



KARDIACHAIN

Blockchain of Blockchains

WORLD'S FIRST NON-INVASIVE &
FULLY INTEROPERABLE BLOCKCHAIN PLATFORM



TỔNG QUAN

Công nghệ chuỗi khối (Blockchain) cung cấp tính Phi tập trung (decentralization) và độ minh bạch chưa từng thấy từ trước tới nay, cùng với đó là sự cân bằng (Trade-off) giữa Hiệu suất hoạt động (Performance) và khả năng hoạt động đa kết nối (inter-connectivity). Trong một tương lai không xa, chúng tôi tin rằng những giải pháp mà Blockchain cung cấp, đặc biệt là Hợp đồng thông minh (smart contract), sẽ giúp con người đạt được các thỏa thuận và hợp tác một cách đơn giản mà không yêu cầu sự tin tưởng lẫn nhau, áp dụng trong tất cả các hoạt động hằng ngày. Tuy nhiên, các cách tiếp cận hiện nay nhằm đạt được mục tiêu trên có xu hướng thay thế và loại bỏ công nghệ của các dự án chuỗi khối khác trên thế giới hoặc yêu cầu các chuỗi khối này phải thay đổi theo quy chuẩn nếu muốn tham gia vào hệ sinh thái chung. KardiaChain tin vào triết lý “Hòa nhập nhưng không hòa tan”, tập trung xây dựng một giải pháp đơn giản và dễ sử dụng cho cả người dùng lẫn các nhà phát triển. KardiaChain phát triển một giải pháp có tính Không Can Thiệp (Non-invasive), được gọi là Nút Mạng Kép (Dual Master Node) (gọi tắt là Nút Kép), cho phép sự tương tác giữa các blockchain hiện nay cũng như giữa các blockchain trong tương lai. Mục tiêu của chúng tôi là tạo ra một hệ sinh thái đồng bộ, nơi mà các nhà phát triển có thể dễ dàng tạo ra những Hợp đồng thông minh (Smart contract) có khả năng hoạt động trên nhiều chuỗi khối khác nhau, nhằm giảm thiểu tối đa chi phí, giảm sự tắc nghẽn của hệ thống, thông qua sự giao tiếp giữa các Smart Contract trên nhiều hệ thống chuỗi khối, trong môi trường an toàn, không yêu cầu sự tin tưởng.



I. Triết lý của KardiaChain

KardiaChain tin rằng con người sẽ sớm tiến đến thời điểm khi những giải pháp mà công nghệ Blockchain cung cấp, đặc biệt là Smart contract, sẽ giúp con người dễ dàng tiến tới những thỏa thuận trong mọi khía cạnh của cuộc sống mà không yêu cầu sự tin tưởng lẫn nhau.

Không giống với cách tiếp cận hiện nay của nhiều dự án chuỗi khối là thay thế hoàn toàn các chuỗi khối cũ và trở thành một hệ thống tích hợp cho tất cả các mục đích sử dụng, KardiaChain thấy rằng, cách thức hoạt động trên thực tế sẽ đi theo một chiều hướng rất khác. Giống như internet là một mạng lưới rộng lớn gồm nhiều các mạng lưới bên trong, tầm nhìn của chúng tôi về một internet của blockchain là sự liên kết giữa rất nhiều những blockchain mở (public/permissionless) và những blockchain tư nhân (private/consortium). Mỗi chuỗi khối có một cấu trúc đặc trưng nhằm phục vụ những mục đích cụ thể, sự độc đáo của từng chuỗi khối này nên được tận dụng triệt để.

Vì vậy, nên có một hệ sinh thái thông minh có khả năng tận dụng và tối ưu hóa những điểm mạnh của các hệ thống chuỗi khối nhằm giải quyết những vấn đề trong khả năng hoạt động diện rộng (discoverability) hay sự biệt lập (isolation) giữa các blockchain. Chúng tôi coi hệ sinh thái thông minh này như một cá thể, trong đó mỗi hệ thống chuỗi khối là một bộ phận, và KardiaChain là con tim của hệ thống nhằm hỗ trợ dòng chảy của máu (chính là các giao dịch) tới từng bộ phận với tốc độ tùy theo nhu cầu sử dụng.

Trong khi có rất nhiều những đề xuất nhằm giải quyết vấn đề tương tác giữa các chuỗi khối, chúng đều yêu cầu những thay đổi căn bản trong các hệ thống chuỗi khối hoặc đòi hỏi các hệ thống này phải tích hợp với một khuôn mẫu nhất định.

