UEH UNIVERSITY

UEH Digital Repository

Book Chapter

2021

Xây dựng thị trường chứng khoán phi tập trung dựa trên công nghệ Blockchain

TS. Nguyễn Hữu Huân TS. Ngô Minh Vũ ThS. Trần Nguyễn Trâm Anh

UEH University

Citation:

TS. Nguyễn Hữu H., TS. Ngô Minh V. and ThS. Trần Nguyễn Trâm A. (2021), "Xây dựng thị trường chứng khoán phi tập trung dựa trên công nghệ Blockchain", Thông tin và Truyền thông

Available at https://digital.lib.ueh.edu.vn/handle/UEH/62541

This item is protected by copyright and made available here for research and educational purposes. The author(s) retains copyright ownership of this item. Permission to reuse, publish, or reproduce the object beyond the bounds of Vietnam Intellectual Property Law (2005, 2009 and 2022) or other exemptions to the law must be obtained from the author(s).

XÂY DỰNG THỊ TRƯỜNG CHỨNG KHOÁN PHI TẬP TRUNG DỰA TRÊN CÔNG NGHỆ BLOCKCHAIN

TS. Nguyễn Hữu Huân

Trường ĐH Kinh Tế Tp HCM;

TS. Ngô Minh Vũ

Trường ĐH Kinh Tế Tp HCM;

ThS. Trần Nguyễn Trâm Anh

Trường ĐH Văn Lang

TÓM TẮT

Nghiên cứu này đề xuất một giải pháp về việc ứng dụng công nghệ Blockchain trong việc xây dựng một thị trường chứng khoán phi tập trung tại Việt Nam. Trong đó chỉ ra rằng việc xây dựng thị trường chứng khoán theo cơ chế phi tập trung sẽ giúp loại bỏ các trung gian không cần thiết từ đó làm giảm thiểu chi phí giao dịch, thời gian giao dịch, thời gian chứng khoán và tiền về tài khoản. Bên cạnh đó, với cơ chế bảo mật của công nghệ Blockchain sẽ giúp cho thị trường rất khó bị tấn công mang lại sự an toàn và tính bền vững cao cho toàn hệ thống. Nghiên cứu đồng thời cũng đề xuất một số giải pháp cho các bên liên quan như chính phủ, ủy ban chứng khoán nhà nước, công ty chứng khoán để có thể xây dựng được thành công thị trường chứng khoán theo cơ chế phi tập trung bằng công nghệ Blockchain.

Từ khóa: *Blockchain, cơ chế phi tập trung, thị trường chứng khoán.*

1. GIỚI THIỆU CHUNG

Theo kế hoạch của chính phủ đến năm 2040, nền kinh tế số sẽ chiếm 40% GDP của Việt Nam, và hiện nay chính phủ và toàn dân đang tập trung trong quá trình chuyển đổi số nền kinh tế để đạt được mục tiêu trên trong tương lai. Trong kỷ nguyên cuộc cách mạng công nghiệp 4.0, các công nghệ được xem là sẽ thay thế dần các ngành truyền thống bao gồm dữ liệu lớn Big data, Internet kết nối vạn vật Internet of thing, trí tuệ nhân tạo machine learning và đặc biệt là công nghệ chuỗi khối Blockchain. Và quá

trình chuyển đổi số của Việt Nam không thể nằm ngoài việc ứng dụng các công nghệ trên.

Hiện nay, chính phủ Việt Nam đã đồng ý cho Bộ giáo dục đào tạo triển khai công nghệ Blockchain trong việc lưu trữ và tra cứu văn bằng. Mới đây nhất, chính phủ cũng đã giao cho Ngân hàng nhà nước nghiên cứu và triển khai tiền điện tử của Việt Nam dựa trên công nghệ Blockchain. Với những thông tin trên, đã đánh dấu việc chính phủ đã nhận thấy được tầm quan trọng trong việc chuyển đổi số các bộ máy quản lý và các cơ quan quản lý, đồng thời cũng nhìn nhận vai trò của công nghệ Blockchain như một nền tảng ứng dụng thiết thực vào trong bộ máy quản lý, điều hành đất nước và các ứng dụng trong đời sống, theo xu hướng phát triển của các nước trong khu vực và thế giới.

Công nghệ Blockchain hiện đã và đang được ứng dụng khá rộng rãi vào mọi ngành nghề, ngóc ngách trong nền kinh tế, từ tài chính, tiền tệ đến việc lưu trữ văn bằng, y tế, giáo dục và thay đổi cả mạng Internet trong tương lai. Trong bài nghiên cứu của mình, Monrat và cộng sự (2019) có đề cập đến việc công nghệ này có thể được triển khai để tìm kiếm các giải pháp cho các lĩnh vực khác nhau, chẳng hạn như chăm sóc sức khỏe, bỏ phiếu, quản lý danh tính, công tác quản trị, chuỗi cung ứng, năng lượng, truy xuất nguồn gốc của thuốc và quản lý dữ liệu bệnh nhân… Foroglou và Tsilidou (2015) cung cấp một số ứng dụng có thể có khác của Blockchain ngoài Bitcoin như hợp đồng thông minh (trong mua bán hàng hóa, chuyển nhượng bất động sản, di chúc, thậm chí là hợp đồng cá cược), bỏ phiếu bầu cử, quyền sở hữu trí tuệ, tài sản thông minh, quản lý vận chuyển, quyền sở hữu bất động sản… Một số ứng dụng tiêu biểu của Blockchain gồm: cơ sở hạ tầng cơ bản, tiền tệ, dịch vụ tài chính, dịch vụ cung cấp bằng chứng, tài sản và quyền sở hữu tài sản, quản lý danh tính, quản trị (Elsden và cộng sự, 2018). Tất cả các lĩnh vực có thể ứng dụng công nghệ Blockchain được (Jaoude và Saade, 2017) tổng hợp lại từ các bài nghiên cứu đã xuất bản gồm: IOT, năng lượng, y tế, tài chính, quản trị nguồn nhân lực, quản trị, trao đổi, vận chuyển, BPM, quản trị bản quyền, tư nhân, chuỗi cung ứng, thành phố thông minh, bảo hiểm, giáo dục, chuyển dữ liệu, mạng xã hội, phát hiện gian lận, môi trường, nghiên cứu, ra quyết định, trách nhiệm giải trình dữ liệu, quản lý truy cập. Trong lĩnh vực y tế, (Mettler, 2016) đề xuất một số ứng dụng sử dụng công nghệ Blockchain gồm có: (1) Quản lý sức khỏe thông minh vì mục tiêu hướng đến lợi ích cao nhất cho bệnh nhân, mô hình này đã được triển khai trên thực tế bằng việc hợp tác giữa Estonia và

Guardtime (Guardtime: công ty vận hành nền tảng chăm sóc sức khỏe dựa trên công nghệ Blockchain) năm 2011 xây dựng một nền tảng chăm sóc sức khỏe dựa trên công nghệ Blockchain nhờ đó, công dân Estonia, nhà cung cấp dịch vụ chăm sóc sức khỏe hoặc công ty bảo hiểm y tế có thể truy xuất tất cả thông tin về các phương pháp điều trị y tế được thực hiện ở Estonia bằng cách sử dụng Blockchain (2) Trao quyền cho người dùng cuối và cho bệnh nhân, 1 ví dụ tác giả đưa ra là công ty Healthbank, một công ty khởi nghiệp về sức khỏe kỹ thuật số toàn cầu của Thụy Sĩ, cung cấp cho người dùng một nền tảng để họ có thể lưu trữ và quản lý thông tin sức khỏe của cá nhân trong một môi trường an toàn. Chủ quyền dữ liệu hoàn toàn nằm trong tay người dùng. Bước tiếp theo, Healthbank sẽ áp dụng và triển khai nhất quán công nghệ Blockchain cho mô hình kinh doanh của mình. Bằng việc sử dụng Blockchain, dữ liệu sức khỏe cá nhân do bệnh nhân tạo (ví dụ: nhịp tim, huyết áp, các loại thuốc đã uống, thói quen ngủ, thói quen ăn uống, v.v.) có thể được truy xuất từ các ứng dụng sức khỏe, thiết bị đeo hoặc thăm khám bác sĩ và được lưu trữ an toàn trong Blockchain của Healthbank. (3) Giám sát quá trình sản xuất thuốc, chống thuốc giả, bằng cách sử dụng Blockchain mỗi loại thuốc được sản xuất đều được đánh dấu thời gian. Từ đó có thể xác định được thuốc được sản xuất khi nào và ở đâu tại bất kỳ thời điểm nào để chống lại việc sản xuất thuốc giả. Sử dụng Blockchain, nguồn gốc của sản phẩm và các thành phần của nó được phát hiện và mọi chuyển nhượng quyền sở hữu trong mỗi trường hợp đều được thực hiện rõ ràng và khả dụng cho mọi người. Hàng giả, kém chất lượng hoặc hàng ăn cắp có thể được theo dõi và xác định. Trong lĩnh vực ứng dụng này, Blockchain góp phần đảm bảo rằng sự an toàn liên quan đến thuốc được tăng lên và giảm chi phí theo dõi liên quan đến sức khỏe. Trong lĩnh vực giáo dục, Grech và Camilleri (2017) đã đề xuất tám kịch bản sử dụng Blockchain trong ngành giáo dục: (1) Sử dụng Blockchain để bảo mật vĩnh viễn chứng chỉ (2) Sử dụng Blockchain để xác minh việc công nhận qua nhiều bước (3) Sử dụng Blockchain để nhận dạng tự động và chuyển các khoản tín dụng để trao học bổng (4).

Với các ưu điểm về tính bảo mật cao, khó bị tấn công bởi Hacker và tính không thể chỉnh sửa của công nghệ Blockchain và tính ứng dụng đa dạng của nó vào trong mọi ngành nghề trong nền kinh tế như đã trình bày ở trên, điều này sẽ rất phù hợp để chúng ta có thể xây dựng một sàn giao dịch chứng khoán trong tương lai theo công nghệ Blockchain này để thay thế các sàn giao dịch chứng khoán theo cơ chế tập trung hiện tại. Vì mọi giao dịch chứng khoán đều sẽ được ghi trên Blockchain và không thể bị sửa đổi thông

tin cũng như không thể tấn công vào một mạng Blockchain để lấy dữ liệu hay đánh sập thị trường, điều mà chúng ta vẫn đang lo ngại trước một cuộc tấn công quy mô lớn vào thị trường chứng khoán hiện tại vì đặc tính quản lý tập trung của nó. Tuy nhiên, việc xây dựng sàn chứng khoán dựa trên công nghệ Blockchain vẫn còn là một khái niêm khá mới mẻ trên thế giới và hiện nay chưa có quốc gia nào phát triển thị trường theo mô hình như trên. Chính vì thế, trong khuôn khổ bài viết này, nhóm nghiên cứu sẽ phân tích về công nghệ Blockchain, khả năng ứng dụng của nó cũng như đề xuất một mô hình sàn chứng khoán theo cơ chế quản lý phi tập trung dựa trên công nghệ Blockchain trong tương lai nhằm tăng tính bảo mật, tính an toàn và đặc biệt là giảm thiểu chi phí giao dịch chứng khoán cũng như loại bỏ các trung gian không cần thiết trên thị trường.

2. GIỚI THIỆU VỀ CÔNG NGHỆ BLOCKCHAIN VÀ CÁC NGHIÊN CỨU VỀ ỨNG DỤNG BLOCKCHAIN TRONG VIỆC XÂY DỰNG THỊ TRƯỜNG CHỨNG KHOÁN

Thị trường chứng khoán truyền thống với hệ thống tập trung có thể là mục tiêu tấn công của các hacker, do đó tính an toàn của mô hình thị trường chứng khoán hiện nay chưa cao. Bên cạnh đó, mô hình thị trường truyền thống này cũng là nơi tập trung quyền lực trong việc kiểm soát, đặt giá và áp đặt các phí liên quan. Hơn nữa, hệ thống vẫn còn phụ thuộc rất nhiều vào các bên trung gian gọi là các nhà môi giới, hưởng lợi từ phí giao dịch, đây là một loại phí không cần thiết và nên được loại bỏ trong mô hình mới. Một hạn chế nữa của mô hình thị trường chứng khoán hiện tại là thời gian xử lý giao dịch quá lâu, quá trình giải quyết mất nhiều thời gian vô hình chung đã phá hủy bản chất năng động của thị trường chứng khoán. Thời đại cách mạng công nghiệp 4.0 cùng với sự ra đời của Blockchain cho phép chúng ta nghĩ đến việc xây dựng một mô hình thị trường chứng khoán hoàn toàn mới với cơ chế hoàn toàn phi tập trung, sẽ là một giải pháp sáng tạo sẽ khắc phục được những tồn tại cố hữu trong mô hình thị trường chứng khoán truyền thống.

