TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KỲ**

**MÔN BLOCKCHAIN VÀ CÔNG NGHỆ SỔ CÁI PHÂN TÁN**

*Người hướng dẫn*: **GV PHẠM THÁI KỲ TRUUNG**

*Người thực hiện*: **NGUYỄN VĂN HẬU - 52000887**

**LƯƠNG PHAN HOÀN NHÂN - 52000899**

**TRẦN MINH QUÂN - 52000706**

**HUỲNH TIẾN CƯỜNG - 52100777**

Lớp **: 505063**

**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**



**ĐỒ ÁN CUỐI KỲ**

**VOTING CHAIN – HỆ THỐNG BỎ PHIẾU ĐIỆN TỬ**

*Người hướng dẫn*: **GV PHẠM THÁI KỲ TRUUNG**

*Người thực hiện*: **NGUYỄN VĂN HẬU - 52000887**

**LƯƠNG PHAN HOÀN NHÂN - 52000899**

**TRẦN MINH QUÂN - 52000706**

**HUỲNH TIẾN CƯỜNG - 52100777**

Lớp **: 505063**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

LỜI CẢM ƠN

“Lời đầu tiên, xin trân trọng gửi lời cảm ơn đến Thầy Phạm Thái Kỳ Trung đã hướng dẫn nhóm, thầy đã tận tình hướng dẫn nhóm trong suốt quá trình học tập cũng như hoàn thành báo cáo một cách tốt nhất.

Xin chân thành cảm ơn các thầy, cô thuộc khoa công nghệ thông tin trường đại học Tôn Đức Thắng đã tận tình giảng dạy cho chúng tôi trong thời gian học tập.

Xin cảm ơn thầy Phạm Thái Kỳ Trung đã đọc bài báo cáo và cho nhóm những nhận xét ý nghĩa và quý báu, chỉnh sửa những thiếu sót của chúng tôi trong bài.

Do kiến thức và khả năng lý luận của chúng em còn giới hạn và có nhiều thiếu sót, kính mong sự chỉ dẫn và đóng góp của Thầy để bài báo cáo của chúng em được hoàn thiện hơn.”

*Xin chân thành cảm ơn!*

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

Tôi xin cam đoan đây là sản phẩm đồ án của chúng 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 chúng em 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 chúng gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Lương Phan Hoàn Nhân*

*Nguyễn Văn Hậu*

*Trần Minh Quân*

*Huỳnh Tiến Cường*

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)

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc154684491)

[ĐỒ ÁN ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG ii](#_Toc154684492)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc154684493)

[MỤC LỤC 1](#_Toc154684494)

[DANH MỤC HÌNH ẢNH 4](#_Toc154684495)

[DANH MỤC BẢNG BIỂU 6](#_Toc154684496)

[DANH MỤC CÁC CHỮ VIẾT TẮT 7](#_Toc154684497)

[CHƯƠNG 1 - TỔNG QUAN ĐỀ TÀI 8](#_Toc154684498)

[1.1 Yêu cầu. 8](#_Toc154684499)

[1.1.1 Nhóm đề xuất 1 chủ đề tìm về Blockchain hay DLT (Distributed Ledger Technology): 8](#_Toc154684500)

[1.1.2 Cài đặt / triển khai 1 nền tảng Enterprise BlockChain: 8](#_Toc154684501)

[1.2 Lý do chọn đề tài. 8](#_Toc154684502)

[1.3 Mục tiêu. 10](#_Toc154684503)

[1.4 Phạm vi nghiên cứu. 11](#_Toc154684504)

[CHƯƠNG 2 - CƠ SỞ LÝ THUYẾT 14](#_Toc154684505)

[2.1 Hướng phát triển sản phẩm. 14](#_Toc154684506)

[2.1.1 Blockchain. 14](#_Toc154684507)

[2.1.1.1 Định nghĩa Blockchain. 14](#_Toc154684508)

[2.1.1.2 Các loại Blockchain. 15](#_Toc154684509)

[2.1.1.3 Các phiên bản công nghệ Blockchain. 16](#_Toc154684510)

[2.1.1.4 Đặc điểm của Blockchain. 18](#_Toc154684511)

[2.1.1.5 Ưu điểm của Blockchain. 19](#_Toc154684512)

[2.1.1.6 Nhược điểm của Blockchain. 21](#_Toc154684513)

[2.1.1.7 Ứng dụng của công nghệ Blockchain trong cuộc sống. 23](#_Toc154684514)

[2.1.2 Phát triển DApp. 24](#_Toc154684515)

[2.1.2.1 Định nghĩa DApp. 24](#_Toc154684516)

[2.1.2.2 Các thành phần của DApp. 25](#_Toc154684517)

[2.1.2.3 Quy trình hoạt động của DApp. 26](#_Toc154684518)

[2.1.2.4 Lợi ích của DApp. 27](#_Toc154684519)

[2.1.2.5 Hạn chế của DApp. 29](#_Toc154684520)

[2.1.2.6 Ứng dụng trong DApp. 31](#_Toc154684521)

[2.1.3 Ví Metamask. 32](#_Toc154684522)

[2.1.3.1 Metamask là gì? 32](#_Toc154684523)

[2.1.3.2 Ví metamask có an toàn không? 33](#_Toc154684524)

[2.1.3.3 Ưu điểm của ví metamask. 34](#_Toc154684525)

[2.1.3.4 Nhược điểm ví metamask. 36](#_Toc154684526)

[2.1.4 Etherum. 38](#_Toc154684527)

[2.1.4.1 Định nghĩa Etherum. 38](#_Toc154684528)

[2.1.4.2 Cách thức hoạt động của Etherum. 39](#_Toc154684529)

[2.1.4.3 Quá trình thực thi hợp đồng đông minh trên Etherum. 41](#_Toc154684530)

[2.1.4.4 Ưu điểm của Etherum. 42](#_Toc154684531)

[2.2 Hướng lý thuyết. 44](#_Toc154684532)

[2.2.1 So sánh các mạng blockchain phổ biến hiện nay. 44](#_Toc154684533)

[2.2.2 Tổng quan về hệ thống bầu cử truyền thống. 46](#_Toc154684534)

[2.2.2.1 Hệ thống bỏ phiếu điện tử là gì? 46](#_Toc154684535)

[2.2.2.2 Bối cảnh nghiên cứu. 47](#_Toc154684536)

[2.2.2.3 Ưu điểm của bầu cử truyền thống. 48](#_Toc154684537)

[2.2.2.4 Nhược điểm của hệ bầu cử truyền thống. 49](#_Toc154684538)

[2.2.3 Tổng quan về hệ thống bầu cử điện tử. 49](#_Toc154684539)

[2.2.3.1 Ý tưởng nghiên cứu. 49](#_Toc154684540)

[2.2.3.2 Các yếu tố then chốt để xây dựng hệ thống bỏ phiếu điện tử. 50](#_Toc154684541)

[2.2.3.3 Ưu điểm của hệ thống. 52](#_Toc154684542)

[2.2.3.4 Nhược điểm của hệ thống. 54](#_Toc154684543)

[2.2.4 So sánh giữa hệ thống bầu cử truyền thống và hệ thống bầu cử điện tử. 55](#_Toc154684544)

[2.3 Hướng ứng dụng. 57](#_Toc154684545)

[2.3.1 Tiềm năng ứng dụng Blockchain trong bầu cử, kiểm phiếu. 57](#_Toc154684546)

[2.3.2 Xây dựng mô hình hệ thống bỏ phiếu điện tử dựa trên công nghệ Blockchain và đánh giá khả năng ứng dụng. 59](#_Toc154684547)

[CHƯƠNG 3 - PHÂN TÍCH VÀ THIẾT KẾ 61](#_Toc154684548)

[3.1 Tác nhân của hệ thống. 61](#_Toc154684549)

[3.2 Các chức năng và module chính. 62](#_Toc154684550)

[3.3 Luồng hoạt động và quy trình bỏ phiếu. 63](#_Toc154684551)

[3.4 Kiến trúc hệ thống và công nghệ sử dụng. 63](#_Toc154684552)

[3.5 Sơ đồ Usecase tổng quát. 64](#_Toc154684553)

[CHƯƠNG 4 - HIỆN THỰC HÓA HỆ THỐNG 66](#_Toc154684554)

[4.1 Cài đặt thực nghiệm. 66](#_Toc154684555)

[4.2 Kết quả thực nghiệm. 76](#_Toc154684556)

[CHƯƠNG 5 - ĐÁNH GIÁ VÀ KẾT LUẬN 80](#_Toc154684557)

[5.1 Đánh giá chung. 80](#_Toc154684558)

[5.2 Kết luận. 81](#_Toc154684559)

[TÀI LIỆU THAM KHẢO 82](#_Toc154684560)

DANH MỤC HÌNH ẢNH

[Hình 1 – Blockchain là gì? 13](#_Toc154682797)

[Hình 2 – Các loại Blockchain 14](#_Toc154682798)

[Hình 3 – Các phiên bản Blockchain 15](#_Toc154682799)

[Hình 4 – Sáu đặc điểm của Blockchain 17](#_Toc154682800)

[Hình 5 – Ưu điểm của Blockchain 18](#_Toc154682801)

[Hình 6 – Nhược điểm của Blockchain 20](#_Toc154682802)

[Hình 7 – Ứng dụng của công nghệ Blockchain 22](#_Toc154682803)

[Hình 8 – DApp là gì? 23](#_Toc154682804)

[Hình 9 – Các thành phần của DApp 24](#_Toc154682805)

[Hình 10 – Quy trình hoạt động của DApp 25](#_Toc154682806)

[Hình 11 – Lợi ích của DApp 26](#_Toc154682807)

[Hình 12 – Hạn chế của DApp 28](#_Toc154682808)

[Hình 13 – Ứng dụng trong DApp 30](#_Toc154682809)

[Hình 14 – Metamask là gì? 31](#_Toc154682810)

[Hình 15 – Is metamask safe? 32](#_Toc154682811)

[Hình 16 – Ưu điểm ví metamask 33](#_Toc154682812)

[Hình 17 – Nhược điểm metamask 35](#_Toc154682813)

[Hình 18 – Etherum là gì? 37](#_Toc154682814)

[Hình 19 – Etherum hoạt động như thế nào? 38](#_Toc154682815)

[Hình 20 – Ưu điểm của Etherum 41](#_Toc154682816)

[Hình 21 – Các mạng Blockchain phổ biến hiện nay 43](#_Toc154682817)

[Hình 22 – Hệ thống bỏ phiếu điện tử là gì? 45](#_Toc154682818)

[Hình 23 – Ưu điểm hệ thống bỏ phiếu điện tử 51](#_Toc154682819)

[Hình 24 – Nhược điểm của hệ thống bỏ phiếu điện tử 53](#_Toc154682820)

[Hình 25 – So sánh giữa Voting online và Voting offline 54](#_Toc154682821)

[Hình 26 – Sơ đồ usecase tổng quát của hệ thống 63](#_Toc154682822)

[Hình 27 – Tạo Blockchain giả lập với công cụ Ganache 65](#_Toc154682823)

[Hình 28 – Kết nối file “truffle-config.js” 66](#_Toc154682824)

[Hình 29 – Connect dự án trên công cụ Ganache 66](#_Toc154682825)

[Hình 30 – Deploy dự án Voting trên Ganache 67](#_Toc154682826)

[Hình 31 – Address và private key của từng account 68](#_Toc154682827)

[Hình 32 – Download ví Metamask cho Chorme 69](#_Toc154682828)

[Hình 33 – Tạo tài khoản vote 69](#_Toc154682829)

[Hình 34 – Tạo mạng riêng 70](#_Toc154682830)

[Hình 35 – Tạo tài khoản Admin 71](#_Toc154682831)

[Hình 36 – Nhập private key vào tài khoản 71](#_Toc154682832)

[Hình 37 – Thực hiện tương tự với Voter 72](#_Toc154682833)

[Hình 38 – Chạy thực nghiệm dự án 72](#_Toc154682834)

[Hình 39 – Kết nối với ví Metamask 73](#_Toc154682835)

[Hình 40 – Cập nhật các input 74](#_Toc154682836)

[Hình 41 – Input voter 1 74](#_Toc154682837)

[Hình 42 – Input voter 2 75](#_Toc154682838)

[Hình 43 – Input voter 3 75](#_Toc154682839)

[Hình 44 – Bắt đầu Vote 76](#_Toc154682840)

[Hình 45 – Chuyển hướng sang trang voting 76](#_Toc154682841)

[Hình 46 – Chuyển qua tài khoản Voter1 77](#_Toc154682842)

[Hình 47 – Chuyển đổi sang tài khoản ADMIN để dừng voting 77](#_Toc154682843)

[Hình 48 – Kết quả người chiến thắng 78](#_Toc154682844)

DANH MỤC BẢNG BIỂU

[Bảng 1 – Bảng hướng dẫn đề tài 7](#_Toc154682733)

[Bảng 2 – Chi tiết các phiên bản BlockChain 16](#_Toc154682734)

[Bảng 3 – So sánh các mạng blockchain phổ biến hiện nay 45](#_Toc154682735)

[Bảng 4 – Bảng so sánh giữa hệ thống bầu cử truyền thống và hệ thống bầu cử điện tử 56](#_Toc154682736)

[Bảng 5 – Các tác nhân của hệ thống 61](#_Toc154682737)

DANH MỤC CÁC CHỮ VIẾT TẮT

* DApp Decentralized application
* API Application Programming Interface
* GUI Graphical User Interface
* TRON Token Road Network
* DLT Distributed Ledger Technology
* ERC Ethereum Request for Comment
* ICO Initial Coin Offering
* DAOs Decentralized Autonomous Organizations
* PoW Proof of Work

1. TỔNG QUAN ĐỀ TÀI
2. Yêu cầu.
3. Nhóm đề xuất 1 chủ đề tìm về Blockchain hay DLT (Distributed Ledger Technology):

|  |  |  |
| --- | --- | --- |
| **Hướng phát triển sản phẩm** | **Hướng lý thuyết** | **Hướng ứng dụng** |
| 1. Phát triển DApp 2. Phát triển Website cho phép thanh toán bằng Crypto 3. Phát triển Ví lưu trữ Crypto 4. Phát triển game NFT | 1. Tìm hiểu và so sánh các mạng blockchain hiện có 2. So sánh Digital Wallet với Crypto Wallet 3. Bảo mật với Blockchain | 1. Sàn giao dịch Blockchain 2. Áp dụng ML phân tích xu hướng của Crypto 3. Áp dụng Blockchain/DLT vào một Business cụ thể |
| **Kết hợp:**   1. Tìm hiểu các ngành nghề có thể ứng dụng Blockchain/DLT 2. Phát triển sàn giao dịch Crypto 3. …. | | |

Bảng 1 – Bảng hướng dẫn đề tài

1. Cài đặt / triển khai 1 nền tảng Enterprise BlockChain:
   1. Xem ví dụ quá trình cài đặt HyperLedger Fabric (file đính kèm) (<https://hyperledger-fabric.readthedocs.io/en/release-2.2/dev-setup/devenv.html>) hay R3 Corda (<https://training.corda.net/getting-started/set-up-your-computer/>)
   2. Tạo 1 chaincode (smart contract) đơn giản bằng command line / gọi API
   3. Đề xuất 1 bài toán để áp dụng & Tích hợp chain code lên trên Website để giải quyết bài toán này
   4. Các đề xuất khác.
2. Lý do chọn đề tài.

* Hệ thống bỏ phiếu truyền thống thường có quy trình phức tạp và tốn nhiều thời gian. Bước đăng ký, xác thực danh tính, đến điểm bỏ phiếu và đếm phiếu có thể mất nhiều ngày. Hệ thống có thể xảy ra các hành vi gian lận như mua phiếu, làm giả phiếu, hoặc gian lận trong quá trình đếm phiếu. Điều này có thể gây ra sự hoài nghi và không tin tưởng từ phía công chúng. Trong khi đó, công nghệ Blockchain đã nổi lên như một giải pháp tiềm năng để giải quyết những vấn đề này. Blockchain cung cấp tính toàn vẹn dữ liệu, tính bảo mật và tính khả dụng cao, giúp đảm bảo tính minh bạch và tin cậy trong quá trình bỏ phiếu. Vì vậy nhóm em quyết định chọn đề tài này nhằm áp dụng công nghệ Blockchain vào hệ thống bỏ phiếu điện tử nhằm:
  + Tăng tính minh bạch trong quá trình bầu cử. Mọi giao dịch bỏ phiếu, bao gồm cả việc tạo phiếu và xác minh, có thể được ghi lại trên blockchain hoặc hệ thống tương tự. Điều này đảm bảo rằng quá trình bỏ phiếu có thể được kiểm tra và xác minh công khai, giúp đảm bảo tính minh bạch và tin cậy của kết quả bầu cử.
  + Hệ thống bỏ phiếu điện tử đáng tin cậy có thể giảm nguy cơ gian lận trong quá trình bầu cử. Công nghệ blockchain cung cấp tính toàn vẹn dữ liệu và tính bảo mật cao, ngăn chặn sự thay đổi hoặc xóa bỏ phiếu một cách trái phép. Hơn nữa, cơ chế đồng thuận trong blockchain đòi hỏi sự thống nhất của nhiều bên tham gia, làm khó khăn cho việc thao túng kết quả bầu cử.
  + Giúp tiết kiệm chi phí và tài nguyên so với hệ thống bầu cử truyền thống. Việc tổ chức và thực hiện quá trình bầu cử truyền thống đòi hỏi nhiều nhân lực và tài chính. Trong khi đó, hệ thống bỏ phiếu điện tử có thể tự động hóa một số hoạt động và loại bỏ các bước trung gian không cần thiết, giảm thiểu chi phí và tăng hiệu quả.
  + Mang lại tính tiện lợi và tốc độ cao hơn cho cử tri. Người dùng có thể bỏ phiếu từ xa, mọi lúc mọi nơi thông qua các thiết bị kết nối internet. Điều này giúp tăng sự tham gia và tạo thuận lợi cho những người không thể tham gia bầu cử truyền thống do giới hạn thời gian hoặc vị trí địa lý.
  + Xây dựng hệ thống bỏ phiếu điện tử đáng tin cậy và minh bạch giúp tăng độ tin cậy và niềm tin của cử tri vào quá trình bầu cử. Việc sử dụng công nghệ hiện đại và cơ chế đồng thuận trong hệ thống giúp đảm bảo tính công bằng, bảo mật và minh bạch, tạo ra một môi trường tin cậy cho việc bỏ phiếu và đếm phiếu.

