HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Văn Quyết

NGHIÊN CỨU VÀ ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN CHO BẦU CỬ ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KỸ THUẬT

(***Theo định hướng ứng dụng***)

HÀ NỘI - 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Văn Quyết

NGHIÊN CỨU VÀ ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN CHO BẦU CỬ ĐIỆN TỬ

Chuyên ngành: Hệ thống thông tin
Mã số: 8.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT
(*Theo định hướng ứng dụng*)

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. ĐẶNG MINH TUẤN

HÀ NỘI - 2020

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi, kết quả đạt được trong luận văn là sản phẩm của riêng cá nhân, không sao chép lại của người khác. Trong toàn bộ nội dung của luận văn, những điều được trình bày hoặc là của cá nhân hoặc là được tổng hợp từ nhiều nguồn tài liệu. Tất cả các tài liệu tham khảo đều có xuất xứ rõ ràng và được trích dẫn hợp pháp. Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tác giả luận văn

Nguyễn Văn Quyết

LỜI CẢM ƠN

Lời đầu tiên tôi xin gửi lời cảm ơn và lòng biết ơn sâu sắc đến thầy giáo TS.Đặng Minh Tuấn, người đã giúp tôi chọn đề tài, định hình hướng nghiên cứu, tận tình hướng dẫn và chỉ bảo tôi trong suốt quá trình thực hiện luận văn tốt nghiệp.

Tôi xin gửi lời cảm ơn chân thành đến các thầy, cô giáo trong trường Học viện Công nghệ và Bưu chính Viễn thông. Các thầy, cô giáo đã dạy bảo và truyền đạt cho tôi rất nhiều kiến thức, giúp tôi có được một nền tảng kiến thức vững chắc sau những ngày tháng học tập tại trường.

Tôi xin gửi lời cảm ơn chân thành tới các bạn khóa 2018 đợt 1 đã ủng hộ khuyến khích tôi trong suốt quá trình học tập tại trường. Cuối cùng, tôi muốn gửi lời cảm ơn sâu sắc nhất đến gia đình và bạn bè – những người thân yêu luôn kịp thời động viên và giúp đỡ tôi vượt qua những khó khăn trong học tập cũng như trong cuộc sống.

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CÁC CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
API	Application Programing Interface	Giao diện lập trình ứng dụng
CPU	Central Processing Unit	Bộ xử lý trung tâm
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số đường cong Elliptic
e-voting	Electronic voting	Bầu cử điện tử
HĐND		Hội đồng nhân dân
HTTP	Hypertext Transfer Protocal	Giao thức truyền tải siêu văn bản
ID	Identification	Mã số định danh
JSON	JavaScript Object Notation	Một kiểu dữ liệu mở trong JavaScript
P2P	Peer to peer	Mạng ngang hàng
Txid	Transaction identification	Số định danh cho giao dịch

DANH SÁCH BẢNG

DANH SÁCH HÌNH VẼ

LỜI MỞ ĐẦU

1. Lý do chọn đề tài

Bầu cử công khai là một trong những hoạt động nền tảng để xây dựng nên một quốc gia, tổ chức dân chủ, công bằng và minh bạch. Từ trước đến nay, các phương pháp bầu cử đã và đang được áp dụng tại hầu hết các quốc gia là bỏ phiếu dựa trên lá phiếu bằng giấy hay bầu cử trên nền tảng điện tử.

Hệ thống bầu cử bằng giấy là hệ thống được sử dụng rộng rãi trên toàn thế giới từ trước đến nay, tuy nhiên bầu cử theo cách truyền thống này gặp phải rất nhiều hạn chế như: lãng phí tài nguyên giấy; việc triển khai đến các khu vực vùng sâu vùng xa là rất khó khăn và tốn nhiều chi phí; tính an ninh của những lá phiếu trong quá trình vận chuyển và kiểm phiếu chưa thực sự được đảm bảo; cần số lượng lớn nhân lực phục vụ cho cuộc bầu cử… Bằng chứng là trong cuộc bầu cử ngày 17/04/2019 tại Indonesia, đã có ít nhất 92 nhân viên phục vụ bầu cử tử vong do làm việc quá tải và 374 người ngã bệnh vì mệt mỏi [1]. Những hạn chế trên là những thách thức vô cùng lớn của hệ thống bầu cử bằng giấy.

Bầu cử điện tử (e-voting) là một khái niệm không còn xa lạ với các nước phát triển, đặc biệt là Bắc Mỹ và Châu Âu. Tuy nhiên, đây là một khái niệm tương đối mới ở Việt Nam. Bầu cử điện tử đã giải quyết được những hạn chế của phương pháp bầu cử bằng giấy. Bằng việc triển khai một hệ thống bầu cử điện tử, mọi cử tri đều có thể tự tay bỏ những lá phiếu của mình cho dù họ đang ở bất kỳ nơi đâu, tính an ninh của những lá phiếu được đảm bảo hơn do phải vận chuyển những lá phiếu một cách thủ công, bầu cử điện tử cũng giảm được số lượng nhân lực cần thiết để phục vụ cho công tác bầu cử xuống mức tối thiểu. Mặc dù có nhiều tiến bộ hơn hệ thống bầu cử truyền thống, nhưng bầu cử điện tử vẫn còn tồn tại một số hạn chế như: hệ thống máy chủ có thể bị tấn công và cài mã độc phá hỏng kết quả bầu cử; kết quả của phiếu bầu vẫn có thể bị thay đổi nếu có người cố tình can thiệp.

Vài năm trở lại đây, công nghệ blockchain (khối chuỗi) nổi lên như một hiện tượng công nghệ với các tính năng ưu việt được dự đoán có thể làm thay đổi cuộc sống của chúng ta. Đề tài **"Nghiên cứu và ứng dụng công nghệ blockchain cho bầu cử điện tử"** nhằm giải quyết sự sai lệch dữ liệu cũng như khả năng bị tấn công phá hỏng kết quả của hệ thống bầu cử điện tử cũ.

2. Cấu trúc của luận văn

Luận văn gồm 3 chương:

- Chương 1: Tổng quan về bầu cử và bầu cử điện tử
- Chương 2: Blockchain và bầu cử điện tử
- Chương 3: Thử nghiệm và kết quả

Trong đó, luận văn tập trung vào chương 2 và chương 3 với mục đích nghiên cứu mô hình ứng dụng công nghệ blockchain cho bầu cử điện tử, sau đó thực hiện các thử nghiệm nhằm đánh giá mô hình này.

CHƯƠNG 1: TỔNG QUAN VỀ BẦU CỬ VÀ BẦU CỬ ĐIỆN TỬ

1.1. Giới thiệu chung về bầu cử và bầu cử tại Việt Nam

1.1.1. Giới thiệu chung về bầu cử

a. Bầu cử là gì

Bầu cử là việc lựa chọn một hoặc nhiều người cho một chức vụ công hoặc tư, từ nhiều ứng cử viên khác nhau. Không chỉ liên quan đến bộ máy nhà nước, bầu cử còn được sử dụng trong tổ chức, hoạt động của các tổ chức xã hội (ví dụ như trong một lớp học, trong một tổ chức công đoàn).

Việc bầu cử thành lập cơ quan hoặc một chức danh công quyền được điều chỉnh bởi hiến pháp và pháp luật do nhà nước ban hành. Thông thường Quốc hội (Nghị viện), các cơ quan đại diện của chính quyền địa phương được thành lập bằng cách tổ chức bầu cử. Ở một số nước, các vị trí, cơ quan nhà nước khác như tổng thống, thống đốc tiểu bang, thị trưởng thành phố... cũng được thành lập thông qua bầu cử.

Các cuộc bầu cử định kỳ là phương tiện kiểm soát thiết yếu của công chúng đối với chính quyền. Bầu cử là để khẳng định quyền lực chính trị xuất phát từ nhân dân và buộc các chính trị gia phải chịu trách nhiệm trước nhân dân về hành vi của mình.

Bầu cử là sự lựa chọn (từ gốc tiếng Latinh eligere - lựa chọn). Thông qua đó các công dân chọn người, chọn đảng để ủy quyền, chọn chính sách để giải quyết các vấn đề của một xã hội, để mang lại hạnh phúc cho cá nhân và cộng đồng. Bầu cử sẽ mất đi ý nghĩa nếu không có sự tự do lựa chọn [2].

b. Vai trò của bầu cử

Bầu cử là phương tiện dân chủ để công dân lựa chọn trong số các ứng cử viên cho vị trí nhất định trong bộ máy nhà nước và trao quyền cho người được bầu hành động nhân danh công chúng trong nhiệm kỳ được bầu.

c. Chức năng của bầu cử

Bầu cử có ý nghĩa quan trọng đối với nhà nước, xã hội và các thành viên của cộng đồng, bởi nó có các chức năng thường được nhắc đến như sau [2]:

- Xác định tính chính đáng của các cơ quan quyền lực nhà nước: cho thấy cơ quan nhà nước, vị trí lãnh đạo được người dân ủng hộ;
- Giúp người dân thực hiện sự ủy quyền và lựa chọn người cầm quyền: nhân dân, chủ thể của quyền lực trong chế độ dân chủ, ủy quyền cho người mà mình tin tưởng sẽ hoạt động nhằm bảo vệ các lợi ích của mình và xã hội;
- Giúp giới tinh hoa, các chính trị gia củng cố quyền lực: người lãnh đạo hợp pháp hóa quyền lực của mình;
- Chống lại sự lộng hành của chính quyền: bảo đảm để người không giữ đúng lời hứa, không có năng lực, làm việc kém hoặc tham nhũng sẽ không thể tiếp tục duy trì quyền lực và bị loại khỏi vị trí;
- Tạo diễn đàn giữa các khuynh hướng chính trị: các đường lối, chính sách khác nhau, thậm chí trái ngược nhau, được trình bày, thảo luận;
- Truyền thông chính trị: thông tin hai chiều giữa các ứng cử viên và công chúng, các cơ quan nhà nước hiểu thêm về các nhu cầu của cử tri, các vấn đề của xã hội, các giải pháp có thể xem xét lựa chọn.

1.1.2. Thực trạng bầu cử tại Việt Nam

a. Bầu cử ở Việt Nam

Thuật ngữ bầu cử ở Việt Nam được cho là gắn kết mật thiết với khái niệm dân chủ, trong đó những cuộc bầu cử tự do và công bằng là phương thức bảo đảm cho việc tôn trọng các quyền tự do, dân chủ đó. Trong một nền dân chủ, quyền lực của Nhà nước chỉ được thực thi khi có sự nhất trí của người dân (người bị quản lý). Cơ chế căn bản để chuyển sự nhất trí đó thành quyền lực nhà nước là tổ chức bầu cử tự do và công bằng.

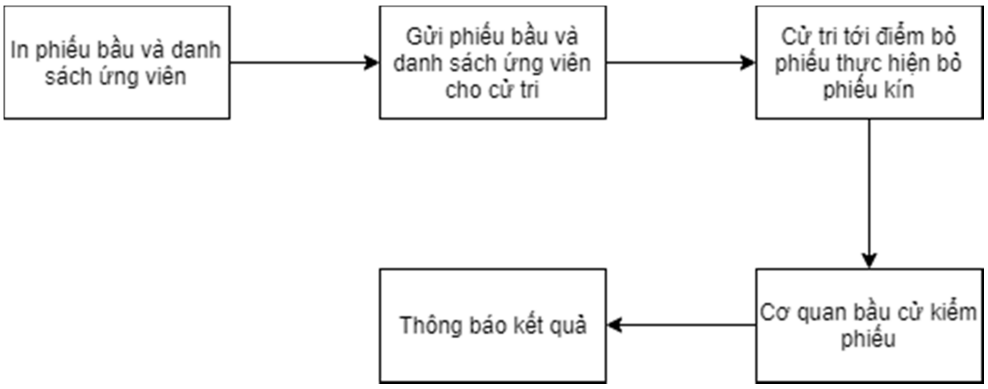
b. Các nguyên tắc bầu cử

Ở Việt Nam, các nguyên tắc bầu cử dân chủ được kế thừa, bổ sung và phát triển để làm một căn cứ thực hiện một chế độ bầu cử mới thực sự dân chủ. Các nguyên tắc bầu cử theo quy định của pháp luật gồm bốn nguyên tắc, đó là [3]:

- Nguyên tắc phổ thông đầu phiếu: đây là nguyên tắc rất quan trọng được khẳng định tại Điều 7 Hiến pháp năm 2013. Theo đó, công dân đủ mười tám tuổi trở lên có quyền bầu cử và đủ hai mươi mốt tuổi trở lên có quyền ứng cử vào Quốc hội và HĐND các cấp. Nguyên tắc này nhằm bảo đảm cho tất cả công dân, không phân biệt thành phần dân tộc, tín ngưỡng, địa vị xã hội, giới tính đều có quyền bầu cử.
- Nguyên tắc bình đẳng: được thể hiện ở một số khía cạnh, như mỗi cử tri không phân biệt đều có số lần bỏ phiếu như nhau, giá trị lá phiếu của mỗi cử tri đều như nhau, số lượng dân cư như nhau thì bầu được số lượng đại biểu bằng nhau.
- Nguyên tắc trực tiếp: nguyên tắc này nhằm bảo đảm cho người dân trực tiếp thể hiện ý chí của mình trong lựa chọn người đại biểu. Cụ thể: cử tri được trực tiếp bỏ phiếu vào thùng phiếu mà không qua người trung gian, cử tri cũng trực tiếp lựa chọn người mình bỏ phiếu, không được nhờ người khác bầu hộ, không bầu bằng cách thức gửi thư.
- Nguyên tắc bỏ phiếu kín: nguyên tắc này nhằm bảo đảm tôn trọng quyền tự do thể hiện ý chí của cử tri, tạo điều kiện để quá trình lựa chọn của mỗi cử tri không bị tác động, ảnh hưởng của các cá nhân khác hoặc tổ chức.

1.2. Giới thiệu về bầu cử truyền thống

1.2.1. Mô hình triển khai



Hình 1.1: Mô hình triển khai bầu cử truyền thống

1.2.2. Ưu nhược điểm của mô hình bầu cử truyền thống

a. Ưu điểm

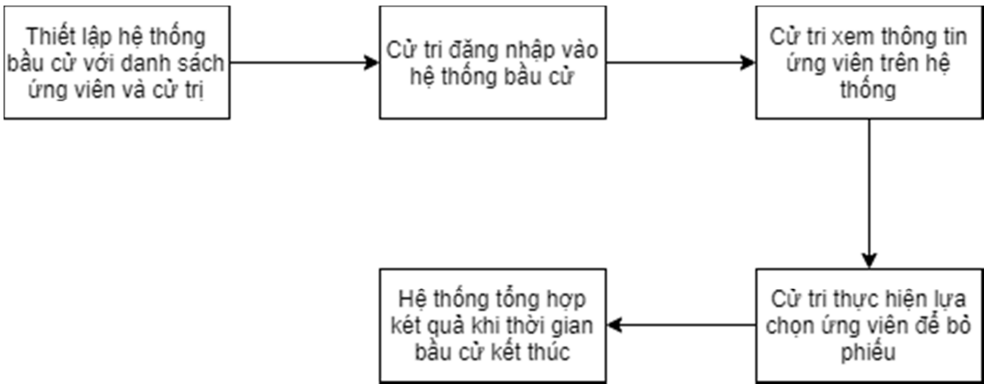
- Không lo sợ việc bị hacker tấn công, do sử dụng phiếu bầu bằng giấy.
- Các lá phiếu bằng giấy rất thân thiện và dễ hiểu, vì vậy không đòi hỏi cử tri phải có kiến thức về công nghệ.
- Không lo sợ các sự cố về điện hoặc mạng internet trong quá trình diễn ra bầu cử.

b. Nhược điểm

- Cần phải in rất nhiều phiếu bầu, gây lãng phí tài nguyên giấy và ảnh hưởng tiêu cực đến môi trường.
- Tốn thời gian trong việc phát phiếu bầu và ký tên hoặc đóng dấu vào phiếu bầu.
- Phiếu bầu có thể bị giả mạo bằng cách giả mạo chữ ký hoặc làm giả con dấu.
- Việc triển khai đến các khu vực vùng sâu vùng xa là rất khó khăn và tốn nhiều chi phí.
- Tính an ninh của những lá phiếu trong quá trình vận chuyển và kiểm phiếu chưa thực sự được đảm bảo.
- Cần số lượng lớn nhân lực phục vụ cho cuộc bầu cử.

1.3. Giới thiệu về bầu cử điện tử

1.3.1. Mô hình triển khai



Hình 1.2: Mô hình triển khai bầu cử điện tử

1.3.2. Ưu nhược điểm của mô hình bầu cử điện tử

a. Ưu điểm

- Dễ dàng trong việc tổng hợp kết quả. Bầu cử điện tử có thể cho kết quả trong vài giờ, vài phút hoặc một số hệ thống có thể đưa ra kết quả theo thời gian thực.
- Dễ dàng trong việc bầu cử. Cử tri có thể thực hiện bầu cử ở bất kỳ đâu thông qua thiết bị có kết nối internet như máy tính, điện thoại…
- Tiết kiệm thời gian. Việc tạo ra số lượng lớn phiếu bầu điện tử chỉ mất một vài phút.
- Cử tri có thể kiểm tra được phiếu bầu của họ đã thành công hay chưa
- Giảm thiểu số lượng phiếu bầu không hợp lệ do hệ thống sẽ từ chối những phiếu bầu này.

b. Nhược điểm

- Hệ thống máy chủ có thể bị tấn công, cài các phần mềm mã độc để phá hoại kết quả bầu cử.
- Cử tri cần có một chút kiến thức về công nghệ.
- Cần chuẩn bị các phương án dự phòng về sự cố điện hoặc sự cố mạng internet.

1.4. Kết luận chương

Chương này đã giới thiệu khái quát về bầu cử nói chung và bầu cử tại Việt Nam nói riêng. Đồng thời, chương cũng đã trình bày mô hình, ưu và nhược điểm của phương pháp bầu cử truyền thống cũng như bầu cử điện tử. Từ đó, là tiền đề để đưa ra đề xuất ứng dụng công nghệ blockchain cho bầu cử điện tử. Phần này sẽ được trình bày chi tiết hơn trong nội dung của chương 2 và chương 3.

CHƯƠNG 2: BLOCKCHAIN VÀ BẦU CỬ ĐIỆN TỬ

2.1. Giới thiệu về công nghệ blockchain

2.1.1. Khái niệm

a. Khái niệm

Blockchain (chuỗi khối), tên ban đầu block chain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã băm (hash) và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới 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 hoặc phải tốn rất nhiều tài nguyên tính toán.

Blockchain được đảm bảo nhờ cách thiết kế sử dụng hệ thống tính toán phân cấp với khả năng chịu lỗi cao. Vì vậy sự đồng thuận phân cấp có thể đạt được nhờ Blockchain. Vì vậy Blockchain phù hợp để ghi lại những sự kiện, hồ sơ y tế, xử lý giao dịch, công chứng, danh tính và chứng minh nguồn gốc. Việc này có tiềm năng giúp xóa bỏ các hậu quả lớn khi dữ liệu bị thay đổi trong bối cảnh thương mại toàn cầu [4].

