

Hệ thống bỏ phiếu điện tử
dựa trên Blockchain và Ring Signature

Yifan Wu
Mã số sinh viên: 1700489
Msc Khoa học Máy tính
Giám sát: David Galindo



Đã nộp phù hợp với các yêu cầu đối với mức độ
Thạc sĩ Khoa học
Khoa Khoa học Máy tính
Đại học Birmingham

Tờ khai

Tài liệu trong luận án này trước đây chưa được nộp để lấy bằng tại Đại học Birmingham. Các nghiên cứu được báo cáo trong luận án này đã được thực hiện bởi tác giả trừ khi có chỉ định khác.

Đã ký tên

trường tượng

Hệ thống bỏ phiếu điện
tử dựa trên Blockchain và Ring Signature
Yifan Wu

Bỏ phiếu điện tử (e-vote) là biểu tượng của các hoạt động dân chủ hiện đại. Do cao quyền riêng tư và khả năng xác minh của lá phiếu, hệ thống bỏ phiếu điện tử đã phát triển vượt bậc trong những năm gần đây.

Đặc biệt, Bitcoin, một hệ thống tiền tệ kỹ thuật số dựa trên mật mã, có tính công khai và minh bạch cao đối với giao dịch cá nhân. Nói cách khác, bất kỳ ai cũng có thể truy cập vào nội dung giao dịch thông qua blockchain. Bên cạnh đó, liên quan đến cách ẩn danh mà nó giao dịch, giao dịch của Bitcoin là không thể theo dõi được.

Dựa trên bút danh của địa chỉ BitCoin và tính mở của blockchain, phù hợp với một phần của yêu cầu bỏ phiếu điện tử. Bài báo này đã đề xuất một giao thức bỏ phiếu điện tử dựa trên blockchain bằng cách sử dụng thuật toán chữ ký vòng. Các yêu cầu có thể được đáp ứng với tính riêng tư của lá phiếu, khả năng xác minh cá nhân, tính đủ điều kiện, tính hoàn chỉnh, tính duy nhất, tính mạnh mẽ và khả năng chống cưỡng chế.

Để chứng minh tính khả thi của giao thức. Thiết kế này đã thực hiện một cuộc bỏ phiếu web tốt phần mềm hệ thống thông qua ngôn ngữ lập trình PHP và JavaScript.

Phân tích bảo mật, phân tích hiệu suất phần mềm và đánh giá được trình bày trong phần cuối cùng.

Sự nhìn nhận

Em xin gửi lời cảm ơn tới thầy giáo TS.David Galindo, người đã giúp đỡ em rất nhiều khi thực hiện luận văn. David giúp tôi thực hiện luận văn đầy thử thách này với lời khuyên của chuyên gia và sự hướng dẫn kiên nhẫn của anh ấy. Anh ấy lắng nghe những suy nghĩ của tôi và đưa ra những đề xuất và cải tiến cho giao thức của tôi, và cuối cùng đã hoàn thành luận án. Tôi cũng muốn cảm ơn các thanh tra viên David Oswald và Per Kristian Lehre của tôi. Họ đã cho tôi những gợi ý tuyệt vời để viết bài báo này.

Tôi xin gửi lời cảm ơn đến người bạn thân nhất của tôi Rujia Li, người đã góp ý và động viên tôi hoàn thành luận văn này và phần mềm BlockVotes. Tôi cũng muốn cảm ơn Ruoyu He, Xi Jin và Amy Li, những người đã giúp tôi giải quyết các vấn đề ngữ pháp của toàn bộ bài báo.

Cuối cùng em xin cảm ơn bố mẹ đã luôn ủng hộ em hết mình
mong muốn.

Nội dung

1. Giới thiệu	6
1.1 Tổng quan.	7
1.2 Biểu quyết điện tử.	7
1.2.1 Công việc liên quan.	7
1.2.2 Các ứng dụng liên quan.	9
1.3 Chuỗi khối.	10
1.3.1 Giới thiệu.	10
1.3.2 Thuộc tính.	10
1.3.3 Cơ chế.	11
1.4 Kết cấu của luận văn.	12
2 Phương pháp luận	13
2.1 Sơ đồ biểu quyết điện tử Các thuộc tính.	14
2.2 Chuỗi khối.	15
2.2.1 Tạo địa chỉ Bitcoin.	15
2.2.2 MỞ QUAY_LẠI.	16
2.3 Mật mã học.	18
2.3.1 Thuật toán RSA.	18
2.3.2 Chữ ký vòng.	18
3 Giao thức	20
3.1 Định nghĩa.	21
3.2 Giao thức.	21
3.2.1 Dàn ý.	21
3.2.2 Các giả định.	22
3.2.3 Giai đoạn chuẩn bị.	22
3.2.4 Giai đoạn đăng ký đầu tiên.	22
3.2.5 Giai đoạn Đăng ký Thứ hai.	23
3.2.6 Giai đoạn xuất bản.	24
3.2.7 Giai đoạn biểu quyết.	24

NỘI DUNG	5
3.2.8 Giai đoạn kiểm đếm.	24
3.2.9 Giai đoạn xác minh.	24
4 Thực hiện	25
4.1 Đặc điểm kỹ thuật.	26
4.2 Yêu cầu.	26
4.3 Mô hình BlockVotes và Cây ghép.	29
4.3.1 Mô hình người dùng.	29
4.3.2 Mô hình RA.	31
4.3.3 Mô hình EA.	33
4.3.4 Mô hình biểu quyết.	35
4.3.5 Mô hình xác minh.	36
4.3.6 Mô hình kiểm đếm.	37
5 Đánh giá	40
5.1 Thuộc tính mong đợi.	41
5.2 Hiệu suất.	43
5.2.1 Hiệu suất chữ ký vòng.	43
5.2.2 Hiệu suất kiểm đếm.	44
5.2.3 Thời gian xác nhận.	45
6. Kết luận	47
6.1 Tóm tắt.	48
6.2 Kết luận.	48
6.3 Công việc trong tương lai.	48
Phụ lục	53
Một hướng dẫn	53

Chương 1

Giới thiệu

1.1 Tổng quan

Bầu cử đóng một vai trò quan trọng trong việc xây dựng một xã hội dân chủ. Thói quen truyền thống yêu cầu cử tri bỏ phiếu tại các điểm bỏ phiếu được chỉ định, điều này thường liên quan đến chi phí rất lớn về thời gian và ngân sách chi phí.

Bỏ phiếu điện tử, một hệ thống bỏ phiếu trực tuyến đáng kể mới được cấu trúc dựa trên kỹ thuật mật mã, đã dẫn được mọi người thực hiện và nhấn mạnh. Hệ thống hỗ trợ bỏ phiếu trực tuyến đầy đủ chức năng bằng các thiết bị gia dụng thông thường và toàn bộ kết quả bỏ phiếu sẽ được tính tự động và ẩn danh. So với bỏ phiếu truyền thống, bỏ phiếu điện tử là một hệ thống kinh tế hơn đề cập đến tính minh bạch và không thiên vị.

Vì hệ thống bầu cử điện tử chủ yếu dựa vào nền tảng internet. Thách thức quan trọng đối với bỏ phiếu điện tử là những rủi ro bảo mật đáng kể mà nó có thể gây ra. Để giảm thiểu rủi ro, trong 40 năm qua, nhiều giao thức khác nhau liên quan đến quyền riêng tư của lá phiếu, khả năng xác minh cá nhân, tính đủ điều kiện, tính đầy đủ, tính công bằng, tính duy nhất, tính mạnh mẽ, khả năng xác minh toàn cầu và tính không nhận được đã được đề xuất rộng rãi. Bên cạnh đó, các giao thức được xuất bản đã triển khai nhiều công nghệ khác nhau, chẳng hạn như chữ ký mù, chữ ký vòng, mã hóa đồng hình, Mix-Net, zero knowledge proof, v.v. [17]. Đặc biệt, việc áp dụng bỏ phiếu điện tử bằng tiền kỹ thuật số đã dẫn trở nên chín muồi hiện nay.

Dựa trên các yêu cầu bảo mật chung của những người tham gia, bài báo này đã đề xuất một giao thức dựa trên chuỗi khối liên kết với các ưu tiên về quyền riêng tư của lá phiếu, khả năng xác minh, tính đủ điều kiện, tính hoàn chỉnh, tính duy nhất, tính mạnh mẽ và khả năng chống cưỡng chế.

Một phần mềm BlockVotes cũng đã được thực hiện để xác minh tính khả thi của giao thức này, bằng cách triển khai một trang web bỏ phiếu trực tuyến ngoài đời thực, cho phép người tham gia bỏ phiếu và xem kết quả dễ dàng.

1.2 Bỏ phiếu điện tử

1.2.1 Công việc liên quan

Trong một thời gian dài, nhiều nhà nghiên cứu đang cố gắng để thiết kế một giao thức bỏ phiếu điện tử an toàn và hiệu quả. Luận án đầu tiên liên quan đến giao thức bỏ phiếu điện tử bằng mật mã được Chaum xuất bản vào năm 1981 và ông đã sử dụng một kênh hoán đổi ẩn danh để mã hóa lá phiếu [7]. Với sự phát triển của mật mã, rất nhiều giao thức với các đặc tính riêng của nó đã được đề xuất.

Năm 1982, Richard A. DeMillo đề xuất một giao thức yêu cầu tất cả cử tri phải tham gia và mã hóa lá phiếu của từng cử tri và cuối cùng bỏ phiếu [12]. Năm 1985, Cohen và Fisher đề xuất một giao thức mật mã có thể tổ chức một cuộc bầu cử lá phiếu an toàn. Tuy nhiên, nó đòi hỏi giai đoạn bỏ phiếu phải đồng thời [9]. Giao thức mã hóa lá phiếu bằng cách sử dụng định lý đồng cấu hình và chính phủ sẽ công bố kết quả kiểm đếm.

Năm 1992, Fujioka, Okamoto và Ohta đề xuất một kế hoạch bỏ phiếu điện tử bí mật thực tế (F00) được sử dụng cho các cuộc bầu cử quy mô lớn, có thể đảm bảo quyền riêng tư của cử tri và tính công bằng của

biểu quyết. Kế hoạch này đã sử dụng chữ ký mù để làm mù thông điệp mà cử tri đã sử dụng để bỏ phiếu và gửi nó cho quản trị viên [14]. Sau khi bài báo này được phát hành, rất nhiều phần mềm bỏ phiếu điện tử đã được triển khai và sử dụng cho thị trường, chẳng hạn như EVOX và SENSUS. Trong kế hoạch này, nó cũng có điểm yếu của nó, nó yêu cầu tất cả cử tri phải bỏ phiếu và một khi ai đó bỏ phiếu trắng, kết quả có thể làm xáo trộn. Quản trị viên không thể tìm ra ai đã giả mạo kết quả. Năm 1996, Juang và Lei đề xuất kế hoạch bỏ phiếu dựa trên chữ ký mù nhưng yêu cầu mọi người phải tham gia sự kiện bỏ phiếu.

Sau 3 năm, M. Ohkubo, F.Miura và M.Abe đã thúc đẩy kế hoạch F00 bằng cách sử dụng giao thức mã hóa ngưỡng và kênh liên lạc Mix-Net có thể giữ quyền riêng tư của người bỏ phiếu. Đối với cử tri, họ có thể không cần tham gia phần kiểm đếm của sự kiện và có thể bỏ đi sau khi bỏ phiếu [25].

Với sự phát triển của hệ thống bầu cử điện tử, có một loạt các hành vi phạm tội liên quan đến bỏ phiếu điện tử, chẳng hạn như gian lận bầu cử, đe dọa cử tri hoặc mua phiếu bầu. Để đối phó với những vấn đề này, nhiều yêu cầu hoặc đặc tính mới của chương trình bỏ phiếu điện tử đã được đề xuất như tính không nhận và khả năng chống cưỡng chế.

Không có biên lai có nghĩa là cử tri không thể chứng minh kết quả bỏ phiếu cho bất kỳ ai sau khi bỏ phiếu. Năm 1994, Benaloh thảo luận đầu tiên về thuật ngữ có tên là tính không nhận [2]. Mặc dù Benaloh sử dụng mã hóa đồng hình để thực hiện miễn phí biên nhận, Martin Hirt lập luận rằng nó sẽ không hợp lệ nếu có nhiều hơn một cơ quan kiểm đếm. Năm 1995, V.Niemi và A.Renvall nêu ra một mưu đồ bằng cách thông qua phiếu thu để cử tri không chứng minh được mình bỏ phiếu cho ai [24]. Đồng thời, K Sako và J Kilian đề xuất giao thức dựa trên Mix-Net đầu tiên thỏa mãn với tính năng không nhận [30]. Giao thức này theo giả định rằng không có kênh riêng giữa trạm bỏ phiếu và cử tri. Sau một năm, Okamoto sử dụng kênh không ẩn danh, kênh riêng tư và bảng thông báo để đề xuất kế hoạch bỏ phiếu đáp ứng tính không cần biên nhận [26]. Thật không may, giao thức này đã được chứng minh là không đáp ứng với tính năng không nhận. Năm 2000, M.Hirt và K.Sako sử dụng kỹ thuật mã hóa ElGamal đồng hình để thiết kế một giao thức kênh riêng với tính năng không nhận, nhưng giao thức này không phù hợp với cuộc bầu cử quy mô lớn [15]. Vào năm 2001, O.Baudron đã đề xuất một sơ đồ mới để đáp ứng tính chất này bằng cách sử dụng hệ thống mật mã Paillier và bằng chứng không-tri thức [1].

Trong những năm gần đây, rất nhiều nhà nghiên cứu tập trung vào tính không cần biên nhận và khả năng chống cưỡng chế của bỏ phiếu điện tử. Vào năm 2010, Juels đã giới thiệu một hướng mới của bỏ phiếu điện tử đặt tên là chống cưỡng chế và đề xuất một kế hoạch [18]. Năm 2012, O.Spycher và R.Koenig quảng bá kế hoạch của mình bằng cách thêm số nguyên ngẫu nhiên f . Lược đồ được đề xuất sẽ nhận được số nguyên C được mã hóa. Cơ quan kiểm đếm có thể đánh giá nếu có bất kỳ lá phiếu giả nào thông qua việc giải mã C thành số nguyên ngẫu nhiên f [32]. Khả năng chống cưỡng chế có thể được thỏa mãn hơn nữa.

Bằng sự phát triển của tiền tệ kỹ thuật số phi tập trung, một số nhà nghiên cứu đã tranh luận về một cách để bỏ phiếu và kiểm đếm trên blockchain. Vào năm 2015, Czepluch đã thảo luận về các ứng dụng của blockchain và lập luận rằng blockchain có thể sử dụng cho việc bỏ phiếu điện tử [11]. Đồng thời, Z.Zhao và THH.Chan đã đề xuất một cách bỏ phiếu bằng cách sử dụng Bitcoin và zk-SNARKs với

các thuộc tính được đặt tên là quyền riêng tư, khả năng xác minh và không thể hủy ngang [34]. Vào năm 2016, một giao thức sử dụng Zerocoin đã được đề xuất và đảm bảo hầu hết các thuộc tính của biểu quyết điện tử [33]. Tuy nhiên, việc sử dụng Zerocoin rất khó thực hiện cho phần mềm. Cùng năm đó, C.Jason, Paul và K.Yuichi đã đề xuất một giao thức sử dụng chữ ký mù và thẻ Bitcoin [16].

Tuy nhiên, nó không thể bảo vệ quyền riêng tư trong một số tình huống, ví dụ: nếu quản trị viên biết địa chỉ Bitcoin của người bỏ phiếu, quản trị viên có thể biết người bỏ phiếu là ai bằng cách liên kết địa chỉ và tin nhắn trên blockchain.

1.2.2 Các ứng dụng liên quan

Việc nghiên cứu hệ thống bầu cử điện tử đang được sử dụng rộng rãi hiện nay. Một số thực hành từng phần được liệt kê như sau.

Năm 2000, bỏ phiếu điện tử đã được sử dụng trong Bầu cử Hoa Kỳ [8]. Mặc dù nó là một thử nghiệm trong một số của Florida, đó là một cột mốc quan trọng trong sự phát triển của bỏ phiếu điện tử.

Năm 2002, Vương quốc Anh đã thử nghiệm hệ thống bỏ phiếu điện tử. 16 cơ quan công quyền đã được trao giải để xây dựng hệ thống bỏ phiếu điện tử. Sau 1 năm, hơn 18 cơ quan chức năng đã được trao giải [22].

Năm 2004, cuộc bầu cử Hoa Kỳ lần đầu tiên sử dụng hệ thống bỏ phiếu điện tử DRE [5]. Ấn Độ sử dụng hệ thống này cho các cuộc bầu cử quốc hội trên quy mô quốc gia.

Năm 2007, đảng UMP của Pháp đã làm nên lịch sử về bỏ phiếu dựa trên internet. Hơn 31.000 cử tri đã bỏ phiếu tại UMP cho đến cuộc bầu cử Tổng thống Pháp năm 2007 [13]. Đây là hoạt động bỏ phiếu điện tử đại chúng đầu tiên trong lịch sử.