Ngược lại, cách tiếp cận độc đáo của KardiaChain có tính khả dụng, KardiaChain có thể xây dựng liên kết giữa các chuỗi khối một cách đơn giản và nhanh chóng mà không yêu cầu sự thay đổi từ các chuỗi khối thành viên. KardiaChain theo đuổi cách tiếp cận “Hòa nhập nhưng không hòa tan” tập trung vào tối giản hóa, đơn giản hóa cho người dùng và các nhà phát triển. Chúng tôi tự hào khi giới thiệu hệ sinh thái thông minh liên chuỗi khối của KardiaChain, một giải pháp mà chúng tôi đang hoàn thiện từng ngày để đưa công nghệ blockchain tới gần hơn với người dùng phổ thông.



II. Nền Tảng

A. Chuỗi đơn

Công nghệ chuỗi khối (Blockchain) cung cấp tính Phi tập trung (Decentralization) và độ minh bạch chưa từng thấy từ trước tới nay, cùng với đó là sự cân bằng (Trade-off) giữa Hiệu suất hoạt động (Performance) và khả năng hoạt động đa kết nối (Inter-connectivity). Đối với hầu hết các chuỗi đơn, mục tiêu chính là tăng khả năng mở rộng của hệ thống (Scalability), hoặc gia tăng Hiệu suất hoạt động với một tiêu chuẩn được đem ra so sánh là tốc độ xử lý giao dịch trong vòng 1 giây (TPS). Một trong những cách thức phổ biến được sử dụng hiện nay đó là phân mảnh (Sharding) nhằm chia hệ thống chuỗi thành nhiều mảnh nhỏ (chuỗi phụ) và xử lý cùng lúc các giao dịch trên từng mảnh/chuỗi đó, phương pháp này hứa hẹn đạt được tốc độ xử lý lên tới hàng nghìn, hàng triệu giao dịch trong 1 giây. Tuy nhiên, kể cả dựa trên những ước tính về mặt lý thuyết nêu trên, không có một dự án chuỗi khối đơn lẻ nào có khả năng đạt tới tốc độ và Hiệu suất cần thiết để đưa blockchain tiếp cận người dùng phổ thông. Lấy ví dụ, những tương tác chính của chúng ta trên Facebook cần tới tốc độ xử lý 16,000 giao dịch 1 giây, vì trong mỗi phút, có 510,000 lượt bình luận, 293,000 trạng thái mới được cập nhật và 136,000 bức ảnh được đăng tải. Instagram có 4 tỷ lượt thích trong một ngày đồng nghĩa với 46,000 lượt thích (tốc độ xử lý giao dịch) trong vòng 1 giây. Trong trường hợp của Youtube, 1 triệu giờ video được xem trong 1 ngày, có nghĩa là gần 7 triệu giao dịch được xử lý trong vòng 1 giây (giả sử một video thông tin được truy cập mỗi 6 giây trong một lần truy cập Youtube của người dùng).

Một lý do cản trở việc tốc độ xử lý giao dịch không đạt tiêu chuẩn để công nghệ chuỗi khối có thể tiếp cận người dùng phổ thông đó là các chuỗi đơn thường thiếu liên kết, chúng không thể giao tiếp được với nhau, vì vậy, quá trình xử lý không thể chạy trên nhiều chuỗi khác nhau. Sự thiếu liên kết này ngăn cản các doanh nghiệp tìm được một giải pháp đảm bảo trên nền tảng blockchain cho các vấn đề của mình. Ví dụ, có rất nhiều chuỗi hỗ trợ hệ thống Hợp đồng thông minh, mỗi chuỗi lại có Hiệu suất xử lý và chức năng xử lý riêng. Điều đó nghĩa là sẽ khó có khả năng để một chuỗi đơn nhất định có thể xử lý tất cả các vấn đề mà doanh nghiệp gặp phải. Không có một giải pháp riêng lẻ nào phù hợp cho tất cả các ứng dụng, dẫn tới khó khăn trong việc xây dựng hệ thống Hợp đồng thông minh hoạt động trên nhiều chuỗi khối khác nhau.