Blockchain đầu tiên được phát minh và thiết kế bởi Satoshi Nakamoto vào năm 2008 và được hiện thực hóa vào năm sau đó như là một phần cốt lõi của Bitcoin, khi công nghệ blockchain đóng vai trò như là một cuốn sổ cái cho tất cả các giao dịch. Qua việc sử dụng mạng lưới ngang hàng và một hệ thống dữ liệu phân cấp, Bitcoin blockchain được quản lý tự động. Việc phát minh ra blockchain cho Bitcoin đã làm cho nó trở thành loại tiền tệ kỹ thuật số đầu tiên giải quyết được vấn đề double spending (chi tiêu gian lận khi 1 lượng tiền được dùng 2 lần). Công nghệ này của Bitcoin đã trở thành nguồn cảm hứng cho một loạt các ứng dụng khác[5].

b. Các loại blockchain

Các loại blockchain có thể chia thành ba loại theo nguyên tắc về quyền đọc ghi dữ liệu và tham gia vào hệ thống: Public (công khai); Private (riêng tư); và Consortium (được phép). Với kiểu public, bất kỳ ai cũng có thể đọc và ghi dữ liệu trên blockchain, ví dụ về các ứng dụng đồng tiền ảo Bitcoin, Ethereum... Với kiểu private, người dùng chỉ có quyền đọc không có quyền ghi dữ liệu vào blockchain, chỉ có một bên thứ ba tin cậy được quyền ghi, ví dụ Ripple. Còn với kiểu Consortium bổ sung thêm sự kết hợp giữa bên thứ ba khi tham gia vào public hay private, ví dụ như các ngân hàng hay tổ chức tài chính liên doanh sử dụng blockchain cho riêng mình [6].

c. Đặc điểm chính của blockchain

- Không thế làm giả, không thế phá hủy các chuỗi blockchain: Theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã blockchain và công nghệ blockchain biến mất khi không còn Internet trên toàn cầu.
- Bất biến: Dữ liệu trong blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.
- Bảo mật: Các thông tin, dữ liệu trong blockchain được phân tán và an toàn tuyệt đối.
- Minh bạch: Ai cũng có thể theo dõi dữ liệu blockchain đi 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 hợp đồng kỹ thuật số được nhúng vào đoạn code if-this-then-that (IFTTT), cho phép chúng tự thực thi mà không cần bên thứ ba. Cụ thể, Hợp đồng thông minh thực ra chỉ là một chương trình nhỏ được lưu trữ trong một blockchain, Hợp đồng này được lập cho những người hỗ trợ (supporters) chuyển tiền cho nhóm dự án tạo sản phẩm họ kỳ vọng. Họ sẽ chuyển tiền vào dự án qua hợp đồng thông minh và hợp đồng này tự động chuyển tiền đến những người thực hiện. Khi dự án đến đích, tức kết thúc thì tiền sẽ tự động chuyển trở lại cho các người hỗ trợ. Hợp đồng thông minh còn có thể sử dụng trong việc tự động cung cấp các khoản vay cho khách hàng của các ngân hàng, trong quá trình thực hiện yêu cầu cầu của các công

ty bảo hiểm hay trong các công ty phân phối và thanh toán. Trong việc này Ethereum là hệ thống đặc biệt được tạo ra và thiết kế cho việc hỗ trợ hợp đồng thông minh trên ngôn ngữ lập trình Solidity [7].

2.1.2. Cơ cở lý thuyết và nguyên tắc hoạt động của blockchain

a. Cơ sở lý thuyết

- Hàm băm (Hash function)

Hàm băm (hash function) là một giải thuật dùng để ánh xạ dữ liệu từ một kích thước bất kỳ sang một giá trị băm có kích thước cố định (Tùy thuộc vào thuật toán sử dụng. Hàm băm là hàm một chiều (one way function), theo đó với mỗi giá trị đầu vào có thể dễ dàng tính ra giá trị băm nhưng không thể làm theo chiều ngược lại [8].

Ngoài ra, hàm băm **h** thỏa mãn các tính chất sau

- Với dữ liệu đầu vào **x**, chỉ thu được giá trị đầu ra duy nhất **h(x)**.
- Nếu giá trị đầu vào **x** bị thay đổi (cho dù chỉ thay đổi 1 bit), ta luôn có **h(x') ≠ h(x)**

Trên thế giới có rất nhiều hàm băm với các thuật toán và tính chất khác nhau. Dưới đây là bảng so sánh một số thuật toán băm

Bảng 2.1*:* **So sánh một số thuật toán băm** [9]

Thuật toán	**Kích thước đầu ra**	**Kích thước khối (block)**	**Xung đột (Collision)**
MD2	128	128	Có
MD4	128	512	Có
MD5	128	512	Có
RIPEMD	128	512	Có
SHA	160	512	Có
SHA-256	256	512	Xác suất rất nhỏ

SHA-512	512	1024	Xác suất rất nhỏ

Thuật toán MD5 được sử dụng rộng rãi cho mục đích băm và nó cung cấp giá trị băm dài 128 bit. MD5 là thuật toán mới nhất trong loạt MD (MD2, MD4, MD5). Thuật toán được thiết kế để sử dụng như một thuật toán băm mật mã nhưng nó phải đối mặt với một số lỗ hổng và khả năng xung đột. Sau đó, RIPEMD là một nhóm hàm băm được phát triển bởi Hans Dobbertin vào năm 1996. Thuật toán này được thiết kế để thay thế MD5 như một sự thay thế an toàn hơn. Nó có một vài biến thể đã xuất hiện theo thời gian bao gồm RIPEMD-128, RIPEMD-160, RIPEMD256 và RIPEMD-320, tuy nhiên nó vẫn xuất hiện lỗ hổng về xung đột.

SHA (Secure Hashing Algorithm) là một loại hàm băm khác. Hàm băm mang lại giá trị băm 160 bit. Thuật toán vẫn không thể chống lại các cuộc tấn công xung đột (collision attack). Trong thời gian này, một số thuật toán mới cũng đã được đề xuất, bao gồm SHA-256 và SHA-512, cho đến thời điểm hiện tại, hai thuật toán này được coi là an toàn và không có xung đột.

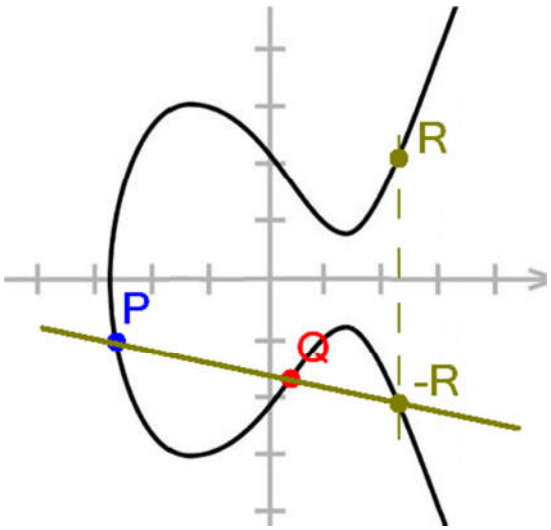
SHA-256 là thuật toán băm được sử dụng trong công nghệ blockchain.

- Chữ ký số và Hệ mật đường cong elliptic (ECDSA)

Chữ ký số là một thông điệp dữ liệu đã được mã hóa gắn kèm theo một thông điệp dữ liệu khác nhằm xác thực người gửi thông điệp đó. Quá trình ký và xác nhận chữ ký như sau: Người gửi muốn gửi thông điệp cho bên khác thì sẽ dùng một hàm băm, băm thông điệp gốc thành một "thông điệp tóm tắt" (Message Digest), thuật toán này được gọi là thuật toán rút gọn (hash function). Người gửi mã hoá bản tóm tắt thông điệp bằng khóa bí mật của mình (sử dụng phần mềm bí mật được cơ quan chứng thực cấp) để tạo thành một chữ ký số. Sau đó, người gửi tiếp tục gắn kèm chữ ký số này với thông điệp dữ liệu ban đầu. Sau đó gửi thông điệp đã kèm với chữ ký một cách an toàn qua mạng cho người nhận. Sau khi nhận được, người nhận sẽ dùng khoá công khai của người gửi để giải mã chữ ký số thành bản tóm tắt thông

điệp. Người nhận cũng dùng hàm băm giống hệt như người gửi đã làm đối với thông điệp nhận được để biến đổi thông điệp nhận được thành một bản tóm tắt thông điệp. Người nhận so sánh hai bản tóm tắt thông điệp này, nếu chúng giống nhau tức là chữ ký đó là xác thực và thông điệp đã không bị thay đổi trên đường truyền đi.

Hệ mật đường cong elliptic là phương trình có dạng: $y^2 = x^3 + Ax + B$, với đồ thị là đường cong đối xứng qua trục x như sau [8]:



Hình 2.1: Đồ thị hệ mật đường cong elliptic

Hệ mật đường cong elliptic có một số tính chất sau:

- Nếu hai điểm $P_1(x_1, y_1)$ và $P_2(x_2, y_2)$ với $x_1 \neq x_2$ nằm trên cùng một đường cong elliptic E, thì đường thẳng qua hai điểm P_1 và P_2 sẽ cắt một điểm duy nhất $P_3(x_3, y_3)$ có thể xác định thông qua P_1, P_2 nằm trên đường cong E.
- Tiếp tuyến của đường cong tại điểm bất kỳ P(x, y) trên đường cong E cũng cắt đường cong E tại một điểm duy nhất nằm trên đường cong E, điểm này cũng có thể xác định được thông qua P.

- Phép cộng: Giả sử $P(x_1, y_1)$ và $Q(x_2, y_2)$ là hai điểm của E. Nếu $x_1=x_2$ và $y_1=-y_2$ thì ta định nghĩ P + Q = *O*. Ngược lại thì P + Q = (x_3, y_3) thuộc E với $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1-x_3) - y_1$
- Phép nhân: Phép nhân một số nguyên k với một điểm P thuộc E là điểm Q được xác định bằng cách cộng k lần điểm P và dĩ nhiên Q thuộc E: k x P = P + P + … + P (k phép cộng điểm P). Vì vậy, nếu G là một điểm thuộc đường cong elliptic E thì với mỗi số nguyên dương k luôn dễ dàng xác định được điểm Q = k x G.

Dựa vào những tính chất đó người ta đã nghiên cứu và chỉ ra rằng các hệ mã hóa bằng đường con elliptic có độ bảo mật cao hơn nhiều lần so với hệ mã hóa công khai RSA. Trong blockchain (cụ thể là bitcoin), hệ mật đường cong elliptic được áp dụng như sau [10]:

- Phương trình E: $y^2 = x^3 + 7$
- Số P cơ sở, P=55066263022277343669578718895168534326250603453777594175500187360389116729240, 32670510020758816978083085130507043184471273380659243275938904335757337482424
- Khóa công khai Q được tạo ra từ khóa bí mật d theo công thức Q = dP
- Private key được tạo ra từ số ngẫu nhiên 256 bit (được sinh ngẫu nhiên)
- Biết Q và P, bài toán tìm d là bài toán cực khó và được gọi là bài toán logarit rời rạc trên E
- Chữ ký số ECDSA
  - Hình thành chữ ký số:

    Thuật toán chữ ký số ECDSA được dùng trong Bitcoin, với văn bản *m* tính giá trị băm *e = SHA256(m)*

    1. Chọn 1 số ngẫu nhiên lớn 256 bit gọi là k.
    2. Tính điểm $R(x_R, y_R) = kP(x_P, y_P)$, và chọn $r = x_R$.

3. Tính giá trị $s = (e + dr)k^{-1} \, mod \, p$. Chữ ký số của văn bản m sẽ là cặp giá trị (r, s). Chữ ký số sẽ gồm 2 số 256 bit (Tổng cộng là 512 bit).

- Xác thực chữ ký số:
  1. Tính giá trị băm của văn bản m': $e' = SHA256(m')$.
  2. Xác thực bằng cách tính điểm $V(x_V, y_V) = s^{-1}eP + s^{-1}rQ$, nếu $r = x_V$ thì chữ ký số hợp lệ (lưu ý khi tính các giá trị số cần phải lấy phần dư $mod \, p$
- Chứng minh tính đúng đắn:
  $V = s^{-1}eP + s^{-1}rQ = s^{-1}(e + dr)P = kP = R$, vậy $V = R$ nên $x_R = x_V = r$ chỉ thỏa mãn khi $e' = e$.

- Mạng ngang hang (peer-to-peer)

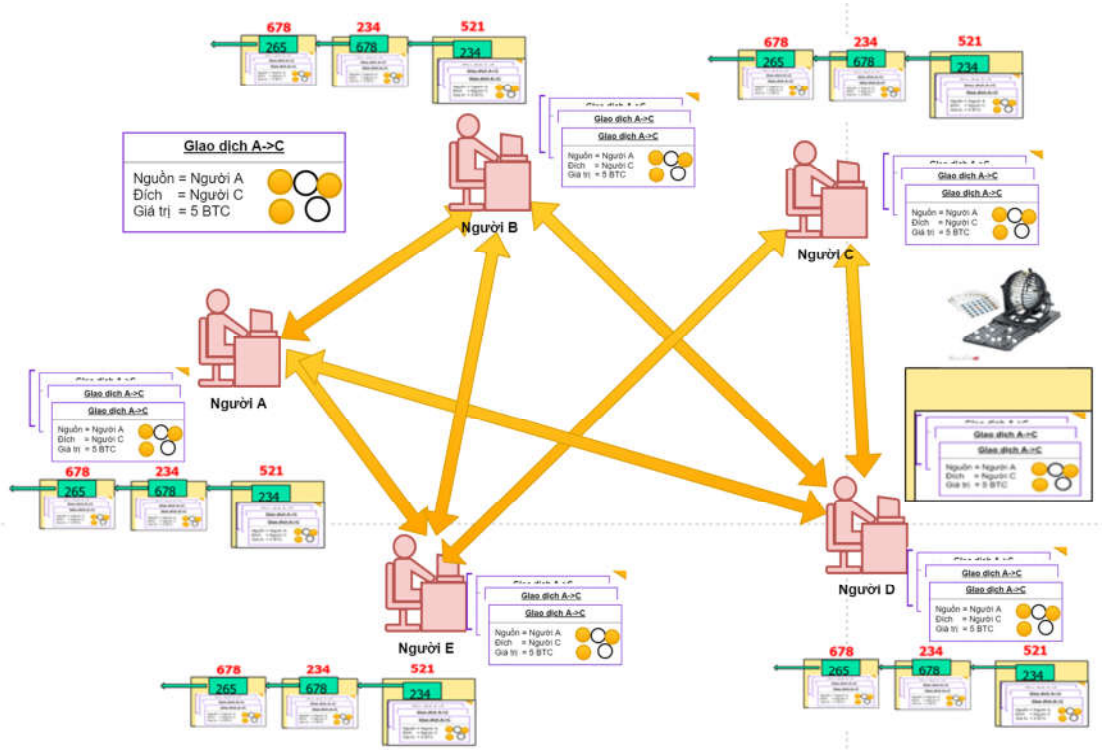
Mạng ngang hàng, hay mạng đồng đẳng (P2P) bao gồm một nhóm các thiết bị cùng lưu trữ và chia sẻ tập tin. Mỗi người tham gia (nút) hoạt động như một đồng đẳng riêng lẻ. Thông thường, tất cả các nút có sức mạnh như nhau và thực hiện các nhiệm vụ giống nhau.

Về bản chất, hệ thống ngang hàng được duy trì bởi một mạng lưới người dùng phân tán. Mạng này thường không có quản trị viên trung tâm hoặc máy chủ vì mỗi nút lưu trữ một bản sao của các tệp và mỗi nút đóng vai trò như một máy khách và máy chủ cho các nút khác. Do đó, mỗi nút có thể tải tệp về từ các nút khác hoặc tải lên tệp cho các nút khác. Đây là điểm khác biệt giữa các mạng ngang hàng với các hệ thống máy chủ-máy khách truyền thống hơn, trong đó các thiết bị máy khách tải xuống các tệp từ một máy chủ tập trung.

Trong giai đoạn đầu của Bitcoin, Satoshi Nakamoto định nghĩa nó là một "Hệ thống tiền mặt điện tử ngang hàng" Bitcoin ban đầu được tạo ra như một dạng tiền kỹ thuật số. Nó có thể được chuyển từ người dùng này sang người dùng khác thông qua mạng ngang hàng, mạng này quản lý một cuốn sổ cái phân tán được gọi là chuỗi khối (blockchain). Trong bối cảnh này, chính kiến trúc ngang hàng, một

công nghệ trung tâm của blockchain cho phép người dùng có thể giao dịch Bitcoin và các loại tiền mã hóa khác trên toàn thế giới mà không cần đến trung gian cũng như bất kỳ máy chủ trung tâm nào. Ngoài ra, bất kỳ ai cũng có thể trở thành một nút trên mạng Bitcoin nếu họ muốn tham gia vào quá trình xác minh và xác thực các khối.

b. Nguyên tắc hoạt động



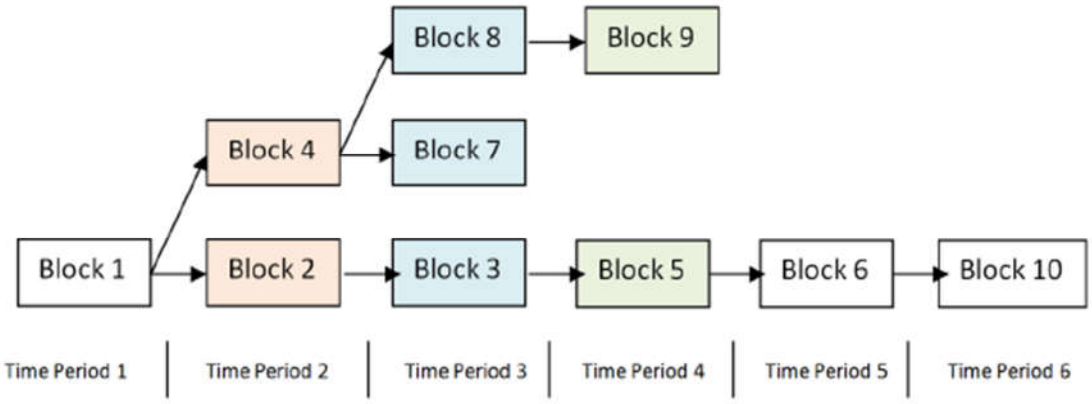
Hình 2.2: Nguyên lý hoạt động của mạng blockchain [10]

Các bước hoạt động trong mạng blockchain được mô tả như sau:

1. Giao dịch (transaction) mới được thông báo (broadcast) tới tất cả các nút.
2. Mỗi nút sẽ tập hợp những giao dịch mới vào 1 khối (block).
3. Mỗi nút sẽ đi tìm giá trị "nonce" phù hợp cho block để có giá trị băm thỏa mãn điều kiện của blockchain (số ký tự 0 ban đầu là x (được gọi là "difficulty")). Công việc này được gọi là bằng chứng công việc (proof-of-work).

4. Khi một nút đã tìm được số "nonce" cho block, nó sẽ thông báo tới tất cả các nút còn lại.
5. Các nút sẽ chấp thuận một block mới khi và chỉ khi tất cả các giao dịch trong block là chính xác và chưa thực hiện.
6. Khối mới được tạo ra bằng cách sử dụng mã băm của khối liền trước và mã băm của các giao dịch trong block. Đồng thời mã băm của block mới này cũng được sử dụng block liền sau của nó.

