Trường Đại học Khoa học Tự nhiên
Khoa Công nghệ thông tin

Các công nghệ mới trong phát triển phần mềm

Đề tài: Lottery Blockchain

Thành viên:
Trần Nhật Phi - 18120504
Trần Phúc Nguyên – 18120488
Trần Đức Năng - 18120475

Giảng viên: **Trần Văn Quý**

Mục lục

I. Ý nghĩa đề tài: 3
II. Các công nghệ sử dụng trong trò chơi: 3
1. Chainlink: 3
2. Chainlink VRF: 4
3. ABI: 5
4. Remix IDE: 6
5. Solidity: 6
6. Web 3.0: 7
III. Quá trình thực hiện: 9
IV. Cách sử dụng: 12
V. Cách thực hiện: 14
VI. Tài liệu tham khảo: 14

I. Ý nghĩa đề tài:

- Random Number Generator là chủ đề về thuật toán phát sinh số ngẫu nhiên được sử dụng trong các ứng dụng ngày nay. Thuật toán phát sinh số ngẫu nhiên có 2 nhóm thuật toán: phát sinh số ngẫu nhiên dựa trên giá trị khởi tạo và phát sinh số ngẫu nhiên dựa vào Oracle
- Nhóm đã dựa vào chủ đề phát sinh số ngẫu nhiên để làm nên trò chơi xổ số: Lottery game dựa vào thuật toán phát sinh số ngẫu nhiên để phát sinh kết quả xổ số. Kết quả này không phụ thuộc vào người tạo nên trò chơi hay người bắt đầu trò chơi, vì vậy tạo nên một trò chơi công bằng đối với tất cả mọi người tham gia

II. Các công nghệ sử dụng trong trò chơi:

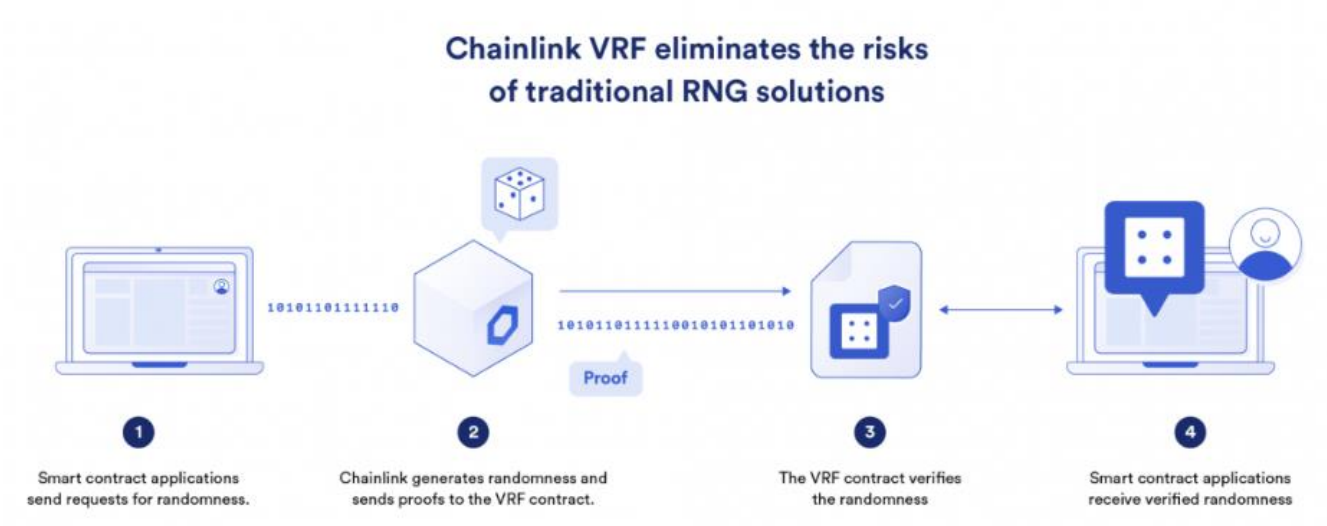
1. Chainlink:

- Chainlink là một mạng lưới Oracle phi tập trung, đóng vai trò là phần mềm trung gian giữa các smart contract và các nguồn dữ liệu bên ngoài, cho phép các smart contract truy cập an toàn vào nguồn dữ liệu ngoài chuỗi
- Hiện tại, Chainlink đang có 6 sản phẩm đóng vai trò cơ sở hạ tầng cho các dự án là:

