TRƯỜNG ĐẠI HỌC CẦN THƠ
KHOA CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG
BỘ MÔN CÔNG NGHỆ THÔNG TIN

LUẬN VĂN TỐT NGHIỆP ĐẠI HỌC
NGÀNH CÔNG NGHỆ THÔNG TIN

ĐỀ TÀI

NGHIÊN CỨU ỨNG DỤNG BLOCKCHAIN TRONG XÂY DỰNG HỆ THỐNG VOTING

Phân hệ: Xây dựng hệ thống private blockchain cho ứng dụng bầu chọn

Sinh Viên: Cao Vĩnh Phát
Mã số: B1400981
Khóa: 40

Cần Thơ, tháng 11 năm 2018

TRƯỜNG ĐẠI HỌC CẦN THƠ

KHOA CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG
BỘ MÔN CÔNG NGHỆ THÔNG TIN

LUẬN VĂN TỐT NGHIỆP ĐẠI HỌC
NGÀNH CÔNG NGHỆ THÔNG TIN

ĐỀ TÀI

NGHIÊN CỨU ỨNG DỤNG BLOCKCHAIN TRONG XÂY DỰNG HỆ THỐNG VOTING

CÁN BỘ HƯỚNG DẪN
Ts. Trần Công Án

SINH VIÊN THỰC HIỆN
Tên: Cao Vĩnh Phát
MSSV: B1400981
Khóa: 40

Cần Thơ, tháng 11 năm 2018

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

•ꕥ🕮ꕥ•

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Cần Thơ, ngày tháng năm 2018

Giáo viên phản biện

(Ký và ghi rõ họ tên)

TS. Trần Công Án

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

•ஜ📖ஜ•

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Cần Thơ, ngày tháng năm 2018

Giáo viên phản biện

(Ký và ghi rõ họ tên)

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

•ஜ📖ஜ•

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Cần Thơ, ngày tháng năm 2018

Giáo viên phản biện

(Ký và ghi rõ họ tên)

LỜI CẢM ƠN

Trong suốt quá trình thực hiện đề tài luận văn em đã học hỏi được rất nhiều kinh nghiệm quý báo từ thực tế, gắn liền với những sự hỗ trợ, giúp đỡ, quan tâm, góp ý từ nhiều người và góp phần củng cố thêm kiến thức chuyên ngành. Bên cạnh đó, nó còn giúp em tự tin và vững bước hơn trên con đường học tập và làm việc sau này.

Với lòng biết ơn sâu sắc nhất, em xin gửi đến quý Thầy Cô khoa Công Nghệ Thông Tin – Trường Đại Học Cần Thơ đã cùng với tri thức và tâm huyết của mình để truyền đạt vốn kiến thức quý báu cho em trong suốt thời gian học tại trường.

Em xin chân thành cảm ơn TS. Trần Công Án đã tận tình chỉ bảo, truyền đạt những kinh nghiệm và cho em những nhận xét quý báu để em có thể hoàn thành tốt đề tài. Nếu không có những lời hướng dẫn và dạy bảo của thầy thì em nghĩ đề tài này của chúng em khó có thể hoàn thiện được. Một lần nữa, em xin chân thành cảm ơn thầy!

Xin cám ơn tất cả anh chị khóa trên và bạn bè đã động viên và giúp đỡ em rất nhiều trong thời gian thực hiện đề tài.

Mặc dù đã rất cố gắng để thực hiện đề tài một cách hoàn chỉnh nhất, nhưng trong một khoảng thời gian có hạn nên không thể tránh khỏi những thiếu sót cũng như những hạn chế. Rất mong nhận được sự góp ý của quý Thầy Cô để đề tài được hoàn thiện hơn.

MỤC LỤC

DANH MỤC HÌNH

DANH MỤC BẢNG

KÍ HIỆU VÀ VIẾT TẮT

Ký hiệu	**Giải thích**
Framework	Là tập hợp các thư viên phần mềm
Client	Là máy tính cá nhân của người dùng
Server	Là máy chủ để chạy hệ thống
DLT	Distributed Ledger
DApps	Decentralized Applications
Method	Cách gọi một phương thức hay một hàm trong chương trình máy tính.
P2P	Peer-to-Peer
GB	Gigabyte
Bytecode	Là kết quả của mã nguồn sau khi được biên dịch
MVC	Model-View-Controller
Node	Là một máy tính trong mạng lưới
IP	Địa chỉ mạng máy tính
Port	Cổng trong mạng
Admin	Người quản trị hệ thống

ABSTRACT

The form of paper voting has been widely used in the world. This is very simple, you just need to write into paper and put it on a ballot. At the end of the vote, the ballots are checked by counting back and the person with the most votes will be the winner. Another form is the form of electronic voting. This form has many advantages over paper voting but there are some disadvantages such as: the ballot will be concentrated in one place. In such forms of voting, Voting results will be affected by issues such as swapping votes or modified voting results, problem voters holding ballots or voting system data on the attack.

There are many other reasons to point out that such elections are risky. To fix the problems we need a voting system which can handle rapidly and conveniently transparently. With the development of the available technology today, people have invented and applied the Ethereum blockchain network which has many advantages.

The subject construction of "Blockchain applications research in building up Voting System" helps all the elect become fairer.

This system provides for three types of users:

Voters: register, login, vote, edit your personal information, change the name, search and see the history of the election and voting results.

Organizers/Creators: register, login, create a poll, vote, edit your personal information, change the name, search or see the history of the election or results.

Admin: log in, update your profile, change your password, see the history of voting, create a poll, approve voting, search, view the vote.

The system which has been developed consisting of two components: the network blockchain with geth command line interface and website display using the framework as ExpressJs, Web3. JS Reactjs based on the client-server model and the model Flux.

TÓM TẮT

Hình thức bỏ phiếu giấy từ lâu đã được sử dụng rộng rãi trên thế giới. Điều này rất đơn giản, bạn chỉ cần viết phiếu bầu của mình lên giấy và đặt nó vào một thùng phiếu. Vào cuối cuộc bầu chọn, các phiếu bầu được kiểm tra bằng cách đếm lại và người được nhiều phiếu bầu nhất sẽ là người thắng cuộc. Một hình thức khác là bỏ phiếu điện tử. Hình thức này có nhiều ưu điểm hơn bỏ phiếu giấy nhưng vẫn có những bất cập như: Phiếu bầu sẽ được tập trung tại một nơi. Trong những hình thức bầu chọn như vậy, kết quả bầu chọn sẽ bị ảnh hưởng bởi các vấn đề như: phiếu bầu bị trao đổi hay kết quả bầu chọn bị chỉnh sửa, người giữ các phiếu bầu có vấn đề hay hệ thống lưu dữ liệu về cuộc bầu chọn bị tấn công…

Còn rất nhiều những lý do nữa để chỉ ra các cuộc bầu chọn kiểu như vậy có nhiều rủi ro. Để khắc phục các nhược điểm trên chúng ta cần một hệ thống bầu chọn có thể xử lý tiện lợi nhanh chóng và đặc biệt là minh bạch không thể bị sửa đổi được. Với sự phát triển của công nghệ hiện nay, người ta đã phát minh ra và đưa vào ứng dụng mạng lưới blockchain Ethereum với nhiều ưu điểm vượt trội.

Đề tài "Nghiên cứu ứng dụng Blockchain trong xây dựng hệ thống Voting" giúp mọi việc bầu chọn có thể trở nên công bằng hơn.

Hệ thống này cung cấp chức năng cho 3 kiểu người dùng:

Người bầu chọn: đăng ký, đăng nhập, bầu chọn, chỉnh sửa thông tin cá nhân, đổi tên, xem lịch sử bầu, xem kết quả bầu chọn, tìm kiếm.

Người tạo bầu chọn: đăng ký, đăng nhập, tạo cuộc bầu chọn, bầu chọn, chỉnh sửa thông tin cá nhân, đổi tên, xem lịch sử bầu, xem kết quả bầu chọn, tìm kiếm.

Admin: đăng nhập, cập nhật hồ sơ, đổi mật khẩu, xem lịch sử bầu chọn, tạo cuộc bầu chọn, phê duyệt cuộc bầu chọn, tìm kiếm, xem cuộc bầu chọn.

Hệ thống được phát triển gồm hai thành phần: Mạng lưới blockchain với geth command line và giao diện website sử dụng các framework như ExpressJs, Web3. js Reactjs dựa theo mô hình client server và mô hình Flux.

PHẦN GIỚI THIỆU

1. Đặt vấn đề.

Blockchain đang được thừa nhận là cuộc cách mạng thứ 5 của khoa học máy tính, phần còn thiếu của cuộc cách mạng Internet. Đây là lý do Blockchain thu hút hàng triệu người tham gia và tìm hiểu về cuộc cách mạng này. Blockchain tạo ra lòng tin vào dữ liệu số. Khi thông tin được ghi vào cơ sở dữ liệu Blockchain gần như không thể thay đổi hay xóa dữ liệu đó đi. Đây là điều chưa bao giờ tồn tại trong kỷ nguyên trước đó. Điều đặc biệt ở Blockchain là các cá nhân tham gia bảo quản, vận hành Blockchain mà không cần phải tin tưởng lẫn nhau, thậm chí có thể là đối thủ kinh doanh với nhau.

Với việc dữ liệu không bị thay đổi được mỗi khi được lưu vào mạng lưới Blockchain giúp cho việc xây dựng các ứng dụng như hệ thống bầu chọn trực tuyến, chuyển tiền online,... có sự minh bạch rõ ràng và công bằng hơn. Chính vì với những ưu điểm vượt trội vừa nếu của Blockchain. Chúng tôi quyết định thực hiện ứng dụng công nghệ này để xây dụng hệ thống bầu chọn dựa trên nền tảng mạng lưới private Blockchain Ethereum.

2. Phạm vi nghiên cứu và mục tiêu đề tài.

2.1. Phạm vi nghiên cứu.

Đề tài tập trung nghiên cứu xây dựng một mạng lưới blockchain riêng cho hệ thống bầu chọn, xây dựng smart contract để lưu trữ dữ liệu cho hệ thống và nghiên cứu reactjs để ứng dụng vào việc xây dựng giao diện cho hệ thống.

2.2. Mục tiêu đề tài.

2.2.1. Nghiên cứu công nghệ blockchain.

Hiểu rõ kiến thức về blockchain, ứng dụng của blockchain đối với thời đại mới. Hiểu về cách thức hoạt động và áp dụng được mạng lưới blockchain ethereum vào thực tiển.

2.2.2. Xây dựng hệ thống voting.

Xây dựng mạng lưới blockchain dựa trên nền tảng blockchain ethereum nhằm hỗ trợ cho việc xây dựng một hệ thống website bầu chọn công bằng và minh bạch.

2.3. Nội dung nghiên cứu.

STT	Tên công việc	Phát	Tiến
1	Tạo smart contract	x	
2	Vẽ Use Case		x
3	Cài đặt đăng ký		x
4	Cài đặt đăng nhập		x

5	Cập nhật thông tin cá nhân	x	
6	Cài đặt đổi mật khẩu		x
7	Cài đặt tạo cuộc bầu chọn	x	
8	Lấy danh sách lịch sử bầu chọn		x
9	Lấy danh sách bầu chọn của user		x
10	Lấy danh sách tất cả các cuộc bầu chọn	x	
11	Tìm kiếm cuộc bầu chọn		x
12	Bầu chọn	x	
13	Lấy danh sách các ứng cử viên		x
14	Xử lý kết quả bầu chọn	x	
15	Phê duyệt bầu chọn	x	
16	Xây dựng mạng blockchain	x	
17	Cài đặt smart contract	x	
18	Viết tài liệu phần giao diện chức năng của đăng ký, đăng nhập, lịch sử bầu chọn		x
19	Viết tài liệu phần giao diện chức năng của tạo bầu chọn, bầu chọn, tìm kiếm, cập nhật thông tin, đổi mật khẩu	x	
20	Viết báo luận văn	x	x
21	Viết slide báo cáo	x	x
22	Nghiên cứu về Blockchain	x	x
23	Nghiên cứu về Ethereum	x	x
24	Nghiên cứu Reactjs		x
25	Nghiên cứu về Ipfs		x
26	Nghiên cứu về web3js	x	
27	Nghiên cứu về sodility	x	

Bảng 1 Nội dung nghiên cứu

3. Bố cục luận văn.

Luận văn được tổ chức theo bố cục sau đây:

- **Phần giới thiệu:** Giới thiệu đề tài và nêu lên một số vấn đề liên quan đến lĩnh vực nghiên cứu từ đó đề xuất hướng giải quyết.
- **Phần nội dung**: gồm 4 chương.
    - Chương 1: Đặt tả và yêu cầu.
    - Chương 2: Cơ sở lý thuyết.
    - Chương 3: Thiết kế và cài đặt ứng dụng.
    - Chương 4: Kiểm thử và kết quả.
- **Phần kết luận**: tổng kết kết quả đạt được, ưu điểm và hạn chế của hệ thống đề xuất từ đó kiến nghị hướng phát triển.
- **Phần tài liệu tham khảo.**

PHẦN NỘI DUNG
CHƯƠNG 1: ĐẶC TẢ VÀ YÊU CẦU

1. Đặc tả đề tài.

Hệ thống bầu chọn trực tuyến là nơi cho phép người dùng tạo ra các cuộc bầu chọn mà mình muốn. Mọi người đều có thể tham gia bầu chọn cho những cuộc bầu chọn mà mình thích bằng cách đăng ký tài khoản tại hệ thống. Đối với người dùng muốn tạo cuộc bầu chọn thì có thể đăng ký một tài khoản tại hệ thống và chọn quyền là tạo cuộc bầu chọn. Người dùng có thể tạo nhiều cuộc bầu chọn khác nhau với các loại bầu chọn khác nhau như: chọn một ứng cử viên, chọn tùy ý hoặc chọn theo số lượng quy định. Đề tài áp dụng các công nghệ mới như nền tảng blockchain ethereum, hệ thống lưu trữ file phân tán IPFS, xây dựng smartcontract với ngôn ngữ solidity.

2. Các chức năng của hệ thống.

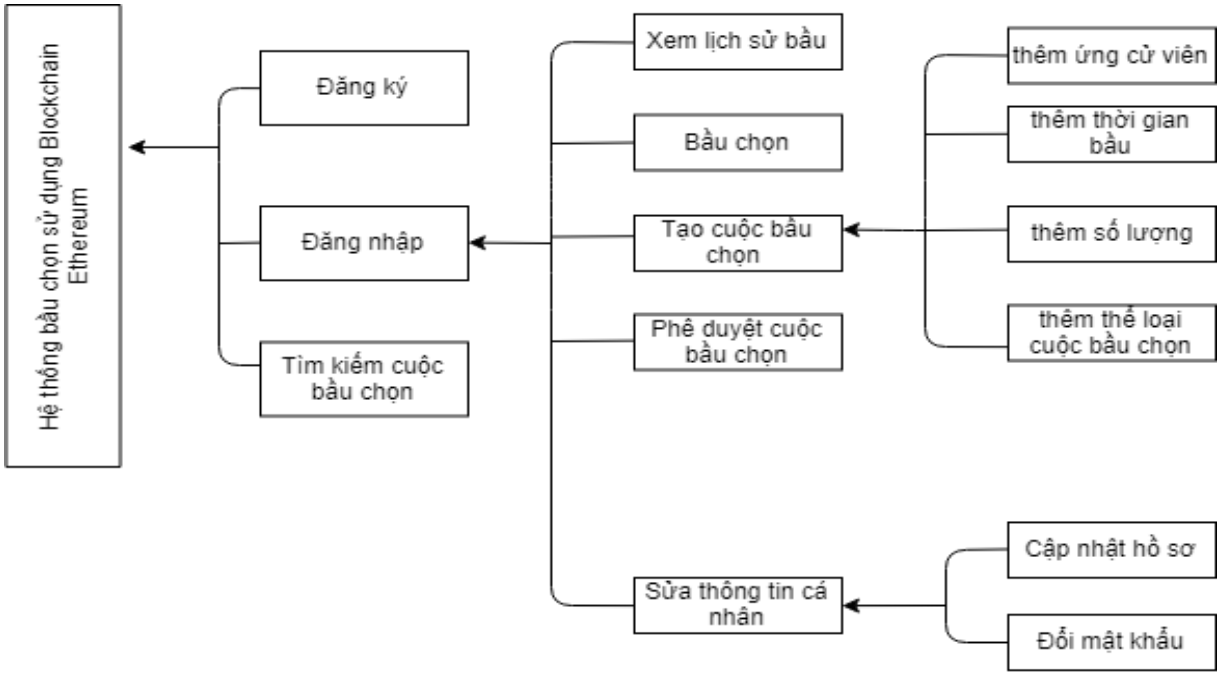
2.1. Bảng chức năng.

Các chức năng của hệ thống bao gồm: Đăng ký, đăng nhập, tìm kiếm, cập nhật tên người dùng, cập nhật hồ sơ, tạo bầu chọn, bầu chọn… Chức năng chi tiết của hệ thống sẽ được mô tả và phân tích trong phần nội dung chương 2 thiết kế và cài đặt giải pháp.

STT	Mã chức năng	Tên chức năng
1	DG01	Đăng ký
2	DG02	Đăng nhập
3	DG03	Đổi mật khẩu
4	DG04	Cập nhật hồ sơ
5	DG05	Tạo cuộc bầu chọn
6	DG06	Bầu chọn
7	DG07	Tìm kiếm
8	DG08	Xem lịch sử bầu chọn
9	DG09	Xem danh sách cuộc bầu chọn
10	DG10	Xem kết quả cuộc bầu chọn
11	DG11	Phê duyệt bầu chọn

12	DG12	Tạo ứng cử viên

Bảng 1. 1.Bảng chức năng hệ thống

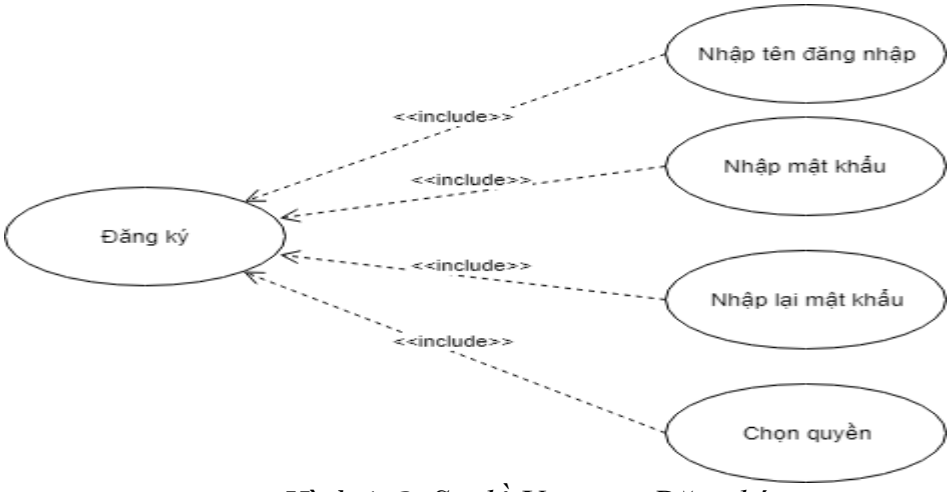


Hình 1. 1. Sơ đồ phân cấp chức năng

2.2. Sơ đồ use case.

2.2.1. Use case "Đăng ký".

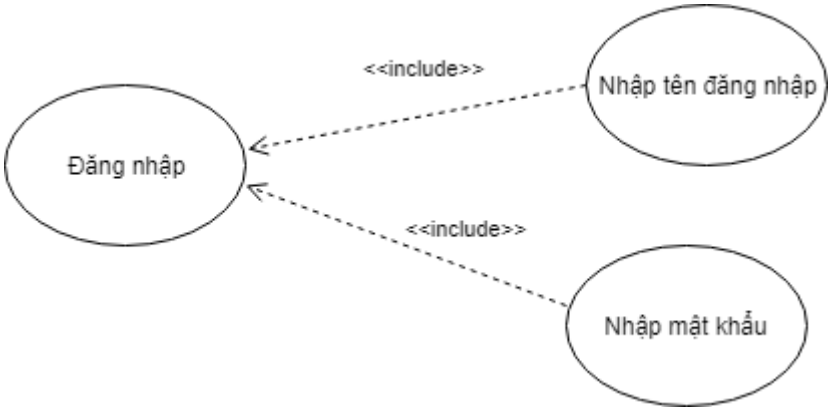
- Tác nhân: người bầu chọn, người tạo cuộc bầu chọn.
- Điều kiện: Mở được hệ thống bầu chọn sử dụng mạng lưới private Blockchain Ethereum.
- Mô tả: Để đăng ký, cần nhập đầy đủ các thông tin như tên đăng nhập, mật khẩu, nhập lại mật khẩu và chọn quyền.



Hình 1. 2. Sơ đồ Use case Đăng ký

2.2.2. Use case “Đăng nhập”.

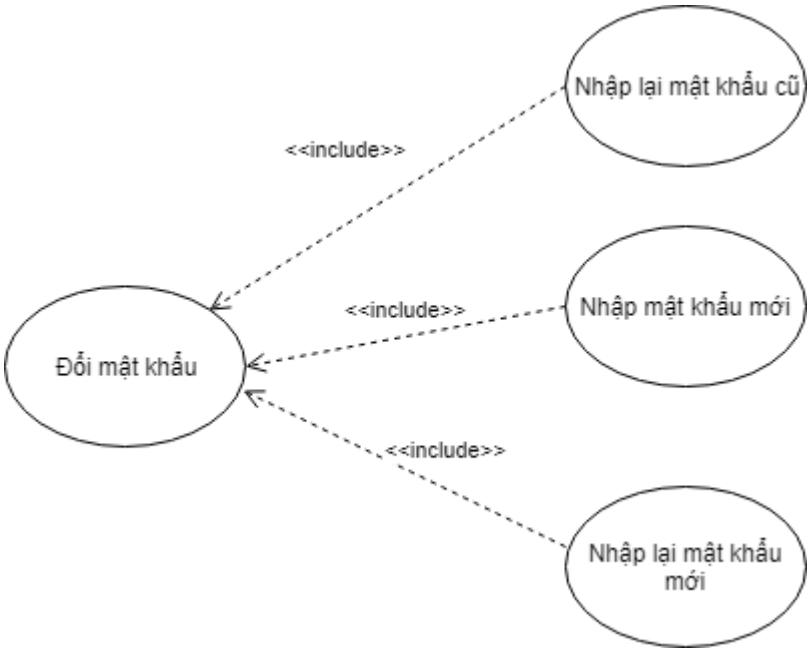
- Tác nhân: người bầu chọn, người tạo cuộc bầu chọn, admin.
- Điều kiện: mở được hệ thống bầu chọn sử dụng mạng lưới Blockchain Ethereum.
- Mô tả: Để đăng nhập, cần nhập đúng tên đăng nhập và mật khẩu.