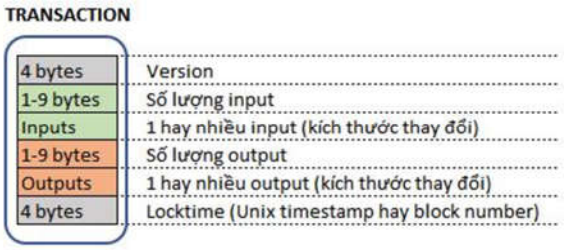
Các nút luôn coi chuỗi dài nhất là chuỗi chính xác và sẽ tiếp tục mở rộng chuỗi này. Nếu hai nút thông báo (broadcast) đồng thời các phiên bản khác nhau của block tiếp theo, một số nút có thể nhận được các block khác nhau. Trong trường hợp này, các nút sẽ làm việc trên nhánh đầu tiên nó nhận được, nhưng lưu lại nhánh còn lại trong trường hợp nó trở nên dài hơn. Việc rẽ nhánh này sẽ bị phá vỡ khi bằng chứng công việc tiếp theo được tìm thấy và một nhánh trở nên dài hơn, các nút đang làm việc trên nhánh khác sau đó sẽ chuyển sang nhánh dài hơn và các giao dịch của nhánh cụt sẽ được các nút tính toán lại và đưa vào nhánh dài.



Hình 2.3: Rẽ nhánh trong blockchain [11]

Giao dịch mới không nhất thiết phải đến tất cả các nút. Miễn là chúng đến được nhiều nút nhất có thể, chúng sẽ được đưa vào một block trước đó rất lâu. Block cũng như vậy, nếu một nút không nhận được một block, nó sẽ yêu cầu block này khi nhận được block tiếp theo và nhận ra nó đã bỏ lỡ một block [5].

- Giao dịch (Transaction)



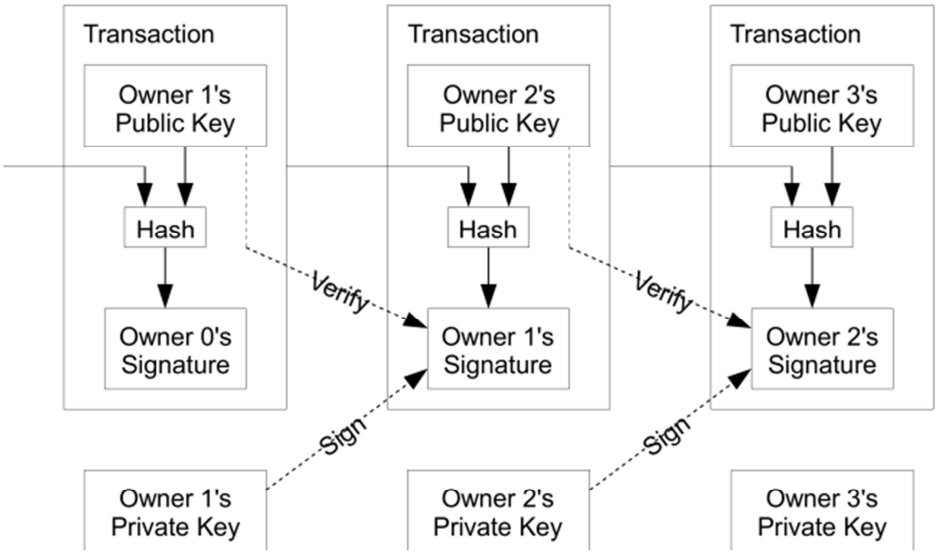
Hình 2.4: Các thành phần của transaction [10]

Một transaction chứa 6 thành phần cơ bản như sau:

Bảng 2.2: Các thành phần của giao dịch

Trường	**Mô tả**	**Kiểu dữ liệu**
Version	Định nghĩa version của giao dịch	Kiểu số
NumberOfInputs	Số lượng phần tử trong dữ liệu đầu vào	Kiểu số
CollectionOfInputs	Dữ liệu đầu vào (một hoặc nhiều)	Tập các véc tơ
NumberOfOutputs	Số lượng phần tử trong dữ liệu đầu ra	Kiểu số
CollectionOfOutputs	Dữ liệu đầu ra (một hoặc	Tập các véc tơ

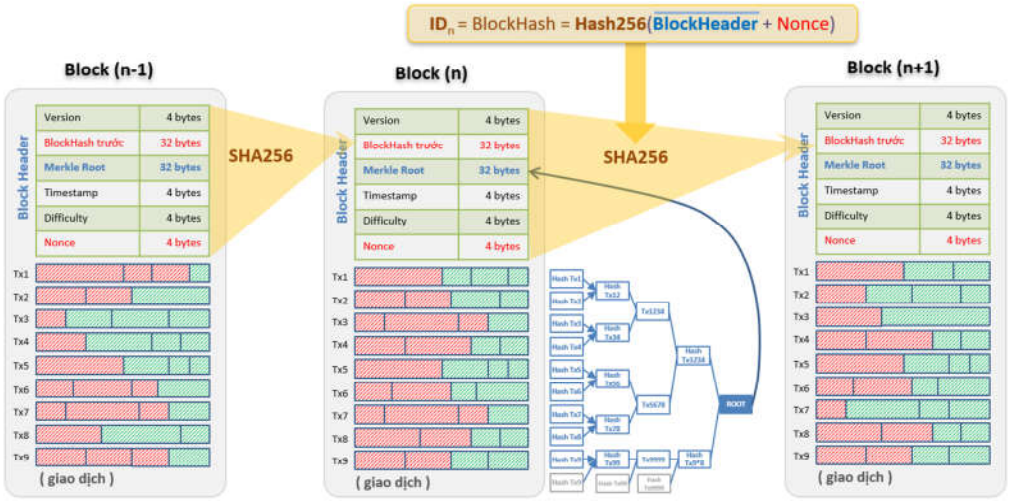
	nhiều)	
LockTimestamp	Thời gian hệ thống	Kiểu số



Hình 2.5: Cấu trúc transaction [5]

Khi thực hiện một giao dịch, người gửi sẽ sử dụng chữ ký điện tử (bằng khóa bí mật) để ký vào giá trị băm của giao dịch liền trước và khóa công khai của người nhận. Bằng cách này, người nhận có thể xác thực được giao dịch có chính xác hay không.

- Khối (block) và chuỗi khối (blockchain)



Hình 2.6: Mô hình khối và chuỗi khối của bitcoin [10]

Mỗi block sẽ chứa block header và block data (là tập hợp các giao dịch trong khối). Block header được sử dụng để xác định một khối cụ thể trên toàn bộ blockchain và được băm liên tục để tạo bằng chứng công việc (proof-of-work), block header bao gồm 6 thành phần:

- Phiên bản của blockchain.
- Mã băm của block trước.
- Merkle root: là tổng hợp mã băm của các giao dịch trong block, merkle root chính là gốc của cây nhị phân các mã băm của giao dịch, trong trường hợp số lượng giao dịch là số lẻ thì giao dịch cuối cùng sẽ được nhân đôi lên để đảm bảo tạo thành cây nhị phân. Merkle root này cũng để xác định tính toàn vẹn của block, bởi chỉ cần một giao dịch bất kỳ trong block thì thay đổi thì giá trị của merkle root này cũng sẽ thay đổi theo.
- Timestamp: Thời gian hệ thống.
- Difficulty: Độ khó quy định để tạo block. Độ khó này thông thường là số lượng bit 0 đầu tiên ở trong mã băm của block.
- Nonce: Là giá trị tăng dần, giá trị này sẽ kết hợp với các data trong block header để tạo ra mã băm thỏa mãn độ khó quy định (difficulty). Mục đích

của số Nonce và Difficulty là để sử dụng sức mạnh CPU của máy tính cũng như thời gian cần thiết để làm tăng chi phí cho việc giả mạo dữ liệu.

Bảng 2.3: Tìm số Nonce thỏa mãn Difficulty bằng 3

Nonce	**Dữ liệu**	**Dữ liệu + Nonce**	**Mã băm**
001	HelloWorld	HelloWorld 001	4EE4B774…
002	HelloWorld	HelloWorld 002	3345B9A3…
003	HelloWorld	HelloWorld 003	72040842…
	…		
613	HelloWorld	HelloWorld 613	E8639001…
614	HelloWorld	HelloWorld 614	00068A3C…

Chuỗi khối (blockchain) là tập hợp các block được liên kết với nhau bằng các mã băm. Khối phía sau luôn chứa mã băm của khối liền trước. Chỉ cần có một thay đổi trong khối liền trước giá trị băm của khối sẽ bị thay đổi làm phá vỡ liên kết trong chuỗi. Điều này đảm bảo tính bất biến dữ liệu trong mạng blockchain.

- Bằng chứng công việc (proof-of-work)

Đây là công việc tìm ra mã băm thỏa mãn độ khó yêu cầu. Công việc này tiêu tốn một lượng thời gian tính toán của CPU. Công việc tìm ra mã băm này đảm bảo rằng không có một giải thuật nào khác ngoài việc phải thử từng số Nonce theo thứ tự tăng dần. Tùy thuộc vào nhóm quản trị blockchain, thời gian để tạo ra mã băm này sẽ được thay đổi dựa theo số Difficulty.

- Cơ chế đồng thuận phân tán

Khi một block được tạo ra tại một nút, nút này sẽ thông báo đến các nút khác trong mạng blockchain. Các nút này sẽ thực hiện xác nhận xem block được tạo ra có hợp lệ hay không, và khi số lượng nút xác nhận đạt đến một tỉ lệ nhất định (51% hoặc một con số bất kỳ do blockchain quy định) thì block này sẽ được công nhận và

được nối vào blockchain. Cơ chế này đảm bảo dữ liệu không do một cá nhân hay tổ chức nào quản lý mà được quản lý và chấp thuận bởi số đông các nút trong mạng.

2.2. Ứng dụng blockchain cho bầu cử điện tử

2.2.1. Yêu cầu của hệ thống bầu cử điện tử, mô hình an toàn và các khả năng tấn công vào hệ thống bầu cử điện tử

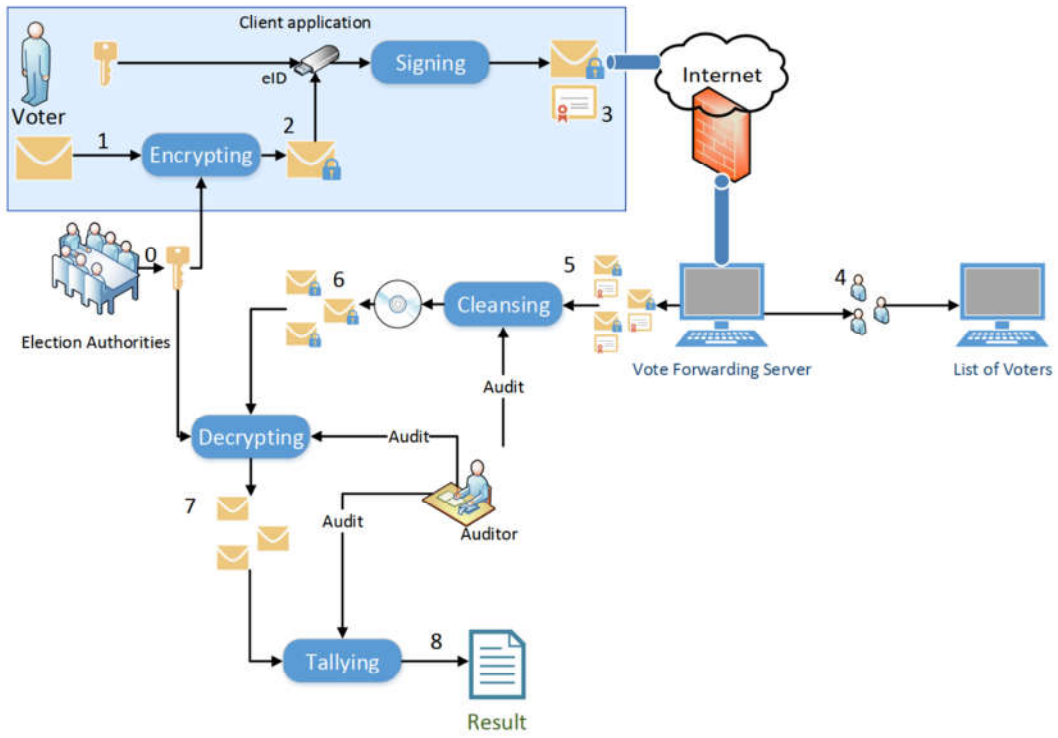
a. Yêu cầu của hệ thống bầu cử điện tử

Các hệ thống bầu cử điện tử được đưa ra với mục đích khắc phục nhược điểm (đặc biệt là riêng tư, bảo mật và chính xác) của việc bầu cử truyền thống bằng giấy. Với việc sử dụng các phương thức mã hóa và quản lý dữ liệu điện tử, các nhược điểm này đã được loại bỏ. Do vậy, một hệ thống bầu cử điện tử cần có những yêu cầu cơ bản sau [12] [13]:

- Tính sẵn sàng: Hệ thống bầu cử điện tử phải luôn sẵn sàng hoạt động trong khoảng thời gian diễn ra bầu cử.
- Tính minh bạch: Hệ thống phải đảm bảo rằng tất cả các lá phiếu đều được ghi nhận và kiểm đếm.
- Tính duy nhất: Hệ thống phải đảm bảo rằng một cử tri chỉ được bỏ phiếu một lần duy nhất.
- Tính toàn vẹn: Hệ thống phải đảm bảo rằng tất cả các lá phiếu đã được cử tri bầu là không thể thay đổi, sửa chữa hoặc xóa bỏ.
- Tính riêng tư: Hệ thống phải đảm bảo rằng không ai (ngoài bản thân cử tri) biết họ đã bầu cho ai.
- Tính đo đếm: Hệ thống phải cung cấp chức năng cho việc kiểm đếm và báo cáo.
- Tính xác thực: Hệ thống phải đảm bảo rằng chỉ những cử tri được cấp quyền mới có thể tham gia bỏ phiếu.
- Tính bảo mật: Dữ liệu bầu cử cần được bảo vệ an toàn, tránh việc đọc được từ bên ngoài.

- Tính tin cậy: Hệ thống bầu cử điện tử cần đảm bảo hoạt động một cách chính xác, không làm mất dữ liệu phiếu bầu.

b. Mô hình an toàn của hệ thống bầu cử điện tử



Hình 2.7: Mô hình bầu cử điện tử của Estonian [14]

Bầu cử điện tử rất chú trọng vào tính an toàn và bảo mật dữ liệu. Vì vậy, hầu hết các hệ thống bầu cử điện tử đều xây dựng cho mình một mô hình an toàn dựa trên các yếu tố cơ bản sau:

- Dữ liệu của cử tri luôn được bảo mật và được quản lý bởi một cơ quan thứ 3.
- Cử tri cần phải được cấp quyền và thực hiện xác thực thông qua cơ quan quản lý bầu cử.
- Trước khi gửi lá phiếu của mình đi, lá phiếu cần được mã hóa bởi chữ ký điện tử của cử tri.
- Dữ liệu tại máy chủ được bảo vệ qua hệ thống tường lửa.

- Cơ quan bầu cử sẽ thực hiện giải mã lá phiếu của cử tri trước khi tổng hợp và đưa ra kết quả.

c. Khả năng tấn công vào hệ thống bầu cử điện tử

Về mặt lý thuyết, các hệ thống bầu cử điện tử có thể bị tấn công bởi việc sử dụng các thuật toán mã hóa chưa đủ độ mạnh, hoặc do sai sót trong quá trình thiết kế giao thức giao tiếp.

Tuy nhiên, một hệ thống bầu cử điện tử được cấu thành bởi nhiều thành phần và được triển khai trên một máy chủ có kết nối Internet. Vì vậy, nó có thể bị tấn công bởi các phương thức tấn công qua mạng như: DDos, Man-in-the-Middle, packet sniffing…

Bên cạnh đó, một điểm cần chú ý là các thành phần được sử dụng cho việc triển khai hệ thống bầu cử điện tử. Chúng có thể chứa những cửa hậu (back-doors) hoặc việc sử dụng các thư viện không đảm bảo an toàn cũng có thể là nguyên nhân gây ra các cuộc tấn công.

2.2.2. Giới thiệu mô hình ứng dụng blockchain cho bầu cử điện tử

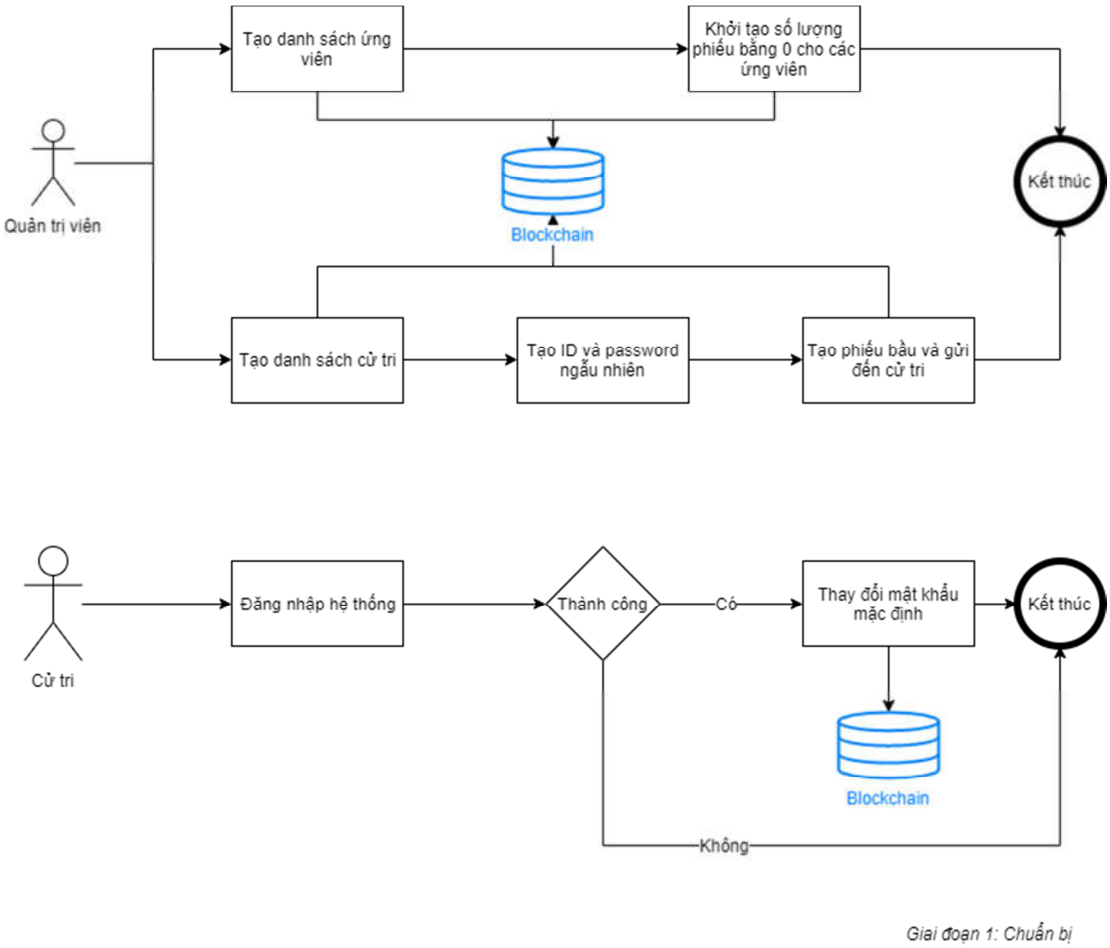
a. Bài toán

Luận văn đưa ra mô hình ứng dụng công nghệ blockchain cho cuộc bầu cử tại một trường đại học, với mục đích chứng minh tính ứng dụng của blockchain cho bầu cử điện tử. Bài toán cụ thể như sau: Tại trường đại học A, ban giám hiệu nhà trường muốn tổ chức một cuộc bầu cử để chọn ra 1 người cho vị trí "Chủ tịch hội đồng sinh viên" của nhà trường. Danh sách các ứng viên đã được lựa chọn qua từng khoa, từng lớp và tổng hợp lại về ban giám hiệu nhà trường. Tất cả sinh viên trong trường đều có quyền bầu cử và tất cả sinh viên trong trường đều có địa chỉ email và mã số sinh viên duy nhất do nhà trường cấp

b. Mô hình ứng dụng blockchain cho bầu cử điện tử

Dựa trên các đặc tính của blockchain cũng như các yêu cầu đối với một hệ thống bầu cử điện tử. Luận văn đưa ra mô hình ứng dụng blockchain cho bầu cử điện tử sử dụng mạng blockchain riêng tư (private blockchain) với 3 giai đoạn như sau:

- Giai đoạn 1: Chuẩn bị



Hình 2.8: Giai đoạn 1 – chuẩn bị bầu cử

- Quản trị viên sẽ tạo ra các địa chỉ ví cho các ứng viên, đồng thời lưu các thông tin cơ bản của ứng viên như: ID định danh, tên, tuổi, địa chỉ, lớp, khoa… đồng thời khởi tạo số lượng phiếu bầu cho mỗi ứng viên bằng 0.

