

Xem các cuộc thảo luận, số liệu thống kê và hồ sơ tác giả cho ấn phẩm này tại: <https://www.researchgate.net/publication/370128892>

Triển khai hệ thống bỏ phiếu điện tử phi tập trung dựa trên chuỗi khối Công nghệ

Điều · Tháng 4 năm 2023

DOI: 10.37896/jxu17.4/027

TRÍ CHỈ DẪN

0

ĐỌC

101

4 tác giả:



Sayon Chakraborty

Đại học Sharda

1 CÔNG BỐ 0 TRÍ CHỈ DẪN

XEM HỒ SƠ



Anupam Abhay

Đại học Sharda

1 CÔNG BỐ 0 TRÍ CHỈ DẪN

XEM HỒ SƠ



Vishwas Srivastava

Đại học Sharda

1 CÔNG BỐ 0 TRÍ CHỈ DẪN

XEM HỒ SƠ



Avjeet Singh

Viện Công nghệ Quốc gia Motilal Nehru

17 CÔNG BỐ 16 TRÍ CHỈ DẪN

XEM HỒ SƠ

Một số tác giả của ấn phẩm này cũng đang thực hiện các dự án liên quan sau:



thuật toán tối ưu Xem dự án



Tối ưu hóa Xem dự án

Triển khai hệ thống bỏ phiếu điện tử phi tập trung Dựa trên công nghệ chuỗi khối

Sayon Chakraborty¹, Anupam Abhay², Vishwas Srivastav³, Avjeet Singh⁴

^{1,2,3,4}Trường Kỹ thuật & Công nghệ,
Đại học Sharda Gr. Noida, Uttar Pradesh, Ấn Độ

Tóm tắt – Bầu cử là quyền cơ bản của mọi công dân trong một nền dân chủ, cho phép họ lựa chọn những nhà lãnh đạo tương lai của đất nước mình. Các nền tảng bỏ phiếu trực tuyến có thể được sử dụng để tiến hành bỏ phiếu và bầu cử một cách an toàn. Họ loại bỏ sự cần thiết của lá phiếu giấy và bỏ phiếu trực tiếp vì họ là một nền tảng kỹ thuật số. Họ cũng cấm cử tri bỏ phiếu nhiều lần để bảo toàn tính hợp lệ của lá phiếu của bạn. Bỏ phiếu điện tử, đôi khi được gọi là "bỏ phiếu điện tử", có nhiều ưu điểm hơn so với các hệ thống trên giấy, bao gồm hiệu quả cao hơn và ít sai sót hơn. Khả năng bỏ phiếu từ bất kỳ vị trí nào và trên bất kỳ thiết bị kết nối internet nào giúp hệ thống bỏ phiếu điện tử tối đa hóa mức độ tương tác của người dùng. Chuỗi khối là một công nghệ mới được phát triển, phi tập trung và phân tán với nền tảng mã hóa vững chắc có tiềm năng nâng cao nhiều doanh nghiệp theo nhiều cách khác nhau. Các vấn đề hiện tại với bỏ phiếu điện tử có thể được giải quyết bằng cách kết hợp công nghệ chuỗi khối. Ở đây, chúng tôi đề xuất một hệ thống bỏ phiếu dựa trên chuỗi khối sẽ giảm gian lận bỏ phiếu và hợp lý hóa, bảo mật và hợp lý hóa quy trình bỏ phiếu.

Từ khóa– Dân chủ, Bỏ phiếu, Bầu cử, Lá phiếu, Bỏ phiếu điện tử, Phi tập trung, Mật mã học, Chuỗi khối

I. GIỚI THIỆU

Thật vậy, việc sử dụng các công nghệ kỹ thuật số, bao gồm cả các công cụ bỏ phiếu trực tuyến, có khả năng tăng cường quá trình dân chủ ở Ấn Độ bằng cách giúp người dân bỏ phiếu thuận tiện hơn và dễ tiếp cận hơn. Aadhaar, hệ thống nhận dạng duy nhất ở Ấn Độ, đã cho phép nhiều công dân tham gia vào sáng kiến Ấn Độ kỹ thuật số, bao gồm việc sử dụng các phương thức bỏ phiếu điện tử. Một trong những ưu điểm của các công cụ bỏ phiếu trực tuyến là loại bỏ các lá phiếu giấy, có thể giảm chi phí, tiết kiệm thời gian và giảm thiểu khả năng xảy ra sai sót khi kiểm phiếu. Máy bỏ phiếu điện tử (EVM) đã được sử dụng ở Ấn Độ trong nhiều năm để tiến hành bầu cử và chúng đã hợp lý hóa quy trình bỏ phiếu bằng cách tự động kiểm phiếu và giảm can thiệp thủ công. Hơn nữa, các công cụ bỏ phiếu trực tuyến có thể nâng cao hiệu quả bằng cách cho phép cử tri bỏ phiếu từ bất kỳ địa điểm nào và trên bất kỳ thiết bị kết nối internet nào, điều này có thể tăng cường sự tham gia và tương tác của cử tri. Điều này đặc biệt phù hợp ở một quốc gia rộng lớn và đa dạng như Ấn Độ, nơi khoảng cách vật lý và khả năng di chuyển có thể là thách thức đối với một số công dân. Việc sử dụng các công cụ bỏ phiếu trực tuyến cũng có thể giúp cải thiện tính chính xác và minh bạch trong quá trình bỏ phiếu. Hồ sơ kỹ thuật số của các phiếu bầu có thể được lưu trữ an toàn và có thể được kiểm toán và xác minh, điều này có thể nâng cao tính toàn vẹn của kết quả bầu cử. Ngoài ra, các công cụ bỏ phiếu trực tuyến có thể mang đến cơ hội theo dõi và phát hiện những điểm bất thường hoặc gian lận trong thời gian thực, cải thiện tính minh bạch tổng thể của quy trình bỏ phiếu.

Tuy nhiên, điều quan trọng là phải đảm bảo rằng việc sử dụng các công cụ bỏ phiếu trực tuyến là an toàn, đáng tin cậy và toàn diện. Cần thực hiện các biện pháp thích hợp để bảo vệ chống lại các mối đe dọa an ninh mạng tiềm ẩn, chẳng hạn như hack hoặc giả mạo phiếu bầu. Cần có cơ chế xác thực và ủy quyền mạnh mẽ để đảm bảo tính toàn vẹn của quy trình bỏ phiếu và ngăn chặn truy cập trái phép. Ngoài ra, cần nỗ lực giải quyết các vấn đề về quyền truy cập và tính toàn diện cho tất cả các cử tri đủ điều kiện, kể cả những người không có quyền truy cập vào các thiết bị kết nối internet hoặc có thể gặp khó khăn khi sử dụng công nghệ kỹ thuật số. Tóm lại, việc sử dụng các công cụ bỏ phiếu trực tuyến ở Ấn Độ có khả năng tăng cường quy trình dân chủ bằng cách làm cho việc bỏ phiếu trở nên thuận tiện, hiệu quả và minh bạch hơn. Tuy nhiên, điều quan trọng là phải đảm bảo rằng các biện pháp thích hợp được áp dụng để giải quyết các mối lo ngại về an ninh và đảm bảo tính toàn diện, liêm chính và minh bạch trong quá trình bỏ phiếu.

1.1 chuỗi khối

Công nghệ chuỗi khối có khả năng cách mạng hóa hệ thống bỏ phiếu điện tử bằng cách cung cấp tính bảo mật, tính minh bạch và hiệu quả năng cao. Các đặc điểm vốn có của blockchain, chẳng hạn như

tính bất biến, phân cấp và ra quyết định dựa trên sự đồng thuận, làm cho nó trở thành một công nghệ đầy hứa hẹn để xây dựng một hệ thống bỏ phiếu điện tử mạnh mẽ và đáng tin cậy. Một trong những lợi thế chính của việc sử dụng chuỗi khối để bỏ phiếu điện tử là khả năng cung cấp một bản ghi minh bạch và chống giả mạo của tất cả các giao dịch. Khi một phiếu bầu được ghi lại trên chuỗi khối, nó không thể bị thay đổi, xóa hoặc giả mạo, đảm bảo tính toàn vẹn của quá trình bỏ phiếu. Bản chất phân tán của chuỗi khối, với nhiều nút được kết nối với nhau xác thực các giao dịch, khiến nó có khả năng chống hack hoặc thao túng cao. Hơn nữa, các hệ thống bỏ phiếu điện tử dựa trên chuỗi khối có thể nâng cao tính minh bạch bằng cách cho phép tất cả các bên liên quan, bao gồm cử tri, ứng cử viên và cơ quan bầu cử, xác minh kết quả một cách độc lập. Bản chất phi tập trung của chuỗi khối đảm bảo rằng không có thực thể đơn lẻ nào có quyền kiểm soát toàn bộ hệ thống, giảm khả năng sai lệch hoặc thao túng.