Với mục tiêu giải quyết những nhược điểm của hệ thống trao đổi chứng khoán tập trung truyền thống, chẳng hạn như phí giao dịch cao, quản trị tập trung dễ bị tấn công và thiếu độ mở đối với các hành động và thuật toán thị trường, bài nghiên cứu của (Pop, 2018) đề xuất một mô hình sáng tạo sử dụng Blockchain để phát triển một sàn giao dịch chứng khoán phi tập trung và một thị trường hoạt động liên tục 24/7. Mô hình này khắc phục được những hạn chế của sàn giao dịch chứng khoán tập trung bằng cách

đảm bảo tính toàn vẹn và bảo mật của tài sản và đơn đặt hàng của chủ sở hữu, việc thực hiện hợp đồng thông minh một cách tự động giữa các bên, thực hiện và giải quyết các lệnh thông qua các thuật toán đồng thuận để đạt được các quyết định dân chủ và đáng tin cậy. Mô hình dựa trên Blockchain này sẽ sử dụng các hợp đồng thông minh để xác nhận quyền của chủ sở hữu cũng như thực hiện và giải quyết chính xác các lệnh, do đó sự tồn tại của chủ thể trung gian là không còn cần thiết nữa. Giải pháp đã được xác thực bằng cách triển khai một nguyên mẫu trong Ethereum cho một tập hợp con các quy tắc cho Sở giao dịch chứng khoán Bucharest. Kết quả thực nghiệm cho thấy rằng giải pháp phi tập trung có thể làm giảm phí giao dịch bằng cách thay vì phải trả phí hoa hồng hay phí giao dịch cho nhà môi giới thì phần phí này sẽ được trả cho các thợ đào trong việc duy trì tính toàn vẹn của hệ thống.

Bài nghiên cứu của Miraz (2018) nghiên cứu về việc sử dụng Blockchain để bảo đảm các giao dịch trao đổi chứng khoán, đặc biệt tập trung vào các khía cạnh công nghệ cũng như pháp lý của các ứng dụng đó. Xem xét cấu trúc hoạt động phức tạp của sở giao dịch chứng khoán, nghiên cứu đề xuất thiết kế, phát triển và triển khai Blockchain hỗn hợp, tùy chỉnh theo nhu cầu của sở giao dịch chứng khoán tương ứng. Nghiên cứu cho thấy rằng việc sử dụng Blockchain như vậy có thể mang lại nhiều lợi ích mà các công nghệ khác hiện đang được sử dụng không thể mang lại. Tuy nhiên, bài nghiên cứu chưa xem xét các luật và các quy định liên quan đến hoạt động giao dịch chứng khoán trong quá trình thiết kế ứng dụng này.

Al-Shaibani (2020) cũng có bài nghiên cứu về việc xây dựng một thị trường chứng khoán hoàn toàn phi tập trung dựa trên công nghệ chuỗi khối. Trong mô hình này, các giao dịch trên sàn chứng khoán được thực hiện hoàn toàn trên một hợp đồng thông minh, các quy định thị trường của chính phủ cũng được đưa vào để xem xét, điểm này khắc phục được hạn chế trong bài nghiên cứu của Miraz (2018). Vì nền tảng mới không gây ra những thay đổi đáng kể nào đối với logic giao dịch của sàn chứng khoán và không loại bỏ bất kỳ bên truyền thống nào khỏi hệ thống, nên bài nghiên cứu thúc đẩy việc áp dụng và triển khai một cách hiệu quả các nền tảng trao đổi chứng khoán phi tập trung. Hơn nữa, tác giả cũng đưa ra được bằng chứng về việc triển khai hợp đồng thông minh, mạng thử nghiệm dựa trên công nghệ ảo để đanh giá hiệu quả của mô hình mới này. Mạng thử nghiệm bao gồm các nút ảo chạy hợp đồng thông minh của sàn giao dịch chứng khoán, thông qua mạng này, chúng tôi đo lường được thông lượng và độ trễ của lệnh mua-bán

trong các kích thước mạng khác nhau và các kịch bản khối lượng công việc giao dịch. Kết quả thu được đã chỉ ra rằng nền tảng giao dịch được đề xuất có thể đạt tới thông lượng 311,8 tx / giây, tương đương với 89% thông lượng tối ưu khi tốc độ gửi là 350 tx / giây. Thông lượng này phần lớn đủ để đáp ứng yêu cầu của các sàn giao dịch chứng khoán lớn, chẳng hạn như thị trường chứng khoán Singapore.

Trong bài báo của mình, (Bansal, 2019) thực hiện nghiên cứu trên một mẫu nhỏ gồm 11 công ty từ thị trường New Connect ở Ba Lan với mục tiêu giới thiệu một giải pháp dựa trên blockchain cho mô hình thị trường chứng khoán sử dụng các hợp đồng thông minh. Bài viết cũng đưa ra mô hình học máy để dự đoán về tương lai của thị trường chứng khoán cũng như cung cấp giải pháp thông minh cho thị trường chứng khoán an toàn. Kết quả cho thấy trong hầu hết các trường hợp, các công ty có thông báo về việc đang áp dụng công nghệ blockchain được mong đợi là có tốc độ tăng trưởng nhanh và cao. Ngoài ra, kết quả cũng đưa ra rằng trong hầu hết các trường hợp được phân tích, các thông báo về việc sử dụng công nghệ blockchain của các công ty này là không đầy đủ, đây có thể là chiến thuật có chủ ý của các pháp nhân này đối với các nhà đầu tư, cũng có thể do sự gia tăng nhanh chóng trong việc định giá công ty, một lý do khác có thể là sự thiếu năng lực và nguồn lực để triển khai công nghệ blockchain. Lời khuyên được đưa ra ở đây là các nhà đầu tư nên phân tích hoạt động kinh doanh của một công ty trước khi đầu tư. Tuy nhiên bài viết này chỉ được nghiên cứu trên một phạm vi khá nhỏ và cần thiết có thêm các nghiên cứu tương tự ở những thị trường lớn hơn như Châu Âu hoặc Hoa Kỳ

Lo và cộng sự (2017) đề xuất một khung đánh giá bao gồm danh sách các tiêu chí và quy trình nhằm giúp các nhà thực hành dựa trên các tiêu chí này có thể đánh giá được tính phù hợp của việc áp dụng blockchain vào mô hình của mình. Trong khi đó, Nowiński và Kozma (2017) đề xuất rằng có ba cách quan trọng mà công nghệ Blockchain có thể ảnh hưởng và phá vỡ các mô hình kinh doanh: bằng cách xác thực hàng hóa được giao dịch, thông qua trung gian và thông qua giảm chi phí giao dịch. Bài báo này chỉ ra các ứng dụng có thể có của công nghệ Blockchain đối với các doanh nghiệp và đặc biệt là tác động của nó đối với các mô hình kinh doanh.

Thông qua các nghiên cứu trên, chúng ta có thể thấy được tính tất yếu của việc thay thế một thị trường chứng khoán theo cơ chế quản lý tập trung

sang cơ chế quản lý phi tập trung trong tương lai nhờ vào những ưu điểm của công nghệ phi tập trung so với các mô hình truyền thống. Ở phần tiếp theo, nhóm nghiên cứu sẽ dựa trên các nghiên cứu này để đề xuất việc ứng dụng công nghệ Blockchain để xây dựng một thị trường chứng khoán mới theo cơ chế quản lý tự động và phi tập trung.

3. ĐỀ XUẤT ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN VÀO VIỆC XÂY DỰNG THỊ TRƯỜNG CHỨNG KHOÁN PHI TẬP TRUNG TẠI VIỆT NAM

Dựa trên các ưu điểm của công nghệ Blockchain như loại bỏ được các trung gian: Sở giao dịch chứng khoán, Công ty chứng khoán, trung tâm lưu ký thanh toán bù trừ góp phần giảm thiểu chi phí giao dịch trên thị trường. Đồng thời làm tăng tính bảo mật và an toàn cho toàn thị trường chứng khoán, nhóm nghiên cứu đề xuất xây dựng mô hình sàn chứng khoán phi tập trung như sau:

Mô hình hoạt động:

Doanh nghiệp thông qua tổ chức bảo lãnh phát hành chứng khoán đăng ký phát hành chứng khoán với ủy ban chứng khoán nhà nước

Đợt IPO trên sàn chứng khoán phi tập trung. Doanh nghiệp có thể đưa mức giá khởi điểm để các nhà đầu tư đấu giá cổ phiếu. Toàn bộ việc khớp lệnh trong phiên đấu giá được thực hiện sau đó các lệnh khớp theo nguyên tắc đấu giá sẽ được ghi nhận vào hệ thống Blockchain. Các nhà đầu tư tham gia vào thị trường sẽ đóng vai trò xác thực các giáo dịch trên để các giao dịch được đưa vào hệ thống Blockchain và từ đó không thể bị chỉnh sửa thông tin được nữa.

Các giao dịch mua bán trên sàn chứng khoán sau đó đều được thực hiện với phương thức trên, tức khi có một giao dịch yêu cầu được xác nhận thì máy tính của các chủ thể tham gia sẽ tự động xem xét và xác thực giao dịch. Việc xem xét và xác thực này sẽ giúp cho những người tham gia nhận được một khoản phí nhỏ xem như là phần thưởng, và phương thức trả thưởng được thực hiện trên nguyên tắc bằng chứng cổ phần (xem phụ lục 1, giao thức bầu cử). Tất cả các giao dịch sẽ được ghi vào sổ cái của Blockchain và mỗi chủ thể tham gia đều sẽ có 1 bản sao của sổ cái khổng lồ này. Nên việc tấn công để xóa hết hoặc chỉnh sửa dữ liệu là không khả thi.

Toàn bộ giao dịch sẽ là smart contract, khi giao dịch được xác thực thì chứng khoán và tiền sẽ tự động được thanh toán bù trừ.

Loại tiền được giao dịch trên hệ thống

Loại tiền tệ được giao dịch sẽ là đồng VNDT, đồng tiền kỹ thuật số ổn định (stable coin). Cứ mỗi 1 đồng VNĐT được phát hành thì sẽ được đảm bảo bởi 1 đồng VNĐ thật.

Công nghệ Blockchain được sử dụng trên sàn

Hiện nay công nghệ Blockchain đang được phát triển không ngừng. Từ Blockchain của Bitcoin với thời gian xác nhận khá lâu tối thiểu là 10 phút đến Blockchain của Etherium với thời gian rút ngắn xuống còn 2 phút, và hiện tại là Blockchain 3.0 của Binance với thời gian xác nhận chưa tới 1 phút. Tuy nhiên, nhóm nghiên cứu đề xuất sử dụng công nghệ Blockchain mới nhất 4.0 với thời gian xác nhận dưới 10 giây và do các nhà nghiên cứu của Việt Nam xây dựng đó là Blockchain của Kivachain.com. Với các ưu điểm về việc xác nhận nhanh, bảo mật và dễ xây dựng các ứng dụng trên này cũng như linh hoạt trong việc lựa chọn đồng tiền để giao dịch. Như các công nghệ Blockchain trên của thế giới thì chúng ta không thể giao dịch bằng đồng tiền riêng của Việt Nam như đề xuất ở trên.

Tiêu chuẩn niêm yết

Các doanh nghiệp đủ tiêu chuẩn phát hành cổ phiếu lần đầu ra công chúng IPO theo quy định của luật chứng khoán và các văn bản có liên quan và có nguyện vọng niêm yết trên sàn chứng khoán phi tập trung dựa trên công nghệ Blockchain.

Vốn điều lệ : Vốn điều lệ tối thiểu là 1 tỷ đồng, tương ứng với quy định về vốn điều lệ tối thiểu phát hành chứng khoán của tổ chức phát hành ở Việt Nam

Các doanh nghiệp niêm yết phải có bảng cáo bạch thể hiện rõ về ngành nghề kinh doanh, tình hình hoạt động sản xuất kinh doanh, các sản phẩm dịch vụ mà công ty cung cấp cũng như các dự án của công ty trong tương lai...

Nguyên tắc khớp lệnh:

Khớp lệnh liên tục tương tự như trên sàn HOSE và HNX, theo nguyên tắc ưu tiên thứ nhất là về giá, ưu tiên cho những người trả giá mua cao nhất và bán thấp nhất được khớp trước. Nguyên tắc thứ hai là về thời gian, ưu

tiên cho những lệnh vào trước khớp trước và nguyên tắc thứ 3 là về khối lượng, ưu tiên cho những lệnh có khối lượng cao hơn được thực hiện trước.