- Chainlink Functions là một nền tảng phát triển không có máy chủ Web3 cho phép bạn truy xuất bất kỳ dữ liệu nào từ bất kỳ API nào và chạy tính toán tùy chỉnh trên mạng lưới an toàn và đáng tin cậy của Chainlink.
- Điểm nổi bật của Chainlink:
  + Mở rộng trên nhiều blockchain
  + Có nhiều sản phẩm phục vụ cho cộng đồng developer và dự án DeFi (7 sản phẩm)
  + Có nhiều đối tác sử dụng và cung cấp dữ liệu
  + Cung cấp cho nhiều dữ liệu On-chain và yêu cầu VRF

2. Chainlink VRF:

- Chainlink VRF (Chainlink Verifiable Random Function) là một liên kết đã được kiểm chứng và xác minh về tính ngẫu nhiên được sắp xếp chính xác cho các smart contract.
- Cách hoạt động của Chainlink VRF:
  + Smart contract yêu cầu một đối tượng ngẫu nhiên bằng cách cung cấp 1 seed phase cho Chainlink. Seed phase này không thể đoán trước được với các Oracle, nó được sử dụng để tạo ra một số ngẫu nhiên, sau đó được gửi đến hợp đồng thông minh trên chuỗi
  + Mỗi oracle sử dụng khóa bị mật của riêng mình khi tạo ra đối tượng ngẫu nhiên này.
  + Khi kết quả được xuất bản trên chuỗi cùng với một bằng chứng, nó sẽ được xác minh bằng cách sử dụng khóa công khai của oracle và seed phase của ứng dụng
  + Dựa vào khả năng xác minh bằng chứng và chữ kí được chấp nhận rộng rãi của một blockchain, điều này cho phép các hợp đồng chỉ sử dụng tính ngẫu nhiên cũng đã được xác minh bởi cùng một môi trường trên chuỗi đang chạy chính hợp đồng đó.



- Lợi ích của việc sử dụng Chainlink VRF:
  + Tính ngẫu nhiên có thể kiểm chứng
  + Lhi nhiều người dùng sử dụng nó, phí người dùng phải trả cho các node tăng lên, tạo động lực cho các nhà khai thác nút cung cấp càng nhiều đảm bảo an ninh càng tốt.

3. ABI:

- ABI (Application Binary Interface) là một phần rất quan trọng của lập trình trên blockchain. Hầu hết các smart contract trên blockchain được viết bằng Solidity, một ngôn ngữ lập trình đặc biệt cho Ethereum. Khi chúng ta viết một smart contract bằng Solidity, nó sẽ được biên dịch thành mã bytecode, đó là một mã nhị phân các máy ảo của Ethereum có thể hiểu được.
- Tuân thủ ABI (có thể hoặc không thể được chuẩn hóa chính thức) thường là công việc của trình biên dịch, hệ điều hành hoặc tác giả thư viện; tuy nhiên, một lập trình viên ứng dụng có thể phải thao tác trực tiếp với ABI khi viết chương trình bằng nhiều ngôn ngữ lập trình, có thể đạt được bằng cách sử dụng các lệnh gọi hàm bên ngoài.
- Để giao tiếp với một smart contract trên blockchain, chúng ta cần sử dụng ABI. ABI mô tả cách các function trong smart contract có thể được gọi và cách các biến trong smart contract có thể được truy cập. ABI chứa thông tin về tên, kiểu dữ liệu và thứ tự đối số của mỗi function trong smart contract. Vì vậy, khi chúng ta muốn tương tác với smart contract từ một ứng dụng bên ngoài, chúng ta phải sử dụng ABI để xác định cách thức giao tiếp chính xác.

4. Remix IDE:

- Remix IDE là một công cụ online hỗ trợ các bạn muốn lập trình Smart Contract ngay lập tức tại trang web: https://remix.ethereum.org.
- Trang web hỗ trợ bạn tạo file với đuôi .sol.
- Compile với các phiên bản từ cũ nhất đến mới nhất của solidity. Có phần console log các lỗi cú pháp, fomat code,... các cảnh báo và các phần compile thành công
- Hỗ trợ các bạn deploy Smart Contract với
  + JavaScriptVM
  + Injected Web3
  + Web3 Provider
- Nếu việc deploy thành công, bạn hoàn toàn có thể test các function của mình một cách dễ dàng ở phần bên dưới và theo dõi quá trình hoạt động của các transaction với console log.