Năm 2009, Trung Quốc đã sử dụng biểu quyết điện tử cho cuộc bầu cử của tổ chức cơ sở ở Hàng Châu. Đã có 3122 cư dân đăng ký hoạt động bỏ phiếu này bằng màn hình cảm ứng điện tử [21].

Năm 2014, cuộc bầu cử Bộ Giáo dục Quốc gia (Pháp) đã nhận được 1.760.000 phiếu bầu [21]. Nó dẫn đầu trong việc bỏ phiếu mạng lưới pháp lý và an ninh, do đó đã phổ biến các kênh bỏ phiếu công việc rỗng.

1.3 Blockchain

1.3.1 Giới thiệu

Năm 2008, người sáng lập Bitcoin S.Nakamoto đã xuất bản một bài báo [23] để chỉ định một hệ thống lần truy cập tiền điện tử dựa trên mạng ngang hàng. Bitcoin đã thay đổi cách thức truyền thống của hệ thống thanh toán tiền mặt. Với sự phát triển của Bitcoin, công nghệ Blockchain đã thu hút sự chú ý của mọi người. Blockchain là một sổ cái công khai, tất cả các cá nhân đều có thể đồng bộ hóa sổ cái mới nhất thành cục bộ và họ không được phép giả mạo nội dung của sổ cái công khai.

Để phân biệt các blockchain khác nhau, có hai cách phân loại của blockchain [27]. Một được phân loại theo yêu cầu của các nút mạng đối với quá trình xác minh.

- Blockchain không có quyền: Không cần dịch vụ trung tâm hoặc cơ quan có thẩm quyền để tính toán trong quá trình xác minh. Thông thường, quá trình tính toán này xảy ra trong thiết bị của bất kỳ ai.
- Blockchain được phép: Có một mạng trung tâm được sử dụng để xác nhận các nút xác minh.

Một cái khác được phân loại theo tính công khai của blockchain.

- Blockchain công khai: Bất kỳ ai trên thế giới đều có thể đọc, tải xuống, phát sóng chuyển tiếp hành động của blockchain.
- Blockchain riêng: Blockchain chỉ thuộc về cá nhân, chính phủ hoặc một tổ chức không công khai.

Trong những năm gần đây, Bitcoin và Ethereum ngày càng phổ biến. Cả hai đều blockchain công khai và không được phép.

Đối với Bitcoin, nó có 2 mạng con, mạng Bitcoin và mạng thử nghiệm. Testnet là môi trường thử nghiệm của mạng Bitcoin. Trong mạng lưới này, đồng xu không có bất kỳ giá trị nào. Nó là miễn phí để sử dụng và nhận tiền thử nghiệm dưới dạng vôi [19].

Ethereum là một loại tiền kỹ thuật số tương tự như Bitcoin. Nó cũng là một tập hợp hoàn chỉnh của nền tảng ứng dụng phi tập trung. Trong khi sử dụng Ethereum để giao dịch tiền kỹ thuật số, bất kỳ ai cũng có thể xuất bản và sử dụng các ứng dụng phi tập trung trên Ethereum. Lợi thế của Ethereum là nó cung cấp một chuỗi công cụ hoàn chỉnh để phát triển, triển khai ứng dụng phi tập trung. Bằng cách sử dụng hợp đồng thông minh, nó làm cho việc phát triển ứng dụng dựa trên chuỗi khối trở nên vô cùng thuận tiện.

1.3.2 Thuộc tính

Kể từ khi blockchain ra đời, blockchain có các thuộc tính phân quyền, tin cậy phi tập trung, bảo trì chung, độ tin cậy của dữ liệu, bảo vệ quyền riêng tư. Nó đã được chú ý chưa từng có và sự phát triển của nó rất nhanh chóng.

- **Phi tập trung:** Blockchain được phân cấp. Không có thiết bị điện toán trung tâm nào để lưu trữ sổ cái các giao dịch. Mọi nút của chuỗi khối đều lưu trữ giống nhau

sao chép.

- **Khó giả mạo:** Do tính phi tập trung, mọi khối phải được phân phối cho mọi nút trên khắp thế giới.

- **Có thể theo dõi giao dịch:** Mỗi giao dịch trong blockchain đều công khai và minh bạch.

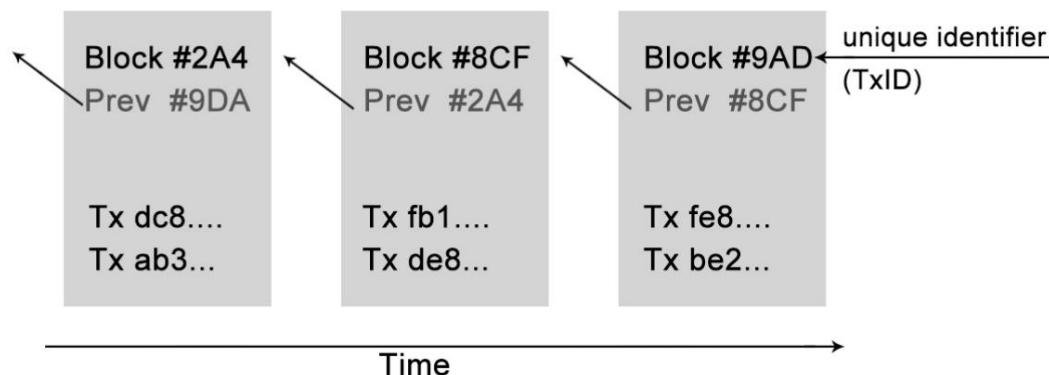
Mọi chi tiết giao dịch bao gồm địa chỉ người gửi và địa chỉ người nhận, bất cứ ai có thể theo dõi một giao dịch.

Trong bài báo này, chúng tôi đã đề xuất một giao thức dựa trên Bitcoin. Đối với mỗi giao dịch, mọi người đều có thể tải xuống thông tin từ blockchain. Trong Bitcoin, mọi địa chỉ Bitcoin không liên quan đến danh tính cá nhân của nó. Do đó, blockchain là biệt danh cho bất kỳ ai và có các giao dịch minh bạch, có các yêu cầu tương tự đối với bỏ phiếu điện tử đặc tính.

1.3.3 Cơ chế

Blockchain bao gồm một tập hợp các nút dựa trên mạng ngang hàng. Đối với mỗi nút, nó duy trì tính nhất quán của dữ liệu bằng cách thực hiện một thuật toán đồng thuận. Để chỉ rõ cơ chế của blockchain, Bitcoin là một đại diện điển hình của blockchain. Để chỉ rõ blockchain, chúng ta nên có một khái niệm cơ bản về khối. Khối này bao gồm tiêu đề khối và phần chính của khối bao gồm một giao dịch thô được tuân thủ.

Phần thô của giao dịch chứa số nhận dạng duy nhất (TxID) là giá trị băm của giao dịch. Giá trị nhận dạng của tất cả các giao dịch trên mỗi khối tạo thành mỗi lá nút của cây Merkel.



Hình 1.1: Chữ ký chiếc nhẫn

Bằng cách lưu trữ TxID khối trước đó vào khối tiếp theo, tất cả các nút được liên kết với tiêu đề khối còn được gọi là blockchain. Khi tạo một khối mới, blockchain

sẽ sử dụng thuật toán đồng thuận để tạo số nhận dạng duy nhất của giao dịch mới. Một khối mới được tạo bởi thuật toán đồng thuận, thuật toán này tạo ra một khối mới bằng cách tính toán giá trị băm của tiêu đề khối. Sau khi hầu hết các nút chấp nhận khối mới, nó sẽ được thêm vào chuỗi khối.

1.4 Kết cấu của luận văn

Luận văn này gồm 6 chương.

Chương 1 là phần giới thiệu của vấn đề và tổng quan tài liệu về các công nghệ liên quan của nó.

Chương 2 là phương pháp luận của vấn đề. Chương này trình bày chi tiết các thuộc tính và yêu cầu của sơ đồ bỏ phiếu điện tử và kỹ thuật hoặc thuật toán khác được sử dụng trong giao thức.

Chương 3 là phần quan trọng nhất của luận văn này. Giao thức được đề xuất cho biết toàn bộ kế hoạch thiết kế của việc thực hiện.

Chương 4 là việc thực hiện giao thức. Bằng cách tạo một ứng dụng có tên là BlockVotes, bất kỳ thuộc tính nào cũng có thể được kiểm tra. Chương này được viết theo phương pháp luận của kỹ thuật phần mềm.

Chương 5 là đánh giá giao thức, đánh giá các thuộc tính của nó và lập luận nguyên nhân.

Chương 6 là phần kết luận của giao thức được đề xuất và việc thực hiện. Phần này thảo luận về công việc trong tương lai.

chương 2

Phương pháp luận

2.1 Các thuộc tính của lược đồ bỏ phiếu điện tử

Trong 30 năm gần đây, ngày càng có nhiều giao thức bỏ phiếu điện tử được xuất bản. Mỗi quan hệ chính đáng của chương trình bỏ phiếu điện tử có thể được mô tả từ các bài báo của Cranor [10], Cetinkaya [6] và Fujioka [14].

Các tính chất cơ bản

Quyền riêng tư của lá phiếu: Bất kỳ ai cũng không thể biết được cử tri đã bỏ phiếu cho ai. Lá phiếu được ẩn khỏi những người quan sát bên ngoài.

Khả năng xác minh cá nhân: Người bỏ phiếu có thể xác minh lá phiếu của mình được đếm chính xác sau khi đã bỏ phiếu.

Tính đủ điều kiện: Chỉ những cử tri hợp pháp mới có thể đăng ký sự kiện bỏ phiếu.

Độ chính xác / Tính đầy đủ: Mỗi phiếu bầu phải được đếm chính xác.

Công bằng: Không điều gì có thể ảnh hưởng đến kết quả của cuộc bỏ phiếu. Nếu hệ thống làm rò rỉ kết quả bỏ phiếu hoặc cơ quan có thẩm quyền thêm một cử tri trong quá trình bỏ phiếu, sự kiện có thể được định nghĩa là không công bằng.

Tính duy nhất: Mỗi người bình chọn chỉ được bình chọn một lần. Người bỏ phiếu sẽ không được phép bỏ phiếu thêm nếu anh ta bỏ phiếu.

Tính chắc chắn: Bất kỳ ai cũng không thể ảnh hưởng hoặc sửa đổi kết quả biểu quyết cuối cùng khi kiểm đếm.

Thuộc tính nâng cao

Khả năng xác minh toàn cầu: Bất kỳ ai cũng có thể xác minh tính đủ điều kiện của mỗi lá phiếu và tính công bằng của kết quả.

Không có biên nhận: Người bỏ phiếu không thể nhận hoặc cố gắng tạo bất kỳ biên nhận nào sau khi đã bỏ phiếu để chứng minh cách họ bỏ phiếu.

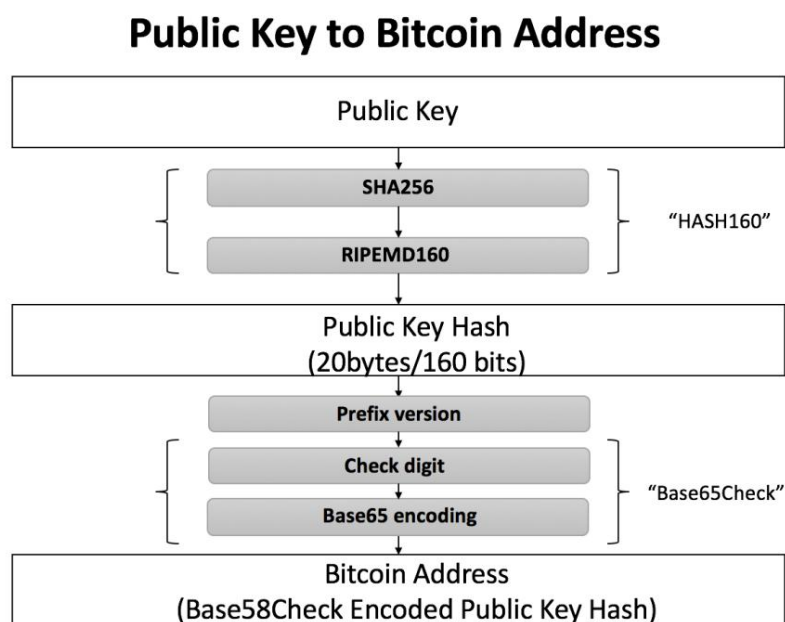
Sự cưỡng chế-phản kháng: Không có người ép buộc nào có thể hợp tác với cử tri. Người bỏ phiếu không thể

chứng minh người mà anh ấy đã bầu chọn.

2.2 Blockchain

2.2.1 Tạo địa chỉ Bitcoin

Để phát một thông điệp trên blockchain, những người tham gia cần có địa chỉ Bitcoin. Bằng cách sử dụng SHA256, RIPEMD160 Hashing và Base58 Encoding, địa chỉ Bitcoin có thể được tạo như Hình 2.1 [20].



Hình 2.1: Khóa công khai đến địa chỉ Bitcoin [20]

1. Tạo khóa riêng tư bằng Thuật toán chữ ký số đường cong Elliptic, nói chung có tên là secp256k1. Kích thước của khóa cá nhân Bitcoin là 256 bit.
2. Tạo khóa công khai Bitcoin từ khóa riêng tư Bitcoin (x, y) với định dạng DER.
3. Băm khóa công khai Bitcoin dưới dạng PHash160 thành hash160 bằng cách tạo SHA256 và thuật toán RIPEMD160.
4. Thêm tiền tố của phiên bản vào đầu PHash160 theo Bảng 2.1. Xác định giá trị băm trung gian của khóa công khai fingerprint = prefix + PHash160, cũng được đặt tên là tệp tham chiếu.
5. Xác định Sha256 (Sha256 (fingerprint)) là số kiểm tra d. Thêm chữ d vào cuối fingerprint.
6. Tạo địa chỉ Bitcoin cuối cùng bằng cách mã hóa fingerprint + d với thuật toán mã hóa Base65. Xác định địa chỉ = Base65 (fingerprint + d) là địa chỉ Bitcoin cuối cùng.

Tiền tố chuỗi khối
BITCOIN '00'
TESTNET '08'

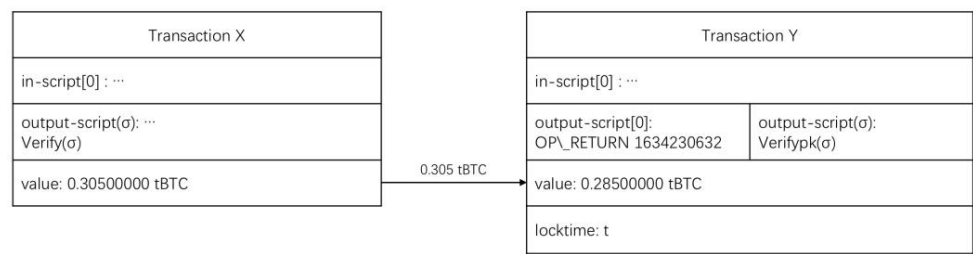
Bảng 2.1: Tiền tố của phiên bản

2.2.2 MỞ QUAY LẠI

Để thảo luận về sự TRỞ LẠI của chuỗi khối, chúng ta nên xem xét giao dịch đầu tiên. Đối với mỗi giao dịch trên Bitcoin, nó chứa tập lệnh đầu vào và tập lệnh đầu ra như Hình 2.2. Hình được hiển thị giao dịch giữa Alice và Bob là những người tham gia giao dịch.

Đây là một ví dụ về giao dịch giữa Alice và Bob với tham chiếu là "haha" trên blockchain của testnet.

Xác định địa chỉ Bitcoin của Alice là mxLqfJvTTEojWVZVTanEcXs1kXaBkdoqfX và địa chỉ Bitcoin của Bob là n4Kc1AwFos3aZRvD3Tc9imzeMeA8E9DEUr.



Hình 2.2: Giao dịch giữa Alice và Bob

Alice tạo Giao dịch Y với đầu vào của một giao dịch. Để xác nhận Giao dịch Y trong blockchain, tập lệnh đầu vào [0] phải tham chiếu đến Giao dịch X. Tập lệnh đầu ra của Giao dịch Y chứa 2 phần. Một là chữ ký cho Giao dịch Y được ký bằng khóa riêng của Alice SK. Một mã khác là mã OP RETURN, là tham chiếu của "haha". OP RETURN là một tập lệnh dựa trên ngăn xếp không có vòng lặp. Vì nó được định nghĩa trong giao thức của Bitcoin, nó có thể lưu trữ tối đa 80 byte trong giao dịch. Thời gian khóa t có nghĩa là Giao dịch Y không nên được đặt trước thời điểm t [34].

Để xác nhận giao dịch này trước t, người tạo giao dịch Alice phải trả phí khai thác cho người khai thác. Người khai thác có thể sử dụng thuật toán PoW (Proof of Work) để tìm một khối bao gồm V erifypk (σ). Cuối cùng, Bob sẽ nhận được tiền với tham chiếu là "haha".