Chuỗi khối cũng có thể cải thiện hiệu quả của quy trình bỏ phiếu bằng cách giảm chi phí hành chính và chi phí liên quan đến các hệ thống bỏ phiếu dựa trên giấy truyền thống. Việc tự động kiểm phiếu và xác minh kết quả có thể giảm đáng kể sai sót của con người và đẩy nhanh quá trình công bố kết quả. Ngoài ra, các hệ thống bỏ phiếu điện tử dựa trên chuỗi khối có khả năng tăng cường sự tham gia của cử tri bằng cách cung cấp các tùy chọn bỏ phiếu thuận tiện và dễ tiếp cận hơn. Cử tri có thể bỏ phiếu từ bất kỳ địa điểm nào và trên bất kỳ thiết bị kết nối internet nào, loại bỏ rào cản địa lý và giúp cử tri ở xa hoặc có khó khăn về thể chất tham gia dễ dàng hơn. Tuy nhiên, điều quan trọng cần lưu ý là việc triển khai hệ thống bỏ phiếu điện tử dựa trên chuỗi khối không phải là không có thách thức. Đảm bảo tính bảo mật và quyền riêng tư của thông tin cử tri, giải quyết các vấn đề tiềm ẩn về khả năng mở rộng và cung cấp khả năng tiếp cận cho mọi công dân, kể cả những người không có quyền truy cập vào công nghệ kỹ thuật số, là một số thách thức cần được giải quyết cẩn thận. Công nghệ chuỗi khối có khả năng biến đổi hệ thống bỏ phiếu điện tử bằng cách cung cấp tính bảo mật, minh bạch và hiệu quả nâng cao. Nó có thể cho phép phát triển một hệ thống bỏ phiếu điện tử phi tập trung và đáng tin cậy nhằm thúc đẩy sự tham gia của cử tri ngày càng tăng và niềm tin vào quy trình dân chủ. Tuy nhiên, việc lập kế hoạch cẩn thận, triển khai và giải quyết các thách thức tiềm ẩn là rất quan trọng để đảm bảo sự thành công của hệ thống bỏ phiếu điện tử dựa trên chuỗi khối.

Công nghệ chuỗi khối có tiềm năng cách mạng hóa hệ thống bỏ phiếu điện tử bằng cách tăng cường tính minh bạch, bảo mật và tin cậy trong quy trình. Chuỗi khối là một sổ cái phi tập trung và phân tán, ghi lại các giao dịch theo cách minh bạch và chống giả mạo. Dưới đây là tóm tắt về việc sử dụng chuỗi khối trong hệ thống bỏ phiếu điện tử:

- Tính minh bạch:

Chuỗi khối cho phép ghi lại tất cả các giao dịch một cách minh bạch và có thể kiểm tra được, bao gồm cả phiếu bầu trong hệ thống bỏ phiếu điện tử. Mỗi phiếu bầu được ghi lại dưới dạng một giao dịch trên chuỗi khối và sau khi được ghi lại, nó không thể bị thay đổi hoặc xóa, đảm bảo tính minh bạch và trách nhiệm giải trình.

- Bảo mật: Chuỗi khối cung cấp các tính năng bảo mật mạnh mẽ giúp các bên tránh phép khó thao túng hoặc giả mạo phiếu bầu. Việc sử dụng các kỹ thuật mật mã đảm bảo rằng mỗi phiếu bầu được mã hóa và bảo mật, giảm nguy cơ bị hack và gian lận.
- Phân cấp: Chuỗi khối loại bỏ sự cần thiết của một cơ quan trung ương để giám sát quá trình bỏ phiếu điện tử. Thay vào đó, các phiếu bầu được ghi lại và xác minh bởi một mạng lưới các nút phân tán, khiến nó có khả năng chống lại các điểm lỗi đơn lẻ và giảm nguy cơ gian lận hoặc thao túng bởi một thực thể duy nhất.
- Tính bất biến: Một khi phiếu bầu được ghi trên blockchain, nó sẽ trở nên bất biến, nghĩa là không thể thay đổi hoặc thay đổi. Điều này đảm bảo rằng tính toàn vẹn của phiếu bầu được bảo toàn và ngăn chặn bất kỳ sửa đổi trái phép nào.
- Khả năng truy cập: Chuỗi khối có thể tăng khả năng truy cập vào hệ thống bỏ phiếu điện tử, vì nó có thể được truy cập từ xa, cho phép tham gia rộng rãi hơn và giảm các rào cản như vị trí địa lý hoặc khuyết tật thể chất.

- Tin cậy và có thể kiểm chứng: Chuỗi khối cung cấp mức độ tin cậy và khả năng kiểm chứng cao trong quy trình bỏ phiếu điện tử. Mỗi phiếu bầu có thể được truy ngược lại nguồn gốc và được xác minh, đảm bảo rằng kết quả là chính xác và đáng tin cậy.
- Hiệu quả về chi phí: Chuỗi khối có khả năng giảm chi phí tiến hành bầu cử bằng cách loại bỏ nhu cầu về phiếu bầu bằng giấy, kiểm phiếu thủ công và sự tham gia của các bên trung gian, giúp quá trình này hiệu quả và tiết kiệm chi phí hơn.

Do đó, việc sử dụng chuỗi khối trong hệ thống bỏ phiếu điện tử có khả năng giải quyết nhiều thách thức liên quan đến hệ thống bỏ phiếu truyền thống, chẳng hạn như tính minh bạch, bảo mật và tin cậy, đồng thời có khả năng nâng cao tính toàn vẹn và toàn diện của quy trình bầu cử. Tuy nhiên, điều quan trọng là phải xem xét cẩn thận các tác động kỹ thuật, pháp lý và xã hội của việc triển khai chuỗi khối trong các hệ thống bỏ phiếu điện tử và để đảm bảo rằng các biện pháp thích hợp được đưa ra để giải quyết các mối quan tâm và thách thức tiềm ẩn.

II. KHẢO SÁT VĂN HỌC

Công nghệ kỹ thuật số đã cải thiện đáng kể nhiều khía cạnh trong cuộc sống của mọi người, nhưng các hệ thống bầu cử truyền thống vẫn phụ thuộc nhiều vào giấy tờ, điều này có thể ảnh hưởng đến tính minh bạch và an ninh. Công nghệ chuỗi khối, được biết đến với cấu trúc phi tập trung và cơ sở dữ liệu phân tán, cung cấp một giải pháp tiềm năng cho những vấn đề này. Khái niệm đột phá về chuỗi khối, bắt nguồn từ các loại tiền điện tử như Bitcoin, đang mở ra một kỷ nguyên mới cho internet và các doanh nghiệp trực tuyến. Trong bài báo này, ngôn ngữ lập trình chuỗi khối Ethereum và Solidity đã được sử dụng để phát triển và đánh giá một ứng dụng bỏ phiếu điện tử ví dụ như một hợp đồng thông minh trên mạng Ethereum. Chuỗi khối là một hệ thống an toàn theo thiết kế với khả năng chịu lỗi cao đối với các lỗi của Byzantine, lần đầu tiên được giới thiệu bởi Satoshi Nakamoto (bút danh), người cũng đã phát minh ra chuỗi khối, cùng với khái niệm về hệ thống thanh toán ngang hàng cho phép rút tiền mặt. giao dịch trên internet mà không cần sự tin tưởng hoặc trung gian tài chính [5]-[6].

Bảng 1: Các mô hình có sẵn

S. KHÔNG.	Tên	Khách quan	Thuật toán/Phương pháp	Kết quả
1	R. Tso, et al. [2]	Bỏ phiếu điện tử phi tập trung Hệ thống dựa trên Công nghệ chuỗi khối	Hệ thống bỏ phiếu dựa trên chuỗi khối được phát triển bao gồm bảy thành phần, bao gồm cử tri và hợp đồng thông minh, và được tổ chức thành năm giai đoạn: giai đoạn, giai đoạn đăng ký, giai đoạn bỏ phiếu, giai đoạn thanh toán và phân tích bảo mật.	Cách tiếp cận tận dụng tính minh bạch đồng minh của hợp đồng để cho phép tất cả các cử tri tham gia vào việc ghi và xác minh các lá phiếu. Nó làm tăng niềm tin của cử tri và giảm bầu cử lãng phí tài nguyên.
2	G. Zyskind, et al. [3]	Sử dụng chuỗi khối để bảo vệ dữ liệu cá nhân trong khi phân cấp quyền riêng tư.	Một nền tảng quản lý dữ liệu cá nhân tập trung vào quyền riêng tư đã được xây dựng bằng cách sử dụng kết hợp các kho lưu trữ chuỗi khối và ngoài chuỗi khối.	Cung cấp một nền tảng phi tập trung giúp thu thập, lưu trữ và chia sẻ dữ liệu dễ dàng và an toàn hơn.
3	A. Kosba, [4] Mật mã	dựa trên chuỗi khối và hợp đồng thông minh để bảo vệ quyền riêng tư.	Công nghệ chuỗi khối đã được sử dụng để tạo ra một trình biên dịch có khả năng triển khai mật mã. Chuỗi khối là chương trình được thực thi bởi tất cả thuận.	Nghiên cứu này đã tạo ra trình biên dịch HAWK. Nó có khả năng tạo ra các chương trình điều đầu, có thể được sử dụng để thực hiện mật mã.
4	Y. Dalvi, [5] Hệ thống	bỏ phiếu điện tử sử dụng chuỗi khối	Hệ thống bỏ phiếu điện tử được đề xuất sử dụng mã hóa khóa đối xứng	Hệ thống được xây dựng trên một phân phối địa lý