B. Các chuỗi khối liên kết

1. Khối hộp đa chiều

Nếu chúng ta nghĩ một chuỗi đơn như là một chiếc máy tính hoặc một mạng cục bộ, Hiệu suất xử lý sẽ lớn hơn khi nhiều máy tính như trên được kết nối với nhau và cùng chia sẻ yêu cầu xử lý dữ liệu, thay vì sử dụng chỉ 1 siêu máy tính có tốc độ xử lý cao. Ở đây, chúng tôi sử dụng khái niệm khối hình hộp đa chiều để hình dung dễ dàng hơn các cách tiếp cận hiện nay của bài toán mở rộng một chuỗi khối.

Trục X = nhân bản theo chiều ngang = Định hướng giao dịch: dữ liệu được lưu trữ trên nhiều nút (nodes) cùng lúc nhằm giảm thiểu ùn tắc.

Trục Y = mở rộng chức năng = Các blockchain khác nhau xử lý các yêu cầu khác nhau: giải pháp được chia ra thành từng yêu cầu riêng biệt, sử dụng những điểm dữ liệu riêng. Do đó, sự ùn tắc trên một chuỗi nhất định sẽ không làm ảnh hưởng tới khả năng xử lý giao dịch của các chuỗi khác.

Trục Z = Phân chia dữ liệu = chia sẻ nhu cầu xử lý dữ liệu giữa các bộ phận của chuỗi (ví dụ như thuật toán phân mảnh): chạy các bản sao giống nhau của code lên nhiều nút cùng một lúc nhằm chia sẻ khối lượng công việc.

Hiện nay giải pháp đang được rất nhiều chuỗi đơn theo đuổi đó là tập trung vào mở rộng trục Z bằng cách áp dụng thuật toán phân mảnh (Sharding). Chúng tôi hướng đến sự mở rộng trên cả 3 chiều, tập trung nhiều vào trục X và Y cùng với đó là tận dụng sharding của những hệ thống chuỗi khối trong hệ sinh thái. Nhờ có khả năng liên kết, các yêu cầu giống nhau được chia sẻ giữa các hệ thống chuỗi khối để đạt được sự mở rộng theo trục X. Đối với mở rộng theo trục Y, chúng tôi có thể chia nhỏ một thao tác thành những thao tác nhỏ hơn và chạy trên nhiều chuỗi khối khác nhau. Đây là sự vượt trội mà khả năng liên kết của KardiaChain mang lại.

2. Các nghiên cứu liên quan

Trong khi nhiều giải pháp đã được thử nghiệm nhằm phát triển khả năng hoạt động liên chuỗi giữa các blockchain, mỗi giải pháp lại có một yêu cầu thay đổi riêng cho các chuỗi khối để tích hợp với quy chuẩn chung, dẫn tới yêu cầu có sự cập nhật phiên bản của chuỗi khối (fork), có 2 loại fork là Phân tách cứng (hard-fork), khi phiên bản chuỗi khối với cập nhật mới không còn tích hợp với phiên bản chuỗi khối cũ hoặc Phân tách mềm (soft-fork) khi phiên bản chuỗi khối mới vẫn có thể tích hợp với phiên bản chuỗi khối cũ. Cố gắng cập nhật những thay đổi trên một chuỗi khối có thể dẫn tới 2 hệ lụy chính đó là:



- 1) Cần tới những cập nhật phiên bản bắt buộc và sự ra đời của một chuỗi khối mới dựa trên lịch sử của chuỗi khối cũ nhằm đáp ứng các yêu cầu tích hợp;
- 2) Các vấn đề liên quan tới bảo mật có thể xảy ra khi cố gắng thay đổi cấu trúc của một hệ thống chuỗi khối như miêu tả ở trên.

Sau đây, chúng ta sẽ phân tích một số hướng tiếp cận phổ biến hiện nay đang được sử dụng nhằm phát triển khả năng giao dịch liên chuỗi (cross-chain)

a. Chuỗi phụ (Sidechain)

Chuỗi phụ là một hệ thống chuỗi chạy song song với hệ thống chuỗi chính, được sử dụng như một cách để gia tăng các chức năng của chuỗi chính thông qua khả năng liên kết lẫn nhau của chuỗi. Hệ thống này cho phép trao đổi và chuyển đổi đồng tiền mã hóa một cách phi tập trung giữa hai chuỗi khối với nhau. Nói một cách khác, bạn có thể chuyển đồng tiền mã hóa của bạn tới chuỗi phụ và sau đó chuyển lại về chuỗi chính.