Hơn nữa, để xác định ví dụ này, ví dụ này đã được thực hiện trong mạng testnet. Các chi tiết có thể được liệt kê trong Bảng.

Từ Bảng 2.2, chúng ta có thể thấy rằng output-script [0] cho biết OP RETURN là 1634230632. Để giải mã OP RETURN, chúng ta có thể sử dụng thuật toán hex2bin () để chuyển nó thành các ký tự.

ID giao dịch 025e4	fd916832c4028b1bcc446c8a41c10798fbea49793ce245ccf700e621d4f
input [0]	mprsHi9HKpn9bH14ZZV7YC7mxdRJ6wws7r (0,12249999)
input-script [0]	3045022100b7a6e8aa5cd553e4c21ad68e851c140c3e87d3eefc4d0a 3045022100ae906a357c927d170f19710aca1de3c5ebcbe2c60fe9 626b24ed876d7f23fad40220354d0b0c254679817deac98f4fcfa 33be48eaf74c77a2e0b4db2046747cb2b3d0102ce592b293c66 88ca587dea59780acca8da8215d4d3261db338e9ea39fc46ae19
input-value	0,30500000
[0] output [0]	MỞ QUAY LẠI 68616861
output-script [0]	OP RETURN 1634230632
giá trị đầu ra [0]	0,00000000
đầu ra [1] n4Kc1Aw	Fos3aZRvD3Tc9imzeMeA8E9DEUr
tập lệnh đầu ra [1]	OP DUP OP HASH160 fa25611aeeed75a33a9fc8cc83d2039059c37d837 OP EQUALVERIFY OP CHECKSIG -
giá trị đầu ra [1]	0,28500000
tx_hex	010000001cfbd41e842b9f6752b8a76e4803ded991bdbf0c1ec193e5add bfc8467c1b6d1c010000006b483045022100ae906a357c927d170f19710a ca1de3c5ebcbe2c60fe9626b24ed876d7f23fad40220354d0b0c25467981 7deac98f4fcfa33be48eaf74c77a2e0b4db2046747cb2b3d012102ce592b 293c6688ca587dea59780acca8da8215d4d3261db338e9ea39fc46ae19ff ffffff02000000000000000066a046861686120e0b201000000001976a9 14fa25611aeeed75a33a9fc8cc83d2039059c37d83788ac00000000

Bảng 2.2: Ví dụ về giao dịch testnet Bitcoin

Trong sơ đồ này, bằng cách giải mã OP RETURN 1634230632, chúng ta có thể nhận được thông báo "Haha". OP RETURN có thể lưu trữ các tin nhắn. Trong triển khai này, chúng tôi sử dụng nó để lưu trữ các chữ ký vòng và id ứng cử viên.

2.3 Mật mã học

2.3.1 Thuật toán RSA

Thuật toán RSA là một loại thuật toán mật mã không đối xứng được sử dụng để mã hóa và giải mã các thông điệp [29]. Tính bảo mật của nó dựa trên độ khó của việc phân hủy số nguyên lớn. Có rất nhiều cách triển khai trong thực tế. Thuật toán cụ thể có thể được mô tả như sau.

1. Chọn hai số nguyên tố lớn khác nhau.
2. Xác định $n = pq$, $\varphi(n) = (p - 1)(q - 1)$.
3. Chọn $e \in [0, \varphi(n) - 1]$.
4. Tính nghịch đảo nhân mô-đun của $\varphi(n)$ dưới dạng d đảm bảo $ed = 1 \bmod \varphi(n)$.
5. Xác định e , n là khóa công khai và p , q , d là khóa riêng.
6. Mã hóa: Cho thông điệp x , tính $y = x^e \bmod n$ để mã hóa tin nhắn bằng cách sử dụng khóa công khai (e, n) .
7. Giải mã: Cho bản mã y , tính $x = y^d \bmod n$ để mã hóa tin nhắn bằng cách sử dụng khóa riêng (p, q, d) .

2.3.2 Chữ ký chiếc nhẫn

Năm 2001, Rivest, Shamir và Tauman đưa ra một câu hỏi rằng làm thế nào để rò rỉ một bí mật [28]. Để trả lời câu hỏi này, họ đã kể một câu chuyện về một thành viên nội các đưa tin chống lại Thủ tướng. Bob là một thành viên trong nội các muốn tiết lộ một thông điệp về các hoạt động bất hợp pháp về Thủ tướng cho nhà báo. Để đảm bảo an toàn cho mình, Bob phải thông báo cho anh ta một kênh ẩn danh sau đó nhà báo có thể dễ dàng xác minh danh tính nội các của anh ta.

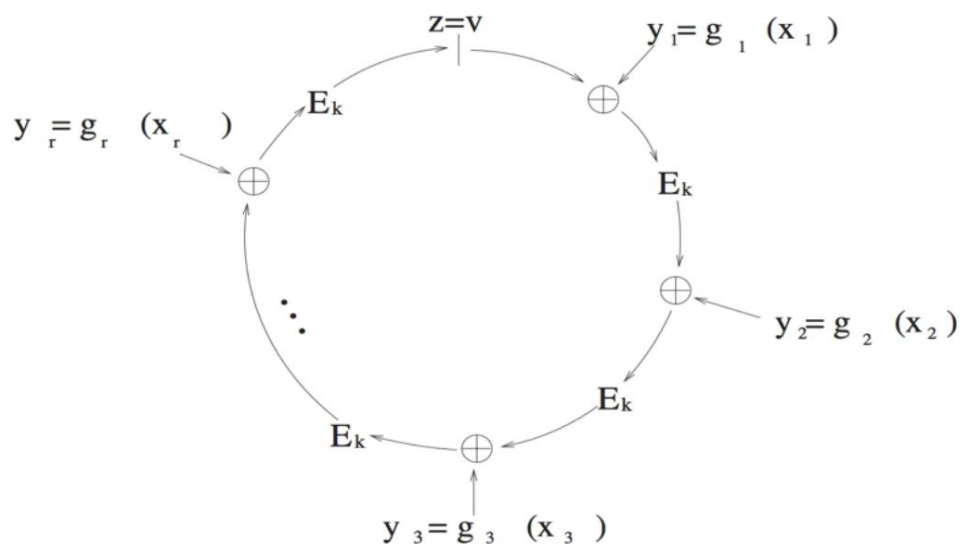
Để giải quyết vấn đề này, Bob không thể sử dụng lược đồ chữ ký nhóm để gửi tin nhắn vì anh ta không thể xác nhận xem quản trị viên nhóm có được kiểm soát bởi Thủ tướng hay không.

Họ đã đề xuất một kế hoạch mới được gọi là chữ ký vòng và mỗi thành viên của nội các là thành viên trong vòng và mọi người đều bình đẳng và ẩn danh.

Sơ đồ chữ ký vòng có thể được mô tả như sau. Giả sử sơ đồ có một, anh ta có khóa công khai của số thành viên n . Đối với mỗi người dùng u_i , riêng mình và khóa riêng của mình x_i và họ ngồi xuống trong một vòng như Hình 2.3.

Lược đồ có thể được chia thành 3 phần: Tạo một cặp khóa, tạo một ký hiệu vòng và xác minh chữ ký.

Tạo cặp khóa: Một thuật toán tạo cặp khóa cho người ký thông qua tính toán ki khóa đối xứng. Thuật toán có thể tính toán từng khóa công khai y_i và khóa riêng tư x_i từ ki .



Hình 2.3: Chữ ký vòng

Tạo chữ ký vòng: Bằng cách nhập thông điệp m , các số của n và danh sách khóa công khai của nó $L = y_1, y_2, y_3, \dots, y_n$ và khóa riêng x_i của người ký, thuật toán có thể xuất ra một chữ ký được gọi là chữ ký vòng như σ .

Xác minh chữ ký: Bằng cách nhập tin nhắn m và chữ ký để kiểm tra σ . Nếu σ là chữ ký của m , đầu ra true và đầu ra khác false.

Đối với chữ ký vòng, các đặc tính bảo mật và ưu điểm có thể được tách biệt thành tính ẩn danh và tính không thể hiểu được [28].

1. Ẩn danh vô điều kiện. Ngay cả khi kẻ tấn công đánh cắp tất cả các khóa riêng của người bỏ phiếu, xác suất xác nhận danh tính của người bỏ phiếu sẽ nhỏ hơn $1/n$, n là số của tất cả các thành viên trong vòng.

2. Tính không khả thi. Ngay cả khi kẻ tấn công bên ngoài giả mạo chữ ký vòng phù hợp với thông điệp m mà không có bất kỳ khóa cá nhân nào của những người bỏ phiếu, xác suất trùng hợp có thể bị bỏ qua.

3. So với lược đồ chữ ký nhóm, không có quản trị viên nào trong nhóm đối với lược đồ chữ ký vòng. Mọi thành viên đều bình đẳng và chương trình không cần bất kỳ bên thứ ba đáng tin cậy nào.

Chương 3

Giao thức

3.1 Định nghĩa

Giao thức được đề xuất bao gồm ba thực thể: Cử tri (Vi), RA (Cơ quan đăng ký), EA (Cơ quan bầu cử) và Nhóm địa chỉ Bitcoin.

Cử tri (Vi): Các cử tri nên là một tập hợp các danh sách. Đối với mỗi cử tri bỏ phiếu có thể được định nghĩa là Vi .

Ứng viên (Ci): Các ứng cử viên phải là một tập hợp các danh sách. Đối với mỗi ứng cử viên để bỏ phiếu có thể được định nghĩa là Ci .

Cơ quan đăng ký (RA): Ban đầu, các cử tri nên đăng ký làm sổ đăng ký trong hệ thống bỏ phiếu điện tử hiện tại. Người bỏ phiếu nên lưu khóa công khai (PKi) và địa chỉ Bitcoin (Ai) của họ vào hệ thống này và hệ thống chuyển nó vào cơ sở dữ liệu. Đối với RA, nó cung cấp ứng cử viên (Ci) cho các cử tri.

Cơ quan bầu cử (EA): Cơ quan bầu cử có trách nhiệm kiểm đếm số phiếu bầu. EA có địa chỉ Bitcoin (AE) của riêng mình. Khi cuộc bỏ phiếu kết thúc, EA sẽ bắt đầu kiểm phiếu và chuyển kết quả đến hệ thống bình chọn.

Nhóm địa chỉ Bitcoin: Nhóm địa chỉ Bitcoin là danh sách tất cả các địa chỉ Bitcoin được tạo ngẫu nhiên từ hệ thống EA bằng cách sử dụng thuật toán ECC. Khóa riêng SKAi của mỗi địa chỉ sẽ lưu trữ vào hệ thống EA.

Giám sát công khai: Để xây dựng giao thức này, một số nội dung phải được công khai và được giám sát dưới sự giám sát của bất kỳ ai như là phần kiểm toán mở. Bất kỳ ai cũng có thể kiểm tra tính đầy đủ và hợp lệ của nó. Tất cả các khóa công khai của PK người bầu cử (ở đây là BitCoin) phải được công khai thông qua API bên trong của hệ thống mà không cần bất kỳ sự cho phép nào.

3.2 Giao thức

3.2.1 Đề cương

Toàn bộ quá trình phát triển giao thức bao gồm bảy giai đoạn tuần tự, mỗi giai đoạn được thực hiện bởi các tác nhân khác nhau.

Giai đoạn chuẩn bị: Để bắt đầu, Cơ quan bầu cử (EA) nên thiết lập một dự án bỏ phiếu mới trước tiên, và sau đó lưu trữ địa chỉ BitCoin làm khóa cá nhân vào hệ thống EA.

Giai đoạn Đăng ký Đầu tiên: Các trạm đăng ký bỏ phiếu do Cơ quan Đăng ký (RA) điều hành nằm gần các khu dân cư. Các cử tri và ứng cử viên bầu cử đủ điều kiện bỏ phiếu sau khi chứng thực hộ chiếu hoặc các giấy tờ tùy thân cần thiết khác. Một mã đăng ký ngẫu nhiên sẽ được RA gửi cho người tham gia dưới dạng một liên kết thông qua email.

Giai đoạn đăng ký thứ hai: Khi người tham gia nhấp vào liên kết mã đăng ký ngẫu nhiên do RA gửi, họ có thể tạo khóa công khai và khóa cá nhân bằng cách sử dụng công cụ cặp khóa hoặc công cụ RSA cục bộ. Khóa công khai mới được tạo nên được lưu trữ trong hệ thống, trong khi khóa cá nhân có thể được giữ riêng tư.

Giai đoạn Xuất bản: Vào ngày kết thúc bỏ phiếu, mọi khóa công khai từ các cử tri sẽ được thu thập dưới sự giám sát. Miễn là nút bắt đầu bỏ phiếu đã được nhấp, RA sẽ

không chấp nhận yêu cầu đăng ký mới nữa.

Giai đoạn bỏ phiếu: Khi cử tri sử dụng khóa cá nhân của họ để ký tên vào ứng cử viên thuận lợi, họ sẽ nhận được một chữ ký nhấn duy nhất sẽ được truyền vào blockchain. Giao thức không yêu cầu mọi cử tri phải tham gia trong giai đoạn bỏ phiếu.

Giai đoạn kiểm phiếu: Giai đoạn kiểm đếm được giám sát chặt chẽ bởi công chúng, mọi người có thể truy cập vào trang kiểm đếm để xem hoặc bỏ phiếu.

Giai đoạn xác minh: Để theo dõi tính hợp lệ của kết quả bỏ phiếu, lịch sử giao dịch EA được mở công khai trên blockchain.

3.2.2 Các giả định

Giao thức được đặt dưới các giả định để thúc đẩy các thuộc tính của quyền riêng tư và khả năng xác minh.

1. Cơ quan Đăng ký và Cơ quan Bầu cử sẽ không tương ứng.
2. Thuật toán băm sha256 () là an toàn.
3. Mọi diễn viên sẽ làm theo các giai đoạn để ghi danh sự kiện bình chọn.

Bây giờ chúng ta sẽ trình bày chi tiết các giai đoạn mà chúng ta đã nói trước đó.

3.2.3 Giai đoạn chuẩn bị

Các chi tiết của giai đoạn này có thể được mô tả theo thứ tự như sau.

1. EA lưu khóa cá nhân Bitcoin (SKb) của riêng mình vào hệ thống.
2. Hệ thống sẽ tạo địa chỉ Bitcoin của EA (AEA) từ khóa cá nhân Bitcoin (SKb) của anh ấy.
3. EA tạo một mục biểu quyết mới với id biểu quyết (Li), tiêu đề, giới hạn của

số biểu quyết (n) và mô tả của mục biểu quyết này.

4. Hệ thống EA sẽ tạo ra số địa chỉ bitcoin n ($A_1, A_2 \dots A_n$) là

Nhóm địa chỉ Bitcoin tự động.

3.2.4 Giai đoạn đăng ký đầu tiên

Các chi tiết của giai đoạn này có thể được mô tả theo thứ tự như sau.