1. Mục tiêu.

* Mục tiêu quan trọng nhất để thực hiện đồ án đó là đảm bảo tính minh bạch trong quá trình bỏ phiếu. Hệ thống bỏ phiếu điện tử nên được thiết kế để ghi lại mọi giao dịch bỏ phiếu, từ việc tạo phiếu cho đến quá trình xác minh, một cách công khai và dễ dàng kiểm tra. Điều này giúp đảm bảo rằng quá trình bỏ phiếu không bị thao túng và kết quả bầu cử là minh bạch và đáng tin cậy.
* Thứ hai, đảm bảo tính bảo mật của hệ thống bỏ phiếu điện tử. Hệ thống phải có các biện pháp bảo mật mạnh mẽ để ngăn chặn cuộc tấn công và đảm bảo rằng dữ liệu bỏ phiếu không bị thay đổi hoặc xem trộm. Các biện pháp bảo mật như mã hóa dữ liệu, xác thực đa yếu tố và kiểm soát truy cập phải được áp dụng để bảo vệ thông tin phiếu bầu và đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập.
* Thứ ba, đảm bảo tính công bằng và chính xác trong quá trình bỏ phiếu. Hệ thống phải đảm bảo rằng mỗi phiếu bầu được đếm chính xác và không bị gian lận. Cơ chế đồng thuận và xác thực phiếu bầu phải được thiết kế sao cho công bằng và đáng tin cậy. Đồng thời, hệ thống phải giúp ngăn chặn và phát hiện các hành vi gian lận như phiếu bầu giả mạo, bỏ phiếu nhiều lần hoặc bỏ phiếu dưới áp lực.
* Thứ tư, tạo ra một hệ thống bỏ phiếu điện tử tiện lợi và tốc độ cao. Cử tri nên có khả năng bỏ phiếu từ xa thông qua các thiết bị kết nối internet, giúp tăng sự tham gia và thuận lợi cho những người không thể tham gia bầu cử truyền thống. Hệ thống cũng nên được thiết kế để xử lý số lượng lớn phiếu bầu một cách nhanh chóng và hiệu quả.
* Cuối cùng, tạo niềm tin và chấp nhận từ cử tri đối với hệ thống bỏ phiếu điện tử. Hệ thống phải được thiết kế và triển khai sao cho cử tri có niềm tin vào tính công bằng, tính toàn vẹn và tính minh bạch của quá trình bỏ phiếu. Việc tạo niềm tin này có thể được đạt được thông qua việc đảm bảo sự tham gia của các bên liên quan, cung cấp thông tin minh bạch và đáng tin cậy và chấp nhận một kiểm định và giám sát nghiêm ngặt từ các tổ chức độc lập.

1. Phạm vi nghiên cứu.

* Hệ thống dự kiến triển khai dành cho bầu cử quy mô nhỏ (hội đoàn thể, khu phố, cơ quan...) với số lượng cử tri giả định khoảng 100-500 người thì cần xem xét các khía cạnh sau:
* *Thiết kế và triển khai giao thức bỏ phiếu điện tử trên blockchain Ethereum*: Phạm vi này tập trung vào việc phát triển và triển khai hệ thống bỏ phiếu điện tử dựa trên blockchain Ethereum và ngôn ngữ Solidity. Điều này bao gồm việc thiết kế và triển khai các hợp đồng thông minh để quản lý danh sách cử tri, quá trình bỏ phiếu, xác minh và lưu trữ phiếu bầu trên blockchain.
* *Xác thực cử tri*: Phạm vi này đảm bảo chỉ những cử tri được ủy quyền mới có thể tham gia bỏ phiếu. Ta có thể triển khai các biện pháp xác thực như xác thực danh tính thông qua thông tin cá nhân, số điện thoại hoặc địa chỉ email. Điều này đảm bảo tính chính xác và đáng tin cậy của quy trình bỏ phiếu.
* *Bảo mật và riêng tư*: Phạm vi này tập trung vào đảm bảo tính bảo mật của dữ liệu bỏ phiếu và thông tin cá nhân của cử tri. Ta có thể áp dụng mã hóa dữ liệu phiếu bầu, sử dụng chứng chỉ số hoặc các phương pháp bảo vệ khác để ngăn chặn truy cập trái phép và đảm bảo tính riêng tư.
* *Giao diện người dùng*: Phạm vi này liên quan đến thiết kế giao diện người dùng (GUI) để cử tri có thể dễ dàng tham gia và bỏ phiếu. Giao diện nên đơn giản, trực quan và dễ sử dụng. Có thể bao gồm các chức năng như tạo tài khoản, đăng nhập, xem thông tin ứng cử viên và bỏ phiếu trong giao diện người dùng.
* *Quản lý quy trình bỏ phiếu*: Phạm vi này tập trung vào quy trình bỏ phiếu, bao gồm tạo phiếu bầu, xác minh và ghi nhận phiếu bầu. Ta cần đảm bảo rằng quy trình bỏ phiếu được thực hiện một cách minh bạch, chính xác và không thể thao túng.
* *Đánh giá hiệu suất và khả năng mở rộng*: Phạm vi này liên quan đến đánh giá hiệu suất của hệ thống bỏ phiếu điện tử. Ta có thể thử nghiệm và đánh giá khả năng xử lý số lượng phiếu bầu lớn và tải trọng cao. Đồng thời, hệ thống cũng cần đảm bảo tính ổn định và khả năng mở rộng khi số lượng cử tri tăng lên.
* *Đảm bảo tính minh bạch và đáng tin cậy*: Phạm vi này tập trung vào đảm bảo tính minh bạch và đáng tin cậy của quá trình bỏ phiếu. Hệ thống cần ghi lại mọi giao dịch bỏ phiếu trên blockchain và đảm bảo rằng kết quả bầu cử là công khai và có thể kiểm tra được.
* *Đánh giá và so sánh với hệ thống truyền thống*: Phạm vi này liên quan đếntriển khai và so sánh hệ thống bầu cử điện tử với hệ thống bầu cử truyền thống. Ta có thể tiến hành một nghiên cứu so sánh để đánh giá hiệu quả, tính bảo mật, tính minh bạch và sự thuận tiện của hệ thống bầu cử điện tử so với phương pháp truyền thống.

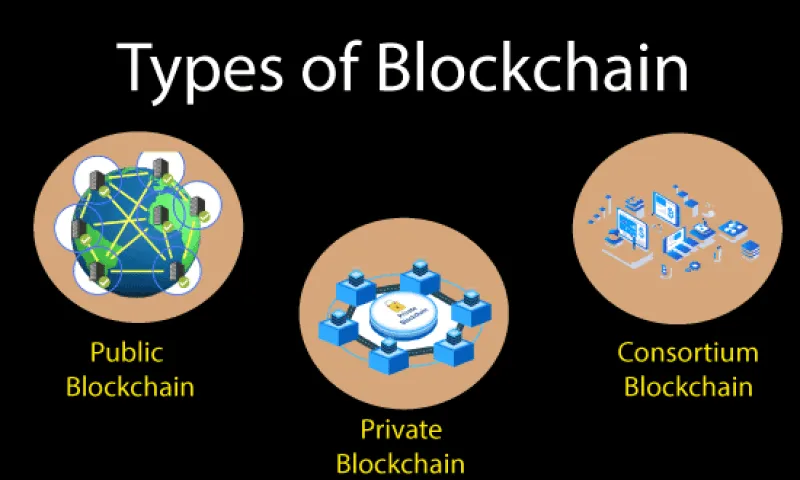
1. CƠ SỞ LÝ THUYẾT
2. Hướng phát triển sản phẩm.
3. Blockchain.
4. Định nghĩa Blockchain.



Hình 1 – Blockchain là gì?

* Blockchain là một công nghệ phi tập trung và phân tán, dựa trên một hệ thống mạng lưới các máy tính (nodes) hoạt động cùng nhau để xác nhận và ghi nhận các giao dịch. Nó được thiết kế để ghi lại các giao dịch và thông tin theo cách không thể sửa đổi hoặc gian lận. Hiểu theo nghĩa đơn giản, Blockchain giống như một cuốn sổ cái, tại đó thông tin sẽ được chứa đựng trong các khối (Block), các Block sẽ được liên kết với nhau bằng “mã hóa”, lớn dần theo thời gian và tạo thành một chuỗi (Chain).
* Một blockchain là một chuỗi liên kết các khối (blocks), trong đó mỗi khối chứa một tập hợp các giao dịch được xác nhận. Mỗi khối được liên kết với khối trước đó thông qua một cơ chế gọi là "mã băm" (hash), tạo thành một chuỗi không thể thay đổi dễ dàng.
* Các khối trong hệ thống BlockChain có sự liên kết với nhau, khối sau sẽ liên kết với khối trước, chứa thông tin về thời gian tạo khối kèm theo một dữ liệu giao dịch kèm mã thời gian tương ứng. **Công nghệ Blockchain** được tạo ra để đảm bảo độ an toàn, chống lại những thay đổi, gian lận dữ liệu bởi không có bất kỳ cách nào có thể thay đổi, thêm hay bớt dữ liệu trong Blockchain.

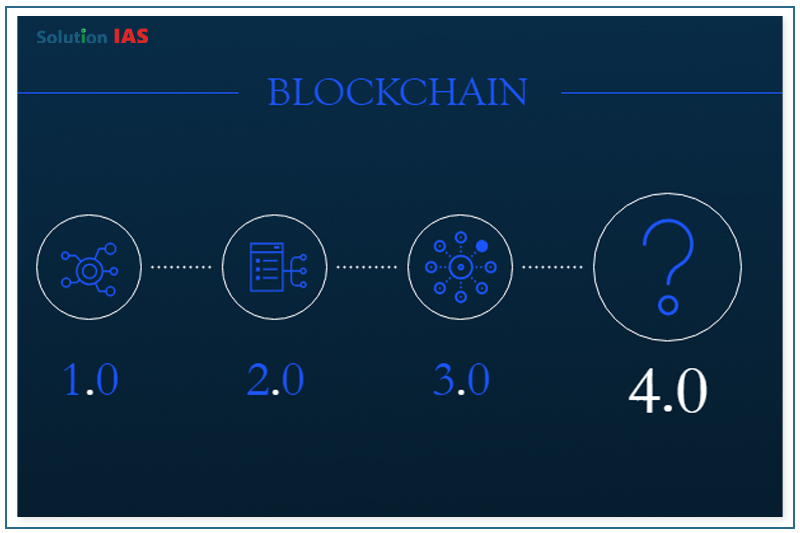
1. Các loại Blockchain.



Hình 2 – Các loại Blockchain

* *Public*: Bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có rất nhiều nút tham gia. Vì vậy, muốn tấn công được vào hệ thống Blockchain này cần chi phí rất lớn và thực sự không khả thi. Ví dụ: Bitcoin, Ethereum,…
* *Private*: Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.
* *Permissioned (hay còn gọi là Consortium):* Một dạng của Private nhưng bổ sung thêm 1 số tính năng khác, đây là sự kết hợp giữa Public và Private. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

1. Các phiên bản công nghệ Blockchain.



Hình 3 – Các phiên bản Blockchain

|  |  |  |
| --- | --- | --- |
| **Phiên bản** | **Đối tượng** | **Chi tiết** |
| **Blockchain 1.0** | - Tiền tệ.  - Thanh toán. | - Blockchain 1.0 được ứng dụng chủ yếu trong tiền mã hóa. Phiên bản này gồm việc kiều hối, chuyển đổi tiền tệ, đồng thời tạo hệ thống thanh toán kỹ thuật số.  - Hay nói cách khác, Blockchain 1.0 giúp những giao dịch tiền ảo trở nên phi tập trung, diễn ra minh bạch, nhanh chóng. |
| **Blockchain 2.0** | - Tài chính.  - Thị trường. | - Blockchain 2.0 ứng dụng trong việc xử lý tài chính, cũng như ngân hàng(trái phiếu, cổ phiếu, nợ, chứng khoán,…).  - Điểm nổi bật của phiên bản này đó chính là được nâng cấp Smart Contract(hợp đồng thông minh). Đây chính là hợp đồng lập trình sẵn, được ký kết giữa các bên tham gia và giám sát chặt chẽ.  - Smart Contract không bị can thiệp bởi các bên thứ 3. Điều này giúp bảo đảm được tính bảo mật ở mức cao nhất. |
| **Blockchain 3.0** | - Thiết kế.  - Giám sát hoạt động. | - Blockchain 3.0 chính là sự kết hợp giữa Smart Contract(Blockchain 2.0) cùng Dapp(ứng dụng phân tán)– nơi dữ liệu được lưu tại kho lưu trữ phi tập trung và được viết bởi ngôn ngữ lập trình.  - Không chỉ phục vụ cho tài chính, phiên bản này còn hướng tới nhiều lĩnh vực khác như giáo dục, Y tế, nghệ thuật hay chính phủ. |
| **Blockchain 4.0** | Doanh nghiệp | - Blockchain 4.0 phát triển tập trung chủ yếu vào các công ty/ doanh nghiệp. Chúng giúp tạo và chạy những ứng dụng giao dịch hiệu quả, an toàn và nhanh chóng hơn.  - Một doanh nghiệp dù mới thành lập vẫn có thể phát triển được ứng dụng phân quyền nhờ Blockchain 4.0.  - Công ty có thể quyết định tới những dữ liệu mà tài khoản được xem nào đó. Tuy nhiên vẫn bảo đảm tính bảo mật, đồng thời không sửa đổi được thông tin, khả năng lưu trữ tự động khi thực hiện giao dịch và thanh toán. |

Bảng 2 – Chi tiết các phiên bản BlockChain

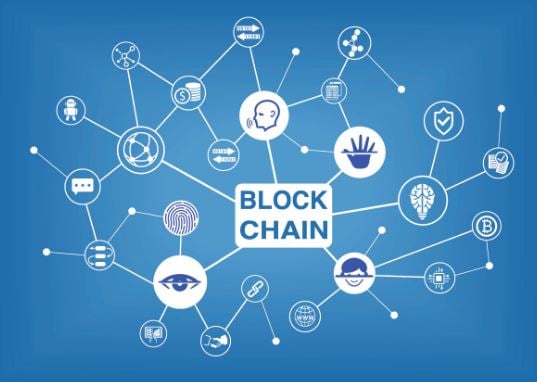
1. Đặc điểm của Blockchain.



Hình 4 – Sáu đặc điểm của Blockchain

* *Phi tập trung*: Không có một tổ chức hoặc cá nhân nào kiểm soát toàn bộ dữ liệu, giao dịch. Dữ liệu được phân tán trên nhiều nút mạng, mỗi nút có bản sao riêng của toàn bộ dữ liệu.
* *An toàn*: Dữ liệu trong blockchain được bảo vệ bằng mã hóa và chữ ký số. Điều đó giúp đảm bảo tính bảo mật của dữ liệu và tránh việc gian lận hoặc sửa đổi.
* *Minh bạch*: Dữ liệu trên Blockchain luôn được ghi lại một cách công khai. Và nó không thể bị xóa hoặc thay đổi, bảo đảm tính minh bạch của hệ thống.
* *Xác thực*: Giao dịch trong Blockchain được xác nhận bởi nhiều nút mạng khác nhau. Nó như các lớp bảo vệ, giúp đảm bảo tính chính xác và xác thực của giao dịch.
* *Tính khả dụng*: Blockchain hoạt động liên tục 24/7 với sự tham gia của nhiều nút mạng khác nhau. Điều này giúp tăng tính khả dụng và ổn định của hệ thống.
* *Không thể sửa đổi*: Khi một khối đã được thêm vào Blockchain, nó không thể bị sửa đổi hoặc xóa bỏ. Nếu thông tin bị thay đổi tất cả mọi người đều sẽ nhanh chóng phát hiện được.

1. Ưu điểm của Blockchain.



Hình 5 – Ưu điểm của Blockchain

Blockchain mang lại nhiều ưu điểm quan trọng, gồm:

* Bảo mật: Blockchain sử dụng mã hóa mạnh và cơ chế xác thực mạnh mẽ để bảo vệ dữ liệu. Mỗi khối trong blockchain được liên kết với khối trước đó thông qua mã băm, tạo ra tính không thể thay đổi và không thể xóa của dữ liệu đã được ghi vào blockchain.
* Tính phi tập trung: Blockchain là một mạng lưới phân tán trong đó dữ liệu và quyết định không tập trung vào một đơn vị duy nhất. Thay vì phụ thuộc vào một tổ chức trung gian, các nodes trong mạng lưới chia sẻ cùng một bản sao của blockchain và tham gia vào việc xác nhận giao dịch và quản lý mạng lưới.
* Minh bạch: Mọi giao dịch và hoạt động trên blockchain được ghi lại và công khai. Điều này tạo ra tính minh bạch, cho phép bất kỳ ai kiểm tra và xem thông tin trên blockchain. Tính minh bạch này có thể đóng vai trò quan trọng trong các ngành công nghiệp như tài chính, chuỗi cung ứng, và bỏ phiếu điện tử.
* An toàn: Vì blockchain là một mạng lưới phân tán, không có một điểm duy nhất mà hacker có thể tấn công để thay đổi dữ liệu. Để thay đổi một khối trong blockchain, hacker sẽ cần kiểm soát hơn 50% sức mạnh tính toán của mạng lưới, điều này rất khó khăn và tốn kém. Do đó, blockchain mang lại tính an toàn cao và khả năng chống lại các cuộc tấn công.
* Tính toàn vẹn dữ liệu: Mỗi khối trong blockchain chứa mã băm của khối trước đó, tạo thành một chuỗi liên kết không thể thay đổi. Điều này đảm bảo tính toàn vẹn của dữ liệu trong blockchain, và không cho phép bất kỳ sửa đổi hay xóa bỏ nào diễn ra một khi đã được ghi vào blockchain.
* Tốc độ và hiệu suất: Mặc dù vẫn còn một số thách thức về tốc độ và hiệu suất trong một số phiên bản blockchain công cộng, nhưng blockchain cũng đã phát triển các công nghệ như Lightning Network và sharding để cải thiện khả năng mở rộng và xử lý giao dịch nhanh hơn.

1. Nhược điểm của Blockchain.

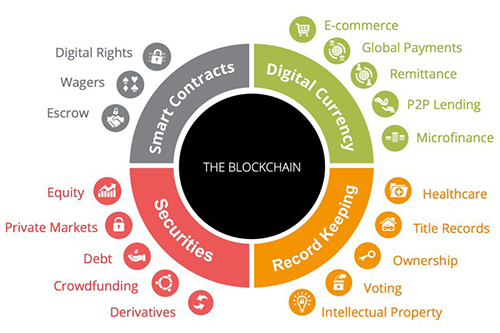


Hình 6 – Nhược điểm của Blockchain

Mặc dù blockchain mang lại nhiều ưu điểm, nhưng cũng có một số nhược điểm cần được lưu ý:

* Tốn kém về năng lượng và tính toán: Quá trình khai thác (mining) trong blockchain công cộng đòi hỏi sự tiêu tốn năng lượng lớn và sức mạnh tính toán cao. Việc giải quyết các bài toán số học phức tạp để tạo khối mới yêu cầu các thiết bị mạnh mẽ và tiêu thụ năng lượng đáng kể, gây ra vấn đề về môi trường và tài nguyên.
* Tốc độ và khả năng mở rộng: Blockchain công cộng có thể gặp khó khăn trong việc xử lý một lượng lớn giao dịch cùng một lúc. Quá trình xác nhận giao dịch và đồng thuận trên toàn mạng lưới có thể tốn thời gian và làm giới hạn khả năng mở rộng của blockchain. Một số công nghệ như Lightning Network và sharding đang được phát triển để giải quyết vấn đề này, nhưng vẫn còn sự cần thiết để tăng cường hiệu suất và tốc độ của blockchain.
* Quyền riêng tư: Mặc dù blockchain cung cấp tính bảo mật cao với việc sử dụng mã hóa mạnh, thông tin trên blockchain công cộng vẫn là công khai và có thể được truy cập bởi bất kỳ ai. Điều này có thể gây ra vấn đề liên quan đến quyền riêng tư và bảo mật dữ liệu, đặc biệt khi áp dụng trong các ngành công nghiệp nhạy cảm như y tế hoặc tài chính.
* Cập nhật và thay đổi: Một blockchain đã được tạo ra và hoạt động trong một thời gian dài có thể gặp khó khăn khi cần thay đổi quy tắc hoặc cập nhật phần mềm. Sự thay đổi này có thể gây ra sự không đồng thuận trong mạng lưới và tạo ra bifurcation (phân chia) trong blockchain, tạo ra một loạt các phiên bản khác nhau và làm mất tính đồng nhất của dữ liệu.
* Phụ thuộc vào kết nối mạng: Blockchain đòi hỏi các nodes trong mạng lưới phải kết nối và giao tiếp với nhau để trao đổi thông tin và xác nhận giao dịch. Nếu một số nodes mất kết nối hoặc không tham gia đủ, có thể gây ra sự gián đoạn hoặc yếu điểm trong mạng lưới.
* Vấn đề pháp lý và quy định: Blockchain đặt ra nhiều thách thức pháp lý và quy định. Sự phổ biến và ứng dụng rộng rãi của blockchain đang đối mặt với việc định rõ quyền và trách nhiệm pháp lý, bảo vệ người dùng và đảm bảo tuân thủ các quy định tài chính, bảo mật và quyền riêng tư.