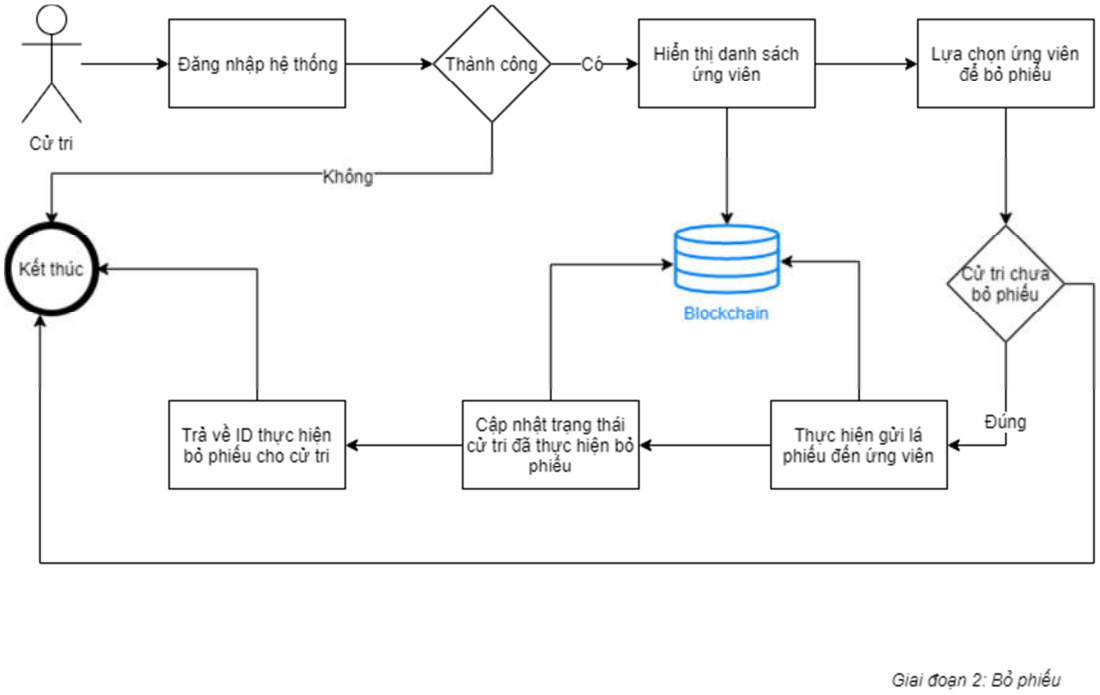
- Dựa theo số lượng cử tri đủ điều kiện tham gia bầu cử, quản trị viên sẽ tạo ra danh sách các ID định danh và địa chỉ ví ngẫu nhiên cho các cử tri. ID và 1 mật khẩu ngẫu nhiên sẽ được gửi đến cử tri để đảm bảo tính trong suốt của dữ liệu (ID định danh sẽ không đi kèm với thông tin về địa chỉ email hay thông tin của cử trị). ID và mật khẩu có thể được gửi đến cử tri thông qua email được nhà trường cung cấp. Tuy nhiên việc gửi email cũng có rủi ro, khi đó quản trị viên có thể biết được ID định danh được gửi đến địa chỉ email nào và tính trong suốt của dữ liệu không được đảm bảo. Để đảm bảo yếu tố trong suốt, luận văn đề xuất xây dựng một hệ thống để đảm nhiệm việc phát phiếu bầu cho cử tri, cụ thể như sau:
    - Tất cả các cử tri cần đến một địa điểm nhất định để nhận ID định danh và mật khẩu ngẫu nhiên (ID và mật khẩu sẽ được in và niêm phong trong phong bì kín giống như khi nhận thẻ ATM và mã PIN từ ngân hàng)
    - Trước khi cử tri bốc phong bì ngẫu nhiên, cử tri cần phải được kiểm duyệt thông qua hội đồng kiểm duyệt để đảm bảo cử tri có mặt trong danh sách được phép tham gia bầu cử và không có sự giả mạo (Kiểm tra thông qua chứng minh nhân dân, thẻ sinh viên, vân tay…)
    - Hệ thống cần lưu lại việc cử tri đã nhận ID và mật khẩu ngẫu nhiên.

  Như vậy, danh tính của cử tri vẫn hoàn toàn được bảo mật (quản trị viên cũng không thể biết ID thuộc về cử tri nào). Tuy nhiên, luận văn sẽ chỉ tập trung vào việc xây dựng hệ thống bầu cử điện tử và giả định rằng quy trình và hệ thống đảm nhiệm việc phát phiếu bầu cho cử tri đã có sẵn.

- Hệ thống sẽ tạo ra số lượng phiếu bầu (“phieu”: trong mạng blockchain sẽ được thể hiện là 1 loại token hoặc asset) tương ứng với số lượng cử tri, đồng thời sẽ gửi đến mỗi địa chỉ ví của cử tri 1 phiếu bầu. Bên cạnh đó, hệ thống cũng ghi nhận thông tin là địa chỉ ví hiện tại của cử trị chưa tham gia bầu cử (Chưa gửi phiếu bầu cho bất kỳ ứng viên nào)

- Tại lần đăng nhập đầu tiên, hệ thống yêu cầu cử tri phải thay đổi mật khẩu mặc định, hệ thống sẽ lưu mật khẩu ở dạng mã hóa

- Giai đoạn 2: Bỏ phiếu

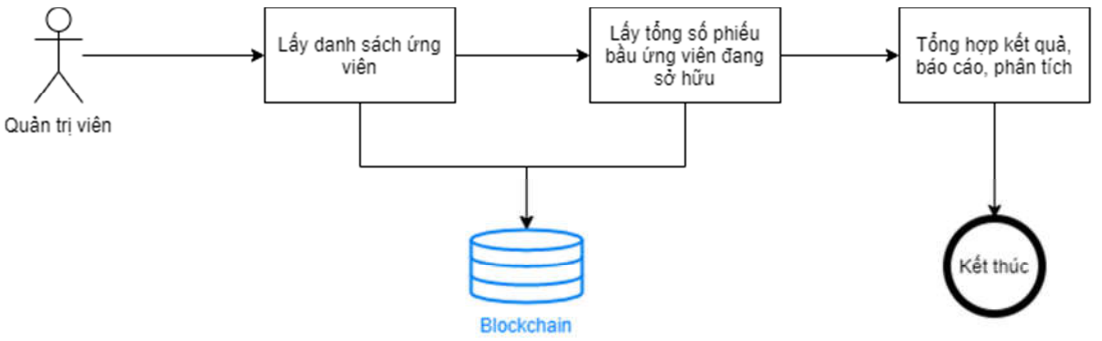


Hình 2.9: Giai đoạn 2 – Bỏ phiếu

- Trong thời gian diễn ra bầu cử, cử tri phải đăng nhập vào hệ thống bằng ID định danh và mật khẩu
- Sau khi đăng nhập thành công, hệ thống sẽ hiển thị ra danh sách các ứng viên để cử tri có thể bỏ phiếu
- Tại bước bỏ phiếu, trước tiên hệ thống sẽ kiểm tra xem cử tri đã tham gia bầu cử hay chưa, nếu chưa thì cử tri có quyền lựa chọn 1 ứng viên và thực hiện bỏ phiếu
- Quá trình bỏ phiếu được thực hiện bằng cách: Cử tri thực hiện 1 giao dịch chuyển lá phiếu của mình đến địa chỉ ví công khai của ứng viên, đồng thời hệ thống sẽ cập nhật trạng thái thể hiện cử tri đã tham gia bầu cử

- Sau khi hoàn thành quá trình bỏ phiếu, cử tri sẽ nhận được 1 mã giao dịch (Txid) để theo dõi quá trình bỏ phiếu của mình
- Giao dịch bỏ phiếu của cử tri sẽ được gửi đến toàn bộ mạng blockchain, lúc này mạng blockchain sẽ thực hiện xác thực (mined) giao dịch và ghi nhận giao dịch vào mạng blockchain

• Giai đoạn 3: Tổng hợp kết quả



Hình 2.10: Giai đoạn 3 – Tổng hợp kết quả

- Khi thời gian bầu cử kết thúc, hệ thống sẽ tiến hành tổng hợp kết quả, phân tích và báo cáo
- Kết quả số phiếu cho mỗi ứng viên chính là số lượng "phieu" mà địa chỉ ví của ứng viên đang có. Từ kết quả này, hệ thống có thể đưa ra biểu đồ, biểu mẫu và kết quả cuối cùng của cuộc bầu cử

c. Chứng minh tính đúng đắn

Mô hình ứng dụng công nghệ blockchain cho bầu cử điện tử đáp ứng các yêu cầu cần thiết đối với một hệ thống bầu cử điện tử

- Tính sẵn sàng: Hệ thống được triển khai trên nền tảng blockchain, sử dụng mạng peer-to-peer, khi một node bị tắt, hệ thống vẫn có thể hoạt động bình thường dựa trên các node khác.
- Tính minh bạch: Các phiếu bầu được ghi nhận dưới dạng giao dịch (transaction) trong hệ thống blockchain, các giao dịch này được ghi nhận

trong các khối (block) và được lưu trữ ở tất cả các node tham gia vào hệ thống, vì vậy dữ liệu là hoàn toàn minh bạch.

- Tính duy nhất: Việc bỏ phiếu 2 lần được loại bỏ do tính chất của blockchain không cho phép double-spending. Ngoài ra, hệ thống sẽ kiểm tra cử tri đã thực hiện bỏ phiếu chưa trước khi thực hiện nên cũng sẽ ngăn chặn việc bỏ phiếu 2 lần.
- Tính toàn vẹn: Các lá phiếu được ghi nhận dưới dạng transaction của hệ thống blockchain, vì vậy dữ liệu này không thể bị thay đổi và xóa bỏ.
- Tính riêng tư: Hệ thống không lưu thông tin cá nhân của cử tri, ID định danh là duy nhất và chỉ có cử tri biết họ đang sở hữu ID nào.
- Tính đo đếm: Mỗi lá phiếu được ghi nhận là 1 token, việc bỏ phiếu tương đương với việc thực hiện giao dịch chuyển token đến ví của ứng viên. Vì vậy, việc kiểm phiếu, tổng hợp là rất dễ dàng.
- Tính xác thực: Chỉ các các cử tri đủ điều kiện mới nhận được ID định danh và mật khẩu, ngoài ra mật khẩu cũng được mã hóa và lưu trong hệ thống blockchain. Vì vậy, chỉ cử tri có quyền mới có thể tham gia bầu cử.
- Tính bảo mật: Hệ thống sử dụng blockchain riêng tư (private blockchain), việc đọc dữ liệu chỉ được cấp quyền cho một số node nhất đinh, vì vậy tính bảo mật luôn được đảm bảo.
- Tính tin cậy: Tính tin cậy đã được chứng minh thông qua nền tảng blockchain, hơn nữa hệ thống được thiết kế sử dụng private blockchain nên tính tin cậy càng được đảm bảo hơn.

d. Chứng minh tính an toàn

Trong phần này, luận văn sẽ phân tích về tính bảo mật, tính riêng tư và khả năng tấn công của hệ thống bầu cử điện tử ứng dụng công nghệ blockchain.

- Tính riêng tư của dữ liệu

Theo như mô hình thiết kế hệ thống, blockchain được lưu trữ tại máy chủ, dữ liệu bầu cử và các thông tin liên quan được lưu trữ trong các block và những block

này là an toàn đối với các loại tấn công và các mối đe dạo khác. Thêm nữa, nếu có bất kỳ hacker nào có được block thì dữ liệu trong block cũng không có ý nghĩa với họ bởi dữ liệu đã được mã hóa.

- Tính bảo mật cho cử tri

Hệ thống không lưu trữ thông tin cá nhân của cử tri, chỉ lưu ID định danh và địa chỉ ví. Vì vậy bản thân hệ thống cũng không biết cử tri đã bỏ phiếu cho ai. Vì vậy, tính bảo mật cho cử tri là cực kỳ được đảm bảo.

- Gian lận trong hệ thống

Hệ thống sử dụng blockchain để chống việc gian lận trong bầu cử. Để đảm bảo không ai có thể bỏ phiếu hai lần, hệ thống sử dụng ID định danh duy nhất để nhận dạng cử tri, ngoài ra hệ thống sẽ ghi nhận lại ID nào đã thực hiện bỏ phiếu rồi. Mỗi block luôn ghi nhận hash (hàm băm) của block trước (previous block), chữ ký và hàm băm của merkle root. Chữ ký được sử dụng để chứng minh tính xác thực và tính toàn vẹn của dữ liệu. Merkle root đảm bảo dữ liệu không bị thay đổi. Do đó, hệ thống đưa ra đảm bảo chống được việc gian lận trong bầu cử.

- Đánh giá hiệu năng hệ thống

Hệ thống sử dụng công nghệ blockchain và mạng peer-to-peer. Vì vậy, hệ thống có thể dễ dàng mở rộng theo chiều ngang. Tuy nhiên việc đánh giá hiệu năng của hệ thống sẽ chịu ảnh hưởng của một số yếu tố khác như: thiết kế hệ thống, lựa chọn công nghệ, cách thức triển khai, số lượng node… Vì vậy, phần đánh giá hiệu năng này sẽ được trình bày rõ hơn ở chương 3.

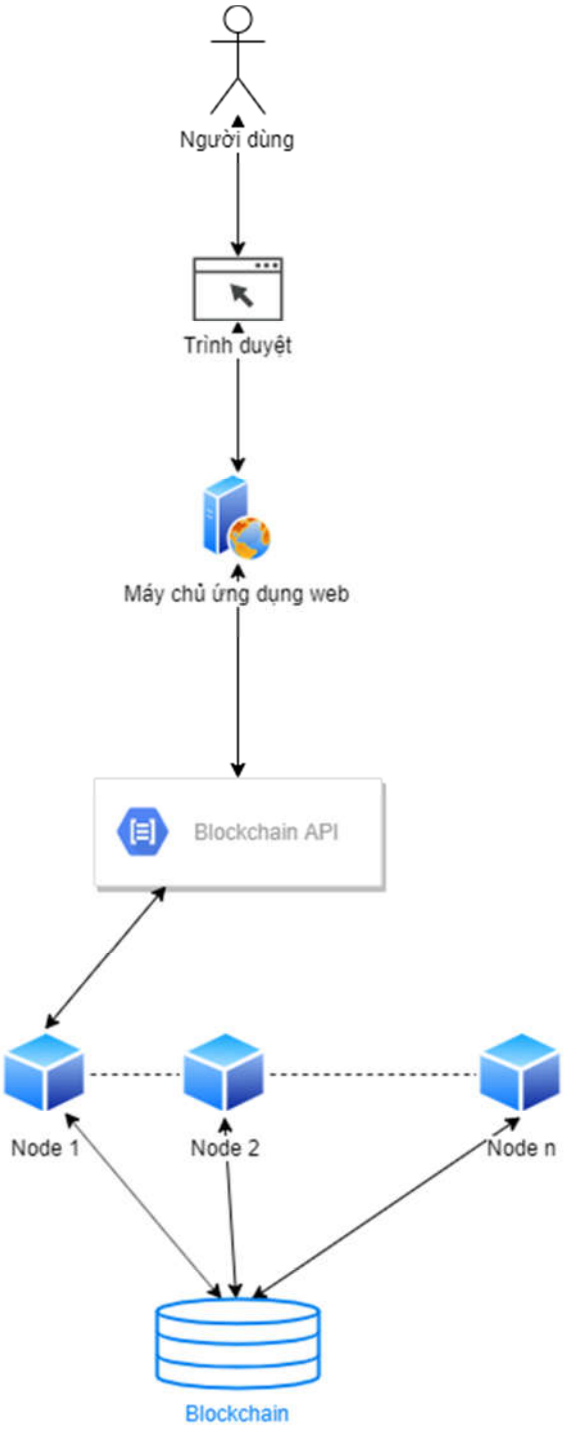
2.3. Kết luận chương

Chương này đã giới thiệu về công nghệ blockchain và mô hình ứng dụng công nghệ blockchain cho bầu cử điện tử. Đồng thời, chương cũng trình bày chi tiết về các giai đoạn của mô hình bầu cử điện tử ứng dụng blockchain và tính đúng đắn

cũng như tính an toàn của mô hình. Ở chương 3, luận văn sẽ đi vào chi tiết xây dựng hệ thống thử nghiệm để chứng minh mô hình.

CHƯƠNG 3: THỬ NGHIỆM VÀ KẾT QUẢ

3.1. Phân tích thiết kế hệ thống



Hình 3.1: Thiết kế hệ thống mô hình bầu cử điện tử ứng dụng blockchain

Để cử tri có thể bỏ phiếu thuận lợi nhất tại bất kỳ đâu. Luận văn đưa ra mô hình thiết kế hệ thống với trình duyệt là kênh tương tác với cử tri cũng như ứng viên và quản trị viên. Khi người dùng tương tác với trình duyệt, các yêu cầu sẽ được xử lý tại máy chủ ứng dụng web. Tại đây, máy chủ ứng dụng web sẽ thực hiện các chức năng khác nhau và tương tác với cơ sở dữ liệu blockchain.