1. Ứng viên (C_i) cầm hộ chiếu của mình và đích thân xác thực với RA.
2. RA xác minh danh tính của ứng viên và hỏi tên của anh ta, mô tả cá nhân của anh ta

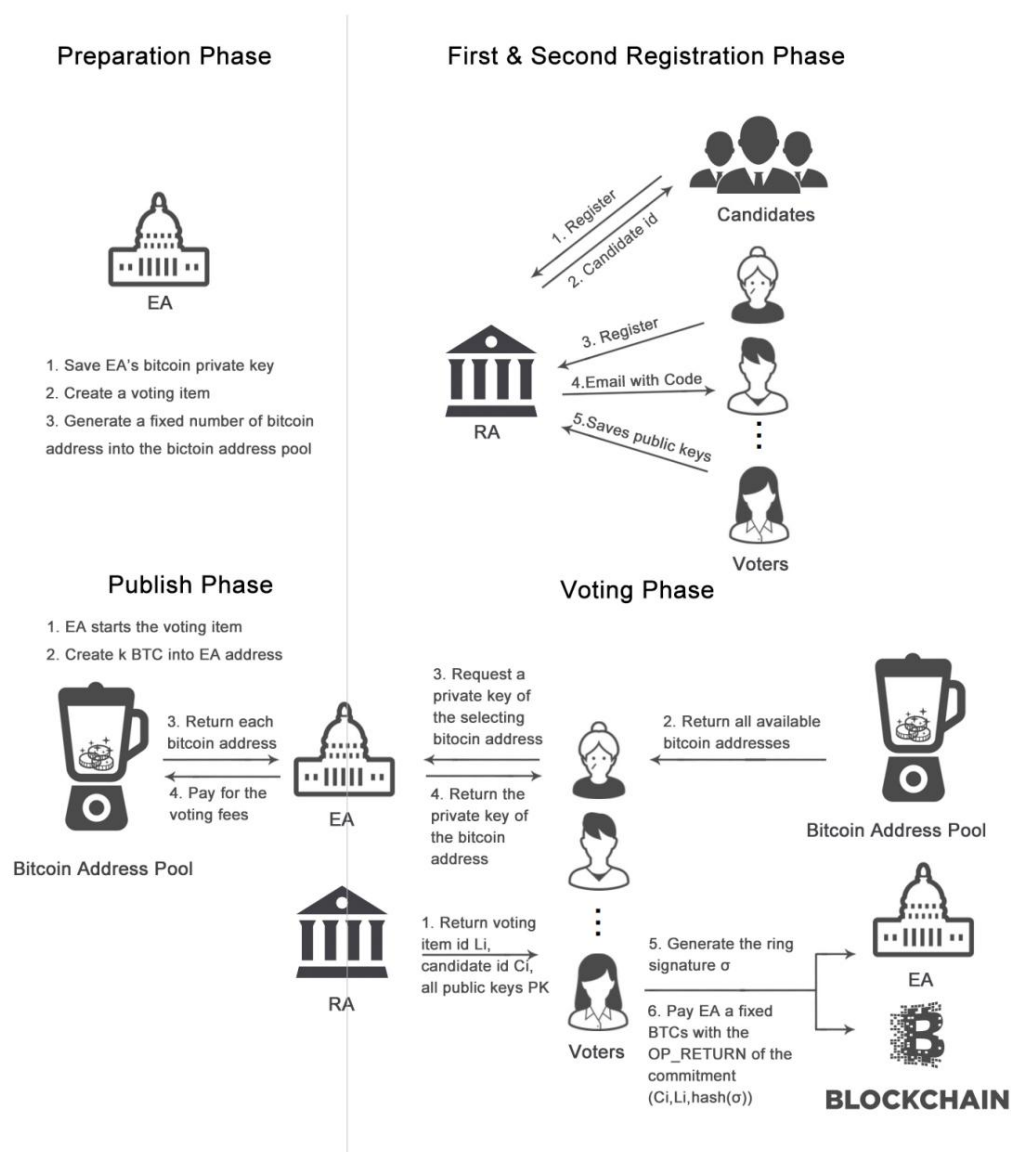
và lưu nó vào hệ thống RA.

3. RA sẽ tạo và cung cấp cho anh ta id ứng cử viên của anh ta (C_i).

4. Cử tri (V_i) cầm hộ chiếu của mình và đích thân xác thực với RA.

5. RA xác minh danh tính của cử tri và hỏi địa chỉ email của cử tri sau đó gửi cho anh ta một email với liên kết mã đăng ký ngẫu nhiên là LK_i để tránh đăng ký nhiều lần.

6. LK_i được tạo ngẫu nhiên và không có mối quan hệ với tên của người bình chọn và địa chỉ email của anh ấy.



Hình 3.1: Nghị định thư đề xuất (Chủ yếu là các giai đoạn)

3.2.5 Giai đoạn đăng ký thứ hai

Các chi tiết của giai đoạn này có thể được mô tả theo thứ tự như sau.

1. Người bình chọn mở các liên kết đăng ký LK_i .
2. Người bình chọn Vi tạo cặp khóa của mình (SK_i , PK_i).
3. Người bình chọn Vi lưu PK_i khóa công khai của mình vào hệ thống.
4. Khi kết thúc đăng ký, tập hợp các cử tri phải được cố định là một số n .

3.2.6 Giai đoạn xuất bản

Các chi tiết của giai đoạn này có thể được mô tả theo thứ tự như sau.

- 1. Vào ngày kết thúc bỏ phiếu, EA quyết định bắt đầu bỏ phiếu có nghĩa là vòng khóa công khai đã được xác nhận và RA sẽ không chấp nhận bất kỳ yêu cầu đăng ký nào.
- 2. EA tạo k BTC trong tài khoản Bitcoin của riêng mình.
- 3. EA trả một lượng k / n bitcoin cố định làm phí biểu quyết cho mỗi Ai, chẳng hạn như 0,0001 BTC. (Sau khi người bỏ phiếu đã bỏ phiếu, phí bỏ phiếu sẽ được gửi lại cho EA)

3.2.7 Giai đoạn bỏ phiếu

Các chi tiết của giai đoạn này có thể được mô tả theo thứ tự như sau.

- 1. Người bỏ phiếu chọn ứng cử viên Ci mà anh ta bỏ phiếu và id biểu quyết hiện tại là Li.
- 2. RA trả về bộ khóa công khai (PK1, PK2, PK3 ... PKn) cho người bỏ phiếu.
- 3. Người bình chọn sử dụng khóa riêng SKi của mình và tất cả các khóa công khai PK để ký chữ ký của ứng viên Ci là σ (Ci, SKi, (PK1, PK2, PK3 ... PKn)). Hệ thống lưu tập hợp của (σ, sha256 (σ)) cùng một lúc.
- 4. Người bỏ phiếu chọn một địa chỉ Bitcoin Ai để xuất bản từ Nhóm địa chỉ Bitcoin và EA trả lại khóa cá nhân SKAi của địa chỉ cho người bỏ phiếu.
- 5. Người bỏ phiếu Vi thanh toán tất cả số dư của Ai the đến EA địa chỉ AEA với OP RETURN – cam kết (sha256 (σ (Ci, SKi, (PK1, PK2, PK3 ... PKn))), Ci, Li).

3.2.8 Giai đoạn kiểm đếm

Các chi tiết của giai đoạn này có thể được mô tả theo thứ tự như sau.

- 1. Hệ thống tự động trả về tất cả các bộ (σ, sha256 (σ)) và tất cả các khóa công khai PK.
- 2. Hệ thống tự động tìm nạp tất cả các giao dịch trong địa chỉ EA Bitcoin AEA.
- 3. Hệ thống tìm nạp biểu mẫu OP RETURN mỗi giao dịch và xác minh chữ ký σ tính hợp lệ.
- 4. Hệ thống đếm từng giao dịch hợp lệ và cộng 1 vào Ci của ứng viên.
- 5. Nếu cử tri Vi vắng mặt thì đánh dấu là bỏ phiếu trắng.
- 6. Nếu lịch sử giao dịch Bitcoin có nhiều hơn hai lần giao dịch từ cùng một Ai, hãy đếm người đầu tiên và, bỏ qua những người khác.

3.2.9 Giai đoạn xác minh

Các chi tiết của giai đoạn này có thể được mô tả theo thứ tự như sau.

- 1. Hệ thống tự động trả về tất cả các khóa công khai (PK1, PK2, PK3 ... PKn).
- 2. Đối với mỗi cử tri Vi, anh ta có thể sử dụng một tập hợp tất cả các khóa công khai (PK1, PK2, PK3 ... PKn), chữ ký chiếc nhẫn σ, ứng cử viên Ci để xác minh phiếu bầu của mình.
- 3. Người bỏ phiếu Vi có thể sử dụng id giao dịch để lấy cam kết từ blockchain để xác minh xem chữ ký có được xuất bản đúng cách hay không.

Chương 4

Thực hiện

4.1 Đặc điểm kỹ thuật

Hệ thống bỏ phiếu điện tử đã được thiết kế bằng cách sử dụng giao thức trên có tên là BlockVotes. Hệ thống sẽ có các thuộc tính về quyền riêng tư của lá phiếu, khả năng xác minh cá nhân, tính đủ điều kiện và v.v.

Khi phát triển dự án này, tôi chọn phát triển lặp đi lặp lại và tăng dần làm mô hình quá trình phát triển phần mềm. Để thực hiện, hệ thống nên xem xét các mô hình cơ bản và các thuộc tính của biểu quyết điện tử.

Nói chung, BlockVotes cho phép cử tri và ứng cử viên đăng ký trong hệ thống. Để tiết kiệm tiền khai thác, chúng tôi khuyên EA sử dụng mạng testnet để tiết kiệm phí khai thác. Người bỏ phiếu có thể bỏ phiếu trong hệ thống và bất kỳ ai cũng có thể xác minh kết quả bỏ phiếu. Cơ quan quản lý có thể được chia thành 2 cơ quan, cơ quan bầu cử và cơ quan đăng ký. Hệ thống BlockVotes nên có các mô hình như sau.

1. Mô hình người dùng là logic đăng nhập.
2. Mô hình RA là một mô hình cho Cơ quan đăng ký bao gồm các API của nó.
3. Mô hình EA là một mô hình cho Cơ quan bầu cử bao gồm các API của nó.
4. Mô hình bỏ phiếu là mô hình để cử tri đăng ký và bỏ phiếu.
5. Mô hình xác minh là một mô hình để bất kỳ ai cũng có thể xác minh chữ ký chiếc nhẫn.
5. Mô hình kiểm đếm là phần quan trọng của cuộc bỏ phiếu cho phép bất kỳ ai cũng có thể đếm kết quả của cuộc bỏ phiếu từ blockchain trong thời gian thực.

4.2 Yêu cầu

Để xây dựng một hệ thống như vậy, các yêu cầu chức năng và phi chức năng cần được thiết lập như sau.

Yêu cầu chức năng

REQ 1.1 Trang phải được chia nhỏ thành trang đăng nhập, trang EA, trang RA, công khai trang.

REQ 1.2 Máy chủ phải hiển thị các trang khác nhau cho vai trò người dùng khác nhau.

REQ 1.3 Máy chủ phải có quyền kiểm soát đặc quyền cho vai trò người dùng khác nhau.

REQ 1.4 Vai trò của người dùng nên chia thành 4 tác nhân: cử tri, Cơ quan đăng ký, Cơ quan bầu cử và công chúng.

Các trang công

khai REQ 2.1 Máy chủ phải có API công khai để công khai một số nội dung, chẳng hạn như công khai địa chỉ phim của PK người bỏ phiếu, Bitcoin AEA của Cơ quan bầu cử và các bộ (σ , sha256(σ)) mà không có bất kỳ sự cho phép nào.

REQ 2.2 Trang xác minh phải được công khai và được giám sát theo giao thức.

REQ 2.3 Trang kiểm đếm phải công khai và được giám sát theo quy trình.

REQ 2.4 Trang bỏ phiếu phải ở chế độ công khai.

REQ 2.5 Trang biểu quyết phải có thể sử dụng thuật toán chữ ký vòng để ký thông điệp.

REQ 2.5 Trang bỏ phiếu phải có thể thực hiện giao dịch với địa chỉ tài khoản blockchain của EA để phát thông báo trên blockchain.

REQ 2.5 Trang bỏ phiếu phải có thể thực hiện giao dịch với địa chỉ tài khoản blockchain của EA để phát thông báo trên blockchain.

REQ 2.6 Trang xác minh có thể lấy mã OP RETURN từ id giao dịch mà người bỏ phiếu nhập.

REQ 2.7 Trang xác minh có thể giải mã cam kết mã OP RETURN cho ứng viên và chữ ký.

REQ 2.8 Trang xác minh phải có thể tìm nạp các chữ ký σ từ sha256 (σ) được tìm nạp từ mã OP RETURN của blockchain thông qua API công khai.

REQ 2.9 Trang xác minh phải có thể xác minh tính hợp lệ của chữ ký vòng σ .

REQ 2.10 Trang xác minh phải có khả năng xác minh tính toàn vẹn của tất cả các khóa công khai.

REQ 2.11 Trang xác minh sẽ có thể xác minh tính đúng đắn giữa các chữ ký và giá trị băm của các chữ ký (σ , sha256 (σ)).

REQ 2.12 Trang xác minh có thể chọn một mục biểu quyết và sau đó chuyển hướng đến trang xác minh tương ứng của nó.

REQ 2.13 Trang kiểm đếm phải có thể tìm nạp tất cả các giao dịch của tài khoản blockchain EA.

REQ 2.14 Trang kiểm đếm phải có thể tìm nạp các chữ ký σ từ sha256 (σ) được tìm nạp từ mã OP RETURN của blockchain thông qua API công khai.

REQ 2.14 Trang kiểm đếm có thể giải mã cam kết mã OP RETURN cho ứng viên và chữ ký.

REQ 2.15 Trang kiểm đếm phải có thể xác minh tính đúng đắn giữa các chữ ký và giá trị băm của các chữ ký (σ , sha256 (σ)).

REQ 2.16 Trang kiểm đếm có thể chọn một mục biểu quyết và sau đó chuyển hướng đến trang kiểm đếm tương ứng của nó.

REQ 2.17 Trang kiểm đếm phải có khả năng xác minh tính hợp lệ của chữ ký vòng σ .

REQ 2.17 Trang kiểm đếm phải có thể kiểm đếm và hiển thị kết quả biểu quyết trong thời gian thực.

Trang đăng ký REQ

3.1 Trang đăng ký phải xác minh tính hợp lệ của mã liên kết, nếu không hợp lệ, hiển thị trang bị cấm.

REQ 3.2 Trang đăng ký có thể cung cấp trình tạo cặp khóa bằng cách sử dụng RSA và chạy tất cả trong giao diện người dùng.

REQ 3.3 Trang đăng ký nên lưu khóa công khai của mỗi cử tri vào hệ thống Cơ quan đăng ký.

REQ 3.4 Trang đăng ký có thể chỉnh sửa khóa công khai nếu cuộc bỏ phiếu chưa được bắt đầu.

REQ 3.5 Trang đăng ký có thể hiển thị ngày bỏ phiếu nếu người bỏ phiếu điền khóa công khai.

REQ 3.6 Trang đăng ký có thể hiển thị mô tả của mục biểu quyết này.

Trang Cơ quan Đăng ký (Trang RA)

- REQ 4.1 Hệ thống RA phải thiết lập tài khoản STMP để gửi email cho cử tri.
- REQ 4.2 Hệ thống RA phải có cơ sở dữ liệu để lưu trữ tất cả các mã liên kết.
- REQ 4.3 Hệ thống RA phải có thể thêm một ứng cử viên có tên và mô tả của anh ta.
- REQ 4.4 Hệ thống RA phải có thể chỉnh sửa hoặc xóa một ứng cử viên.
- REQ 4.5 Hệ thống RA phải có khả năng tạo mã liên kết bằng cách sử dụng một thuật toán ngẫu nhiên.
- REQ 4.6 Hệ thống RA phải cung cấp một API để người bầu chọn lấy id, tên và mô tả của tất cả các ứng cử viên.

Trang Cơ quan Bầu cử (Trang EA)

- REQ 5.1 Hệ thống EA sẽ có thể tạo một mục biểu quyết với tiêu đề, số biểu quyết tối đa n và mô tả.

- REQ 5.1 Hệ thống EA sẽ có thể chỉnh sửa hoặc xóa một mục biểu quyết.
- REQ 5.2 Hệ thống EA có thể xem tất cả các ứng viên.
- REQ 5.3 Hệ thống EA phải có khả năng lưu trữ khóa cá nhân tài khoản blockchain của EA.
- REQ 5.4 Hệ thống EA phải có khả năng chuyển đổi khóa cá nhân của tài khoản blockchain EA thành địa chỉ bitcoin của EA.
- REQ 5.5 Hệ thống EA có thể thiết lập các mạng blockchain khác nhau, chẳng hạn như Bitcoin (BTC) và Bitcoin testnet (TESTNET).
- REQ 5.6 Hệ thống EA phải cung cấp một API cho người bỏ phiếu để tìm nạp các khóa cá nhân từ Nhóm địa chỉ Bitcoin.
- REQ 5.7 Hệ thống EA phải có khả năng tạo một số n địa chỉ Bitcoin và các khóa riêng của nó vào Nhóm địa chỉ Bitcoin một cách ngẫu nhiên.
- REQ 5.8 Hệ thống EA phải có khả năng thực hiện các giao dịch trên mạng blockchain giữa các địa chỉ của Bitcoin Address Pool và địa chỉ Bitcoin AEA của chính nó.
- REQ 5.9 Hệ thống EA phải có khả năng tìm nạp tất cả các giao dịch của tài khoản blockchain EA.

Những yêu cầu phi lý

- REQ 6.1 Phần phụ trợ nên được phát triển trong PHP bằng cách sử dụng khuôn khổ MVC.
- REQ 6.2 Giao diện người dùng nên được phát triển bằng Javascript.
- REQ 6.3 Thời gian phản hồi của trang biểu quyết phải dưới 300 mili giây.
- REQ 6.4 Thời gian phản hồi của API công khai phải dưới 300 mili giây.
- REQ 6.5 Thời gian phản hồi của trang bỏ phiếu phải dưới 300 mili giây.
- REQ 6.6 Hệ thống có thể sử dụng API của bên thứ ba để thực hiện giao dịch trên blockchain.
- REQ 6.7 Hệ thống kiểm đếm phải đủ ổn định để hiển thị kết quả chính xác.
- REQ 6.8 Hệ thống bỏ phiếu phải đủ ổn định để phát đi cam kết chuỗi khối.
- REQ 6.9 Hệ thống nên sử dụng cơ sở dữ liệu quan hệ để lưu trữ thông tin của mục bỏ phiếu, địa chỉ Bitcoin của các ứng cử viên và cử tri.
- REQ 6.10 Hệ thống nên được kiểm tra với trình duyệt và hệ điều hành khác nhau.
- REQ 6.10 Trang công khai phải có trải nghiệm người dùng thân thiện.

