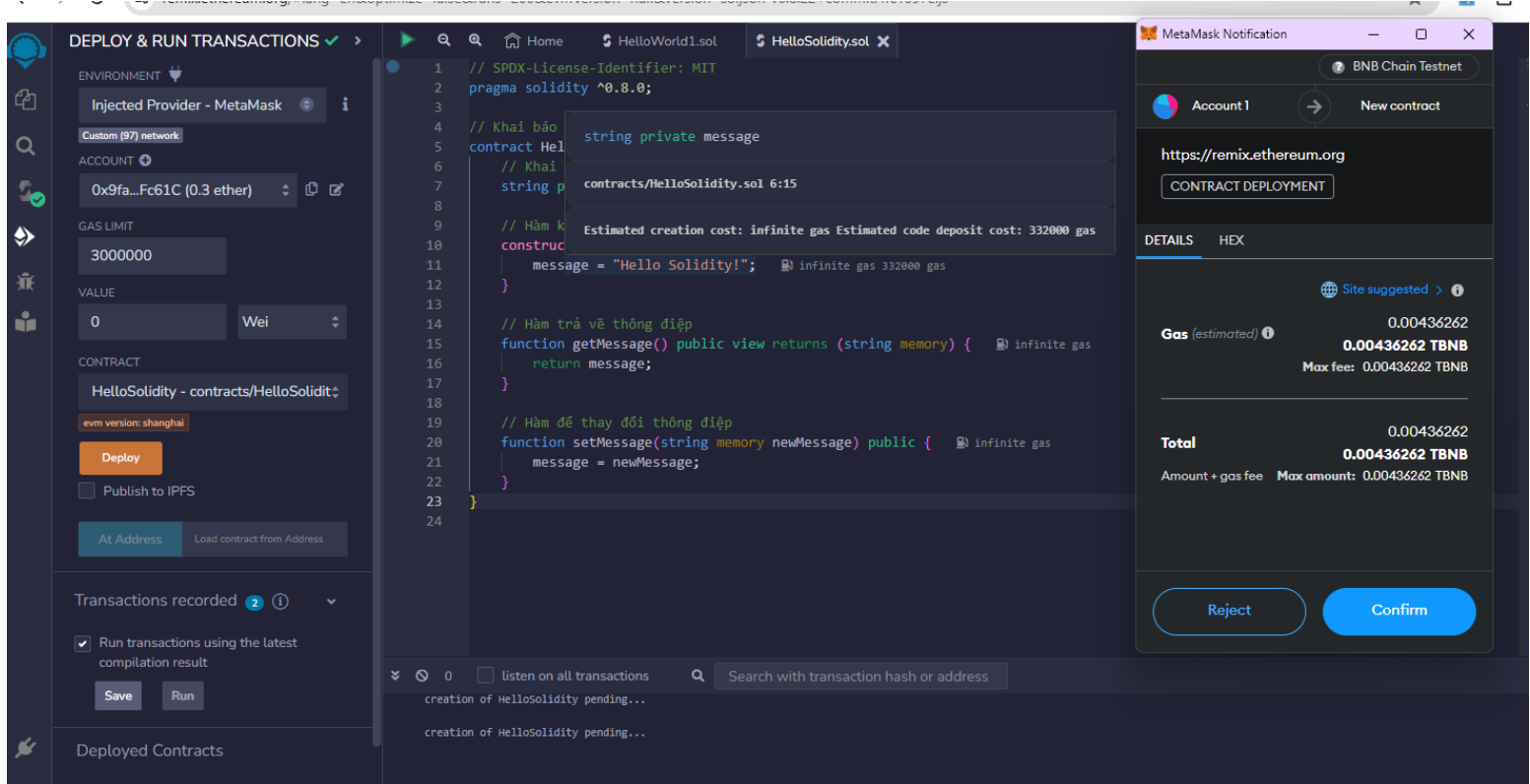
Hình 20: Tạo File HelloSolidity.sol

- Bước 2: Sau khi biên dịch và chuyển sang phần Deploy ngay bên dưới phần Compile và chọn Injected Provider MetaMask thay cho RemixVM(Shanghai) như hình dưới đây:



Hình 21: Sét Environment Deploy

- Bước 3: Bây giờ hợp đồng đã sẵn sàng để được triển khai. Nhấp nút Deploy và MetaMask sẽ yêu cầu xác nhận như sau:



Hình 22: Xác nhận đã triển khai



- Bước 4: Bây giờ, để xác minh xem giao dịch (quy trình) có được thực hiện thành công hay không, bạn có thể kiểm tra số dư của mình trên MetaMask như hình dưới đây:

Contract deployment

Status
Confirmed

[View on block explorer](#)
[Copy transaction ID](#)

From

 0x9fa25...Fc... 

To
New contract

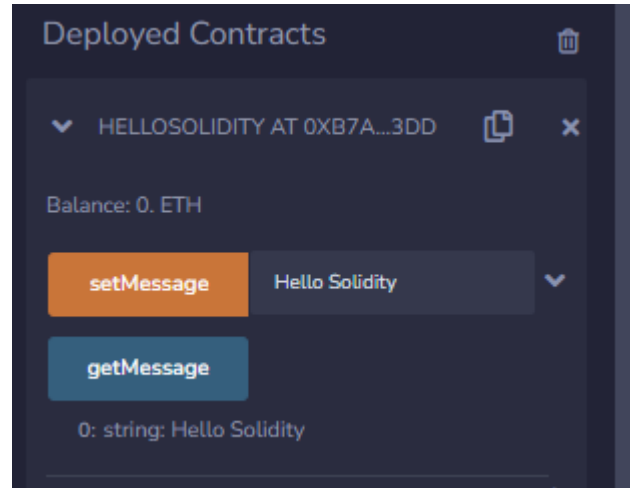
Transaction

Nonce	0
Amount	-0 TBNB
Gas Limit (Units)	436262
Gas Used (Units)	436262
Base fee (GWEI)	0
Priority fee (GWEI)	10
Total gas fee	0.004363 TBNB
Max fee per gas	0.00000001 TBNB
Total	0.00436262 TBNB

[+ Activity log](#)

Hình 23: Contract Deployment

- Bước 5: Sau khi contract đã xác nhận thì mình có thể thực thi code và in ra kết quả như sau:



Hình 24: Kết quả code sau khi deployed contracts

Đây là cách triển khai cơ bản của MetaMask với Solidity.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. <https://vbpo.com.vn/news/blog-40/blockchain-la-gi-hoat-dong-cua-blockchain-nhu-the-nao-ung-dung-ra-sao>
2. <https://bytesoft.vn/cong-nghe-blockchain-1-0-la-gi>
3. <https://coin98.net/blockchain-101>
4. <https://zipmex.com/th/en/learn/what-is-smart-contract/>
5. <https://www.devteam.space/blog/dapps-in-blockchain/>
6. <https://coin68.com/smart-contract-la-gi/>
7. <https://youtu.be/-VHMet5Nthc?si=YkhGMeSDNkjQ2z9m>
8. <https://poe.com/chat/1z69g40n3lr8h5ue4ee>