3.2. Lựa chọn công nghệ và triển khai hệ thống

Lợi thế khi sử dụng Bitcoin làm nền tảng blockchain để ứng dụng cho bầu cử điện tử là cơ sở hạ tầng đã khá hoàn thiện và được thử nghiệm rất lớn. Tuy nhiên, do sự biến động giá đáng kể của bitcoin, chi phí hiện tại và tương lai của loại tiền điện tử này và các khoản phí mà các nhà khai thác yêu cầu để nhanh chóng xác thực các giao dịch, sử dụng chuỗi khối Bitcoin có là rất tốn kém và không đảm bảo thời gian cho quá trình bỏ phiếu (Thời gian để xác nhận 1 phiếu bầu có thể lên tới 10 phút). Vì vậy, luận văn đề xuất một nền tảng blockchain khác đó là Multichain. Về nền tảng cho việc xây dụng ứng dụng web, luận văn đề xuất sử dụng JavaEE.

JavaEE là một nền tảng được phát triển bởi Sun (hiện tại đã thuộc sở hữu của Oracle). Đây là một nền tảng tương đối nổi tiếng và phổ biến. Vì vậy, luận văn sẽ không đi sâu vào phần giới thiệu các đặc điểm của JavaEE mà sẽ tập trung giới thiệu một số tính chất của Multichain.

MultiChain [15] là một nền tảng để tạo và triển khai các chuỗi khối riêng (private blockchain). Mục tiêu ban đầu và cũng là mục tiêu chính của nó là đơn giản hóa việc triển khai công nghệ blockchain trong lĩnh vực tài chính cho tổ chức, bằng cách cung cấp nhiều quyền riêng tư và kiểm soát hơn. MultiChain hỗ trợ các hệ điều hành khác nhau như Windows, Linux và Mac. Ngoài ra, nó cung cấp một giao diện lệnh (command interface) và API đơn giản.

Multichain giải quyết các vấn đề liên quan đến khai thác (mining), quyền riêng tư và tính mở thông qua quản lý tích hợp các quyền của người dùng. Để giải quyết các vấn đề trên, Multichain tập trung vào 3 khía cạnh:

- Đầu tiên, đảm bảo rằng hoạt động chuỗi khối chỉ hiển thị cho những người tham gia được chọn.
- Thứ hai, giới thiệu cách thức kiểm soát giao dịch (giao dịch nào được phép, giao dịch nào không).
- Thứ ba, để tránh chi phí và thời gian PoW trong giai đoạn mining, nó đưa ra cơ chế đảm bảo tính bảo mật nhưng sẽ giảm các chi phí liên quan.

Để kiểm soát quyền truy cập, MultiChain xây dựng cơ chế mà bất kỳ tin nhắn nào cũng phải được người dùng ký để chứng minh rằng họ sở hữu khóa riêng tương ứng với một địa chỉ cụ thể. MultiChain sử dụng tính năng này để hạn chế quyền truy cập blockchain. Quá trình bắt tay (handshake) trên mạng blockchain xảy ra khi hai nút blockchain kết nối được mô tả theo bốn bước:

- Mỗi nút đưa ra định danh của nó chính là địa chỉ công khai trong danh sách được phép truy cập.
- Mỗi nút xác minh rằng địa chỉ còn lại nằm trong danh sách được phép của chính nó.
- Mỗi nút gửi một thông điệp thách thức (challenge message) cho bên kia.
- Mỗi nút gửi lại một chữ ký của thông điệp thách thức (challenge message), chứng minh quyền sở hữu của họ đối với khóa riêng tương ứng với địa chỉ công khai mà họ đã đưa ra.

Trong MultiChain, có 8 loại quyền có thể được cấp trên cơ sở mỗi địa chỉ:

- connect: để kết nối với các nút khác và xem nội dung chuỗi khối.
- send: để gửi tài sản (fund).
- receive: để nhận tài sản.
- issue: phát hành tài sản.
- create: để tạo các stream.
- mine: để khai thác (mine) các khối.
- activate: để thay đổi kết nối, gửi và nhận các nhiệm vụ cho người dùng khác.

- admin: để thay đổi tất cả các quyền cho người dùng khác, bao gồm cả issue, mine, active và admin.

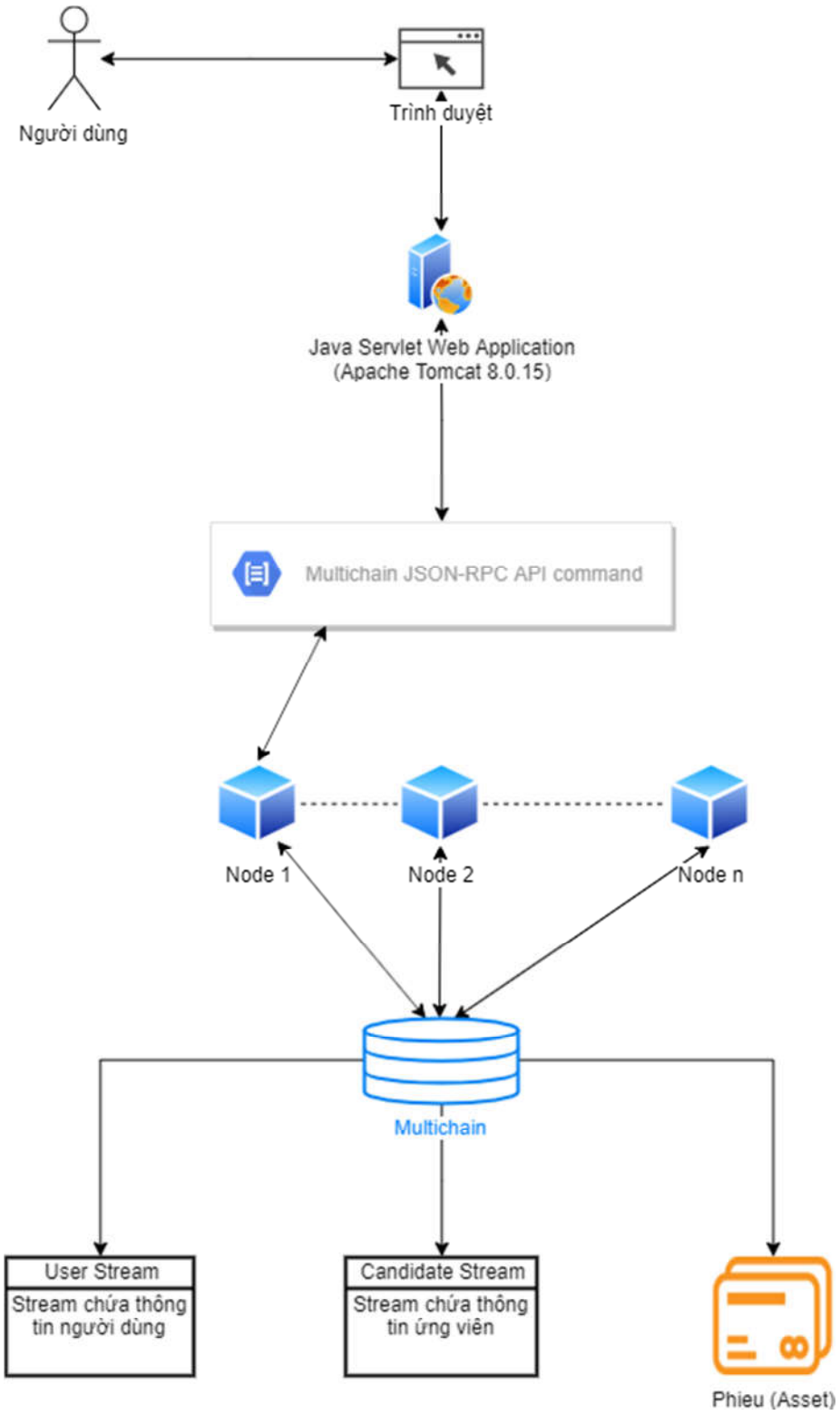
Nói chung, các quyền có thể được thực hiện tạm thời bằng cách giới hạn chúng theo phạm vi số khối cụ thể: theo cách này, chúng chỉ khả dụng đối với các giao dịch xuất hiện trong khoảng thời gian của các khối này.

Về hiệu năng, Multichain tỏ ra nổi trội hơn hẳn so với Bitcoin (giới hạn 4 giao dịch trên giây), dưới đây là kết quả về hiệu năng của Multichain khi cài đặt blockchain với 1 nút cho 5 phiên bản đã được công bố (Các thử nghiệm được thực hiện bằng cách sử dụng công cụ đo điểm chuẩn máy chủ HTTP gửi hai yêu cầu đồng thời đến API "sendtoaddress". Thông số kỹ thuật của máy chủ: Intel Core i7-4770, 4 nhân @ 3,4 MHz, RAM 32 GB, Seagate 2 TB 7200 RPM SATA, CentOS 6.4) [16]:

Bảng 3.1: Các giao dịch trung bình mỗi giây của Multichain

Tổng số giao dịch	Phiên bản 1.0 alpha 3	Phiên bản 1.0 alpha 21	Phiên bản 1.0 alpha 22	Phiên bản 1.0 beta 1	Phiên bản 1.0 beta 2
100	6.5 tps	7.8	541.7	830.6	1465.7
1000	7.0	7.7	583.9	889.4	1199.6
10000	4.1	6.4	566.9	746.6	1071.2
100000	-	6.6	558.0	771.9	1034.2
1000000	-	-	548.6	773.6	1055.4

Mô hình hệ thống ứng dụng blockchain cho bầu cử điện tử sử dụng Multichain sẽ được triển khai chi tiết như sau:



Hình 3.2: Mô hình thiết kế hệ thống sử dụng JavaEE và Multichain

Hình trên mô tả mô hình tổng quan của ứng dụng. Các nút trong mạng lưới sẽ được tạo ra dựa trên một vài nút "admin" (Nút "admin" đóng vai trò quản trị toàn bộ mang lưới, bao gồm phân quyền cho các nút còn lại). Để truy cập vào multichain, luận văn sử dụng JSON-RPC API Client [17][18] cho Java.

Thay vì sử dụng cơ sở dữ liệu thứ hai cho việc lưu trữ thông tin người dùng và xác thực người dùng, luận văn sử dụng trực tiếp multichain để lưu trữ và xác thực. Hai stream được tạo ra gồm: User Stream để lưu trữ thông tin của cử tri và quản trị viên (cử tri có quyền bầu cử và theo dõi lá phiếu của mình, quản trị viên có quyền xem báo cáo tổng hợp số lượng phiếu bầu cho các ứng viên), Candidate Stream để lưu trữ thông tin về ứng viên.

Bảng 3.2: Mô tả dữ liệu cử tri

Trường dữ liệu	**Kiểu dữ liệu**	**Mô tả**
UserId	Kiểu chuỗi	ID được sinh ngẫu nhiên, dùng để đại diện cho cử tri
Address	Kiểu chuỗi	Địa chỉ ví của cử tri, dùng để nhận phiếu bầu tử quản trị viên và bỏ phiếu cho ứng viên
Password	Kiểu chuỗi	Mật khẩu được mã hóa SHA256
Salt	Kiểu chuỗi	Dãy Salt được sinh ngẫu nhiên để tăng tính bảo mật
IsVoted	Kiểu logic (Đúng/Sai)	Giá trị thể hiện việc cử tri đã tham gia bỏ phiếu hay chưa
Txid	Kiểu chuỗi	ID của giao dịch mà cử tri thực hiện bỏ phiếu, để cử tri có thể theo dõi lá phiếu của mình

Thông tin của cử tri là hoàn toàn bí mật, hệ thống không lưu trữ thông tin cá nhân của cử tri. Địa chỉ ví và UserId được sinh ngẫu nhiên, mỗi địa chỉ ví của ứng viên sẽ được được nhận một phiếu bầu duy nhất từ quản trị viên. Sau khi nhận được

phiếu bầu, các địa chỉ ví này sẽ chỉ còn quyền "send" chứ không còn quyền "receive" để đảm bảo mỗi cử tri chỉ bỏ phiếu một lần duy nhất. Sau khi bỏ phiếu thành công, cử tri sẽ được ghi nhận là đã bỏ phiếu (IsVoted = true) và ID giao dịch được gửi cho cử tri để theo dõi quá trình bỏ phiếu của mình.

Bảng 3.3: Mô tả dữ liệu quản trị viên

Trường dữ liệu	Kiểu dữ liệu	Mô tả
UserId	Kiểu chuỗi	ID được sinh ngẫu nhiên, dùng để đại diện cho quản trị viên
FullName	Kiểu chuỗi	Họ tên của quản trị viên
Password	Kiểu chuỗi	Mật khẩu được mã hóa SHA256
Salt	Kiểu chuỗi	Dãy Salt được sinh ngẫu nhiên để tăng tính bảo mật

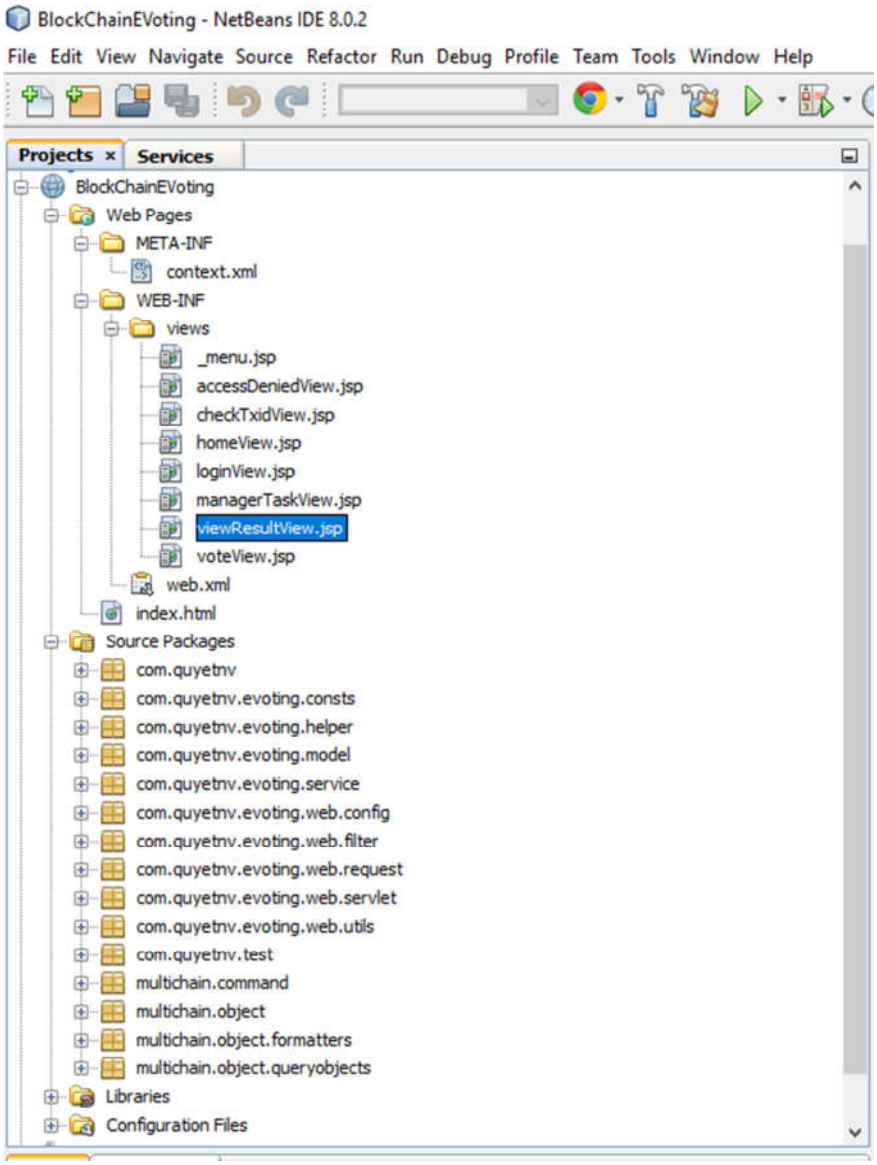
Người dùng với vai trò Quản trị viên sẽ có nhiệm vụ tạo UserID, địa chỉ ví cho cử tri và ứng viên. Sau đó thông tin UserID, password mặc định sẽ được gửi cho cử tri và ứng viên. Ngoài ra Quản trị viên cũng đóng vai trò gửi các lá phiếu đến cho cử tri đồng thời tổng hợp kết quả sau khi cuộc bầu cử kết thúc.

Bảng 3.4: Mô tả dữ liệu ứng viên

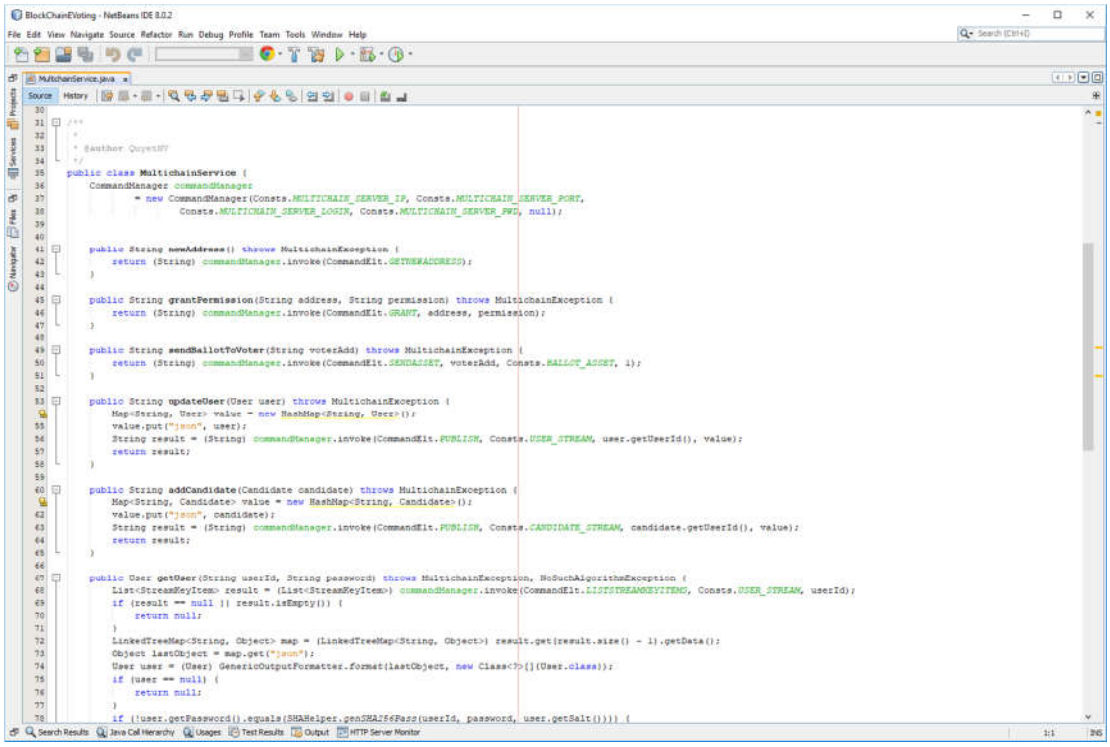
Trường dữ liệu	Kiểu dữ liệu	Mô tả
UserId	Kiểu chuỗi	ID được sinh ngẫu nhiên, dùng để đại diện cho ứng viên
Address	Kiểu chuỗi	Địa chỉ ví của ứng viên, dùng để nhận phiếu bầu từ các cử tri
Password	Kiểu chuỗi	Mật khẩu được mã hóa SHA256
Salt	Kiểu chuỗi	Dãy Salt được sinh ngẫu nhiên để tăng tính bảo mật
FullName	Kiểu chuỗi	Họ tên của ứng viên
Info	Kiểu chuỗi	Các thông tin cơ bản của ứng viên

Mỗi ứng viên cũng sẽ được tạo ra một ID định danh và địa chỉ ví. Địa chỉ ví này sẽ được công khai đến toàn bộ cử tri. Cử tri dựa vào họ tên ứng viên và các thông tin cơ bản để quyết định sẽ bỏ phiếu cho ai thông qua việc gửi lá phiếu từ địa chỉ ví của mình đến địa chỉ ví của ứng viên.