4.3 Mô hình BlockVotes và Cây ghép

BlockVotes đã được phát triển bằng ngôn ngữ lập trình PHP. Để làm rõ ràng logic, khuôn khổ MVC có tên Slim đã được sử dụng để định tuyến trang. Laravel / Illuminate được sử dụng cho Đối tượng truy cập dữ liệu (DAO) và TWIG được sử dụng để kết nối trang front-end với back-end. Để quản lý các phần phụ thuộc, Composer đã được sử dụng làm công cụ quản lý phần phụ thuộc. Hệ thống được phát triển với cơ sở dữ liệu MYSQL và testnet của Bitcoin. Git được sử dụng để kiểm soát phiên bản của toàn bộ dự án.

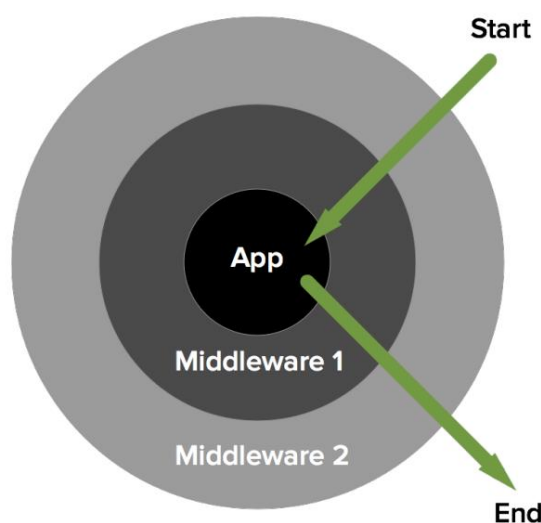
Để xây dựng hệ thống này, nhiều thư viện của bên thứ ba đã được lựa chọn. Kho lưu trữ từ Github có tên chữ ký vòng để tạo chữ ký. BitcoinJS được sử dụng để tạo hex Tx. BitcoinECDSA đã được sử dụng để tạo địa chỉ tài khoản blockchain.

Để phát một hex Tx trên blockcahin, không cần thiết phải thiết lập một ứng dụng khách blockchain cục bộ. Có rất nhiều API quảng bá. Đối với việc cấy ghép này, SoChain và smartbit đã được chọn để tìm nạp các giao dịch từ chuỗi khối hoặc phát một hệ lục phân Tx.

4.3.1 Mô hình người dùng

Theo giao thức, người dùng có thể được chia thành cử tri, ứng cử viên, RA, EA và giám sát công khai.

Khi EA hoặc RA muốn đăng nhập vào hệ thống, anh ta có thể sử dụng tên người dùng và mật khẩu của mình để nhập vào hệ thống. Hệ thống sẽ kiểm tra mật khẩu xem có đúng không. Và nếu đúng, họ sẽ nhập vào các trang khác nhau tùy theo vai trò người dùng của nó. Nếu mật khẩu không khớp, hệ thống sẽ thông báo cho họ biết.



Hình 4.1: Phần mềm trung gian của Slim framework [31]

Bằng cách sử dụng phần mềm trung gian của khuôn khổ, việc kiểm soát đặc quyền có thể dễ dàng được đề cập. Phần mềm trung gian cho phép nhà phát triển thực hiện một hành động cụ thể sau khi tải khung-

hoạt động nhưng trước khi chạy bộ điều khiển ứng dụng như Hình 4.1.

Đây là một mẫu mã kiểm soát đặc quyền cho EA. Để đánh giá vai trò của người dùng, hệ thống nên tìm nạp vai trò người dùng biểu mẫu vùng chứa. Nếu vai trò người dùng không phải là 2 (id vai trò của EA người dùng), hệ thống sẽ không cho phép người dùng xem.

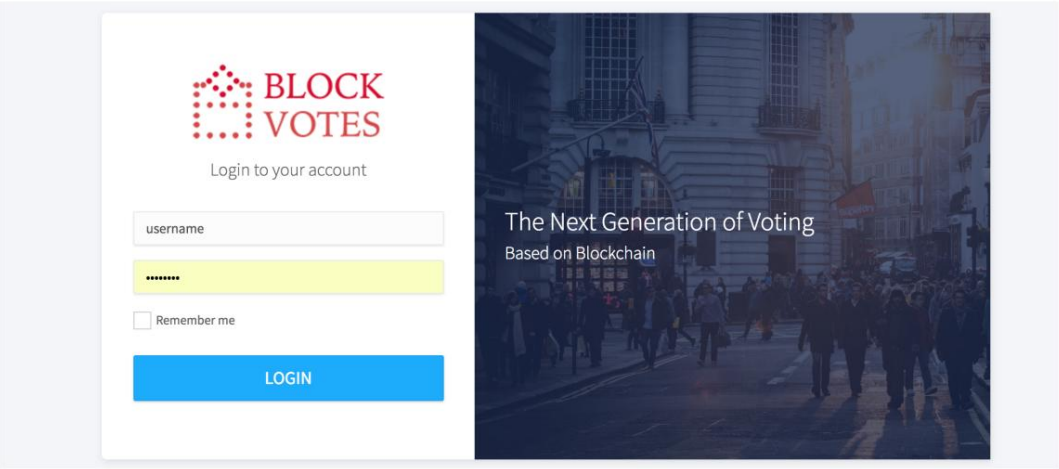
```
1 hàm công khai __invoke ($ yêu cầu, $ phản hồi, $ tiếp theo) {
2     if (! $ this -> container -> auth -> check ()) {
3         $ this -> container -> flash -> addMessage ( 'lỗi', 'Làm ơn thoát mái đi si gninbefore
        d oin gthat ' );
4         return $ response -> withRedirect ($ this -> container -> router -> pathFor ( '
        auth. đăng nhập ' ));
5     } else if ( $ this -> container -> auth -> user () -> role! = 2) {
6         $ this -> container -> flash -> addMessage ( 'show to lỗi', 'Trang này onl y
        the El ec ti on Au th o ri ty' );
7         return $ response -> withRedirect ($ this -> container -> router -> pathFor ( '
        nha ' ));
8     }
9     $ response = $ tiếp theo ($ yêu cầu, $ phản hồi);
10    trả về $ phản hồi;
11 }
```

Trong hệ thống BlockVotes, vai trò người dùng có thể được mô tả như sau.

id tên người dùng biệt hiệu			vai trò mật khẩu	
1	ngày	Cơ quan đăng ký ...		1
2	của	Cơ quan bầu cử	...	2

Bảng 4.1: Bảng vai trò người dùng

Đây là thiết kế giao diện người dùng đăng nhập cho EA và RA. Đối với cử tri hoặc công chúng, họ không cần đăng nhập và nhập URL để vào trang.



Hình 4.2: Giao diện đăng nhập

4.3.2 Mô hình RA

Đối với Cơ quan đăng ký, họ ký trong hệ thống và phục vụ cử tri và ứng cử viên.

Như vậy, hệ thống phải thỏa mãn các tính năng cơ bản này.

- Thêm một cử tri với địa chỉ email của anh ấy và gửi email cho anh ấy.
- Thêm một ứng cử viên với tên, mô tả và hình ảnh đại diện của anh ta.
- Chỉnh sửa hoặc xóa một ứng cử viên.

Khi gửi email, khung công tác sẽ tải tệp thuộc tính cấu hình env trước tiên bao gồm các thuộc tính máy chủ SMTP. Và sau đó hệ thống sử dụng sự phụ thuộc của bên thứ ba có tên Swift Mailer để tạo kết nối với máy chủ SMTP và đăng email lên địa chỉ email mục tiêu. Một số mã từng phần có thể được viết như dưới đây.

```
1 $ transport = (new \ Swift_SmtpTransport ( getenv ( 'SMTP_SERVER' ), -getenv ( '
    CỘNG SMTP.' ) ssl' ) ) ,
2         -> setUsername ( getenv ( 'SMTP_USERNAME' ) )
3         -> setPassword ( getenv ( 'MẬT KHẨU SMTP' ) );
4 $ mailer = new \ Swift_Mailer ( $ vận chuyển );
5 $ message = (new \ Swift_Message ( 'S tart your vo te now' ) )
6         -> setFrom ( array ( getenv ( 'SMTP_USERNAME' ) => -> 'Nhóm BlockVotes' ) )
7         setTo ( array ( $ email => Người bình chọn ' ) )
8         -> setBody ( $ content )
9         -> setContentType ( "text / html" );
```

Hình 4.3: Thêm giao diện cử tri

Để tạo liên kết mã, mã phải ngẫu nhiên và không có mối quan hệ với danh tính cử tri. Kỹ thuật đằng sau liên kết mã là sử dụng thuật toán ngẫu nhiên.

```
1 hàm công khai makeCard () {
2 $ ngẫu nhiên = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";
```



```

3 $ kết quả = "";
4 cho ($ i = 0; $ i < 16; $ i ++ )
5     $ results. = $ randomdict [ mt_rand (0 , strlen ($ chars) -1)];
6 trả về kết quả $;
7 }

```

The screenshot shows the 'Candidate Registration' interface. On the left is a dark sidebar with navigation links: Dashboard, Voters, Candidates (selected), Add a candidate, Candidate List, View Result, Change Password, and Sign Out. The main content area is divided into two sections. The left section, titled 'Addition Photo', contains an 'Avatar' placeholder and an 'Upload' button. The right section, titled 'Candidate Registration', contains a form with three main parts: 'Candidate Name / Vote Item Name' with a text input containing 'Yifan', 'Description' with a text area containing 'Candidate short description', and 'Vote For' with a dropdown menu showing '2017 Student Union Election'. A green 'Create' button is at the bottom right of the form.

Hình 4.4: Thêm giao diện ứng viên

The screenshot shows the 'Candidate List' for the '2017 Student Union Election'. The sidebar is the same as in the previous screenshot. The main content area has a dropdown menu at the top showing '2017 Student Union Election' and a 'Go!' button. Below this is a grid of six candidate cards. Each card displays the candidate's name, ID, a short description, and 'Edit' and 'Delete' buttons. The candidates are: Tanno Tom (#1) with description 'I can lead you to the future.', Yifan Wu (#2) with 'Please vote me!', Taylor Hayward (#3) with 'I love you guys', Rhys Scott (#4) with 'Vote me! Vote me!', Andrew Phillips (#5) with 'No reasons', and Fernando Arcuri (#6) with 'For the future of student life'.

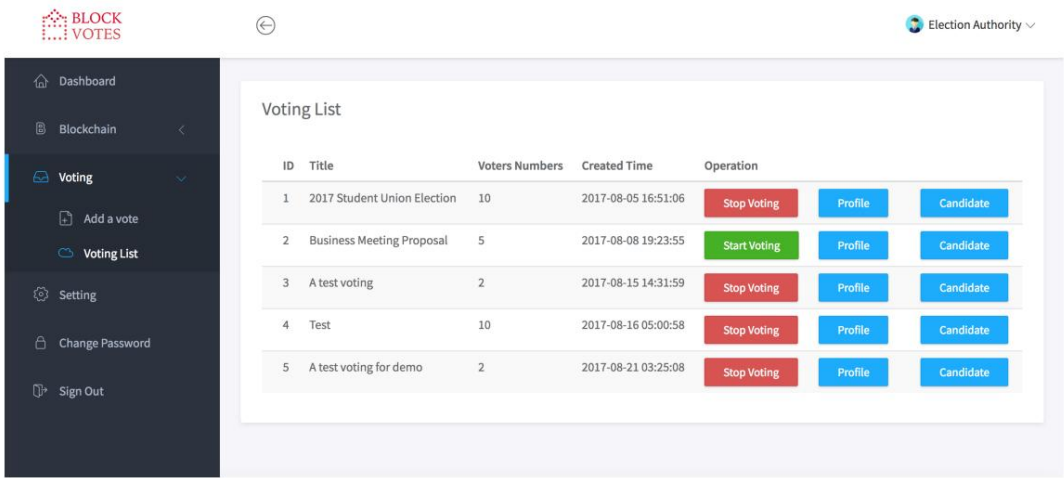
Hình 4.5: Giao diện quản lý ứng viên RA

4.3.3 Mô hình EA

Đối với Cơ quan bầu cử, hệ thống phải đáp ứng các tính năng cơ bản này.

- Bảng điều khiển để hiển thị số dư của tài khoản chuỗi khối EA, chuỗi khối mạng và thông tin bỏ phiếu.
- Kiểm tra số dư của tài khoản blockchain được tạo từ Nhóm địa chỉ Bitcoin.
- Trả phí bỏ phiếu cho tất cả hoặc một địa chỉ tài khoản blockchain duy nhất.
- Tạo sự kiện bình chọn với tiêu đề, mô tả và hình ảnh.
- Chỉnh sửa hoặc xóa một sự kiện biểu quyết.
- Bắt đầu hoặc dừng một sự kiện biểu quyết.
- Xem ứng cử viên của một sự kiện bỏ phiếu.
- Trang cài đặt để thiết lập khóa cá nhân của chuỗi khối EA.

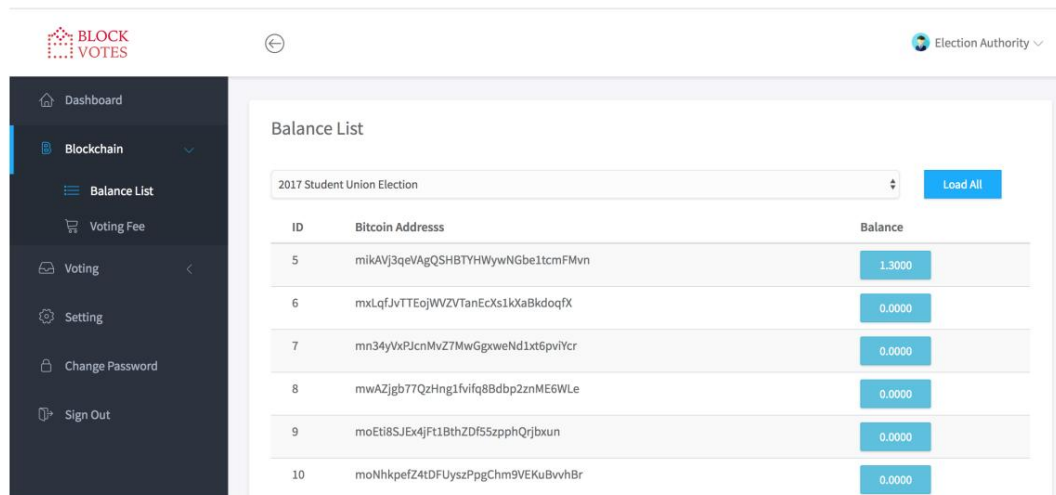
Khi EA tạo một mục bỏ phiếu, hệ thống sẽ sử dụng BitcoinECDSA phụ thuộc để tạo địa chỉ bitcoin với số đầu vào là n.



Hình 4.6: Giao diện Quản lý Danh sách Bầu cử

EA có thể kiểm tra số dư của nhóm địa chỉ tài khoản blockchain (Nhóm địa chỉ Bitcoin) anh ấy đã tạo ra trước đó.

Để thực hiện giao dịch giữa hai địa chỉ Bitcoin, hệ thống sử dụng thư viện Javascript của bên thứ ba có tên BitcoinJS để tạo giao dịch được tuân thủ hóa dưới dạng giá trị thập lục phân. Bằng cách sử dụng API của bên thứ ba để phát giá trị thập lục phân trên blockchain, nghĩa là để thực hiện giao dịch thực sự.



The screenshot shows the BLOCK VOTES application interface. On the left is a dark sidebar with navigation links: Dashboard, Blockchain (selected), Balance List, Voting Fee, Voting, Setting, Change Password, and Sign Out. The main content area is titled 'Balance List' and shows a dropdown menu for '2017 Student Union Election' with a 'Load All' button. Below this is a table with three columns: ID, Bitcoin Address, and Balance.