			<p>thuật toán bảo mật tiến trình.</p> <p>Hệ thống lưu trữ dữ liệu của người dùng trong cơ sở dữ liệu và mã hóa dữ liệu đó bằng thuật toán mã hóa khóa đối xứng để tăng cường bảo mật.</p>	<p>mạng bao gồm cả chính phủ và cơ sở hạ tầng công cộng.</p> <p>Cơ sở hạ tầng phân tán này giúp đảm bảo tính toàn vẹn và bảo mật của hệ thống bỏ phiếu điện tử bằng cách ngăn chặn bất kỳ điểm lỗi đơn lẻ nào và nâng cao tính minh bạch trong quy trình.</p>
5	Ahmed, Md Razu et al. [6]	Việc sử dụng Blockchain trong các hệ thống bỏ phiếu điện tử trong tương lai.	Trong hệ thống bỏ phiếu điện tử dựa trên chuỗi khối được đề xuất, Khối và Chuỗi là hai thành phần chính. Cử tri có thể chọn một lá phiếu và ký tên bằng khóa riêng bằng cách sử dụng ID cử tri duy nhất của họ. Lá phiếu và chữ ký sau đó được xác minh tính toàn vẹn và tính xác thực.	Hệ thống này được thiết kế để trở nên đáng tin cậy và có thể kiểm chứng được, với các biện pháp được áp dụng để ngăn chặn các phiếu bầu trùng lặp. Việc sử dụng quy tắc "chuỗi dài nhất", một cơ chế đồng thuận phổ biến trong công nghệ chuỗi khối, giúp đảm bảo rằng chỉ những phiếu bầu hợp lệ mới được đưa vào.
6	M. Pathak et al. [1]	E dựa trên chuỗi khối hệ thống bỏ phiếu	Cách tiếp cận này đảm bảo rằng các cử tri không có điện thoại di động cũng có thể tham gia vào quá trình bỏ phiếu, đồng thời duy trì tính bảo mật và bảo mật thông tin của họ.	Hệ thống được đề xuất, sử dụng chuỗi khối như một hệ thống bỏ phiếu tập trung. Thông tin của cử tri được mã hóa và thông tin đăng nhập của họ được xác minh trước khi được lưu trữ trong cơ sở dữ liệu an toàn.
7	Friðrik Þ. Hjalmarsson; và cộng sự [7]	Cách tiếp cận bỏ phiếu điện tử sử dụng Blockchain Công nghệ	Một nền tảng quản lý dữ liệu cá nhân tập trung vào quyền riêng tư đã được xây dựng bằng cách sử dụng kết hợp các kho lưu trữ chuỗi khối và ngoài chuỗi khối.	Cung cấp một nền tảng phi tập trung giúp thu thập, lưu trữ và trao đổi dữ liệu để đáng và an toàn hơn. Cũng được đề cập là những phát triển blockchain tiềm năng trong tương lai.
8	R. Manifatunnisa, et al. [số 8]	Dịch vụ hệ thống và Thiết kế hệ thống bỏ phiếu điện tử	Một trình biên dịch có thể triển khai mật mã đã được tạo bằng công nghệ chuỗi khối. Tất cả các nút đồng thuận trên chuỗi khối đều chạy phần mềm, tuy nhiên người quản lý là một thực thể riêng biệt hỗ trợ việc thực hiện các hợp đồng Hawk.	Cách tiếp cận này đã sử dụng trình biên dịch hawk. Bạn có thể sử dụng nó để tạo các ứng dụng mới triển khai mật mã. Blockchain được trình biên dịch sử dụng để chạy các ứng dụng trong nhiều giai đoạn khác nhau.
9	R. Taş, [11]	Một cuộc kiểm tra toàn diện về những khó khăn và triển vọng của blockchain đối với việc bỏ phiếu điện tử.	Phân tích tập trung vào việc đánh giá bối cảnh hiện tại của các hệ thống bỏ phiếu dựa trên chuỗi khối, mục tiêu là đánh giá tình trạng hiện tại và dự báo sự phát triển trong tương lai trong lĩnh vực hệ thống bỏ phiếu điện tử dựa trên chuỗi khối.	Làm nổi bật tầm quan trọng của mật mã đối xứng và bất đối xứng trong quá trình phát triển của các hệ thống chuỗi khối, nhấn mạnh vai trò của chúng trong việc phát triển các hệ thống minh bạch và bỏ phiếu điện tử.

Bỏ phiếu điện tử có khả năng thu hút dân số trẻ, am hiểu công nghệ vào quá trình dân chủ. Một tùy chọn để nâng cao tính minh bạch, cởi mở và khả năng kiểm toán trong bỏ phiếu điện tử là tận dụng công nghệ chuỗi khối. Tuy nhiên, điều quan trọng là phải thừa nhận rằng công nghệ chuỗi khối có những hạn chế có thể cản trở tiềm năng đầy đủ của nó [7]. Trong những năm qua, bỏ phiếu điện tử đã được sử dụng dưới nhiều hình thức khác nhau kể từ những năm 1970, mang lại những lợi thế như tăng hiệu quả và giảm sai sót so với các phương pháp trên giấy [8]. Nhiều nỗ lực đã được thực hiện để khám phá việc sử dụng công nghệ chuỗi khối như một giải pháp cho bỏ phiếu điện tử hiệu quả, tận dụng nền tảng mật mã và minh bạch của nó. Một sáng kiến như vậy được mô tả trong nghiên cứu đã triển khai phương pháp được đề xuất bằng cách sử dụng Multichain và tiến hành phân tích toàn diện để chứng minh tính hiệu quả của nó trong việc đáp ứng các điều kiện thiết yếu của hệ thống bỏ phiếu điện tử [9]. Quản lý danh tính kỹ thuật số an toàn là một thách thức kỹ thuật quan trọng trong các hệ thống bỏ phiếu điện tử, mặc dù đây không phải là thách thức duy nhất. Việc đăng ký các công dân tương lai với hệ thống bầu cử nên được xử lý dễ dàng bằng kỹ thuật số, với thông tin nhận dạng của họ được giữ kín hoàn toàn. Các hệ thống bỏ phiếu lỗi thời gặp phải các vấn đề như bỏ phiếu ẩn danh không an toàn, thiếu quy trình bỏ phiếu được cá nhân hóa, không có xác minh Aadhaar, chi phí thiết lập cao, lo ngại về bảo mật, thiếu minh bạch và tin cậy, bỏ phiếu không hiệu quả và chậm trễ trong bỏ phiếu từ xa. Để giảm thiểu những rủi ro này, nên triển khai các phương pháp tiếp cận phần mềm như ngăn chặn việc xóa bằng chứng và đảm bảo tính minh bạch với quyền riêng tư [7]-[9].

Công nghệ chuỗi khối có khả năng giải quyết một số yêu cầu đối với hệ thống bỏ phiếu điện tử an toàn và minh bạch. Một số ưu điểm của việc sử dụng chuỗi khối trong bỏ phiếu điện tử bao gồm xác thực cử tri đã đăng ký, đảm bảo ẩn danh bằng cách tách biệt danh tính của cử tri khỏi lá phiếu của họ, ghi phiếu bầu chính xác và an toàn, đồng thời cho phép xác minh tất cả phiếu bầu bằng hệ thống [10]. Nhiều quốc gia đã áp dụng các phương pháp bỏ phiếu điện tử do tiến bộ công nghệ và bất kỳ hệ thống bỏ phiếu nào hướng tới sự công bằng đều phải tuân thủ các nguyên tắc khách quan và cởi mở. Tuy nhiên, điều quan trọng là phải bảo vệ hệ thống khỏi các cuộc tấn công mạng và tấn công từ chối dịch vụ (DDOS) có thể làm gián đoạn quá trình bỏ phiếu và ảnh hưởng đến tính công bằng của nó. Để giải quyết những thách thức này, bài báo đề xuất một phương pháp bảo mật mạng cho các hệ thống bỏ phiếu dựa trên chuỗi khối, trong đó tính toàn vẹn của dữ liệu có thể được xác thực bởi bất kỳ người dùng nào trong chuỗi khối, đảm bảo tính công khai và công bằng trong quá trình bỏ phiếu. Ngoài ra, kiến trúc phân tán của chuỗi khối có thể cung cấp khả năng phục hồi chống lại việc tắt hệ thống do các cuộc tấn công mạng độc hại gây ra [11]. Những tính năng này của công nghệ chuỗi khối có thể góp phần xây dựng một hệ thống bỏ phiếu điện tử an toàn và minh bạch, giải quyết một số hạn chế của phương thức bỏ phiếu truyền thống và nâng cao niềm tin vào quy trình bầu cử [10]-[11].

III. HỆ ĐỀ XUẤT

3.1 Bỏ phiếu dựa trên chuỗi khối

Một hệ thống bỏ phiếu dựa trên chuỗi khối có khả năng giải quyết một số mối lo ngại trong bỏ phiếu điện tử và tăng cường tính toàn vẹn và bảo mật của quy trình bỏ phiếu. Bằng cách tận dụng bản chất phi tập trung và phân tán của công nghệ chuỗi khối, hệ thống bỏ phiếu dựa trên chuỗi khối có thể cung cấp tính minh bạch, tính bất biến và bảo mật cho toàn bộ quá trình bỏ phiếu. Một trong những lợi thế chính của việc sử dụng blockchain trong bỏ phiếu là tính minh bạch mà nó mang lại.