1. Ứng dụng của công nghệ Blockchain trong cuộc sống.



Hình 7 – Ứng dụng của công nghệ Blockchain

* 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)

1. Phát triển DApp.
2. Định nghĩa DApp.



Hình 8 – DApp là gì?

* DApp (Decentralized application) - ứng dụng phi tập trung là một ứng dụng có thể hoạt động tự chủ, thường thông qua việc sử dụng hợp đồng thông minh, chạy trên hệ thống điện toán phi tập trung, chuỗi khối hoặc hệ thống sổ cái phân tán khác. Giống như các ứng dụng truyền thống, DApp cung cấp một số chức năng hoặc tiện ích cho người dùng. Nó là một loại ứng dụng máy tính được xây dựng và triển khai trên nền tảng blockchain phi tập trung. Điểm đặc biệt của DApp là nó hoạt động dựa trên các hợp đồng thông minh (smart contracts) có tính tự thực thi và không cần sự can thiệp từ bên thứ ba.
* Trong một DApp, dữ liệu và logic của ứng dụng được lưu trữ và thực thi trên mạng lưới blockchain thay vì trên một máy chủ trung tâm. Các giao dịch và hoạt động của DApp được kiểm tra và xác nhận bởi các nút mạng trong mạng lưới blockchain, đảm bảo tính toàn vẹn và minh bạch.

1. Các thành phần của DApp.



Hình 9 – Các thành phần của DApp

* *Giao thức Blockchain*: DApp được xây dựng trên một giao thức blockchain cụ thể như Ethereum, EOS, hoặc TRON. Giao thức này cung cấp cơ sở hạ tầng để lưu trữ và xử lý thông tin của DApp.
* *Hợp đồng thông minh (Smart contracts)*: DApp sử dụng các hợp đồng thông minh để định nghĩa các quy tắc và điều kiện trong ứng dụng. Hợp đồng thông minh là các đoạn mã tự thực thi và không thể thay đổi, giúp đảm bảo tính toàn vẹn và đáng tin cậy của các giao dịch.
* *Giao diện người dùng (User Interface)*: DApp thường có một giao diện người dùng tương tác, cho phép người dùng truy cập và sử dụng ứng dụng thông qua trình duyệt web hoặc ứng dụng di động. Giao diện này có thể cung cấp các chức năng và tương tác với hợp đồng thông minh và blockchain.
* *Token và kinh tế của DApp*: Một số DApp sử dụng token hoặc tiền điện tử để thực hiện các giao dịch và khuyến khích sự tham gia của người dùng. Token trong DApp có thể có các chức năng khác nhau, như đại diện cho quyền sử dụng dịch vụ, đại diện cho giá trị, hoặc tham gia vào cơ chế thưởng.

1. Quy trình hoạt động của DApp.



Hình 10 – Quy trình hoạt động của DApp

* DApp vẫn còn mới trong nền công nghệ hiện nay, nên các ứng dụng của nó vẫn còn giới hạn trong phân khúc tài chính phi tập trung (DeFi). Quy trình làm việc của DApp gồm các bước:
* DApp chạy trên Backend, thường là trên Smart Contract
* Nếu các yêu cầu trong Smart Contract được đáp ứng, giao dịch diễn ra sẽ được ghi lại, lưu trữ và phân phối vĩnh viễn trên một sổ cái công khai.
* Sổ cái công khai sẽ hạn chế sửa đổi với chức năng bảo mật và mật mã độc đáo giúp DApp không thể phá hủy.
* Ngược lại, nếu yêu cầu trên Smart Contract không được đáp ứng, giao dịch sẽ trở về trạng thái ban đầu.

1. Lợi ích của DApp.



Hình 11 – Lợi ích của DApp

* *Tính phi tập trung:* DApp hoạt động trên nền tảng blockchain hoặc các hệ thống phân tán khác, loại bỏ nhu cầu về một bên thứ ba trung gian. Điều này mang lại tính phi tập trung, không cần phụ thuộc vào một tổ chức trung gian duy nhất và giúp giảm bớt các rủi ro liên quan đến việc tin tưởng và phụ thuộc vào một bên thứ ba.
* *Tính minh bạch và công khai*: DApp sử dụng công nghệ blockchain, trong đó thông tin được ghi lại và xác minh bởi một mạng lưới các nút phân tán. Điều này tạo ra tính minh bạch và công khai, vì mọi người có thể xem xét và xác minh các giao dịch và sự thay đổi dữ liệu trên blockchain. Điều này đảm bảo tính trung thực và tăng cường niềm tin trong hệ thống.
* *An ninh và bảo mật*: DApp sử dụng mã hóa và chữ ký số để bảo vệ dữ liệu và giao dịch. Do dữ liệu được phân tán trên nhiều nút và mỗi khối được liên kết bằng mã hóa, việc thay đổi dữ liệu trở nên rất khó khăn và không thể chỉnh sửa. Điều này tạo ra một môi trường an toàn và bảo mật cho việc lưu trữ và truyền tải thông tin.
* *Tính linh hoạt và khả năng mở rộng*: DApp có thể được phát triển và triển khai trên nhiều nền tảng blockchain khác nhau. Việc sử dụng giao thức và tiêu chuẩn chung giữa các blockchain cho phép tính linh hoạt và khả năng mở rộng. Nó cũng cho phép tương tác và tích hợp giữa các ứng dụng khác nhau trên cùng một mạng lưới blockchain.
* *Quyền sở hữu và kiểm soát dữ liệu*: Với DApp, người dùng có quyền sở hữu và kiểm soát dữ liệu của mình. Thay vì gửi dữ liệu cho các bên trung gian, người dùng có thể lưu trữ và quản lý dữ liệu của mình trên blockchain. Điều này giúp giảm bớt rủi ro về việc lộ thông tin cá nhân và tạo ra một môi trường tự do hơn cho người dùng.
* *Tính khả tra và theo dõi*: Do các giao dịch được ghi lại trên blockchain, DApp mang lại khả năng khả tra và theo dõi cao. Tất cả các giao dịch và sự thay đổi dữ liệu được lưu trữ và có thể được truy xuất một cách dễ dàng. Điều này hữu ích trong việc giám sát và xác minh các hoạt động và quy trình kinh doanh.
* *Kiểm duyệt miễn phí*: DApp được phát triển bởi một nhà phát triển và được quản lý bởi cộng đồng người dùng. Không có thực thể nào trên mạng có thể chặn người dùng giao dịch, triển khai DApp và đọc dữ liệu từ Blockchain.

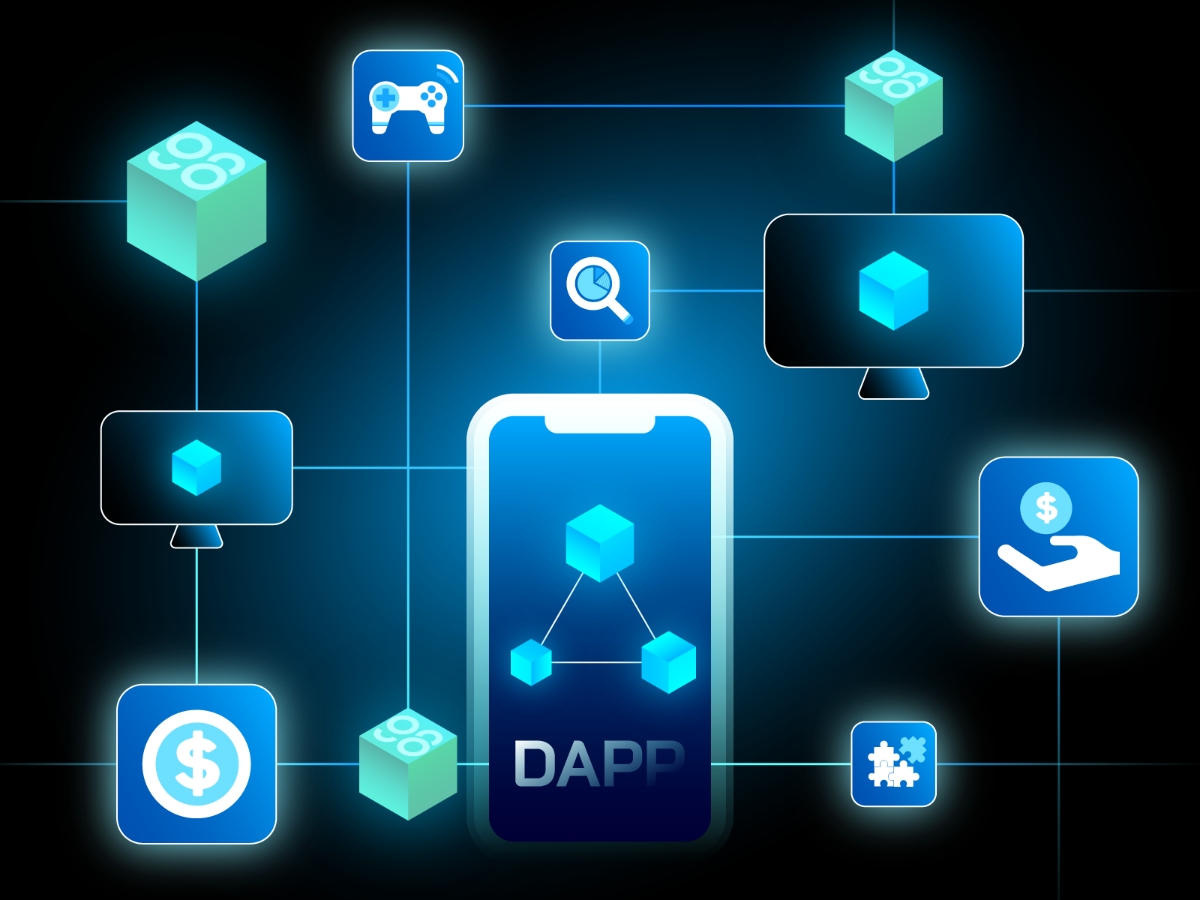
1. Hạn chế của DApp.



Hình 12 – Hạn chế của DApp

* *Tốc độ xử lý chậm*: Do việc xử lý và xác minh các giao dịch trên blockchain phải thông qua quá trình khai thác mỏ hoặc xác minh giao dịch, nên tốc độ xử lý của DApp thường chậm hơn so với các ứng dụng truyền thống. Việc xử lý chậm này có thể làm hạn chế khả năng mở rộng và hiệu suất của DApp trong một số trường hợp sử dụng.
* *Chi phí giao dịch*: Việc thực hiện các giao dịch trên blockchain đòi hỏi phải trả các khoản phí giao dịch cho các nút mạng tham gia quá trình xác minh và khai thác. Điều này có thể tạo ra chi phí cao cho người dùng và là một rào cản đối với việc sử dụng DApp trong một số trường hợp sử dụng với giao dịch hàng ngày nhỏ.
* *Quy mô mạng lưới*: DApp phụ thuộc vào mạng lưới blockchain hoặc hệ thống phân tán khác để hoạt động. Sự phát triển và mở rộng của DApp có thể bị hạn chế bởi quy mô và khả năng mở rộng của mạng lưới đó. Nếu mạng lưới không đủ mạnh mẽ hoặc không đáp ứng được lưu lượng giao dịch, DApp có thể gặp khó khăn trong việc đáp ứng nhu cầu người dùng.
* *Giao diện người dùng phức tạp*: Một số DApp có giao diện người dùng phức tạp và khó sử dụng đối với người dùng thông thường. Việc tương tác với các khối thông tin, mã hóa và chữ ký số có thể đòi hỏi kiến thức kỹ thuật cao và làm giảm trải nghiệm người dùng.
* *Vấn đề bảo mật*: Mặc dù DApp được xây dựng dựa trên các nguyên tắc bảo mật, nhưng vẫn có thể tồn tại các lỗ hổng bảo mật hoặc lỗi trong việc triển khai và quản lý DApp. Nếu một lỗ hổng bảo mật xảy ra, dữ liệu và tài sản trong DApp có thể bị đe dọa.
* *Tiếp cận người dùng*: Hiện nay, việc sử dụng DApp vẫn chưa phổ biến và tiếp cận của người dùng vẫn còn hạn chế. Để sử dụng DApp, người dùng cần có kiến thức về blockchain và các công nghệ liên quan. Điều này có thể tạo ra rào cản cho việc mở rộng và chấp nhận rộng rãi của DApp.

1. Ứng dụng trong DApp.



Hình 13 – Ứng dụng trong DApp

* Ứng dụng trong phát triển DApp (Decentralized Application) là một chủ đề rất thú vị trong lĩnh vực Blockchain và DLT. DApp là các ứng dụng phi tập trung được xây dựng trên nền tảng Blockchain hoặc DLT, có tính chất mở, minh bạch và không thể gian lận. Dưới đây là một số ý tưởng về ứng dụng trong phát triển DApp:
* *Hệ thống thanh toán*: DApp có thể sử dụng các đồng tiền số để thực hiện các giao dịch một cách nhanh chóng và bảo mật hơn so với các hệ thống thanh toán truyền thống.
* *Hệ thống phân phối*: để tạo ra các hệ thống phân phối độc lập, giúp đảm bảo tính minh bạch và công bằng trong các giao dịch.
* *Hệ thống lưu trữ và chia sẻ dữ liệu*: để giúp người dùng lưu trữ và chia sẻ dữ liệu một cách bảo mật và đáng tin cậy.
* *Hệ thống đấu giá và trò chơi*: tạo ra các trò chơi và hoạt động kinh doanh mới với tính minh bạch và công bằng cao.
* *Hệ thống quản lý tài sản*: sử dụng các hệ thống blockchain để quản lý tài sản và các giao dịch liên quan đến tài sản, giúp đảm bảo tính toàn vẹn và đáng tin cậy của hệ thống.

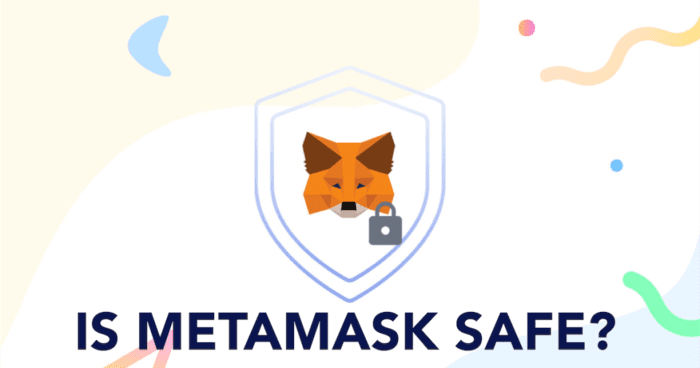
1. Ví Metamask.
2. Metamask là gì?



Hình 14 – Metamask là gì?

* [MetaMask](https://metamask.io/) là một tiện ích mở rộng trình duyệt phổ biến và được thiết lập, có chức năng như một [ví tiền điện tử](https://coinmarketcap.com/alexandria/glossary/hot-wallet) kết nối với blockchain [Ethereum](https://coinmarketcap.com/vi/currencies/ethereum/). MetaMask cho phép người dùng tương tác với hệ sinh thái Ethereum, nơi lưu trữ một vũ trụ rộng lớn gồm [các ứng dụng phi tập trung (Dapps)](https://coinmarketcap.com/alexandria/glossary/decentralized-applications-dapps), mà không cần phải tải xuống toàn bộ [blockchain](https://coinmarketcap.com/alexandria/glossary/blockchain) trên thiết bị của họ.
* Metamask cho phép người dùng tạo và lưu trữ các tài khoản Ethereum, quản lý khóa riêng tư (private keys) và thực hiện các giao dịch trên blockchain Ethereum. Nó cung cấp một giao diện đồ họa dễ sử dụng để người dùng có thể gửi và nhận Ether (đơn vị tiền tệ của Ethereum) và các token chuẩn ERC-20 và ERC-721.

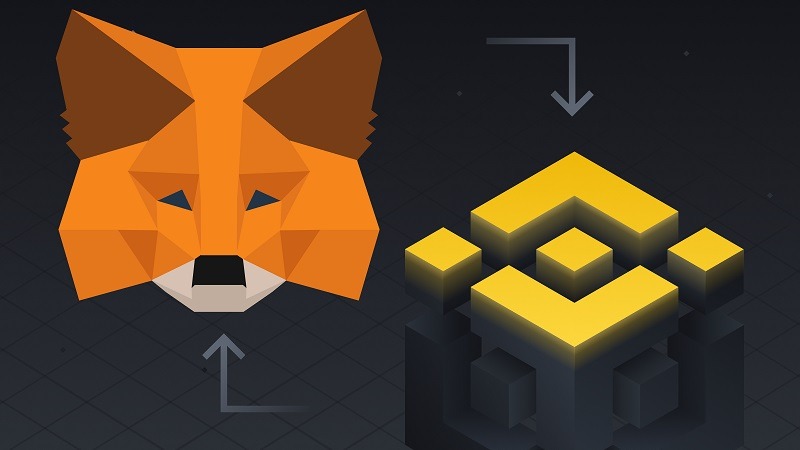
1. Ví metamask có an toàn không?



Hình 15 – Is metamask safe?

* Metamask là một Non-custodial Wallet, tức chỉ đơn thuần là một nơi để đăng nhập ví. Thêm nữa, đây hiện đang là một trong những ví nổi tiếng nhất Crypto, nên rất khó có khả năng Metamask gây tổn thất đến tài sản của bạn.
* Tuy nhiên, vẫn có trường hợp mất mát khi đăng nhập vào Metamask, có thể là do người dùng lộ Private Key, hay bị mã độc được cài trong máy tính đọc được Private Key khi đang thao tác trên ví,… Do đó, cần cẩn thận trong việc bảo vệ máy tính, điện thoại của mình.

1. Ưu điểm của ví metamask.