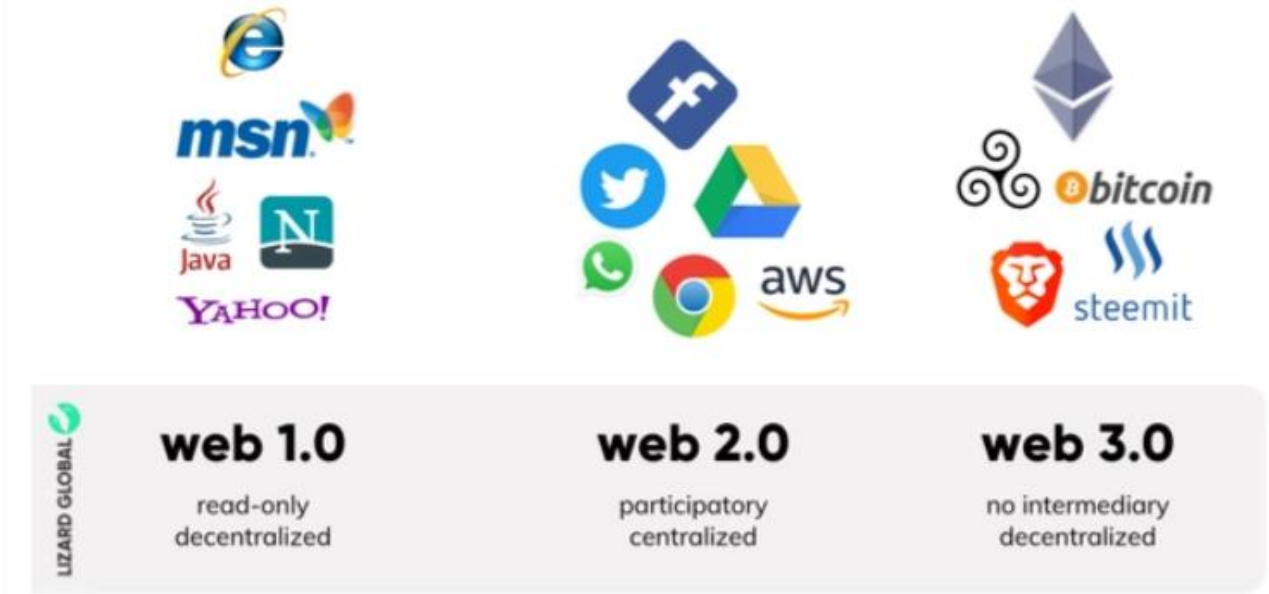
5. Solidity:

- Solidity là một ngôn ngữ lập trình để tạo nên các smart contract (hợp đồng thông minh) trên nền tảng Ethereum. Đây được xem là một nền tảng hợp đồng thông minh phi tập trung hàng đầu trong lĩnh vực crypto. Cơ bản có thể xây dựng NFT marketplace (chợ nghệ thuật kỹ thuật số), Metaverse, sàn giao dịch phi tập trung (DEX), sàn tài chính phi tập trung (DeFi)... trên Ethereum.
- Cách thức hoạt động của Solidity
  + Sau khi các developer viết ra các chương trình, một trong những thành phần quan trọng giúp thực thi Solidity Code là EVM. Nó được mô tả giống như một máy tính ảo trên blockchain, nó giúp biến solidity code của các nhà phát triển thành các ứng dụng chạy trên Ethereum
  + Ở cấp độ cao hơn, Solidity cho phép nhà phát triển ra các "machine level" code có thể thực thi được trên EVM. Sau đó, trình biên dịch chia nhỏ các dòng code mà lập trình viên viết, sẽ biến thành các lệnh mà bộ xử lý có thể hiểu được và thực thi nó.
- Ưu, nhược điểm của Solidity
  + Ưu điểm: Solidity cho phép tạo ra các hợp đồng thông minh một cách an toàn, minh bạch và đáng tin cậy, tăng hiệu quả vận hành hệ thống, giảm chi phí nhân sự và phụ thuộc bên thứ ba.