Hình 1. 3. Sơ đồ Use case Đăng nhập

2.2.3. Use case “Đổi mật khẩu”.

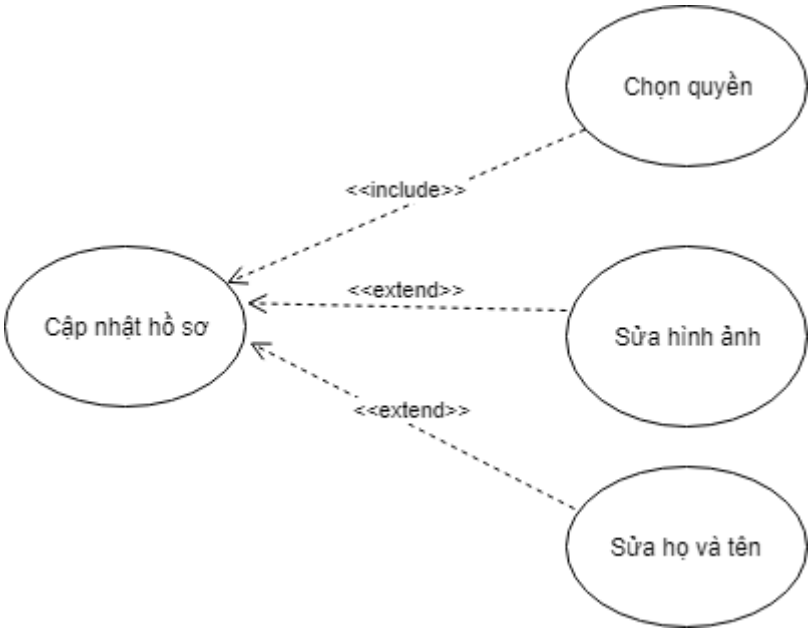
- Tác nhân: người bầu chọn, người tạo cuộc bầu chọn, admin.
- Điều kiện: Mở được hệ thống bầu chọn và đăng nhập thành công.
- Mô tả: Nhập thông tin mật khẩu củ, mật khẩu mới và xác nhận lại mật khẩu bên dưới.



Hình 1. 4. Sơ đồ Use case Đổi mật khẩu

2.2.4. Use case “Cập nhật hồ sơ”

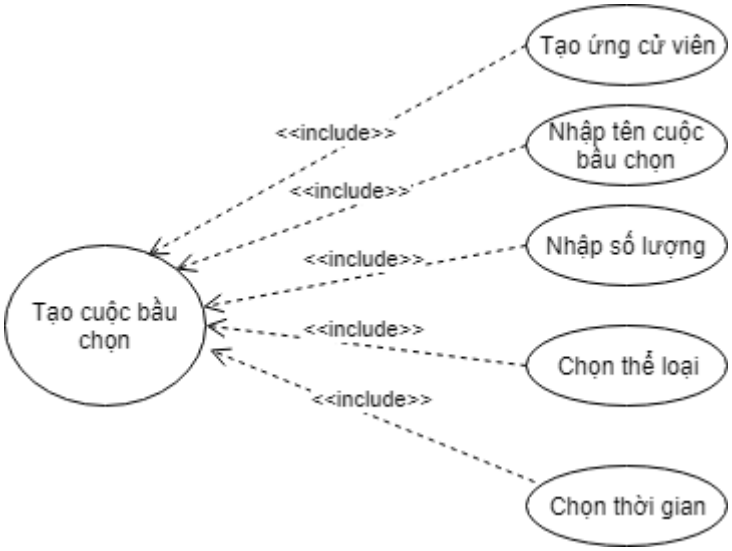
- Tác nhân: người bầu chọn, người tạo cuộc bầu chọn, admin.
- Điều kiện: mở được hệ thống bầu chọn và đăng nhập thành công.
- Mô tả: Hệ thống cho phép người dùng thay đổi thông tin như tên đăng nhập, hình đại diện, chọn quyền, tên.



Hình 1. 5. Sơ đồ Use case Cập nhật hồ sơ

2.2.5. Use case "Tạo cuộc bầu chọn".

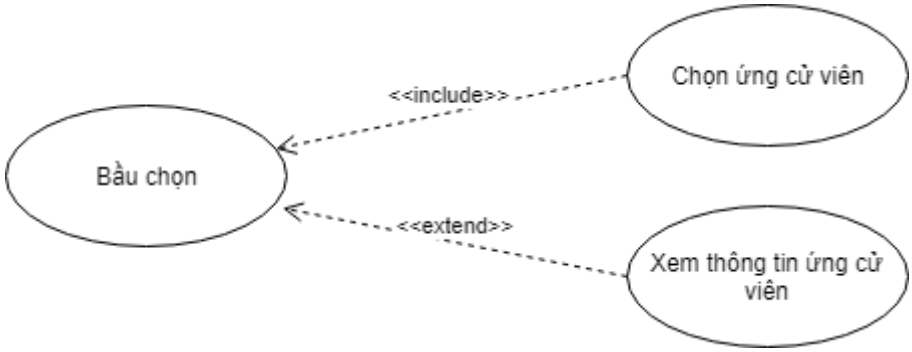
- Tác nhân: người tạo cuộc bầu chọn, admin.
- Điều kiện: Mở được hệ thống bầu chọn, đăng nhập thành công với loại người dùng là admin hoặc người tạo cuộc bầu chọn.
- Mô tả: Người dùng khi tạo cuộc bầu chọn cần nhập đầy đủ thông tin về cuộc bầu chọn như thời gian bầu, số lượng, tên bầu chọn và thêm ứng cử viên.



Hình 1. 6. Sơ đồ Use case Tạo cuộc bầu chọn

2.2.6. Use case "Bầu chọn".

- Tác nhân: người tạo cuộc bầu chọn, admin, người bầu chọn.
- Điều kiện: Mở được hệ thống bầu chọn và đăng nhập thành công.
- Mô tả: Người dùng đăng nhập vào hệ thống, di chuyển đến trang chủ sau đó lựa chọn một cuộc bầu chọn sau đó chọn ứng cử viên mình mong muốn để bầu chọn.

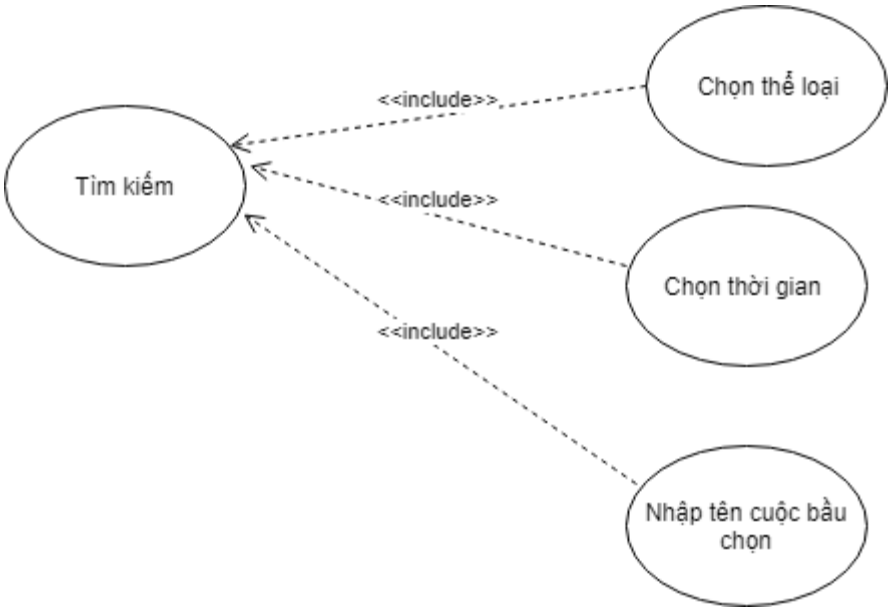


Hình 1. 7. Sơ đồ Use case Bầu chọn

2.2.7. Use case "Tìm kiếm".

- Tác nhân: người tạo cuộc bầu chọn, admin, người bầu chọn.
- Điều kiện: Mở được hệ thống bầu chọn.

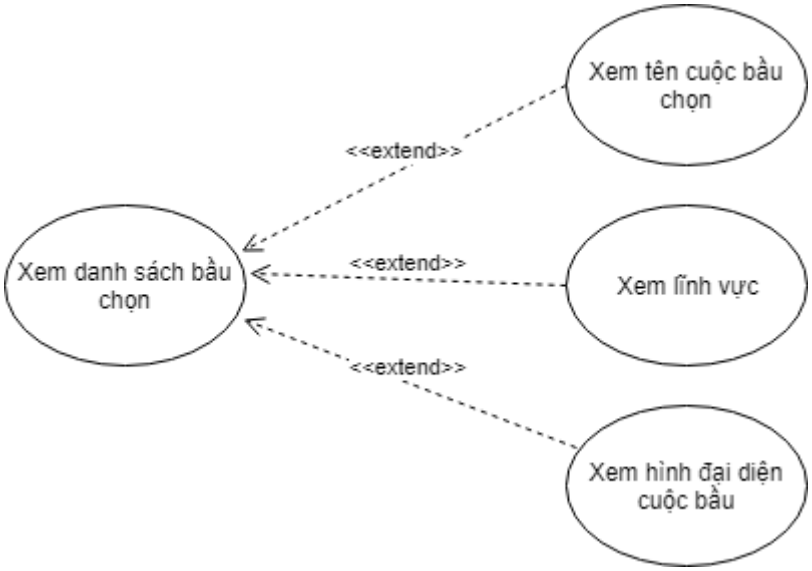
- Mô tả: Người dùng truy cập vào trang chủ hệ thống, danh sách các cuộc bầu chọn hiện ra, người dùng có thể tìm kiếm các cuộc bầu chọn theo: lĩnh vực, tên và thời gian kết thúc của cuộc bầu chọn...



Hình 1. 8. Sơ đồ Use case Tìm kiếm

2.2.8. Use case "Xem danh sách cuộc bầu chọn".

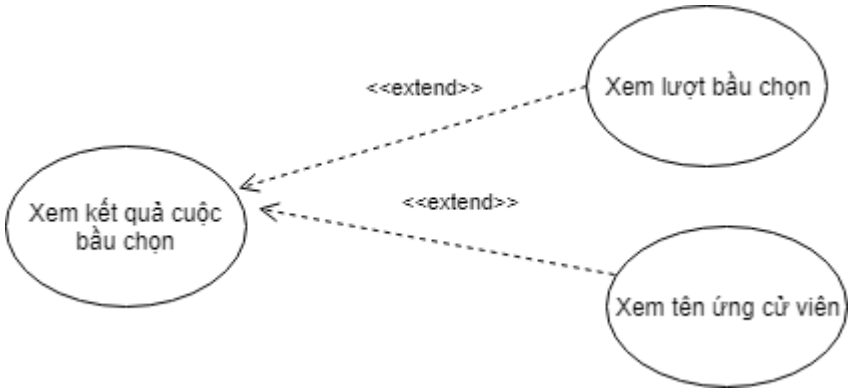
- Tác nhân: người tạo cuộc bầu chọn, admin, người bầu chọn.
- Điều kiện: Mở được hệ thống bầu chọn.
- Mô tả: Người dùng truy cập vào hệ thống, chuyển đến trang chủ và xem danh sách các cuộc bầu chọn.



Hình 1. 9. Sơ đồ Use case Xem danh sách bầu chọn

2.2.9. Use case “Xem kết quả cuộc bầu chọn”

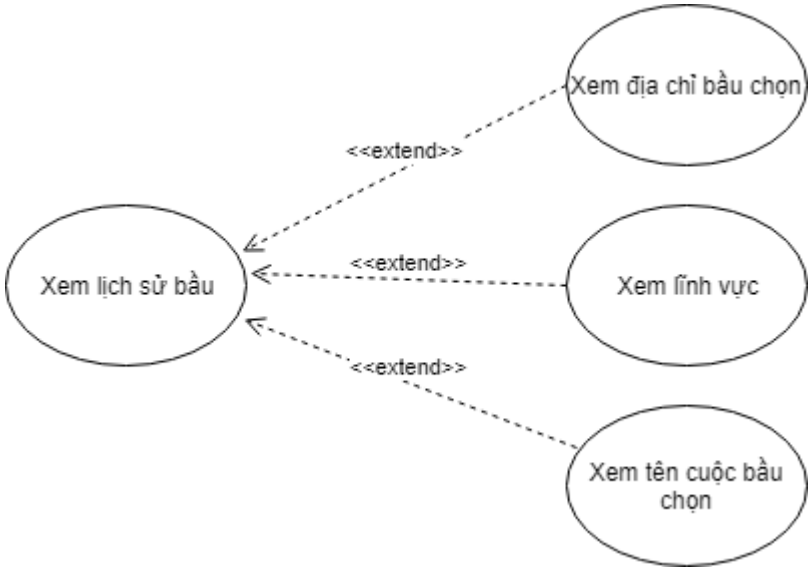
- Tác nhân: người tạo cuộc bầu chọn, admin, người bầu chọn.
- Điều kiện: Mở được hệ thống bầu chọn và đăng nhập thành công.
- Mô tả: Người dùng truy cập vào hệ thống sau đó đăng nhập và chọn một cuộc bầu chọn đã hết thời gian.



Hình 1. 10. Sơ đồ Use case Xem kết quả bầu chọn

2.2.10. Use case “Xem lịch sử bầu chọn”.

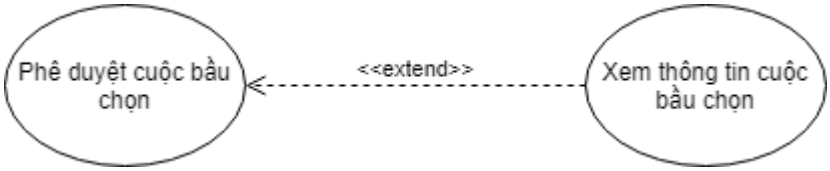
- Tác nhân: người tạo cuộc bầu chọn, admin, người bầu chọn.
- Điều kiện: Mở được hệ thống bầu và đăng nhập thành công.
- Mô tả: Người dùng truy cập vào hệ thống sau đó đăng nhập rồi chuyển đến trang cá nhân và xem thông tin về lịch sử cuộc bầu chọn của mình.



Hình 1. 11. Sơ đồ Use case Xem lịch sử bầu chọn

2.2.11. Use case “Phê duyệt bầu chọn”.

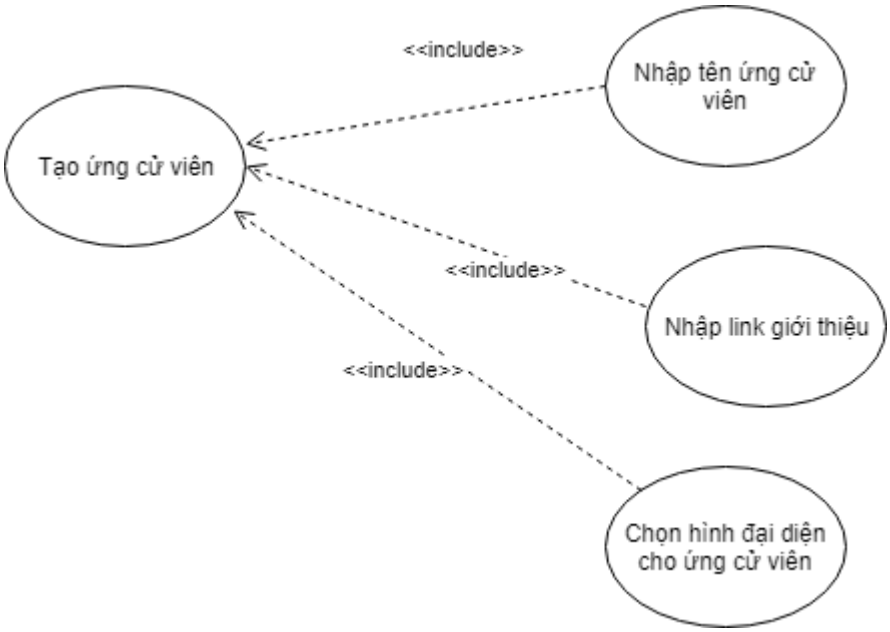
- Tác nhân: admin.
- Điều kiện: Mở được hệ thống bầu chọn và đăng nhập thành công.
- Mô tả: admin sau khi đăng nhập, vào trang phê duyệt cuộc bầu chọn để phê duyệt các cuộc bầu chọn.



Hình 1. 12. Sơ đồ Use case Phê duyệt bầu chọn

2.2.12. Use case “Tạo ứng cử viên”.

- Tác nhân: admin, người tạo cuộc bầu chọn.
- Điều kiện: Mở được hệ thống bầu chọn và đăng nhập thành công.
- Mô tả: người tạo cuộc bầu và admin sau khi đăng nhập và đã tạo cuộc bầu chọn, sau đó là tạo các ứng cử viên.

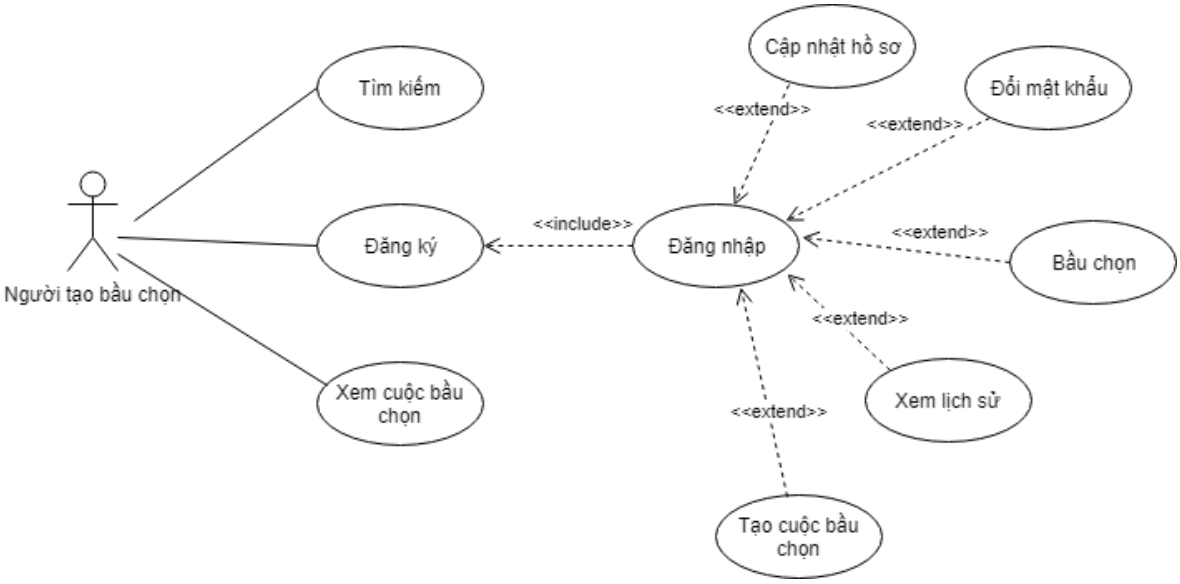


Hình 1. 13. Sơ đồ Use case Tạo ứng cử viên

3. Đặc điểm người dùng.

3.1. Người tạo bầu chọn

Các chức năng của người tạo bầu chọn: Đăng ký, đăng nhập, tạo cuộc bầu

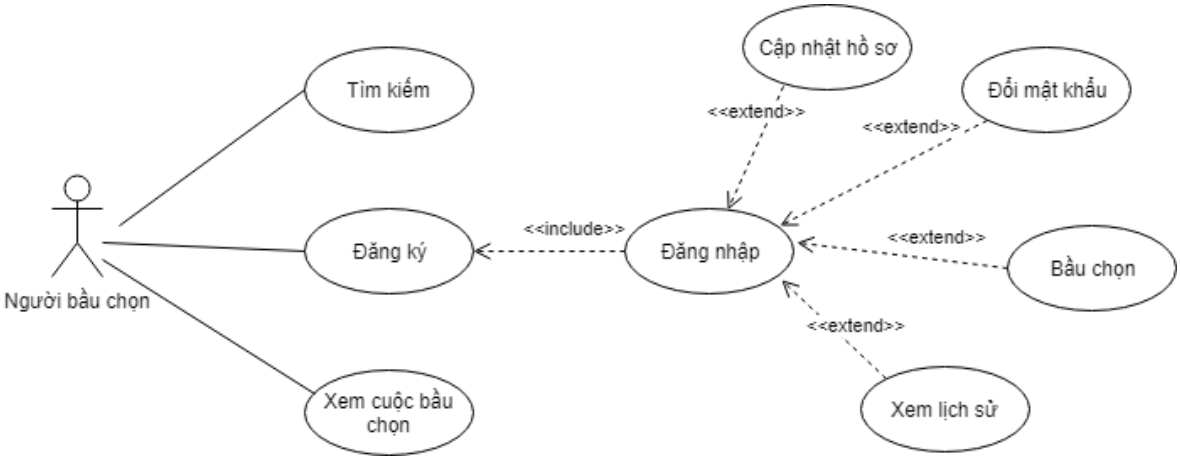


Hình 1. 14. Sơ đồ Use case Người tạo bầu chọn

chọn, bầu chọn, cập nhật hồ sơ, xem danh sách các cuộc bầu chọn, xem lịch sử bầu chọn, xem kết quả bầu chọn, tìm kiếm và đổi mật khẩu.