Hình 16 – Ưu điểm ví metamask

Sử dụng ví Metamask mang lại nhiều lợi ích và ưu điểm cho người dùng. Dưới đây là một số ưu điểm chính khi sử dụng ví Metamask:

* *Quản lý dễ dàng*: Metamask cung cấp một giao diện đồ họa thân thiện và dễ sử dụng để quản lý các tài khoản Ethereum và các token chuẩn ERC-20 và ERC-721. Bạn có thể tạo và lưu trữ nhiều tài khoản Ethereum trên cùng một ví Metamask và dễ dàng chuyển đổi giữa chúng.
* *Tương tác với ứng dụng phi tập trung (DApps)*: Metamask cho phép bạn kết nối với các ứng dụng phi tập trung (DApps) trên nền tảng Ethereum. Bằng cách kích hoạt Metamask trên trình duyệt web của bạn, bạn có thể tham gia vào các hoạt động như bỏ phiếu, tham gia ICO, chơi trò chơi phi tập trung và thực hiện các giao dịch trên các ứng dụng phi tập trung.
* *An toàn và bảo mật*: Metamask đi kèm với các biện pháp bảo mật cơ bản như mã PIN và xác thực hai yếu tố (2FA) để bảo vệ tài khoản của bạn. Ngoài ra, Metamask không bao giờ yêu cầu bạn cung cấp khóa riêng tư khi sử dụng DApps, giúp ngăn chặn các cuộc tấn công lừa đảo.
* *Quản lý token và tiền điện tử*: Metamask cho phép bạn quản lý các token chuẩn ERC-20 và ERC-721. Bạn có thể thêm, xem và gửi token dễ dàng từ giao diện Metamask. Điều này giúp bạn kiểm soát và quản lý tài sản tiền điện tử của mình một cách thuận tiện.
* *Tích hợp với ví phần cứng:* Metamask cung cấp tích hợp với các ví phần cứng như Trezor và Ledger. Điều này cho phép bạn kết hợp lợi ích của Metamask với bảo mật cao của ví phần cứng để lưu trữ khóa riêng tư và xác thực giao dịch.
* *Đa nền tảng*: Metamask không chỉ có sẵn trên trình duyệt web như Chrome, Firefox và Brave, mà còn có ứng dụng di động cho Android và iOS. Điều này cho phép bạn truy cập vào tài khoản của mình và tương tác với DApps từ điện thoại di động của mình.

1. Nhược điểm ví metamask.



Hình 17 – Nhược điểm metamask

Mặc dù Metamask có nhiều ưu điểm, nhưng cũng có một số nhược điểm cần được lưu ý:

* *Phụ thuộc vào trình duyệt*: Metamask là một phần mở rộng của trình duyệt web, điều này có nghĩa là nó chỉ hoạt động trên trình duyệt được hỗ trợ. Nếu bạn không sử dụng trình duyệt web hoặc không có kết nối internet, bạn sẽ không thể truy cập vào ví Metamask của mình.
* *Mất quyền kiểm soát*: Khi bạn sử dụng Metamask, khóa riêng tư của bạn được lưu trữ trên thiết bị của bạn. Điều này có nghĩa là bạn hoàn toàn chịu trách nhiệm bảo mật và bảo vệ khóa riêng tư của mình. Nếu bạn mất thiết bị hoặc không sao lưu khóa riêng tư, bạn có thể mất truy cập vào tài khoản của mình vĩnh viễn.
* *Rủi ro về bảo mật:* Mặc dù Metamask được thiết kế để bảo mật, nhưng vẫn có thể tồn tại các lỗ hổng bảo mật hoặc lỗi phần mềm. Những người tấn công có thể cố gắng khai thác các lỗ hổng này để truy cập vào tài khoản của bạn. Do đó, việc cập nhật Metamask và tuân thủ các biện pháp bảo mật cơ bản là rất quan trọng để giảm thiểu rủi ro.
* *Không phục hồi mật khẩu*: Metamask không cung cấp tính năng phục hồi mật khẩu. Nếu bạn quên mật khẩu của mình, bạn sẽ không thể khôi phục truy cập vào tài khoản của mình. Điều này đảm bảo an toàn cho người dùng, nhưng đồng thời khiến việc khôi phục truy cập trở nên khó khăn nếu không có sao lưu khóa riêng tư.
* *Rủi ro từ các ứng dụng phi tập trung (DApps)*: Metamask cho phép bạn tương tác với các ứng dụng phi tập trung trên Ethereum. Tuy nhiên, không phải tất cả các DApps đều được kiểm tra và đảm bảo an toàn. Sử dụng các DApps không đáng tin cậy hoặc không được kiểm tra có thể tạo ra rủi ro bảo mật và mất tài sản của bạn.

1. Etherum.
2. Định nghĩa Etherum.



Hình 18 – Etherum là gì?

* [Ethereum](https://vi.wikipedia.org/wiki/Ethereum) là nền tảng điện toán phân tán, mã nguồn mở dựa trên công nghệ chuỗi khối (blockchain) có khả năng thực thi hợp đồng thông minh (smart contract) - tức là điều khoản được ghi trong hợp đồng sẽ được thực thi một cách tự động khi các điều kiện trước đó được thỏa mãn, không ai có thể can thiệp vào.
* Ethereum là một dự án Blockchain Layer 1 cho phép nhiều các lập trình viên xây dựng các ứng dụng phi tập trung (DApps) và các tổ chức tự trị phi tập trung (DAOs). Trong đó:
* Các ứng dụng phi tập trung (DApps - Decentralized Application) là các phần mềm được triển khai độc lập, không nằm trên một máy chủ duy nhất mà được lưu trữ một cách phân tán trên các kho lưu trữ phi tập trung và có thể được viết bằng bất kỳ ngôn ngữ nào.
* Các tổ chức tự trị phi tập trung (DAOs - Decentralized Autonomous Organizations) là một tổ chức được vận hành bởi các thành viên dựa trên một bộ quy tắc được mã hóa bằng code. Tất cả các thành viên đều có quyền biểu quyết các quyết định quan trọng của DAOs.

1. Cách thức hoạt động của Etherum.



Hình 19 – Etherum hoạt động như thế nào?

Ethereum hoạt động dựa trên một mạng lưới blockchain công cộng và sử dụng một ngôn ngữ lập trình đặc biệt được gọi là Solidity để tạo và thực thi các hợp đồng thông minh. Dưới đây là một cái nhìn tổng quan về cách Ethereum hoạt động:

* Blockchain Ethereum: Ethereum sử dụng một blockchain để lưu trữ thông tin và giao dịch. Blockchain Ethereum bao gồm một chuỗi các khối (blocks) liên kết với nhau, trong đó mỗi khối chứa một danh sách các giao dịch và thông tin khác. Mỗi khối được "đào" (mined) và thêm vào blockchain theo một quy trình cụ thể.
* Đồng Ether (ETH): Ether là đơn vị tiền tệ của mạng lưới Ethereum. Nó được sử dụng để thực hiện các giao dịch và trả phí cho việc sử dụng tài nguyên mạng. Ether cũng có thể được giao dịch và lưu trữ như một loại tài sản kỹ thuật số.
* Hợp đồng thông minh: Ethereum nổi tiếng với khả năng hỗ trợ hợp đồng thông minh. Hợp đồng thông minh là các chương trình tự thực thi và thỏa thuận, được lưu trữ và thực thi trên blockchain Ethereum. Hợp đồng thông minh có thể thực hiện các hành động tự động khi một số điều kiện được đáp ứng và có thể được sử dụng để tạo ra các ứng dụng phi tập trung.
* Quy trình đồng thuận: Ethereum sử dụng một cơ chế đồng thuận để xác nhận và thêm các giao dịch vào blockchain. Trước khi một khối mới được thêm vào blockchain, các thợ đào (miners) trên mạng phải giải quyết một bài toán khó để chứng minh rằng họ đã thực hiện công việc tính toán. Quy trình này, gọi là Proof of Work (PoW), đòi hỏi sự tiêu tốn năng lượng tính toán và giúp ngăn chặn các hành vi gian lận.
* Ethereum 2.0 và Proof of Stake: Hiện tại, Ethereum đang chuẩn bị chuyển từ cơ chế Proof of Work sang Proof of Stake (PoS) trong phiên bản Ethereum 2.0. PoS sẽ thay thế quy trình khai thác đào bằng một quy trình đồng thuận dựa trên việc đặt cọc và chọn ngẫu nhiên các "đồng thuận viên" (validators) để xác nhận giao dịch và tạo khối mới. Chuyển đổi này dự kiến sẽ giúp tăng tốc độ xác nhận giao dịch và giảm thiểu tiêu thụ năng lượng.
* Các ứng dụng và chuẩn token: Ethereum cung cấp một môi trường phát triển mạnh mẽ cho việc xây dựng các ứng dụng và dịch vụ sử dụng blockchain. Nó hỗ trợ chuẩn token ERC-20, được sử dụng rộng rãi cho việc phát hành token tiêu chuẩn, và chuẩn token ERC-721, được sử dụng cho việc tạo và quản lý các tài sản phi tập trung.
* Tóm lại, Ethereum hoạt động dựa trên một mạng lưới blockchain công cộng, sử dụng hợHợp đồng thông minh (smart contracts) là chương trình tự thực thi và thỏa thuận, được lưu trữ và thực thi trên blockchain Ethereum. Mỗi hợp đồng thông minh được viết bằng ngôn ngữ Solidity và chứa mã lệnh để thực hiện các hành động cụ thể khi các điều kiện được đáp ứng.

1. Quá trình thực thi hợp đồng đông minh trên Etherum.

* *Gửi giao dịch*: Người dùng tạo một giao dịch và gửi nó đến địa chỉ hợp đồng thông minh. Giao dịch này chứa dữ liệu và hàm mà người dùng muốn thực thi trên hợp đồng.
* *Xác thực giao dịch:* Mạng Ethereum xác thực giao dịch bằng cách sử dụng quy trình đồng thuận (Proof of Work hiện tại và sẽ chuyển sang Proof of Stake trong Ethereum 2.0). Quá trình này đảm bảo rằng giao dịch là hợp lệ và được thêm vào blockchain.
* *Thực thi hợp đồng thông minh*: Khi giao dịch được xác thực, các nút trong mạng Ethereum bắt đầu thực thi hợp đồng thông minh. Mã lệnh trong hợp đồng được thực thi bước từ bước và tương tác với dữ liệu và trạng thái của hợp đồng.
* *Ghi lại kết quả*: Kết quả của việc thực thi hợp đồng thông minh được ghi lại trên blockchain. Trạng thái của hợp đồng và dữ liệu liên quan sẽ được cập nhật theo kết quả này.

Quan trọng nhất, Ethereum cung cấp một môi trường phát triển dễ dùng và mạnh mẽ để xây dựng các ứng dụng phi tập trung (Decentralized Applications - DApps) sử dụng hợp đồng thông minh. Các DApp có thể tận dụng tính năng của Ethereum để tạo ra các ứng dụng trong nhiều lĩnh vực, như tài chính, chuỗi cung ứng, trò chơi điện tử, bất động sản và nhiều hơn nữa.

1. Ưu điểm của Etherum.



Hình 20 – Ưu điểm của Etherum

* *Hợp đồng thông minh*: Ethereum nổi tiếng với khả năng hỗ trợ hợp đồng thông minh. Điều này cho phép người dùng tạo ra các ứng dụng phi tập trung (DApps) và hợp đồng thông minh, mở ra một loạt các tác động tiềm năng trong các lĩnh vực như tài chính, bất động sản, chuỗi cung ứng và nhiều lĩnh vực khác.
* *Mạng lưới phân cấp*: Ethereum có một cấu trúc mạng lưới phân cấp, trong đó các nút (nodes) có thể tham gia vào việc xác nhận giao dịch và tạo khối mới. Điều này tạo ra một mạng lưới phân quyền và phi tập trung, cho phép việc phân phối quyền kiểm soát và đảm bảo tính bền vững của mạng lưới.
* *Chuẩn token tiêu chuẩn*: Ethereum hỗ trợ chuẩn token ERC-20, là một chuẩn tiêu chuẩn để phát hành và quản lý token trên mạng lưới. Điều này đã tạo ra một hệ sinh thái phong phú của các dự án token và ICOs (Initial Coin Offerings), tạo điều kiện cho việc tài trợ và phát triển các dự án.
* *Môi trường phát triển phong phú*: Ethereum cung cấp một môi trường phát triển mạnh mẽ với các ngôn ngữ lập trình như Solidity và Vyper. Điều này giúp cho các nhà phát triển có thể dễ dàng xây dựng các ứng dụng và hợp đồng thông minh trên nền tảng Ethereum.
* *Khả năng mở rộng*: Ethereum đang phát triển phiên bản Ethereum 2.0, với mục tiêu tăng khả năng mở rộng và hiệu suất của mạng lưới. Chuyển đổi từ Proof of Work sang Proof of Stake và triển khai sharding (phân mảnh) sẽ giúp tăng tốc độ xử lý giao dịch và giảm thiểu phí giao dịch.
* *Tiềm năng tài chính phi tập trung*: Ethereum đã tạo ra một hệ sinh thái phong phú của các ứng dụng tài chính phi tập trung (DeFi), bao gồm các sàn giao dịch phi tập trung, các giao thức vay mượn, giao thức giao dịch tiền tệ và các sản phẩm tài chính khác. Điều này mở ra cơ hội mới cho việc tài trợ, đầu tư và sử dụng các dịch vụ tài chính một cách phi tập trung và toàn cầu.

1. Hướng lý thuyết.
2. So sánh các mạng blockchain phổ biến hiện nay.



Hình 21 – Các mạng Blockchain phổ biến hiện nay

Dưới đây là một bảng so sánh giữa một số blockchain phổ biến hiện nay, bao gồm Bitcoin, Ethereum, Binance Smart Chain, Solana và Polkadot:

| **Blockchain** | **Mã nguồn mở** | **Thuật toán chính** | **Tốc độ xử lý giao dịch** | **Khả năng mở rộng** | **Ngôn ngữ lập trình chính** | **Hợp đồng thông minh** | **Độ phân cấp mạng lưới** | **Phí giao dịch** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bitcoin | Có | Proof of Work | Khoảng 7-10 giao dịch/giây | Hạn chế | Bitcoin Script | Không | Peer-to-Peer (P2P) | Cao |
| Ethereum | Có | Proof of Stake | Khoảng 15-30 giao dịch/giây | Đang nỗ lực cải thiện | Solidity, Vyper | Có | Peer-to-Peer (P2P) | Cao |
| Binance Smart Chain | Có | Proof of Stake | Khoảng 100-300 giao dịch/giây | Tốt | Solidity | Có | Peer-to-Peer (P2P) | Thấp |
| Solana | Có | Proof of History | Khoảng 50.000 giao dịch/giây | Tốt | Rust, C, C++ | Có | Peer-to-Peer (P2P) | Thấp |
| Polkadot | Có | Relay Chain | Tùy thuộc vào các Parachains | Tốt | Substrate, Rust | Có | Cấu trúc đa lớp | Thấp |

Bảng 3 – So sánh các mạng blockchain phổ biến hiện nay

1. Tổng quan về hệ thống bầu cử truyền thống.
2. Hệ thống bỏ phiếu điện tử là gì?



Hình 22 – Hệ thống bỏ phiếu điện tử là gì?

* Bỏ phiếu điện tử là một hình thức bỏ phiếu trong đó việc đánh giá và ghi lại phiếu bầu được thực hiện thông qua công nghệ điện tử. Thay vì sử dụng giấy phiếu và hộp bỏ phiếu truyền thống, bỏ phiếu điện tử cho phép cử tri sử dụng thiết bị điện tử như máy tính, điện thoại di động hoặc máy tính bảng để tham gia quá trình bỏ phiếu.
* Bỏ phiếu điện tử là một hình thức đã được quy định tại Luật Doanh nghiệp 2020 và các cổ đông thực hiện việc bỏ phiếu điện tử cũng được coi là tham dự và biểu quyết tại cuộc họp Đại hội cổ đông (ĐHCĐ) như các cổ đông tham dự và biểu quyết trực tiếp. Trên cơ sở đó, VSDC đã xây dựng và hoàn thiện hệ thống bỏ phiếu điện tử (V-Vote) với mong muốn cung cấp dịch vụ tiện ích cho các Tổ chức phát hành, công ty đại chúng và các cổ đông.

1. **Bối cảnh nghiên cứu**.

* Hệ thống bỏ phiếu truyền thống thường gặp phải nhiều thách thức, bao gồm khả năng gian lận, thiếu minh bạch và độ tin cậy không cao. Trong khi đó, công nghệ Blockchain đã nổi lên như một giải pháp tiềm năng để giải quyết những vấn đề này. Blockchain cung cấp tính toàn vẹn dữ liệu, tính bảo mật và tính khả dụng cao, giúp đảm bảo tính minh bạch và tin cậy trong quá trình bỏ phiếu.
* Bối cảnh bầu cử hiện nay đang đối mặt với nhiều hạn chế và vấn đề, bao gồm:
* *Gian lận*: Hệ thống bầu cử truyền thống có thể dễ dàng bị tấn công và gian lận. Ví dụ, việc đánh đồng phiếu, mua phiếu, hoặc thậm chí là thao túng kết quả bầu cử là những vấn đề thường gặp. Điều này gây mất niềm tin của người dân vào quá trình bầu cử và có thể gây ra sự thiếu công bằng và bất ổn xã hội.
* *Khó kiểm soát*: Quá trình bầu cử truyền thống thường khó kiểm soát. Từ việc kiểm đếm phiếu, quản lý danh sách cử tri đến việc phân phối các tài liệu liên quan, có thể gặp phải nhiều vấn đề liên quan đến sự chính xác, đồng nhất và theo dõi.
* *Chi phí cao*: Quá trình bầu cử truyền thống thường đòi hỏi một số lượng lớn nhân lực và tài chính. Cần có nhân viên để quản lý và thực hiện các hoạt động liên quan đến bầu cử, từ việc cử tri đăng ký, đến việc thiết lập trạm bỏ phiếu và kiểm đếm phiếu. Chi phí này có thể rất lớn và đôi khi gây áp lực tài chính lên ngân sách công cộng.

1. Ưu điểm của bầu cử truyền thống.

* *Tin cậy và thực tế*: Hệ thống bỏ phiếu truyền thống đã được sử dụng trong nhiều thập kỷ và được công nhận là một phương pháp tin cậy. Việc bỏ phiếu trực tiếp và đếm phiếu công khai cho phép người dân tham gia quan sát quá trình bầu cử, tăng tính minh bạch và đáng tin cậy của quá trình.
* *Dễ sử dụng*: Hệ thống bỏ phiếu truyền thống đơn giản và dễ sử dụng. Người bầu cử chỉ cần đến trạm bỏ phiếu, đánh dấu lựa chọn của mình trên phiếu bầu và đưa phiếu vào hòm phiếu. Quy trình này rất rõ ràng và các nguyên tắc cơ bản có thể được giảng dạy một cách dễ dàng cho mọi người.
* *Bảo mật và riêng tư*: Hệ thống bỏ phiếu truyền thống thường bảo vệ quyền riêng tư và bí mật của người bầu cử. Phiếu bầu được đặt trong một phong bì và không tiết lộ lựa chọn của người bầu cho đến khi được đếm. Điều này giúp bảo vệ danh tính và lựa chọn của người bầu.
* *Khả năng kiểm tra và xác minh*: Với hệ thống bỏ phiếu truyền thống, phiếu bầu được lưu trữ vật lý và có thể giữ lại để kiểm tra và xác minh lại kết quả bầu cử. Điều này tạo ra khả năng kiểm tra lại và rà soát quá trình bầu cử để đảm bảo tính chính xác và công bằng.
* *Dễ dàng triển khai và chi phí thấp*: So với triển khai hệ thống bỏ phiếu điện tử hoặc sử dụng công nghệ blockchain, triển khai hệ thống bỏ phiếu truyền thống đơn giản và có chi phí thấp hơn. Không cần đầu tư vào công nghệ cao cấp hoặc đào tạo phức tạp, điều này làm cho hệ thống này phổ biến và dễ tiếp cận.