ID	Bitcoin Address	Balance
5	mikAVj3qeVAgQSHBTYHwywNGbe1tcmFMvn	1.3000
6	mxLqfJvTTEojWVZVTanEcXs1kXaBkdoqfX	0.0000
7	mn34yVxPjcnMvZ7MwGgxweNd1xt6pvYcr	0.0000
8	mwAZjgb77QzHng1fvfq8Bdp2znME6WLe	0.0000
9	moEt8SJEx4jFt1BthZDf5SzpphQrjbxun	0.0000
10	moNhkpefZ4tDFUyszPpgChm9VEKuBvvhBr	0.0000

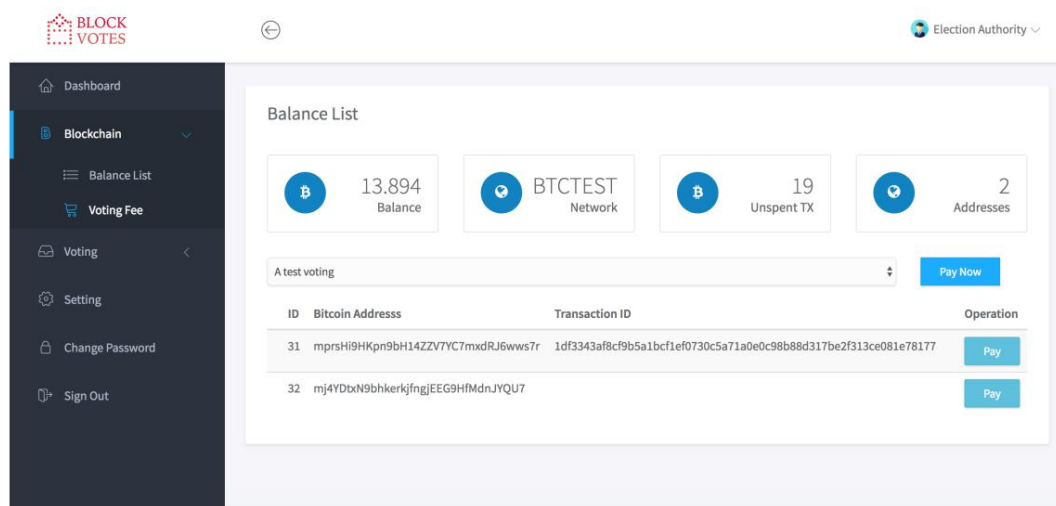
Hình 4.7: Kiểm tra số dư của giao diện Nhóm địa chỉ Bitcoin

Đây là một mẫu mã về cách thực hiện một giao dịch từ sourceAddress đến targetAddress trên mạng thử nghiệm bitcoin.

```

1 hàm makeTransaction (itemid, targetAddress, pbbash) {
2     if (! lock) {
3         $. getJSON ("https: // chain .so / api / v2 / get_tx_unspent / BTCTEST /" +
4             địa chỉ nguồn ,function (kết quả) {
5             khóa = true ;
6             var last = kết quả. dữ liệu . txs. chiều dài - 1;
7             var unsent_txid = kết quả. dữ liệu . txs [cuối cùng]. txid;
8             var unsent_vout = kết quả. dữ liệu . txs [cuối cùng]. đầu ra không có;
9             txb = Bitcoin mới . TransactionBuilder (mạng);
10            thb. addInput (unsent_txid, unsent_vout);
11            value = Number (kết quả. dữ liệu. txs [cuối]. value * 100000000);
12            trả = 0,0001 * 100000000; // phí khai thác
13            thay đổi = parseInt (giá trị - trả tiền);
14            var commit = new Buffered (pbbash);
15            var dataScript = Bitcoin. script . nullData. đầu ra. mã hóa (cam kết);
16            txb. addOutput (dataScript, txb. 0);
17            addOutput (targetAddress, thay đổi);
18            thb. dấu (0, keyPair);
19            var txRaw = txb. xây dựng () ;
20            var txHex = txRaw. toHex ();
21            postdata = {tx_hex: txHex};
22            postTransaction (itemid, postdata);
23        });
24        trả về true ;
25    }
26 }

```

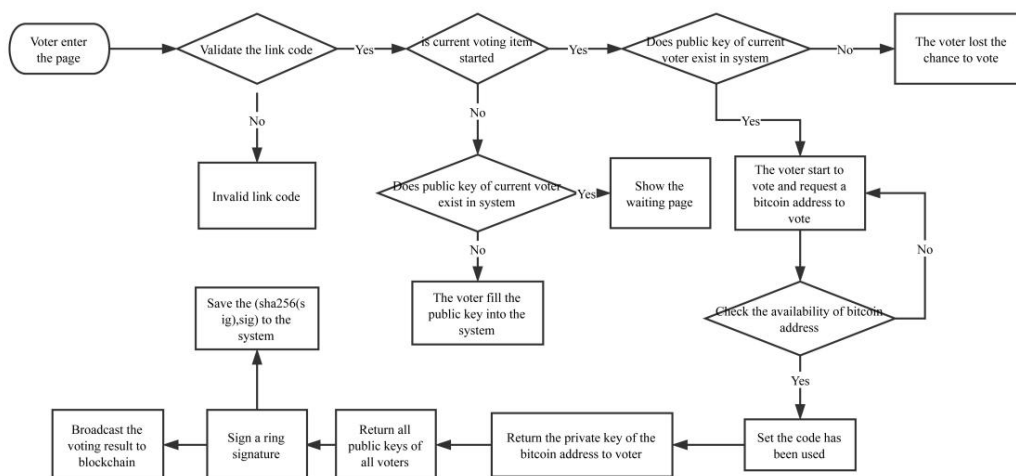


Hình 4.8: Giao diện thanh toán phí bỏ phiếu của EA

4.3.4 Mô hình bỏ phiếu

Khi người bỏ phiếu đã đăng ký trong Cơ quan đăng ký, anh ta phải mở liên kết mã từ email của mình. Khi anh ta mở liên kết, hệ thống sẽ thực hiện phân đoán logic để chuyển hướng anh ta đến trang khác. Sơ đồ logic có thể được mô tả như Hình 4.2.

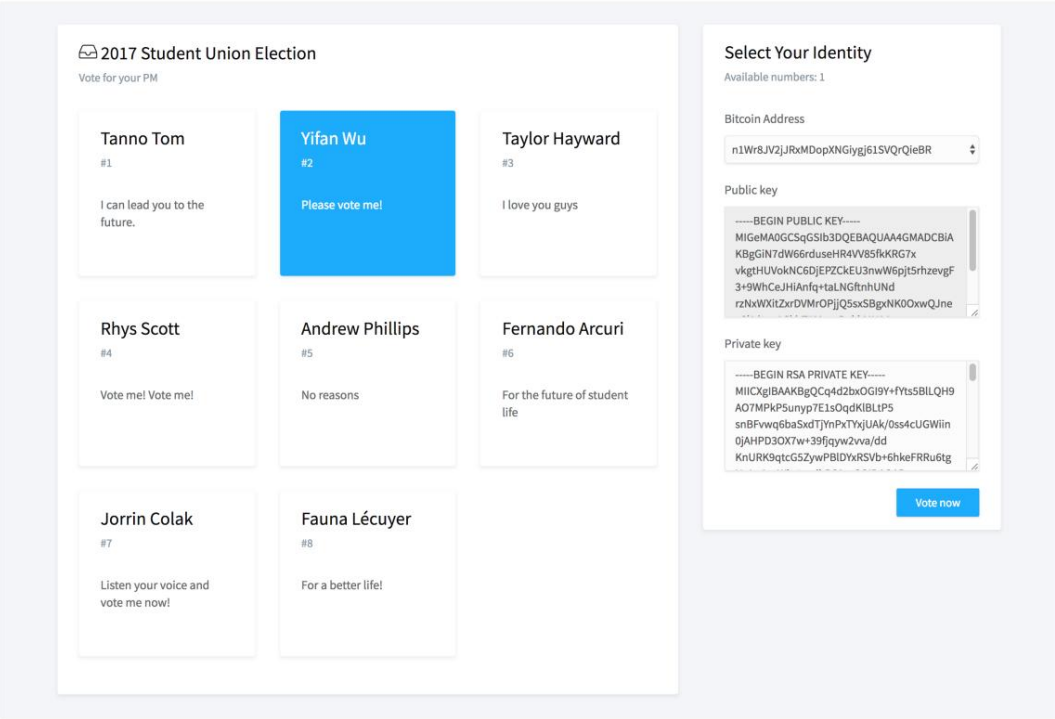
Người bỏ phiếu nên dán khóa công khai của mình và lưu vào hệ thống. Nếu trong ngày bỏ phiếu, người bình chọn mở link và hệ thống sẽ cho người đó tham gia bình chọn. Bằng cách nhập khóa cá nhân và chọn các ứng cử viên mà anh ấy bỏ phiếu, trang bỏ phiếu sẽ tự động phát phiếu bầu của anh ấy trên blockchain.



Hình 4.9: Luồng công việc logic biểu quyết

Để tạo chữ ký vòng, hệ thống sử dụng thư viện Javascript của bên thứ ba có tên chữ ký vòng. Thư viện này bao gồm các phương pháp tạo chữ ký để chuồng và xác minh chữ ký để chuồng bằng tin nhắn. Một số mã quan trọng có thể được viết như sau.

```
1 chìa khóa. push ( new JSEncryptRSAKey (value. public_key)); // đẩy khóa công khai 2 var z = Math. tăng
(Math. random () * (các phím. chiều dài +1)); 3 chìa khóa. splice (z, 0, privkey); 4 init (phím); 5 var sig
= sign (ứng cử viên z); // lấy bằng điều khiển chữ ký vòng 6 .log (key_match (sig, các phím)); // xác minh
chữ ký chiếc nhẫn
```



Hình 4.10: Giao diện quản lý ứng viên RA

4.3.5 Mô hình xác minh

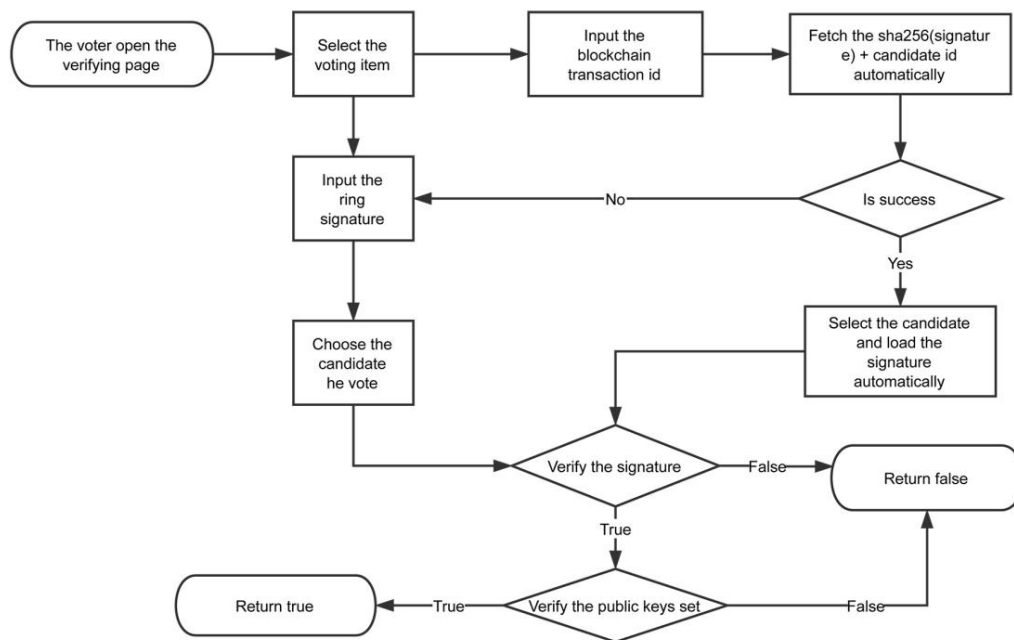
Khi người bỏ phiếu đã bỏ phiếu, người bỏ phiếu sẽ nhận được chữ ký của chiếc nhẫn hoặc id blockchain làm biên nhận. Để xác minh phiếu bầu được đếm chính xác, người bỏ phiếu nên vào trang xác minh. Sơ đồ logic có thể được thể hiện như Hình 4.11.

Hệ thống cung cấp 2 cách để xác minh kết quả bình chọn.

- 1. ID giao dịch: Nó có thể tự động tìm nạp id ứng viên, băm chữ ký vòng từ blockchain. Và sau đó nó có thể tìm nạp chữ ký vòng từ API công khai theo hàm băm của nó.

2. Chữ ký chiếc nhẫn: Người bỏ phiếu hoặc bất kỳ ai có thể nhập chữ ký chiếc nhẫn và chọn id ứng viên theo cách thủ công. Quá trình này sẽ không có kết nối với bất kỳ máy chủ nào.

Và sau đó trang xác minh sẽ sử dụng hàm Javascript `verify()` để xác minh xem ứng cử viên có khớp với chữ ký vòng như Hình 4.12 hay không. Hơn nữa, anh ta có thể kiểm tra xem các khóa công khai có khớp với API được tìm nạp từ máy chủ hay không như Hình 4.13.



Hình 4.11: Quy trình làm việc của Trang xác minh

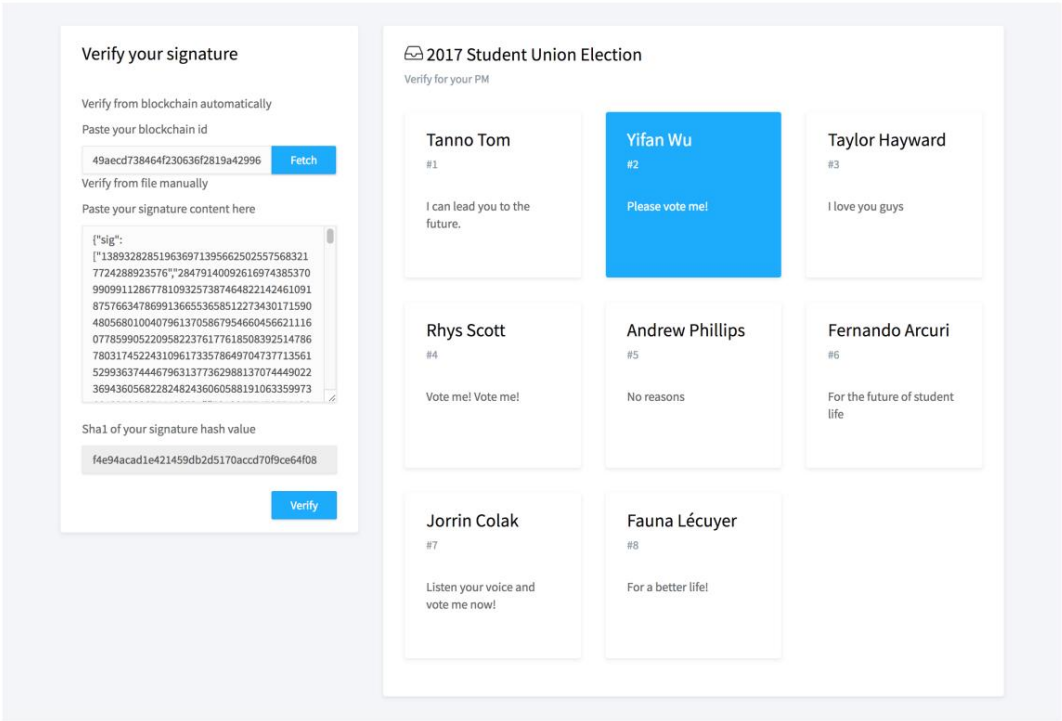
4.3.6 Mô hình kiểm đếm

Giai đoạn kiểm phiếu là phần quan trọng nhất của cuộc bỏ phiếu. Giai đoạn này phải diễn ra trong giao diện người dùng để đảm bảo bất kỳ ai cũng có thể kiểm đếm trong thời gian thực. Chi tiết của giai đoạn này có thể là được mô tả như sau.

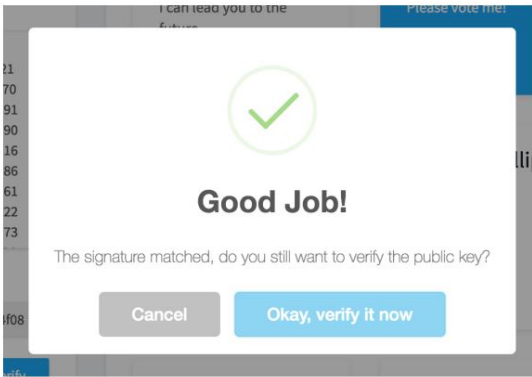
1. Tìm nạp tất cả các khóa công khai và lưu trữ nó cục bộ.
2. Tìm nạp tất cả các giao dịch của tài khoản blockchain của EA.
3. Giải mã cam kết của mã OP RETURN thành id ứng_viên và giá trị băm

của chữ ký nhẫn.