Vấn đề mà chuỗi phụ hay gặp phải đó là tài sản mà bạn muốn chuyển tới chuỗi phụ từ chuỗi chính (và ngược lại) sẽ bị khóa trong một khoảng thời gian nhất định gọi là thời gian thử thách (contestant period) trước khi có thể được luân chuyển. Mặc dù ý tưởng sử dụng chuỗi phụ đã được đề cập từ năm 2014, nhưng cho tới nay, vẫn chưa có nhiều ứng dụng cho thấy phương án này mang tính khả thi.

b. Phân lớp truyền tin (Message layer)

Phân lớp truyền tin được thiết kế như một bộ phận trung gian tiếp nhận dữ liệu từ các chuỗi ngoài. Việc coi mỗi giao dịch như một tin nhắn yêu cầu hệ thống phải tạo ra thêm một phân lớp riêng để sàng lọc và sắp xếp những tập tin này theo thứ tự. Nói một cách đơn giản, hệ thống sẽ phải sàng lọc tất cả những tin nhắn này trước khi ghi chúng vào sổ cái. Quá trình này có thể tiêu tốn một phần Hiệu suất, dẫn tới những vấn đề về Hiệu suất xử lý tổng của hệ thống. Theo chúng tôi, chúng ta có thể trực tiếp chọn lọc những dữ liệu quan trọng từ chuỗi ngoài thông qua khả năng không bị thay đổi (immutability) của chuỗi khối, qua đó, loại bỏ phân lớp mà có lẽ là không cần thiết này.

c. Mô-đun nguồn / Mô-đun kết nối / Mô-đun chuyển đổi (Hub / Connector / Adaptor)

Mô-đun nguồn được thiết kế để hoạt động như một kênh liên lạc thông tin giữa các chuỗi khối thành viên. Thông qua nó, những chuỗi này có thể tương tác với nhau nhằm gửi/nhận và trao đổi tài sản. Vấn đề then chốt mà giải pháp này vấp phải đó là mỗi mô-đun nguồn sẽ yêu cầu những chuỗi thành viên phải đồng bộ hóa để có thể tương tác với các



chuỗi thành viên khác, nghĩa là những chuỗi khối hiện tại sẽ phải cập nhật để tham gia hệ thống này. Nói một cách khác, mô-đun nguồn không tích hợp với các hệ thống chuỗi, mà ngược lại, yêu cầu các hệ thống chuỗi tích hợp theo mình. Cách tiếp cận này, theo nhận định của chúng tôi, là một ví dụ đi ngược lại với định nghĩa về hoạt động liên chuỗi khối và khả năng áp dụng thực tiễn.

3. Cách tiếp cận “Hòa nhập nhưng không hòa tan” của KardiaChain

Nói một cách đơn giản, chúng tôi tích hợp theo bạn. Mục tiêu lớn nhất của chúng tôi là cung cấp một hệ thống gốc, sẵn sàng để đi vào hoạt động và đảm bảo những yêu cầu như:

- Tích hợp với những hệ thống chuỗi thành viên và cho phép quá trình hoạt động xuyên suốt từ thiết kế giải pháp đến ứng dụng thực tế.
- Giữ nguyên những điểm mạnh nhất của các chuỗi thành viên và đặc biệt hơn là không hề có sự thay đổi nào trong mức độ an toàn hay cơ chế đồng thuận (consensus) của các chuỗi này.
- Minh bạch và rõ ràng cho những nhà thiết kế Dapp, KardiaChain sẽ cùng lúc xử lý các hoạt động liên chuỗi, đồng thời vẫn cung cấp cho nhà phát triển khả năng áp dụng và xây dựng theo ý tưởng riêng của họ.

III. GIẢI PHÁP CỦA KARDIACHAIN

(Đang chờ được cấp bằng sáng chế)

Nhằm giải quyết những thách thức trong việc tương tác và sau đó là vấn đề mở rộng hệ thống chuỗi khối, KardiaChain hướng đến cung cấp một cơ sở hạ tầng đồng bộ mà ở đó các ứng dụng có thể chạy trên nhiều chuỗi khối khác nhau thông qua khả năng liên kết chuỗi mà vẫn đảm bảo được sự đơn giản trong xây dựng cho các nhà phát triển. Một trong những điểm nổi bật của KardiaChain mà chưa từng xuất hiện trước đây là cho phép người dùng kích hoạt giao dịch trên một chuỗi khối nhưng dẫn tới kết quả của giao dịch được xuất hiện trên một chuỗi khối khác.