1. Nhược điểm của hệ bầu cử truyền thống.

* Độ chính xác: Quá trình đếm phiếu bằng tay có thể gặp phải sai sót và lỗi đếm. Những sai sót nhỏ có thể ảnh hưởng đáng kể đến kết quả bầu cử. Điều này đặc biệt đúng khi có một số lượng lớn phiếu bầu cần được xử lý hoặc khi quá trình đếm không được giám sát cẩn thận.
* Độ tin cậy: Hệ thống bỏ phiếu truyền thống có thể bị ảnh hưởng bởi các yếu tố như gian lận hoặc thao túng. Có thể xảy ra việc mất cắp hoặc thay đổi phiếu bầu, hoặc trái ngược lại, việc đưa vào phiếu bầu giả. Điều này đặc biệt đúng nếu không có các biện pháp đảm bảo an ninh và giám sát chặt chẽ trong quá trình bỏ phiếu và đếm phiếu.
* Độ minh bạch: Hệ thống bỏ phiếu truyền thống có thể thiếu tính minh bạch. Việc đếm phiếu diễn ra trong một phạm vi hẹp và không thể được quan sát bởi công chúng. Điều này có thể tạo ra sự nghi ngờ và tranh cãi về tính công bằng và chính xác của quá trình bầu cử.
* Độ tiện lợi: Hệ thống bỏ phiếu truyền thống đòi hỏi người dân phải đến các trạm bỏ phiếu trong một khoảng thời gian cụ thể. Điều này có thể gây khó khăn cho những người không thể đi lại dễ dàng hoặc không có thời gian phù hợp. Ngoài ra, việc tính toán và công bố kết quả cũng có thể mất nhiều thời gian và tạo ra sự chờ đợi.
* Khả năng mở rộng: Hệ thống bỏ phiếu truyền thống có thể gặp khó khăn trong việc xử lý các cuộc bầu cử quy mô lớn hoặc có số lượng bầu cử viên đông đảo. Quá trình đếm và xử lý phiếu bầu có thể trở nên tốn kém về thời gian và công sức, đồng thời tăng nguy cơ sai sót và làm giảm tính chính xác.

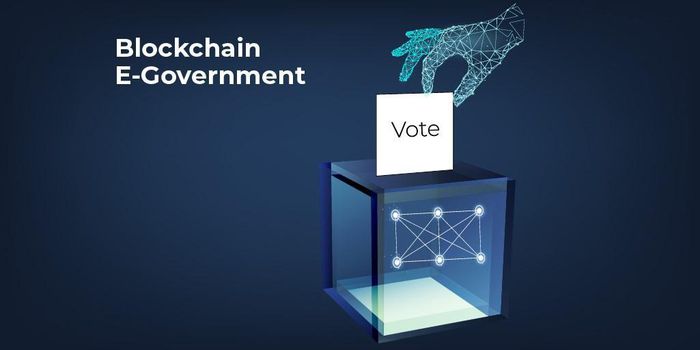
1. Tổng quan về hệ thống bầu cử điện tử.
2. Ý tưởng nghiên cứu.

* *Thiết kế và triển khai giao thức bỏ phiếu điện tử dựa trên công nghệ blockchain*: Nghiên cứu này tập trung vào việc phát triển một giao thức bỏ phiếu điện tử sử dụng công nghệ blockchain để đảm bảo tính toàn vẹn dữ liệu và tính bảo mật cao. Nghiên cứu này có thể tập trung vào việc xác định cách thức tạo và xác minh phiếu bầu, cơ chế đồng thuận và quản lý danh sách cử tri.
* *Phân tích và đánh giá tính bảo mật của hệ thống bỏ phiếu điện tử*: Nghiên cứu này tập trung vào việc phân tích và đánh giá các lỗ hổng bảo mật có thể tồn tại trong hệ thống bỏ phiếu điện tử và đề xuất các biện pháp để ngăn chặn và bảo vệ chống lại các cuộc tấn công. Các vấn đề như bảo mật dữ liệu, xác thực cử tri và sự riêng tư có thể được xem xét trong nghiên cứu này.
* *Đánh giá tác động xã hội và chính trị của hệ thống bỏ phiếu điện tử*: Nghiên cứu có thể tiến hành khảo sát và phỏng vấn cử tri, chính trị gia và các chuyên gia để hiểu quan điểm và ý kiến của họ về việc sử dụng hệ thống bỏ phiếu điện tử, cũng như những thay đổi xã hội và chính trị có thể xảy ra.
* *Phát triển mô hình mô phỏng và mô phỏng hệ thống bỏ phiếu điện tử*: Bằng cách sử dụng dữ liệu thực tế hoặc dữ liệu mô phỏng, nghiên cứu có thể đánh giá hiệu suất, tải trọng và khả năng mở rộng của hệ thống, giúp tối ưu hóa thiết kế và triển khai.
* *So sánh hệ thống bỏ phiếu điện tử với hệ thống bầu cử truyền thống*: Nghiên cứu có thể tiến hành so sánh dựa trên các yếu tố như chi phí, thời gian, tính toàn vẹn dữ liệu và sự tham gia của cử tri.

1. Các yếu tố then chốt để xây dựng hệ thống bỏ phiếu điện tử.

* *An ninh và bảo mật*: Đảm bảo tính bảo mật của hệ thống là một yếu tố quan trọng. Áp dụng các biện pháp an ninh mạnh mẽ để bảo vệ dữ liệu phiếu bầu, ngăn chặn tấn công từ bên ngoài và đảm bảo rằng thông tin phiếu bầu không bị rò rỉ. Đồng thời, xác thực và kiểm soát truy cập của người dùng để đảm bảo rằng chỉ những người có quyền được bỏ phiếu mới có thể truy cập vào hệ thống.
* *Xác thực người dùng*: Đảm bảo rằng chỉ những người được phép có quyền bỏ phiếu mới có thể truy cập vào hệ thống. Sử dụng các phương pháp xác thực như tài khoản người dùng, xác thực hai yếu tố hoặc xác thực sinh trắc học để đảm bảo tính chính xác và tin cậy của người dùng.
* *Bảo mật phiếu bầu*: Đảm bảo tính riêng tư và bảo mật của phiếu bầu là rất quan trọng. Sử dụng mã hóa dữ liệu để bảo vệ thông tin phiếu bầu trong quá trình truyền và lưu trữ. Hãy đảm bảo rằng chỉ có người được ủy quyền mới có thể giải mã và xem nội dung phiếu bầu.
* *Đáng tin cậy và kiểm tra*: Hệ thống bỏ phiếu điện tử cần được xây dựng với khả năng đáng tin cậy và kiểm tra. Đảm bảo rằng các thông tin phiếu bầu được ghi lại chính xác và không bị thay đổi. Kiểm tra hệ thống thường xuyên để đảm bảo rằng nó hoạt động đúng cách và không có lỗi.
* *Dễ sử dụng và thân thiện với người dùng*: Thiết kế giao diện người dùng thân thiện và dễ sử dụng là một yếu tố quan trọng. Hãy đảm bảo rằng người dùng có thể dễ dàng điều hướng trong quá trình bỏ phiếu và không gặp khó khăn trong việc sử dụng hệ thống.
* *Tính mở rộng và mô đun*: Xây dựng hệ thống có khả năng mở rộng để có thể xử lý số lượng lớn cử tri và tăng cường khả năng mở rộng theo nhu cầu. Tính mô đun cũng quan trọng để có thể nâng cấp và mở rộng các tính năng mới theo thời gian.
* *Kiểm soát và giám sát*: Đảm bảo có các cơ chế kiểm soát và giám sát để theo dõi quá trình bỏ phiếu điện tử. Điều này đảm bảo tính minh bạch và đáng tin cậy của hệ thống.
* *Sự khả dụng và khả năng dự phòng*: Đảm bảo rằng hệ thống bỏ phiếu điện tử có khả năng hoạt động liên tục và sẵn sàng sử dụng trong suốt quá trình bỏ phiếu. Cung cấp các biện pháp dự phòng để xử lý các sự cố kỹ thuật và đảm bảo rằng hệ thống có khả năng phục hồi sau sự cố.
* *Tương thích và chuẩn hóa*: Đảm bảo rằng hệ thống bỏ phiếu điện tử tương thích với các tiêu chuẩn và quy định pháp luật liên quan. Chuẩn hóa giao thức truyền thông và định dạng dữ liệu để đảm bảo tính tương thích và tương tác với các hệ thống khác.
* *Đào tạo và hỗ trợ người dùng:* Cung cấp đào tạo và hỗ trợ cho người dùng về cách sử dụng hệ thống bỏ phiếu điện tử. Đảm bảo rằng cử tri và nhân viên có đủ thông tin và hỗ trợ để sử dụng hệ thống một cách hiệu quả.

1. Ưu điểm của hệ thống.

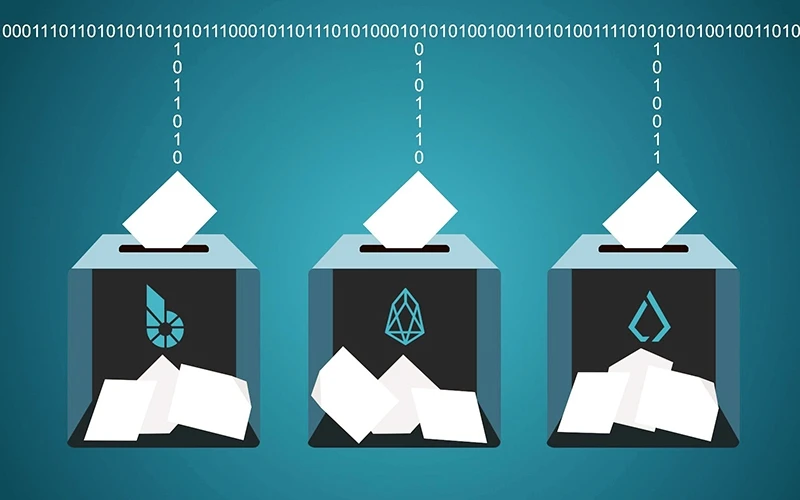


Hình 23 – Ưu điểm hệ thống bỏ phiếu điện tử

VoteChain là một hệ thống bỏ phiếu điện tử dựa trên công nghệ blockchain. Dưới đây là một số ưu điểm của hệ thống bỏ phiếu điện tử VoteChain:

* *Tính minh bạch*: Công nghệ blockchain của VoteChain cho phép lưu trữ toàn bộ quá trình bỏ phiếu và kết quả trên một sổ cái công khai và không thể thay đổi. Điều này tạo ra một môi trường minh bạch và giúp tăng cường niềm tin của người dùng vào quá trình bỏ phiếu.
* *Bảo mật*: Công nghệ blockchain của VoteChain cung cấp một cơ chế bảo mật mạnh mẽ. Dữ liệu bỏ phiếu được mã hóa và ghi lại trên blockchain, ngăn chặn việc thay đổi hay xóa bỏ phiếu sau khi đã được ghi lại. Điều này giúp đảm bảo tính toàn vẹn và bảo mật của quá trình bỏ phiếu.
* *Xác thực người dùng*: VoteChain có thể sử dụng các công nghệ xác thực như mã hóa định danh và chữ ký số để đảm bảo rằng chỉ người dùng hợp lệ mới có thể tham gia vào quá trình bỏ phiếu. Điều này giúp ngăn chặn việc giả mạo và đảm bảo rằng chỉ những người được ủy quyền mới có thể tham gia vào quá trình bỏ phiếu.
* *Tiết kiệm thời gian và tài nguyên*: Hệ thống bỏ phiếu điện tử VoteChain có thể giảm thiểu hoặc loại bỏ nhu cầu về các hoạt động như in ấn, gửi thư và xử lý thủ công. Điều này giúp tiết kiệm thời gian và tài nguyên, đồng thời tăng tính hiệu quả và giảm thiểu sai sót trong quá trình bỏ phiếu.
* *Tính dễ dàng kiểm tra*: Với VoteChain, bất kỳ ai cũng có thể kiểm tra kết quả bỏ phiếu một cách công khai và độc lập. Điều này tạo ra một hệ thống có thể xem xét lại và đánh giá một cách công bằng, giúp tăng cường niềm tin của các bên liên quan.
* *Khả năng mở rộng*: Công nghệ blockchain của VoteChain có khả năng mở rộng, cho phép xử lý hàng ngàn giao dịch bỏ phiếu cùng một lúc. Điều này giúp đáp ứng được nhu cầu quy mô lớn trong các quá trình bầu cử có quy mô rộng lớn.

1. Nhược điểm của hệ thống.



Hình 24 – Nhược điểm của hệ thống bỏ phiếu điện tử

Mặc dù hệ thống bỏ phiếu điện tử VoteChain mang lại nhiều ưu điểm, nhưng cũng có một số nhược điểm cần được xem xét:

* *Phụ thuộc vào công nghệ*: Hệ thống bỏ phiếu điện tử VoteChain đòi hỏi sự phụ thuộc vào công nghệ blockchain. Nếu có lỗi trong công nghệ hoặc xảy ra sự cố kỹ thuật, có thể ảnh hưởng đến tính khả dụng và đáng tin cậy của hệ thống.
* *Đòi hỏi kiến thức kỹ thuật*: Sử dụng và quản lý hệ thống bỏ phiếu điện tử VoteChain yêu cầu kiến thức kỹ thuật cao. Cần có sự hiểu biết về công nghệ blockchain và quá trình triển khai, cũng như kỹ năng quản lý và bảo mật hệ thống.
* *Rủi ro bảo mật*: Một rủi ro tiềm năng khi sử dụng hệ thống bỏ phiếu điện tử VoteChain là việc tấn công mạng và xâm nhập vào hệ thống. Nếu kẻ tấn công có thể kiểm soát được đủ số nút trong mạng blockchain hoặc tạo ra các giao dịch giả mạo, tính toàn vẹn của quá trình bỏ phiếu có thể bị đe dọa.
* *Quyền riêng tư và ẩn danh*: Hệ thống bỏ phiếu điện tử VoteChain có thể đối mặt với thách thức về quyền riêng tư và ẩn danh. Mặc dù các giao dịch trên blockchain được mã hóa, nhưng việc liên kết các giao dịch với người dùng cụ thể vẫn có thể gây ra mối lo ngại về quyền riêng tư.
* *Thay đổi quyền lực*: Một trong những thách thức lớn của hệ thống bỏ phiếu điện tử VoteChain là thay đổi quyền lực và ảnh hưởng. Việc triển khai hệ thống này có thể yêu cầu sự thay đổi trong cách thức hoạt động và quản lý của các tổ chức bầu cử, và không phải lúc nào cũng dễ dàng để thực hiện sự thay đổi này.
* *Kỹ thuật phức tạp*: Công nghệ blockchain và hệ thống bỏ phiếu điện tử VoteChain đòi hỏi sự hiểu biết và kỹ năng kỹ thuật chuyên sâu. Điều này có thể tạo ra một rào cản cho việc triển khai và sử dụng hệ thống, đặc biệt là đối với các quốc gia hoặc tổ chức có nguồn lực và khả năng kỹ thuật hạn chế.

1. So sánh giữa hệ thống bầu cử truyền thống và hệ thống bầu cử điện tử.



Hình 25 – So sánh giữa Voting online và Voting offline

Dưới đây là một bảng so sánh giữa hệ thống bầu cử truyền thống (bỏ phiếu giấy) và hệ thống bầu cử điện tử sử dụng Blockchain:

|  | **Hệ thống bầu cử truyền thống** | **Hệ thống bầu cử điện tử** |
| --- | --- | --- |
| ***Độ tin cậy*** | Có tin cậy và được sử dụng từ lâu. Quá trình đếm phiếu công khai và có thể kiểm tra, xác minh kết quả. | Công nghệ blockchain cung cấp tính tin cậy cao bằng cách sử dụng mã hóa và phân tán dữ liệu. Kết quả bầu cử được lưu trữ và kiểm tra bởi nhiều người tham gia, giảm nguy cơ gian lận. |
| ***Độ chính xác*** | Có thể gặp sai sót và lỗi đếm khi đếm phiếu bằng tay. | Quá trình bầu cử điện tử blockchain có khả năng đếm chính xác và tự động. Dữ liệu bầu cử được lưu trữ trong khối blockchain mà không thể thay đổi sau khi được ghi vào. |
| ***Minh bạch*** | Quá trình bỏ phiếu và đếm phiếu diễn ra công khai và có thể quan sát được. | Công nghệ blockchain cung cấp tính minh bạch cao. Mọi giao dịch và thông tin bầu cử đều được lưu trữ trên blockchain, có thể được kiểm tra bởi mọi người. |
| ***Tiện lợi*** | Cần người dân đi đến trạm bỏ phiếu trong một khoảng thời gian cụ thể. | Cho phép bỏ phiếu từ xa thông qua giao diện điện tử. Người dân có thể bỏ phiếu từ bất kỳ đâu có kết nối internet. |
| ***Khả năng mở rộng*** | Có thể gặp khó khăn trong xử lý các cuộc bầu cử quy mô lớn hoặc đông đảo. | Công nghệ blockchain có khả năng mở rộng tốt. Quá trình bầu cử điện tử có thể được thực hiện trên mạng lưới blockchain toàn cầu, xử lý số lượng lớn phiếu bầu một cách hiệu quả. |
| ***Chi phí*** | Chi phí triển khai và quản lý thấp. | Yêu cầu đầu tư cao vào hạ tầng công nghệ blockchain và bảo mật. Tuy nhiên, giảm được nhiều chi phí liên quan đến in ấn và vận chuyển phiếu bầu giấy. |
| ***Tiếp cận*** | Dễ tiếp cận cho người dân mà không yêu cầu kỹ năng công nghệ. | Yêu cầu kiến thức công nghệ và truy cập internet. Cần đảm bảo rằng mọi người có đủ khả năng sử dụng giao diện điện tử và hiểu về công nghệ blockchain. |

Bảng 4 – Bảng so sánh giữa hệ thống bầu cử truyền thống và hệ thống bầu cử điện tử

1. Hướng ứng dụng.
2. Tiềm năng ứng dụng Blockchain trong bầu cử, kiểm phiếu.

Nhờ những ưu điểm vượt trội từ công nghệ blockchain, ta hoàn toàn có thể ứng dụng nó trong việc ứng dụng trong lĩnh vực bầu cử, kiểm phiếu.