Mỗi phiếu bầu trên blockchain được ghi lại một cách minh bạch và không thay đổi, có nghĩa là một khi phiếu bầu được ghi lại, nó không thể bị thay đổi hoặc giả mạo. Tính minh bạch này đảm bảo rằng quy trình bỏ phiếu diễn ra công bằng và có trách nhiệm giải trình, vì tất cả các phiếu bầu đều có thể được kiểm tra và xác minh bởi các bên liên quan, bao gồm cử tri, ứng cử viên và cơ quan bầu cử. Ngoài ra, bản chất phi tập trung và phân tán của chuỗi khối đảm bảo rằng không có điểm lỗi hoặc lỗ hổng duy nhất nào trong hệ thống. Các hệ thống bỏ phiếu điện tử truyền thống có thể dễ bị hack, thao túng hoặc giả mạo, nhưng hệ thống bỏ phiếu dựa trên chuỗi khối phân phối phiếu bầu trên nhiều nút trong mạng, khiến nó có khả năng chống lại các cuộc tấn công cao. Chuỗi khối cũng cung cấp mức độ bảo mật cao thông qua các kỹ thuật mã hóa của nó. Mỗi phiếu bầu được mã hóa và ký điện tử, đảm bảo rằng chỉ những cá nhân được ủy quyền mới có thể bỏ phiếu và tính toàn vẹn của phiếu bầu được duy trì

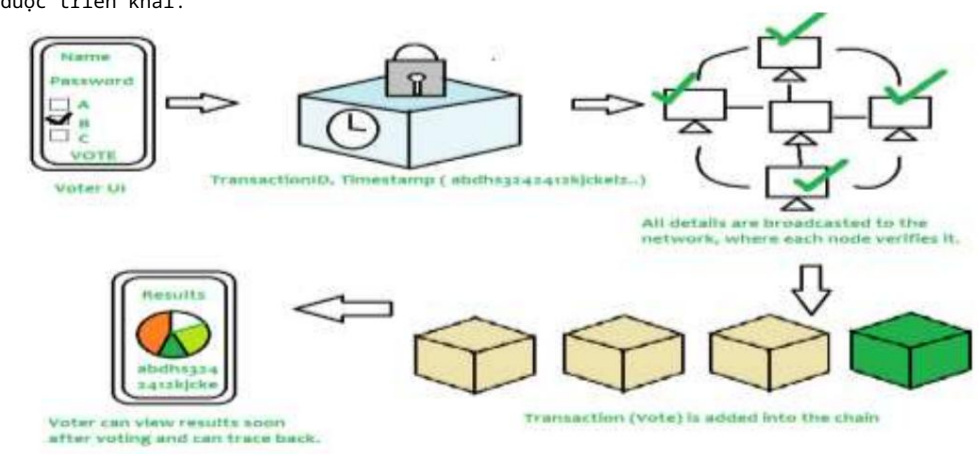
trong suốt quá trình. Điều này giúp loại bỏ khả năng xảy ra các hoạt động gian lận, chẳng hạn như bỏ phiếu hai lần hoặc nhồi nhét phiếu bầu, vì mỗi phiếu bầu được xác định và xác minh duy nhất. Một ưu điểm khác của việc sử dụng blockchain trong bỏ phiếu là khả năng tăng cường sự tham gia của cử tri. Các nền tảng bỏ phiếu trực tuyến dựa trên chuỗi khối có thể mang lại sự tiện lợi và khả năng tiếp cận, cho phép cử tri bỏ phiếu từ bất kỳ vị trí nào và trên bất kỳ thiết bị kết nối internet nào. Điều này có thể giúp tăng tỷ lệ cử tri đi bỏ phiếu, đặc biệt là trong thế hệ trẻ, những người quen thuộc hơn với công nghệ kỹ thuật số.

Hơn nữa, một hệ thống bỏ phiếu dựa trên chuỗi khối cũng có thể nâng cao hiệu quả của quá trình bỏ phiếu. Vì các phiếu bầu được ghi lại trên một chuỗi khối trong thời gian thực, nên quy trình kiểm phiếu có thể được tự động hóa, giảm nhu cầu kiểm phiếu thủ công và giảm thiểu khả năng xảy ra lỗi của con người. Điều này có thể giúp hợp lý hóa quy trình bỏ phiếu và cung cấp kết quả nhanh hơn và chính xác hơn. Tuy nhiên, điều quan trọng cần lưu ý là việc triển khai hệ thống bỏ phiếu dựa trên chuỗi khối cũng đi kèm với những thách thức và cân nhắc. Việc đảm bảo quyền riêng tư và ẩn danh của cử tri trong khi duy trì tính minh bạch và bảo mật có thể phức tạp. Bảo vệ chống lại các cuộc tấn công tiềm ẩn, chẳng hạn như tấn công 51% hoặc thông đồng giữa các nút, yêu cầu lập kế hoạch cẩn thận và các biện pháp bảo mật mạnh mẽ. Đảm bảo quyền truy cập và tính toàn diện cho tất cả các cử tri đủ điều kiện, bao gồm cả những người không có truy cập internet hoặc kiến thức kỹ thuật, cũng là một yếu tố quan trọng cần xem xét. Tóm lại, một hệ thống bỏ phiếu dựa trên chuỗi khối có khả năng giải quyết một số lo ngại trong bỏ phiếu điện tử và cung cấp một phương pháp an toàn, minh bạch và hiệu quả để tiến hành bầu cử. Tuy nhiên, việc lập kế hoạch cẩn thận, thử nghiệm kỹ lưỡng và sự tham gia của các bên liên quan là điều cần thiết để đảm bảo triển khai và áp dụng thành công một hệ thống như vậy.

3.2 Phương pháp

Luận Hệ thống được đề xuất gợi ý một kiến trúc phân tầng, trong đó hệ thống có thể có nhiều tầng dựa trên nhu cầu của quốc gia. Kiến trúc theo cấp độ này được thiết kế để cung cấp giải pháp nhanh chóng, đáng tin cậy và an toàn, có thể được tùy chỉnh dựa trên đặc điểm và yêu cầu của từng quốc gia.

Một trong những cơ chế của chính phủ để lưu trữ dữ liệu công dân để bỏ phiếu là thông qua cơ sở dữ liệu cử tri. Những công dân đủ điều kiện bỏ phiếu nhưng chưa bỏ phiếu có thể bỏ phiếu cho một trong các ứng cử viên. Thông tin của các ứng cử viên cũng sẽ được lưu trữ trong các hệ thống liên kết với chính phủ, có thể là trong một cơ sở dữ liệu hoặc hệ thống riêng biệt. Sau khi thủ tục xác thực hoàn tất, công dân sẽ có thể bỏ phiếu bằng cách chọn một trong các ứng cử viên được đưa ra hoặc bằng cách bỏ phiếu trắng nếu họ không muốn bỏ phiếu cho bất kỳ ứng cử viên cụ thể nào. Cơ sở dữ liệu chứa mối quan hệ giữa các thùng phiếu và các ứng cử viên sẽ được sử dụng để đảm bảo rằng chỉ những ứng cử viên đủ tiêu chuẩn mới được đưa ra để lựa chọn trong hệ thống. Cách tiếp cận này đảm bảo rằng quy trình bỏ phiếu an toàn và đáng tin cậy, vì nó dựa trên dữ liệu cử tri được xác thực và các ứng cử viên được lưu trữ trong một hệ thống liên kết với chính phủ. Nó cũng cho phép linh hoạt trong việc tùy chỉnh hệ thống dựa trên nhu cầu và yêu cầu cụ thể của từng quốc gia, vì số lượng tầng và kiến trúc tổng thể có thể được điều chỉnh tương ứng. Kiến trúc được phân cấp cung cấp khả năng mở rộng và khả năng thích ứng để phù hợp với các kịch bản và đặc điểm khác nhau của các quốc gia nơi hệ thống được triển khai.

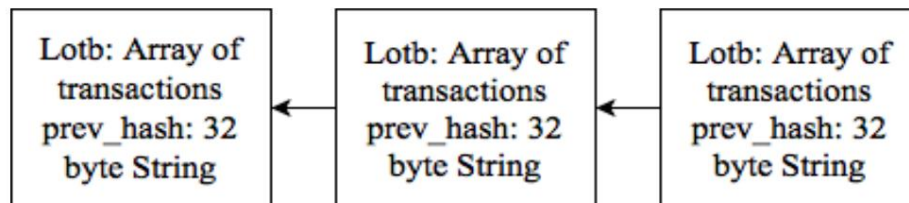


Hình 1 Frontend và Backend của Hệ thống bỏ phiếu

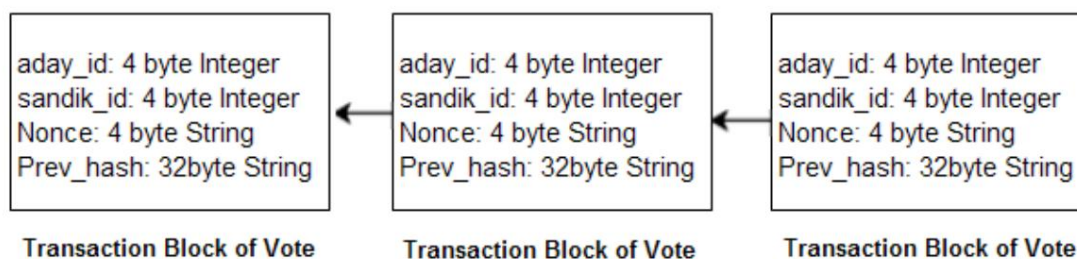
Kế hoạch làm việc được đề xuất bao gồm hai mô-đun, front-end và back-end, sẽ được hoàn thành trong ba giai đoạn.