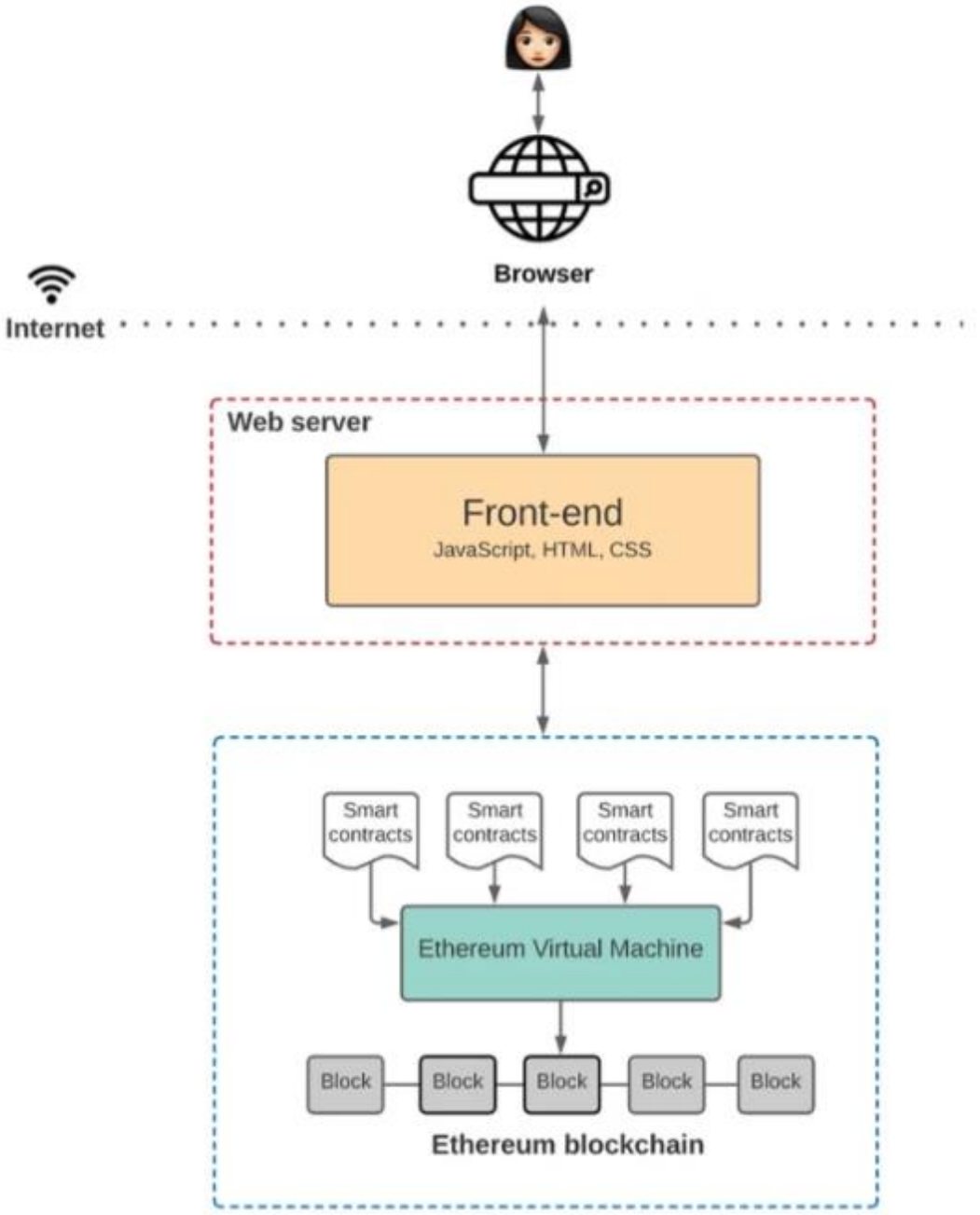
+ Nhược điểm: Không thể thay đổi thông tin.

6. **Web 3.0:**

- Web 3.0 (còn được gọi là web3), là thế hệ thứ ba của các dịch vụ Internet kết nối dữ liệu với nhau theo cách phi tập trung để mang lại trải nghiệm người dùng nhanh hơn và được cá nhân hóa hơn. Web 3.0 được xây dựng bằng trí tuệ nhân tạo (AI), máy học (machine learning) và web ngữ nghĩa (Semantic Web), đồng thời sử dụng hệ thống bảo mật blockchain để giữ cho thông tin được an toàn và bảo mật.