KardiaChain là một hệ thống chuỗi khối liên kết các hệ thống chuỗi và các ứng dụng trên cả hệ sinh thái chuỗi khối. Mục tiêu của dự án là tạo ra một hệ sinh thái đồng bộ có khả năng tổng hợp và sử dụng những điểm mạnh nhất từ những chuỗi khối khác, để mở đường cho xu hướng sử dụng công nghệ blockchain trên diện rộng trong thời gian không xa. Công cụ chính mà KardiaChain sử dụng là Nút Mạng Kép (viết tắt là Nút Kép) bao gồm ba bộ phận chính: Mô-đun Dịch, Mô-đun Dẫn và Mô-đun Tổng Hợp (Translator, Router, and Aggregator). Những công cụ này cung cấp tính thực tiễn, không xâm lấn (non-invasive)



cho kết nối liên chuỗi được diễn ra trong môi trường an toàn và phi tập trung, qua đó giảm giá thành sử dụng và tăng tốc độ xử lý.

A. Ưu điểm công nghệ

Giải pháp của Kardia cung cấp các bước tiến trong công nghệ như:

- Cách tiếp cận bằng thuật toán trong việc định hướng các giao dịch nhằm giảm thiểu chi phí và tăng tốc độ xử lý một cách tối đa
- Hệ thống hợp đồng thông minh đồng bộ về thuật ngữ nhằm gia tăng khả năng phát triển rộng rãi
- Giải pháp không xâm lấn giữa các hệ thống chuỗi sẽ cung cấp khả năng tương tác ngược và không yêu cầu các chuỗi khác phải thay đổi nếu muốn tương tác trong hệ sinh thái của KardiaChain
- Ứng dụng thực tiễn hiệu quả
- An toàn và phi tập trung

B. Những bộ phận quan trọng

Nút Kép có khả năng truy cập lần lượt tới dữ liệu sổ cái của hai hệ thống chuỗi (KardiaChain và một chuỗi tùy chọn). Nút Kép này có thể nhận các giao dịch từ hệ thống chuỗi ngoài và cập nhật nó vào KardiaChain một cách an toàn mà không cần phải thay đổi bất cứ gì từ cả hai chuỗi. Nút Kép đạt được tính phi tập trung vì ai cũng có thể chạy được nó (không phân quyền/permissionless) và có một cơ chế đồng thuận giữa các Nút Kép để xác nhận dữ liệu của mỗi hệ thống chuỗi. Nút Kép rất an toàn vì dữ liệu của tất cả các giao dịch giữa liên chuỗi đến hoặc đi từ KardiaChain không thể bị giả mạo, chúng được bảo vệ bởi các tính năng đa chữ ký ví dụ như hệ thống chữ ký mã hóa Schnorr.

Mô-đun Phiên Dịch sẽ tối ưu hóa hệ thống hợp đồng thông minh đồng nhất các loại ngôn ngữ của Kardia (Kardia unified Smart contract language KSML) để phá bỏ những rào cản về ngôn ngữ lập trình giữa các loại hợp đồng thông minh trên những chuỗi khác nhau, nhằm thành lập một sự “am hiểu chung” giữa KardiaChain và các hệ thống chuỗi ngoài.

Mô-đun Điều phối sẽ quyết định hệ thống chuỗi nào là tốt nhất để dịch chuyển những yêu cầu của người dùng tới chuỗi đó và xử lý, những thông số mà Mô-đun Điều Phối dựa vào để định hướng giao dịch có thể kể tới Khả năng thực hiện giao dịch của hệ thống trong một thời điểm cụ thể, phí giao dịch, thời gian hoàn thành giao dịch và dung lượng.

Mô-đun Tổng Hợp sẽ tổng hợp các cập nhật từ những chuỗi thành viên để giảm sức ép



lên KardiaChain, có thể giảm từ một khối hoặc một giao dịch trên Kardia. Sự phối hợp giữa những bộ phận trên sẽ tạo ra tiềm năng vô hạn cho hệ thống chuỗi khối và xây dựng một nền tảng vững chắc cho công nghệ chuỗi khối được áp dụng trên toàn cầu, kể cả trong những ứng dụng hằng ngày.