3.2. Người bầu chọn

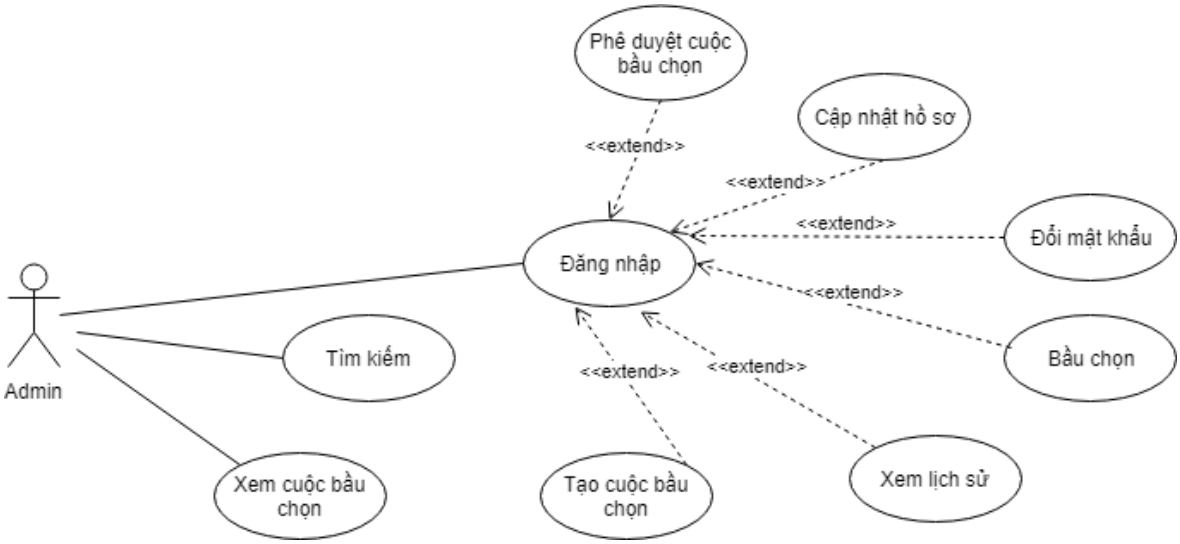
Các chức năng của người bầu chọn: Đăng ký, đăng nhập, bầu chọn, cập nhật hồ sơ, xem lịch sử bầu chọn, xem danh sách các cuộc bầu chọn, xem kết quả bầu chọn, tìm kiếm và đổi mật khẩu.



Hình 1. 15. Sơ đồ Use case Người bầu chọn

3.3. Admin

Các chức năng của người quản trị hệ thống: Đăng nhập, cập nhật hồ sơ, đổi mật khẩu, xem lịch sử bầu chọn, tạo cuộc bầu chọn, phê duyệt cuộc bầu chọn, tìm kiếm, xem danh sách các cuộc bầu chọn.



Hình 1. 16. Sơ đồ Use case Admin

4. Đặt tả yêu cầu.

4.1. Đăng ký.

Mã yêu cầu	DG01
Tên chức năng	Đăng ký tài khoản người dùng
Đối tượng sử dụng	Người bầu chọn và người tạo cuộc bầu chọn
Tiền điều kiện	Mở được hệ thống bầu chọn.
Cách xử lý	B1: Mở hệ thống bầu chọn. B2: Đến trang đăng ký. B3: Nhập các thông tin để tạo tài khoản, chọn quyền mong muốn (Tạo bầu chọn, bầu chọn). B4: Chọn nút "Đăng ký" • Nếu không có sự cố thì sẽ đăng ký thành công. • Ngược lại, nếu có sự cố sẽ thông báo đăng ký thất bại.

Kết quả	Đăng ký tài khoản người dùng thành công.
Ghi chú	Các thông tin bắt buộc chọn là tên đăng nhập, mật khẩu và quyền mong muốn là tạo bầu chọn hay là bầu chọn

Bảng 1. 2. Chức năng đăng ký

4.2. Đăng nhập.

Mã yêu cầu	DG02
Tên chức năng	Đăng nhập tài khoản người dùng
Đối tượng sử dụng	Người bầu chọn và người tạo cuộc bầu chọn, admin
Tiền điều kiện	Mở được hệ thống bầu chọn, có tài khoản trên hệ thống.
Cách xử lý	B1: Mở hệ thống bầu chọn và đến trang đăng nhập. B2: Nhập tên đăng nhập và mật khẩu. B3: Chọn nút "Đăng nhập" • Nếu tên đăng nhập và mật khẩu đúng thì đăng nhập thành công • Ngược lại, thông báo đăng nhập nhất bại.
Kết quả	Đăng nhập tài khoản người dùng thành công.
Ghi chú	Các thông tin bắt buộc nhập đầy đủ và chính xác: tên đăng nhập và mật khẩu

Bảng 1. 3. Chức năng đăng nhập

4.3. Đổi mật khẩu.

Mã yêu cầu	DG03
Tên chức năng	Đổi mật khẩu
Đối tượng sử dụng	Người bầu chọn và người tạo cuộc bầu chọn, admin

Tiền điều kiện	Mở được hệ thống bầu chọn và đăng nhập thành công
Cách xử lý	B1: Mở hệ thống bầu chọn và tiến hành đăng nhập. B2: Vào trang thông tin cá nhân B3: Nhấn nút "Sửa thông tin". B4: Nhập mật khẩu cũ, mật khẩu mới và nhập lại mật khẩu mới sau đó chọn nút "Lưu". B5: Hệ thống sẽ tự động đăng xuất.
Kết quả	Đổi mật khẩu thành công.
Ghi chú	Các thông tin bắt buộc nhập đầy đủ là mật khẩu cũ và mới và nhập lại mật khẩu mới.

Bảng 1. 4. Chức năng đổi mật khẩu

4.4. Cập nhật hồ sơ.

Mã yêu cầu	DG04
Tên chức năng	Cập nhật hồ sơ.
Đối tượng sử dụng	Người bầu chọn và người tạo cuộc bầu chọn, admin
Tiền điều kiện	Mở được hệ thống bầu chọn và đăng nhập thành công
Cách xử lý	B1: Mở hệ thống bầu chọn và tiến hành đăng nhập. B2: Đến trang cá nhân và chọn nut "Sửa thông tin". B3: Các thông tin của người dùng sẽ được hiển thị: tên đăng nhập, địa chỉ Ether, quyền tạo cuộc bầu chọn hay bầu chọn, họ và tên người dùng và hình đại diện. Người dùng có thể sửa đổi họ và tên, hình đại diện và chuyển đổi quyền của mình, sau đó chọn nút "Lưu. • Nếu lưu thông tin thành công sẽ có thông báo thành công và trang web tự động cập nhật thông tin mới. • Ngược lại, sẽ có thông báo cập nhật thất bại.

Kết quả	Cập nhật hồ sơ thành công.
Ghi chú	

Bảng 1. 5. Chức năng cập nhật hồ sơ

4.5. Tạo cuộc bầu chọn.

Mã yêu cầu	DG05
Tên chức năng	Tạo cuộc bầu chọn
Đối tượng sử dụng	Người tạo cuộc bầu chọn, admin.
Tiền điều kiện	Mở được hệ thống bầu chọn và đăng nhập thành công.
Cách xử lý	B1: Mở hệ thống bầu chọn và tiến hành đăng nhập. B2: Đến trang "Quản lý bầu chọn". B3: Nhập thông tin để tạo cuộc bầu chọn: tên cuộc bầu chọn, số lượng, lĩnh vực, loại bầu chọn, thời gian kết thúc sau đó nhấn nút "Tạo". • Nếu không có sự cố gì ngoài ý muốn thì sẽ tạo cuộc bầu chọn thành công • Ngược lại, sẽ có thông báo tạo thất bại.
Kết quả	Tạo cuộc bầu chọn thành công.
Ghi chú	Các thông tin bắt buộc chọn hoặc nhập đầy đủ và chính xác: tên cuộc bầu chọn, loại bầu chọn, lĩnh vực, số lượng, và thời gian kết thúc cuộc bầu chọn.

Bảng 1. 6. Chức năng tạo cuộc bầu chọn

4.6. Bầu chọn.

Mã yêu cầu	DG06
Tên chức năng	Bầu chọn
Đối tượng sử dụng	Người bầu chọn và người tạo cuộc bầu chọn, admin

Tiền điều kiện	Mở được hệ thống bầu chọn và đăng nhập thành công.
Cách xử lý	B1: Mở hệ thống bầu và tiến hành đăng nhập. B2: Vào trang chính để có thể xem các cuộc bầu chọn, lựa chọn cuộc bầu chọn mong muốn rồi chọn ứng cử viên mình muốn bầu. B3: Chọn nút "Bầu chọn". • Nếu không có sự cố gì sẽ có thông bào bầu chọn thành công và cập nhật số lượt bầu cho ứng cử viên. • Ngược lại, sẽ có thông báo bầu chọn thất bại.
Kết quả	Bầu chọn thành công chọn đối tượng mong muốn
Ghi chú	Một người dùng chỉ có thể bầu một lần duy nhật cho một cuộc bầu chọn.

Bảng 1. 7. Chức năng bầu chọn

4.7. Tìm kiếm.

Mã yêu cầu	DG07
Tên chức năng	Tìm kiếm cuộc bầu chọn
Đối tượng sử dụng	Người bầu chọn, người tạo cuộc bầu chọn, admin
Tiền điều kiện	Mở được hệ thống bầu chọn.
Cách xử lý	B1: Mở hệ thống bầu chọn. B2: Vào trang chính để có thể xem các cuộc bầu chọn rồi chọn hình thức tìm kiếm như: chọn lĩnh vực hoặc thời gian kết thúc bầu chọn hoặc nhập tên bầu chọn để tìm cuộc bầu chọn mong muốn. B3: Nhấp nút "Tìm".
Kết quả	Tìm kiếm cuộc bầu chọn thành công.
Ghi chú	Phải có cuộc bầu chọn để tìm kiếm

Bảng 1. 8. Chức năng tìm kiếm

4.8. Xem lịch sử bầu chọn.

Mã yêu cầu	DG08
Tên chức năng	Xem lịch sử bầu chọn
Đối tượng sử dụng	Người bầu chọn và người tạo cuộc bầu chọn, admin
Tiền điều kiện	Mở được hệ thống bầu chọn.
Cách xử lý	B1: Đến trang đăng nhập và tiến hành đăng nhập. B2: Vào trang thông tin cá nhân. B3: Quan sát lịch sử bầu chọn.
Kết quả	Xem được lịch sử bầu chọn
Ghi chú	Nếu chưa thực hiện cuộc bầu chọn nào thì sẽ là bảng trống

Bảng 1. 9. Chức năng xem lịch sử bầu

4.9. Xem danh sách cuộc bầu chọn.

Mã yêu cầu	DG09
Tên chức năng	Xem danh sách cuộc bầu chọn.
Đối tượng sử dụng	Người bầu chọn và người tạo cuộc bầu chọn, admin
Tiền điều kiện	Mở được hệ thống bầu chọn.
Cách xử lý	B1: Mở hệ thống bầu chọn và đến trang chính B2: Quan sát danh sách các cuộc bầu chọn.
Kết quả	Xem được danh sách cuộc bầu chọn
Ghi chú	Người chưa có tài khoản cũng có thể xem danh sách cuộc bầu chọn

Bảng 1. 10. Chức năng xem danh sách cuộc bầu chọn

4.10. Xem kết quả cuộc bầu chọn.

Mã yêu cầu	DG010
Tên chức năng	Xem kết quả cuộc bầu chọn
Đối tượng sử dụng	Người bầu chọn, người tạo cuộc bầu chọn, admin
Tiền điều kiện	Mở được hệ thống bầu chọn.
Cách xử lý	B1: Mở hệ thống bầu chọn. B2: Đến trang đăng nhập và tiến hành đăng nhập. B3: Vào trang chính của hệ thống và xem danh sách cuộc bầu chọn. B4: Chọn một cuộc bầu chọn đã hết thời gian. B5: Quan sát kết quả cuộc bầu chọn.
Kết quả	Xem được kết quả cuộc bầu chọn
Ghi chú	Cuộc bầu chọn phải hết thời gian mới thông báo kết quả

Bảng 1. 11. Chức năng xem kết quả cuộc bầu chọn

4.11. Phê duyệt bầu chọn.

Mã yêu cầu	DG011
Tên chức năng	Phê duyệt bầu chọn
Đối tượng sử dụng	admin
Tiền điều kiện	Mở được hệ thống bầu chọn.
Cách xử lý	B1: Đến trang đăng nhập và đăng nhập với tài khoản admin B2: Chuyển đến trang phê duyệt. B3: Xem danh sách bầu chọn chưa phê duyệt. B4: Nhấn nút “phê duyệt” và quan sát thông tin các cuộc bầu chọn.

	B5: Nhấn nút phê duyệt nếu cuộc bầu chọn phù hợp và nhấn nút không phê duyệt nếu cuộc bầu chọn không phù hợp
Kết quả	Phê duyệt cuộc bầu chọn
Ghi chú	Chỉ admin mới có thể phê duyệt cuộc bầu chọn mới.

Bảng 1. 12. Chức năng phê duyệt bầu chọn

4.12. Tạo ứng cử viên.

Mã yêu cầu	DG012
Tên chức năng	Tạo ứng cử viên
Đối tượng sử dụng	Người tạo cuộc bầu chọn, admin
Tiền điều kiện	Mở được hệ thống bầu chọn, đã đăng nhập và tạo cuộc bầu chọn thành công.
Cách xử lý	B1: Tạo cuộc bầu chọn thành công. B2: Nhập thông tin cho từng ứng cử viên. B3: Nhấn nút "Lưu".
Kết quả	Tạo thành công cuộc bầu chọn
Ghi chú	Chỉ admin và người tạo cuộc bầu chọn mới có thể tạo

Bảng 1. 13. Chức năng tạo ứng cử viên

5. Yêu cầu phi chức năng.

5.1. Yêu cầu thực thi.

Phải chạy tốt trên các hệ điều hành. Hỗ trợ và sử dụng các trình duyệt hiện nay như Google Chrome, Cốc Cốc...

5.2. Yêu cầu bảo mật

Phải kiểm tra người dùng có quyền thao tác với các chức năng khác nhau. Với người tạo cuộc bầu chọn thì phải có quyền tạo cuộc bầu chọn và bầu chọn, còn người bầu chọn thì chỉ có quyền bầu chọn. Người dùng có quyền xem lịch sử các

cuộc bầu chọn, tìm kiếm cuộc bầu chọn theo lĩnh vực, tên bầu chọn và thời gian kết thúc. Đối với chức năng đăng nhập chỉ có người quản trị hệ thống mới có quyền thao tác. Mật khẩu người dùng sẽ được mã hóa trước khi lưu lên mạng lưới blockchain.

5.3. Đặt điểm hệ thống.

Ngôn ngữ sử dụng thuần việt, từ ngữ đơn nghĩa, dễ hiểu, không sai chính tả.

Giao diện thân thiện, dễ sử dụng, không gây khó chịu cho người dùng khi họ sử dụng hệ thống trong thời gian dài.

Đảm bảo tuân thủ các quy định của pháp luật.

5.4. Môi trường vận hành.

Hệ thống bầu chọn phía client sử dụng trên các trình duyệt như Google Chrome, Cốc Cốc,… và mạng lưới private blockchain ethereum chạy trên hệ điều hành Ubuntu.

Các ràng buộc thực thi và thiết kế:

- Đảm bảo tính chính xác và nhanh chóng.
- Đảm bảo tính dễ sử dụng.
- Đảm bảo tính an toàn dữ liệu.
- Đảm bảo tính bảo mật.

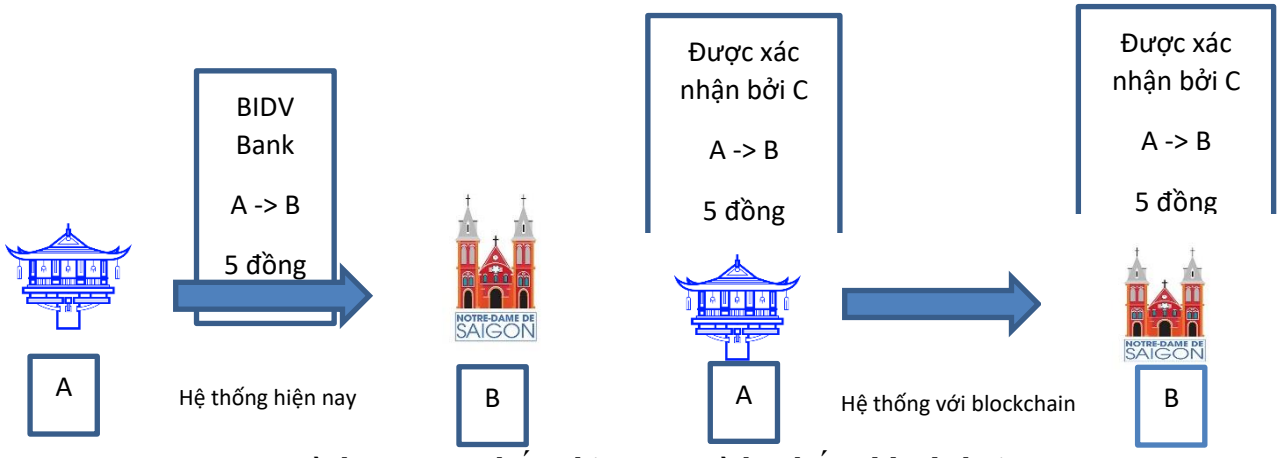
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

1. Giới thiệu Blockchain.

1.1. Blockchain là gì ?

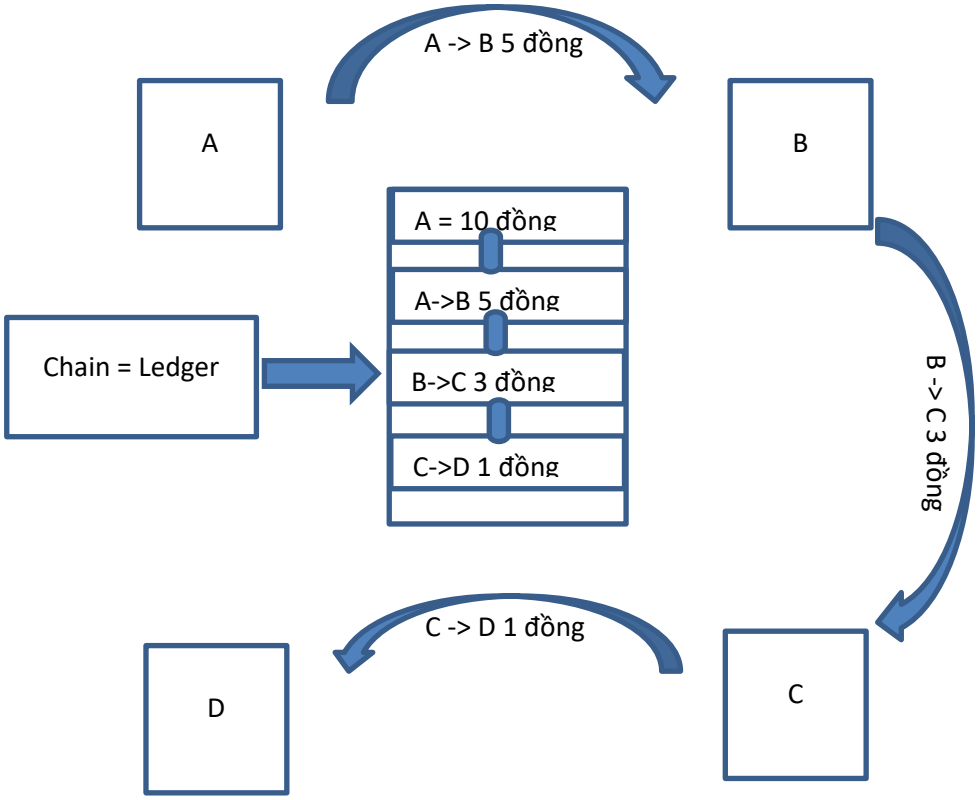
Blockchain (chuỗi khối), tên ban đầu block chain là một cơ sở dữ liệu phân tán lưu trữ thông tin trong các khối được liên kết với nhau bằng mã hash và mở rộng theo thời gian. Mỗi khối đều chứa thông tin về thời gian khởi tạo và được liên kết với khối trước đó, kèm một mã thời gian và dữ liệu giao dịch. Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó [5].

Blockchain là một công nghệ nền tảng hỗ trợ cho sự phát triển của các ứng dụng khác nhau. Bitcoin hay Ethereum là các loại tiền mã hóa chúng được phát triển dựa trên công nghệ blockchain. Blockchain là công nghệ giúp cho việc lưu trữ tiền mã hóa và chuyển tiền mã hóa từ một cá nhân nào đó đến với một cá nhân khác. Trong tài liệu này sẽ không nói nhiều về Bitcoin hay Ethereum mà sẽ tập trung nghiên cứu về công nghệ blockchain do đó phải khẳng định lại một lần nữa là blockchain không phải một loại tiền mã hóa nào cả. Chúng ta xét một bài toán về chuyển tiền sau: người A đến từ Hà Nội cần chuyển 10 đồng cho một người B ở Hồ Chí Minh. Do khoảng cách địa lý quá xa việc trao tiền tận tay là quá khó nên việc chuyển tiền này trong thực tế sẽ cần một bên thứ ba ví dụ như ngân hàng. Nhưng với hình thứ này người A hoặc người B sẽ phải chịu một chi phí nào đó nên nếu chuyển 10 đồng tổng tiền cần phải chuyển sẽ lớn hơn 10 đồng. Thời gian cũng là một vấn đề cần lưu tâm. Hiện nay các ngân hàng đều đã có các dịch vụ chuyển tiền online những các giao dịch chuyển tiền cũng cần đến vài phút để hoàn thành. Blockchain sinh ra để giải quyết vấn đề này. Với blockchain việc chuyển tiền giữa hai người sẽ không cần một bên thứ ba và thời gian có thể tính bằng giây, chi phí cho các giao dịch cũng không cao như việc chuyển tiền trong thực tế hiện nay.