- Đặc điểm:
  + Open: là phần mềm mã nguồn mở
  + Trustless: dữ liệu không đáng tin cậy
  + Permissionless: không cần sự cho phép của tổ chức kiểm soát
  + Ubiquitous: Web 3.0 sẽ cung cấp Internet cho tất cả chúng ta, bất cứ lúc nào và từ bất kỳ vị trí nào
- Cách hoạt động:



- Kiến trúc:
  + Ethereum Blockchain
  + Smart Contracts
  + Máy ảo Ethereum (EVM)
  + Front End
- Ưu, nhược điểm:
  + Ưu điểm:

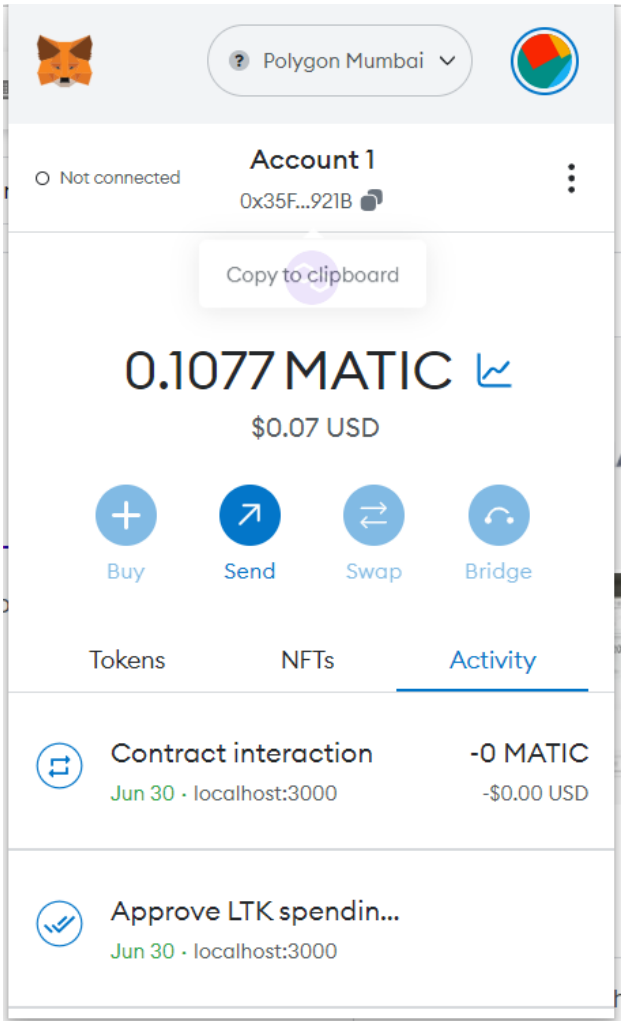
- Quyền riêng tư và kiểm soát dữ liệu
- Dịch vụ liền mạch
- Tính minh bạch
- Khả năng tiếp cận dữ liệu mở
- Nền tảng không hạn chế
- Tạo hồ sơ duy nhất
- Xử lý dữ liệu nâng cao

+ Nhược điểm:

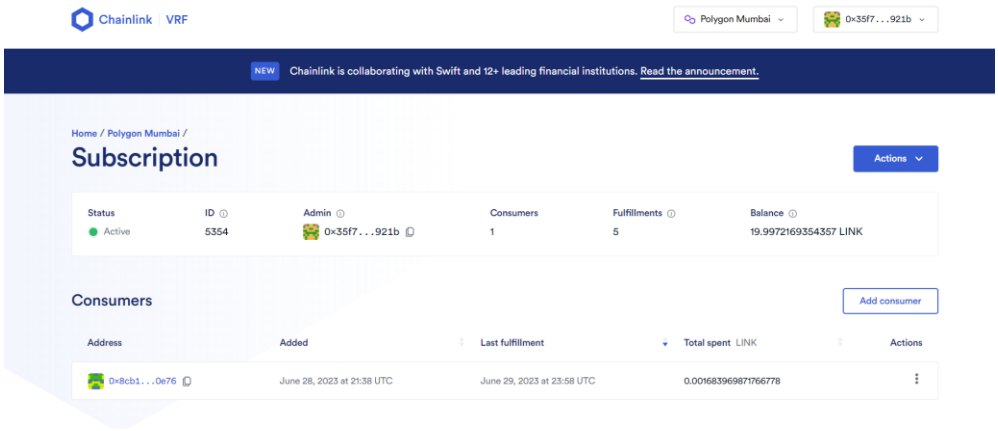
- Yêu cầu thiết bị nâng cao
- Các trang web Web 1.0 sẽ trở nên lỗi thời
- Chưa sẵn sáng cho việc áp dụng rộng rãi
- Nhu cầu về quản lý danh tiếng tăng
- Chức năng phức tạp