Giai đoạn 1 sẽ tập trung vào mô-đun giao diện người dùng, bao gồm xây dựng giao diện người dùng tương tác cho cả quản trị viên và người dùng, đồng thời tiến hành nghiên cứu liên quan đến việc triển khai chuỗi khối trong ứng dụng phi tập trung.

Dưới đây là các ví dụ về cấu trúc khối theo cấp độ. Dữ liệu liên quan đến bầu cử được lưu trữ trong khối như hình dưới đây thông qua hệ thống.



Hình 2 Cấu trúc khối từ cấp 1 trở lên



Hình 3 Cấu trúc khối ở mức 0 (mức thấp nhất)

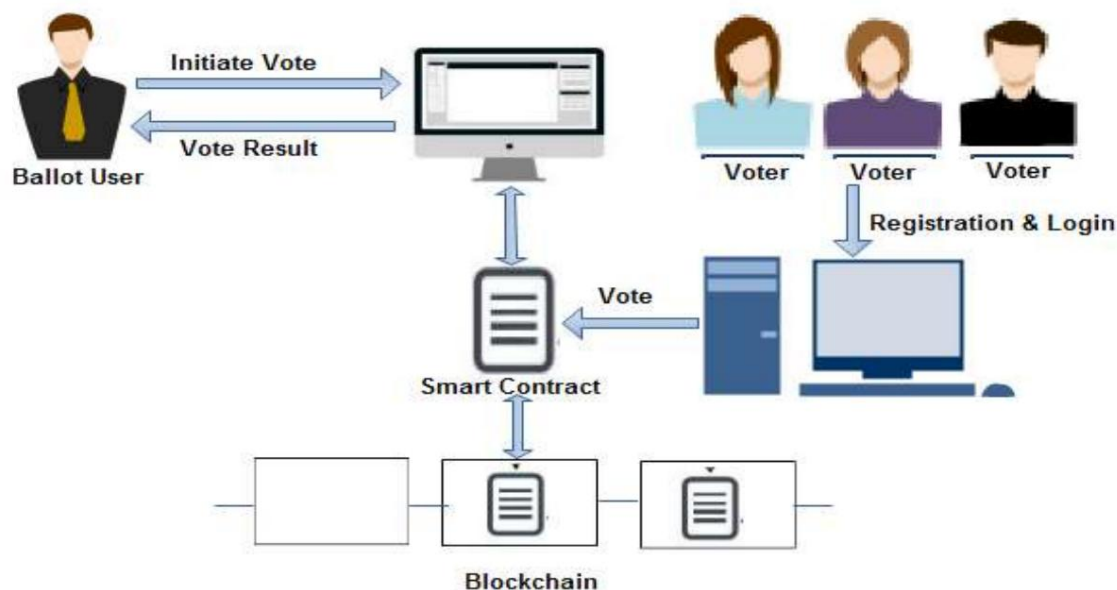
Kiến trúc được đề xuất đề xuất hai loại khối khác nhau để xây dựng chuỗi khối ở mức thấp nhất. Một loại khối sẽ lưu trữ thông tin về ứng cử viên và thùng phiếu, cùng với trường "nonce" để băm và trường "prev_hash" để tạo khối sẽ được thêm vào chuỗi khối. Loại khối khác sẽ bao gồm trường "prev_hash" để xây dựng chuỗi khối và một trường khác. Khi xây dựng hàm băm từ một khối trong hệ thống, một mẫu được chọn cho mỗi chuỗi, chẳng hạn như "hàm băm phải bắt đầu bằng 4 số 0 ở cuối." Nếu hàm băm không khớp với mẫu, chuỗi "nonce" sẽ được điều chỉnh cho đến khi mẫu băm phù hợp với chuỗi. Cách tiếp cận này sử dụng nhiều tài nguyên máy tính hơn vì thuật toán băm cần được lặp lại cho đến khi mẫu khớp, nhưng nó cũng cải thiện tính bảo mật vì bất kỳ bên độc hại nào cố gắng thêm một khối vào chuỗi cũng phải biết về mẫu băm. Điều này gây khó khăn cho các bên thứ ba trong việc dự đoán hoặc tạo ra một hàm băm có thể được chấp nhận, vì mô hình chuỗi sẽ khác nhau đối với mỗi cuộc bầu cử. Ở cấp độ thấp nhất (cấp độ 0), mỗi khối sẽ chứa một giao dịch, trong kịch bản bỏ phiếu điện tử được đề xuất, đại diện cho một phiếu bầu. Tất cả thông tin liên quan về giao dịch, chẳng hạn như thông tin về ứng cử viên và thùng phiếu, sẽ được lưu trong mỗi khối. Ở các cấp độ cao hơn, các phiếu bầu từ cấp độ bên dưới được lưu giữ trong các cụm được gửi trong các khoảng thời gian khác nhau và tất cả đều được lưu giữ trong một cấu trúc nguyên khối duy nhất.

Cách tiếp cận này đảm bảo rằng chuỗi khối được xây dựng an toàn và toàn vẹn, vì mỗi khối chứa một giao dịch đại diện cho một phiếu bầu và các mẫu băm khiến các bên độc hại khó can thiệp vào chuỗi khối. Việc sử dụng các loại và cấp độ khối khác nhau cho phép linh hoạt trong việc quản lý và sắp xếp dữ liệu trong chuỗi khối, tùy thuộc vào các yêu cầu cụ thể của kịch bản bỏ phiếu điện tử.

Mô-đun quản trị được chia thành năm thành phần:

Tôi. Bảng điều khiển: Thành phần này sẽ hiển thị các biểu đồ và dữ liệu khác nhau, chẳng hạn như số lượng bên, cử tri, v.v., để cung cấp một cái nhìn tổng quan về hệ thống bầu cử.

thứ hai. Thêm ứng cử viên: Quản trị viên sẽ có khả năng thêm các ứng cử viên đang tranh cử. Các phía người dùng của ứng dụng sẽ hiển thị các ứng viên được thêm vào.



Hình 4 Kiến trúc hệ thống bỏ phiếu điện tử

iii. Tạo cuộc bầu cử: Quản trị viên sẽ có thể tạo cuộc bầu cử bằng tính năng này. Chỉ sau khi quản trị viên tạo cuộc bầu cử, người dùng mới có thể bỏ phiếu trong ngày bắt đầu và ngày kết thúc cuộc bầu cử.

v.v. Chi tiết bầu cử: Quản trị viên có thể cập nhật các chi tiết bầu cử như ngày bắt đầu, ngày kết thúc, v.v. trong phần này.

v. Thông tin chi tiết về ứng viên: Thành phần này sẽ hiển thị tất cả các ứng viên do quản trị viên thêm vào. Quản trị viên sẽ cũng có khả năng cập nhật thông tin chi tiết về ứng viên nếu có bất kỳ mục nhập nào không chính xác.

Mô-đun người dùng được chia thành bốn thành phần:

Tôi. Bảng điều khiển: Người dùng sẽ có thể xem thông tin về các bên và ứng cử viên của họ trên bảng điều khiển người dùng. Người dùng sẽ có quyền truy cập vào tất cả các thông tin ứng cử viên.

thứ hai. Đăng ký cử tri: Trong phần này, người dùng sẽ cần tự đăng ký trước để đủ điều kiện tham gia.
bỏ phiếu.

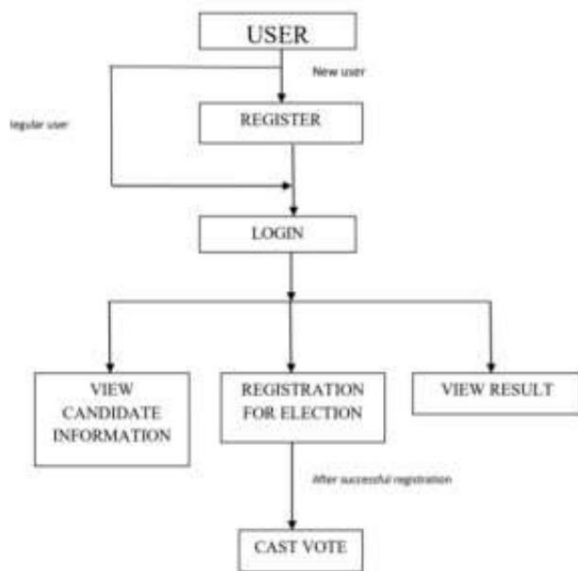
iii. Khu vực bỏ phiếu: Chỉ những người dùng đã đăng ký mới được phép truy cập trang này và bỏ phiếu sau khi sự đăng ký.

v.v. Kết quả: Trong thành phần này, người dùng sẽ có thể xem kết quả của cuộc bầu cử.