Thanh toán bù trừ:

Khi giao dịch được xác lập bởi các thành viên trong hệ thống thì việc thanh toán bù trừ sẽ tự động được thực hiện.

Tiền kỹ thuật số sẽ được chuyển từ người mua sang người bán và chứng khoán sẽ được chuyển từ người bán vào ví của người mua.

Phương thức giao dịch trên sàn sử dụng công nghệ Blockchain của Kivachain

Phần này trình bày một giải pháp phi tập trung nhằm mục đích cung cấp giải pháp khắc phục tất cả các nhược điểm của thị trường tập trung bằng cách cung cấp: (1) hợp đồng mang tính toàn cầu cho tất cả các giao dịch, (2) xác nhận tự động thông qua các hợp đồng thông minh, (3) tính minh bạch của các thuật toán thông qua mã hợp đồng thông minh và (4) phí giao dịch thấp thông qua thị trường cạnh tranh ngang hàng.

Một hợp đồng thông minh là một đoạn mã mô tả các quy tắc kinh doanh cần được xác minh và chấp nhận. Do đó, một hợp đồng pháp lý thực tế có thể xem như là một tập hợp các chỉ dẫn. Các hợp đồng này được đăng ký trong Blockchain, tương tự như các giao dịch. Chúng có thể được kích hoạt trong tương lai bằng các lệnh gọi giao dịch (transaction calls) và trạng thái của nó sẽ được cập nhật dựa trên kết quả thực hiện hợp đồng thông minh. Các hợp đồng thông minh nên được xem là một nhân tố có trạng thái, có chức năng và có thể được kích hoạt bất kỳ lúc nào sau khi triển khai thành công. Mục đích của hợp đồng thông minh là thay thế các bên thứ ba (thẩm phán, người công chứng, người ký quỹ, nhà môi giới, v.v.) bằng một đại lý trung lập hoạt động theo một bộ các quy tắc đã được xác định trước. Các điều khoản cụ thể của một hợp đồng thông minh phụ thuộc rất nhiều vào khuôn khổ triển khai nó.

Để mô hình hóa nền tảng thị trường phi tập trung, chúng tôi phát triển một hợp đồng thông minh, hợp đồng StockMarket hoạt động giống như một danh sách lệnh nâng cao. Như các trạng thái của hợp đồng thông minh, chúng tôi xác định thông tin sau:

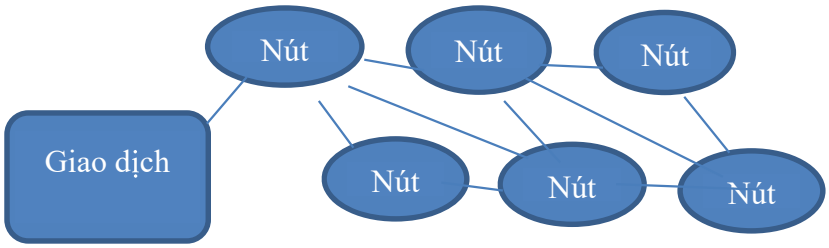
- Biểu tượng - đại diện cho tên của tài sản được giao dịch
- Ownedstocks – Ghi nhận địa chỉ chủ sở hữu và số lượng tài sản sở hữu của chủ sở hữu

- Marketprice - đại diện cho mức giá mà tại đó hành động mới nhất được thực hiện
- Bids – Danh sách các lệnh bán đã đăng ký nhưng chưa được thực hiện
- Ask– Danh sách các lệnh mua đã đăng ký nhưng chưa được thực hiện

Theo hợp đồng thông minh, mỗi thao tác đặt lệnh là một cấu trúc chứa các thông tin sau:

- Địa chỉ của người thực hiện lệnh
- Thời gian khi lệnh được đăng ký trong hệ thống
- Số lượng tài sản đã giao dịch
- Giá sẵn sàng bán / mua
- Bên đặt lệnh (Bán hoặc Mua)
- Loại lệnh (Limit hay Market)

Bên cạnh những thông tin trên, mỗi giao dịch này còn tạo ra một lệnh mới với nội dung phong tỏa một lượng tiền nhất định để thanh toán.



Ghi chú: Khi một giao dịch được thực hiện, thông tin giao dịch sẽ được truyền đi đến các nút mạng trong hệ thống và được sao lưu trên sổ cái của các nút mạng này, khi một trong các nút mạng bị tấn công nhằm chỉnh sửa dữ liệu trên sổ cái thì ngay lập tức các nút mạng khác sẽ đóng vai trò phục hồi dữ liệu tự động cho các nút mạng bị tấn công.

Hình 1. Giao dịch thực hiện một lệnh mới.

Nguồn: Tác giả tự xây dựng

Hợp đồng StockMarket được xây dựng trên chuỗi với nền tảng kiến thức về chứng khoán được sở hữu bởi những người nắm giữ. Ánh xạ giữa địa chỉ chủ sở hữu và số lượng chứng khoán sở hữu, hoạt động như một

Kho lưu ký phi tập trung, theo dõi tất cả các tài sản và cung cấp bản sao dữ liệu trên toàn mạng. Hơn nữa, bất kỳ sửa đổi nào đối với lưu ký được điều chỉnh bởi sự đồng thuận giữa các bên tham gia trong hệ thống và bất kỳ loại tấn công nào là không khả thi vì trạng thái của việc lưu ký được lưu trữ trong các khối theo cơ chế chống đánh cắp.

Một khi có thông báo sai lệch về giao dịch đặt lệnh giữa các mạng ngang hàng, tính toàn vẹn của lệnh sẽ được kiểm tra trong nền tảng trước khi thực hiện. Với nhiệm vụ của một nhà thanh toán bù trừ phi tập trung, mỗi nút trong mạng sẽ kiểm tra tính hợp lệ của lệnh bằng cách đảm bảo giao dịch chắc chắn được thực hiện khi khớp lệnh. Đối với mỗi giao dịch MUA, nó sẽ xác thực xem liệu người mua đã phong tỏa tiền hay chưa trong trường hợp giao dịch có đủ tiền để thanh toán. Điều này được kiểm tra tương ứng với số lượng và mức giá yêu cầu, tùy thuộc vào từng loại lệnh (giao dịch BÁN không cần phong tỏa tiền). Bằng cách phong tỏa tiền bên trong giao dịch, số tiền thực tế sẽ được sử dụng, không cần phải ký quỹ. Kể từ thời điểm này, tiền sẽ được phong tỏa và kiểm soát bởi hợp đồng và được chuyển đến người bán sau khi lệnh được thực hiện. Tương tự, bất cứ khi nào một giao dịch BÁN được triển khai, mạng lưới sẽ xác nhận xem liệu người bán có sở hữu đủ số lượng chứng khoán mà anh ta sẵn sàng bán hay không, bằng cách kiểm tra các mục nhập của Kho lưu ký phi tập trung.

Mỗi người bán trên thị trường sẽ đưa ra lệnh bán với đề xuất về số lượng và giá cả. Tương tự, người mua sẽ đưa ra lệnh mua chứa số lượng và giá họ sẵn sàng trả. Sau khi tạo lệnh, các lệnh này sẽ được ghi nhận và nhân rộng trong các khối trên tất cả các nút trong mạng.

Các cơ chế đồng thuận được triển khai trong hệ thống blockchain, theo dõi tất cả những thay đổi này và xác nhận từng trạng thái cập nhật tương ứng với mỗi mức giá bán /mua mà người giao dịch tương ứng nhận được. Vì hợp đồng StockMarket được sao chép trên tất cả các nút trong mạng, các giao dịch tiếp theo chứa trong một khối, được xác nhận bởi từng nút trong mạng theo cách sau. Để tạo một khối hợp lệ, nó phải chứa các giao dịch cùng với trạng thái mới nhất của tài khoản, trong trường hợp của chúng tôi là Hợp đồng StockMarket. Các trạng thái mới nhất được xác định bởi thợ đào sau khi áp dụng chuỗi hành động được đại diện bởi các giao dịch được lưu trữ trong khối đó. Khi một thợ đào chiến thắng, khối của nó sẽ được truyền tới toàn bộ mạng để xác minh và chấp nhận. Mỗi nút của mạng sẽ nhận được khối mới được khai thác này và sẽ xác thực các chuyển đổi trạng thái, bằng cách thực hiện tất cả các giao dịch liên quan đến trạng

thái đã biết từ khối trước đó và sau đó so sánh kết quả giữa khối nhận được từ thợ đào và tính toán của chính họ . Trạng thái đã thay đổi được đề xuất được chấp nhận nếu và chỉ khi xác thực là chính xác, nếu không khối sẽ bị loại bỏ và các đề xuất khối mới được chấp nhận.

Do đó, hệ thống cung cấp một ứng dụng phi tập trung hoàn toàn được nhân rộng và có độ tin cậy cao, trong đó mỗi nút có trách nhiệm xác thực tính toàn vẹn của các hành động đã đăng ký: tài sản sở hữu, giá thầu và ưu đãi, giá thị trường, giá thanh toán, v.v. Hệ thống đề xuất quản lý cung cấp phân quyền hoàn toàn, đồng thời cung cấp một hệ thống dân chủ, nơi mỗi bên liên quan có thể có quyền truy cập minh bạch vào tất cả các thuật toán và hành động được triển khai, đồng thời xác minh và xác thực tính toàn vẹn của các hành động này. Hơn nữa, một cải tiến quan trọng của hệ thống là phí thấp hơn thu được bằng cách loại bỏ các đại lý trung gian đang đại diện cho khách hàng. Các khoản phí này được thay thế bằng phí khai thác cần thiết để cung cấp tính bảo mật và tính toàn vẹn của hệ thống, bằng cách thưởng cho những thợ đào vì công việc trung thực của họ

4. THỰC NGHIỆM VÀ KẾT QUẢ

Chúng tôi đã phát triển hai nguyên mẫu để kiểm tra tính khả thi của hệ thống phi tập trung đối với hệ thống tập trung.

Một mạng blockchain riêng đã được định cấu hình bằng cách sử dụng Blockchain của Kiva Smartchain, trên bốn máy tính, từ đó có hai nút khai thác và hai nút thông thường. Hai nút khai thác được triển khai trên hai máy tính để bàn, có CPU I5-7600K, bộ nhớ RAM 16GB DDR4 và GPU nVidia 1050 2GB GDDR5 chạy Windows 10. Các nút thông thường được chạy trên hai máy tính để bàn có CPU I7-870 và bộ nhớ RAM 8GB DDR3, cũng chạy Windows 10.

Hệ thống tiến hành giả lập các giao dịch, cụ thể ba trong số các nút mạng được sử dụng để mô phỏng các khách hàng thị trường đang tương tác với hợp đồng thông minh bằng cách triển khai các lệnh mới. Các lệnh được khớp chính xác trong cả hai hệ thống tập trung và phi tập trung. Tuy nhiên, sự khác biệt đáng chú ý nhất giữa hai hệ thống là phí mà khách hàng cần phải trả để triển khai lệnh của họ.

Trong hệ thống tập trung, các khoản phí khách hàng phải trả tỷ lệ thuận với số tiền do khách hàng quản lý trong 3 tháng qua. Một khách hàng không thường xuyên của hệ thống được tính phí 0,3%, tuy nhiên, khách hàng đó có doanh thu càng cao thì hoa hồng càng giảm. Hoa hồng thấp nhất

mà hệ thống được tính là 0,1% giá trị giao dịch, được áp dụng cho các khách hàng đã giao dịch với mức giao dịch trên 100 tỷ 1 tháng. Trong khi đó, mức phí giao dịch trên Kivachain chỉ là 0.001% giá trị giao dịch và đồng đều cho tất cả các lệnh giao dịch từ thấp đến cao. Điều này sẽ mang lại lớn ích rất lớn cho các khách hàng nhỏ lẻ khi phí giao dịch của họ là ngang bằng với các giao dịch lô lớn trên thị trường chứng khoán.

Ngoài ra, với hợp đồng thông minh Stockmarket như trên, giao dịch sẽ được thực hiện ngay lập tức, tiền và chứng khoán sẽ được thanh toán bù trừ ngay chỉ trong vòng chưa đến 3 giây, thay vì phải mất 3 ngày như thị trường tập trung hiện nay bởi việc đi qua quá nhiều khâu trung gian. Điều này giúp tăng tính thanh khoản rất lớn cho các chứng khoán được giao dịch trên thị trường theo cơ chế phi tập trung.