Luồng hoạt động của một nút kép có thể được chia thành các bước sau:

- Bước 0: người dùng kích hoạt giao dịch TX(r(i)) với i=1,2,3 nhằm sử dụng hợp đồng thông minh SMC_A
- Bước 1,2 Mô-đun Điều Phối và Mô-đun Phiên Dịch sẽ định vị giao dịch và như xử lý nó
- Bước 3 Nút Kép thực thi lệnh Func_call(j) với j=1,2,3 nhằm tới các hệ thống chuỗi ngoài
- Bước 4 Kết quả TX(u(l)) với l=1,2,3 được chuyển tới từ những chuỗi ngoài
- Bước 5 Nút Kép chuyển đổi những kết quả TX(u(l)) về lại với quy chuẩn của các hệ thống chuỗi ngoài
- Bước 6,7 Mô-đun Tổng Hợp và Mô-đun Phiên Dịch sẽ thực hiện một giao dịch duy nhất TX(k)=[value:(1,2,3)]
- Bước 8 Các thay đổi (1,2,3) được thực hiện ở SMC_A và được ghi lại vào sổ cái

Như bạn đã thấy, cách xử lý mới của Kardia cho phép chúng ta tổng hợp Hiệu suất thực hiện giao dịch của tất cả các chuỗi thành viên và tái định nghĩa khái niệm về tốc độ xử lý giao dịch trong 1 giây (TPS)

$$KardiaTPS = \sum_{i=0}^n K_i + [\min(R, E, Kt) \times (1 - \frac{1}{t})]$$

Ki: Hiệu suất xử lý giao dịch sẵn có mà Kardia có thể thực hiện (i=0)

R: Hiệu suất giao dịch thu nhận được từ các chuỗi thành viên (i=1,...,n)