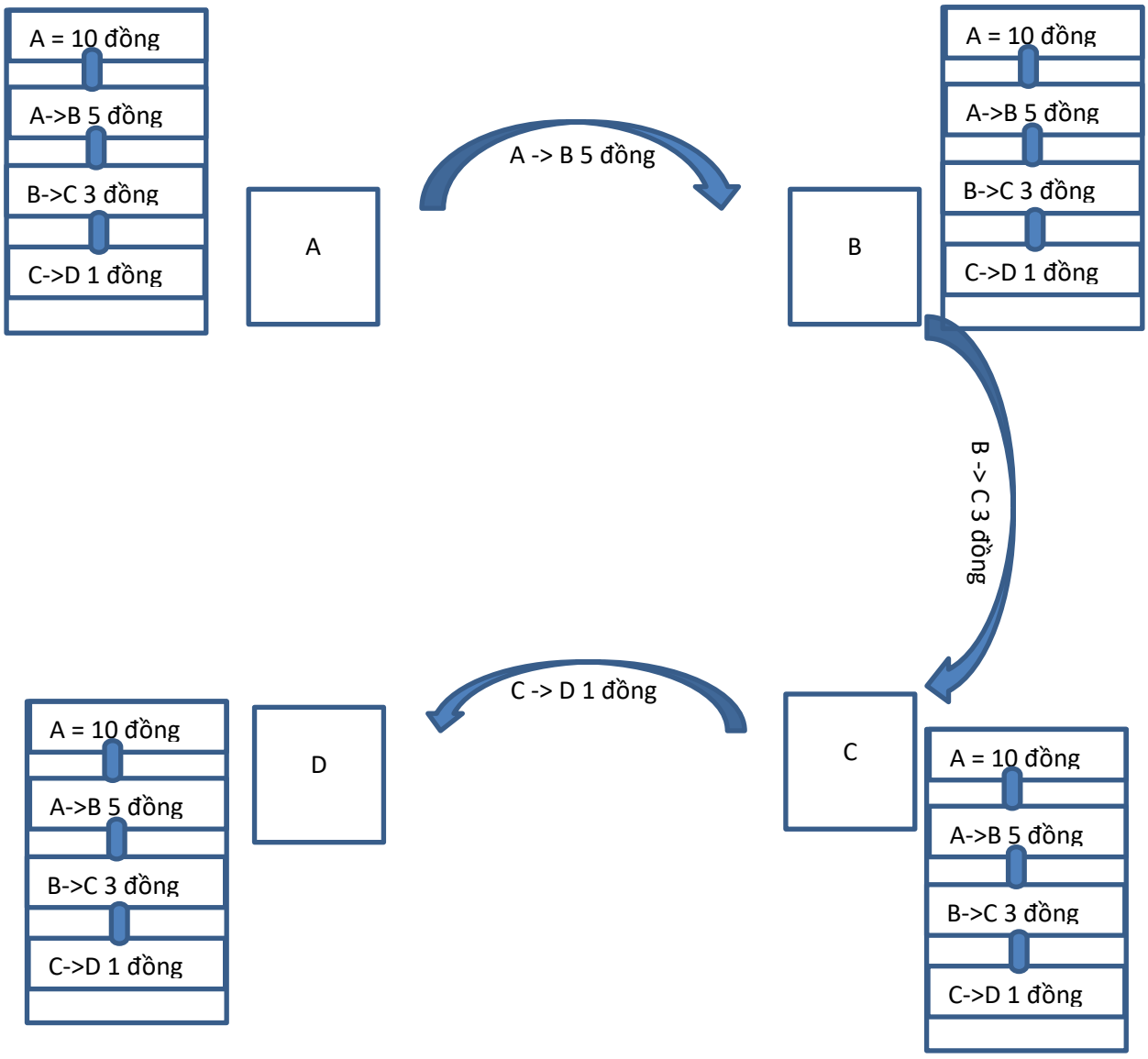
Hình 2. 1.Hệ Thống hiện nay và hệ thống blockchain

Một khái niệm khác trong công nghệ blockchain là Open Ledger hay có thể gọi ngắn là Ledger. Vẫn là một ví dụ về chuyển tiền, giải sử chung ta có bốn người A, B, C, D. Người A ban đầu sẽ có 10 đồng trong tay. Người A quyết định chuyển cho người B 5 đồng, tiếp theo người B lại chuyển cho người C 3 đồng cuối cùng người C quyết định chuyển cho người D 1 đồng. Mỗi lần chuyển tiền như vậy sẽ có một giao dịch được tạo ra và các giao dịch này sẽ được liên kết với nhau thành một chuỗi các giao dịch hay còn gọi là chain. Một chuỗi các giao dịch này chính là Open Ledger. Trong ví dụ này ledger đang tập trung tại một nơi và chuyện gì sẽ xảy ra nếu A cố gắn chuyển tiếp 10 đồng cho B. Lúc này người A chỉ còn 5 đồng và giao dịch chuyển 10 đồng của A là không hợp lệ do đó giao dịch này sẽ không được thêm vào Ledger.



Hình 2. 2. Mô hình với Ledger tập trung

Để xác định được giao dịch này có hợp lệ hay không cần hiểu được về distributed ledger. Distributed ledger là cơ chế giúp cho ledger không tập trung lại một nơi mà mỗi người A, B, C hay D đều có một bản sao của ledger đồng thời các bản sao này sẽ được đồng bộ cập nhật một các liên túc giữa mỗi người trong mạng với nhau để đảm bảo các giao dịch bên trong là giống nhau.



Hình 2. 3. Mô hình với Ledger phi tập trung

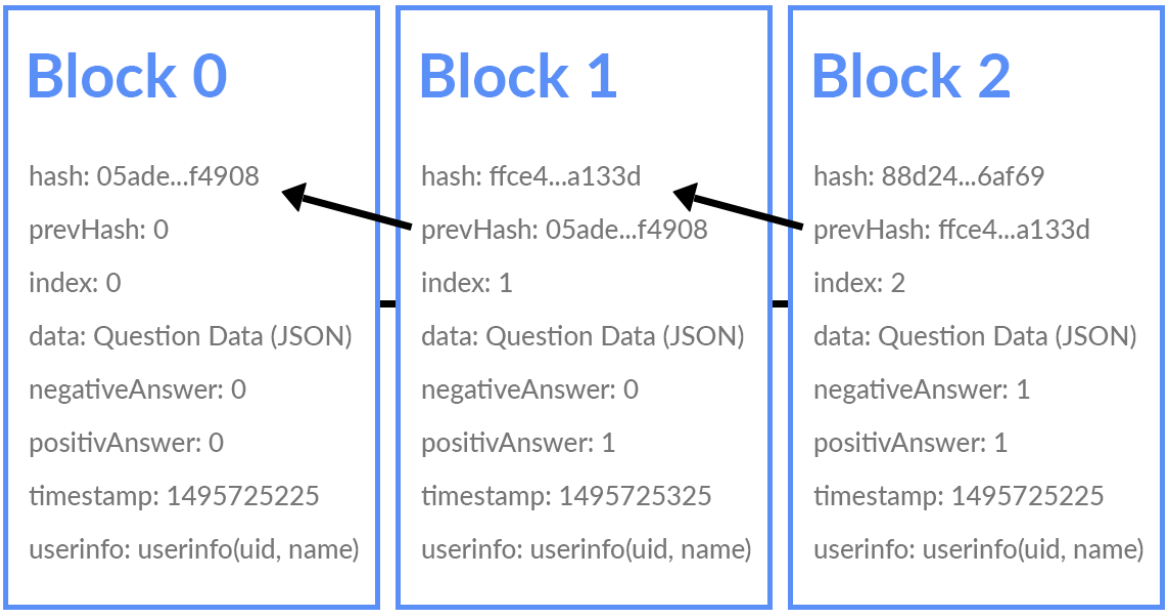
Đây là một mạng lưới blockchain phi tập trung và mỗi người A, B, C hay D là một node trong mạng lưới. Với cơ chế này khi một giao dịch được tạo ra ví dụ như người C cần chuyển 2 đồng đến người A thì lúc này giao dịch sẽ được thông báo lên cho tất cả mọi người trong mạng. Một người trong mạng lưới sẽ xác minh xem giao dịch của người C có hợp lệ hay không hay nói cách khác là người C có đủ 2 đồng để chuyển cho người A hay không.

Đến đây sẽ có thêm một khái niệm khác nữa đó là miner. Miner chính là node trong mạng lưới không tham gia giao dịch hiện tại ví dụ như ở đây là B. Người B sẽ lấy giao dịch này và kiểm tra xem nó có hợp lệ hay không nếu hợp lệ người B sẽ lưu giao dịch này vào ledger của mình đồng thời thông báo các những người khác trong mạng. Những người khác sẽ xác minh lại một lần nữa và nếu hợp lệ thì mọi

người tham gia trong mạng lưới sẽ cập nhật giao dịch này cho ledger của mình. Trong Bitcoin, miner khi xác nhận thành công một giao dịch họ sẽ nhận được một phần thưởng là một lượng bitcoin nào đó.

Với những ví dụ vừa đặt ra có thể thấy blockchain tương đồng với cơ sở dữ liệu, chỉ khác ở việc tương tác với cơ sở dữ liệu. Để hiểu blockchain, cần nắm được năm định nghĩa sau: chuỗi khối (blockchain), cơ chế đồng thuận phân tán đồng đẳng (Distributed), tính toán tin cậy (trusted computing), hợp đồng thông minh (smart contracts) và giao thức đồng thuận (consensus).

Một blockchain được hình thành từ một danh sách các block. Nó được bắt đầu từ một block nguyên thủy thường được gọi là Genesis Block. Mỗi block sẽ lưu trữ các thông tin sau: index, timestamp, hash của block, hash của blockchain, data and nonce.



Hình 2. 4. Chi tiết Block

- index: là vị trí của block hiện tại trong chain, với block nguyên thủy index sẽ là 0.
- timestamp: là thời gian của block đó được tạo ra.
- hash: là một chuỗi ký tự mã hóa không trùng nhau.
- prevHash: là chuỗi hash cha của block.

1.2. Smart Contract là gì ?

Hợp đồng thông minh là các khối để xây dựng nên các ứng dụng phi tập trung. Một hợp đồng thông minh tương đương với một chương trình nhỏ mà bạn có thể tin tưởng với một đơn vị giá trị và quản lý giá trị đó. Ý tưởng cơ bản đằng sau hợp đồng thông minh là sự quản lý bằng khế ước đối với một giao dịch giữa hai bên

liên quan hay nhiều hơn có thể được xác minh theo thứ tự thông qua chuỗi khối, thay vì thông qua một quan tòa tập trung. Sao phải dựa vào một quyền lực tập trung trong khi hai hay nhiều bên tham gia có thể đồng thuận lẫn nhau, và khi họ có thể đưa ra các điều khoản và thực thi sự đồng thuận bằng chương trình và các điều kiện, tiền sẽ được chuyển tự động khi hoàn thành một số dịch vụ.[2][5]

1.3. Mining để làm gì ?

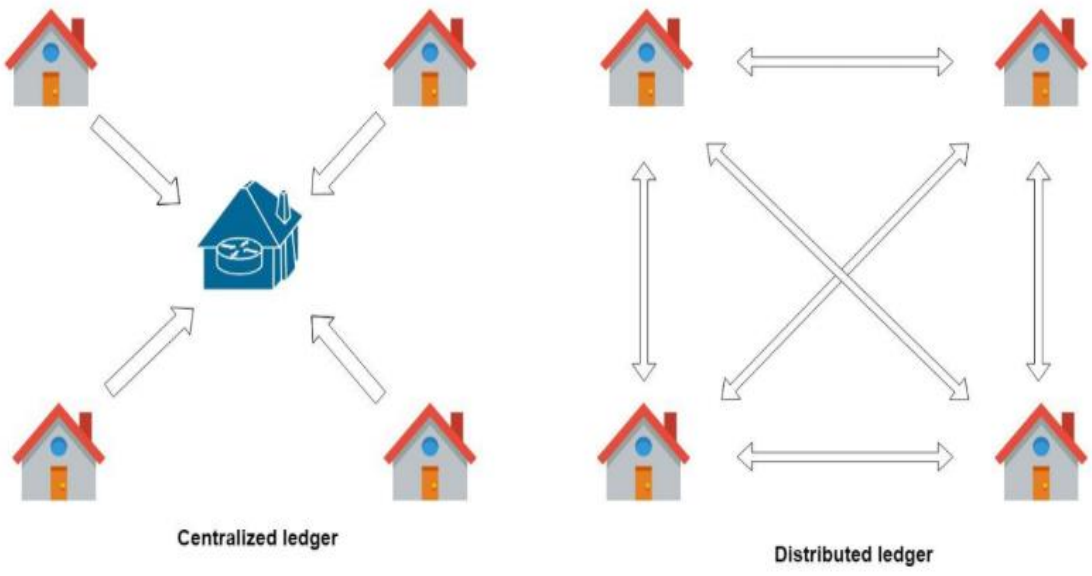
Trong mạng lưới blockchain của bitcoin, mining là quá trình xác nhận một giao dịch và tính toán các phép tính toán học phức tạp để tìm ra một block hợp lệ và nhận được một phần thưởng là một lượng tiền từ hệ thống. [2][5]

1.4. Cơ chế đồng thuận phân tán đồng đẳng.

Cơ chế này ngược lại với mô hình cổ điển là cơ chế đồng thuận tập trung. Nghĩa là khi đó có một cơ sở dữ liệu tập trung được dùng để quản lý việc xác thực giao dịch. Cơ chế này cho phép các node của mạng lưới liên tục lưu trữ các giao dịch trên một block và, tạo nên một chuỗi độc nhất khi đó sẽ gọi là blockchain. Mỗi khối kế tiếp chứa một hash (một mã hóa duy nhất) của khối trước nó. Mã hash này được sử dụng để đảm bảo tính xác thực của nguồn giao dịch và loại bỏ sự cần thiết phải có một trung gian tập trung. Sự kết hợp của mã hóa và công nghệ blockchain lại đảm bảo rằng sẽ không bao giờ một giao dịch được lưu trữ lại hai lần. [2][5]

1.5. Cơ chế đồng thuận.

1.5.1. Proof of work.



Hình 2. 5. Mô hình Proof of work

Proof of work (PoW) là thuật toán đồng thuận ban đầu của mạng lưới Blockchain. Khái niệm Proof of Work đã tồn tại trước khi có khái niệm về Bitcoin.

Satoshi Nakamoto đã áp dụng kỹ thuật này cho đồng tiền số của mình, tạo nên một cuộc cách mạng hóa các giao dịch truyền thống được thiết lập trước đó. Trên thực tế, khái niệm PoW ban đầu được Cynthia Dwork và Moni Naor đưa ra năm 1993, nhưng từ "Proof of Work" đã được Markus Jakobsson và Ari Juels đặt ra trong một tài liệu xuất bản năm 1999. Thuật toán này được dùng để xác nhận giao dịch và tạo ra các khối (block) mới. Với PoW, các thợ đào coin cạnh tranh với nhau để hoàn tất giao dịch trên mạng lưới và nhận phần thưởng. Người có máy tính càng mạng sẽ có thể xử lý được càng nhiều giao dịch và nhận được càng nhiều coin. PoW được sử dụng trong nhiều crypto. Ứng dụng danh tiếng nhất của PoW là Bitcoin và Bitcoin cũng đã đặt nền móng cho cơ chế đồng thuận này. [3]

1.5.2. Proof of State.

Proof of Stake (PoS) là một cách khác để xác thực cho các giao dịch. PoS thực tế vẫn là một giao thức với mục đích giống như PoW nhưng quá trình để đạt được mục tiêu thì khác hoàn toàn. Các thợ đào trong giải thuật PoS này phải đóng góp một lượng coin hoặc token cụ thể để tham gia xác minh cho các giao dịch. PoS được xem là một hệ thống công bằng hơn so với PoW do ở đây tất cả mọi người đều có thể trở thành thợ đào. Không phân biệt về sức mạnh của máy tính, quy mô khai thác sẽ tỉ lệ tuyến tính với số lượng cổ phần sở hữu. Điều này giúp khuyến khích công đồng tham gia vào việc xác nhận giao dịch, tăng khả năng phân cấp và dân chủ hơn.[3]

1.5.2.1. Proof of Authority.

Proof of Authority (PoA) là một thuật toán sử dụng cơ chế đồng thuận thay thế. Theo đó, thay vì sử dụng hash để giải quyết các vấn đề toán học khó nhằn, PoA sử dụng một tập hợp các lệnh ủy quyền cho phép tạo block mới, đồng thời đảm bảo tối đa tính an toàn của blockchain.

1.5.3. Mục đích phát triển Proof of Authority.

Hiện nay, xây dựng dịch vụ trên một blockchain công cộng gặp phải hai vấn đề lớn: rào cản kỹ thuật khi tiến hành truy cập và chi phí trả trước tương đối cao. Do đó, nhiều doanh nghiệp nhỏ và vừa bị loại khỏi việc áp dụng và hưởng lợi từ công nghệ blockchain. Với mong muốn khắc phục tình trạng trên, đội ngũ phát triển của PoA hướng tới xây dựng một mạng lưới công cộng kết hợp tốc độ, an ninh với mức chi phí phải chăng (những ưu điểm trước đây chỉ xuất hiện trên mạng cá nhân).

1.5.4. Đặc điểm của PoA

- Mạng lưới với thuật toán PoA hỗ trợ xây dựng các ứng dụng phi tập trung tốt hơn.
- Quá trình xác thực trên PoA được thực hiện bởi những người có danh tính rõ ràng, có khả năng xác nhận tính hợp lệ của các khối.
- Thời gian tạo block trung bình: 5. 05 giây.

- Không cần "đào". Việc tạo khối trong các PoA không đòi hỏi nhiều nguồn lực tính toán như Proof of Work.
- Hệ sinh thái token của PoA: là Mạng lưới công cộng dựa trên Ethereum với sự đồng thuận của PoA, giúp hợp đồng thông minh được tiến hành nhanh chóng và tiết kiệm chi phí.
- Hỗ trợ DApp: Mạng lưới hỗ trợ xây dựng các DApp.

Có thể thấy, mô hình 'Proof of Authority' đã loại bỏ đi một số quan niệm bình đẳng trong các mô hình đồng thuận yếu kém hơn, thay thế chúng bằng các chữ kí mã hóa và hợp đồng kinh doanh được mạng lưới chứng nhận và quy định thực hiện.

1.5.5. Ưu điểm của PoA so với PoW và PoS.

Như ta đã biết, PoW là thuật toán sử dụng cơ chế "đào", PoS hoạt động bằng cách sử dụng một thuật toán lựa chọn những người tham gia có số cổ phần cao nhất làm người xác nhận, giả sử rằng các bên liên quan cao nhất được khuyến khích để đảm bảo một giao dịch được xử lý. Theo đó, nếu như PoW làm việc bằng cách xác minh công việc (đào) đã được thực hiện và "tặng thưởng" cho các thợ đào, PoS hoạt động bằng cách sử dụng một thuật toán lựa chọn những người tham gia có số cổ phần cao nhất làm người xác nhận thì PoA chỉ sử dụng danh tính người dùng làm căn cứ duy nhất để xác minh thẩm quyền mà không cần đến những thuật toán đào. Cụ thể, người dùng chỉ cần cung cấp danh tính và mạng lưới sẽ tự động thực hiện toàn bộ quá trình: từ cấp quyền, tích lũy điểm cho đến quá trình thực hiện giao dịch. Bên cạnh đó, với PoA, việc bổ nhiệm thẩm quyền là tự động, loại bỏ tình trạng mất cân bằng do các cổ phần không đồng đều của PoS. Trong PoA, danh tính của người dùng được

Hình 2. 6. mô hình PoA PoW PoS

xác nhận thông qua DApps và các thông tin nhận dạng này có sẵn trong mạng lưới công cộng để người dùng có thể tham khảo chéo.

Có thể thấy, trong PoA, các cá nhân đều có quyền trở thành người phê chuẩn, đây là động lực để duy trì vị trí mà họ đã đạt được. Bằng cách gắn danh tiếng vào hồ sơ nhận dạng, người dùng (lúc này đóng vai trò là người phê duyệt) được khuyến khích duy trì tiến trình giao dịch. Mặt khác, PoA chỉ chấp thuận các khối không liên tục (non- consecutive blocks) từ người kiểm chứng, góp phần ngăn chặn các hành vi xấu có thể gây thiệt hại đến mạng lưới.

1.6. Cấu tạo và tính chất của Blockchain

- Blockchain được cấu tạo từ ba phần chính:

Block: là bản danh sách các giao dịch được ghi vào sổ cái trong một khoảng thời gian. Kích thước, thời gian và các sự kiện là tùy theo từng kiểu Blockchain khác nhau.

Chain: là một chuỗi hash được mã hóa từ nội dụng của block bằng các thuật toán phức tạp dùng để nối các block với nhau.

Mạng lưới: là một tổ hợp của các node đầy đủ. Đó là các máy tính chạy thuật toán để bảo toàn cả mạng lưới. Mỗi node chứa toàn bộ bản ghi đầy đủ của mọi giao dịch trên toàn hệ thống Blockchain. Các node được định vị trên toàn cầu và có thể được vận hành bởi bất cứ ai. Việc vận hành một nút đầy đủ là khó khăn, tốn công sức, thời gian, tiền bạc và vì thế mà một node phải được trả công. Thuật toán nền tảng của Blockchain sẽ trả công cho các node.

- Các tính chất của Blockchain:
  - Không thể làm giả, không thể phá hủy các chuỗi blockchain: Các chuỗi Blockchain gần như không thể bị phá hủy được, và theo lý thuyết thì chỉ có máy tính lượng tử mới có thể can thiệp vào và giải mã chuỗi blockchain và nó chỉ bị phá hủy hoàn toàn khi không còn internet trên toàn cầu
  - Bất biến: Dữ liệu trong blockchain không thể sửa đổi được và các dữ liệu đó sẽ lưu giữ mãi mãi.
  - Bảo mật Dữ liệu: Các thông tin, dữ liệu trong các chuỗi blockchain được phân tán và an toàn tuyệt đối chỉ có người nắm giữ private key mới có quyền truy xuất dữ liệu đó
  - Minh bạch: Ai cũng có thể theo dõi được đường đi của dữ liệu trong blockchain từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.
  - Hợp đồng thông minh: là các kỹ thuật số được nhúng bởi một đoạn code if-this-then-that (IFTTT) trong hệ thống, cho phép chúng tự thực thi mà không cần bên thứ ba. Blockchain không cần bên thứ ba tham gia vào hệ thống, và nó đảm bảo rằng tất cả các bên tham gia đều biết được chi tiết hợp đồng và các điều khoản sẽ được tự động thực hiện một khi các điều kiện được bảo đảm.

1.7. Phân loại Blockchain.

Phân loại blockchain thì có nhiều tiêu chí khác nhau sẽ cho ra nhiều loại blockchain khác nhau. Tuy nhiên trong tài liệu này phân loại blockchain sẽ dựa vào tiêu chí công nghệ và mục đích sử dụng blockchain. Có thể tạm chia blockchain thành ba loại: Blockchain cho Crypto, Blockchain kết hợp Crypto và Business và Blockchain cho Business.