Ưu điểm của mô hình giao dịch chứng khoán phi tập trung so với mô hình tập trung

- Khó bị tấn công

Do mỗi chủ thể tham gia đều sẽ được sao lưu một sổ cái giao dịch theo nguyên tắc phi tập trung và phân tán, nên việc mất mát dữ liệu là điều khó có thể xẩy ra, trừ khi hacker có thể tấn công vào máy tính của tất cả những người tham gia vào thị trường chứng khoán này cùng 1 lúc.

- Các giao dịch khó bị sửa lỗi

Khả năng tấn công quá bán 51% theo lý thuyết lẫn thực tế là điều không khả thi vì hacker phải chiếm quyền kiểm soát 51% các nút mạng trên hệ thống để có thể sửa bất cứ giao dịch nào, bên cạnh đó, việc sửa giao dịch chỉ có thể thực hiện ở các block mới được sinh ra chứ khogn6 thể sửa các block trong quá khứ khi nó đã được gắn vào Blockchain.

- Giảm thiểu chi phí giao dịch

Việc loại bỏ các trung gian như sở giao dịch chứng khoán, công ty chứng khoán, môi giới chứng khoán sẽ làm giảm thiểu tối đa chi phí giao dịch cho các nhà đầu tư. Các giao dịch đều được xác nhận tự động thông qua hệ thống máy tính của những người tham gia.

- Giảm thiểu thời gian thanh toán bù trừ

Sau khi hợp đồng thông minh được thực hiện thì việc thanh toán bù trừ giữa người mua và người bán sẽ được tự động thực hiện ngay lập tức mà không cần phải chờ đến T+3 như giao dịch theo phương thức truyền thống

hiện nay. Giúp tăng tính thanh khoản và giảm thiểu thời gian thanh toán bù trừ cho nhà đầu tư.

- Tránh hiện tượng làm giá, đưa lệnh ảo trên sàn

Việc giao dịch công khai, và chỉ có thể giao dịch nếu như có cổ phiếu thực sẽ tránh được các hiện tượng làm giá, đẩy lệnh ảo trên sàn gây méo mó thị trường như các thị trường giao dịch chứng khoán truyền thống.

- Tránh được việc nghẽn lệnh, quá tải của hệ thống tập trung

Do cơ chế giao dịch là cơ chế mạng ngang hàng Peer to Peer, nên việc dồn lệnh vào một hệ thống máy chủ để xử lý dẫn đến quá tải sẽ không xảy ra với mô hình giao dịch phi tập trung khi các lệnh được thực hiện ngang hàng và đồng thời với nhau thông qua các nút mạng phân tán, chính vì thế hạn chế được hiện tượng quả tải của cơ chế giao dịch tập trung cũ.

Nhược điểm của mô hình

Không thể bị sửa lỗi, đây vừa là ưu điểm nhưng cũng là nhược điểm của mô hình. Một khi giao dịch đã được thực hiện và được xác nhận đưa vào Blockchain thì không thể sửa hoặc xóa giao dịch đó trên hệ thống Blockchain được nữa, nên khi đặt lệnh sai và lệnh đã được khớp thì không thể sửa lệnh lại được.

5. CHÍNH SÁCH VÀ ĐỀ XUẤT LỘ TRÌNH THỰC HIỆN XÂY DỰNG THỊ TRƯỜNG CHỨNG KHOÁN TRÊN NỀN TẢNG BLOCKCHAIN ĐỐI VỚI CÁC BÊN LIÊN QUAN

5.1. Chính sách và vai trò của chính phủ

Trước xu thế đó, việc nghiên cứu và chấp thuận để có thể xây dựng thành công thị trường chứng khoán theo cơ chế phi tập trung là một , chính phủ và các nhà làm luật cần nghiên cứu và thông qua các quy định cho phép việc thành lập một sàn giao dịch chứng khoán dựa trên cơ chế phi tập trung. Trong đó việc quan trọng nhất là công nhận hợp pháp hợp đồng thông minh (Smart contract) trong việc giao dịch chứng khoán một cách tự động và không thông qua các trung gian như sở giao dịch chứng khoán, công ty chứng khoán như hiện tại.

Ngoài ra, chính phủ cũng cần thông qua việc công nhận dựa trên đồng tiền kỹ thuật số, mà như trong phần giải pháp, nhóm nghiên cứu có đề xuất là chính phủ hoặc Ngân hàng nhà nước có thể phát hành đồng tiền kỹ thuật số ổn định (stable coins) hoặc đồng tiền kỹ thuật số chính phủ (Govcoins)

để trở thành đơn vị tiền tệ chính thức thực hiện các giao dịch của hợp đồng thông minh. Các đồng tiền này sẽ vận hành theo cơ chế 1 đồng tiền kỹ thuật số được đảm bảo bởi 1 Việt Nam đồng, tức thực tế là chúng ta thực hiện việc mã hóa tiền Việt Nam đồng trong giao dịch trên công nghệ Blockchain.

Về loại hình công nghệ để thực hiện, như đã phân tích ở phần trên, chính phủ nên chọn một giải pháp công nghệ Blockchain ít tốn thời gian để xác minh và với chi phí thấp nhất. Nếu như sử dụng đồng Bitcoin thì do hiện nay giá của đồng Bitcoin đã rất cao nên chi phí giao dịch nếu tính trên đồng Bitcoin sẽ không khả thi và thơi gian để xác thực giao dịch với công nghệ Blockchain của Bitcoin tốn đến hơn 30 phút, điều này cũng tương tự với đồng Ethereum và các đồng phổ biến hiện tại. Bên cạnh đó còn có một khó khăn nữa là việc chuyển đổi tiền tệ từ VNĐ sang các đồng Bitcoin và Ethereum sẽ tốn các khoản chi phí chuyển đổi, và thật sự không hay nếu như chúng ta lại sử dụng một đồng tiền mã hóa của nước ngoài cho các giao dịch trong nước. Chính vì thế, nhóm nghiên cứu đề xuất chính phủ nên sử dụng công nghệ Blockchain của Kivachain để khắc phục được các nhược điểm trên.

5.2. Vai trò và giải pháp cho Ủy ban chứng khoán nhà nước

Ủy ban chứng khoán nhà nước trong mô hình này sẽ đóng vai trò là người làm luật hơn là người quản lý, nói cách khác, ủy ban sẽ là cơ quan đưa ra các quy định và giám sát các chủ thể tham gia vào thị trường chứng khoán tuân thủ các quy định chặt chẽ ở trên.

Cụ thể là các quy định tương tự như với thị trường chứng khoán tập trung để đảm bảo thị trường hoạt động một cách công khai, minh bạch như: quy định về công bố thông tin của tổ chức niêm yết, các quy định chống làm giá chứng khoán trên thị trường, quy định về xử phạt các vi phạm trong giao dịch chứng khoán…

Bên cạnh đó, Ủy ban chứng khoán cũng vẫn đóng vai trò là đơn vị kiểm định, cấp phép cho các công ty đủ điều kiện để có thể niêm yết trên sàn giao dịch chứng khoán phi tập trung tương tự với sàn giao dịch chứng khoán tập trung hiện tại như Sở giao dịch chứng khoán Thành phố Hồ Chí Minh và Hà Nội. Tuy nhiên với mô hình này thì các sở giao dịch chứng khoán sẽ không còn tồn tại với vai trò là cơ quan tổ chức thị trường nữa, giảm bớt một khâu trung gian và từ đó làm giảm thiểu chi phí giao dịch.

Khác với các mô hình phi tập trung trên thế giới, sàn giao dịch chứng khoán phi tập trung này được xây dựng trên cơ chế ghi danh chứ không ẩn danh, nhằm đảm bảo tạo điều kiện để các cơ quan như Ủy ban chứng khoán nhà nước có thể theo dõi, giám sát hoạt động giao dịch chứng khoán của các cá nhân, tổ chức, nhằm đảm bảo thị trường được vận hành một cách công khai, minh bạch, chống các hiện tượng tiêu cực như rửa tiền, làm giá chứng khoán…

Cùng với đó, Ủy ban chứng khoán Nhà nước cần có một bộ phận lập trình viên để xây dựng các ứng dụng quản lý dựa trên công nghệ học máy Machine learning và học sâu Deep learning để tự động theo dõi các giao dịch chứng khoán trên thị trường thông qua các thuật toán, từ đó phát hiện được các hành vi gian lận, làm giá chứng khoán, hay các hành vi vi phạm khác của các bên tham gia, đảm bảo và bảo vệ quyền lợi chính đáng cho các nhà đầu tư và các chủ thể tham gia thị trường. Ngoài ra, việc mở tài khoản giao dịch cũng cần ứng dụng công nghệ định danh khách hàng trực tuyến EKYC để xác thực danh tính và thông tin khách hàng. Các cá nhân và tổ chức khi muốn mở tài khoản chứng khoán cũng không cần đến các công ty chứng khoán nữa mà có thể làm trực tiếp thông qua ứng dụng của Ủy ban chứng khoán nhà nước.

Thông qua các công nghệ này, vai trò của trung tâm lưu ký và thanh toán bù trừ cũng như ngân hàng thanh toán cũng sẽ không còn nữa vì tất cả các giao dịch là hoàn toàn tự động từ việc thanh toán bù trừ về chứng khoán và tiền vốn trong các giao dịch đều thông qua hợp đồng thông minh hoàn toàn tự động. Việc này cũng góp phần làm giảm thiểu các nguồn lực không cần thiết, ứng dụng công nghệ để giảm chi phí giao dịch và mang lại lợi ích cho các nhà đầu tư cũng như các công ty niêm yết trên sàn.

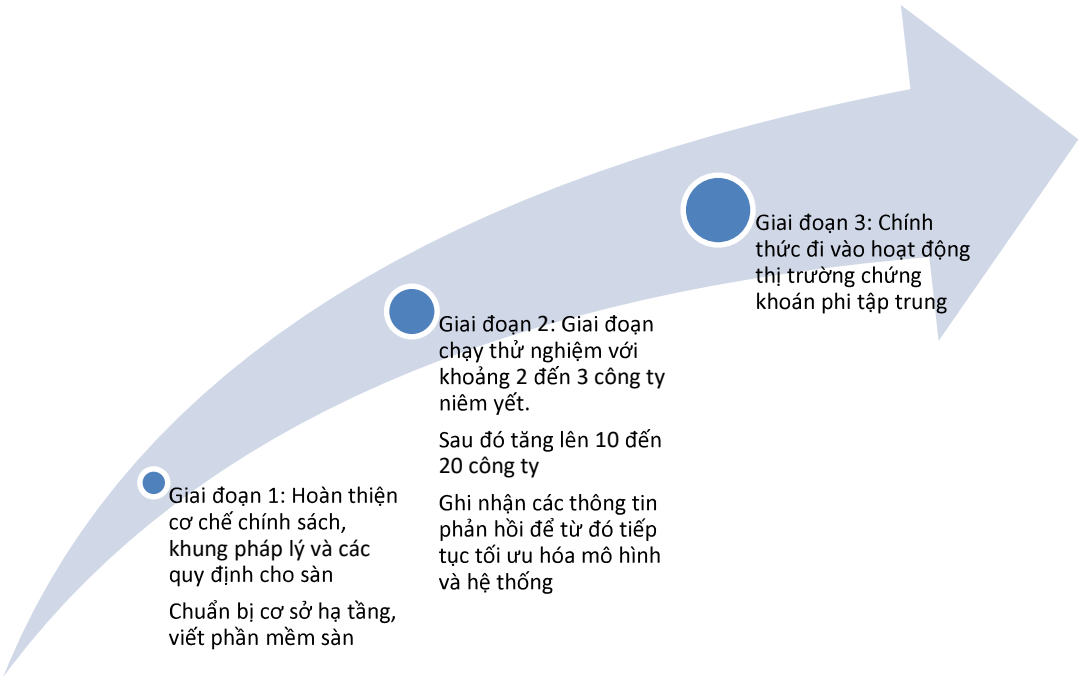
5.3. Vai trò và giải pháp cho Công ty chứng khoán

Với mô hình sàn giao dịch chứng khoán phi tập trung như trên, công ty chứng khoán sẽ không còn đóng vai trò là nhà môi giới chứng khoán, trung gian giữa người mua và người bán chứng khoán nữa, mà chỉ đơn thuần là đơn vị cung cấp các thông tin về thị trường, về các doanh nghiệp niêm yết và thực hiện nghiệp vụ tư vấn đầu tư chứng khoán cho nhà đầu tư có nhu cầu.