Dưới đây là cấu trúc mã nguồn (source code) của ứng dụng cũng như một số dòng lệnh thực thi các tác vụ trên Multichain của hệ thống bầu cử điện tử ứng dụng blockchain mà luận văn đã triển khai.

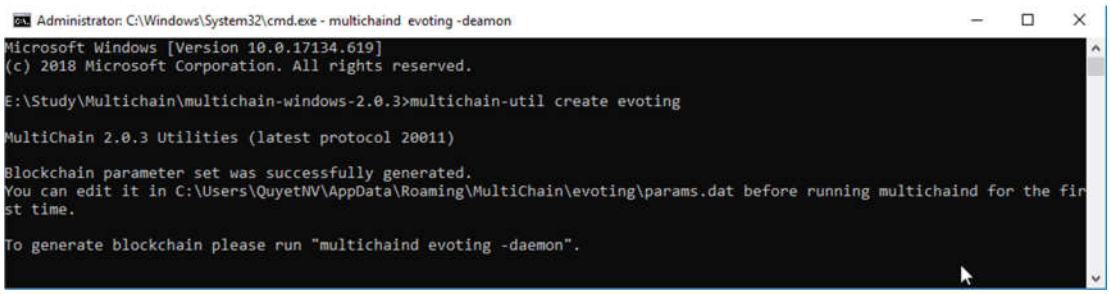


Hình 3.3: Cấu trúc mã nguồn của ứng dụng



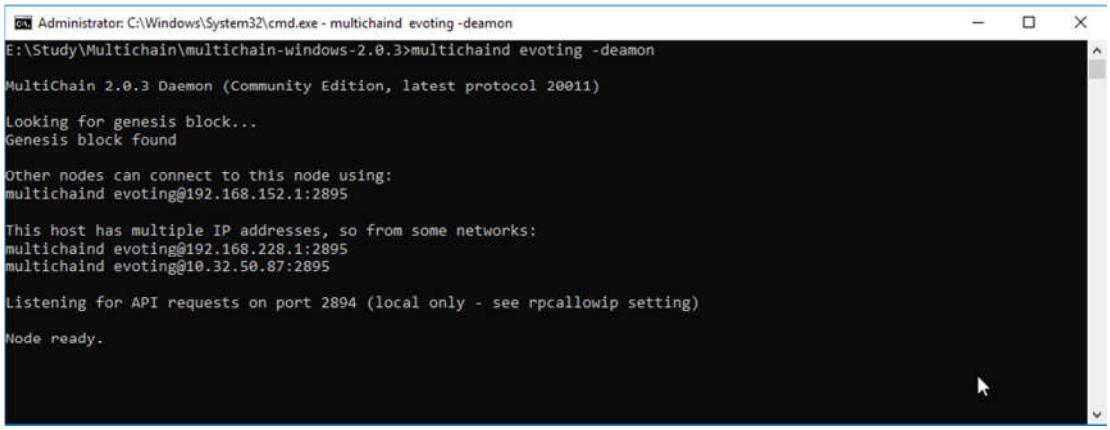
```
/**
 *
 * @author QuyetNV
 */
public class MultichainService {
    CommandManager commandManager
            = new CommandManager(Consts.MULTICHAIN_SERVER_IP, Consts.MULTICHAIN_SERVER_PORT,
                    Consts.MULTICHAIN_SERVER_LOGIN, Consts.MULTICHAIN_SERVER_PWD, null);


    public String newAddress() throws MultichainException {
        return (String) commandManager.invoke(CommandElt.GETNEWADDRESS);
    }

    public String grantPermission(String address, String permission) throws MultichainException {
        return (String) commandManager.invoke(CommandElt.GRANT, address, permission);
    }

    public String sendBallotToVoter(String voterAdd) throws MultichainException {
        return (String) commandManager.invoke(CommandElt.SENDASSET, voterAdd, Consts.BALLOT_ASSET, 1);
    }

    public String updateUser(User user) throws MultichainException {
        Map<String, User> value = new HashMap<String, User>();
        value.put("json", user);
        String result = (String) commandManager.invoke(CommandElt.PUBLISH, Consts.USER_STREAM, user.getUserId(), value);
        return result;
    }

    public String addCandidate(Candidate candidate) throws MultichainException {
        Map<String, Candidate> value = new HashMap<String, Candidate>();
        value.put("json", candidate);
        String result = (String) commandManager.invoke(CommandElt.PUBLISH, Consts.CANDIDATE_STREAM, candidate.getUserId(), value);
        return result;
    }

    public User getUser(String userId, String password) throws MultichainException, NoSuchAlgorithmException {
        List<StreamKeyItem> result = (List<StreamKeyItem>) commandManager.invoke(CommandElt.LISTSTREAMKEYITEMS, Consts.USER_STREAM, userId);
        if (result == null || result.isEmpty()) {
            return null;
        }
        LinkedTreeMap<String, Object> map = (LinkedTreeMap<String, Object>) result.get(result.size() - 1).getData();
        Object lastObject = map.get("json");
        User user = (User) GenericOutputFormatter.format(lastObject, new Class<?>[](User.class));
        if (user == null) {
            return null;
        }
        if (!user.getPassword().equals(SHAHelper.genSHA256Pass(userId, password, user.getSalt()))) {
```

Hình 3.4: Mã nguồn dùng JSON-RPC API để tương tác với Multichain

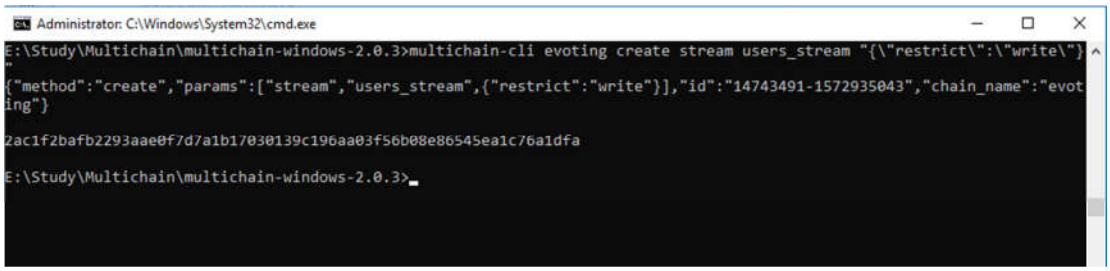


```
Administrator: C:\Windows\System32\cmd.exe - multichaind evoting -deamon
Microsoft Windows [Version 10.0.17134.619]
(c) 2018 Microsoft Corporation. All rights reserved.

E:\Study\Multichain\multichain-windows-2.0.3>multichain-util create evoting

MultiChain 2.0.3 Utilities (latest protocol 20011)

Blockchain parameter set was successfully generated.
You can edit it in C:\Users\QuyetNV\AppData\Roaming\MultiChain\evoting\params.dat before running multichaind for the fir
st time.

To generate blockchain please run "multichaind evoting -daemon".
```