III. Quá trình thực hiện:

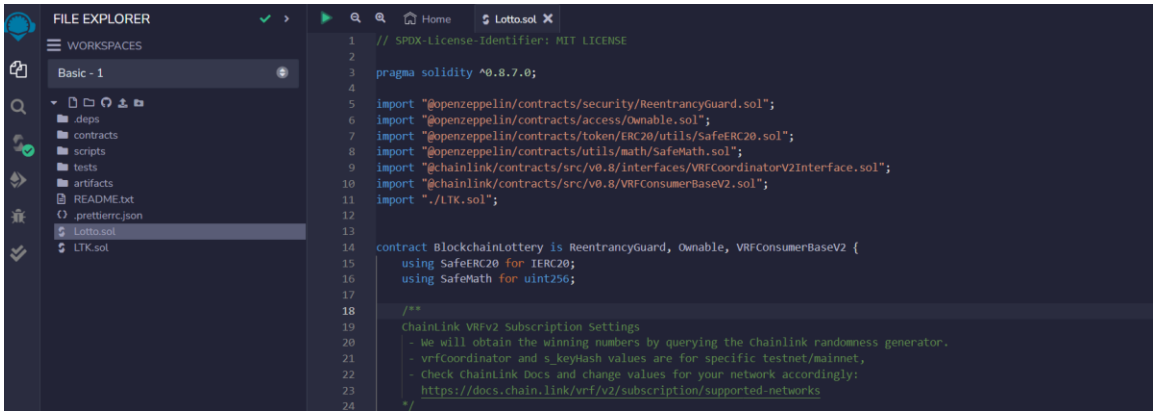
- Vì nhóm quyết định sử dụng ví metamask là nơi giao dịch chính của ứng dụng xổ số cho nên đầu tiên khi mọi người muốn sử dụng ứng dụng cần phải có ví Metamask trên browser của mình.



-
- Đồng thời chuyển network của metamask sang Polygon mumbai(network chính nhóm sẽ sử dụng để deploy và demo)
- Vào lúc này chúng ta cần kiếm 1 ít coin Link cũng như Matic coin để có phí để sử dụng các chức năng của VRF. (có rất nhiều web gửi free coin cho chúng ta, chỉ cần cung cấp địa chỉ ví cho chọ)
- Tiếp theo là kết nối ví với chainlink VRF(bên thứ 3 giúp tạo số ngẫu nhiên) như sau:



- Tùy chọn mạng để subscrip cũng là mạng polygon mumbai và sẽ sử dụng coin LINK như 1 mức phí ảo mỗi lần gọi số ngẫu nhiên.
- Tiếp theo là việc đi viết smart contract cho hệ thống lotto trong web remix có giao diện như sau:

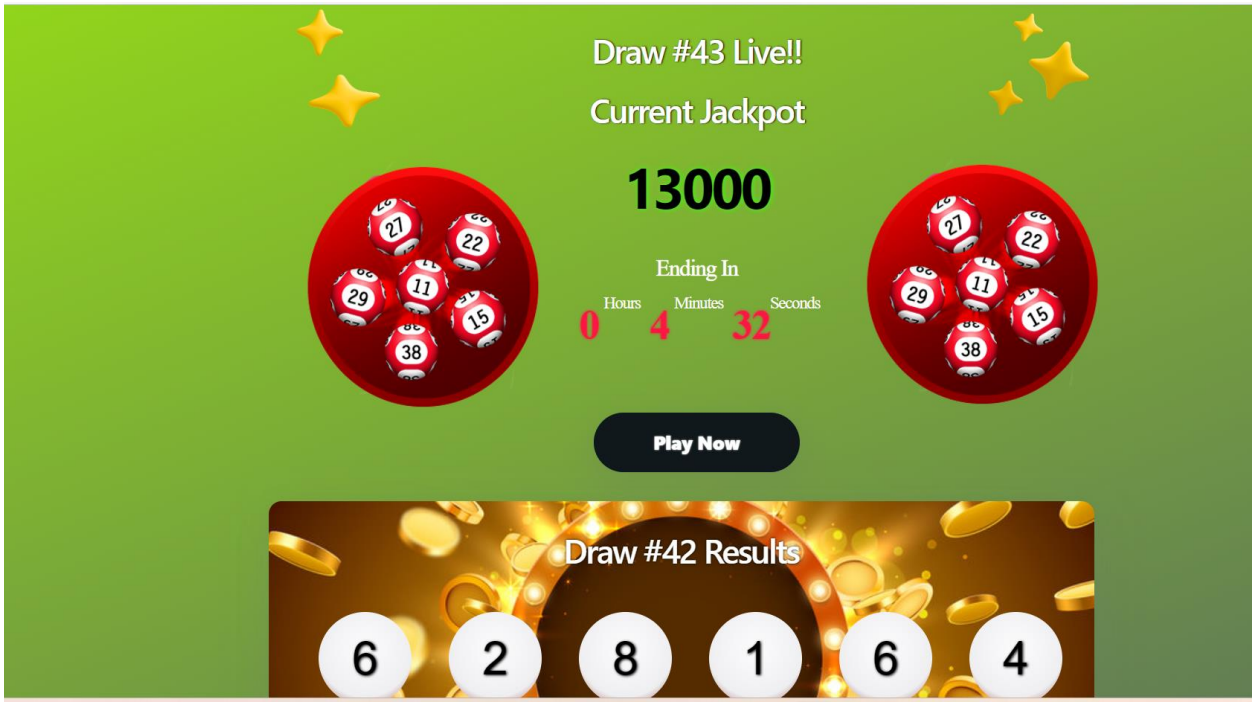


- Ta deploy contract lotto lên và add consumer ở VRF để VRF có thể nhận dạng và lưu trữ contract đó để sau này thực thi việc trả về các function theo ý contract.
- Sau khi đã hoàn thành smart contract và deploy cũng như kiểm thử vài function contract thành công như ý thì tiếp theo ta sẽ lấy ABI(remix hỗ trợ copy đầy đủ ABI) dựa trên các contract đó dưới dạng file json để có thể gọi các contract trong Vscode.

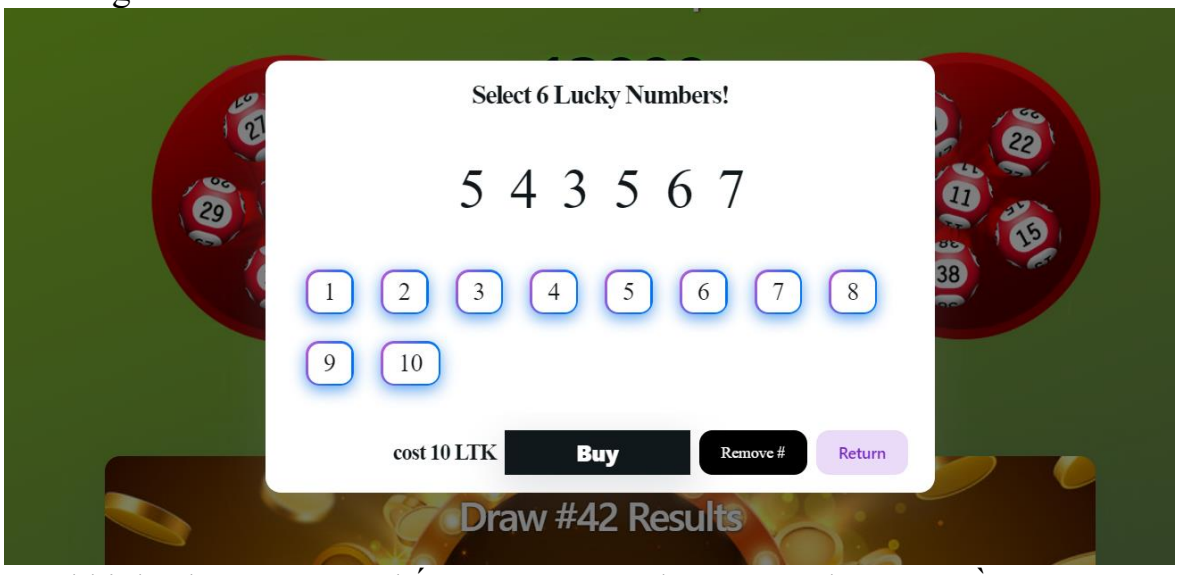
- Sau khi đã có ABI thì nhóm xây dựng BE dựa trên ABI cùng package ether để có thể gọi các contract ở BE.
- Và cuối cùng là nhóm xây dựng FE để có thể test các luồng cơ bản.