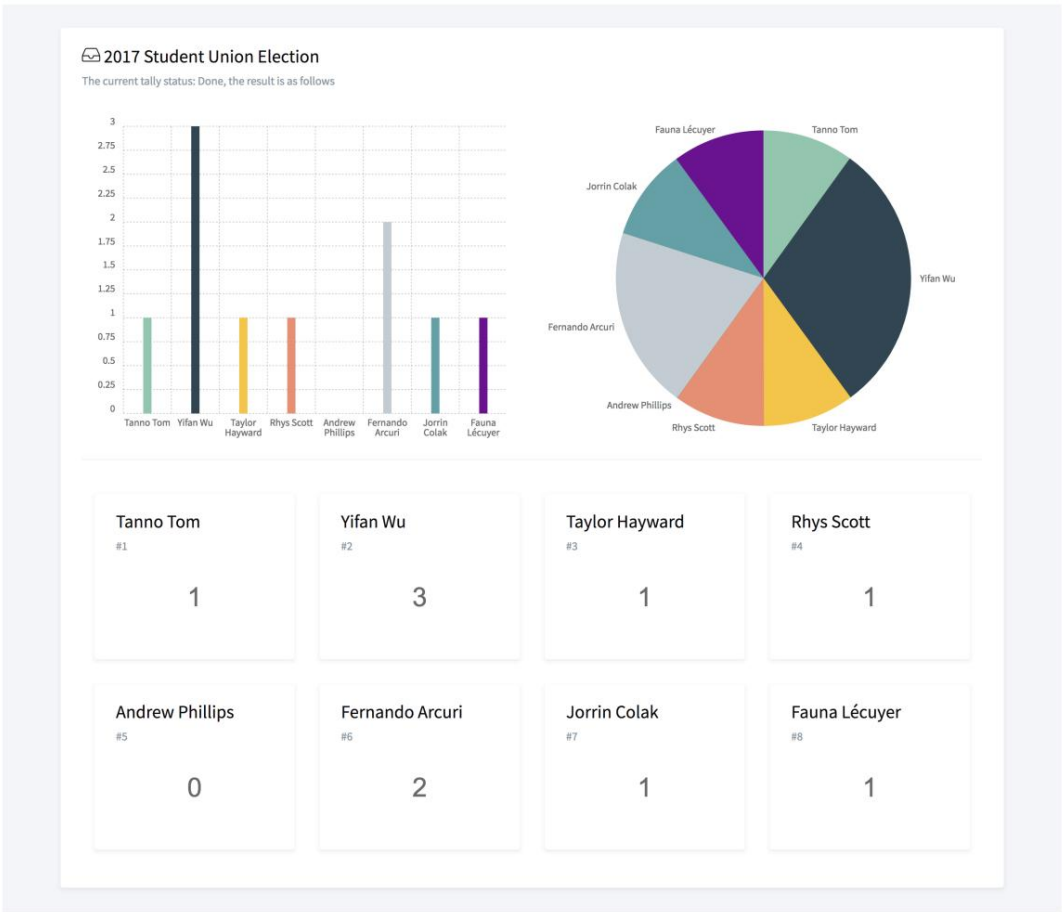
4. Xác minh tính hợp lệ của từng chữ ký nhẫn.
5. Đếm lá phiếu hợp lệ.



Hình 4.12: Giao diện quản lý ứng viên RA



Hình 4.13: Giao diện quản lý ứng viên RA



Hình 4.14: Giao diện quản lý ứng viên RA

Chương 5

Sự đánh giá

5.1 Thuộc tính mong đợi

Theo các thuộc tính được mô tả ở trên, các thuộc tính của sơ đồ biểu quyết là đủ. Đối với giao thức và cách triển khai này, các thuộc tính có thể được liệt kê như bên dưới.

Quyền riêng tư của lá phiếu: Bất kỳ ai cũng không thể biết được cử tri đã bỏ phiếu cho ai.

Địa chỉ tài khoản blockchain là ngẫu nhiên và không có người quan sát bên ngoài hoặc thậm chí hệ thống không thể biết mối quan hệ giữa những người bỏ phiếu và địa chỉ Bitcoin. Đối với chữ ký nhẵn, nó có thuộc tính ẩn danh.

Không ai có thể phỏng đoán danh tính thực sự của người bỏ phiếu từ chữ ký chiếc nhẵn.

Khả năng xác minh cá nhân: Người bỏ phiếu có thể xác minh lá phiếu của mình được đếm chính xác sau khi đã bỏ phiếu. Người bỏ phiếu có thể sử dụng (σ , sha256 (σ)) để xác minh sha256 (σ) được xuất bản lên blockchain một cách chính xác, trong đó σ là chữ ký. Người bỏ phiếu có thể sử dụng chữ ký nhẵn của mình σ để xác minh rằng mình bỏ phiếu cho ứng cử viên phù hợp.

Tính đủ điều kiện: Chỉ người bỏ phiếu hợp pháp mới có thể đăng ký sự kiện bỏ phiếu.

Trong hệ thống này, người bỏ phiếu nên đăng ký RA và lấy liên kết mã nếu họ được xác minh là hợp pháp để bỏ phiếu. Khi bắt đầu bỏ phiếu, chỉ người bỏ phiếu có liên kết mã mới có thể đăng ký bỏ phiếu biến cố.

Tính đầy đủ: Mọi phiếu bầu phải được đếm chính xác.

Tất cả các phiếu bầu có thể được đếm một cách chính xác. Bằng cách sử dụng chữ ký vòng, hệ thống sẽ cung cấp tất cả các khóa công khai. Tài khoản blockchain EA sẽ nhận được một lượng bitcoin khi cuộc bỏ phiếu kết thúc. Hệ thống kiểm đếm có thể dễ dàng đếm KHOẢN TRẢ LẠI của mỗi giao dịch.

Bất kỳ ai không bỏ phiếu nhưng lưu PKI khóa công khai của mình vào hệ thống sẽ được coi là sự bỏ phiếu trắng.

Tính duy nhất: Mỗi người bình chọn chỉ được bình chọn một lần. Người bỏ phiếu sẽ không được phép bỏ phiếu thêm nếu anh ta bỏ phiếu.

Giao thức có một phương pháp để bỏ qua các phiếu bầu bổ sung từ cùng một cử tri. Trong giai đoạn kiểm đếm, nếu lịch sử giao dịch Bitcoin có nhiều hơn hai lần giao dịch từ cùng một Ai đầu tiên và bỏ qua những người khác.đếm

Tính chắc chắn: Bất kỳ ai cũng không thể ảnh hưởng hoặc sửa đổi kết quả biểu quyết cuối cùng khi kiểm đếm. Kết quả đã được truyền đến blockchain nếu người bỏ phiếu bỏ phiếu. Blockchain thật khó

để rèn và sửa đổi.

Sự cưỡng chế-phản kháng: Không có người ép buộc nào có thể hợp tác với cử tri. Người bỏ phiếu không thể chứng minh mình đã bỏ phiếu cho ai.

Giao thức có thể đảm bảo tính chất này chỉ xảy ra khi số lượng cử tri n đủ lớn. Nếu ai đó đe dọa một cử tri bỏ phiếu cho anh ta, người đó có thể cho anh ta biết id giao dịch và chữ ký vòng bỏ phiếu cho mối đe dọa từ API công khai. Đối với sự uy hiếp, ông không thể xác nhận chữ ký mà cử tri đưa cho ông là của cử tri.

Hệ thống kiểm đếm tìm nạp tất cả các giao dịch của địa chỉ tài khoản blockchain của EA. Khi kiểm đếm phiếu bầu, hệ thống sẽ xác minh tính hợp lệ của chữ ký vòng và chỉ kiểm phiếu bầu đầu tiên và hợp pháp.

Không phải tất cả các thuộc tính đều hài lòng với giao thức và cách triển khai này. Dưới đây là các thuộc tính không thỏa mãn với việc triển khai.

Công bằng: Không điều gì có thể ảnh hưởng đến kết quả của cuộc bỏ phiếu.

Hệ thống kiểm đếm theo thời gian thực. Hệ thống không thể đảm bảo tài sản này.

Không có biên nhận: Người bỏ phiếu không thể nhận hoặc cố gắng xây dựng bất kỳ biên nhận nào sau khi đã bỏ phiếu để chứng minh cách họ bỏ phiếu.

Khi người bỏ phiếu bắt đầu bỏ phiếu, anh ta sẽ nhận được chữ ký nhấn σ , sha256 (σ) và id giao dịch của mình trên blockchain. Đây là biên lai để cử tri kiểm chứng lá phiếu của mình.

5.2 Hiệu suất

Để đảm bảo kết quả kiểm tra có tính thuyết phục, chúng tôi đã thực hiện đầy đủ các bài kiểm tra trên Testnet (Môi trường thử nghiệm Bitcoin) để đánh giá thuật toán và phần mềm.

5.2.1 Hiệu suất chữ ký vòng

Đối với giao thức được đề xuất, nếu số lượng thành viên cử tri n đủ nhỏ, hãy bỏ chuỗi chữ ký sẽ được hiệu quả ký và xác minh. Ngược lại, kích thước khóa công khai, vòng kích thước chữ ký và hiệu quả của việc ký và xác minh sẽ tăng dần.

Bài kiểm tra đơn vị chạy trên trình duyệt web Chrome 62 của máy tính xách tay có Intel Core i5 2,9 GHz. Các kết quả đã được minh họa trên Bảng 5.1. Chúng tôi nhận thấy rằng các lỗi của thử nghiệm đơn vị phụ thuộc vào hiệu suất của nhiều CPU khác nhau.

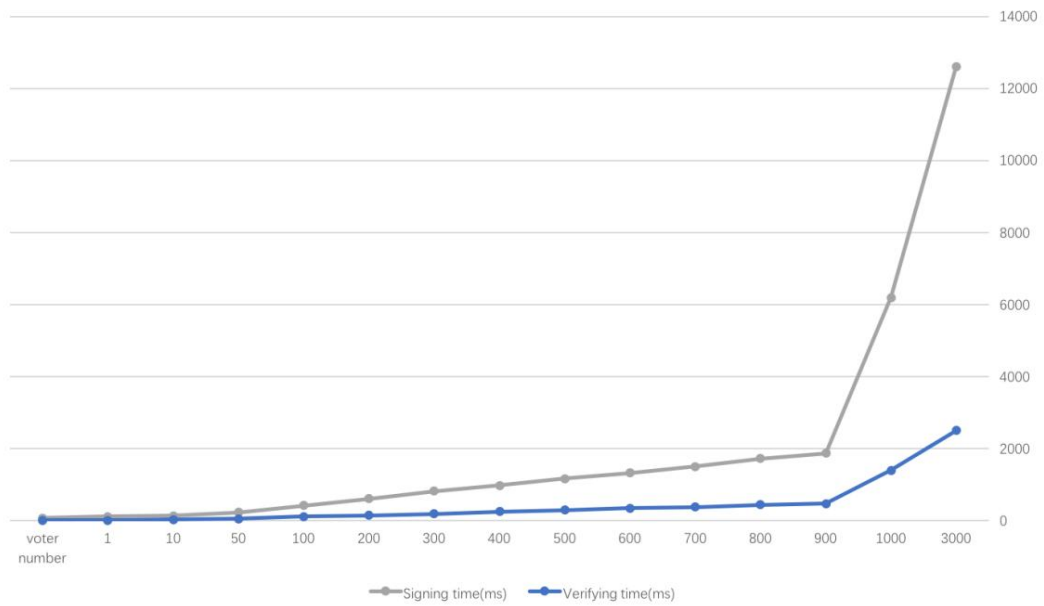
Số khóa công khai	Thời gian ký (mili giây)	Thời gian xác minh (mili giây)	Kích thước chữ ký (byte)
1	2.386962891	10.9831543	69.88598633
10		109.7609863	
50		135.7580566	28.3449707
100		232.9682617	54.00390625
200		414.2949219	107.8620605
300		607.6271973	145.9350586
400		813.138916	190.0830078
500		976.5891113	248.5419922
600		1160.855957	292.5158691
700		1325.011963	344.0258789
800		1500.853027	375.4931641
900		1721.103271	437.5969238
1000		1866.314209	474.9248047
3000		6189.906006	1392.203125
5000		12598.85913	2501.8479
			1539489

Bảng 5.1: Hiệu suất của chữ ký vòng

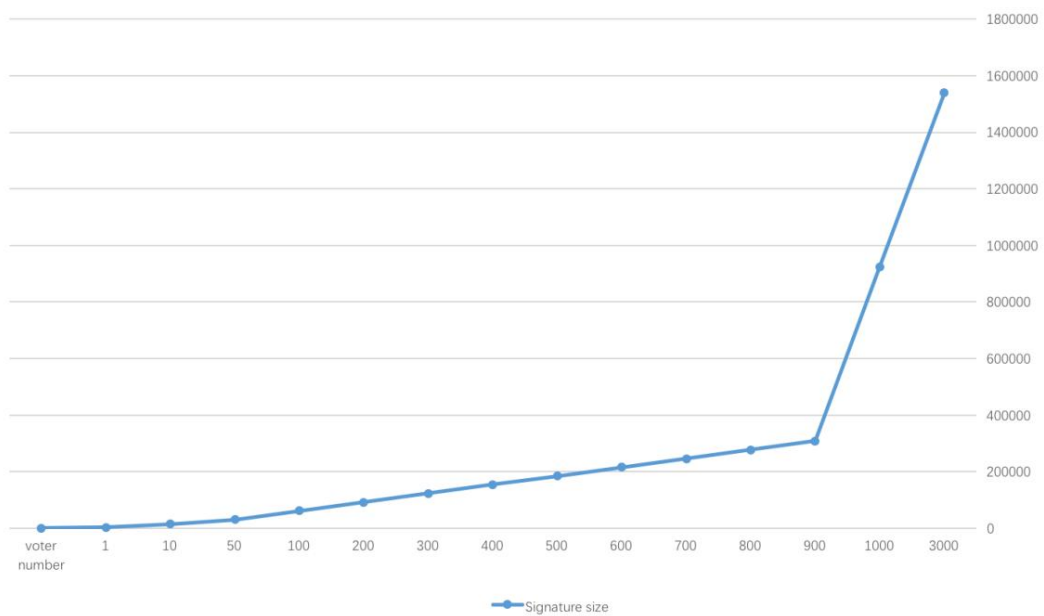
Theo Hình 5.1 và Hình 5.2, có một mối quan hệ tuyến tính giữa công số phím (số người bầu chọn) và các thông số khác như thời gian hát hoặc xác minh, kích thước chữ ký. Càng nhiều cử tri đăng ký tham gia, thì hiệu quả càng kém.

Chúng tôi khuyến nghị rằng số lượng cử tri nên ít hơn 3000 để mọi cử tri sẽ không chờ hơn 1 phút để lấy chữ ký nhấn. Và kích thước của tệp chữ ký sẽ nhỏ hơn hơn 93KB trong trường hợp đó.

Giao thức được đề xuất không phù hợp với hoạt động bầu cử lớn nếu cử tri muốn có được trải nghiệm người dùng tốt hơn nhiều.



Hình 5.1: Mối quan hệ giữa số lượng cử tri và thời gian ký xác nhận



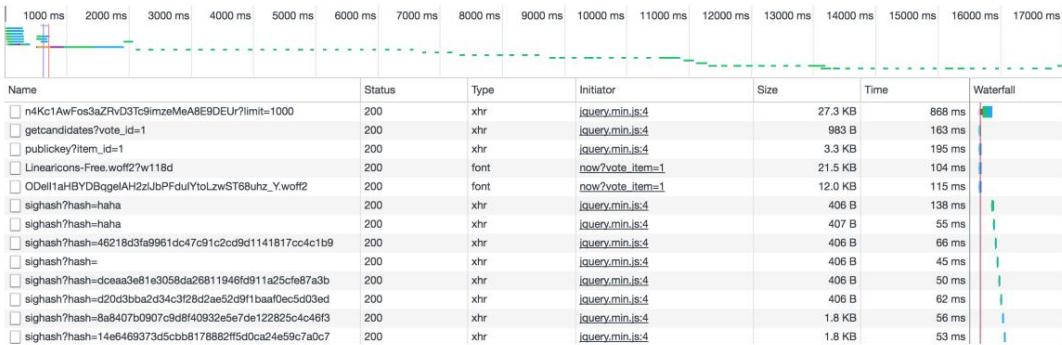
Hình 5.2: Mối quan hệ giữa số lượng cử tri và kích thước khóa chữ ký

5.2.2 Hiệu suất kiểm đếm

Giai đoạn kiểm phiếu là phần quan trọng nhất của cuộc bỏ phiếu. Hiệu suất của giai đoạn này có thể được đánh giá.

Khi thực hiện đánh giá, có 3 yếu tố ảnh hưởng đến toàn bộ hiệu quả của khâu kiểm đếm theo Hình 5.3.

- Blockchain API: Có trách nhiệm tìm nạp tất cả các giao dịch của EA theo giao thức được đề xuất. Nó phụ thuộc vào mạng lưới cử tri và số lượng giao dịch viên. Thời gian đáp ứng được thử nghiệm là 868ms trong môi trường thử nghiệm (Hình 5.3).
- API công khai của việc nhận ứng viên: Để nhận được tất cả các ứng viên, trình duyệt phải gửi một yêu cầu đến máy chủ. Thời gian có thể được ước tính là 163 ms trong môi trường thử nghiệm (Hình 5.3).
- API công khai của việc nhận tất cả các khóa công khai: Để nhận tất cả các khóa công khai và xác minh chữ ký vòng, trình duyệt phải gửi một yêu cầu đến máy chủ. Thời gian có thể được ước tính là 195ms trong môi trường thử nghiệm (Hình 5.3).
- API công khai của việc đối sánh chữ ký vòng thông qua giá trị băm: Khi khách hàng nhận được tất cả các giao dịch, nó sẽ gửi một yêu cầu đến máy chủ. Thời gian trung bình có thể được ước tính là 55ms trong môi trường thử nghiệm (Hình 5.3).
- Thời gian xác minh: Thời gian xác minh chữ ký chiếc nhẫn có thể được đánh giá là Phần 5.2.1 đã thảo luận.