- Blockchain cho Crypto: Đại diện ứng dụng tiêu biểu cho loại blockchain này là Bitcoin. Blockchain loại này được phát triển với mục đích tạo ra nền tảng cho các loại tiền mã hóa có được các giao dịch nhanh chóng và an toàn.
- Blockchain kết hợp Crypto và Business: Đại diện ứng dụng tiêu biểu cho loại blockchain này là Ethereum. Ethereum hiện tại vừa dùng để giao dịch tiền mã hóa và cũng có thể xây dựng các DApp phục vụ các công việc cho các lĩnh vực khác nhau nhờ có ngôn ngữ lập trình solidity tạo ra các smart contract.
- Blockchain cho Business: Hyperledger là dự án mã nguồn mở do Linux Foundation khởi xướng (12-2015). Hyperledger được phát triển trên nhiều dự án con bên trong nó với cùng mục đích chung là giúp đưa công nghệ blockchain ứng dụng vào các lĩnh vực trong doanh nghiệp nhưng lại được phát triển với các use case khác nhau (có thể coi như Hyperledger là một hệ sinh thái). Hyperledger có nhiều Frameworks như: Hyperledger Iroha: Được thiết kế cho các dự án mobile, thuật toán đồng thuận Sumeragi, Hyperledger Sawtooth: Được thiết kế cho các dự án liên quan đến IoT, thuật toán đồng thuận Proof of Elapsed Time (PoET) có khả năng xử lý hàng triệu transaction/giây, Hyperledger Fabric: Kiến trúc có tính mô đun hóa, plug-and-play components, Hyperledger Burrow: Sử dụng Ethereum Virtual Machine (EVM) cho việc thực thi smartcontract, Hyperledger Indy: Hỗ trợ xác định danh tính người dùng,... Có thể nói hệ sinh thái Hyperledger là tiềm năng để ứng dụng công nghệ blockchain vào đời sống hằng ngày.[8]

1.8. Ứng dụng của Blockchain.

1.8.1. Đối với sản xuất.

Áp dụng đặc điểm không thể làm giả, không thể phá hủy của Blockchain vào ngành công nghiệp sản xuất sẽ giúp người tiêu dùng truy xuất được nguồn gốc xuất xứ của sản phẩm đang được chào bán.

Ví dụ: Nếu một doanh nghiệp sản xuất sữa áp dụng Blockchain vào quản lý chất lượng sản phẩm thì nhà quản lý người tiêu dùng có thể truy xuất được các thông tin rất minh bạch.

Đối với nhà sản xuất họ có thể thống kê và lưu trữ toàn bộ những hộp sữa đó trên thị trường để biết được những hộp sữa đó đã tiêu thụ chưa, tiêu thụ được bao nhiêu, bao nhiêu hộp còn hạn sử dụng và bao nhiêu hộp đã hết hạn sử dụng. Đối với

người tiêu dùng: Có thể kiểm tra thông tin hộp sữa đó có phải hàng chính hãng hay không sẽ ngăn chặn toàn bộ những sản phẩm nhái, hàng giả trên thị trường.

1.8.2. Đối với lĩnh vực y tế.

Khi người bệnh đi khám hay xét nghiệm, mọi kết quả của họ sẽ được lưu trữ sử dụng công nghệ blockchain sẽ giúp người bệnh bảo mật toàn bộ thông tin và chỉ số xét nghiệm của mình. Trong trường hợp người bệnh có nhu cầu chuyển sang bệnh viện khác ở bất kỳ đâu trên thế giới, họ chỉ cần truy xuất thông tin và kết quả chỉ số xét nghiệm của mình trên chuỗi blockchain mà cho dù hai bệnh viện (nơi khám ban đầu và nơi chữa bệnh mới) không cùng ngôn ngữ hay sử dụng phần mềm khác nhau.

Việc này giúp người bệnh giảm thiểu chi phí xét nghiệm lại khi đến các bệnh viện mới cũng như góp phần giúp nơi tiếp nhận bệnh nhân mới có thể truy xuất tiền sử bệnh tật, phác đồ điều trị hay các phản ứng phụ đối với các loại thành tố thuốc trước đây của bệnh nhân. Để từ đó giúp chẩn đoán và đưa ra liệu trình điều trị phù hợp, mang lại hiệu quả cao cho người bệnh.

1.8.3. Đối với giáo dục.

Những năm gần đây với công nghệ ngày càng tiên tiến hiện tượng bằng giả xuất hiện ngày càng tinh vi và khó phát hiện. Việc thẩm định bằng cấp, chứng chỉ là một vấn đề phức tạp và chưa bao giờ hết nóng mới đối với nhiều nước trên thế giới. Khi tìm kiếm trên google, chúng ta có thể dễ dàng nhận thấy việc mua bán bằng cấp, chứng chỉ giả ở nhiều website trên thế giới. Việc quản lý các chứng chỉ, bằng cấp của các trường đại học nói chung hay các cơ sở đào tạo nghề nói riêng nếu được áp dụng công nghệ Blockchain sẽ góp phần minh bạch hóa hồ sơ học viên cũng như giúp các nhà tuyển dụng dễ dàng truy xuất nguồn gốc cơ sở đào tạo hay quá trình học tập của các ứng viên từ thấp đến cao.

1.8.4. Đối với ngành tài chính.

Nhiều ngân hàng và các tổ chức tài chính khác nhau đã nghiên cứu, áp dụng công nghệ Blockchain vào các hoạt động nghiệp vụ của mình. Ba ngân hàng lớn của Nhật Bản gồm Mizuho Bank, Sumitomo Mitsui Banking và Bank of Tokyo-Mitsubishi UFJ đã công bố việc áp dụng công nghệ blockchain trong hoạt động của mình. Lâu nay, các ngân hàng thường bị người tiêu dùng phàn nàn vì phí dịch vụ chuyển tiền cao. Dự án chuyển tiền ngang hàng sử dụng công nghệ blockchain là một phần trong những nỗ lực cung cấp dịch vụ tài chính an toàn, bảo mật cao với chi phí thấp. Tại Châu Á, OCBC Bank là ngân hàng đầu tiên trên thế giới sử dụng công nghệ blockchain (khối chuỗi) trong dịch vụ chuyển tiền nội địa và quốc tế, làm tăng hiệu suất, sự minh bạch, giảm chi phí và cải thiện trải nghiệm cho khách hàng.

Blockchain được xem như là một cách để cắt giảm chi phí và thời gian thanh toán bù trừ giao dịch liên ngân hàng, cũng như tạo ra hệ thống an toàn hơn. Tại thời điểm này, nhiều tổ chức tài chính đang có cuộc chiến tranh giành nhau nhằm hình thành các liên minh mới để thương mại hóa công nghệ blockchain.

1.8.5. Đối với thương mại điện tử.

Thị trường bán lẻ hiện nay nên dần dần chuyển dịch vụ của mình sang bán hàng trực tuyến, tận dụng lợi thế thương hiệu với chiến lược đa kênh để đạt được thành công và bảo vệ vị trí hiện tại. Nhìn chung, sự tin tưởng của người tiêu dùng và chi phí cao cho mô hình phân phối là những thách thức lớn cần được các doanh nghiệp giải quyết để thương mại điện tử tiến xa hơn nữa. Những thách thức lớn đó của thương mại điện tử có thể được xử lý bằng các hợp đồng thông minh (smart contract) khi ứng dụng công nghệ Blockchain.

1.9. So sánh Blockchain và cơ sở dữ liệu.

1.9.1. Lợi ích của blockchain so với cơ sở dữ liệu.

- **Phân tán:**

Đây là tính chất quan trong nhất của blockchain. Với blockchain dữ liệu được tập trung lại một nơi mà sẽ được lưu trữ ở tất cả các node tham gia vào mạng lưới. Điều này có lợi khi một node nào đó trong mạng lưới bị tấn công dữ liệu vẫn còn tồn tại và tiếp tục được sử dụng.

- **Minh bạch:**

Khi các blockchain được chia sẻ và mọi người có thể thấy những gì có trong blockchain, điều này cho phép hệ thống được minh bạch và kết quả là sự tin tưởng được thiết lập. Đây là một ưu điểm đặc biệt của blockchain so với cơ sở dữ liệu tập trung.

- **Tính không thay đổi:**

Một khi dữ liệu đã được lưu vào blockchain, rất khó để thay đổi nó. Nó không thực sự bất biến nhưng, do thực tế là việc thay đổi dữ liệu là vô cùng khó khăn và hầu như không thể, đây được coi là một lợi ích đối với những dữ liệu quan trong cần lưu giữ lâu dài tránh thất thoát.

- **Độ an toàn cao:**

Tất cả các giao dịch trên một blockchain được bảo mật bằng mật mã.

- **Tiết kiệm thời gian và chi phí:**

Đối với giao dịch tài chính, Ứng dụng blockchain vào các loại tiền mã hóa giúp giảm đước đáng kể chi phi giao dịch cho người dung, thời gian giao dịch được rút ngắn hơn rất nhiều so với cơ sở dữ liệu tập trung thông thường.

1.9.2. Bất lợi của blockchain so với cơ sở dữ liệu.

- **Thông tin lưu trữ mãi mãi và không thể sửa được:**

Đây vừa là một lợi thế lớn của blockchain nhưng cũng là một bất lợi không nhỏ khi so vơi cơ sở dữ liệu tập trung thông thương. Với việc lưu trữ thông tin mãi mãi sẽ gây tốn kém với những dữ liệu không quan trong do đó hệ thống khi

một hệ thông cần kiểm soát độ lớn của dữ liệu thì giải pháp blockchain là không khả thi.

- **Vấn đề băng thông**

Mỗi node trong mạng lưới cần liên lạc với những node khác để nhận giao dịch về, xác thực giao dịch và công bố kết quả kiểm tra giao dịch. Những nhiệm vụ này làm tốn băng thông mạng, có thể ảnh hưởng lớn tới mạng Internet trong khu vực.

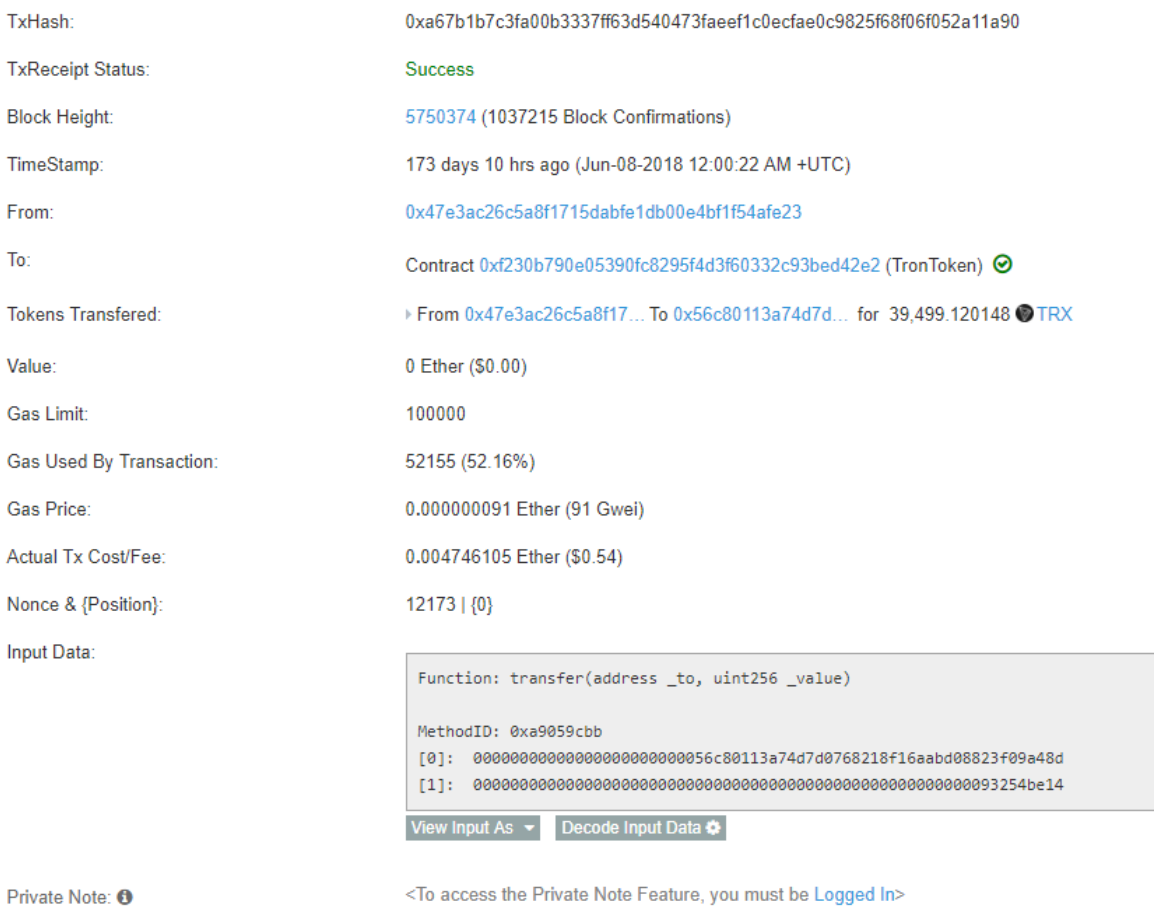
2. Tổng quan về Ethereum.

2.1. Giới thiệu về Ethereum.

Ethereum là một nền tảng điện toán có tính chất phân tán, công cộng, mã nguồn mở dựa trên công nghệ Blockchain. Nó có tính năng tạo ra các hợp đồng thông minh tạo thuận lợi cho các thỏa thuận hợp đồng trực tuyến. Nền tảng này bao gồm một máy ảo gọi là Ethereum Virtual Machine (EVM), có thể thực thi các kịch bản bằng cách sử dụng một mạng lưới máy tính Ethereum. Ethereum cũng cung cấp một loại tiền mã hóa gọi là "Ether", có thể được chuyển giữa các tài khoản và được sử dụng để trả công cho các thợ đào giúp thực hiện việc tính toán. "Gas" là một cơ chế giá giao dịch nội bộ, được sử dụng để giảm thiểu giao dịch rác và phân bổ các nguồn lực trên mạng lưới.

Ethereum đã được đề xuất vào cuối năm 2013 bởi Vitalik Buterin, một nhà nghiên cứu tiền mã hóa và nhà lập trình. Việc phát triển Ethereum ban đầu được tài trợ qua hình thức crowdfunding (tài trợ đám đông) suốt tháng 7 và tháng 8 năm 2014. Hệ thống này đã được khởi động vào ngày 30 tháng 7 năm 2015, với 11, 9 triệu đồng ether đã được đào sẵn (premined) để bán lại cho những người đã tài trợ. Số tiền này chiếm khoảng 13% tổng số ether được lưu hành.

Giao dịch trong mỗi ứng dụng blockchain là một thành phần không thể thiếu và Ethereum cũng vậy. Mỗi giao dịch trong blockchain của Ethereun không chỉ là chuyển tiền từ người này sang người khác mà còn có thể là lưu trữ dữ liệu nào đó lên mạng lưới blockchain.



Hình 2. 7.Cấu trúc của một transaction trong mạng lưới blockchain ethereum

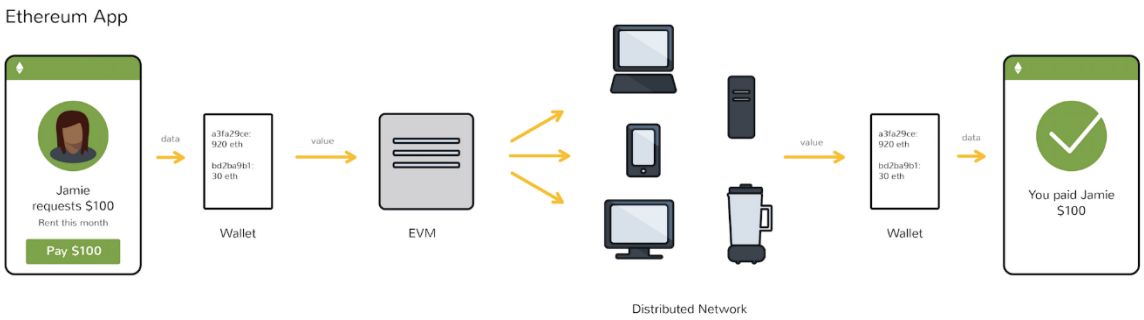
- TxHash là mã hash của giao dịch.
- Status: là trạng thái của giao dịch. Trong hình ví dụ trạng thái của giao dịch là success ngoài ra có các trạng thái là field và pending
- Block Height: là giá trị index của block trong mạng lưới ethereum hiện tại.
- TimeStamp: là thời gian giao dịch được tạo ra.
- From: là địa chỉ ethereum tạo ra giao dịch.
- To: là địa chỉ ethereum của bên nhận. Ở giá trị from và to này có thể là địa chỉ của một người tham gia vào mạng lưới hoặc cũng có thể là một địa chỉ của smart contract được triển khai lên mạng lưới.
- Value: là lượng ether mà người dùng muốn gửi đi trong giao dịch.
- Gas Limit: là lượng gas tối đa mà phải trả cho một giao dịch.
- Gas Used by Transaction: là số gas thực sự được dùng.
- Gas Price: là lượng gas được quyết định bởi thợ đào.

- Actual Tx Cost/Fee: là chi phí mà người dùng phải trả cho một giao dịch. Giá trị này được tính bằng Gas Price * Gas Used.
- Nonce: là số lần địa chỉ đã giao dịch
- Input data: là dữ liệu truyền vào khi gọi một hàm trong smart contract.

2.2. Cách thức hoạt động của smart contract Ethereum.

Cũng như bất kỳ blockchain nào, Ethereum cũng cần hàng ngàn người chạy phần mềm trên máy tính để tiếp sức cho mạng lưới. Mỗi node hay chính là một máy tính trong mạng lưới sẽ chạy một thứ gọi là Ethereum Virtual Machine (EVM). Hãy nghĩ về EVM như một hệ điều hành có thể hiểu và chạy các phần mềm được viết bằng ngôn ngữ lập trình riêng của Ethereum. Phần mềm hay ứng dụng chạy trên EVM được gọi là các hợp đồng thông minh (smart contract).

Với Ethereum, mỗi khi một chương trình được sử dụng, một mạng lưới hàng ngàn máy tính sẽ tham gia xử lý nó. Hợp đồng thông minh được viết bằng ngôn ngữ lập trình có tên là Solidity và được biên dịch thành 'bytecode' tượng tự ngôn ngữ lập trình Java, để máy ảo EVM có thể đọc và thực thi được code. Tất cả các node là các máy tính thực hiện hợp đồng này sử dụng EVM trên chính nó. Mỗi node trong mạng lưới giữ một bản sao của giao dịch và lịch sử hợp đồng thông minh của mạng'. Mỗi khi người dùng thực hiện một số hành động, tất cả các node trên mạng cần phải đi đến thỏa thuận rằng thay đổi này đã diễn ra và chấp thuận nó. Máy ảo EVM thực hiện hợp đồng với bất kỳ quy tắc nào mà nhà phát triển lập trình ra lúc đầu.



Hình 2. 8. Quá trình thực hiện của Ethereum App

Việc tính toán thực tế EVM được thực hiện thông qua bytecode được biên dịch từ một ngôn ngữ lập trình bậc cao đó là Solidity. Với sự góp mặt của EVM nền tảng blockchain của ethereum không còn đơn giản chỉ là những giao dịch tiền tệ qua lại của người dùng như blockchain bitcoin mà nó có thể được áp dụng rộng rãi ở nhiều lĩnh vực khác nhau. Hợp đồng thông minh cho phép các nhà phát triển có thể tạo ra các luật đảm bảo ứng dụng được thực thi chính xác và là trung gian xử lý các thỏa thuận của những người liên quan mà không cần đến bên thứ ba. Nhờ những cải

tiến so với người tiền nhiệm bitcoin, ethereum giờ đây không chỉ là một đồng tiền mã hoá mà nó được xem là một mạng lưới.

2.3. Ứng dụng của Ethereum.

Nhìn chung, sẽ có 3 nhóm ứng dụng dựa trên nền tảng Ethereum:

- Các ứng dụng tài chính:

Cung cấp cho người dùng những cách quản lý và ký kết hợp đồng bằng tiền của họ. Nó bao gồm các đơn vị tiền tệ, các công cụ tài chính phát sinh, các hợp đồng bảo hiểm rủi ro, ví tiền tiết kiệm, di chúc, và thậm chí một số các loại hợp đồng lao động.

- Các ứng dụng bán tài chính:

Trong đó có tiền tệ và những thứ phi tiền tệ, ví dụ như các giải pháp tính toán phân tán. Và cuối cùng là các ứng dụng như bầu chọn trực tuyến, quản trị phân quyền hoàn toàn không liên quan đến tài chính và tiền tệ.

- Các ứng dụng khác:

Hệ thống token, đơn vị tài chính tiền tệ có sự ổn định (hoặc có thể điều chỉnh để trở nên ổn định) dùng trong các hợp đồng, hệ thống nhận dạng, xác nhận chủ sở hữu tài sản, hệ thống lưu trữ file phân tán, các tổ chức tự trị phi tập trung (Decentralized Autonomous Organizations) … DApp (Decentralized Application – Các ứng dụng phi tập trung) đã đưa World Wide Web đến sự tiến hóa tự nhiên tiếp theo của nó, giới thiệu các ứng dụng phân quyền với giao thức peer-to-peer và đưa chúng vào sử dụng trong mọi khía cạnh của ứng dụng web. Thuật ngữ được sử dụng để mô tả sự tiến hóa này là Web3 (version 3 of web) được đề xuất bởi Gavin Wood, Web3 đại diện cho tầm nhìn và trọng tâm mới cho các ứng dụng web, chuyển từ các ứng dụng do trung tâm quản lý tới các ứng dụng được xây dựng trên giao thức phi tập trung.

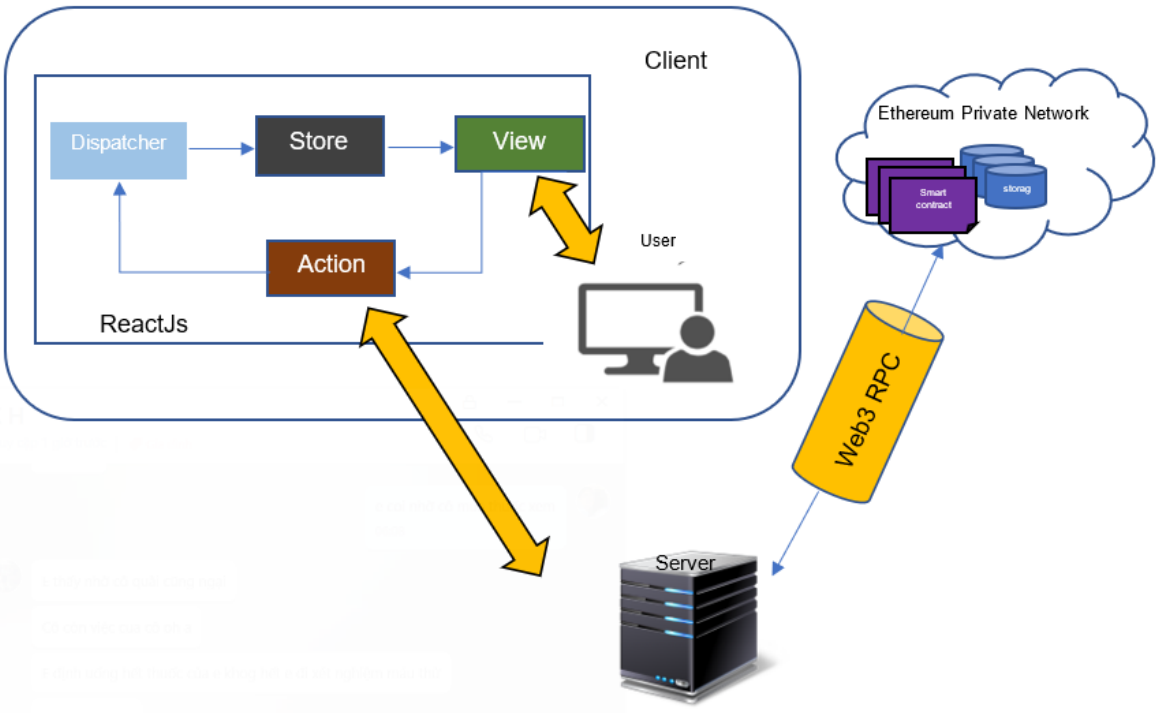
CHƯƠNG 3: KIẾN TRÚC HỆ THỐNG VÀ CÀI ĐẶT HỆ THỐNG

1. KIẾN TRÚC HỆ THỐNG.

Hệ thống sử dụng mô hình Flux kết hợp với mô hình client – server để xây dựng hệ thống website quản lý bầu chọn dựa trên nền tảng mạng lưới blockchain ethereum.