* Tính minh bạch: Blockchain có thể giúp đảm bảo tính minh bạch của quá trình bầu cử bằng cách cho phép mọi người trong mạng truy cập và xem dữ liệu về kết quả bầu cử. Điều này có thể giúp giảm thiểu gian lận và tham nhũng trong bầu cử.Blockchain có thể được sử dụng để lưu trữ danh sách cử tri, kết quả bỏ phiếu và các thông tin liên quan khác. Mọi người có thể truy cập vào dữ liệu này để đảm bảo rằng quá trình bầu cử diễn ra công bằng và minh bạch.
* Tính bất biến :Blockchain có thể giúp đảm bảo tính bất biến của kết quả bầu cử bằng cách lưu trữ dữ liệu kết quả bỏ phiếu trong một sổ cái phân tán. Điều này có nghĩa là dữ liệu kết quả bỏ phiếu không thể bị thay đổi một cách dễ dàng. Ứng dụng của blockchain có thể kể đến như được sử dụng để tạo ra một hệ thống bỏ phiếu trực tuyến. Trong hệ thống này, mỗi cử tri sẽ được cấp một mã duy nhất để bỏ phiếu. Mã này sẽ được sử dụng để xác minh kết quả bỏ phiếu của cử tri và ngăn chặn việc gian lận.
* Tính bảo mật: Blockchain có thể giúp đảm bảo tính bảo mật của kết quả bầu cử bằng cách sử dụng mã hóa. Điều này giúp bảo vệ dữ liệu khỏi bị truy cập trái phép. Ứng dụng blockchain có thể được sử dụng để lưu trữ dữ liệu kết quả bỏ phiếu bằng cách mã hóa dữ liệu này. Mã hóa sẽ giúp ngăn chặn việc truy cập trái phép vào dữ liệu và ngăn chặn việc thay đổi dữ liệu.
* Ngoài ra, blockchain còn có thể giúp cải thiện hiệu quả của quá trình bầu cử bằng cách tự động hóa các quy trình. Điều này có thể giúp giảm thiểu chi phí và thời gian cần thiết để tổ chức bầu cử. Ví dụ như blockchain có thể được sử dụng để tự động hóa quá trình đăng ký cử tri, kiểm phiếu và công bố kết quả bầu cử. Điều này có thể giúp giảm thiểu thời gian và công sức cần thiết để tổ chức bầu cử.

Tiềm năng ứng dụng của blockchain trong lĩnh vực bầu cử, kiểm phiếu: Công nghệ blockchain có tiềm năng cách mạng hóa lĩnh vực bầu cử, kiểm phiếu. Các đặc điểm của blockchain có thể giúp cải thiện đáng kể tính minh bạch, hiệu quả và an toàn của quá trình bầu cử.

Một số ứng dụng cụ thể của blockchain trong lĩnh vực bầu cử, kiểm phiếu bao gồm:

* Lưu trữ danh sách cử tri: Blockchain có thể được sử dụng để lưu trữ danh sách cử tri một cách an toàn và minh bạch. Điều này có thể giúp ngăn chặn việc gian lận trong quá trình đăng ký cử tri.
* Quản lý phiếu bầu: Blockchain có thể được sử dụng để quản lý phiếu bầu một cách an toàn và hiệu quả. Điều này có thể giúp giảm thiểu chi phí và thời gian cần thiết để tổ chức bầu cử.
* Kết quả bầu cử: Blockchain có thể được sử dụng để lưu trữ kết quả bầu cử một cách minh bạch và an toàn. Điều này có thể giúp ngăn chặn việc gian lận trong quá trình kiểm phiếu.

1. Xây dựng mô hình hệ thống bỏ phiếu điện tử dựa trên công nghệ Blockchain và đánh giá khả năng ứng dụng.

Để hiểu rõ hơn chúng ta sẽ có một số giải đáp cho đề tài này.

* Câu hỏi: Làm thế nào để đảm bảo quyền riêng tư của cử tri trong hệ thống bỏ phiếu điện tử blockchain?
* Các giao dịch trên blockchain là ẩn danh. Thông tin cá nhân của cử tri có thể được tách rời khỏi phiếu bầu điện tử trước khi lưu lên blockchain. Như vậy không ai có thể dò ngược từ phiếu bầu đến danh tính cụ thể của cử tri.
* Câu hỏi: Những thách thức lớn nhất khi áp dụng bỏ phiếu điện tử blockchain là gì?
* Một số thách thức có thể kể đến là chi phí đầu tư ban đầu, tính khả dụng của công nghệ cho tất cả cử tri, nguy cơ mất kết nối mạng, sự chấp nhận của công chúng và nguồn nhân lực có kỹ năng về blockchain.
* Câu hỏi: Blockchain hoạt động như thế nào để đảm bảo tính bảo mật và minh bạch cho hệ thống bỏ phiếu điện tử?
* Blockchain sử dụng các công nghệ mã hóa và phân tán dữ liệu để đảm bảo tính bảo mật. Mỗi phiếu bầu được mã hóa và lưu trữ trên một chuỗi khối phân tán. Việc thay đổi dữ liệu trên blockchain là cực kỳ khó khăn do yêu cầu sự đồng thuận của hầu hết các nút trong mạng. Điều này ngăn chặn gian lận và đảm bảo tính minh bạch.
* Câu hỏi: Làm thế nào để đảm bảo mỗi cử tri chỉ được bỏ phiếu một lần trong hệ thống bỏ phiếu điện tử blockchain?
* Hệ thống có thể sử dụng các cơ chế như chữ ký số, mã token duy nhất hoặc ID điện tử để xác thực danh tính của cử tri. Mỗi cử tri được cấp một mã token hoặc khóa bí mật chỉ được sử dụng một lần. Khi họ bỏ phiếu, mã token này sẽ được ghi lại trên blockchain để tránh bỏ phiếu kép.
* Câu hỏi: Ai có thể xác minh kết quả bỏ phiếu trong hệ thống bỏ phiếu điện tử blockchain?
* Do tính minh bạch của blockchain, bất kỳ ai cũng có thể xác minh kết quả bỏ phiếu. Các nút trong mạng lưu trữ bản sao của sổ cái ghi lại mọi phiếu bầu. Các ứng cử viên, đảng phái, tổ chức giám sát bầu cử... đều có thể kiểm tra lại kết quả nếu cần thiết.

1. PHÂN TÍCH VÀ THIẾT KẾ
2. Tác nhân của hệ thống.

Hệ thống gồm các tác nhân:

| **Tác nhân** | **Mô tả** |
| --- | --- |
| Admin | - Quản trị viên hệ thống, có trách nhiệm xây dựng và quản lý hệ thống bỏ phiếu điện tử sử dụng công nghệ blockchain.  - Cấu hình và quản lý các thông tin liên quan đến quyền truy cập và phân quyền của các tác nhân khác trong hệ thống.  - Xác thực và phê duyệt các giao dịch bầu cử trong hệ thống.  - Đảm bảo tính bảo mật, toàn vẹn và minh bạch của hệ thống. |
| Đại biểu | - Người được ứng cử và đại diện cho ý chí của cử tri trong quá trình bỏ phiếu.  - Sử dụng giao diện điện tử để tham gia bỏ phiếu và gửi phiếu bầu vào hệ thống.  - Đảm bảo tính bí mật và an toàn của phiếu bầu.  - Theo dõi quá trình bỏ phiếu và kiểm tra kết quả bầu cử. |
| Cử tri | - Người dân hoặc thành viên trong cộng đồng có quyền bỏ phiếu và tham gia quá trình bầu cử.  - Đăng ký và xác thực thông tin cá nhân để có quyền bỏ phiếu trong hệ thống. |
|  | - Sử dụng giao diện điện tử để tham gia bỏ phiếu và gửi phiếu bầu vào hệ thống.  - Xem và xác minh thông tin liên quan đến đại biểu và các ứng cử viên.  - Theo dõi quá trình bầu cử và kiểm tra tính minh bạch và công bằng của hệ thống. |

Bảng – Các tác nhân của hệ thống

1. Các chức năng và module chính.

* *Module đăng ký cử tri*: Cho phép đăng ký và xác thực cử tri, cấp mã bỏ phiếu duy nhất cho mỗi cử tri.
* *Module đăng ký đại biểu*: Cho phép đăng ký và xác thực đại biểu trên blockchain.
* *Module bỏ phiếu*: Giao diện cho phép cử tri lựa chọn ứng cử viên và gửi phiếu bầu điện tử lên blockchain.
* *Module kiểm phiếu*: Tự động kiểm đếm phiếu và công bố kết quả bầu cử dựa trên dữ liệu trên blockchain.
* *Module minh bạch*: Cho phép công khai các thông tin như số cử tri đã bỏ phiếu, tổng số phiếu, kết quả bầu cử.
* *Module xác thực*: Sử dụng cơ chế ký số điện tử, mã token để đảm bảo tính xác thực và bảo mật.
* *Module phân quyền*: Phân quyền truy cập dựa trên vai trò người dùng khác nhau.
* *Module bảo trì*: Quản lý việc nâng cấp và bảo trì hệ thống.
* *Module lưu trữ dữ liệu*: Lưu trữ các dữ liệu bỏ phiếu điện tử trên blockchain.

1. Luồng hoạt động và quy trình bỏ phiếu.

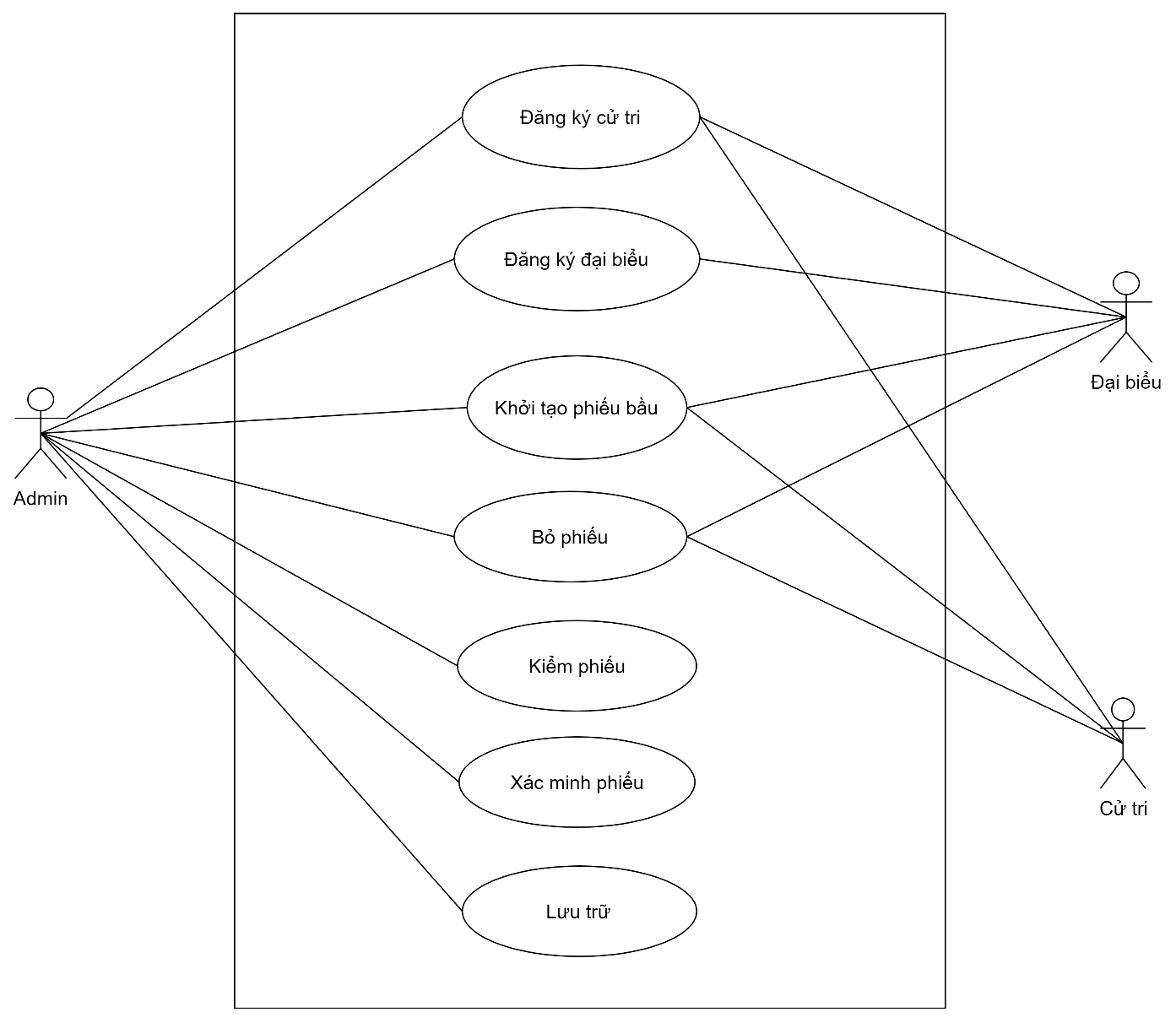
* *Đăng ký cử tri*: Cử tri đăng nhập vào tài khoản ví blockchain của mình. Hệ thống sẽ cấp một mã bỏ phiếu duy nhất cho mỗi cử tri.
* *Đăng ký đại biểu*:  Đại biểu có nhiệm vụ quản lý quá trình đăng ký và xác thực đại biểu.
* *Khởi tạo phiếu bầu*: Hệ thống khởi tạo một phiếu bầu điện tử cho mỗi cử tri đã đăng tạo tài khoản.
* *Bỏ phiếu*: Cử tri sử dụng tài khoản ví của mình để truy cập vào hệ thống, xem danh sách ứng cử viên và lựa chọn ứng cử viên mong muốn. Hệ thống ghi lại phiếu bầu và lưu lên blockchain.
* *Kiểm phiếu*: Hệ thống sẽ tự động kiểm đếm các phiếu bầu trên blockchain và công bố kết quả.
* *Xác minh phiếu*: Các bên liên quan có thể xác minh lại kết quả thông qua việc truy vấn trực tiếp lên blockchain.
* *Lưu trữ*: Toàn bộ dữ liệu bầu cử được lưu trữ bất biến trên blockchain.

1. Kiến trúc hệ thống và công nghệ sử dụng.

* *Blockchain platform*: Sử dụng một nền tảng blockchain như Ethereum để xây dựng hệ thống
* *Front-end*: Ứng dụng web (Dapp) cho phép người dùng tương tác với hệ thống. Sử dụng ReactJS, JavaScript.
* *Back-end*: Xây dựng các API phục vụ frontend và tích hợp với blockchain. Sử dụng ReactJS
* *Ví Blockchain*: Ví metamask
* *Database*: Lưu trữ dữ liệu người dùng, ứng cử viên, v.v.
* *Smart contracts*: Các smart contracts để thực thi các chức năng của hệ thống như khởi tạo phiếu bầu, kiểm phiếu, xác thực người dùng.
* *Cloud hosting*: Sử dụng các dịch vụ điện toán đám mây như AWS, Azure để lưu trữ và triển khai hệ thống.
* *Security layers*: Các tầng bảo mật như mã hóa, token, firewall để đảm bảo an toàn hệ thống.

1. Sơ đồ Usecase tổng quát.

* Dựa vào các module và luồng sự kiện mô tả ở trên, ta có được sơ đồ usecase tổng quát:



Hình – Sơ đồ usecase tổng quát của hệ thống

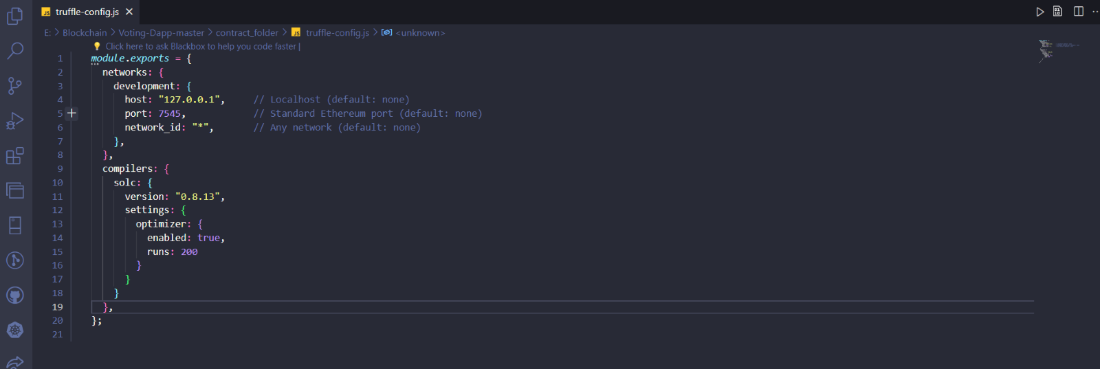
1. HIỆN THỰC HÓA HỆ THỐNG
2. Cài đặt thực nghiệm.

* **Các bước cài đặt:**
* Bước 1: Đầu tiên chúng ta cần một công cụ “Ganache Blockchain” - Ganache là bộ giả lập một mạng Blockchain trên máy tính cá nhân (local) của mình. Khi chúng ta chạy chương trình Ganache, nó sẽ tạo ra một mạng Blockchain giả lập có đầy đủ các tính năng như một mạng Blockchain thật sự (mạng Ethereum).