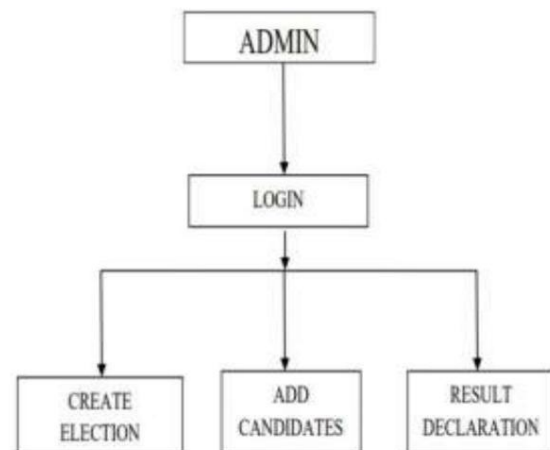
Điều quan trọng cần lưu ý là trong khi mô-đun giao diện người dùng đang được phát triển, nghiên cứu liên quan đến việc triển khai chuỗi khối trong ứng dụng phi tập trung cũng sẽ được tiến hành song song. Sau khi hoàn thành mô-đun giao diện người dùng, giai đoạn tiếp theo sẽ liên quan đến việc kết nối và kiểm tra các mô-đun giao diện người dùng và giao diện người dùng để đảm bảo chức năng và tích hợp trơn tru của toàn bộ hệ thống.

Giai đoạn 2: Trong giai đoạn này, chúng tôi sẽ đề cập đến mô-đun back-end, chúng tôi sẽ triển khai Blockchain bằng cách sử dụng Ethereum framework và chuyển đổi hệ thống thành một ứng dụng phi tập trung.

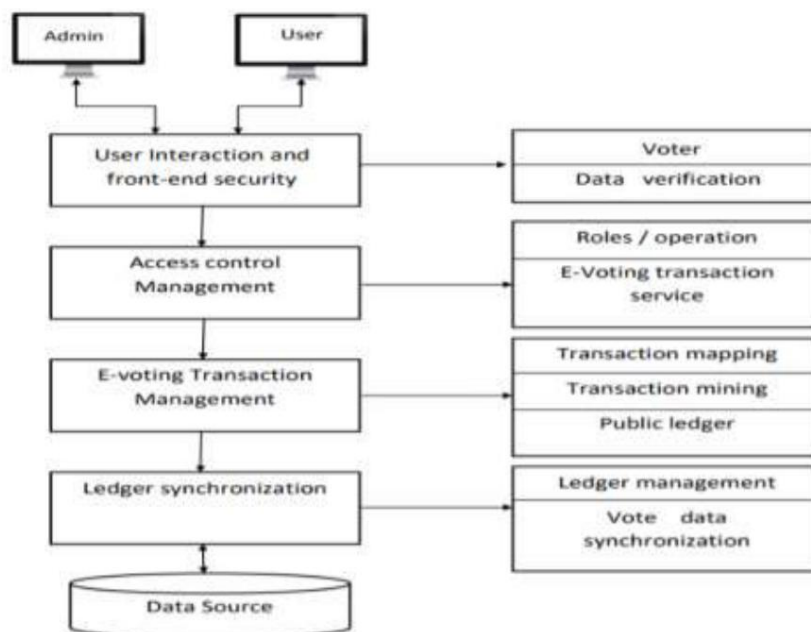
Giai đoạn 3: Việc kết nối hai mô-đun khác nhau cùng với việc thử nghiệm nền tảng sẽ được hoàn thành trong giai đoạn này.



Hình 5: Sơ đồ luồng người dùng



Hình 6: Sơ đồ luồng quản trị



Hình 7: Phương pháp nghiên cứu (Giai đoạn 2)

IV. PHÂN TÍCH KẾT QUẢ

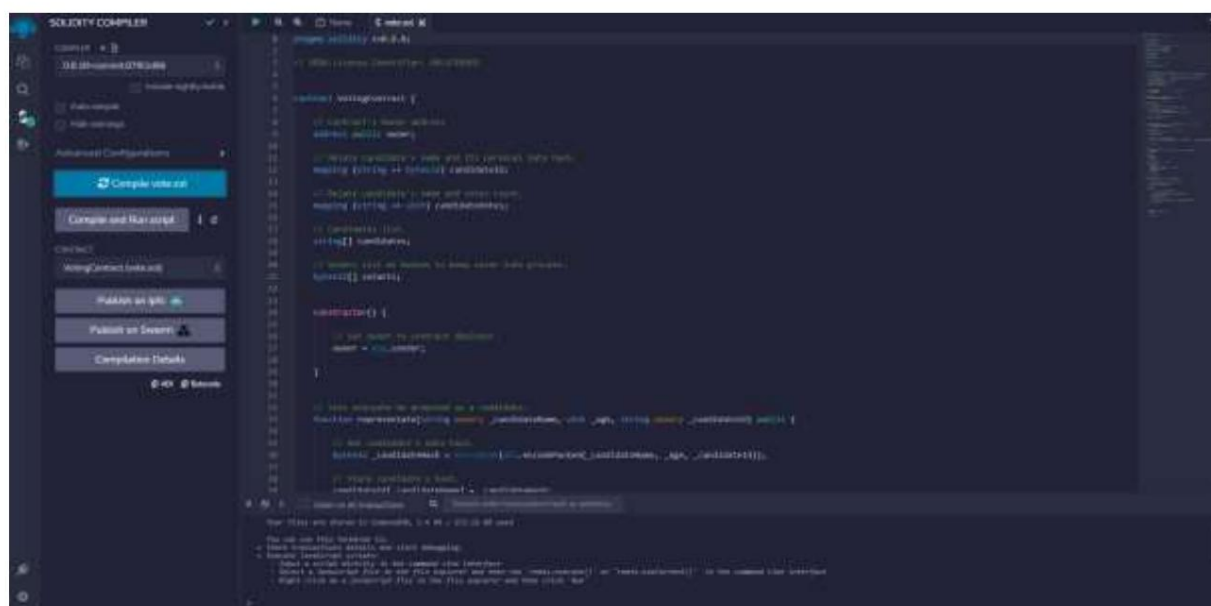
Trong chuỗi khối Ethereum, các hợp đồng thông minh được phát triển bằng ngôn ngữ lập trình phổ biến Solidity.

Đây là một số cách mà Solidity có thể được triển khai trong hệ thống bỏ phiếu điện tử: Tạo hợp đồng thông minh: Sử dụng Solidity, các nhà phát triển có thể viết hợp đồng thông minh chỉ định các quy tắc và tiêu chuẩn để bỏ phiếu. Các quy tắc có thể được thực thi, danh tính cử tri có thể được kiểm tra và phiếu bầu có thể được tính thông qua hợp đồng thông minh

- Tính minh bạch: Chuỗi khối đảm bảo rằng có lẽ quá trình bỏ phiếu là minh bạch vì đây là một hồ sơ mở và minh bạch. Bất kỳ ai cũng có thể kiểm tra kết quả bầu cử và không thể xảy ra gian lận.

- Phi tập trung hóa: Bằng cách loại bỏ sự cần thiết của một cơ quan trung ương hoặc người trung gian, một hệ thống bỏ phiếu điện tử phi tập trung có thể làm giảm nguy cơ gian lận. Một ứng dụng phi tập trung (dApp) cho phép bỏ phiếu mà không yêu cầu cơ quan tập trung có thể được tạo bằng Solidity.
- Bảo mật: Solidity có thể được sử dụng để xây dựng một hệ thống bỏ phiếu an toàn có thể chống lại sự thao túng hoặc hack. Ví dụ: sử dụng các phương pháp mã có thể đảm bảo rằng chỉ những cử tri đủ điều kiện mới có thể bỏ phiếu và phiếu bầu của họ được kiểm đếm chính xác.
- Tính bất biến: Các bản ghi phiếu bầu được tạo thành bất biến và không thể thay đổi nhờ sử dụng công nghệ chuỗi khối. Điều này ngụ ý rằng thậm chí nhiều năm sau khi cuộc bầu cử diễn ra, kết quả vẫn có thể được xác nhận.

Remix, một môi trường phát triển tích hợp dựa trên web, được sử dụng để tạo và xây dựng các hợp đồng thông minh Solidity (IDE). Mạng Ethereum thường được sử dụng như một công cụ bởi các nhà phát triển xây dựng các ứng dụng phi tập trung trên đó. Khi phát triển một hệ thống bỏ phiếu điện tử, các nhà phát triển có thể sử dụng Remix để viết, xây dựng và kiểm tra các hợp đồng thông minh của họ.