E: Khả năng định tuyến của các khối kép

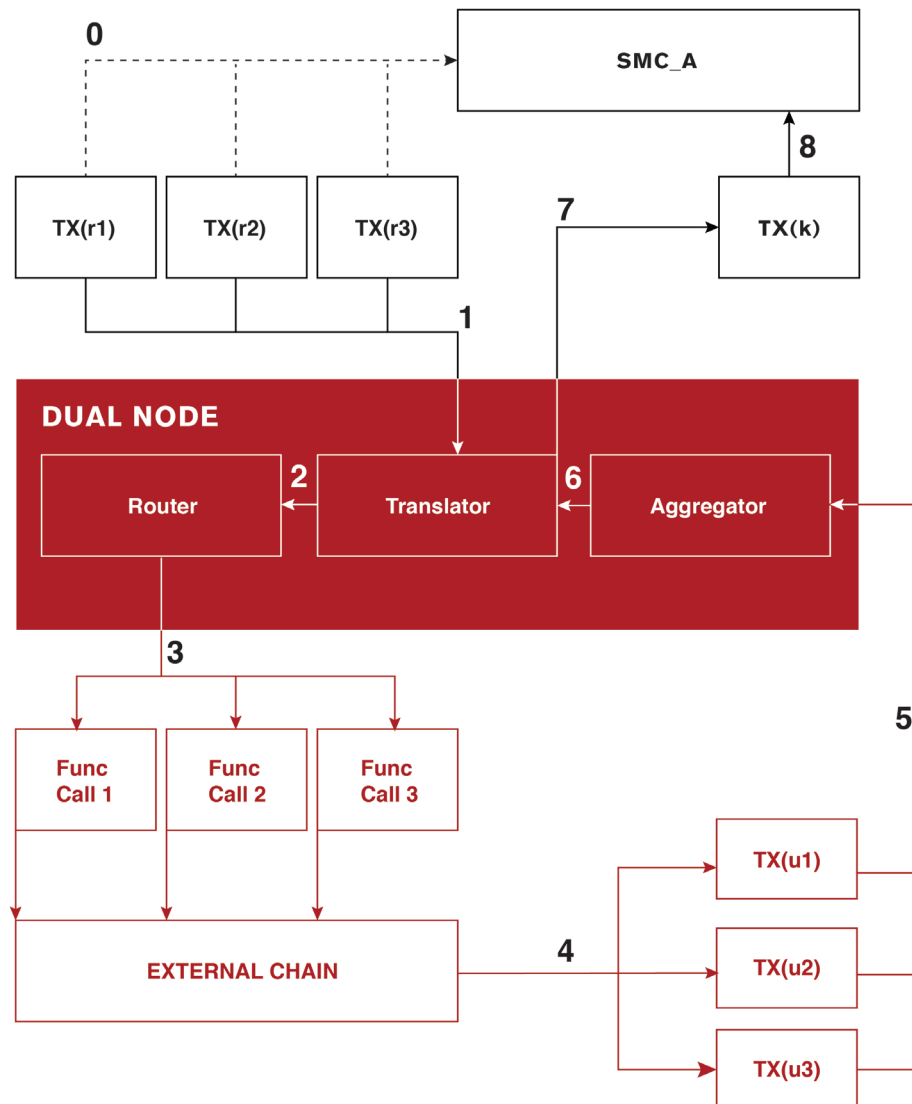
t: Tỷ lệ tổ hợp của khối

Lưu ý rằng, t sẽ thay đổi khi ngày càng nhiều chuỗi được hỗ trợ bởi Kardia, cũng như dựa vào Block_Size và Block_Time của từng chuỗi. Cụ thể, t nằm trong khoảng từ 1 đến giá trị tuyệt đối.

$$t_{max} = \frac{\sum_{i=1}^n (tps)_i}{\sum_{i=1}^n \frac{1}{Block_Time_i}}$$

(1...) là tổ hợp của tất cả các chuỗi thành viên

*t=1 là một trường hợp đặc biệt khi chỉ có 1 giao dịch/lệnh được phát hiện và xử lý, dẫn tới 1 cập nhật duy nhất lên Kardia, vì vậy tỉ lệ tổ hợp là 1





IV. CÔNG NGHỆ CỦA KARDIACHAIN

A. Các bộ phận của Nút Mạng

Để miêu tả rõ hơn, chúng tôi phân chia cấu trúc của một nút ra thành 3 bộ phận, như cấu trúc bộ phận sinh học người đó là: Trái Tim, Động Mạch và các Ven. Nút Kép trực tiếp sử dụng cả 3 bộ phận này duy trì sự kết nối liên chuỗi. Trái Tim có chức năng lưu trữ giao dịch và gửi chúng tới những chuỗi khối thành viên thông qua Động Mạch, những giao dịch này sẽ quay trở lại Kardia qua hệ thống Ven dẫn. Nếu vì một lý do nào đó, một Nút đưa ra lựa chọn sẽ không tham gia vào hệ sinh thái kết nối liên chuỗi, nó sẽ chỉ sử dụng bộ phận Trái Tim và trở thành một Nút Tiêu Chuẩn có khả năng xử lý các giao dịch ở chuỗi nguồn.

1. Trái tim

a) Bộ Công Cụ phát triển của Kardia

Mục tiêu của Kardia là đơn giản hóa quá trình học hỏi cấu trúc hợp đồng thông minh của các hệ thống chuỗi khác, chúng tôi sẽ cung cấp một tập hợp những UI, API and SDK nhằm đơn giản hóa cấu trúc của hợp đồng thông minh Kardia. Bộ công cụ này được biết tới như một hệ thống dẫn sẽ giữ cho Trái Tim hoạt động liên tục.

- Hệ thống UI thân thiện với người dùng sẽ cung cấp khuôn mẫu để xây dựng một hợp đồng thông minh của Kardia. Khuôn mẫu này sẽ giúp các nhà phát triển có ít kinh nghiệm hoặc sở hữu kiến thức chưa sâu về ngôn ngữ lập trình của hợp đồng thông minh có thể thay đổi nhiều hơn những chi tiết của hợp đồng theo ý mình.
- API hiệu suất cao sẽ trực tiếp xây dựng những hợp đồng thông minh Kardia phức tạp hơn. Công cụ này hướng tới những nhà phát triển chuyên nghiệp hơn, cho phép họ ứng dụng bất cứ một loại logic nào lên nhiều chuỗi cùng lúc.
- SDK Hiệu suất lớn cho phép các nhà thiết kế Dapp tự do tìm hiểu và điều chỉnh tất cả các chi tiết trong hợp đồng thông minh Kardia. SDK cho phép các nhà lập trình có toàn bộ quyền quản lý đối với tất cả những hoạt động liên chuỗi của hợp đồng thông minh Kardia: từ khả năng tạo ra các hợp đồng phụ ở chuỗi ngoài, tới tùy chỉnh phương thức cập nhật thông tin mới, tất cả sẽ do nhà lập trình chọn lựa.