1.1. Sơ đồ tổng quan hệ thống.

User sẽ tương tác với view để tạo ra action (trong kiến trúc Flux). Sau đó Action sẽ gọi đến server để lấy dữ liệu hoặc thêm dữ liệu vào mạng lưới blockchain. Trong sơ đồ này là sự kết hợp giữa kiến trúc Flux được sử dụng trong Reactjs và mô hình Client – Server truyền thống. Tuy nhiên dữ liệu ở đây sẽ không là những hệ quản trị cơ sở dữ liệu thông thường thấy mà sẽ là mạng lưới blockchain được xây dựng và mô tả ở hình 3.1.



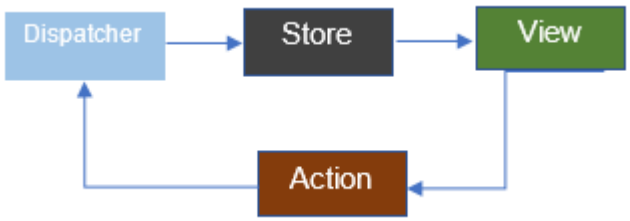
Hình 3. 1. Sơ đồ tổng quan hệ thống

- **ReactJs**: được dùng để xây dựng giao diện tương tác với người dùng. Mỗi khi người dùng thực hiện một thao tác nào đó ví dụ như đăng nhập thì react sẽ gọi đến server để lấy kết quả về.
- **Server:** Là nơi nhập và xử lý các hành động của người dùng. Ví dụ như tính năng đăng nhập server sẽ dùng web3 gọi đến hàm Login(…) trong smartcontract để gửi kết quả về cho ReactJs.

- **Web3:** Là bộ phần trung gian giao tiếp giữa server và mạng lưới blockchain vừa xây dựng. Mỗi khi một hành động nào đó xảy ra thông thương server đều sẽ dùng web3 để tương tác với mạng lưới blockchain.

1.2. Mô hình Flux.

Flux là mô hình kiến trúc được Facebook đề xuất trong framework reactjs. Đây là mô hình kiến trúc mới thường được so sánh với mô hình MVC.

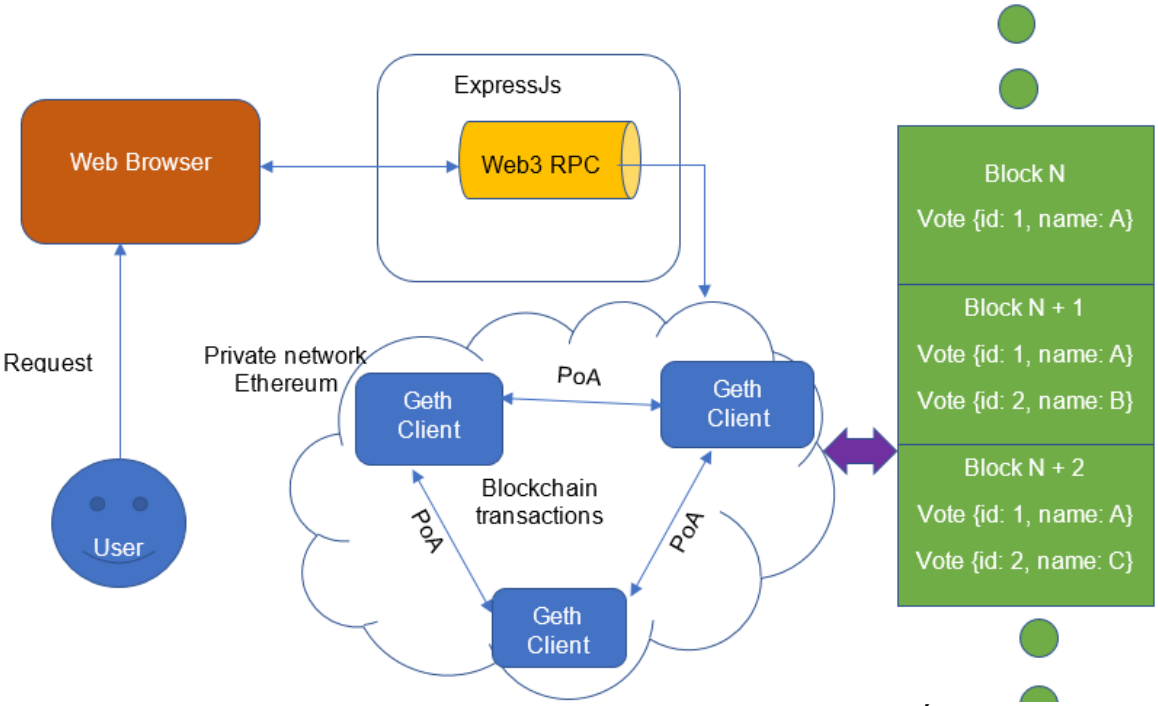


Hình 3. 2. Sơ đồ mô hình Flux

Trong mô hình này View sẽ là giao diện hiển thị các thông tin. Người dùng tương tác với View sẽ gọi đến Action là nơi khởi tạo hành động. Action ở đây sẽ có 2 loại:

- Action gọi Dispatcher đểu phát đi hành động thay đổi dữ liệu
- Action gọi đến Server để lấy dữ liệu.

1.3. Mối quan hệ giữa các công nghệ.



Hình 3. 3. Các công nghệ được ứng dụng trong hệ thống

1.3.1. Geth client.

Geth là giao diện dòng lệnh dùng để chạy một node trong mạng lưới Ethereum và nó được phát triển bằng ngôn ngữ Go. Geth giúp chúng ta có thể giao tiếp với mạng lưới Ethereum blockchain, thực hiện các giao dịch, smart contract, mining.

1.3.2. Proof of Authority(PoA).

Cơ chế đồng thuận được sử dụng trong mạng private blockchain ethereum này là Proof of Authority (PoA – thuật toán ủy quyền). Đây là một thuật toán sử dụng cơ chế đồng thuận thay thế. Thay vì sử dụng hash để giải quyết các vấn đề toán học khó khăn, PoA sử dụng một tập hợp các lệnh ủy quyền cho phép tạo block mới đồng thời đảm bảo tối đa tính an toàn của blockchain.

PoA giúp người dùng thực hiện giao dịch ngay lập tức và đồng thuận liên tục trên một mạng lưới phân quyền. Giải thuật đồng thuận này dựa trên các node được tin tưởng, có danh tính rõ ràng để xác nhận và tạo block mới. Mỗi node trong mạng lưới sẽ lần lướt nhau xác nhận và tạo block mới. Trong cơ chế đồng thuận này khi khởi tạo mạng lưới ta cần khởi tạo các Sealer là những người xác nhận block cho mạng lưới. Với PoA chúng ta sẽ không còn được nhận phần thưởng là một lượng coin nào đó sau khi xác nhận một block mới do đó khi khởi tạo các Sealer ta cần cập một lượng coin thật lớn cho các Sealer này để các Sealer này xác minh các giao dịch trong hệ thống hoặc cung cấp lượng coin cho nhưng người khác. Số lượng Sealer tối thiểu của mỗi mạng lưới sử dụng cơ chế đồng thuận này sẽ tuân theo công thức int(N/2 + 1) trong đó N là số lượng Sealer. Khi mạng lưới đã được khởi tạo muốn thêm node xác nhận cho block thì phải có sự đồng ý của (N/2 + 1) node chấp nhận và file genesis. jon chính là file khởi tạo ra block đầu tiên của mạng lưới. Khi mạng lưới đã được tạo ra một node mới sẽ được gọi là Signer. Về cơ bản Signer và Sealer là giống nhau đều có quyền xác nhận một block mới, có quyền chấp nhận một Signer mới tham gia vào mạng tuy nhiên Sealer là node được khởi tạo bạn đầu do đó để phân biệt người ta gọi các node được thêm vào sau khi mạng lưới blockchain đã được hình thành là Signer.

PoA là cơ chế đồng thuận mới, nó được đề xuất nhằm khắc phục các nhược điểm như tốn kém điện năng hay chi phí bỏ ra rất cao của các cơ chế đồng thuận tiền nhiệm như Proof of Work hay Proof of State. Với PoA một block mới được tạo ra bởi một node có danh tính rõ ràng, ít tốn kém điện năng, thời gian hoàn thành một block khá nhanh khoản 5 giây.

2. CÀI ĐẶT HỆ THỐNG.

2.1. Thiết kế và cài đặt smart contract.

2.1.1. Cấu trúc smartcontract.

Trong smartcontract này có 3 struct lần lược đại diện cho người dùng, ứng cử viên và cuộc bầu chọn. Struct User là cấu trục thông tin về người dùng sẽ được

lưu vào hệ thống blockchain, Struct Candidate là cấu trúc thông tin của ứng cử viên, Struct Vote là cấu trúc thông tin của cuộc bầu chọn.

```
struct Candidate{
  uint id; //id của ứng cử viên
  string hash; //chuỗi ký tự băm sử dụng để lấy thông tin ứng cử viên
  string hashImage; //chuỗi ký tự băm để lấy hình đại diện
  uint vote; //lượng phiếu bầu của ứng cử viên
}

struct User {
  Roles role; //Loại người dùng
  mapping (address => mapping(uint => bool)) voted; //đã bầu chọn nào
  mapping (address => mapping(uint => uint[])) voteFor; //đã bầu cho ai
  string hash; //hash thông tin
  string hashImage; //hash hình ảnh
  bool exist; //kiểm tra sự tồn tại của người dùng
  string pass; //mật khẩu đăng nhập
  string passAddr; //mật khẩu địa chỉ ethereum
  address addr; //địa chỉ ethereum
}

struct Vote {
  mapping(uint => string) hash; //hash thông tin
  mapping(uint => string) hashImage; //hash hình ảnh
  mapping(uint => Candidate[]) candidates; //mảng ứng cử viên
  mapping(uint => TypeVote) typeVote; //loại của cuộc bầu chọn
  mapping(uint => uint) number; //số lượng bầu chọn
  mapping(uint => uint256) deadLine; //ngày hết hạng
}
```

Tiếp theo trong smartcontract này sẽ định nghĩa một mảng chứa các username, và ba kiểu mapping lưu trữ danh sách người dùng, danh sách các cuộc bầu chọn và số lượng các cuộc bầu chọn. Kiểu dữ liệu mapping trong solidity là kiểu dữ liệu dạng key value tương tự như kiểu dữ liệu dictionary ở các ngôn ngữ khác.

```
string[] private userNames; //danh sách tên người dùng

mapping (string => User) private users; //danh sách thông tin người dùng

mapping(string => Vote) private votes; // danh sách các cuộc bầu chọn

mapping(string => uint) private countVote; //tổng số cuộc bầu chọn
```

2.1.2. Các hàm quan trọng trong smart contract.

- **Hàm tạo người dùng:**

Trong hàm này sẽ xử lý thêm dữ liệu người dùng vào smart contract.

```
function CreateUser (string _userName, address _addr, string _hash, string
_hashImage, uint _role, string _pass, bool _passAdd) public {
    if(!users[_userName]. exist){
      userNames. push(_userName);
    }

    if(_passAdd) {
      users[_userName]. passAddr = _pass;
      users[_userName]. pass = _pass;
    }

    users[_userName]. addr = _addr;
    users[_userName]. hash = _hash;
    users[_userName]. hashImage = _hashImage;
    users[_userName]. exist = true;
    if(_role == 0){
      users[_userName]. role = Roles. CREATEVOTE;
    }
    else{
      users[_userName]. role = Roles. VOTE;
    }
  }
```

- **Hàm tạo cuộc bầu chọn:**

Hàm này sẽ thêm dữ liệu một cuộc bầu chọn mới vào smart contract

```
function CreateVote(string _hash, uint _type, uint256 _deadLine, uint
_number, string _userName, string _hashImage) public {
    require(CheckUserName(_userName), "Bạn không có quyền");
    require(users[_userName]. role == Roles. CREATEVOTE ||
users[_userName]. role == Roles. ADMIN, " Bạn không có quyền ");

    countVote[_userName] += 1;
    if(_type == 0){
      votes[_userName]. typeVote[countVote[_userName]] = TypeVote. All;
    }
    else if(_type == 1){
      votes[_userName]. typeVote[countVote[_userName]] = TypeVote. One;
    }
    else if(_type == 2){
      votes[_userName]. typeVote[countVote[_userName]] = TypeVote. MofN;
    }
    votes[_userName]. hashImage[countVote[_userName]] = _hashImage;
    votes[_userName]. hash[countVote[_userName]] = _hash;
    votes[_userName]. number[countVote[_userName]] = _number;
```

```
    votes[_userName]. deadLine[countVote[_userName]] = _deadLine;
  }
```

- **Hàm tạo ứng cử viên:**

Hàm này sẽ thêm dữ liệu từng ứng cử viên vào smart contract. Do hạng chế của ngôn ngữ solidity là không nhận tham số truyền vào là mảng chuỗi nên tạm thời sẽ phải tạo từng ứng viên riêng lẽ:

```
function CreateCandidate (string _hash, string _hashImage, string _userName)
public {
    require(CheckUserName(_userName), "Bạn không có quyền");
    require(users[_userName]. role == Roles. CREATEVOTE || users[_userName].
role == Roles. ADMIN, " Bạn không có quyền ");

    uint indexCandidate = votes[_userName].
candidates[countVote[_userName]]. length;
    votes[_userName]. candidates[countVote[_userName]].
push(Candidate(indexCandidate + 1, _hash, _hashImage, 0));
  }
```

- **Hàm bầu chọn:**

Hàm này sẽ lưu lại thông tin mà người dùng sẽ bầu chọn cho ứng viên nào đồng thời tăng số lượt bầu chọn cho ứng cử viên và ghi nhận lại người dùng đã bầu chọn cho cuộc bầu chọn nào. Hàm này xử lý bầu chọn đồng thời cho nhiều ứng cử viên.

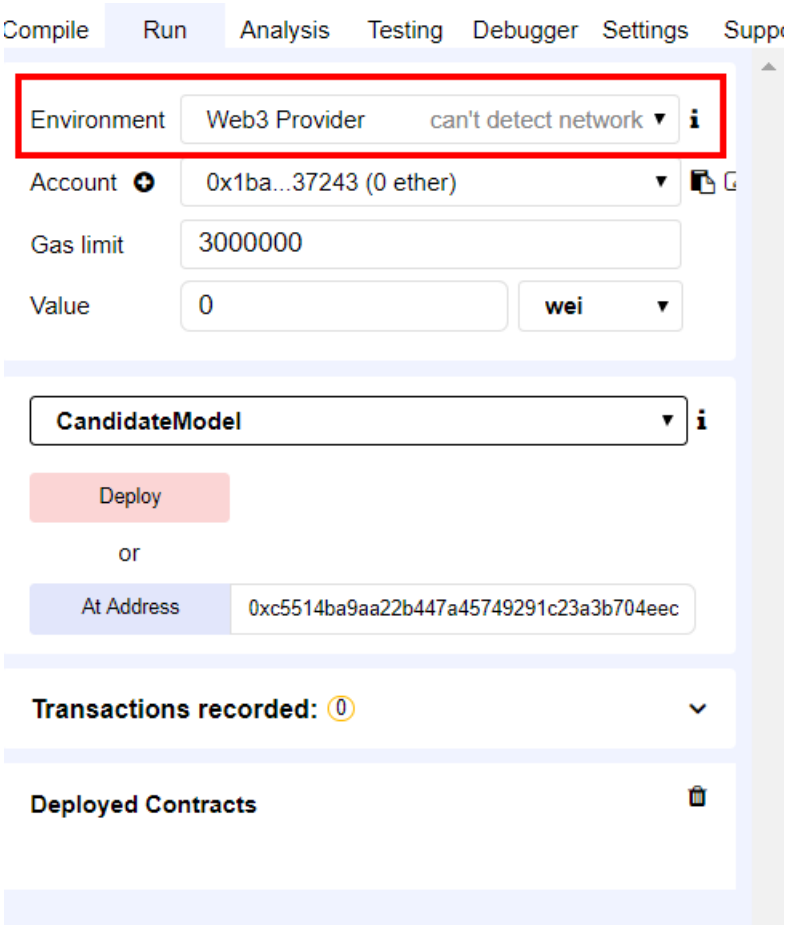
```
function Voting (address _addr, string _userVote, string _userName, uint[]
_idCandidate, uint _idVote) public payable {
        require(CheckUserName(_userName), "User chưa tồn tại");
        require(!CheckVoted(_userName,_idVote,_addr), "User đã bầu cho cuộc
bầu chọn này");
        require(_idVote > 0 && _idVote <= countVote[_userVote], "Số lượng
ungws cử viên không đúng");
        for(uint i = 0; i < _idCandidate.length; i++){
            votes[_userVote].candidates[_idVote][_idCandidate[i]].vote += 1;
            users[_userName].voteFor[_addr][_idVote].push(_idCandidate[i]);
        }

        users[_userName].voted[_addr][_idVote] = true;
    }
```

2.1.3. Cài đặt smart contract.

Sử dụng remix.ethereum.org là IDE hỗ trợ phát triển smartcontract để triển khai smart contract đã viết lên mạng lưới blockchain được xây dựng. Trang web sẽ có giao diện như hình 3.5.

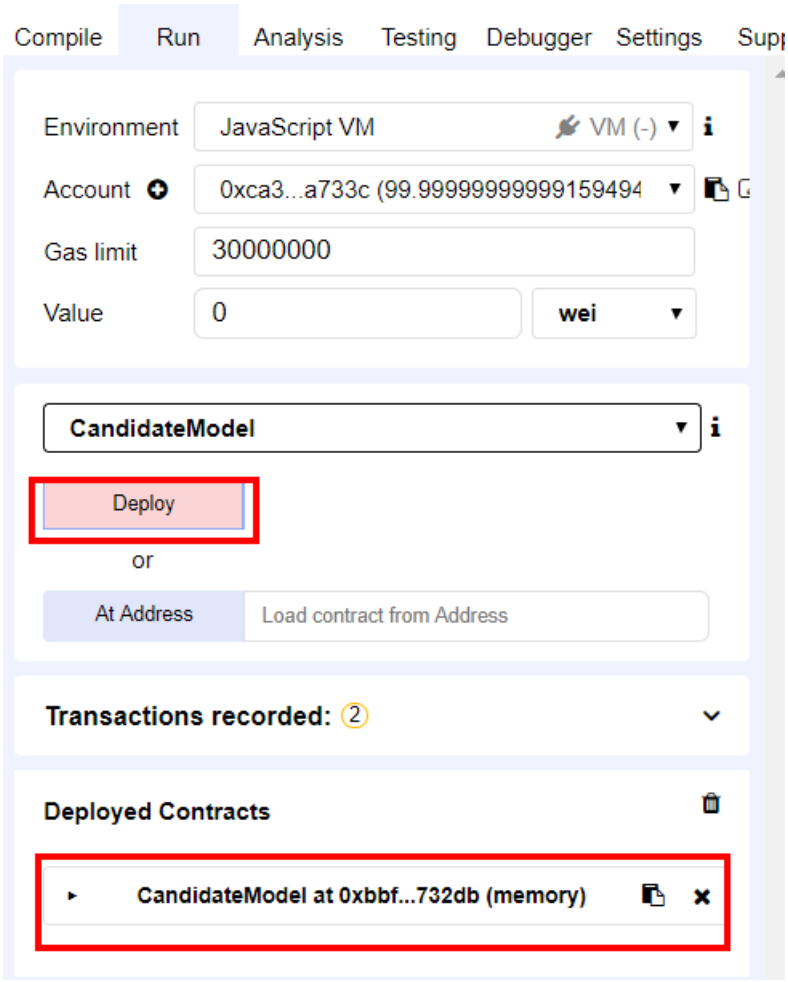
Hình 3. 5. Giao diện trang Remix.

Ở tab Run chọn Environment rồi chọn Web3 Pr ovider sau đó nhập địa chỉ IP và Port của mạng blockchain vào.



Hình 3. 4.Giao diện chọn kết nối đến mạng private blockchain ethereum

Sau khi kết nối thanh công click Deploy để thực hiện đưa smart contract lên mạng private blockchain



Hình 3. 6. Giao diện deploy smartcontract

2.2. Cài đặt mạng private blockchain ethereum.

2.2.1. Một số khái niệm cơ bản.

- **Thuật toán đồng thuận**: Là một giải thuật dùng để quy định ra các luật giúp những người tham gia vào mạng lưới blockchain có sự thống nhất trong việc lưu trữ dữ liệu.
- **Clique**: Mạng lưới Ethereum sử dụng cơ chế đồng thuận Proof of Authority còn được gọi là Clique.
- **Genesis. json**: Là file khởi tạo cho block đầu tiên trong mạng private blockchain ethereum.
- **Puppeth**: Là công cụ hỗ trợ tạo file genesis. json đơn giản để khởi tạo được một mạng blockchain Ethereum.