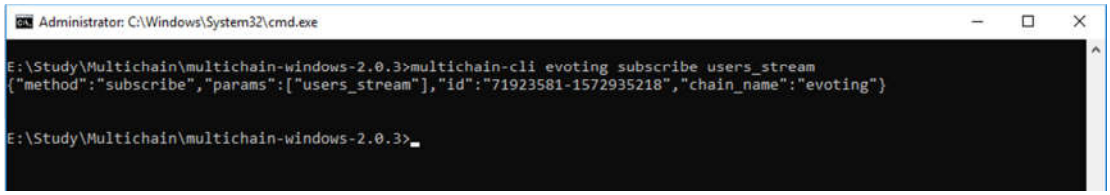
Hình 3.5: Tạo blockchain



Hình 3.6: Khởi động blockchain

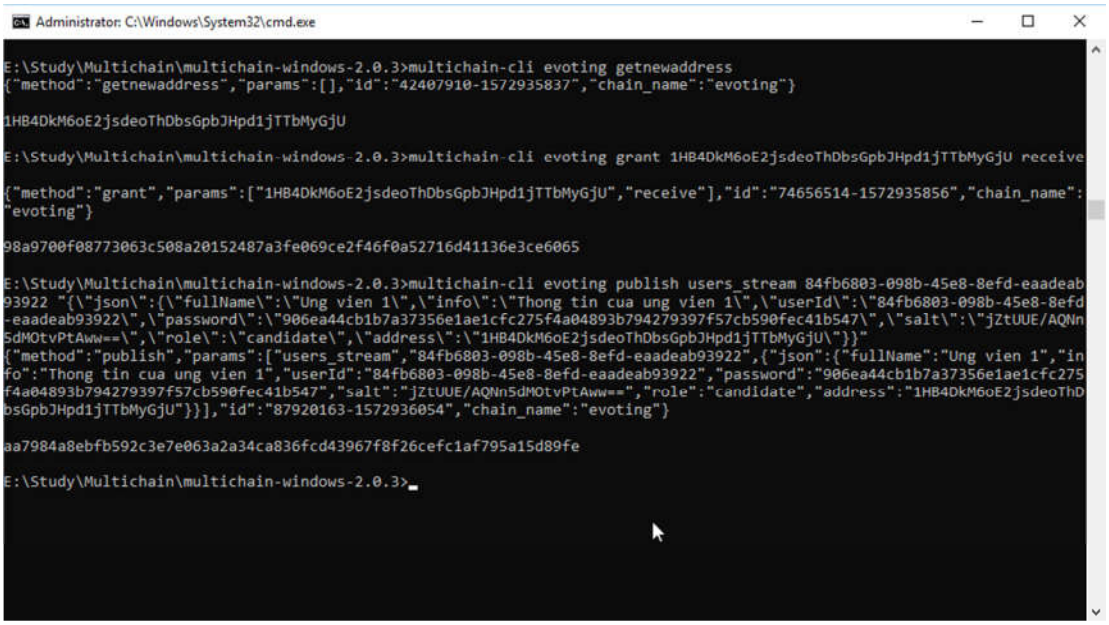


Hình 3.7: Tạo stream user

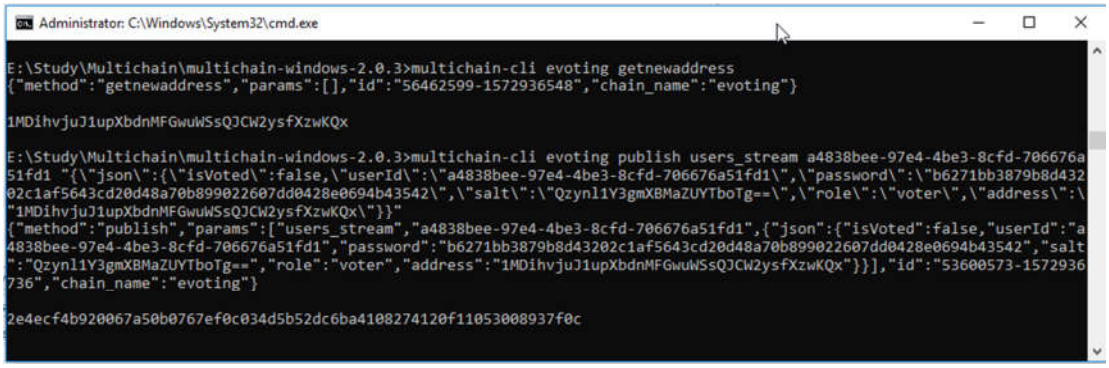


Hình 3.8: Đăng ký (subcribe) stream user

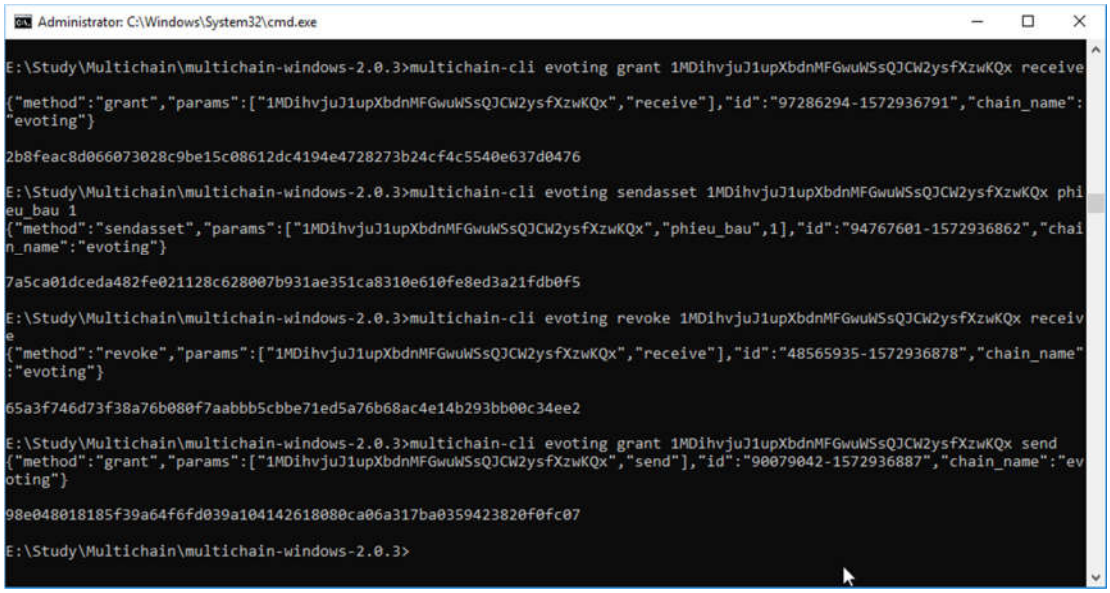
Hình 3.9: Tạo quản trị viên



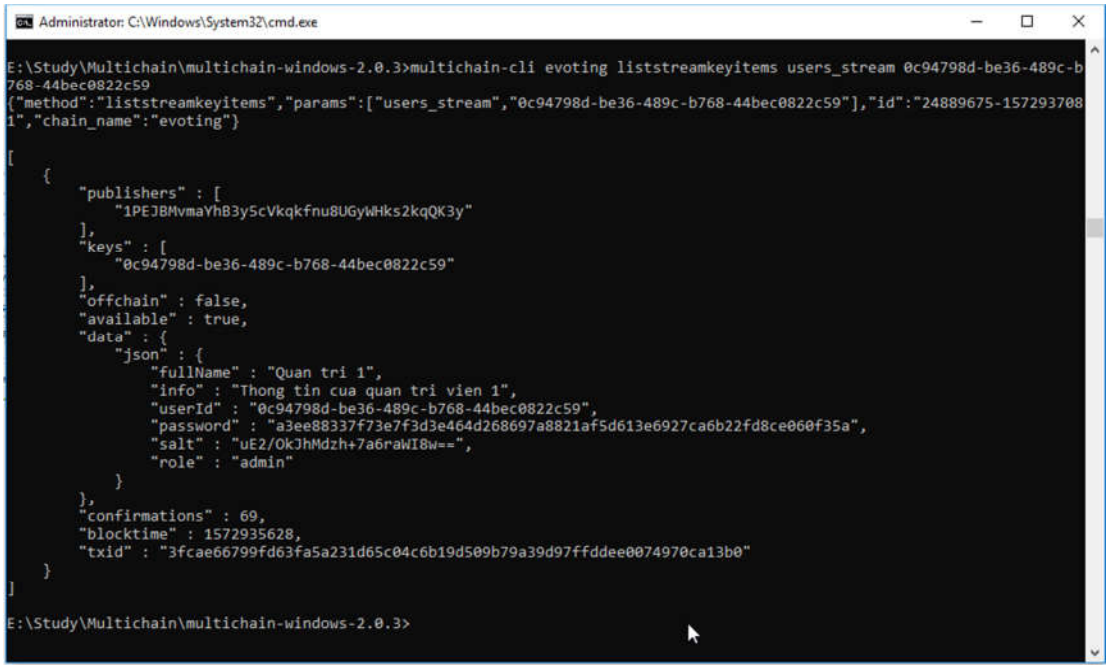
Hình 3.10: Tạo ứng viên



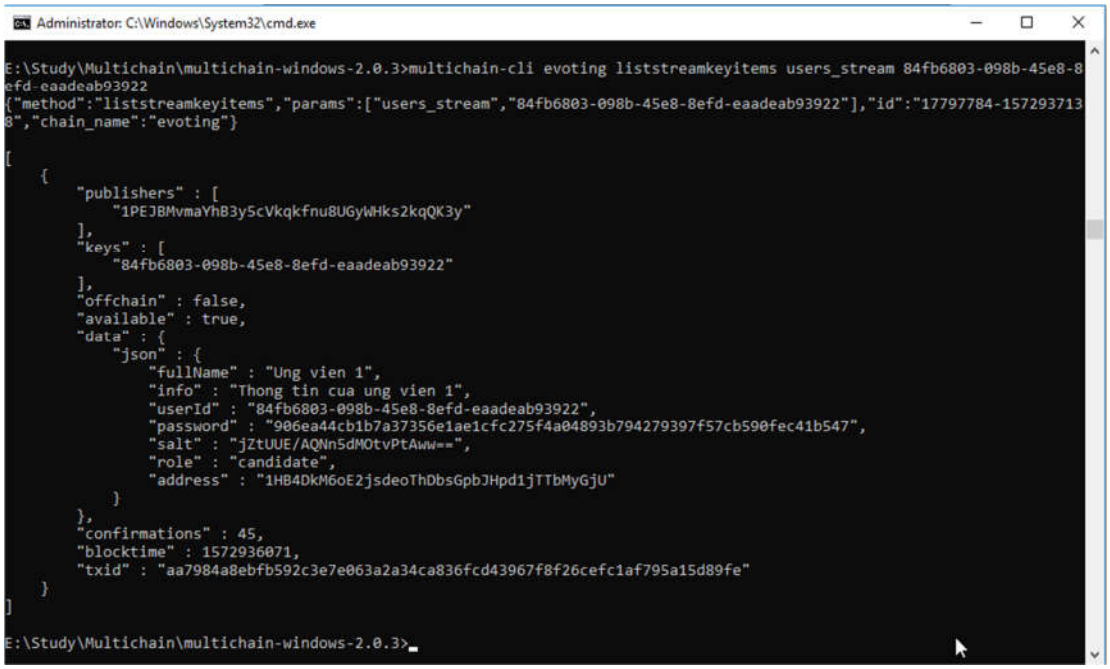
Hình 3.11: Tạo cử tri



Hình 3.12: Gửi phiếu bầu cho cử tri

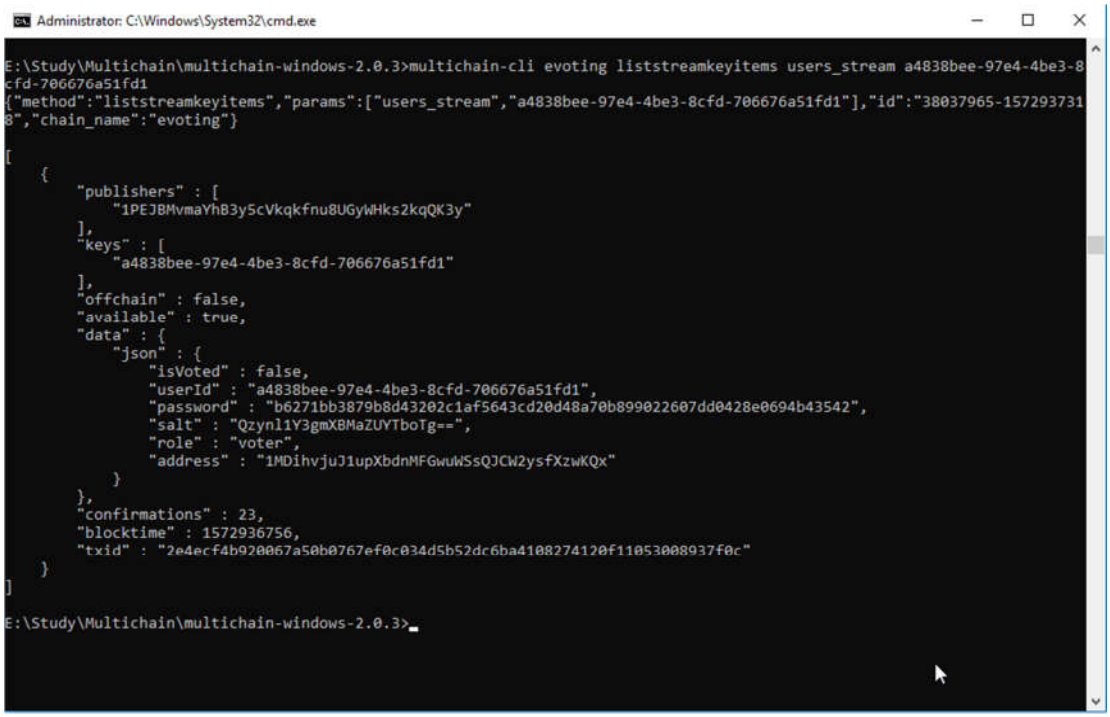


Hình 3.13: Xem thông tin quản trị viên

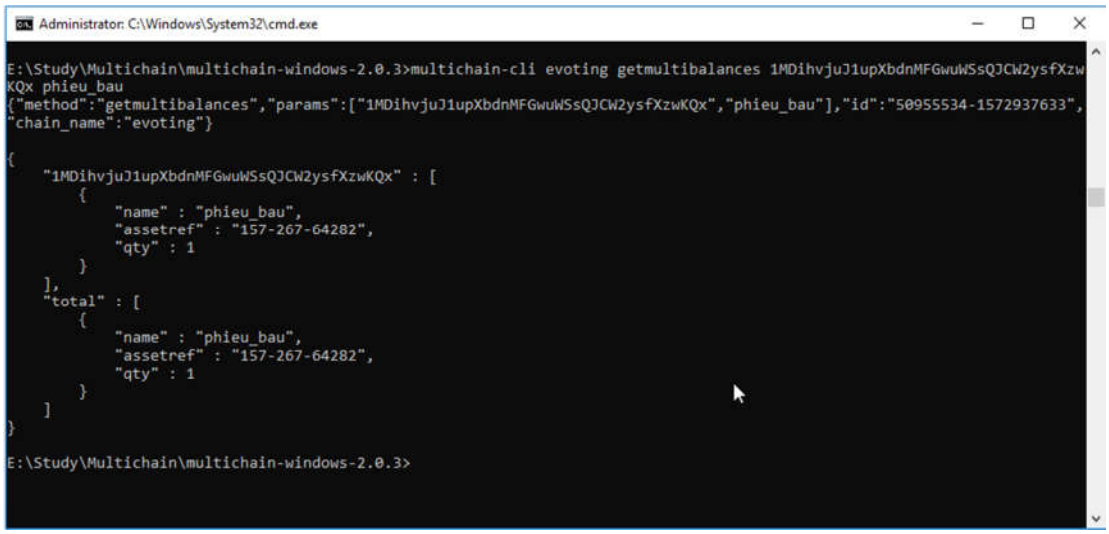


Hình 3.14: Xem thông tin ứng viên

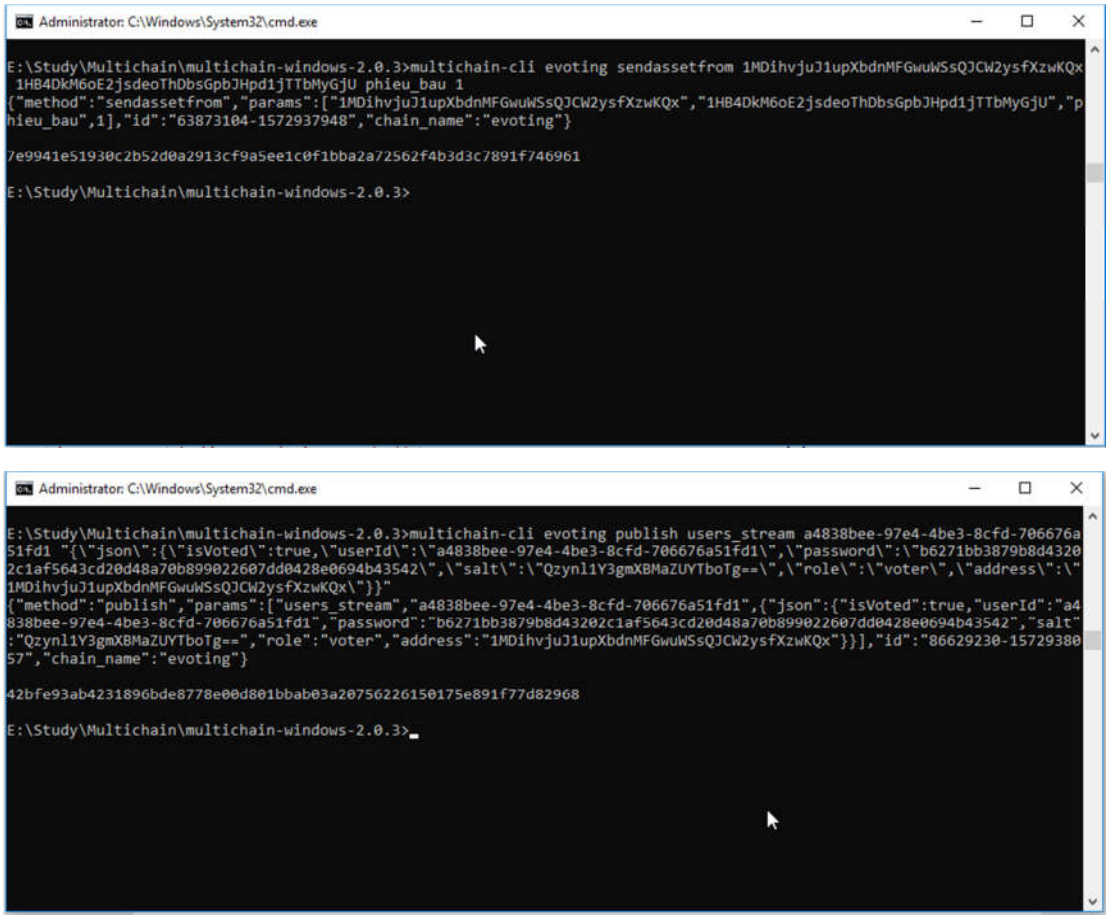
Hình 3.15: Kiểm tra số lượng phiếu bầu của ứng viên



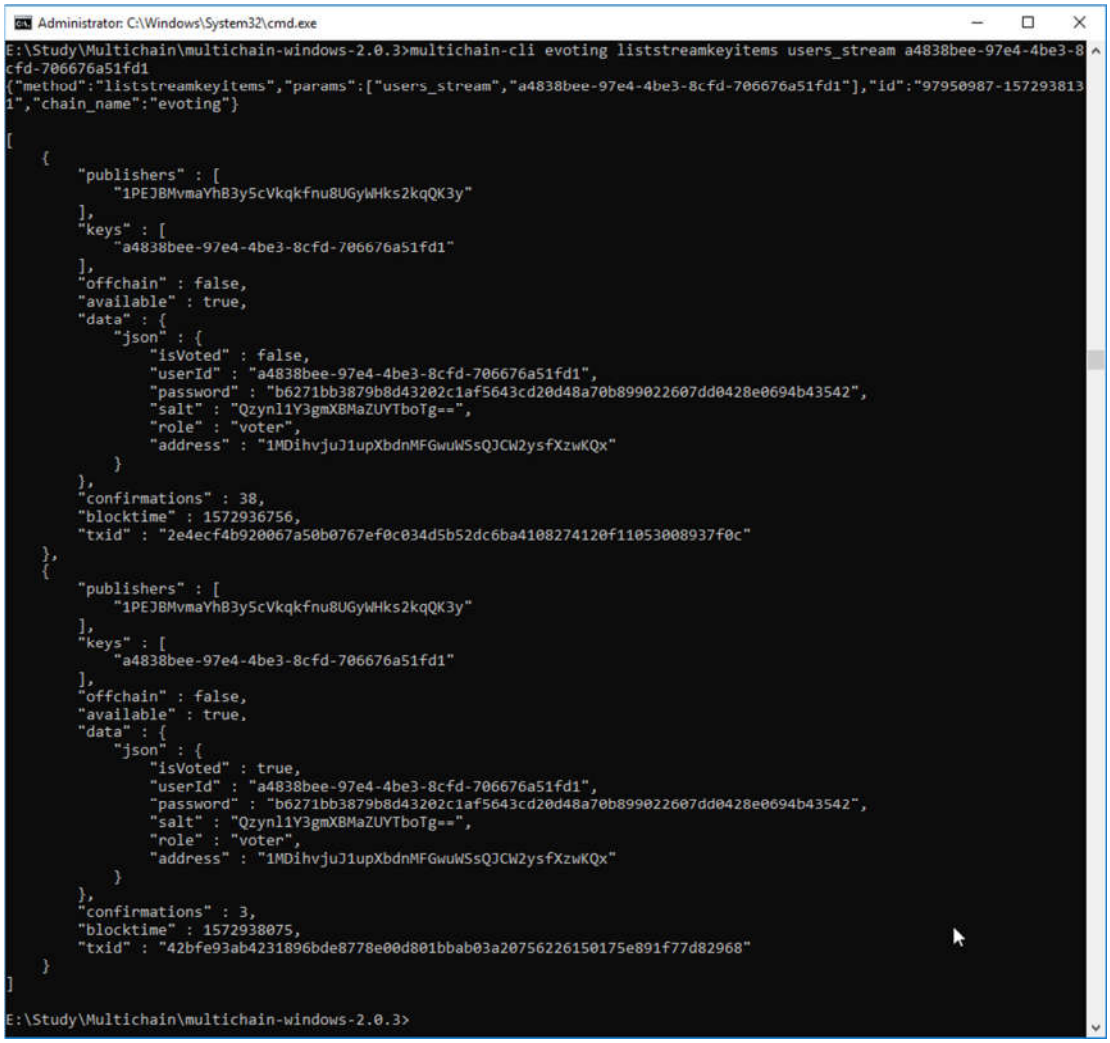
Hình 3.16: Xem thông tin của cử tri

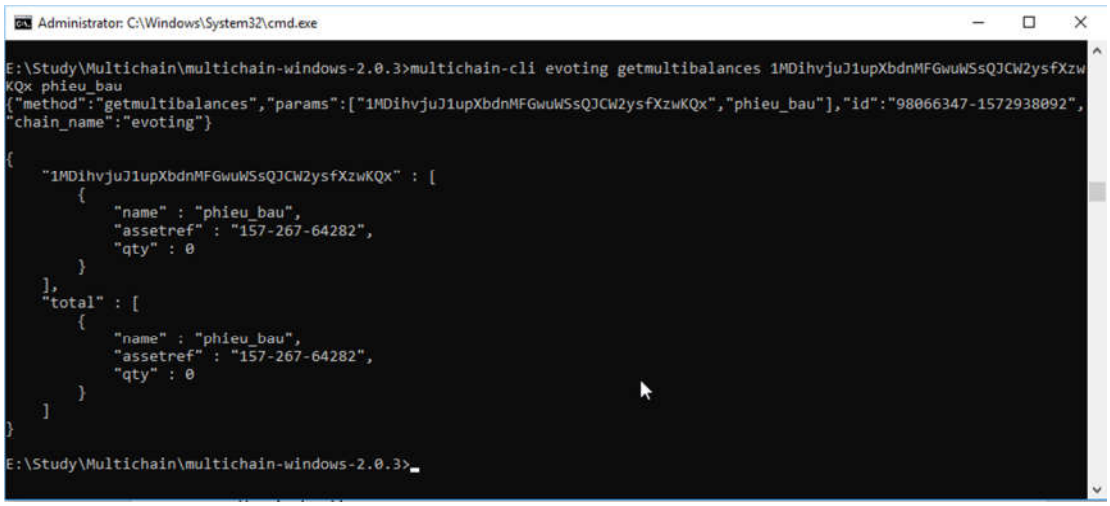


Hình 3.17: Lấy thông tin số lượng phiếu bầu của cử trị



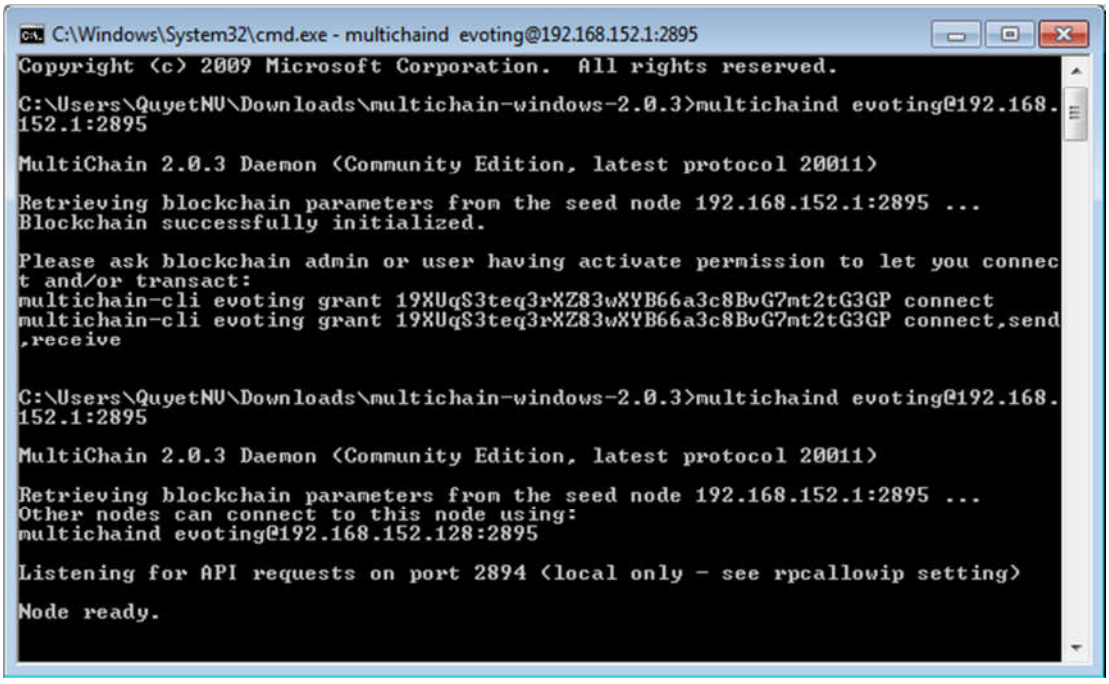
Hình 3.18: Cử tri thực hiện bỏ phiếu và cập nhật trạng thái bỏ phiếu cho cử tri





Hình 3.19: Kiểm tra lại thông tin cử tri sau khi đã bỏ phiếu

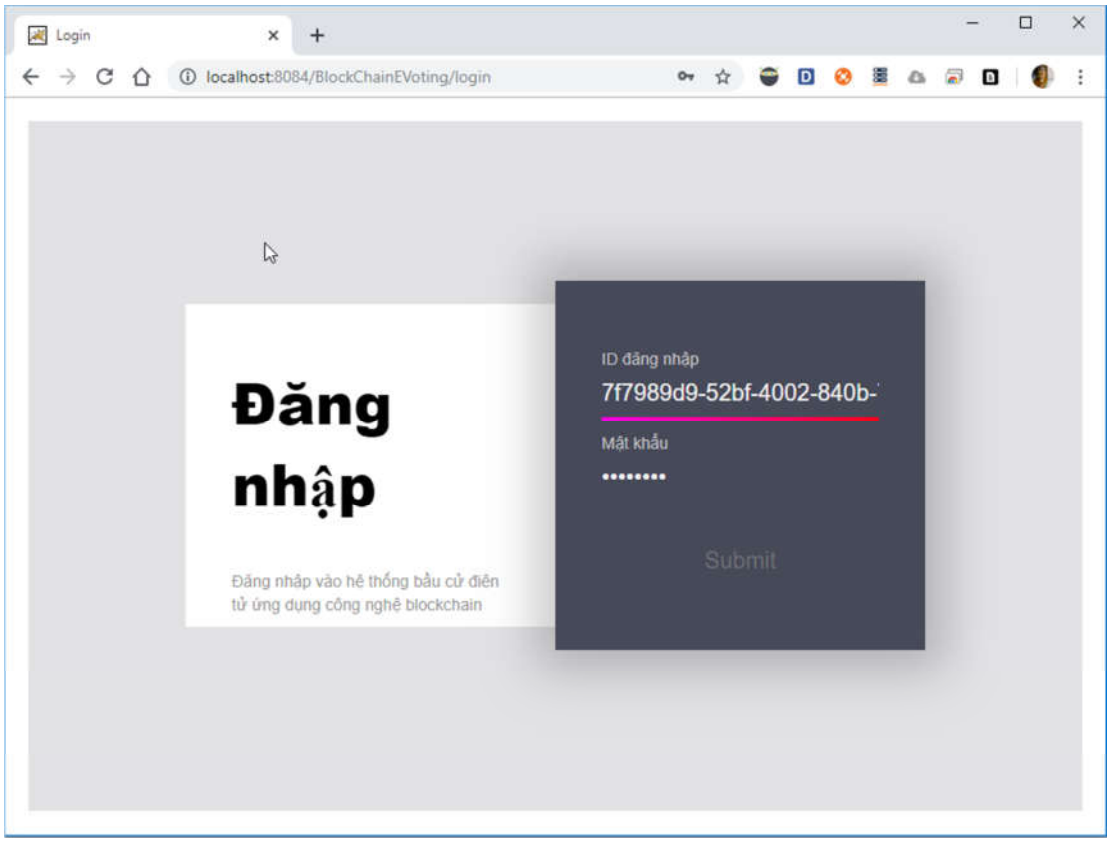
Hình 3.20: Lấy thông tin số lượng phiếu bầu của ứng viên