Hình – Tạo Blockchain giả lập với công cụ Ganache

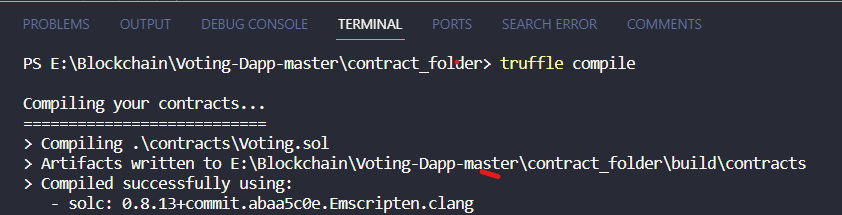
* Bước 2: Sau khi có Ganache Blockchain thì chúng ta phải kết nối tới file truffle để nó có thể tạo ra một mạng blockchain trên máy tính cá nhân của mình



Hình – Kết nối file “truffle-config.js”

* Bước 3: Tiếp theo chúng ta phải connect dự án Voting trên ganache của chúng ta bằng câu lệnh:

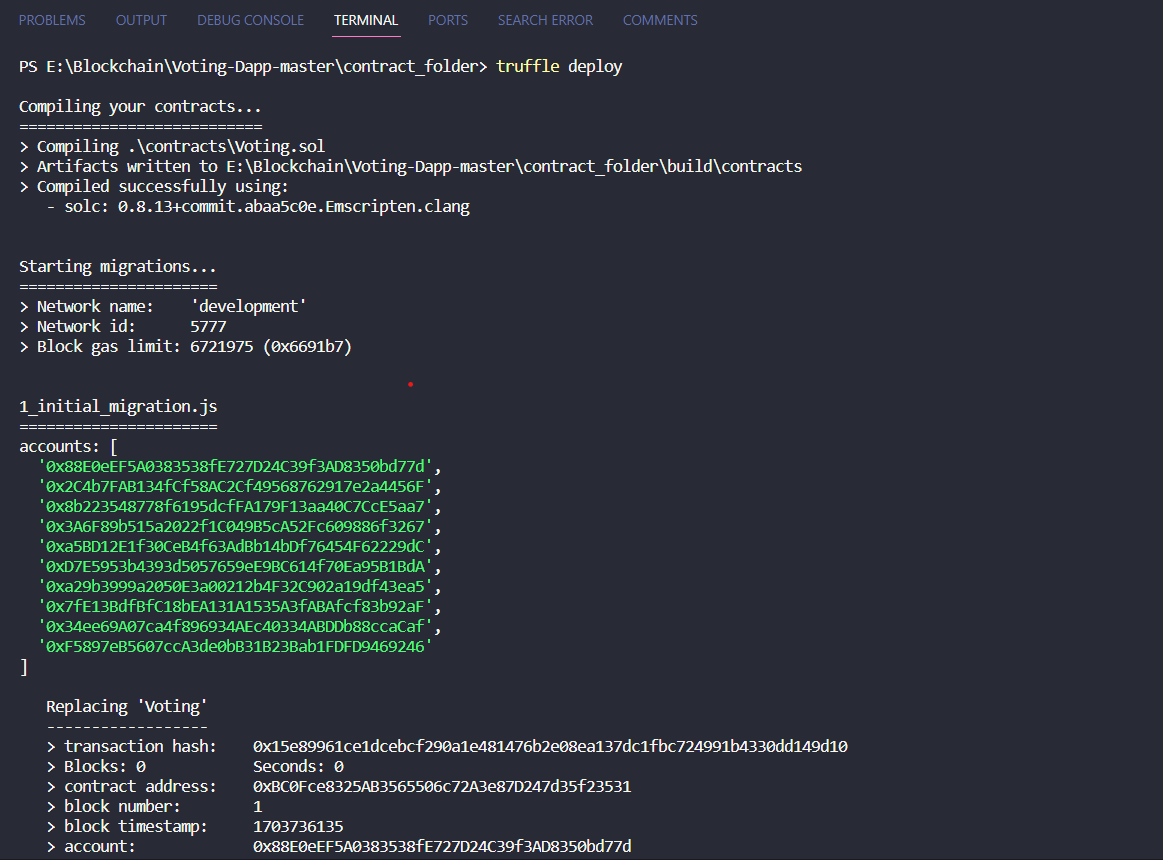
*truffle compile*



Hình – Connect dự án trên công cụ Ganache

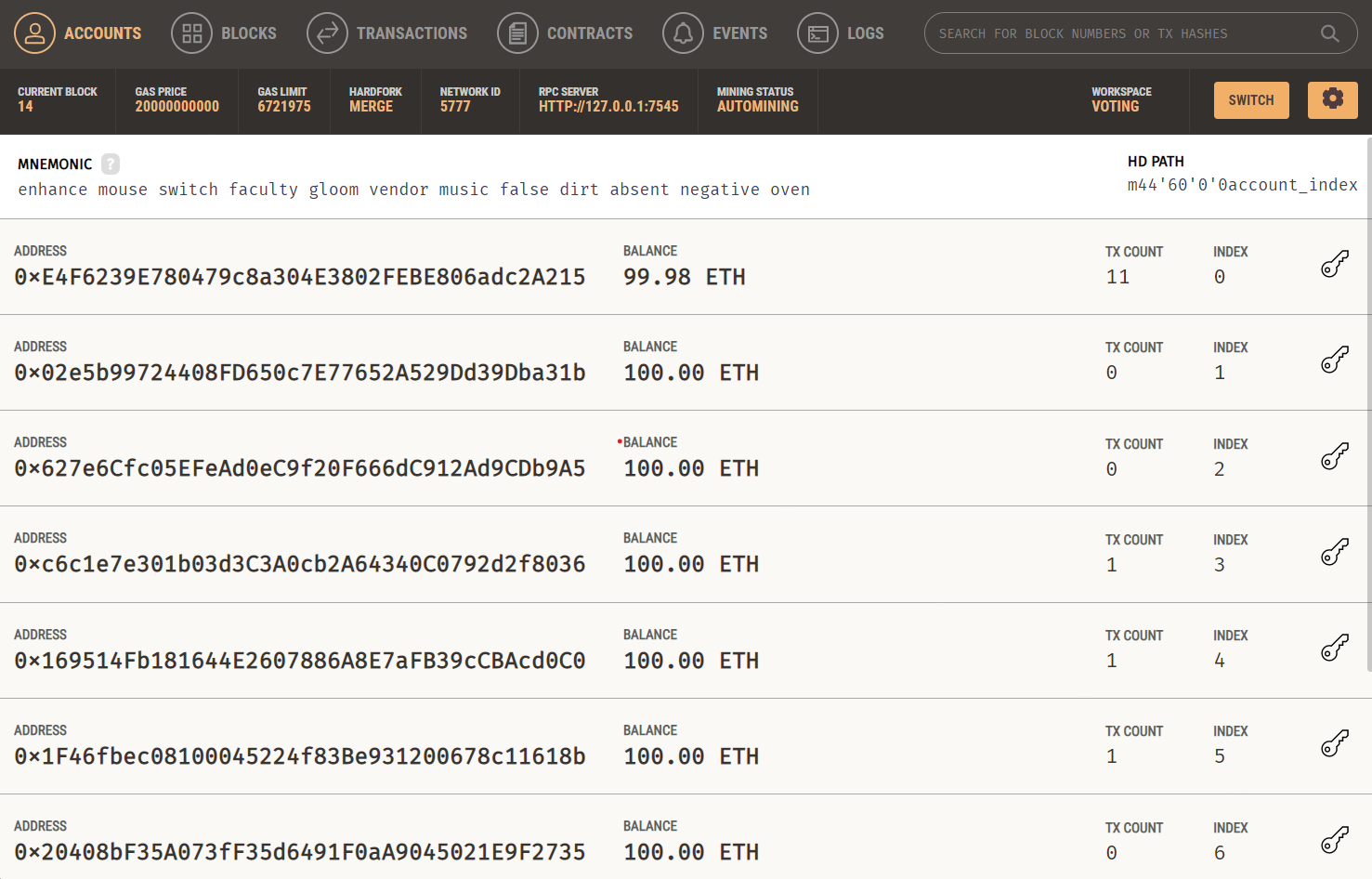
* Bước 4: Tiếp theo chúng ta phải Deploy dự án Voting trên ganache của chúng ta bằng câu lệnh:

*truffle deploy*



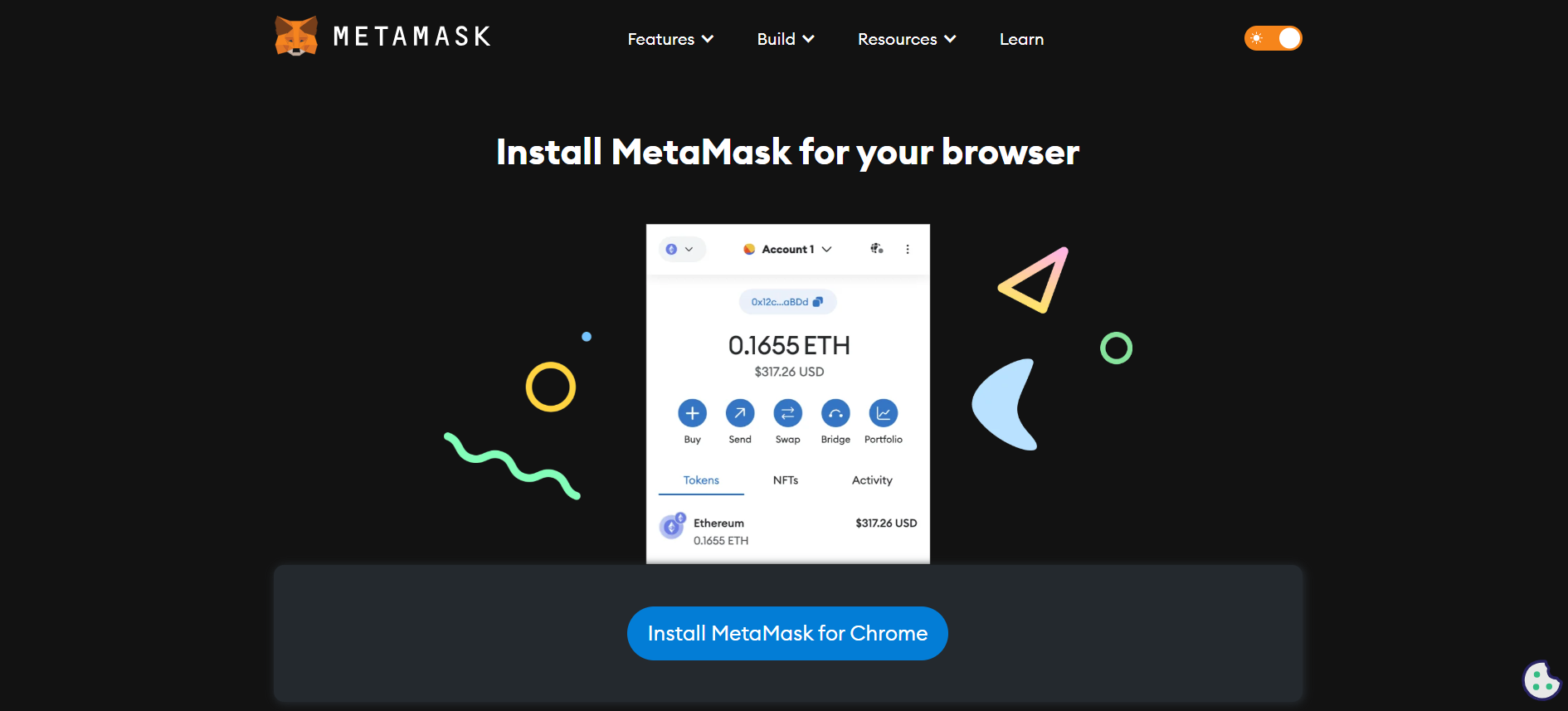
Hình – Deploy dự án Voting trên Ganache

* Bước 5: Sau đó chúng ta qua bên Account sẽ thấy có rất nhiều account được đánh số index 0 – 9, address và private key của từng account



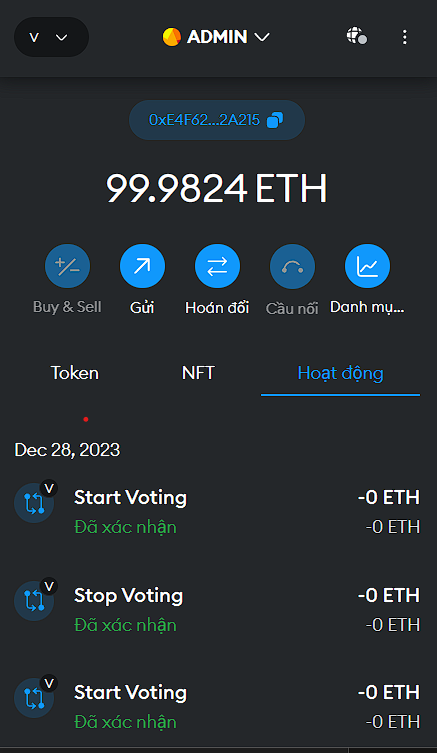
Hình – Address và private key của từng account

* Sau khi hoàn tất phần Ganeche thì chúng ta qua bên ví Metamask. Ở đây chúng ta sẽ tạo ra 1 ADMIN và 3 Voter.
* Bước 6: chúng ta phải tải ví metamask về trình duyệt



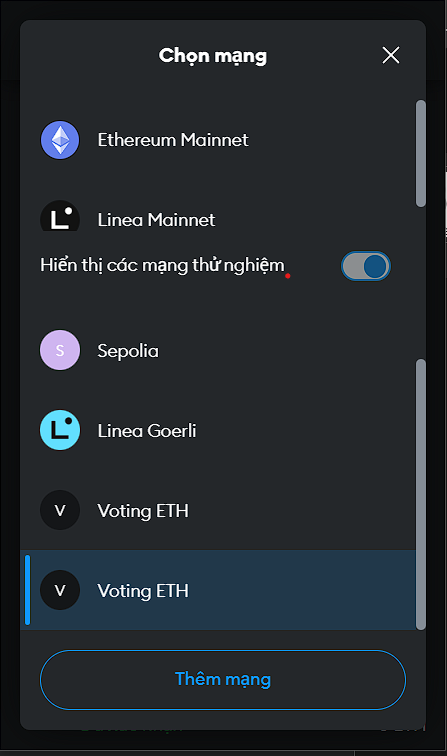
Hình – Download ví Metamask cho Chorme

* Bước 7: Tiếp theo chúng ta tạo tài khoản



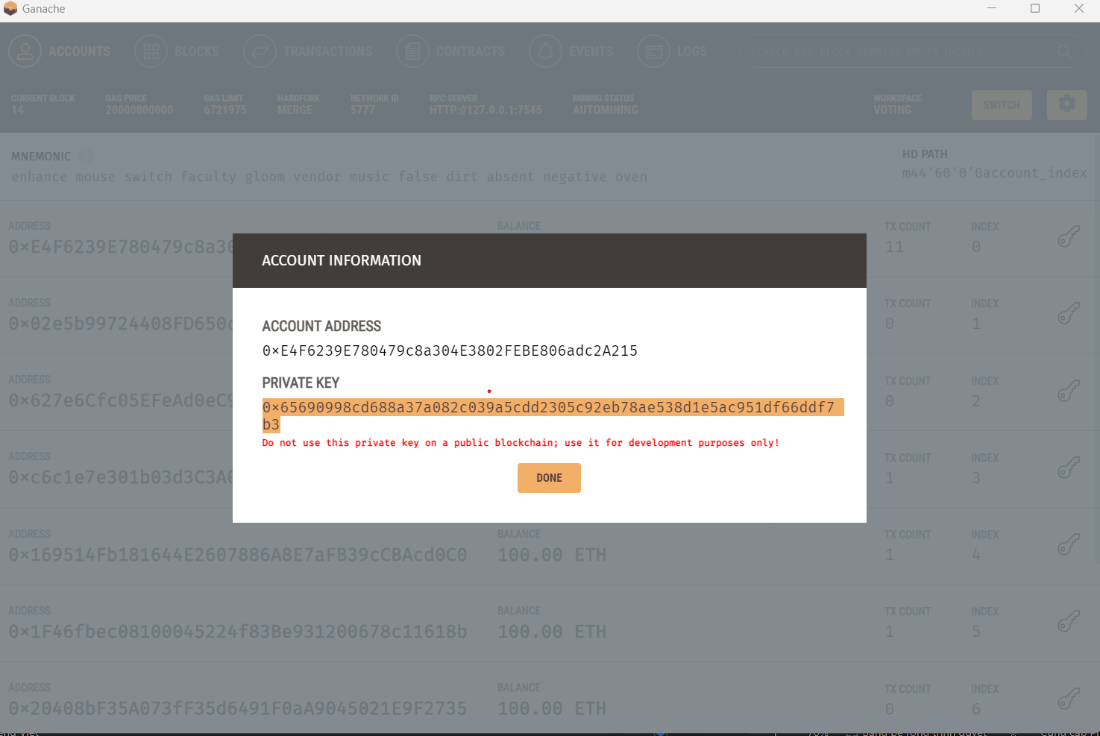
Hình – Tạo tài khoản vote

* Bước 8: Chúng ta sẽ tạo thêm cho mình một mạng riêng bằng cách thêm mạng thủ công



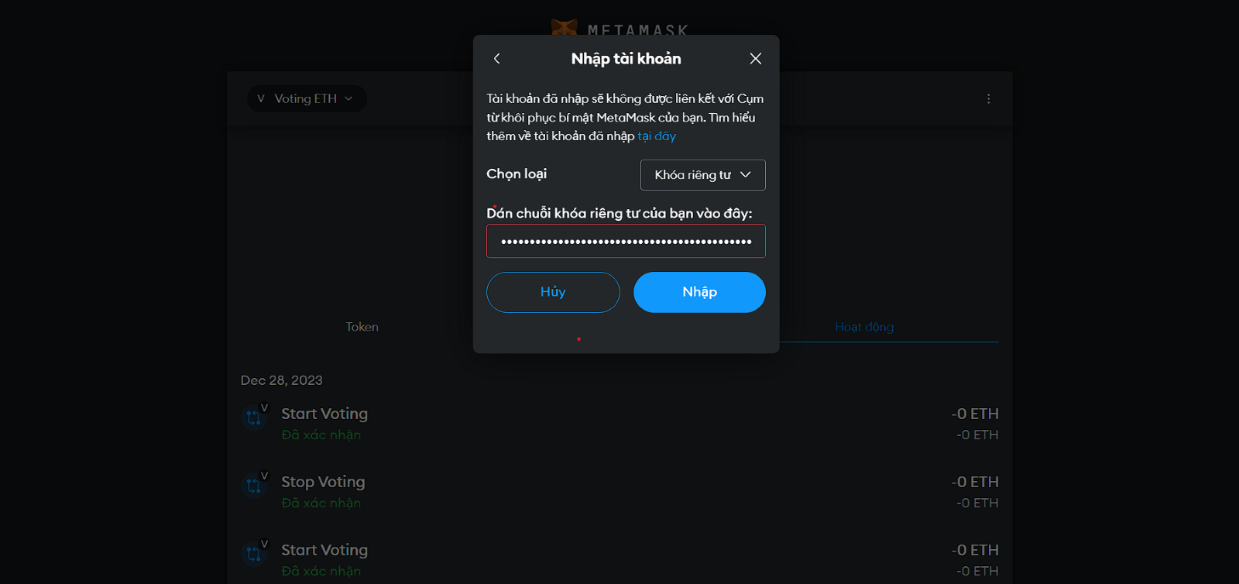
Hình – Tạo mạng riêng

* Bước 9: Sau đó chúng ta sẽ tạo tài khoản ADMIN bằng cách copy private key trên Ganache



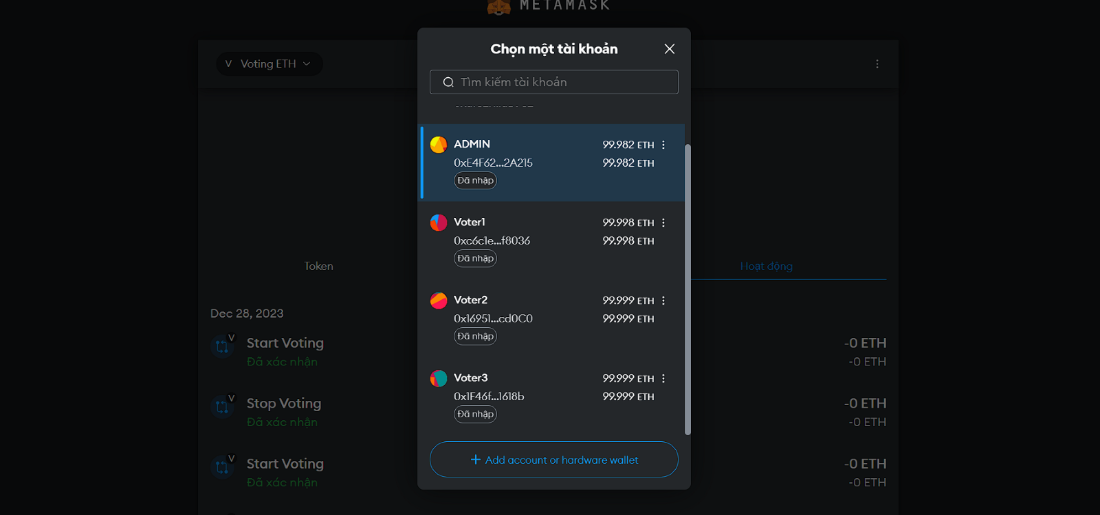
Hình – Tạo tài khoản Admin

* Bước 10: Sau đó chúng ta nhập đoạn private key này vào trong ô tạo tài khoản bằng private key