2.2.2. Giới thiệu về genesis. json.

Genesis. json là file cấu hình cho block đầu tiên được khởi tạo trong mạng. Sử dụng lệnh puppeth để tạo file genesis. json như sau:

```
Please specify a network name to administer (no spaces, please)
> devnet
What would you like to do? (default = stats)
 1. Show network stats
 2. Configure new genesis
 3. Track new remote server
 4. Deploy network components
> 2
Which consensus engine to use? (default = clique)
 1. Ethash - proof-of-work
 2. Clique - proof-of-authority
> 2
How many seconds should blocks take? (default = 15)
> 5 // for example
Which accounts are allowed to seal? (mandatory at least one)
> 0x87366ef81db496edd0ea2055ca605e8686eec1e6
> 0x08a58f09194e403d02a1928a7bf78646cfc260b0
Which accounts should be pre-funded? (advisable at least one)
> 0x87366ef81db496edd0ea2055ca605e8686eec1e6 // free ethers !
> 0x08a58f09194e403d02a1928a7bf78646cfc260b0
Specify your chain/network ID if you want an explicit one (default = random)
> 1515 // for example. Do not use anything from 1 to 10
Anything fun to embed into the genesis block? (max 32 bytes)
>
What would you like to do? (default = stats)
 1. Show network stats
 2. Manage existing genesis
 3. Track new remote server
 4. Deploy network components
> 2
1. Modify existing fork rules
 2. Export genesis configuration
> 2
Which file to save the genesis into? (default = devnet. json)
> genesis. json
INFO [01-23|15:16:17] Exported existing genesis block
What would you like to do? (default = stats)
 1. Show network stats
 2. Manage existing genesis
 3. Track new remote server
 4. Deploy network components
> ^C // ctrl+C để thoát khỏi lệnh puppeth
```

Sau khi thao tác xong các lệnh bên trên ta sẽ được file genesis. json dưới đây:


```
{
 "config": {
   "chainId": 1515,
   "homesteadBlock": 1,
   "eip150Block": 2,
   "eip150Hash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
   "eip155Block": 3,
   "eip158Block": 3,
   "byzantiumBlock": 4,
   "clique": {
     "period": 5,
     "epoch": 30000
   }
 },
 "nonce": "0x0",
 "timestamp": "0x5a722c92",
 "extraData":
"0x0000000000000000000000000000000000000000000000000000000000000000008a58f091
94e403d02a1928a7bf78646cfc260b087366ef81db496edd0ea2055ca605e8686eec1e600000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000",
 "gasLimit": "0x59A5380",
 "difficulty": "0x1",
 "mixHash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
 "coinbase": "0x0000000000000000000000000000000000000000",
 "alloc": {
   "08a58f09194e403d02a1928a7bf78646cfc260b0": {
     "balance":
"0x2000000000000000000000000000000000000000000000000000000000000000"
   },
   "87366ef81db496edd0ea2055ca605e8686eec1e6": {
     "balance":
"0x2000000000000000000000000000000000000000000000000000000000000000"
   },
   "F464A67CA59606f0fFE159092FF2F474d69FD675": {
     "balance":
"0x2000000000000000000000000000000000000000000000000000000000000000"
   }
 },
 "number": "0x0",
 "gasUsed": "0x0",
```

```
 "parentHash":
"0x0000000000000000000000000000000000000000000000000000000000000000"
}
```

- chainId: là Id của mạng private blockchain đang xây dựng. Vì Ethereum không chỉ bao gồm một blockchain duy nhất mà thực tế là có rất nhiều các network khác nhau. Hệ thống blockchain đang chạy thực tế có tên là Mainnet với chainId là 1 ngoài ra còn có các phiên bản network blockchain khác của ethereum như: ropsten (chainId: 3), rinkeby (chainId: 4), kovan (chainId: 42). Private chain mặc định sẽ có id mặc định là 1337 theo khuyến cáo của EIP 155. Trong mạng blockchain đang xây dựng chainId sẽ là 1515.
- period: là thời gian để tạo mới một block trong mạng. Vì theo đánh giá của các chuyên gia thời gian an toàn và đảm bảo cho một block được tạo ra không bị lỗi tốt nhất là 5 giây nên trong trường hợp này giá trị của period sẽ là 5.
- extraData: Là nơi khai báo các Sealer lúc khởi tạo mạng lưới.
- alloc: Do PoA không thưởng coin cho việc xác nhận các giao dịch vì thế đây là nơi khởi tạo một lượng coin nào đó cho các tài khoản ethereum để sử dụng trong mạng lưới sau này.
- gasLimit: gas là giá nội bộ dùng để chạy các giao dịch hoặc hợp đồng trên Ethereum. Mỗi lệnh tính toán sẽ được gửi đến EVM (Ethereum Virtual Machine) và để chạy 1 lệnh cụ thể sẽ tiêu tốn một số lượng gas tương ứng.
- timestamp: Là thời gian mà block được khởi tạo.

2.2.3. Lệnh Geth chạy mạng lưới.

Giới thiệu về lệnh chạy một node trong mạng lưới private blockchain đang xây dựng:

```
geth --datadir node1/ --syncmode 'full' --port 30311 --rpc --rpcaddr '192.
168. 1. 144' --rpccorsdomain "*" --rpcport 8501 --rpcapi 'admin, personal,
db,      eth,      net,      web3,      txpool,      miner'      --bootnodes
'enode://42f1baa671447e1adea7bf1b0f0d1cf92cc70782747b59e89a7c61ce5ff53a02cf2
1ac3e33a8136b4c8d10baa3013e6b282439f183b5666da662fc128f08fbec@192.  168.  1.
144:30310'    --networkid    1515    --gasprice    '1'    --mine    -unlock
'0x593307ed1041881d7eb2cb6779b8e894d6e4ec92' --password node1/password. txt
```

- --datadir: là tham số khai báo thư mục node sẽ chứa dữ liệu đồng bộ hóa từ mạng lưới.
- --syncmode: là chế độ đồng bộ hóa dữ liệu trong mạng lưới blockchain ethereum. Trong lệnh này đang để là full nghĩa là toàn bộ dữ liệu từ các node khác nhau sẽ được đồng bộ với nhau. Ngoài ra còn có chế độ fast và light giúp quá trình đồng bộ dữ liệu của node nhanh hơn mà vẫn đảm bảo thực thi đúng. Vơi chế độ fast node sẽ chỉ lấy thông tin header, body của block. Còn với light node sẽ chỉ lấy trạng

thái hiện tại do đó để hoạt động nó sẽ cần hỏi những node xung quanh đầy đủ thông tin.

- --port: cổng cho việc thực thi của node trong mạng lưới.
- --rpcapi: khai báo các module được phép sử dụng trong mạng lưới. Các module này có thể dùng để đọc thông tin về node, đọc thông tin tài khoản ethereum, đọc thông tin một giao dịch hay một block thâm chí tạo ra một giao dịch trong mạng lưới.
- --bootnodes: Khai báo này là địa chỉ của node để khởi động.
- --networkid: là tham số chainId được định nghĩa trông file genesis. json

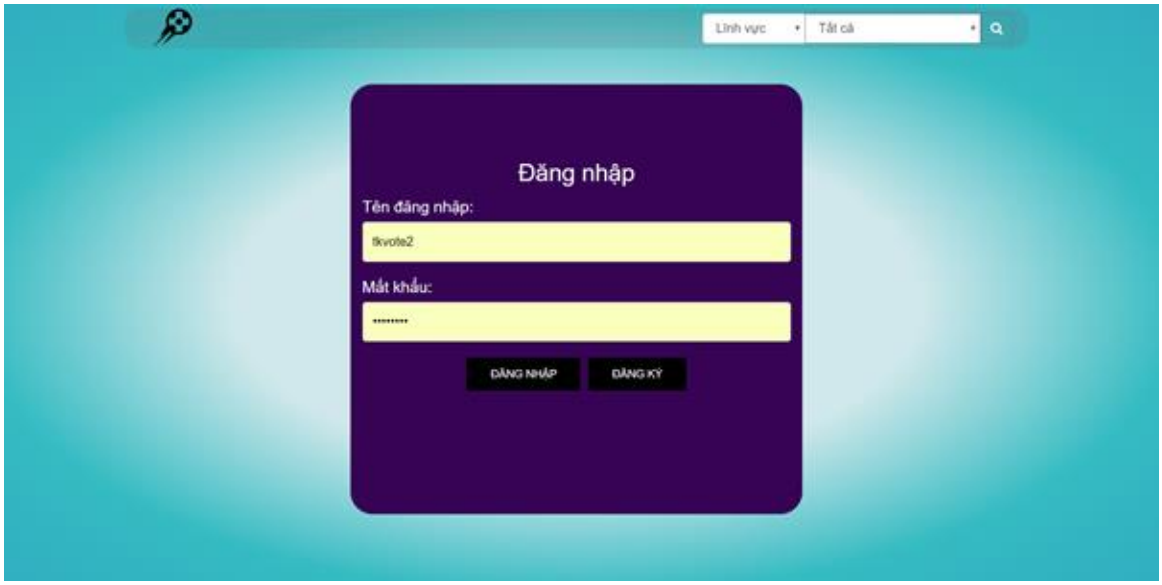
3. CÀI ĐẶT CÁC CHỨC NĂNG

3.1. Chức năng đăng nhập.

3.1.1. Mục đích.

Nhằm cấp phép cho những người có tài khoản tham gia bầu chọn các ứng cử viên trong cuộc bầu chọn mình mong muốn

3.1.2. Giao diện.



Hình 3. 7. Giao diện đăng nhập

3.1.3. Các thành phần trong giao diện.

STT	Loại điều khiển	Nội dung thực hiện	Giá trị mặc định	Lưu ý
1	Textbox	Ô nhập tên đăng nhập		Bắt buộc nhập

2	Textbox	Ô nhập mật khẩu		Bắt buộc nhập
3	Button	Nút đăng nhập		

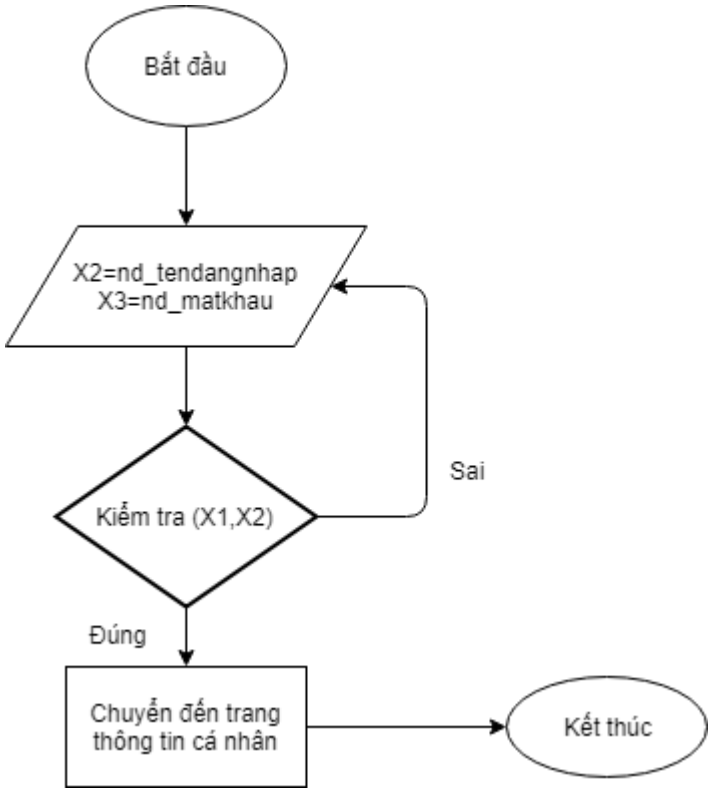
Bảng 3. 1. Các thành phần trong giao diện Đăng nhập

3.1.4. Thao tác dữ liệu.

STT	**Loại người dùng**	**Phương thức**	
		Thêm	**Truy vấn**
1	Admin		X
2	Tạo bầu chọn		X
3	Bầu chọn		X

Bảng 3. 2. Các thao tác dữ liệu Đăng nhập

3.1.5. Cách xử lý.



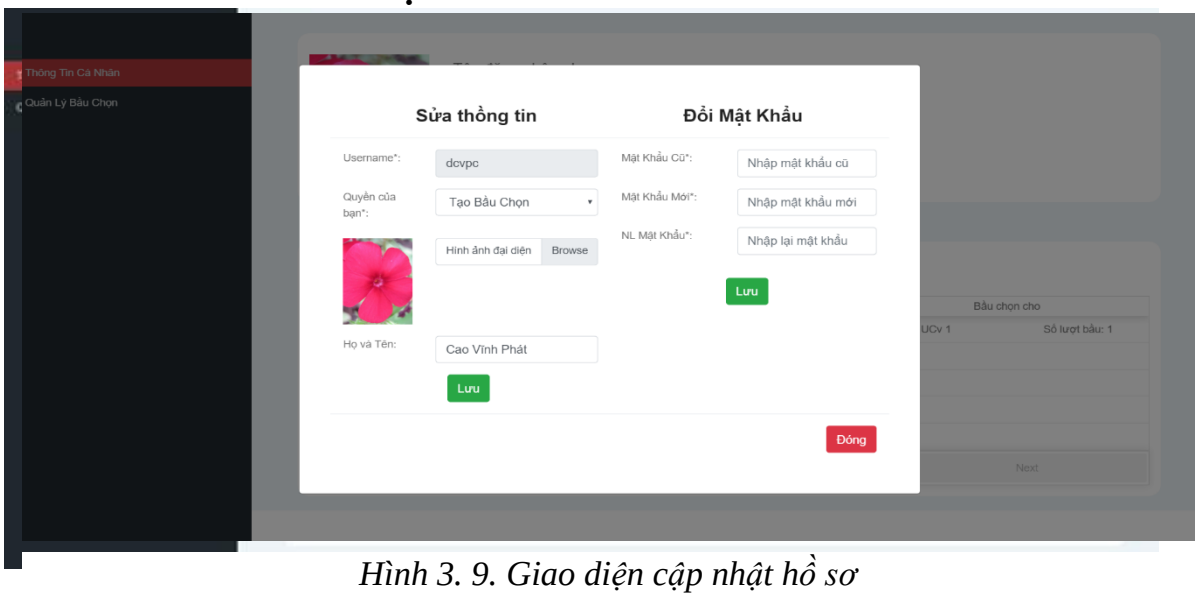
Hình 13. Sơ đồ xử lý đăng nhập

3.2. Chức năng cập nhật hồ sơ người dùng.

3.2.1. Mục đích.

Nhằm mục đích thay đổi thông tin người dùng.

3.2.2. Giao diện.



Hình 3. 9. Giao diện cập nhật hồ sơ

3.2.3. Các thành phần trong giao diện.

STT	Loại điều khiển	Nội dung thực hiện	Giá trị mặc định	Lưu ý
1	Button	Sửa thông tin		Bắt buộc nhập
2	Textbox	Sửa tên truy cập		Bắt buộc nhập
3	Combobox	Quyền người dùng		
4	FileInput	Hình đại diện		
5	Textbox	Sửa họ và tên		
6	Button	Lưu		
7	Button	Đóng		

Bảng 3. 3. Các thành phần trong giao diện Cập nhật hồ sơ

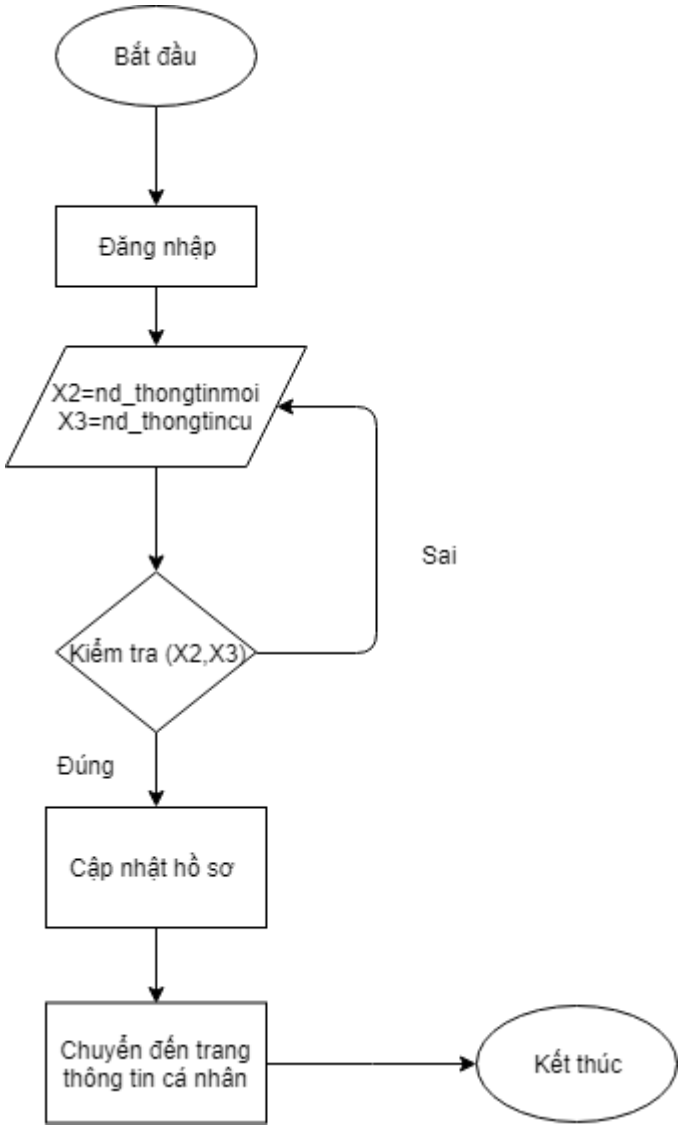
3.2.4. Thao tác dữ liệu.

STT	Loại người dùng	Phương thức	
		Thêm	**Truy vấn**

1	Admin	X	X
2	Tạo bầu chọn	X	X
3	Bầu chọn	X	X

Bảng 3. 4. Các thao tác dữ liệu Cập nhật hồ sơ

3.2.5. Cách xử lý.



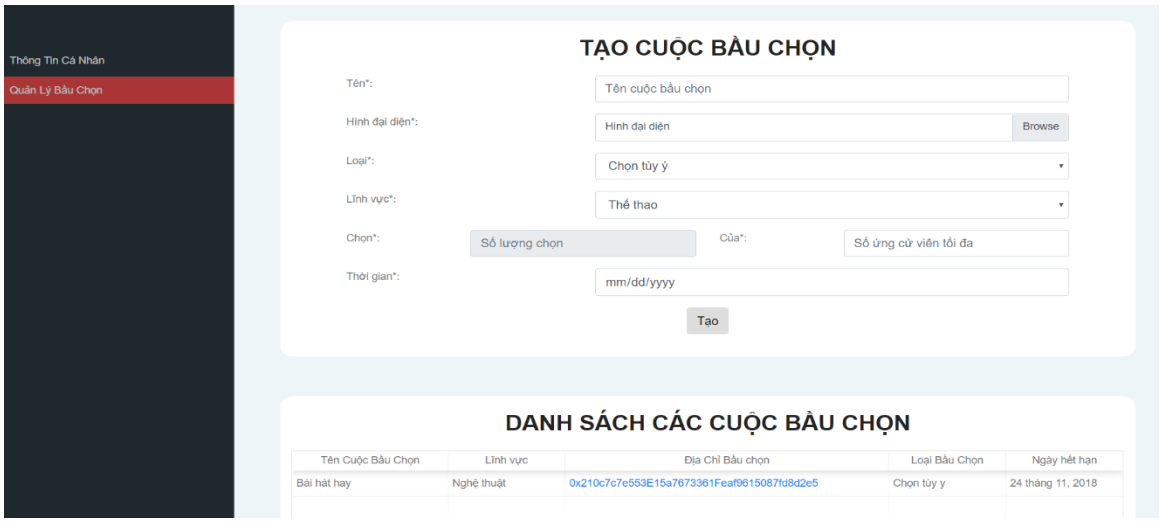
Hình 14. Sơ đồ xử lý cập nhật hồ sơ

3.3. Chức năng Tạo cuộc bầu chọn.

3.3.1. Mục đích.

Nhằm mục đích tạo cuộc bầu chọn, sau đó tạo ứng cử viên.

3.3.2. Giao diện.



Hình 3. 10. Giao diện tạo cuộc bầu chọn

3.3.3. Các thành phần trong giao diện.

STT	Loại điều khiển	Nội dung thực hiện	Giá trị mặc định	Lưu ý
1	Textbox	Tên		Bắt buộc nhập
2	FileInput	Hình đại diện		Bắt buộc nhập
3	Textbox	Loại	Chọn tùy ý	Bắt buộc nhập
4	Textbox	Lĩnh vực	Thể thao	Bắt buộc nhập
5	Textbox	Ứng cử viên tối đa		Bắt buộc nhập
6	Textbox	Thời gian		Bắt buộc nhập
7	Button	Tạo		

Bảng 3. 5. Các thành phần trong giao diện Tạo cuộc bầu chọn

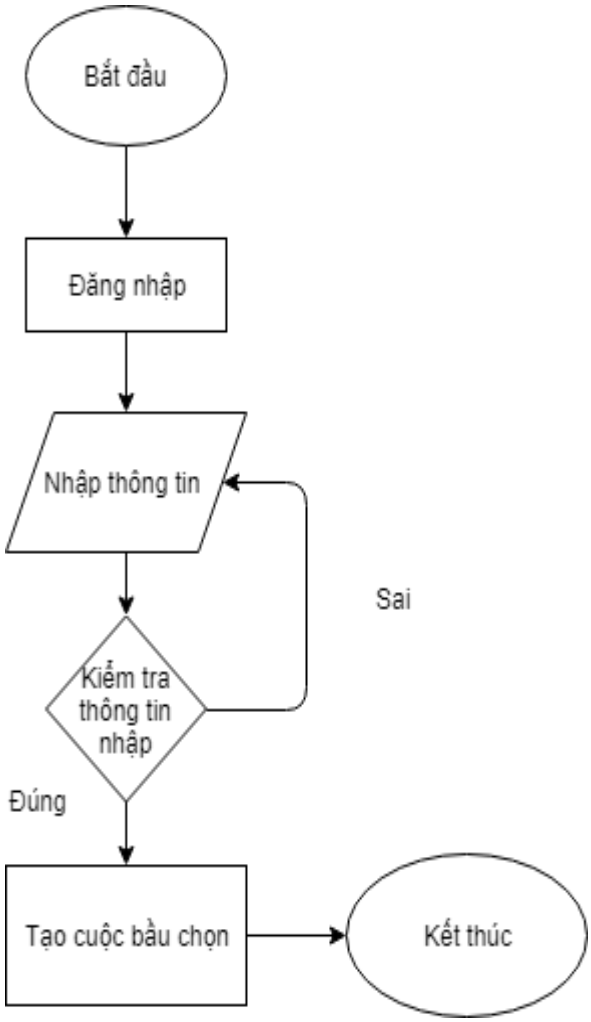
3.3.4. Thao tác dữ liệu.