Để tối đa hóa hiệu quả hoạt động, công ty chứng khoán cũng cần chuyển đổi số mô hình kinh doanh. Trong đó tập trung vào ứng dụng các công nghệ như học máy, học sâu để có thể xây dựng việc tư vấn chứng

khoán tự động cho nhà đầu tư (Robo advisors) như dựa trên các đặc tính của nhà đầu tư từ việc EKYC mà có thể đưa ra các danh mục đầu tư phù hợp với khẩu vị rủi ro của từng nhà đầu tư khác nhau. Từ đó có thể chăm sóc được nhiều nhà đầu tư hơn một cách tự động hóa hoàn toàn.

5.4. Lộ trình và kế hoạch triển khai



Hình 2. Lộ trình triển khai sàn chứng khoán phi tập trung.

Nguồn: Tác giả tự xây dựng.

Giai đoạn 1:

Bộ tài chính cần nghiên cứu hoàn thiện các cơ chế chính sách, ban hành khung pháp lý chuẩn cho thị trường chứng khoán phi tập trung dựa trên công nghệ Blockchain.

Ủy ban chứng khoán Nhà nước sẽ dựa trên các quy định trên làm cơ sở để ban hành các quy định giao dịch trên sàn, quy định về quyền và trách nhiệm của các bên liên quan.

Song song với đó, Ủy ban chứng khoán Nhà nước sẽ là đơn vị phụ trách xây dựng cơ sở hạ tầng cho sàn như hệ thống bảng điện tử, phần mềm và apps giao dịch cho các nhà đầu tư, xây dựng hệ thống quản lý như xác thực thông tin cá nhân online EKYC để nhà đầu tư có thể mở tài khoản giao dịch trực tuyến, xây dựng hệ thống phân tích cơ sở dữ liệu tự động để quản

lý và phát hiện các hành vi gian lận, sai phạm trong quá trình giao dịch bằng công nghệ học máy Machine learning.

Do công nghệ Blockchain của Kivachain là mã nguồn mở và được tài trợ và chuyển giao công nghệ miễn phí bởi công ty Kivachain nên Bộ Tài chính sẽ giảm thiểu được chi phí cho phần phát triển công nghệ. Các công nghệ khác được nêu trên như EKYC, phân tích dữ liệu bằng công nghệ học máy Machine learning cũng sẽ được phát triển bằng nguồn xã hội hóa, công ty Kivachain và các công ty công nghệ Việt Nam như FPT sẽ hỗ trợ để phát triển phần này. Vai trò của Ủy ban chứng khoán Nhà nước là phân công đội vận hành để cùng phát triển phần mềm và nhận chuyển giao phần mềm khi hoàn thành.

Giai đoạn 2:

Sau khi phần mềm đã được hoàn thiện, bước tiếp theo là tiến hành chạy thử nghiệm giao dịch ảo với khoảng 2 đến 3 mã chứng khoán trên sàn để kiểm tra hệ thống. Từ đó có những phản hồi điều chỉnh kịp thời cho đội phát triển phần mềm để chỉnh sửa và tối ưu hóa hệ thống.

Tiếp theo là kiểm tra hệ thống trên diện rộng với sự tham gia của 20 đến 30 mã chứng khoán trên sàn, và các nhà đầu tư được giới thiệu để tham gia vào quá trình kiểm tra hệ thống trong giai đoạn thử nghiệm. Đội vận hành sẽ ghi nhận lại các phản hồi từ các bên liên quan để có những thông tin điều chỉnh cho đội phát triển phần mềm chỉnh sửa lần cuối trước khi tung bản giao dịch chính thức.

Song song với đó, Ủy ban chứng khoán sẽ tiếp nhận các đơn đăng ký của các doanh nghiệp có nhu cầu niêm yết trên thị trường chứng khoán phi tập trung để xem xét và phê duyệt.

Giai đoạn 3: Giai đoạn chạy chính thức

Đưa hệ thống giao dịch chứng khoán phi tập trung vào chạy chính thức. Các mã cổ phiếu sẽ được niêm yết chính thức trên sàn và các nhà đầu tư có thể tham gia để đầu tư giao dịch mua bán các cổ phiếu trên.

Đội vận hành hệ thống của Ủy ban chứng khoán sẽ là đội quản lý trực tiếp hệ thống giao dịch chứng khoán này.

Trong mô hình này, việc vận hành thị trường sẽ tự động hóa dựa trên các hợp đồng thông minh và loại bỏ tối đa các trung giant ham gia hệ thống như Sở giao dịch chứng khoán và công ty chứng khoán. Lúc này công ty

chứng khoán chỉ đóng vai trò là một đơn vị cung cấp thông tin và tư vấn đầu tư độc lập cho các nhà đầu tư có nhu cầu.

6. KẾT LUẬN

Trong bài viết này, chúng tôi đề xuất một giải pháp phi tập trung cho Thị trường chứng khoán để khắc phục những hạn chế của kiến trúc tập trung và giảm phí giao dịch do các nhà môi giới và các cơ quan quản lý tập trung. Chúng tôi tích hợp các yếu tố thị trường chứng khoán trong một kiến trúc blockchain cùng với các hợp đồng thông minh được liên kết để đảm bảo sự tự thực thi các lệnh thực hiện.

Bài báo cũng đã dựng mô phỏng hợp đồng thông minh để giao dịch thử chứng khoán trong Kivachain để xác thực và kiểm tra kiến trúc được đề xuất. Kết quả đầy hứa hẹn cho thấy rằng giải pháp giao dịch dựa trên blockchain có lợi thế rõ ràng là cung cấp mức phí thấp hơn đến hàng trăm lần so với giao dịch truyền thống. Điều này giúp làm giảm thiểu phí giao dịch, giảm thời gian thanh toán bù trừ và các vấn đề phát sinh trong quá trình giao dịch rất nhiều cho các nhà đầu tư đặc biệt là các nhà đầu tư nhỏ lẻ. Bên cạnh đó, bài báo cũng đề xuất các chính sách và lộ trình nhằm xây dựng thị trường chứng khoán theo cơ chế phi tập trung trong tương lai tại Việt Nam, nhằm tận dụng và phát huy việc ứng dụng công nghệ trong cuộc cách mạng 4.0 giúp Việt Nam tiệm cận với các nước trong khu vực và trên thế giới trong cuộc đua về công nghệ. Khi cải tiến trong tương lai, chúng tôi đề xuất nghiên cứu việc tích hợp thêm các thuật toán tối ưu để cung cấp cho hệ thống khả năng mở rộng hàng triệu giao dịch mỗi giây, đồng thời giảm phí gần bằng không.

TÀI LIỆU THAM KHẢO

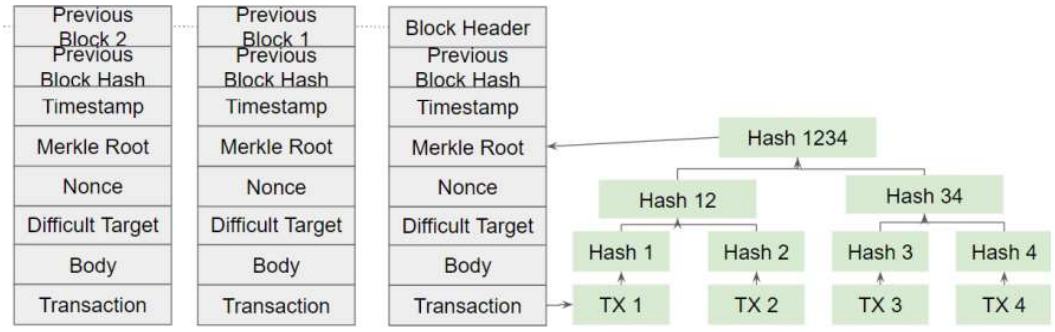
2. Al-Shaibani, H., Lasla, N., & Abdallah, M. (2020). Consortium Blockchain-Based Decentralized Stock Exchange Platform. IEEE Access, 8, 123711-123725. doi: 10.1109/access.2020.3005663.
3. Bansal, G., Hasija, V., Chamola, V., Kumar, N., & Guizani, M. (2019). Smart Stock Exchange Market: A Secure Predictive Decentralized Model. 2019 IEEE Global Communications Conference (GLOBECOM). doi: 10.1109/globecom38437.2019.9013787.
4. Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., & Vines, J. (2018). Making Sense of Blockchain Applications. Proceedings Of The 2018 CHI Conference On Human Factors In Computing Systems. doi: 10.1145/3173574.3174032.
5. Foroglou, G., & Tsilidou, A. L. (2015, May). Further applications of the blockchain. In 12th student conference on managerial science and technology (pp. 1-8).
6. George Foroglou, Anna-Lali Tsilidou (2015). Further applications of the blockchain.
7. Grech, A., & Camilleri, A. F. (2017). Blockchain in education. Luxembourg: Publications Office of the European Union.
8. Jaoude, J. A., & Saade, R. (2019). Business Applications of Blockchain Technology-A Systematic Review. IEEE Access.
9. Lo, S. K., Xu, X., Chiam, Y. K., & Lu, Q. (2017, November). Evaluating suitability of applying blockchain. In 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS) (pp. 158-161). IEEE.
10. Marcinkowska, E. (2020). Blockchain effect on the New Connect Stock Exchange. Journal Of Economics And Management, 40, 52-73. doi: 10.22367/jem.2020.40.03Lo, S., Xu, X., Chiam, Y., & Lu, Q. (2017). Evaluating Suitability of Applying Blockchain. 2017 22Nd International Conference On Engineering Of Complex Computer Systems (ICECCS). doi: 10.1109/iceccs.2017.26.
11. Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). IEEE.
12. Miraz, M., & Donald, D. (2018). Application of Blockchain in Booking and Registration Systems of Securities Exchanges. 2018 International

Conference On Computing, Electronics & Communications Engineering (Iccece). doi: 10.1109/iccecome.2018.8658726.
13. Monrat, A., Schelen, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. IEEE Access, 7, 117134-117151. doi: 10.1109/access.2019.2936094.
14. Nowiński, W., & Kozma, M. (2017). How Can Blockchain Technology Disrupt the Existing Business Models?. Entrepreneurial Business And Economics Review, 5(3), 173-188. doi: 10.15678/eber.2017.050309.
15. Pop, C., Pop, C., Marcel, A., Vesa, A., Petrican, T., & Cioara, T. et al. (2018). Decentralizing the Stock Exchange using Blockchain An Ethereum-based implementation of the Bucharest Stock Exchange. 2018 IEEE 14Th International Conference On Intelligent Computer Communication And Processing (ICCP). doi: 10.1109/iccp.2018.8516610.

PHỤ LỤC 1

1. Cơ chế giao dịch của sàn dựa trên Kivachain

Kivachain lưu trữ và truyền khóa người dùng bằng cách sử dụng hệ thống ngang hàng phi tập trung không cần kiểm duyệt độ tin cậy Trust Authority (TA) và khắc phục được một điểm lỗi duy nhất. Bản đồ này cho thấy cấu trúc cơ bản của blockchain. Tiêu đề khối bao gồm phiên bản, hàm băm của khối trước đó (PreHash), gốc Merkle, dấu thời gian (TS), mục tiêu độ khó và nonce. Gốc Merkle là mã băm gốc của cây băm Merkle (MHT). Nếu blockchain sử dụng giao thức đồng thuận bằng chứng công việc (PoW), thì mục tiêu độ khó được các thợ đào tính toán là Hash (PreHash | TS | MerkleRoot | nonce) <mục tiêu độ khó. Sau khi người khai thác tìm thấy một khối nonce và khối phát sóng trong mạng, nếu khối này thuộc về blockchain mẹ, các nút khác sẽ thừa nhận tính hợp lệ của khối này.



2. Quy trình sản xuất chuỗi khối

Trình xác thực của mạng blockchain thu thập các giao dịch mới được tạo trong mạng blockchain, xác minh tính hợp pháp của các giao dịch này, đóng gói các giao dịch trong một khối, ghi lại chúng dưới dạng một trang mới trên sổ cái và phát tán trang đó tới toàn bộ mạng blockchain. Các nút khác sẽ nhận được trang mới và xác minh tính hợp pháp của dữ liệu giao dịch trên trang và thêm nó vào sổ cái của riêng họ. Vì trình xác thực sẽ lặp lại quá trình này, tất cả dữ liệu giao dịch mới trong hệ thống blockchain có thể được ghi lại trong sổ cái.