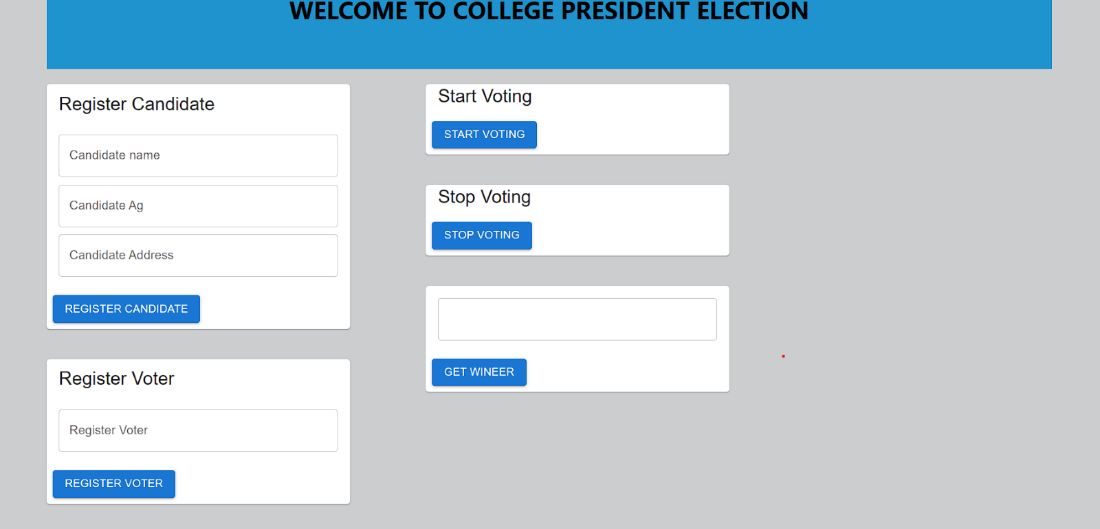
Hình – Nhập private key vào tài khoản

* Bước 11: Tiếp đến tài khoản Voter cũng như thế, chúng ta sẽ có các tài khoản sau



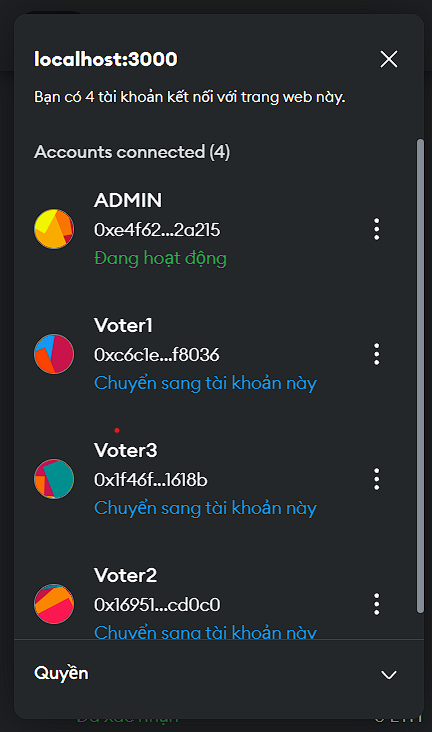
Hình – Thực hiện tương tự với Voter

* Bước 12: Sau khi đã connect và deploy trên ganache và đã có tài khoản Metamask. Chúng ta sẽ chạy dự án của mình



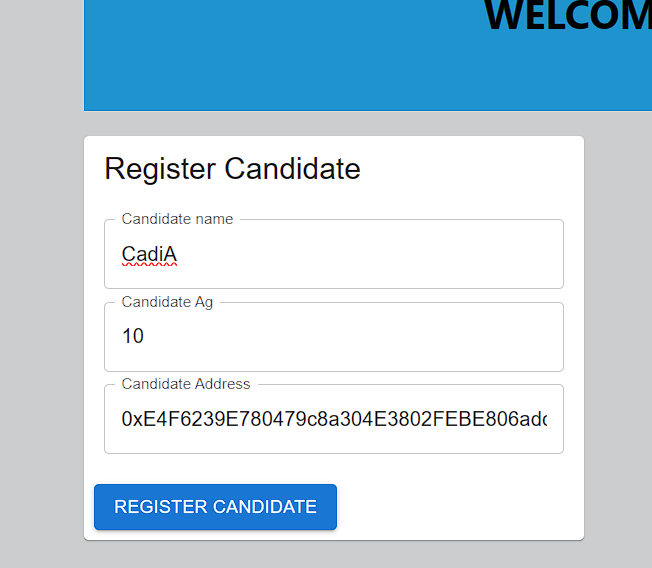
Hình – Chạy thực nghiệm dự án

* Bước 13: Sau đó chúng ta sẽ kết nối ví metamask



Hình – Kết nối với ví Metamask

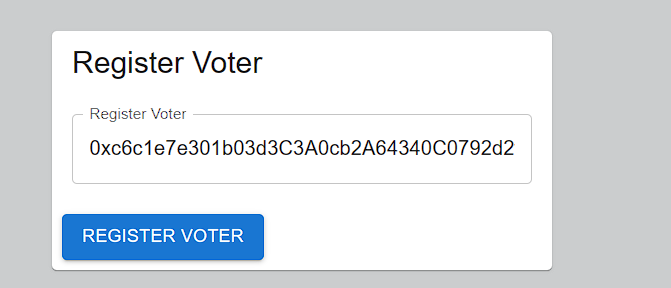
* Bước 14: Sau khi kết nối được với ví, chúng ta sẽ nhập các input



Hình – Cập nhật các input

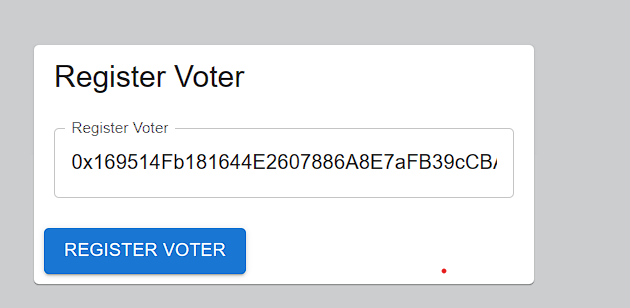
* Bước 15: Tiếp đến sẽ là input của Voter

+ Voter 1:



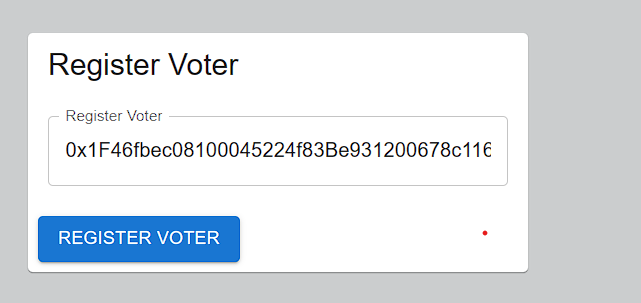
Hình – Input voter 1

+ Voter 2:



Hình – Input voter 2

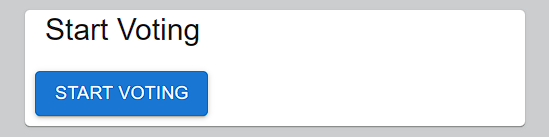
+ Voter 3:



Hình – Input voter 3

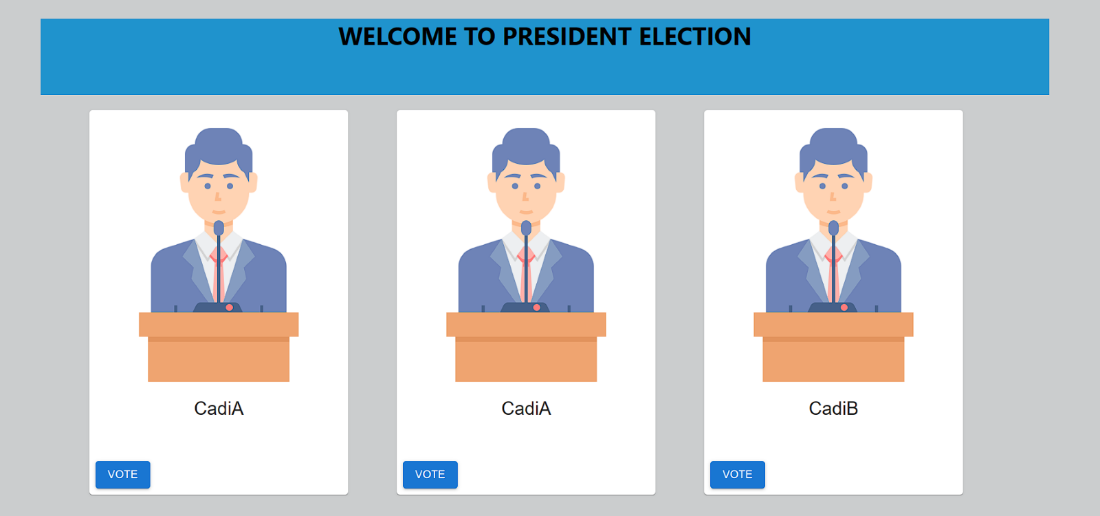
1. Kết quả thực nghiệm.

* Sau khi đã cài đặt thực nghiệm theo từng bước trên hệ thống, thì chúng ta sẽ bắt đầu thực hiện vote
* Sau khi đã có dữ liệu chúng ta sẽ bất đầu ấn vào “START VOTING” để Vote:



Hình – Bắt đầu Vote

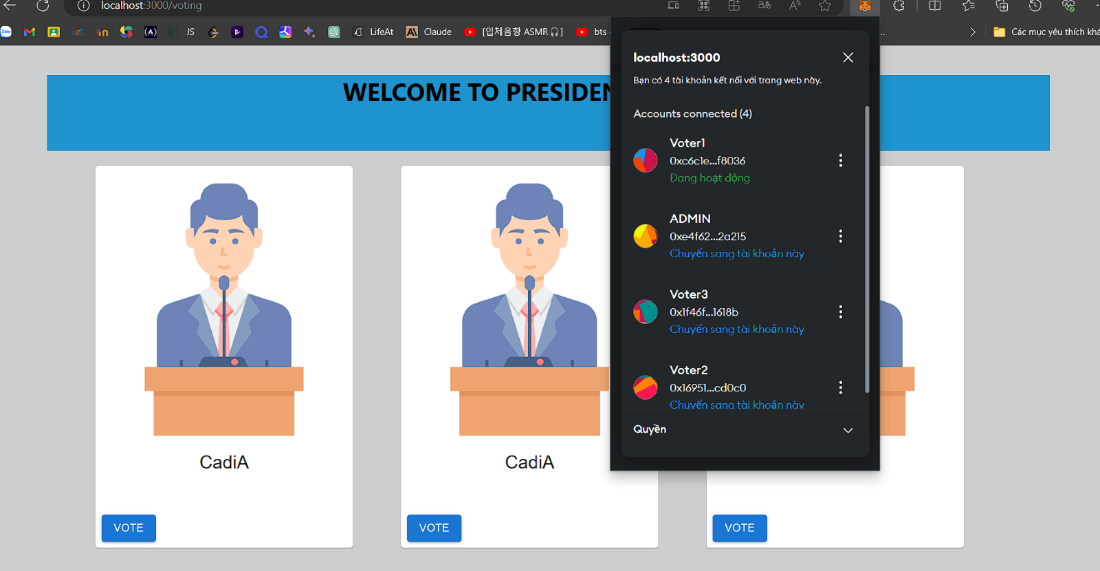
* Tiếp theo, chúng ta sẽ qua trang voting - ‘http://localhost:3000/voting’



Hình – Chuyển hướng sang trang voting

* Tại đây, chúng ta sẽ bình chọn, nhưng nếu muốn bình chọn chúng ta phải chuyển qua tài khoản Voter

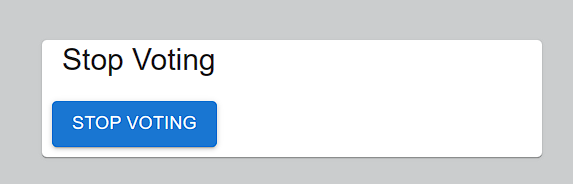
+ Nếu muốn bình chọn cho CadiA thì chúng ta phải chuyển qua tài khoản Voter1:



Hình – Chuyển qua tài khoản Voter1

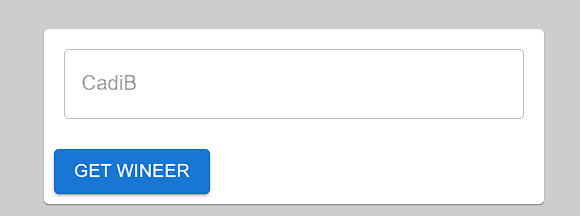
+ Cũng như nếu muốn bình chọn cho CadiB thì chúng ta thực hiện tương tự là sẽ chuyển qua tài khoản Voter 2 hoặc Voter3

* Chúng ta sẽ bầu cho CadiA: 1 phiếu và CadiB: 2 phiếu
* Sau khi bình chọn xong chúng ta sẽ quay lại trang chủ và chuyển đổi sang tài khoản ADMIN, tiếp theo chúng ta sẽ ngưng cuộc bình chọn này lại bằng cách nhấn vào “Stop Voting”



Hình – Chuyển đổi sang tài khoản ADMIN để dừng voting

* Và kết quả cuối cùng sẽ hiển thị ra người được người chiến thắng.



Hình – Kết quả người chiến thắng

1. ĐÁNH GIÁ VÀ KẾT LUẬN
2. Đánh giá chung.

Qua quá trình thiết kế và xây dựng hệ thống, ta thấy được việc xây dựng hệ thống bỏ phiếu điện tử sử dụng công nghệ blockchain là một quá trình phức tạp và đòi hỏi sự cân nhắc kỹ lưỡng. Mặc dù có nhiều lợi ích tiềm năng, cần đối mặt với các thách thức về bảo mật, quyền riêng tư, mở rộng, chấp nhận từ các bên liên quan và sự tin cậy của công nghệ. Việc thực hiện thành công một hệ thống bỏ phiếu điện tử sử dụng công nghệ blockchain đòi hỏi sự kết hợp giữa công nghệ, chính sách và sự hỗ trợ từ cộng đồng liên quan. Dưới đây là một đánh giá của đề tài:

* Công nghệ blockchain có tiềm năng cung cấp một môi trường bảo mật cao, nhưng việc đảm bảo an toàn cho hệ thống bỏ phiếu điện tử vẫn là một thách thức. Cần đảm bảo rằng kỹ thuật mã hóa mạnh mẽ được sử dụng để bảo vệ dữ liệu phiếu bầu và thông tin cá nhân của người dùng. Ngoài ra, cần xem xét các biện pháp bảo vệ chống lại các cuộc tấn công như tấn công 51%, tấn công kỹ thuật số và tấn công từ bên trong.
* Việc bảo vệ quyền riêng tư của cử tri và người tham gia trong quá trình bỏ phiếu là một yếu tố quan trọng. Cần thiết kế hệ thống sao cho thông tin cá nhân không bị tiết lộ và chỉ có những người được ủy quyền mới có thể truy cập vào dữ liệu phiếu bầu. Việc sử dụng các phương pháp mã hóa và chứng thực danh tính có thể giúp đảm bảo quyền riêng tư của người dùng.
* Một hệ thống bỏ phiếu điện tử thành công cần có khả năng xử lý một lượng lớn giao dịch bầu cử. Công nghệ blockchain cung cấp khả năng mở rộng ngang hàng (horizontal scalability) và khả năng mở rộng dọc (vertical scalability) để đáp ứng nhu cầu của quá trình bỏ phiếu. Tuy nhiên, việc đảm bảo hiệu suất và tốc độ xử lý của hệ thống là một yếu tố quan trọng để đảm bảo trải nghiệm người dùng tốt và tránh tình trạng quá tải.
* Để thành công, một hệ thống bỏ phiếu điện tử cần có sự chấp nhận và tham gia từ các bên liên quan như cử tri, đại biểu và cơ quan chính phủ. Cần tiến hành các cuộc thảo luận và xây dựng sự đồng thuận để đảm bảo rằng hệ thống được công nhận là đáng tin cậy và công bằng. Đồng thời, cần giải quyết các mối quan ngại về an ninh, quyền riêng tư và tính bảo mật của các bên liên quan.
* Công nghệ blockchain đã được chứng minh là tin cậy và an toàn trong nhiều lĩnh vực khác nhau. Tuy nhiên, việc triển khai một hệ thống bỏ phiếu điện tử sử dụng công nghệ này đòi hỏi sự kiểm tra và xác minh kỹ lưỡng. Cần đảm bảo rằng công nghệ blockchain được triển khai đúng cách, và các lỗ hổng bảo mật và vấn đề kỹ thuật khác được giải quyết một cách nhanh chóng và hiệu quả.
* Việc xây dựng hệ thống bỏ phiếu điện tử sử dụng công nghệ blockchain đòi hỏi sự thay đổi văn hóa và pháp lý. Cần có sự chấp nhận và sẵn lòng thay đổi từ các bên liên quan, bao gồm chính phủ, các tổ chức bầu cử, và cử tri. Ngoài ra, cần xem xét và thực hiện các quy định pháp lý và quyền lực cho việc sử dụng công nghệ blockchain trong quá trình bỏ phiếu, điều này có thể bao gồm việc cập nhật luật bầu cử hiện hành và xác định rõ vai trò của các bên liên quan trong việc xác minh và giám sát quá trình bỏ phiếu.

1. Kết luận.

Tóm lại, hệ thống bỏ phiếu điện tử "Voting Chain" sử dụng công nghệ blockchain, ví Metamask và các tiện ích hỗ trợ khác có tiềm năng đem lại nhiều lợi ích như tính an toàn, minh bạch, công bằng, xác thực dễ dàng, tiện lợi và khả năng theo dõi. Tuy nhiên, việc triển khai một hệ thống như vậy đòi hỏi sự đánh giá kỹ lưỡng và xem xét các vấn đề liên quan đến bảo mật, quyền riêng tư và khả năng mở rộng của blockchain. Ngoài ra, cần có sự cân nhắc và tham gia của các bên liên quan để đảm bảo sự thành công và chấp nhận của công nghệ Blockchain.

# TÀI LIỆU THAM KHẢO

* + - 1. Tài liệu môn học thuộc khoa công nghệ thông tin của trường đại học Tôn Đức Thắng
      2. [Wikipedia. Decentralized application.](https://en.wikipedia.org/wiki/Decentralized_application)
      3. [Pum. (Apr 06, 2023). DAPP LÀ GÌ? DAPP HAY NHƯNG CÓ HOÀN HẢO.](https://200lab.io/blog/dapp-la-gi/)
      4. [Obaotrinh. (Aug 23, 2023). Blockchain là gì? Ưu & nhược điểm của các ứng dụng Blockchain.](https://200lab.io/blog/uu-va-nhuoc-diem-cua-blockchain/)
      5. [VBPO. Blockchain là gì? Hoạt động của Blockchain như thế nào? Ứng dụng ra sao?](https://vbpo.com.vn/news/blog-40/blockchain-la-gi-hoat-dong-cua-blockchain-nhu-the-nao-ung-dung-ra-sao)
      6. [NESTECH. (05/04/2023). ỨNG DỤNG CỦA CÔNG NGHỆ BLOCKCHAIN TẠI VIỆT NAM.](https://nestech.vn/ung-dung-cua-cong-nghe-blockchain-tai-viet-nam/)
      7. [Werner Vermaak. (2 years ago). MetaMask là gì?.](https://coinmarketcap.com/academy/vi/article/what-is-metamask)
      8. [Lê Anh. (Jul 5,2021). Ethereum là gì? Tìm hiểu tổng quan về ETH cho người mới từ A - Z.](https://coin98.net/ethereum-la-gi)