STT	Loại người dùng	Phương thức	
		Thêm	**Truy vấn**

1	Admin	X	X
2	Tạo bầu chọn	X	X

Bảng 3. 6.Thao tác dữ liệu Tạo cuộc bầu chọn

3.3.5. Cách xử lý.



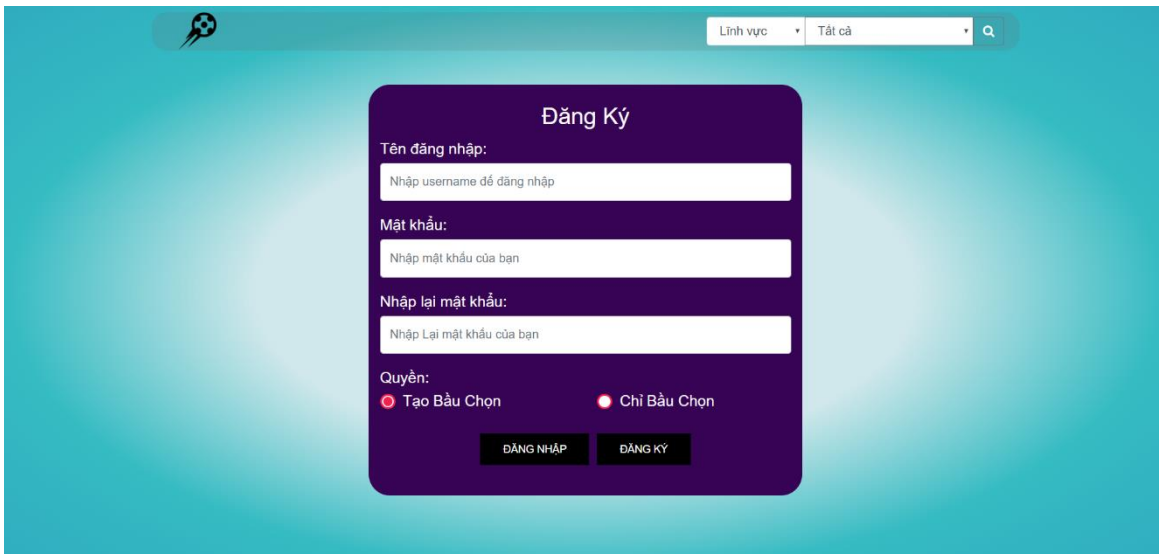
Hình 1. Sơ đồ xử lý Tạo cuộc bầu chọn

3.4. Chức năng Đăng ký.

3.4.1. Mục đích.

Nhằm mục đích đăng ký tài khoản người dùng.

3.4.2. Giao diện.



Hình 3. 11. Giao diện đăng ký

3.4.3. Các thành phần trong giao diện.

STT	Loại điều khiển	Nội dung thực hiện	Giá trị mặc định	Lưu ý
1	Textbox	Tên đăng nhập		Bắt buộc nhập
2	Textbox	mật khẩu		Bắt buộc nhập
3	Textbox	nhập lại mật khẩu		Bắt buộc nhập
4	RadioButton	Tạo bầu chọn		Bắt buộc nhập
5	RadioButton	Chỉ bầu chọn		Bắt buộc nhập
6	Button	Đăng ký		

Bảng 3. 7. Các thành phần trong giao diện Đăng ký

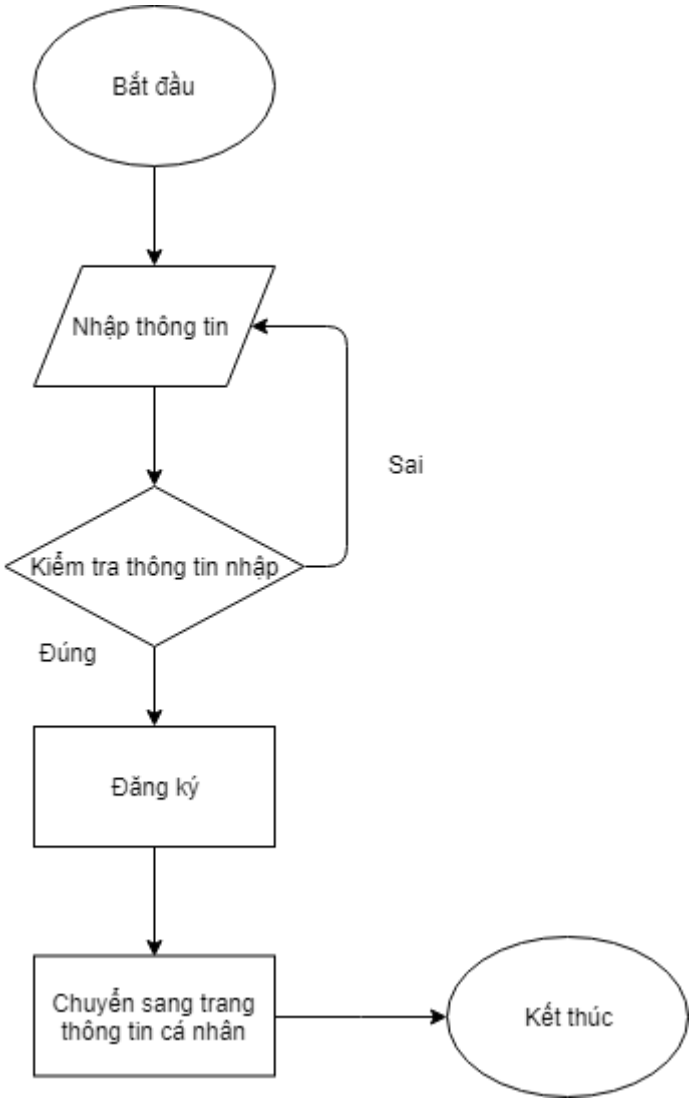
3.4.4. Thao tác dữ liệu.

STT	Loại người dùng	Phương thức	
		Thêm	**Truy vấn**
1	Tạo bầu chọn	X	X

2	Bầu chọn	X	X

Bảng 3. 8. Thao tác dữ liệu Đăng ký

3.4.5. Cách xử lý.



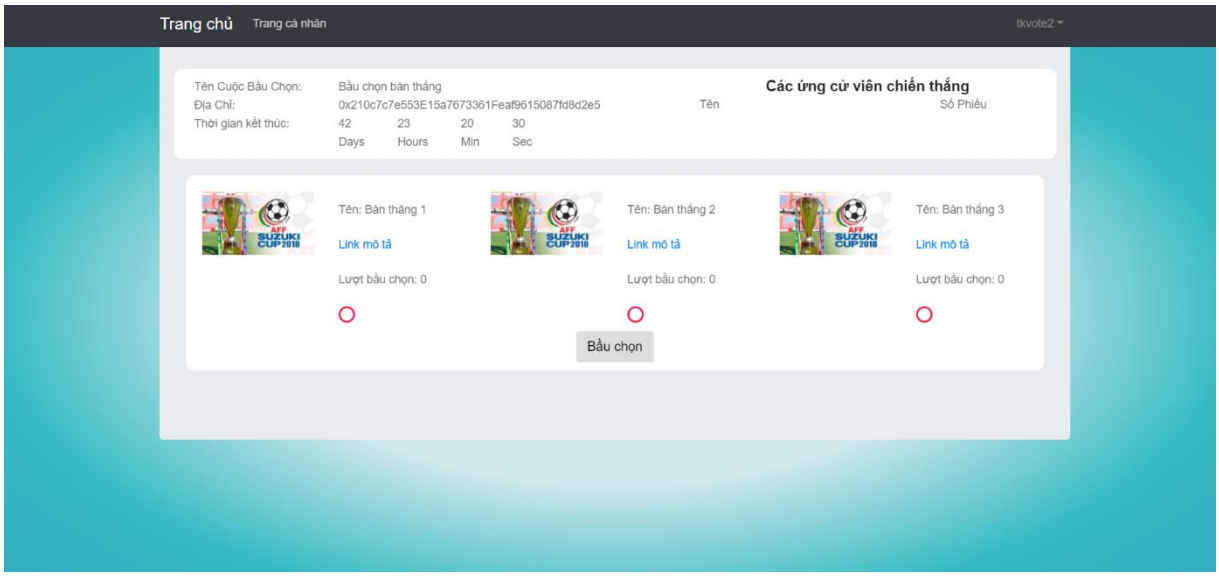
Hình 3. Sơ đồ xử lý Đăng ký

3.5. Chức năng bầu chọn.

3.5.1. Mục đích.

Nhằm mục đích bầu chọn cho ứng cử viên mong muốn.

3.5.2. Giao diện.



Hình 3. 12. Giao diện bầu chọn

3.5.3. Các thành phần trong giao diện.

STT	Loại điều khiển	Nội dung thực hiện	Giá trị mặc định	Lưu ý
1	Checkbox	ứng cử viên		Bắt buộc nhập
2	Button	Bầu chọn		

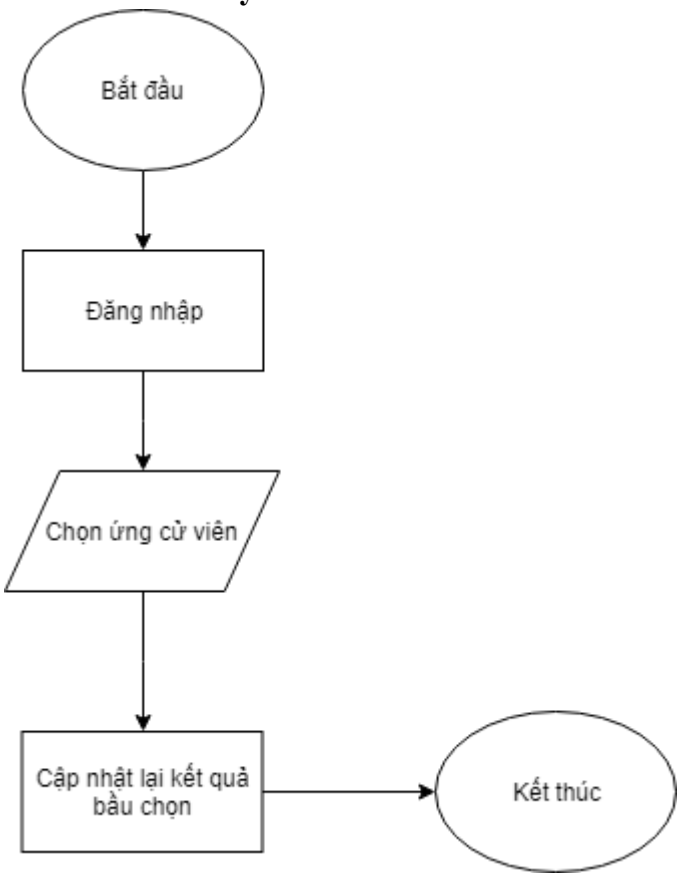
Bảng 3. 9. Các thành phần trong giao diện Bầu chọn

3.5.4. Thao tác dữ liệu.

STT	Loại người dùng	Phương thức	
		Thêm	**Truy vấn**
1	Admin		X
2	Tạo bầu chọn		X
3	Bầu chọn		X

Bảng 3. 10. Thao tác dữ liệu Bầu chọn

3.5.5. Cách xử lý.



Hình 4. Sơ đồ xử lý Bầu chọn

CHƯƠNG 4: ĐÁNH GIÁ VÀ KIỂM THỬ

1. Mục tiêu.

- Nhằm phát hiện lỗi, kiểm tra chương trình có chạy đúng yêu cầu đã được đặc tả hay không.
- Tạo tài liệu cho giai đoạn bảo trì.

2. Chi tiết kế hoạch kiểm thử.

2.1. Các chức năng sẽ kiểm thử.

Các chức năng được kiểm thử gồm các chức năng: đăng ký, đăng nhập, tìm kiếm, tạo cuộc bầu chọn, bầu chọn, cập nhật hồ sơ người dùng, phê duyệt bầu chọn, đổi mật khẩu, xử lý kết quả bầu chọn.

2.2. Các chức năng sẽ không kiểm thử.

Các chức năng không kiểm thử: Lấy danh sách các cuộc bầu chọn, lấy danh sách các ứng cử viên, Lấy danh sách lịch sử bầu chọn.

2.3. Tiêu chí kiểm thử thành công/thất bại.

- Tiêu chí kiểm thử thành công là kết quả kiểm thử đúng với kết quả mong đợi.
- Tiêu chí kiểm thử thất bại là kết quả bị sai lệch với kết quả mong đợi, hệ thống xuất hiện lỗi không biết trước.

2.4. Món bàn giao kiểm thử.

- Tài liệu đặc tả phần mềm.
- Tài liệu thiết kế phần mềm.
- Kế hoạch kiểm thử.
- Thiết kế kiểm thử.
- Dữ liệu nhập, xuất.
- Các trường hợp kiểm thử.
- Các thủ tục kiểm thử.
- Các ghi chú kiểm thử.
- Các báo cáo kiểm thử.

3. Quản lý kiểm thử.

3.1. Các hoạt động / công việc được lập kế hoạch; Sự tiến hành kiểm thử.

- Lập kế hoạch kiểm thử.
- Tạo các testcase
- Tiến hành kiểm thử.

3.2. Môi trường.

- Phần cứng:
  - Bô vi xử lý: Intel Core i5

- Ram 4GB
- Đĩa cứng 500GB

- Phần mềm:
  - Hệ điều hành Windows 10 Home Single Language
  - Server: Ubuntu server 18. 04
  - Geth command line cho mạng blockchain
  - Trình duyệt: Cốc cốc, Chrome.

3.3. Kế hoạch dự đoán và chi phí.

Tên công việc	Thời gian bắt đầu	Thời gian kết thúc
Kiểm thử đăng ký	10h00 ngày 11/11/2018	10h10 ngày 11/11/2018
Kiểm thử đăng nhập	10h10 ngày 11/11/2018	10h20 ngày 11/11/2018
Kiểm thử cập nhật hồ sơ	10h20 ngày 11/11/2018	10h30 ngày 11/11/2018
Kiểm thử đổi mật khẩu	10h30 ngày 11/11/2018	10h40 ngày 11/11/2018
Kiểm thử tạo bầu chọn	10h40 ngày 11/11/2018	11h00 ngày 11/11/2018
Kiểm thử phê duyệt bầu chọn	11h00 ngày 11/11/2018	11h10 ngày 11/11/2018
Kiểm thử bầu chọn	11h10 ngày 11/11/2018	11h20 ngày 11/11/2018
Kiểm thử kết quả bầu chọn	11h00 ngày 13/11/2018	11h01 ngày 13/11/2018

Bảng 4. 1. Kế hoạch dự đoán và chi phí

4. Các trường hợp kiểm thử.

4.1. Chức năng cập nhật hồ sơ.

- Mô tả:
  - Truy cập vào trang thông tin cá nhân.
  - Chọn nút sửa thông tin cá nhân.
  - Nhập thông tin cần sửa.
  - Kiểm tra thông tin nếu đúng sẽ có thông báo “Cập nhật thông tin thành công”. Ngược lại, sẽ có thông báo “Cập nhật thông tin thất bại”.
- Tiền điều kiện:
  Truy cập được vào trang hệ thống bầu chọn, đã có tài khoản và đăng nhập thành công vào trang thông tin cá nhân
- Kịch bản:

STT	Mô tả dữ liệu kiểm thử	Kết quả mong đợi	Kết quả thực tế	Thành công/ Thất bại
1	- Tên đăng nhập: “phat” - Họ và tên: “Cao Vĩnh Phát” - Quyền: Tạo bầu chọn	Thành công	Thành công	Thành công

Bảng 4. 2. Kiểm tra cập nhật hồ sơ

4.2. Chức năng tạo cuộc bầu chọn.

- Mô tả:
  - Truy cập vào trang quản lý bầu chọn với tài khoản có quyền tạo bầu chọn.
  - Nhập các thông tin của cuộc bầu chọn như: tên cuộc bầu chọn, hình đại diện, thể loại, số ứng cử viên, thời gian kết thúc bầu chọn.
  - Sau khi nhập xong nhấn nút tạo
  - Hệ thống sẽ tiến hành tạo cuộc bầu chọn. Sau khi cuộc bầu chọn được tạo một popup tạo ứng cử viên sẽ hiện ra để tiếp tục tạo ứng cử viên. Sau khi nhập đầy đủ thông tin tạo ứng cử viên
- Tiền điều kiện:
  Truy cập được vào trang hệ thống bầu chọn, đã có tài khoản với quyền tạo cuộc bầu chọn và đăng nhập thành công vào trang quản lý bầu chọn
- Kịch bản:

STT	Mô tả dữ liệu kiểm thử	Kết quả mong đợi	Kết quả thực tế	Thành công/ Thất bại

1	- Tên bầu chọn: “Bầu chọn đá quý”.
	- Thời gian: 10/10/2018
	- Lĩnh vực: Khác
	- Loại: Bầu chọn một
	- Ứng viên:
	  - Đá cẩm thạch
	  - Đá kim cương
	  - Đá pha lê
		Thành công	Thành công	Thành công

Bảng 4. 3. Kiểm thử Tạo cuộc bầu chọn

4.3. Chức năng bầu chọn.

- Mô tả:
  - Truy cập vào trang đăng nhập và tiến hành đăng nhập sau đó đến trang danh sách các cuộc bầu chọn.
  - Chọn cuộc bầu chọn "Bầu chọn đá quý".
  - Chọn một ứng cử viên Đá cẩm thạch và nhấn bầu chọn.
- Tiền điều kiện:
  Truy cập được và trang hệ thống bầu chọn và đã có tài khoản.
- Kịch bản:

STT	Mô tả dữ liệu kiểm thử	Kết quả mong đợi	Kết quả thực tế	Thành công/ Thất bại

1	- Tên bầu chọn: "Bầu chọn đá quý".
	- Thời gian: 12/11/2018
	- Lĩnh vực: Khác
	- Loại: Bầu chọn một
	- Ứng viên:
	  - Đá cẩm thạch: số lượt 1
	  - Đá kim cương: số lượt 1
	  - Đá pha lê: số lượt 0
		- Đá cẩm thạch: số lượt 2	- Đá cẩm thạch: số lượt 2	Thành công

Bảng 4. 4. Kiểm thử Bầu chọn

4.4. Phê duyệt bầu chọn.

- Mô tả:
  - Truy cập vào trang đăng nhập tiến hành đăng nhập với tài khoản có quyền admin.
  - Tại tab phê duyệt bầu chọn xem cuộc bầu chọn "Bầu chọn đá quý" và nhấn nút phê duyệt.
- Tiền điều kiện:

Tài khoản người dùng là admin và truy cập được vào hệ thống bầu chọn

- Kịch bản:

STT	Mô tả dữ liệu kiểm thử	Kết quả mong đợi	Kết quả thực tế	Thành công/ Thất bại

1	- Tên bầu chọn: “Bầu chọn đá quý”.
	- Thời gian: 12/11/2018
	- Lĩnh vực: Khác
	- Loại: Bầu chọn một
	- Trạng thái: chờ phê duyệt
	- Ứng viên:
	  - Đá cẩm thạch: số lượt 0
	  - Đá kim cương: số lượt 0
	  - Đá pha lê: số lượt 0
		- Trạng thái: đã phê duyệt	- Trạng thái: đã phê duyệt	Thành công

Bảng 4. 5.Kiểm thửu Phê duyệt bầu chọn

PHẦN KẾT LUẬN.

1. Hệ thống

Hệ thống đã đáp ứng được một số chức năng: tạo bầu chọn, bầu chọn, phê duyệt bầu chọn, tìm kiếm, xem lịch sử bầu...

2. Khả năng ứng dụng

Hệ thống bầu chọn ứng dụng Blockchain Ethereum có thể cho phép người dùng tao ra các cuộc bầu chọn trong thực tế hằng ngày, đảm bảo các cuộc bầu chọn minh bạch với nhiều thể loại khác nhau.

3. Kiến thức đạt được

2.1. Về kiến thức

- Hiểu được kiến thức về Blockchain, ethereum.
- Nâng cao khả năng phân tích thiết kế hệ thống thông tin, khắc phục điểm yếu.
- Bổ sung thêm kiến thức về reactjs, ipfs, sodility , web3js.
- Tiếp thu được khả năng lập trình với mô hình kiến trúc Flux.

b. Về đề tài

- Bước đầu xây dựng thành công hệ thống bầu cử ứng dụng blockchain.
- Xây dựng các chức năng đáp ứng nhu cầu của người dùng.

4. Hạn chế

Không có thời gian nhiều đầu tư vào giao diện, thiết kế smart contract chưa tốt bảo trì và phát triển gặp khó khăn.

5. Hướng phát triển

- Phát triển giao diện thân thiện hơn.
- Cải tiến smartcontract
- Áp dụng hệ thống bầu cử vào nhiều lĩnh vực khác nhau.

TÀI LIỆU THAM KHẢO

Sách.

[1]Mayukh Mukhopadhyay, Ethereum Smart Contract Development.

[2]Josh Thompsons, Blockchain: The Blockchain For Beginners Guide To Blockchain Technology And Leveraging Blockchain Programming.

[3]David Nguyễn, Lưu Thế Lợi, Blockchain và đâu tư ICOS căn bản con đường tới tự do tài chính, NXB Thanh Niên.

Luận văn.

[4]Dr. Iftene Adrian, Báo cáo Blockchain usage in secured voting.

Online.

[5]Blockchain, https://en. wikipedia. org/wiki/Blockchain, lần truy cập gần nhất 25/11/2018.

[6]Tuấn Phong, Blockchain là gì ?, https://quantrimang. com/blockchain-la-gi-bong-bong-hay-cuoc-cach-mang-thuc-su-sau-internet-143099, lần truy cập gần nhất 25/11/2018.

[7]Ethereum, https://en. wikipedia. org/wiki/Ethereum, lần truy cập gần nhất 26/11/2018.

[8]Hyperledger, https://www. hyperledger. org/about, lần truy cập gần nhất 27/11/2018.

[9]Prashant Ram, Setting Up A Private Blockchain, https://hackernoon. com/set-up-a-private-ethereum-blockchain-and-deploy-your-first-solidity-smart-contract-on-the-caa8334c343d, lần truy cập gần nhất 20/10/2018.

[10]Document Web3js, https://web3js. readthedocs. io/en/1. 0/, lần truy cập gần nhất 30/11/2018.

[11]Solidity document, https://solidity. readthedocs. io/en/v0. 4. 25/, truy cập gần nhất ngày 20/11/2018.

[12] Proof of Authority, https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256, truy cập lần gần nhất 06/12/2018