3. Tổng quan về Bằng chứng ủy quyền cổ phần- Proof of Stake (DPOS)

Vai trò của sự đồng thuận là chọn những người xác nhận trong hệ thống blockchain. Người xác thực xác minh dữ liệu giao dịch và giữ tài khoản để phát tài khoản mới đến các nút khác trong mạng và nhận được sự chấp thuận của các tài khoản mới từ các nút khác. Là một triển khai cụ thể của sự đồng thuận, DPoS hoạt động theo cách sau.

Sự đồng thuận DPoS chọn một số nút làm trình xác nhận trong hệ thống blockchain dựa trên số phiếu bầu mà họ nhận được. Đầu tiên, khi hệ thống blockchain bắt đầu hoạt động, một số số lượng mã thông báo sẽ được phát hành và sau đó các mã thông báo sẽ được trao cho các nút trong hệ thống blockchain. Một nút có thể đăng ký trở thành ứng cử viên xác thực trong hệ thống blockchain với một phần mã thông báo. Bất kỳ nút nắm giữ mã thông báo nào trong hệ thống blockchain đều có thể bỏ phiếu cho những ứng cử viên này. Mỗi khoảng thời gian T, phiếu bầu cho tất cả các ứng cử viên sẽ được tính. N nút ứng cử viên hàng đầu có nhiều phiếu bầu nhất sẽ trở thành trình xác nhận cho khoảng thời gian T tiếp theo. Sau khoảng thời gian T, các phiếu bầu sẽ được đếm lại để bầu ra những người xác nhận mới và chu kỳ tiếp tục.

- Kivachain: đề cập đến mạng Kivachain. Tài liệu không phân biệt giữa Kivachain, chuỗi khối Kivachain, hệ thống chuỗi khối Kivachain, v.v.
- Kivachain coin: đề cập đến mã thông báo vốn được phát hành và lưu hành trong Kivachain, được gọi là Kiva.
- Ứng cử viên trình xác thực: các nút đủ điều kiện để trở thành trình xác nhận trong Kivachain.

- Trình xác thực: các nút trong Kivachain đủ điều kiện để lưu giữ sổ sách. Chúng thường được gọi là trình xác nhận trong đồng thuận DPoS. Trong Kivachain, sẽ có 33 trình xác nhận, còn được gọi là siêu nút (hoặc SR). Ở đây, chúng ta sẽ không phân biệt giữa bookkeeper, validator, supernode, SR, v.v.
- Ghi sổ kế toán: quá trình xác minh các giao dịch và ghi chúng vào sổ cái.

Vì sổ cái trong Kivachain được thực hiện theo các khối, nên quá trình ghi sổ kế toán còn được gọi là tạo khối. Chúng tôi sẽ không phân biệt giữa việc ghi sổ và tạo khối trong tài liệu.

- Trình tự ghi sổ: thứ tự tạo khối. Thứ tự giảm dần của 33 người xác nhận dựa trên số phiếu bầu mà họ nhận được.
- Thời gian chặn: Kivachain đặt thời gian chặn là 3 giây. Điều này có nghĩa là một khối được tạo ra sau mỗi 3 giây.
- Khe: sau mỗi khối được tạo, nó có thể được đưa vào một khe; và mỗi khối được tạo sẽ chiếm một vị trí. Ví dụ, có 20 khe cho mỗi phút. Khi một khối được tạo trong thời gian khối, vị trí tương ứng sẽ được lấp đầy. Tuy nhiên, nếu một khối không được tạo, thì vị trí tương ứng sẽ trống. Khối tiếp theo được tạo sẽ điền vào một vị trí mới tương ứng.
- Kỷ nguyên: Kivachain đặt Kỷ nguyên là 6 giờ. Thời gian khối 2 cuối cùng của một Kỷ nguyên là khoảng thời gian bảo trì, trong đó thứ tự tạo khối cho Kỷ nguyên tiếp theo sẽ được quyết định.
- Thời gian duy trì: Kivachain đặt khoảng thời gian là 2 block time, là 6 giây. Khoảng thời gian này được dùng để kiểm phiếu cho các ứng cử viên. Có 4 Kỷ nguyên trong 24 giờ và đương nhiên là 4 kỳ bảo trì. Trong thời gian bảo trì, không có khối nào được tạo và thứ tự tạo khối cho Kỷ nguyên tiếp theo được quyết định.

4. Giao thức bầu cử

Trong mỗi giai đoạn (Epoch), 33 trình xác nhận sẽ thay phiên nhau tạo các khối theo thứ tự ghi sổ. Mỗi trình xác nhận chỉ có thể tạo các khối khi đến lượt của họ. Trình xác thực đóng gói dữ liệu của nhiều giao dịch đã xác minh vào mỗi khối. Hàm băm của khối trước đó sẽ được bao gồm trong mỗi khối mới như là parentHash. Trình xác thực sẽ ký dữ liệu của khối này bằng

khóa cá nhân của mình và điền vào validators_signature, cùng với địa chỉ của trình xác thực, chiều cao khối và thời gian khối đó được tạo, v.v.

Thông qua việc lưu trữ băm của khối trước đó, các khối được kết nối một cách hợp lý. Cuối cùng, chúng tạo thành một chuỗi. Một cấu trúc blockchain điển hình được thể hiện trong hình sau: Trong trường hợp lý tưởng, quy trình ghi sổ trong hệ thống blockchain dựa trên sự đồng thuận DPoS sẽ tiến hành theo thứ tự ghi sổ được tính toán trước. Lần lượt các khối được tạo bởi trình xác nhận. Tuy nhiên, trên thực tế, mạng blockchain là một hệ thống phức tạp phân tán và không đáng tin cậy theo ba cách sau đây. - Do môi trường mạng kém, các khối được tạo bởi một số trình xác thực không thể được các trình xác nhận khác nhận trong thời gian hợp lệ. - Không thể luôn đảm bảo hoạt động bình thường của một trình xác nhận nhất định.

- Một số trình xác nhận độc hại sẽ tạo ra các khối fork để phân tách chuỗi.

Như đã đề cập ở trên, cơ sở để hệ thống blockchain hoạt động bình thường là hầu hết các nút trong hệ thống đều trung thực và đáng tin cậy. Hơn nữa, đảm bảo chính cho tính bảo mật của hệ thống blockchain là tính bảo mật của sổ cái, có nghĩa là dữ liệu bất hợp pháp không thể được ghi vào sổ cái một cách độc hại và các bản sao sổ cái được lưu trên mỗi nút cũng phải nhất quán. Dựa trên sự đồng thuận của DPoS, quy trình ghi sổ kế toán được thực hiện bởi những người xác nhận. Do đó, sự an toàn của Kivachain phụ thuộc vào độ tin cậy của đa số người xác nhận. Kivachain đã đặt các khối đã được xác nhận vào hệ thống là không thể thay đổi. Đồng thời, để chống lại các hành vi độc hại của một số lượng nhỏ các nút trình xác thực, Kivachain công nhận chuỗi dài nhất là chuỗi chính dựa trên "nguyên tắc chuỗi dài nhất".

5. Trình xác thực

Mọi tài khoản trong mạng Kivachain đều có thể đăng ký và có cơ hội trở thành người xác thực. Mọi người đều có thể bỏ phiếu cho các ứng cử viên xác nhận. 33 ứng cử viên hàng đầu có nhiều phiếu bầu nhất sẽ trở thành người xác nhận quyền và nghĩa vụ tạo ra các khối. Các phiếu bầu được đếm cứ sau 6 giờ và những người xác nhận sẽ thay đổi tương ứng. Để ngăn chặn các cuộc tấn công độc hại, bạn phải trả một cái giá để trở thành một ứng cử viên xác thực. Khi nộp đơn, 300.000 Kiva sẽ được đốt từ tài

khoản của người nộp đơn. Sau khi thành công, một tài khoản như vậy có thể tham gia cuộc bầu cử người xác nhận.

6. Nguyên tắc khối xác nhận

Các khối mới được sản xuất ở trạng thái chưa được xác nhận và chỉ những khối được "chấp thuận" hơn 70% (tức là 27 * 70% = 18, làm tròn xuống) trong số 33 Trình xác thực mới được coi là khối không thể đảo ngược, thường được gọi là các khối được củng cố và các giao dịch chứa trong các khối đã được củng cố đã được xác nhận bởi toàn bộ mạng lưới blockchain. Cách "phê duyệt" khối trạng thái chưa được xác nhận là Trình xác thực tạo ra các khối tiếp theo sau nó, Trình xác thực C tạo ra khối 103, Trình xác thực E tạo ra 104 'trên cơ sở khối 103, khối 105', 106 'và 107 'được tạo ra tương ứng bởi Trình xác thực G, A và B, cũng là các khối tiếp theo của khối thứ 103, có nghĩa là bốn khối này chấp thuận khối thứ 103. Có thể thấy rằng khi khối có chiều cao 121 được sản xuất thì khối thứ 103 trở thành khối đông đặc lại, vì lúc này khối thứ 103 có 18 khối tiếp theo, và điểm cần nhấn mạnh ở đây là Người xác nhận sản xuất 18 khối này phải khác nhau và từ Trình xác thực tạo ra khối thứ 103.

7. Chuỗi thông minh Kiva

Kiva Smart Chain là một giải pháp sáng tạo để mang lại khả năng lập trình và khả năng tương tác cho Kiva Chain. Kiva Smart Chain dựa trên hệ thống 33 trình xác nhận có sự đồng thuận của Proof of Staked 11Authority (PoSA) có thể hỗ trợ thời gian khối ngắn và phí thấp hơn. Các ứng cử viên xác thực liên quan nhất của việc đặt cược sẽ trở thành người xác nhận và tạo ra các khối. Phát hiện dấu hiệu kép và logic cắt khác đảm bảo tính bảo mật, ổn định và tính cuối cùng của chuỗi. Kiva Smart Chain cũng hỗ trợ các giao thức và hợp đồng thông minh tương thích với EMV. Có thể chuyển giao xuyên chuỗi và các giao tiếp khác do khả năng tương tác được hỗ trợ. Kiva DEX vẫn là một địa điểm trao đổi tài sản thanh khoản trên cả hai chuỗi.

Kiến trúc chuỗi kép này sẽ lý tưởng để người dùng tận dụng lợi thế của giao dịch nhanh ở một bên và xây dựng các ứng dụng phi tập trung của họ ở phía bên kia. Chuỗi thông minh Kiva sẽ là:

- Một blockchain tự chủ: Cung cấp bảo mật và an toàn với những người xác nhận được bầu chọn.
- Tương thích với EVM: Hỗ trợ tất cả các công cụ Ethereum hiện có cùng với khả năng hoàn thiện nhanh hơn và phí giao dịch rẻ hơn.

- Có thể tương tác: Đi kèm với giao tiếp chuỗi kép bản địa hiệu quả; Được tối ưu hóa để mở rộng các dApp hiệu suất cao yêu cầu trải nghiệm người dùng nhanh và mượt mà.
- Phân tán với quản trị trên chuỗi: Proof of Staked Authority mang lại sự phân quyền và những người tham gia cộng đồng. Là mã thông báo gốc, Kiva Smart Chain sẽ đóng vai trò vừa là nguồn cung cấp thực thi hợp đồng thông minh vừa là mã thông báo để đặt cược.