IV. Cách sử dụng:

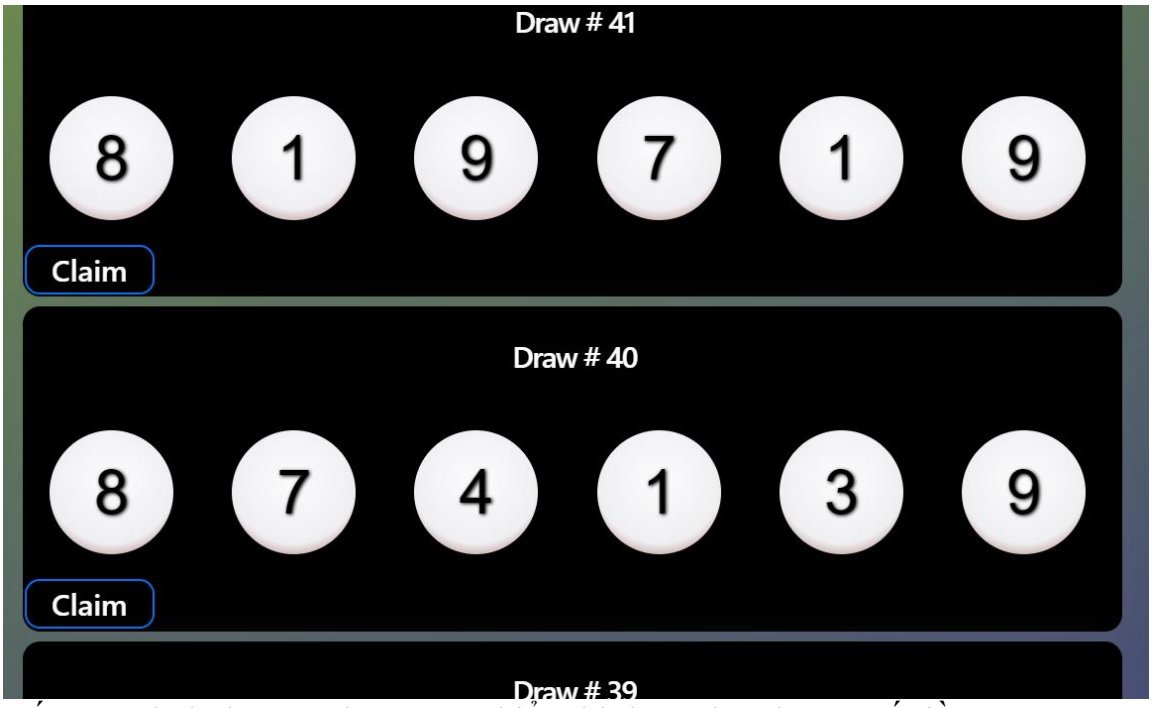
- Giao diện chính của người dùng:



- Web hiển thị đơn giản số tiền thưởng hiện tại, thời gian lần xổ số hiện tại còn lại, các kết quả trúng thưởng gần nhất và 1 nút play đơn giản giúp những người cần chơi có thể chơi
- khi người chơi nhấn play thì sẽ hiển bảng chọn để người chơi chọn 6 số mong muốn:



- Sau khi đã chọn xong sẽ nhấn nút Buy, sau đó metamask sẽ yêu cầu người chơi tốn 10 LTK(coin của xổ số) để mua bộ số này. Người chơi chỉ cần confirm, đợi giao dịch và đã có thể nhận bộ số của mình về.
- Nếu người chơi kiểm tra việc trúng giải dựa trên các kết quả sổ số đã hiển thị chỉ cần nhấn “Claim”



- Nếu người chơi trúng thưởng, sẽ hiển thị thông báo lên và số tiền thưởng sẽ được chuyển về địa chỉ ví metamask của người chơi

V. Cách thực hiện:

- Mở 1 VisualCode bất kì và làm theo sau:
  git clone https://github.com/nhatphi2000/LotteryBlockchain.git
  cd LotteryBlockchain
  cd backend
  node backend.js (chạy backend)
  cd ..
  cd lotery-frontend
  npm run dev (chạy frontend để hiển thị giao diện người chơi)

VI. Tài liệu tham khảo:

- https://coin98.net/chainlink-link
- https://en.wikipedia.org/wiki/Application_binary_interface
- https://coinf.io/chainlink-vrf-la-gi/#:~:text=Chainlink%20VRF%20l%C3%A0%20vi%E1%BA%BFt%20t%E1%BA%AFt,c%C3%A1c%20h%E1%BB%A3p%20%C4%91%E1%BB%93ng%20th%C3%B4ng%20minh.

- https://viblo.asia/p/smart-contract-va-remix-ide-djeZ1RQglWz
- https://bizflycloud.vn/tin-tuc/solidity-la-gi-20220701155424067.htm
- https://bizflycloud.vn/tin-tuc/web-30-la-gi-tim-hieu-chi-tiet-ve-web-30-ky-nguyen-moi-cua-internet-phan-1-20220316164228356.htm
- www.youtube.com/@net2dev
- docs.chain.link/vrf/v2/introduction
- docs.soliditylang.org/en/v0.5.3/abi-spec.html