Hình 5.3: Bảng điều khiển dành cho nhà phát triển Chrome của trang kiểm đếm

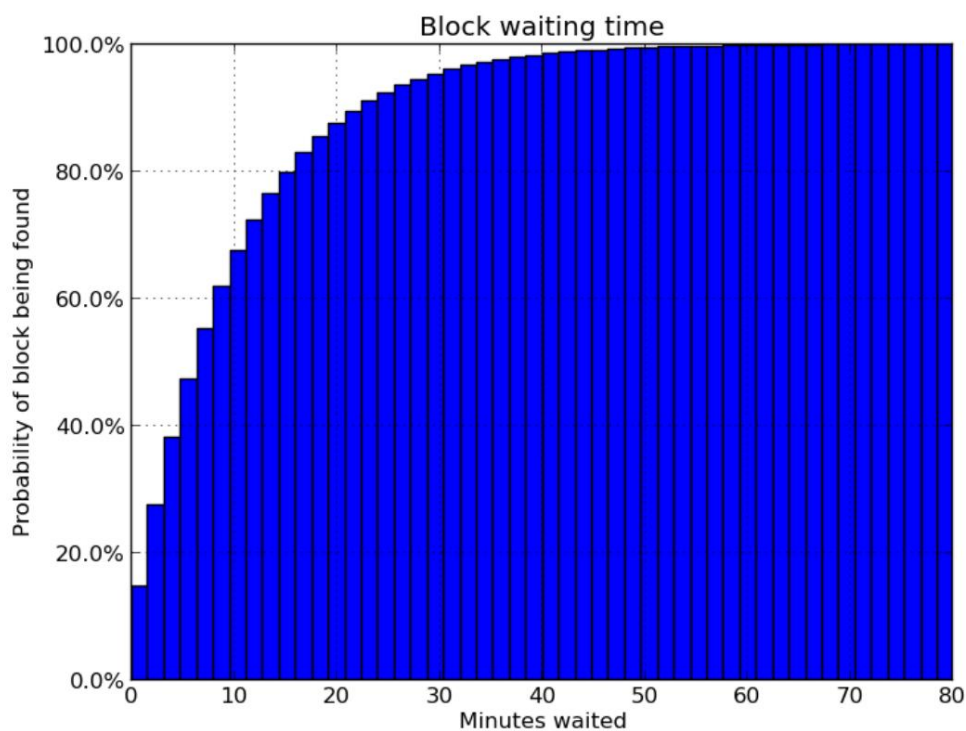
Nhìn chung, nếu giao dịch của EA đủ lớn, toàn bộ quá trình sẽ tăng đáng kể. Để tránh điều này, EA nên thay thế địa chỉ blockchain của mình thường xuyên sau khi mục bỏ phiếu bị dừng.

5.2.3 Thời gian xác nhận

Thời gian xác nhận là biểu tượng của việc phát đi kết quả bình chọn trên toàn thế giới trong việc thực hiện này. Theo giao thức của Bitcoin, Khi một giao dịch với

MỞ QUAY LẠI bao gồm id ứng cử viên và giá trị băm của chữ ký vòng được phát tới mạng blockchain, các thợ đào phải tìm thấy nó và xác nhận nó.

Các thợ đào nên sử dụng thuật toán đồng thuận để xác nhận giao dịch. Chúng tôi ước tính khoảng thời gian đó là 10 phút và kết quả thỏa mãn quy trình poisson [3].



Hình 5.4: Thời gian chờ khối [3]

Như hình 5.4 cho thấy, trong 10 phút đầu, có khoảng 60 phần trăm khối có thể được xác nhận. Thời gian này cũng bị ảnh hưởng bởi phí khai thác. Đối với EA, cần cân bằng giữa phí khai thác và thời gian xác nhận. Nói chung, đối với Bitcoin, mối quan hệ giữa phí khai thác và thời gian xác nhận có thể dễ dàng tìm nạp từ API dự đoán phí Bitcoin [4].

Trong các thử nghiệm hiện tại, ngay cả khi giao dịch chưa được xác nhận, kết quả cũng có thể được tính. Nếu giao dịch được xác nhận, kết quả bỏ phiếu có thể đáng tin cậy hơn.

Chương 6

Kết luận

6.1 Tóm tắt

Bài báo này chủ yếu khám phá khái niệm cơ bản về bỏ phiếu điện tử và blockchain bằng cách chỉ định thuật toán địa chỉ Bitcoin và khái niệm OP RETURN.

Một giao thức dựa trên blockchain với bảy giai đoạn đã được đề xuất sau này. Định nghĩa và quá trình của từng giai đoạn cũng đã được giải thích chi tiết.

Toàn bộ quá trình phát triển giao thức cũng đã được mô tả từ quan điểm phát triển phần mềm chuyển tiếp, chẳng hạn như cách giao dịch blockchain xảy ra và một số phân tích cơ chế của hệ thống bỏ phiếu.

Cuối cùng, bài báo đánh giá hiệu suất và rủi ro bảo mật tiềm ẩn đối với giao thức, những hạn chế hơn nữa đã được thảo luận ở phần cuối.

6.2 Kết luận

Mặc dù giao thức được tạo thỏa mãn với các thuộc tính của quyền riêng tư lá phiếu, khả năng xác minh riêng lẻ, tính đủ điều kiện, tính hoàn chỉnh, tính duy nhất, tính mạnh mẽ và khả năng chống cưỡng chế.

Tuy nhiên, nó không đáp ứng nhu cầu của sự công bằng và không có biên lai.

Trong đánh giá hiệu suất, giao thức hoạt động hiệu quả đối với chữ ký vòng, đặc biệt khi số lượng người bỏ phiếu ít hơn 3000. Do đó, hiệu quả của thuật toán chữ ký vòng bị giới hạn bởi số lượng người tham gia.

Ưu điểm chính của giao thức này là đảm bảo tính xác thực của biểu quyết điện tử. Vì mọi lá phiếu sẽ được phát tới blockchain khi cuộc bỏ phiếu bắt đầu. Hơn nữa, vì blockchain là một sổ cái công khai phi tập trung, kết quả phiếu bầu được trình bày trong thời gian thực và không thể được sửa đổi bởi một cá nhân, điều này đáp ứng thiết kế kiểm toán mở.

BlockVotes đã xác nhận tính khả thi của giao thức được đề xuất dưới dạng nguy trang. Mục đích của việc chọn testnet làm mạng blockchain, chủ yếu nằm ở việc nó miễn phí và dễ dàng không đòi hỏi phải có Bitcoin. Ngoài ra, là một lý do chính khác để testnet được chỉ định phát sóng kết quả bỏ phiếu.

6.3 Công việc trong tương lai

Giao thức bỏ phiếu điện tử dựa trên chuỗi khối vẫn còn nhiều khả năng để cải thiện, chẳng hạn như cải thiện tính minh bạch của nó, hoàn thành các chức năng chưa được tích hợp trong trạng thái hiện tại và giảm API công khai.

Đối với BlockVotes, các chức năng như chuyển đổi nhiều mạng hơn giữa BitCoin, testnet và LiteCoin có thể được thêm vào. Ngoài ra, nhiều phiếu bầu thành tích trong một phiếu bầu có thể là một chủ đề lý tưởng để nghiên cứu thêm.

Thư mục

- [1] Baudron, O., Fouque, P.-A., Pointcheval, D., Stern, J., và Poupard, G.
Hệ thống bầu cử đa ứng cử viên thực tế. Trong Kỷ yếu của hội nghị chuyên đề ACM hàng năm lần thứ 20 về Các nguyên tắc của máy tính phân tán (2001), ACM, trang 274-283.
- [2] Benaloh, J., và Tuinstra, D. Các cuộc bầu cử bỏ phiếu kín không có biên nhận. Trong Kỷ yếu hội nghị chuyên đề ACM hàng năm lần thứ hai mươi sáu về Lý thuyết máy tính (1994), ACM, trang 544-553.
- [3] Bitcoin-Wiki. Xác nhận - bitcoin wiki. [https://en.bitcoin.it/wiki/Xác nhận](https://en.bitcoin.it/wiki/Xác_nhận).
- [4] bitcoinfees.21.co. Dự đoán phí bitcoin cho các giao dịch. [https:// bitcoinfees.21.co/](https://bitcoinfees.21.co/).
- [5] Card, D., và Moretti, E. Công nghệ bỏ phiếu có ảnh hưởng đến kết quả bầu cử không? màn hình cảm ứng bỏ phiếu và cuộc bầu cử tổng thống năm 2004. Tạp chí Kinh tế và Thống kê 89, 4 (2007), 660-673.
- [6] Cetinkaya, O., và Cetinkaya, D. Hướng tới bầu cử điện tử an toàn ở gà tây: yêu cầu các yếu tố và nguyên tắc. Về Tính sẵn sàng, Độ tin cậy và Bảo mật, 2007. ARES 2007. Hội nghị Quốc tế lần thứ hai về (2007), IEEE, trang 903-907.
- [7] Chaum, DL Thư điện tử không thể truy cập, địa chỉ trả lại và bút danh kỹ thuật số. Thông tin liên lạc của ACM 24, 2 (1981), 84-90.
- [8] Christian Schaupp, L., và Carter, L. Bỏ phiếu điện tử: từ thờ ơ đến nhận con nuôi. Journal of Enterprise Information Management 18, 5 (2005), 586-601.
- [9] Cohen, JD và Fischer, MJ Một kế hoạch bầu cử an toàn bằng mật mã mạnh mẽ và có thể xác minh được. Đại học Yale. Khoa Khoa học Máy tính, 1985.
- [10] Cranor, LF và Cytron, RK Sensus: Một hệ thống bỏ phiếu điện tử có ý thức bảo mật cho Internet. Trong Khoa học Hệ thống, 1997, Kỷ yếu Hội nghị Quốc tế Hawaii lần thứ ba về (1997), tập. 3, IEEE, trang 561-570.

- [11] Czepluch, JS, Lollike, NZ và Malone, SO Việc sử dụng công nghệ chuỗi khối nology trong các lĩnh vực ứng dụng khác nhau. Đại học CNTT Copenhagen, Copenhagen (2015).
- [12] Các giao thức DeMillo, RA, Lynch, NA và Merritt, MJ Cryptographic. Trong Kỷ yếu của hội nghị chuyên đề ACM hàng năm lần thứ mười bốn về Lý thuyết máy tính (1982), ACM, trang 383-400.
- [13] Fraunholz, B., và Unnithan, C. Quản trị điện tử: kích hoạt cuộc cách mạng web 2.0 của Pháp? Trong Nền tảng của chính phủ điện tử (2007), [Hội nghị quốc tế về quản trị điện tử] Nhà xuất bản hàn lâm, trang 344-359.
- [14] Fujioka, A., Okamoto, T., và Ohta, K. Một kế hoạch bỏ phiếu kín thực tế cho các cuộc bầu cử quy mô lớn. Trong Hội thảo Quốc tế về Lý thuyết và Ứng dụng của Kỹ thuật Mật mã (1992), Springer, trang 244-251.
- [15] Hirt, M. và Sako, K. Bỏ phiếu hiệu quả không cần biên nhận dựa trên tion mã hóa đồng hình. Trong Những tiến bộ trong mật mã học EUROCRYPT 2000 (2000), Springer, trang 539-556.
- [16] Jason, PC và Yuichi, K. Hệ thống bỏ phiếu điện tử dựa trên giao thức bitcoin và chữ ký mù quảng. TOM 10, 1 (2017), 14-22.
- [17] Jonker, H., Mauw, S., và Pang, J. Quyền riêng tư và khả năng xác minh trong hệ thống bỏ phiếu: Phương pháp, sự phát triển và xu hướng. Tạp chí Khoa học Máy tính 10 (2013), 1-30.
- [18] Juels, A., Catalano, D., và Jakobsson, M. Elec điện tử kháng cưỡng bức hàng tấn. Hướng tới Cuộc bầu cử đáng tin cậy 6000 (2010), 37-63.
- [19] kiwi. Hộp cát testnet bitcoin. <https://testnet.manu.backend.hamburg/faucet>.
- [20] Lee, K., James, JI, Ejeta, TG và Kim, H. Dịch vụ bỏ phiếu điện tử sử dụng chuỗi khối. Tạp chí Pháp y Kỹ thuật số, An ninh và Luật: JDFS 11, 2 (2016), 123.
- [21] Luo, F. Thiết kế và phân tích sơ đồ bỏ phiếu điện tử chống cưỡng chế. Thạc sĩ luận án, Đại học Sư phạm Phúc Kiến, 2015.
- [22] Macintosh, A. Đặc trưng cho sự tham gia của điện tử vào quá trình hoạch định chính sách. Trong Khoa học Hệ thống, 2004. Kỷ yếu Hội nghị Quốc tế Hawaii Thường niên lần thứ 37 về (2004), IEEE, trang 10 - pp.
- [23] Nakamoto, S. Bitcoin: Hệ thống tiền điện tử ngang hàng, 2008.
- [24] Niemi, V. và Renvall, A. Làm thế nào để ngăn chặn việc mua phiếu bầu trong các cuộc bầu cử trên máy tính. Trong Hội nghị Quốc tế về Lý thuyết và Ứng dụng của Mật mã (1994), Springer, trang 164-170.

- [25] Ohkubo, M., Miura, F., Abe, M., Fujioka, A., và Okamoto, T. Bảo mật thông tin (1999), 771-771.
- [26] Okamoto, T. Một sơ đồ bỏ phiếu điện tử. Trong Công cụ CNTT nâng cao. Springer, 1996, trang 21-30.
- [27] Peters, GW và Panayi, E. Tìm hiểu sổ cái ngân hàng hiện đại thông qua công nghệ blockchain: Tương lai của xử lý giao dịch và hợp đồng thông minh trên internet tiền tệ. Trong Ngân hàng Ngoài Ngân hàng và Tiền. Springer, 2016, trang 239-278.
- [28] Rivest, R., Shamir, A., và Tauman, Y. Làm thế nào để rò rỉ một bí mật. Tiến bộ trong Mật mã họcASIACRYPT 2001 (2001), 552-565.
- [29] Rivest, RL, Shamir, A., và Adleman, L. Một phương pháp lấy chữ ký số và hệ thống mật mã khóa công khai. Thông tin liên lạc của ACM 21, 2 (1978), 120-126.
- [30] Sako, K. và Kilian, J. Sơ đồ bỏ phiếu kiểu hỗn hợp không có biên nhận. Đang ứng trước trong CryptologyEUROCRYPT95 (1995), Springer, trang 393-403.
- [31] Mỏng. Phần mềm trung gian - mỏng. <https://www.slimframework.com/docs/concept/middleware.html>.
- [32] Spycher, O., Koenig, R., Haenni, R., và Schlapfer, M. Một cách tiếp cận mới hướng tới bỏ phiếu điện tử từ xa chống cưỡng chế trong thời gian tuyến tính. Trong Hội nghị Quốc tế về Mật mã Tài chính và Bảo mật Dữ liệu (2011), Springer, trang 182-189.
- [33] Takabatake, Y., Kotani, D., và Okabe, Y. Một điện tử phân phối ẩn danh hệ thống bỏ phiếu sử dụng zerocoin.
- [34] Zhao, Z. và Chan, T.-HH Cách bỏ phiếu riêng tư bằng bitcoin. Trong Hội nghị Quốc tế về An ninh Thông tin và Truyền thông (2015), Springer, trang 82-96.

Phụ lục

Phụ lục A

Hướng dẫn

Dự án đã được tải lên kho git-giảng dạy git. Để tải xuống dự án, vui lòng chạy lệnh sau.

```
git clone https://git-teaching.cs.bham.ac.uk/mod-msc-proj-2016/yxw689.git
```

Để xây dựng và chạy dự án, môi trường chạy được yêu cầu như sau.

- Mac OS X hoặc Linux hoặc Windows
- Apache 2.4.27 hoặc Nginx 1.12.1
- MySQL 5.7.19 (ít nhất là 5.4)
- PHP 7.1.8 (ít nhất 7.0)
- php7.0-gmp
- nhà soạn nhạc

Để chạy hệ thống, một số thông tin quan trọng nhưng riêng tư không được tải lên bởi gitingore tập tin. Vui lòng thêm tệp .env vào thư mục gốc của thư mục dự án này.

```
1 DB_DRIVER = mysql 2
DB_HOST = 127.0.0.1
3 DB_DATABASE = blockvotes
4 DB_USERNAME = gốc
5 DB_PASSWORD =
6 DB_PORT = 3306
7
8 STMP_SERVER = smtp.gmail.com 9 STMP_PORT
= 465
10 STMP_USERNAME = xxx@gmail.com 11
STMP_PASSWORD = mật khẩu
```

Tệp SQL mẫu được tạo và tải lên dưới dạng tệp blockvotes.sql, vui lòng chuyển tệp đó sang MySQL. Cuối cùng, hãy đặt thư mục mặc định thành / public trong tệp cấu hình Nginx hoặc Apache.