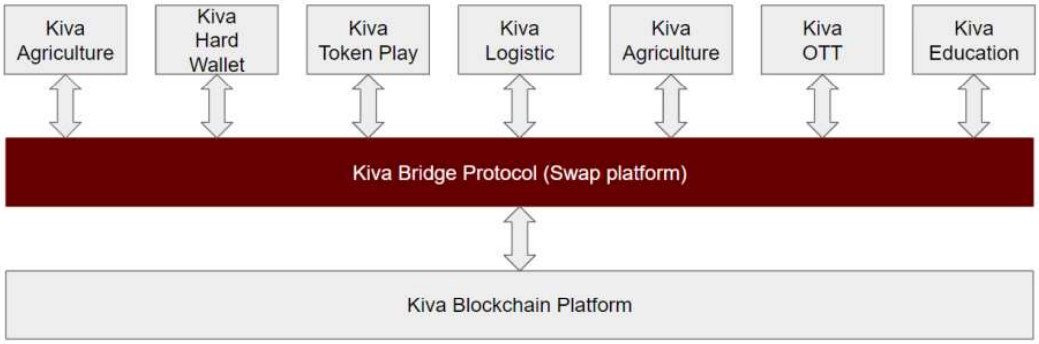
8. Nguyên tắc thiết kế

Blockchain độc lập: về mặt kỹ thuật, Kiva Smart Chain (KSC) là một blockchain độc lập, thay vì giải pháp lớp 2. Hầu hết các chức năng kỹ thuật và kinh doanh cơ bản của KSC nên được khép kín để hoạt động tốt ngay cả khi Kivachain ngừng hoạt động trong một thời gian ngắn. Khả năng tương thích của Ethereum: Nền tảng Hợp đồng thông minh thực tế và được sử dụng rộng rãi đầu tiên là Ethereum. Để tận dụng lợi thế của các ứng dụng và cộng đồng tương đối trưởng thành, KSC chọn tương thích với mạng chính Ethereum hiện có. Điều này có nghĩa là hầu hết các dApp, thành phần hệ sinh thái và công cụ sẽ hoạt động với KSC và yêu cầu không hoặc thay đổi tối thiểu; Các nút KSC sẽ yêu cầu các thông số kỹ thuật và kỹ năng phần cứng tương tự (hoặc cao hơn một chút) để chạy và vận hành. Việc triển khai sẽ để lại khoảng trống cho KSC để bắt kịp với các nâng cấp Ethereum hơn nữa. 12 Đồng thuận và Quản trị có sự tham gia của Thực hiện: Sự đồng thuận dựa trên sự cố định thân thiện hơn với môi trường và để lại các lựa chọn linh hoạt hơn cho quản trị cộng đồng. Dự kiến, sự đồng thuận này sẽ cho phép hiệu suất mạng tốt hơn qua các hệ thống blockchain bằng chứng công việc, tức là thời gian chặn nhanh hơn và khả năng giao dịch cao hơn. Giao tiếp chuỗi chéo bản địa: Kivachain sẽ được triển khai với sự hỗ trợ riêng cho giao tiếp chuỗi chéo giữa hai blockchain. Giao thức truyền thông phải là hai hướng, phi tập trung và không đáng tin cậy. Nó sẽ tập trung vào việc di chuyển tài sản kỹ thuật số giữa Kivachain và KSC, tức là mã thông báo BEP2 và cuối cùng là các mã thông báo BEP khác được giới thiệu sau đó. Giao thức nên quan tâm đến mức tối thiểu các mục khác được lưu trữ trong trạng thái của các blockchains, chỉ với một số ngoại lệ.

9. Giao tiếp giữa các chuỗi

Chuỗi bên giao tiếp với chuỗi gốc và các chuỗi khác thông qua hợp đồng thông minh. Kivachain cung cấp hệ thống hợp đồng thông minh cho giao tiếp này được gọi là giao thức Kiva Bridge. Các quỹ từ chuỗi bên cũng

được giữ trên chuỗi gốc. Điều này cho phép chứng minh gian lận tiền gửi và rút tiền trên chuỗi bên thông qua chuyển đổi trạng thái. Chuỗi bên không tiết lộ tất cả thông tin trên chuỗi gốc. Thay vào đó, các hàm băm của blockheader và danh sách các trạng thái được gửi và nếu có bằng chứng về gian lận trên root-chain, thì block sẽ được khôi phục và người tạo block sẽ bị phạt bởi hệ thống hợp đồng thông minh do root-chain quản lý. Giao thức Kiva Bridge cũng giúp Kivachain giao tiếp với các nền tảng Blockchain khác. I E. thông tin, mã thông báo để trao đổi với Kiva Wallet, Kiva Agricultural, Kiva OTT, Kiva Education, v.v. Trong trường hợp trao đổi mã thông báo sang các nền tảng Blockchain khác, giao thức Kiva Bridge hoạt động như một sàn giao dịch phi tập trung



10. Thuật toán đồng thuận DPoS-HotStuff

Sự đồng thuận là trung tâm của bất kỳ nền tảng Blockchain nào. Thuật toán đồng thuận phổ biến trong Bitcoin và Ethereum là Proof of Work (PoW) tiêu thụ một lượng lớn năng lượng điện để đảm bảo một sổ cái. Loại thuật toán đồng thuận này làm cho Blockchain hoàn toàn minh bạch, công khai và phi tập trung nhưng không thể mở rộng quy mô để thích ứng với khối lượng giao dịch lớn. Trong bài báo này, Chúng tôi áp dụng Bằng chứng Cổ phần được Ủy quyền (DPoS) cho nền tảng của chúng tôi. DPoS không phải là một thuật toán đồng thuận mới. Nó đã được áp dụng ở Bitshare, Konla và những nơi khác. Tuy nhiên, chúng tôi kết hợp DPoS với HotStuff và kiến trúc chuỗi bên để làm cho hệ thống của chúng tôi có thể mở rộng và đạt được tính cuối cùng của Khối sau một giây DPoS là một thuật toán đồng thuận được phát triển để bảo mật một Blockchain bằng cách đảm bảo đại diện cho các giao dịch bên trong nó. DPoS được thiết kế để thực hiện nền dân chủ dựa trên công nghệ. Sử dụng các quy trình bầu cử và bầu cử để bảo vệ các Blockchains khỏi việc tập trung hóa và sử dụng độc

hại. Trước khi bạn có thể hiểu đầy đủ về cách hoạt động của Kivachain DPoS, chúng ta cần làm rõ một số thuật ngữ:

Tài khoản: Một danh tính duy nhất trên Kivachain. Mỗi tài khoản có một cặp khóa rất riêng. Các địa chỉ là một đại diện tài khoản trên Blockchain.

- Kiva Coin: Đây là mã thông báo gốc của Kivachain.
- Bên liên quan: Bất kỳ tài khoản nào có số dư mã thông báo> 014 ● Nút: thích các nút thông thường và là một phần mềm mà bất kỳ ai cũng có thể tải xuống để chạy và duy trì sổ cái, xác thực- và cập nhật các giao dịch.
- Nút trình xác thực: Một nút 'đầy đủ' đại diện cho một tài khoản có tối thiểu 3 tỷ đồng tiền và nhận đủ phiếu bầu chấp thuận từ cộng đồng. Các giao dịch và khối chỉ được xác thực bởi các nút trình xác thực. Trong Kivachain, có 33 nút trình xác nhận theo mặc định. Con số đó có thể được tăng lên. Để trở thành một nút xác thực, các Bên liên quan phải gửi ít nhất 3 tỷ mã thông báo vào tài khoản của họ và sau đó phát sóng các giao dịch để đăng ký làm ứng cử viên cho nút xác thực. Các bên liên quan khác sẽ bỏ phiếu để quyết định người xác nhận. Sức mạnh của phiếu bầu dựa trên số lượng token mà các bên liên quan có. 33 ứng cử viên hàng đầu với số phiếu "lớn nhất" sẽ trở thành nút xác nhận. Quá trình bỏ phiếu được lặp lại sau mỗi 1670 khối được gọi là kỷ nguyên. Trong mỗi nút xác thực kỷ nguyên có khả năng tạo ra tổng cộng 32 khối. Cách các nút xác thực tạo ra khối trong Kivachain Sau quá trình bầu chọn, 100 nút xác nhận được bầu chọn hiện đã sẵn sàng để sản xuất khối. Thuật toán DPoS truyền thống ‘round-robin’ tạo ra các khối. I E. khối n được tạo ra bởi trình xác nhận n

Trình xác thực ∈ {1, 2, 3, n - 1, n}

Khối ∈ {1, 2, 3, n - 1, n}

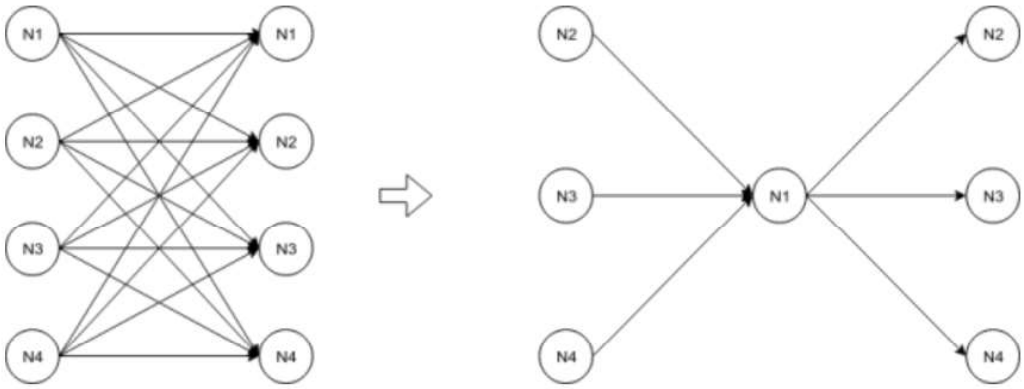
Quá trình được dự đoán và có thể bị phá vỡ bởi một nút xác thực không trung thực. Để bảo vệ khối tạo ra các dự đoán không bị xoay chuyển, chúng tôi đề xuất một trình xác thực ngẫu nhiên tạo ra các khối trong khi đảm bảo rằng mọi trình xác thực tạo ra số lượng khối bằng nhau (32 khối cho mỗi kỷ nguyên).

Trình xác thực thuật toán được chọn ngẫu nhiên. chỉ được biết đến tại thời điểm tính toán xử lý, magicNumber là số chưa biết và do đó trình xác

nhận được chọn tiếp theo vẫn là một bí mật. Bằng cách sử dụng các công thức như được hiển thị ở trên, một trình xác nhận có thể được chọn theo n-time để tạo ra một khối và nó có thể vượt quá khả năng của 32 lần tương ứng. Để giải quyết vấn đề này, khi bất kỳ trình xác thực nào đạt đến số lượng khối sản xuất tối đa, Nó sẽ bị loại bỏ khỏi nhóm lựa chọn ngẫu nhiên và cho một trình xác thực khác một cơ hội.

HotStuff

HotStuff là một giao thức sao chép khả năng chịu lỗi (BFT) của Byzantine dựa trên người dẫn đầu cho mô hình đồng bộ một phần. Nó được sử dụng trong dự án Libra và giảm độ phức tạp của giao tiếp - tuyến tính trong số lượng bản sao. HotStuff thay đổi giao tiếp BFT từ mạng lưới thành mạng hình sao, dựa vào người dẫn đầu



BFT truyền thống thực tế sử dụng hai vòng trao đổi tin nhắn. Giai đoạn đầu tiên đảm bảo tính duy nhất của đề xuất thông qua việc hình thành chứng chỉ số đại biểu (QC) bao gồm (n - f) phiếu bầu. Giai đoạn thứ hai đảm bảo rằng nhà lãnh đạo tiếp theo có thể thuyết phục các bản sao bỏ phiếu cho một đề xuất an toàn. Thuật toán để một nhà lãnh đạo mới thu thập thông tin và đề xuất nó cho các bản sao được gọi là thay đổi chế độ xem. Hai giai đoạn thay đổi chế độ xem dựa trên BFT truyền thống và không đơn giản hoặc dễ xảy ra lỗi. Bất kỳ đề xuất nào trong BFT đều có dấu vết giao tiếp của trình xác thực O (n 3). 16Tổng số 3 trình xác thực được truyền - nếu O (n) lần thay đổi chế độ xem xảy ra trước khi đạt được một quyết định đồng thuận - là O (n 4). HotStuff có ba giai đoạn, cho phép một nhà lãnh đạo mới chỉ cần chọn QC cao nhất mà họ biết. Nó giới thiệu giai đoạn thứ hai cho phép các bản sao “thay đổi ý kiến” sau khi bỏ phiếu trong giai đoạn mà không yêu cầu bằng chứng về người lãnh đạo. Điều này

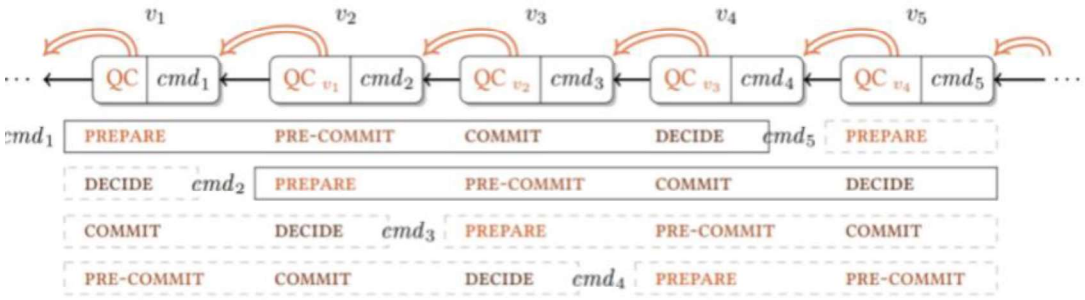
làm giảm bớt sự phức tạp ở trên và đồng thời đơn giản hóa đáng kể quy trình giao thức thay thế người lãnh đạo.