Hình 8: Phôi lại trình biên dịch solidity

```

ontract VotingContract {

    // Contract's Owner address
    address public owner;

    // Relate candidate's name and its personal data hash.
    mapping (string => bytes32) candidateId;

    // Relate candidate's name and votes count.
    mapping (string => uint) candidateVotes;

    // Candidates list.
    string[] candidates;

    // Voters list as hashes to keep voter info private.
    bytes32[] votants;
  }

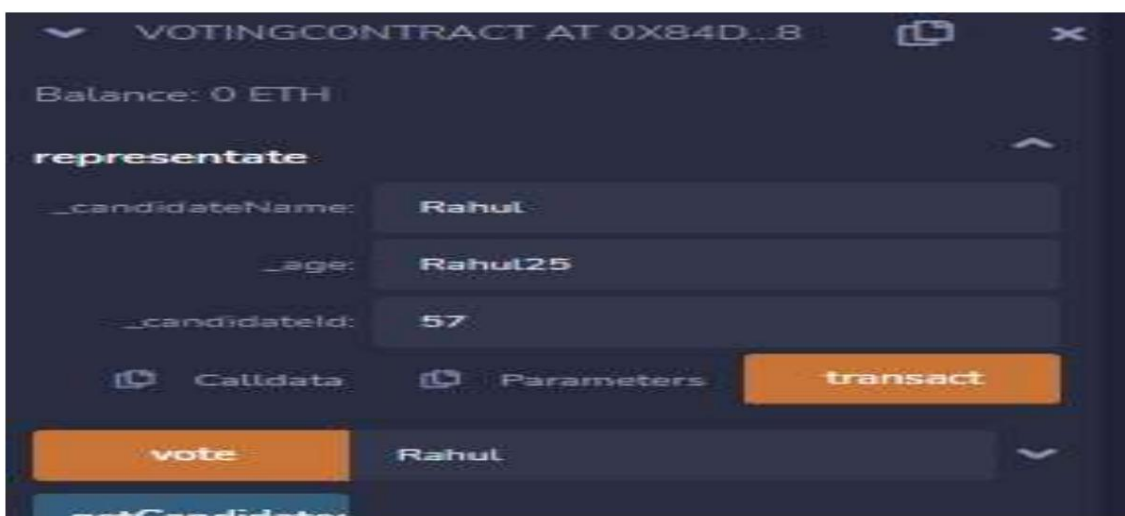
```

Hình 9 Sử dụng bản đồ băm để tạo cử tri và ứng cử viên.

Quá trình bỏ phiếu có thể được tích hợp vào hợp đồng thông minh và được triển khai trên chuỗi khối Ethereum bằng Solidity. Các lập trình viên có thể sử dụng hàm băm để tạo ID duy nhất cho từng cử tri và ứng cử viên có thể được thêm vào hệ thống và lưu trong bản đồ băm. Bản đồ băm sau đó có thể được sử dụng để xác minh danh tính của từng cử tri và ứng cử viên. Hệ thống có thể được kết nối với ví Ethereum tương thích với nền tảng để thực hiện các giao dịch và quản lý quy trình bỏ phiếu. Remix cung cấp một môi trường thân thiện và dễ sử dụng để phát triển và thử nghiệm các hợp đồng thông minh Solidity cho một hệ thống bỏ phiếu điện tử. Các giai đoạn bên dưới minh họa cách một hệ thống bỏ phiếu dựa trên chuỗi khối có thể hoạt động, cung cấp một phương pháp tiến hành bầu cử an toàn và minh bạch:

- Bước 1: Đăng ký làm Ứng cử viên và Cử tri

Để đảm bảo quy trình bỏ phiếu công bằng và minh bạch, mỗi ứng cử viên đủ điều kiện được cấp một ID duy nhất và mỗi cử tri được chỉ định địa chỉ chuỗi khối của riêng họ. Điều này tạo ra một chữ ký điện tử được kết nối với lá phiếu của cử tri, giúp dễ dàng xác nhận rằng lá phiếu đã được bầu bởi chính cá nhân đó.



Hình 10 Thêm chi tiết ứng viên

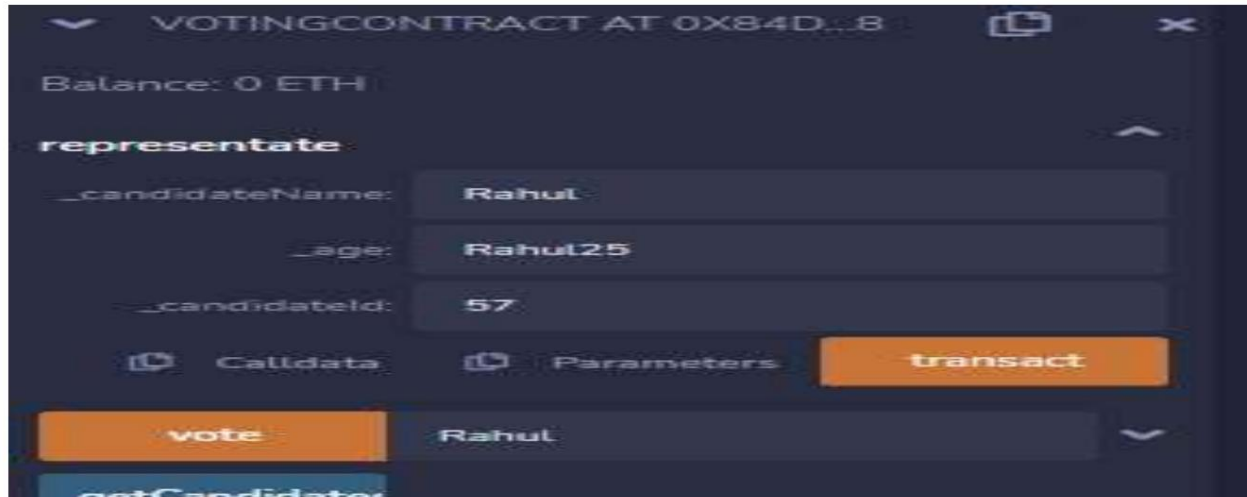


Hình. 11 Khởi chi tiết từng ứng viên được tạo

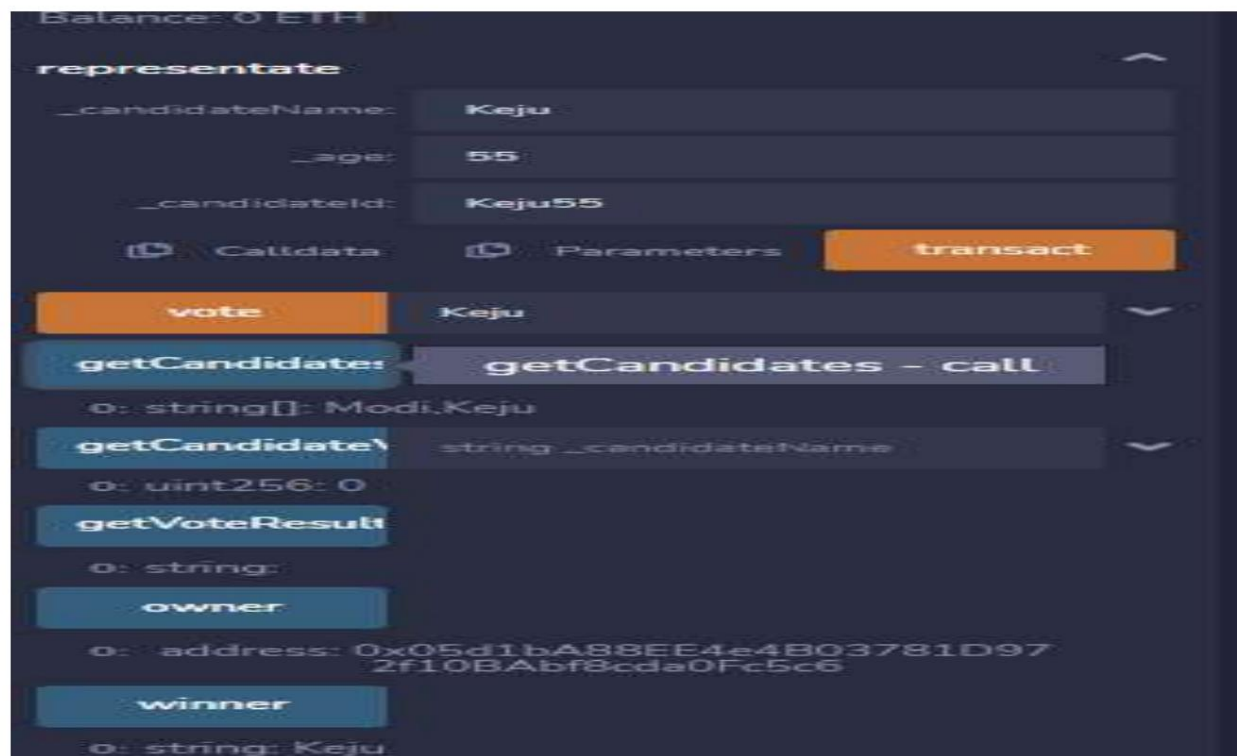
- Bước 2: Ghi phiếu bầu trên chuỗi khối

Mỗi phiếu bầu được ghi lại dưới dạng một khối duy nhất trên chuỗi khối, cùng với địa chỉ chuỗi khối của cử tri và ID của ứng cử viên, sau khi cử tri bỏ phiếu. Điều này đảm bảo rằng phiếu bầu được bảo mật và không thể bị thao túng, dẫn đến mức độ bảo mật cao.