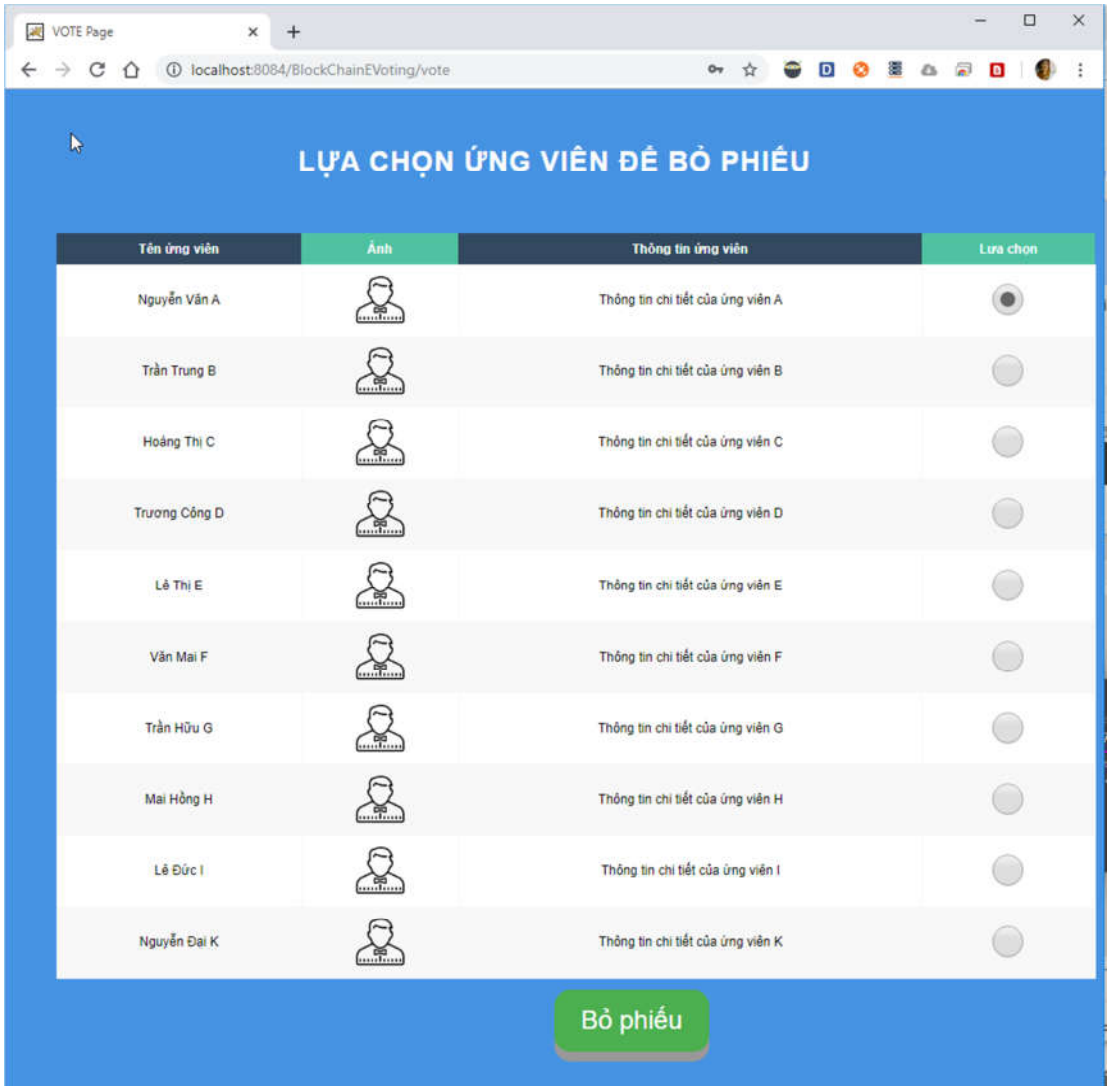
Hình 3.21: Kết nối nút mới vào mạng blockchain hiện có

3.3. Xây dựng mô hình và kịch bản thử nghiệm

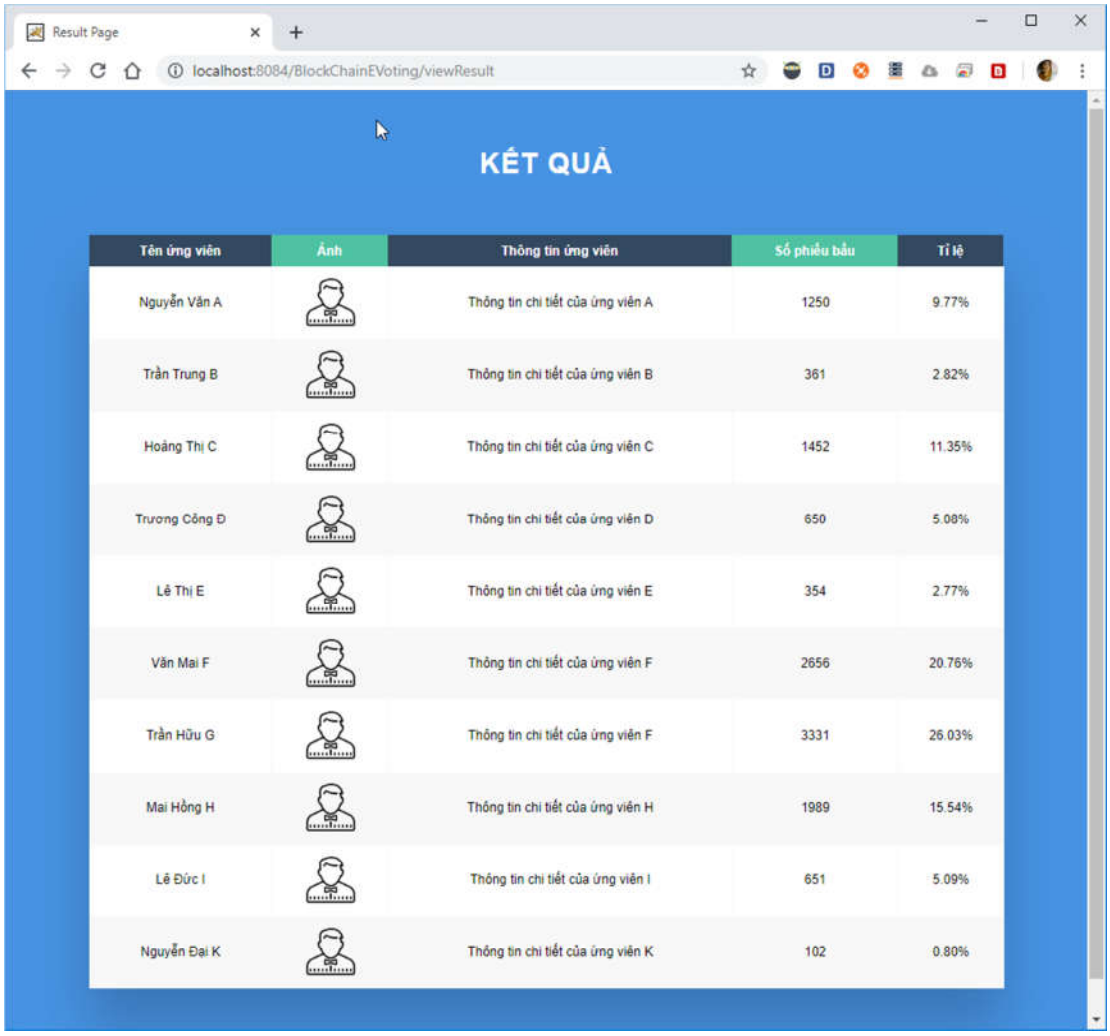
Sau khi triển khai hệ thống, luận văn đã thử nghiệm việc bỏ phiếu (vai trò của cử tri) và tổng hợp kết quả (vai trò của quản tri viên) và đạt được kết quả như sau:



Hình 3.22: Đăng nhập hệ thống



Hình 3.23: Tiến hành bỏ phiếu



Hình 3.24: Tổng hợp kết quả

Để đánh giá hiệu năng của hệ thống, luận văn đã tiến hành thử nghiệm việc gửi yêu cầu lấy dữ liệu (request get data) và yêu cầu tạo dữ liệu (request put data) lần lượt trên hệ thống blockchain với 1 nút và 2 nút như sau:

- Luận văn viết đoạn script giả lập (chạy multithread) để tạo ra số lượng yêu cầu cần thiết.
- Yêu cầu lấy dữ liệu (request get data): Luận văn thực hiện yêu cầu lấy tổng số phiếu bầu mà ứng viên đang sở hữu (Số phiếu mà ứng viên được bầu).
- Yêu cầu tạo dữ liệu (request put data): Luận văn thực hiện yêu cầu gửi phiếu bầu từ địa chỉ ví của cử tri đến địa chỉ ví của ứng viên (Thực hiện bỏ phiếu).

- Tổng số yêu cầu: Là số lượng thread được tạo ra để chạy thực nghiệm.
- Thời gian trung bình xử lý yêu cầu (ms): Là trung bình cộng của thời gian xử lý mỗi yêu cầu.
- Số lượng yêu cầu được xử lý trên giây: Là số yêu cầu mà hệ thống có thể xử lý được trong 1 giây (Do các yêu cầu có thể được xử lý đồng thời).
- Thời gian trung bình xác nhận giao dịch (ms): Là trung bình cộng của thời gian xác nhận mỗi yêu cầu.

Dưới đây là một số kết quả thực nghiệm:

Bảng 3.5: Thực nghiệm gửi yêu cầu lấy dữ liệu trên hệ thống blockchain với 1 nút

Tổng số yêu cầu	Thời gian trung bình xử lý yêu cầu (ms)	Số lượng yêu cầu được xử lý trên giây
10	296.91	33.56
50	371.3	120.19
100	419.2	198.81
500	1033.69	299.4
1000	971.79	31.73
5000	6084.33	113.34
10000	11838.36	181.31

Bảng 3.6: Thực nghiệm gửi yêu cầu tạo dữ liệu trên hệ thống blockchain với 1 nút

Tổng số yêu cầu	Thời gian trung bình xử lý yêu cầu (ms)	Số lượng yêu cầu được xử lý trên giây	Thời gian trung bình xác nhận giao dịch (ms)
10	108.32	12.87	4.6
50	221.72	74.96	3.58
100	369.28	96.71	7.95
500	2173.59	93.46	16.53

1000	64730.7	7.85	8.94
5000	483365.43	5.03	8.62
10000	1642601.62	2.91	8.29

Bảng 3.7: Thực nghiệm gửi yêu cầu lấy dữ liệu trên hệ thống blockchain với 2 nút

Tổng số yêu cầu	Thời gian trung bình xử lý yêu cầu (ms)	Số lượng yêu cầu được xử lý trên giây
10	298.21	32.01
50	380	117.37
100	448.63	186.92
500	1119.44	302.66
1000	1102.32	32.54
5000	4528.08	99.64
10000	11686.45	78.77

Bảng 3.8: Thực nghiệm gửi yêu cầu tạo dữ liệu trên hệ thống blockchain với 2 nút

Tổng số yêu cầu	Thời gian trung bình xử lý yêu cầu (ms)	Số lượng yêu cầu được xử lý trên giây	Thời gian trung bình xác nhận giao dịch (ms)
10	114.42	12.34	17.77
50	237.13	75.58	4.72
100	342.15	91.53	20.88
500	2256.12	90.14	22.73
1000	65567.43	7.12	8.64
5000	491322.42	4.52	9.95
10000	1698271.32	2.89	8.85

3.4. Một số kết quả, nhận xét và đánh giá

Trong thực tế, hệ thống bầu cử điện tử có thể bị tấn công bất kỳ lúc nào. Luận văn đưa ra một vài tình huống giả định mà hệ thống có thể bị tấn công và cách thức chống tấn công của hệ thống như sau:

- Hacker giả mạo ID của cử tri để xâm nhập vào hệ thống: Để có thể xâm nhập vào hệ thống, hacker cần có mã ID của cử tri (là một 32 ký tự bất kỳ), nếu dùng phương pháp thử, hacker cần tối đa 36^{32} lần thử, trong trường hợp tìm ra được ID của cử tri, hacker cũng cần phải tìm ra khẩu tương ứng. Ngoài ra, hacker cũng có thể tự sinh ra một chuỗi ID bất kỳ gồm 32 ký tự và thử đăng nhập vào hệ thống. Tuy nhiên, danh sách ID được quản lý trong blockchain và nếu ID mà hacker tự sinh không tồn tại trong blockchain thì hệ thống sẽ từ chối truy cập. Như vậy, việc giả mạo ID của cử tri để xâm nhập vào hệ thống là rất khó khăn.
- Quản trị viên cố tình vào theo dõi xem cử tri đã bỏ phiếu cho ai: Việc này là không thể, do hệ thống không lưu thông tin cá nhân của cử tri. Quản trị viên chỉ có thể xem được phiếu bầu đã được gửi từ địa chỉ (tương ứng với ID) của cử tri đến địa chỉ nào cử ứng viên mà thôi. Việc truy xuất ra thông tin cử tri là không thể.
- Quản trị viên cố tình đăng nhập bằng ID của cử tri để thực hiện bỏ phiếu: Quản trị viên có thể xem được ID của cử tri. Tuy nhiên mật khẩu lưu trong blockchain đã được mã hóa bằng thuật toán SHA256 và có sử dụng salt. Việc nhìn thấy mật khẩu mã hóa không thể giúp cho cử tri có thể dịch ngược ra mật khẩu thực sự của cử tri.

Sau khi xây dựng hệ thống bầu cử điện tử ứng dụng công nghệ blockchain, luận văn đã thực hiện so sánh giữa 3 mô hình bầu cử: bầu cử truyền thống, bầu cử điện tử (Client-Server), bầu cử điện tử ứng dụng blokchain. Kết quả được thể hiện ở bảng dưới đây:

Bảng 3.9: So sánh các hình thức bầu cử

Nội dung so sánh	Bầu cử truyền thống	Bầu cử điện tử (Client – Server)	Bầu cử điện tử (Blockchain)
Thiết bị sử dụng	Giấy và Hòm bỏ phiếu	Máy chủ và thiết bị điện tử có sử dụng Internet	Máy chủ và thiết bị điện tử có sử dụng Internet
Chi phí	Cao (Chi phí giấy và nhân công)	Thấp (Chỉ tốn chi phí triển khai ban đầu)	Thấp (Chỉ tốn chi phí triển khai ban đầu)
Quy mô	Phụ thuộc vào kích thước hòm bỏ phiếu	Dễ dàng mở rộng ở quy mô lớn	Dễ dàng mở rộng ở quy mô lớn
Tổng hợp kết quả	Khó khăn và tốn nhân công	Dễ dàng	Dễ dàng
Bảo mật cho cử tri	Đảm bảo	Không đảm bảo	Đảm bảo
Nguy cơ tấn công	Không sợ bị tấn công	Có thể tấn công vào máy chủ và thay đổi kết quả	Xác suất tấn công và thay đổi đổi kết quả là rất nhỏ

Như vậy, luận văn đã đưa ra mô hình ứng dụng công nghệ blockchain cho bầu cử điện tử, đồng thời cũng đã xây dựng mô hình thực nghiệm sử dụng JavaEE và Multichain làm nền tảng. Mô hình đã chứng minh được tính ứng dụng để có thể thay thế mô hình bầu cử bằng giấy truyền thống và cũng đưa ra được các điểm mấu chốt để đảm bảo an toàn so với mô hình bầu cử điện tử hiện tại (Client-Server).

Tuy nhiên, luận văn mới chỉ dừng lại ở việc thử nghiệm 2 nút mạng blockchain và 1 web server. Trong tương lai, luận văn mong muốn có điều kiện để có thể mở rộng hệ thống và đưa vào ứng dụng thực tế.

KẾT LUẬN

Luận văn tập trung nghiên cứu về bầu cử và ứng dụng công nghệ blockchain cho bầu cử điện tử. Cụ thể, luận văn đã đạt được một số kết quả sau:

- Tìm hiểu về bầu cử, bầu cử truyền thống và bầu cử điện tử theo mô hình cũ (Client – Server)
- Tìm hiểu, nghiên cứu về blockchain và khả năng ứng dụng blockchain cho bầu cử điện tử
- Đưa ra mô hình thử nghiệm với nền tảng Multichain và đã đạt được một số kết quả nhất định

Luận văn có thể tiếp tục phát triển theo hướng sau:

Tìm hiểu thêm các nền tảng blockchain khác, mở rộng số lượng nút trong mạng lưới blockchain và số lượng web server để có thể đưa vào ứng dụng trong thực tế.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Ánh Ngọc, "Hơn 90 nhân viên kiểm phiếu tử vong vì kiệt sức trong cuộc bầu cử Indonesia," *vnexpress*, 2019. [Online]. Available: https://vnexpress.net/the-gioi/hon-90-nhan-vien-kiem-phieu-tu-vong-vi-kiet-suc-trong-cuoc-bau-cu-indonesia-3913896.html. [Accessed: 28-Jul-2019].

[2] L.K.Tùng, "Hỏi - Đáp: ABC về bầu cử," *Nhà xuất bản Hồng Đức*, 2016.

[3] PGS.TS. Nguyễn Quốc Sửu, "Bầu cử ở Việt Nam – Những nội dung cần quan tâm," *Quản lý nhà nước*, 2019. [Online]. Available: https://www.quanlynhanuoc.vn/2019/08/01/bau-cu-o-viet-nam-nhung-noi-dung-can-quan-tam/. [Accessed: 30-Aug-2019].

[4] Wikipedia, "Blockchain," *Wikipedia*, 2019. [Online]. Available: https://vi.wikipedia.org/wiki/Blockchain. [Accessed: 25-Sep-2019].

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *J. Gen. Philos. Sci.*, vol. 39, no. 1, pp. 53–67, 2008.

[6] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.

[7] A. Tar, "Smart Contracts, Explained," *Cointelegraph*, 2017. [Online]. Available: https://cointelegraph.com/explained/smart-contracts-explained. [Accessed: 26-Sep-2019].

[8] W. Stallings and M. J. Horton, *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION British Library Cataloguing-in-Publication Data*. .

[9] M. Sumagita and I. Riadi, "Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application," vol. 7, no. 4, pp. 373–381, 2018.

[10] Dang Minh Tuan, "Tổng quan về blockchain." 2019.

[11] A. Kujawa, “Bitcoins, Pools and Thieves,” *Malwarebytes lab blog*, 2016. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2013/11/bitcoins-pools-and-thieves/. [Accessed: 30-Sep-2019].

[12] A. Schneider, C. Meter, and P. Hagemeister, “Survey on Remote Electronic Voting,” 2017.

[13] L. Fouard, M. Duclos, and P. Lafourcade, “Survey on electronic voting schemes,” *Support. by ANR …*, 2007.

[14] R. Verbij, “Dutch e-voting opportunities,” *EEMCS Univ. Twente*, vol. 8, no. 33, p. 44, 2014.

[15] C. S. L. Dr Gideon Greenspan, Founder and CEO, “MultiChain Private Blockchain — White Paper,” *Web*, vol. 29, no. 3, pp. 274–279, 2002.

[16] Gideon Greenspan, “MultiChain 1.0 beta 2 and 2.0 roadmap,” *MultiChain*, 2017. [Online]. Available: https://www.multichain.com/blog/2017/06/multichain-1-beta-2-roadmap/. [Accessed: 02-Oct-2019].

[17] Multichain, “MultiChain JSON-RPC API commands,” *Multichain*, 2019. [Online]. Available: https://www.multichain.com/developers/json-rpc-api/. [Accessed: 20-Aug-2019].

[18] SimplyUb, “MultichainJavaAPI,” *Github*, 2019. [Online]. Available: https://github.com/SimplyUb/MultiChainJavaAPI. [Accessed: 01-Oct-2019].