	Authenticator complexity		
Protocol	*Correct leader*	*view-change*	*f leader failures*
DLS	$O(n^4)$	$O(n^4)$	$O(n^4)$
PBFT	$O(n^2)$	$O(n^3)$	$O(fn^4)$
SBFT	$O(n)$	$O(n^2)$	$O(fn^2)$
Tendermint/Casper	$O(n^2)$	$O(n^2)$	$O(fn^2)$
HotStuff	$O(n)$	$O(n)$	$O(fn)$

Trong HotStuff:

- Giai đoạn tiền cam kết: Người lãnh đạo nhận được phiếu chuẩn bị cho đề xuất hiện tại. Nó kết hợp để chuẩn bịQC và sau đó phát pre-commit tới tất cả các nút trong mạng - Giai đoạn cam kết: Leader nhận được các phiếu pre-commit từ (n-f) các nút, sau đó kết hợp nó thành bản tin precommitQC và cuối cùng là phát tới tất cả các nút trong mạng. Khi các bản sao nhận được thông báo, Nó sẽ khóa yêu cầu chuyển đổi trạng thái để q`1 của quyết định đồng thuận có thể đạt được. - Giai đoạn quyết định: Khi người lãnh đạo nhận đủ phiếu cam kết từ mạng, nó sẽ kết hợp chúng lại với commitQC sau đó phát thông báo quyết định tới mạng. Các bản sao trong mạng nhận được thông báo quyết định thực hiện chuyển đổi trạng thái, xác nhận trạng thái và sau đó bắt đầu chế độ xem tiếp theo. The pipelined HotStuff

HotStuff luôn có 'giai đoạn giống nhau': Chuẩn bị (không phải giai đoạn chính thức), cam kết trước, cam kết và quyết định. 17 Cấu trúc luồng: các nút khác bỏ phiếu cho một thông báo và người dẫn đầu kết hợp các phiếu bầu và phát chúng đến các nút khác. Các giai đoạn này có thể được biểu diễn đồng nhất và phân chia



Trở thành một nút xác thực

Mọi bên liên quan cũng có thể là một ứng cử viên xác nhận. Các bên liên quan phải có ít nhất 300.000 Kiva Coin trong ví của họ. Các bước sau đây mô tả cách bên liên quan K trở thành người xác nhận:

- K gửi 300.000 Kiva Coin vào ví K's Kiva, Số tiền này sẽ được đốt trực tiếp làm phí xác thực.
- K tạo giao dịch đề xuất để trở thành nút xác thực
- Nếu giao dịch của K là hợp lệ, K sẽ được liệt kê là ứng cử viên xác thực và xếp hàng chờ quá trình bỏ phiếu
- Các bên liên quan khác có thể xem danh sách các nút xác thực trong nhóm và bắt đầu bỏ phiếu cho các nút đáng tin cậy. Quyền biểu quyết phụ thuộc vào tổng số token mà các bên liên quan có.
- 33 ứng cử viên nút xác thực nhận được nhiều phiếu bầu nhất sẽ trở thành nút xác thực chính thức. Phần còn lại sẽ vẫn ở trong nhóm cho quá trình bỏ phiếu tiếp theo. Trong trường hợp một nút xác thực không tạo ra một khối kịp thời, các ứng viên đang chờ cũng có thể trở thành nút xác thực đầy đủ.

11. Mô hình khuyến khích

Để thu hút nhiều người hơn đến với Kivachain, mô hình khuyến khích sau đã được tạo ra:

18 Đối với mỗi kỷ nguyên, một trạm kiểm soát được tạo. Người xác thực khi kết thúc lặp lại kỷ nguyên sẽ chịu trách nhiệm tính toán phần thưởng mạng. Token cho phần thưởng mạng trong một năm sẽ là ~ 1% tổng số mã thông báo (10 triệu mã thông báo). Nó bằng với tỷ lệ lạm phát hàng năm là 1%. Tổng phần thưởng mã thông báo cho mỗi kỷ nguyên là Kỷ nguyên mã thông báo thưởng = $TBolokceknppeerryyeeaarr$ x Khối mỗi kỷ nguyên = (60 * 36,00 * 0204.0 * 30605) / 3 x7200 = 2055 mã thông báo Mã thông báo phần thưởng mạng được chia thành hai phần: 40% đầu tiên chuyển trực tiếp đến các nút xác thực đang hoạt động và 60% còn lại sẽ được chia sẻ giữa các bên liên quan đã bỏ phiếu cho các nút xác thực.

Đặc điểm kỹ thuật của Kivachain

- Thời gian chặn: 3 giây
- Giao dịch mỗi giây (TPS): 50.000 giao dịch

- Xác nhận khối (tính cuối cùng) 1 / s
- Mã thông báo gốc: Kivachain Coin
- Tổng số mã thông báo: 1.000.000.000 (Một tỷ mã thông báo)
- Phí giao dịch: Dựa trên độ phức tạp tính toán. mã thông báo chuyển thông thường có giá 0,0001 mã thông báo
- Thuật toán đồng thuận: DPoS-HotStuff
- Số nút xác thực: 33 nút
- Ngôn ngữ hợp đồng thông minh: Solidity. (Javascript và GoLang trong tương lai)
- Thuật toán chữ ký số: ECDSA
- Đa chuỗi: Có
- Giao tiếp chuỗi chéo: Có

Thông số kỹ thuật	**Bitcoin**	**Ethereum**	**IOTA**	**Konla**	**Kivachain**
Thuật toán đồng thuận	PoW	PoW	Tangle	DPOS-BFT	DPOS and Hotstuff
Số lượng giao dịch mỗi giây	3	15	300	hàng nghìn	50 nghìn
Thời gian chặn (giây)	600	15	NA	1	3
Thời gian xác thực (giây)	3300	150	NA	1	1
Hợp đồng thông minh	x	✔	x	✔	✔
Đa chuỗi	x	x	x	x	✔
Giao tiếp chuỗi chéo	x	x	x	x	✔
Nút xác nhận	x	x	x		✔

12. Tự trị phi tập trung

Mô hình (DAO)

DAO là gì?

Một mô hình tự trị phi tập trung (DAO) là một mô hình tổ chức cụ thể về chuỗi khối nhằm giải quyết một thách thức cố hữu hiện nay trong hầu hết các ngành và tổ chức:

Vấn đề giữa người làm chủ và người thừa hành. Bất cứ khi nào một hệ thống được cấu trúc theo cách mà một cá nhân hoặc tổ chức ("tác nhân") có khả năng đưa ra quyết định hoặc thực hiện các hành động thay mặt cho 20 cá nhân hoặc tổ chức khác ("chủ thể"), thì sẽ có rủi ro cố hữu trong sự khác biệt mục tiêu, ưu tiên hoặc quyền truy cập thông tin quan trọng của các bên tương ứng. Đây là vấn đề giữa người chủ và người thừa hành và điều đó có nghĩa là người đại diện có thể có động cơ để hành động vì lợi ích riêng của mình, ngay cả khi người đại diện được lựa chọn để đưa ra quyết định thay mặt cho lợi ích của người làm chủ.

Hiện tại, vấn đề này là một thách thức phổ biến ảnh hưởng đến nhiều tổ chức công và tư. Nhằm mục đích giải quyết vấn đề này bằng cách giảm hoặc bỏ qua sự can thiệp phân cấp của con người hoặc điều phối tập trung, các DAO thường được gọi là hệ thống "không tin cậy" . Bằng cách đảm bảo rằng các cấu trúc khuyến khích và luồng thông tin trong một tổ chức được điều chỉnh phù hợp theo định dạng hệ thống hóa, các DAO đóng vai trò trung tâm trong việc giảm thiểu các vấn đề điển hình liên quan đến cổ đông và người đại diện. Sự liên kết của các động cơ là một khái niệm xác định của các giao thức blockchain và các DAO áp dụng logic tương tự cho các tổ chức và quản trị. Một DAO được thực thi đúng cách sẽ điều chỉnh các động cơ của các bên liên quan - từ người sáng lập, đến chủ sở hữu mã thông báo, người dùng và cộng đồng nói chung - trong việc quản lý một tổ chức hoặc nền tảng phi tập trung. Những tác động tiềm tàng của việc triển khai DAO trên quy mô rộng là rất lớn, cũng như những thách thức trong thế giới thực của việc áp dụng hiệu quả công nghệ cho phép một DAO.

DAO	TỔ CHỨC TRUYỀN THỐNG
Thường là ngang bằng, và được dân chủ hóa hoàn toàn.	Thường có thứ bậc.
Biểu quyết theo yêu cầu của các thành viên cho bất kỳ các thay đổi	Tùy thuộc vào từng mô hình, các thay đổi có thể được yêu cầu từ một

sẽ được thực hiện	bên duy nhất hoặc có thể đưa ra biểu quyết.
Phiếu bầu được kiểm tra và kết quả được thực hiện tự động mà không cần trung gian đáng tin cậy.	Nếu được phép bỏ phiếu, các phiếu bầu sẽ được kiểm tra nội bộ và kết quả của việc bỏ phiếu phải được xử lý theo cách thủ công
Các dịch vụ cung cấp được xử lý tự động theo cách phi tập trung (ví dụ: phân phối quỹ từ thiện).	Yêu cầu con người xử lý, hoặc tự động hóa được điều khiển tập trung, dễ bị thao túng.
Tất cả các hoạt động là minh bạch và hoàn toàn công khai.	Hoạt động thường là riêng tư và hạn chế công khai

DAO hoạt động như thế nào?

Trong khi các cơ chế cơ bản cụ thể cung cấp năng lượng cho DAO khác nhau trên các dự án blockchain khác nhau, có một số giai đoạn chung mà DAO phải trải qua để khởi chạy một cách bền vững.

Cách thức:

● Thiết lập hợp đồng thông minh: Trước khi một DAO có thể được triển khai, các quy tắc cơ bản phải được xác định và mã hóa trong một loạt các hợp đồng thông minh. Do những thay đổi trong tương lai đối với quy trình hoạt động, hệ thống quản trị và cơ cấu khuyến khích của DAO sẽ cần được bỏ phiếu để có hiệu lực, giai đoạn này được cho là bước quan trọng nhất để tạo ra một DAO bền vững và thực sự tự chủ, vì bất kỳ sai lầm ban đầu nào hoặc những chi tiết bị bỏ qua có thể gây mất ổn định cho dự án.

● Tài trợ: Sau khi người tạo DAO đã thiết lập các hợp đồng thông minh quản lý của nó, DAO cần nhận được tài trợ để hoạt động. Các hợp đồng thông minh của DAO phải bao gồm việc tạo và phân phối một số dạng tài sản nội bộ, chẳng hạn như mã thông báo gốc có thể được sử dụng bởi DAO, được sử dụng trong các cơ chế bỏ phiếu hoặc được sử dụng để khuyến khích các hoạt động nhất định. Từ đó, các cá nhân hoặc tổ chức quan tâm đến việc tham gia vào sự phát triển của DAO có thể mua hoặc có được mã thông báo gốc, thường dẫn đến việc có được quyền biểu quyết.

● Triển khai: Sau khi một DAO nhận đủ kinh phí để triển khai, tất cả các quyết định của DAO được đưa ra thông qua một cuộc bỏ phiếu đồng

thuận. Do đó, tất cả chủ sở hữu mã thông báo trở thành các bên liên quan có thể đưa ra các đề xuất liên quan đến tương lai của DAO và cách sử dụng tiền của DAO. Nếu chính sách phân phối mã thông báo của DAO và cơ chế đồng thuận được xác định trong kiến trúc hợp đồng thông minh cơ bản của nó được thiết kế tốt, thì DAO các bên liên quan đương nhiên sẽ làm việc hướng tới kết quả có lợi nhất cho toàn bộ mạng DAO

Do đó, tổ chức DAO có thể hoạt động độc lập với những người tạo ra nó hoặc bất kỳ cơ quan trung ương nào khác. Vì DAO là mã nguồn mở, tất cả các quy tắc, giao dịch và hoạt động của chúng đều được ghi lại trên blockchain và có thể được xem xét bởi bất kỳ ai, điều này thường đảm bảo tính minh bạch và bất biến hoàn toàn. Nói tóm lại, các bên liên quan của DAO được ràng buộc với nhau bởi một mục tiêu chung, mà họ sẽ bỏ phiếu để tiến tới thông qua việc theo đuổi các khuyến khích mạng cụ thể được xác định bởi các chính sách đồng thuận cơ bản của DAO.