Để bỏ phiếu, cử tri nhập địa chỉ chuỗi khối duy nhất của họ vào máy bỏ phiếu. Giai đoạn này có thể so sánh với bỏ phiếu truyền thống, nhưng việc sử dụng công nghệ chuỗi khối mang lại mức độ bảo mật và minh bạch cao hơn. Thông tin của mỗi ứng cử viên được ghi vào chuỗi khối, cùng với ID duy nhất của họ. Tất cả các cử tri đều có quyền truy cập vào thông tin này, cho phép họ đưa ra các lựa chọn có hiểu biết.



Hình 12 Bắt đầu bỏ phiếu cho các đại diện.



Hình 13 Người chiến thắng trong cuộc bình chọn

- Bước 3: Công bố kết quả Phiếu bầu

được kiểm khi buổi bình chọn kết thúc và ứng cử viên có số phiếu bầu cao nhất được tuyên bố là người chiến thắng. Kết quả được tuyên bố công khai và tất cả cử tri đều có thể tiếp cận ngay lập tức, tạo ra sự cởi mở và đảm bảo rằng tất cả các bên đều chấp nhận phán quyết.

V. KẾT LUẬN VÀ PHẠM VI TƯƠNG LAI

Hệ thống bỏ phiếu điện tử được đề xuất, được xây dựng bằng Solidity trên Remix và được triển khai trên chuỗi khối Ethereum, nhằm mục đích cung cấp một nền tảng mở, an toàn và không thể xâm nhập để tiến hành bầu cử. ID duy nhất được chỉ định cho mỗi cử tri và ứng cử viên thông qua băm trong hashmap, đảm bảo tính công bằng và minh bạch trong quá trình bầu cử. Việc tích hợp ví Ethereum vào hệ thống cho phép người dùng tương tác với nó dễ dàng hơn và thực hiện các giao dịch nhanh hơn. Việc sử dụng Ganache, một chuỗi khối riêng tư, để phát triển Ethereum bổ sung thêm một lớp bảo mật và phân tách để thử nghiệm và gỡ lỗi các hợp đồng thông minh. Điều này đảm bảo rằng các hợp đồng thông minh được kiểm tra và xác thực kỹ lưỡng trước khi được triển khai trên chuỗi khối Ethereum chính, giảm nguy cơ lỗ hổng và vi phạm bảo mật.

Xây dựng hệ thống bỏ phiếu điện tử trên Remix với Ganache, ví Ethereum và các thành phần khác cung cấp một nền tảng an toàn và đáng tin cậy để tiến hành các cuộc bầu cử kỹ thuật số. Tính linh hoạt và khả năng mở rộng của chuỗi khối Ethereum cho phép cải tiến và sửa đổi hệ thống trong tương lai khi cần, đảm bảo rằng hệ thống có thể thích ứng với các yêu cầu và công nghệ thay đổi. Nhìn chung, kiến trúc và công nghệ đề xuất được sử dụng trong hệ thống bỏ phiếu điện tử nhằm mục đích cung cấp một nền tảng mạnh mẽ và an toàn để tiến hành các cuộc bầu cử kỹ thuật số công bằng và minh bạch, đồng thời tận dụng các lợi thế của công nghệ chuỗi khối, hợp đồng thông minh và các công cụ hệ sinh thái Ethereum.

Phạm vi tương lai

Thật vậy, có một số con đường tiềm năng để tiến bộ trong các hệ thống bỏ phiếu dựa trên chuỗi khối và việc tích hợp sinh trắc học Aadhaar là một trong những khả năng như vậy. Aadhaar, là một hệ thống nhận dạng duy nhất sử dụng dữ liệu sinh trắc học để xác thực, có khả năng nâng cao tính bảo mật và độ chính xác của quy trình bỏ phiếu bằng cách đảm bảo rằng chỉ những cử tri đủ điều kiện mới có thể bỏ phiếu, do đó giảm nguy cơ gian lận.

Một lĩnh vực khác để phát triển có thể là việc áp dụng thẻ địa chỉ chuỗi khối duy nhất cho cử tri. Những thẻ này có thể cung cấp một cơ chế an toàn và được xác minh để cử tri truy cập chuỗi khối và bỏ phiếu của họ.

Việc sử dụng thẻ địa chỉ chuỗi khối có thể tăng cường đáng kể tính bảo mật của quy trình bỏ phiếu, vì bất kỳ ai cũng sẽ rất khó bỏ phiếu gian lận nếu không có thẻ địa chỉ chuỗi khối hợp lệ.

Hơn nữa, việc áp dụng thẻ địa chỉ chuỗi khối cũng có thể giải quyết những lo ngại về tính ẩn danh của cử tri, vì sẽ rất khó để theo dõi địa chỉ chuỗi khối của một cử tri cá nhân mà không có thẻ địa chỉ chuỗi khối tương ứng.

Nhìn chung, tương lai của các hệ thống bỏ phiếu dựa trên chuỗi khối hứa hẹn, với những tiến bộ và đột phá tiềm năng trong tương lai. Với các biện pháp bảo vệ và đổi mới phù hợp, có thể xây dựng một phương pháp thực sự an toàn, minh bạch và dễ tiếp cận để tiến hành bầu cử bằng công nghệ chuỗi khối. Tuy nhiên, điều quan trọng là phải đánh giá và giải quyết triệt để mọi mối lo ngại tiềm ẩn về quyền riêng tư, bảo mật và đạo đức liên quan đến việc tích hợp sinh trắc học hoặc các công nghệ khác vào hệ thống bỏ phiếu và đảm bảo rằng các nguyên tắc cơ bản của nền dân chủ, chẳng hạn như tính minh bạch, công bằng và tính toàn diện, được duy trì trong thiết kế và triển khai các hệ thống như vậy.

NGƯỜI GIỚI THIỆU

- [1] Pathak, Mrunal, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, và Prashant Parde. "Hệ thống bỏ phiếu điện tử dựa trên chuỗi khối." Tạp chí Nghiên cứu Khoa học Quốc tế về Khoa học và Công nghệ (2021): 134-140.
- [2] Hsiao, Jen-Ho, Raylin Tso, Chien-Ming Chen và Mu-En Wu. "Hệ thống bỏ phiếu điện tử phi tập trung dựa trên công nghệ chuỗi khối." Tạm ứng trong Khoa học máy tính và điện toán phổ biến: CSA-CUTE 17, trang 305-309. Mùa xuân Singapore, 2018.

- [3] Zyskind, Guy và Oz Nathan. "Phân cấp quyền riêng tư: Sử dụng chuỗi khối để bảo vệ dữ liệu cá nhân." Trong 2015 IEEE Security and Privacy Workshops, pp. 180-184. IEEE, 2015.
- [4] Kosba, A. Miller, E. Shi, Z. Wen và C. Papamanthou, "Hawk: Mô hình chuỗi khối về mật mã và hợp đồng thông minh bảo vệ quyền riêng tư," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, trang 839-858, doi: 10.1109/SP.2016.55.
- [5] Dalvi, Yash, Shivam Jaiswal, và Pawan Sharma. "Bỏ phiếu điện tử sử dụng chuỗi khối. Int J Eng Res Technol 10, số 3 (2021): 2278-0181.
- [6] Ahmed, Md Razu, FM Javed Mehedi Shamrat, Md Asraf Ali, Md Rajib Mia, và Ms Arifa Khatun. "Tương lai của hệ thống bỏ phiếu điện tử sử dụng chuỗi khối." Tạp chí Nghiên cứu Khoa học Công nghệ Quốc tế 9 (2020): 4131-4134.
- [7] Hjálmarsson, Friðrik Þ., Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, và Gísli Hjálmtýsson. "Hệ thống bỏ phiếu điện tử dựa trên chuỗi khối." Năm 2018 IEEE Hội nghị quốc tế lần thứ 11 về điện toán đám mây (CLOUD), trang 983-986. IEEE, 2018.
- [8] Hanifatunnisa, Rifa, và Budi Rahardjo. "Thiết kế hệ thống ghi âm bỏ phiếu điện tử dựa trên chuỗi khối." Năm 2017 Hội nghị quốc tế lần thứ 11 về Ứng dụng và Dịch vụ Hệ thống Viễn thông (TSSA), trang 1-6. IEEE, 2017.
- [9] Fusco, Francesco, Maria Ilenia Lunesu, Filippo Eros Pani và Andrea Pinna. "Crypto-voting, Hệ thống bỏ phiếu điện tử dựa trên chuỗi khối." Trong KMIS, trang 221-225. 2018.
- [10] Khan, Kashif Mehboob, Junaid Arshad, và Muhammad Mubashir Khan. "Điều tra các hạn chế về hiệu suất cho hệ thống bỏ phiếu điện tử an toàn dựa trên chuỗi khối." Hệ thống máy tính thế hệ tương lai 105 (2020): 13-26.
- [11] Taş, Ruhu, và Ömer Özgür Tanrıöver. "Đánh giá một cách có hệ thống các thách thức và cơ hội của blockchain đối với bỏ phiếu điện tử." Đối xứng 12, không. 8 (2020): 1328.
- [12] Alam, Asraful, SM Zia Ur Rashid, Md Abdus Salam, và Ariful Islam. "Hướng tới hệ thống bỏ phiếu điện tử dựa trên chuỗi khối." Năm 2018 hội nghị quốc tế về đổi mới khoa học, kỹ thuật và công nghệ (ICISSET), trang 351-354. IEEE, 2018.