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

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: Tiến sĩ Đặng Minh Tuấn

Phản biện 1: Tiến sĩ Phùng Văn Ổn

Phản biện 2: Tiễn sĩ Nguyễn Trọng Đường

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 09 giờ 00 ngày 11 tháng 01 năm 2020

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỤC LỤC

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 không mất quá trình vận chuyển 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).

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.

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

1.2. Giới thiệu về bầu cử truyền thống

1.2.1. Mô hình triển khai

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

a. Ưu điểm

b. Nhược điểm

1.3. Giới thiệu về bầu cử điện tử

1.3.1. Mô hình triển khai

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

a. Ưu điểm

b. Nhược điểm

1.4. Kết luận chương

Chương này đã giới thiệu khái quát về bầu cử nói chung và bầu cử tại Việt Nam. 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.

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).

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 luợng 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 luu trữ mãi mãi.
- Bảo mật: Các thông tin, dữ liệu trong blockchain đuợc phân tán và an toàn tuyệt đối.
- Minh bạch

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.

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

- 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.

b. Nguyên tắc hoạt động

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.

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

- 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 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

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.

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

c. Bài toán

d. 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
- Giai đoạn 2: Bỏ phiếu
- Giai đoạn 3: Tổng hợp kết quả

e. Chứng minh tính đúng đắn

f. Chứng minh tính an toàn

- Tính riêng tư của dữ liệu
- Tính bảo mật cho cử tri
- Gian lận trong hệ thống

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

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 dựng ứng dụng web, luận văn đề xuất sử dụng JavaEE.

3.3. Xây dựng mô hình và kịch bản thử nghiệm

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

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].