b) Máy ảo của Kardia (KVM)

Máy ảo Kardia là một bản nâng cấp của Máy ảo Ethereum, tích hợp thêm các chức năng hoạt động liên chuỗi. Hợp đồng thông minh chạy trên Máy ảo Kardia có thể xử lý những giao dịch ngoài từ các chuỗi thành viên và ghi chúng vào sổ cái mà không cần thay



đổi cơ chế đồng thuận của Kardia. Máy ảo Kardia duy trì hai hệ thống thu phí, từ những giao dịch trên chuỗi khối chính và những giao dịch liên chuỗi.

Một cơ chế thu phí phù hợp sẽ được áp dụng cho các giao dịch liên chuỗi để khuyến khích các nút thành viên tích cực hơn trong việc xử lý các giao dịch liên chuỗi nhằm đảm bảo sự hoạt động trơn tru của cả hệ thống.

Máy ảo Kardia cũng hỗ trợ một bộ công cụ đặc biệt giúp quản lý giao dịch liên chuỗi liên quan tới quá trình xử lý và tổng hợp các cập nhật từ các chuỗi ngoài.

c) Trí tuệ của hệ sinh thái (EcoKnow)

EcoKnow lưu trữ chỉ số của các hệ thống chuỗi mà Kardia đang kết nối cùng. Đây là bộ phận giúp Kardia vượt trội hơn các hệ thống khác khi nó cung cấp một lượng thông tin khổng lồ giúp Kardia đưa ra những giải pháp vượt trội cho cơ chế định hướng giao dịch bằng thuật toán thông minh. Bên cạnh những cập nhật về giao dịch, cập nhật về thông số cũng sẽ được thu thập và phân tích ngay lập tức. EcoKnow cô đọng và lưu trữ những thông số này thành một điểm dữ liệu toàn diện và cho phép hệ sinh thái sử dụng chúng để đưa ra các phương án tối ưu nhất. EcoKnow được xem như nguồn kiến thức của cả hệ thống, ngay cả các nút mạng mới cũng có khả năng tiếp cận nguồn này để lấy thông tin của toàn hệ thống.

d) Sổ cái chính

Sổ cái chính được lưu trữ trên tất cả các Nút (Tiêu chuẩn lẫn Nút Kép) và chứa đầy đủ dữ liệu của các Khối Chính (đọc thêm phần Cấu trúc của khối để hiểu rõ hơn). Sổ Cái Chính được cấu tạo theo cấu trúc giống với cây, khi mà mỗi Khối Chính giữ một chỉ dẫn tới các sổ cái phụ được tạo ra bởi Nút Kép. Sổ Cái Chính thể hiện trạng thái tổng quan của Máy ảo Kardia, trong đó bất cứ một giao dịch nào trên Kardia và trên các chuỗi ngoài đều sẽ làm thay đổi trạng thái của sổ chính. Mục tiêu của Sổ Cái Chính là cung cấp một cái nhìn tổng quan, liên tục về dữ liệu lịch sử của cả hệ thống mà không quan tâm hệ thống chuỗi nào thực hiện một giao dịch bất kỳ.

e) Ví chính

Ví chính là một địa chỉ an toàn để lưu trữ tài sản của người dùng với mức an toàn cao, nó cũng cho phép người dùng thực hiện các giao dịch liên chuỗi mà không cần phải sở hữu nhiều mã khóa cá nhân hay mã khóa công cộng cho từng chuỗi.

2. Các động mạch

Động mạch cho phép các giao dịch được thông suốt từ Kardia tới các chuỗi khác trong khi



đảm bảo các hoạt động liên chuỗi được thực hiện liền mạch. Đây là một quá trình gồm nhiều bước, trong đó có sự trao đổi hai chiều giữa Mô-đun Dịch và Mô-đun Dẫn, cũng như các lệnh smc thông qua Mô-đun Xử Lý.

a) Mô-đun Dịch

Mô-đun dịch sử dụng thuật toán để chuyển đổi hợp đồng thông minh Kardia có sẵn thành một bộ biên dịch mã byte chứa các SMCs phù hợp với các chuỗi thành viên, nhằm nâng cấp Hợp đồng thông minh Kardia và xử lý lỗi trên các chuỗi thành viên.

b) Hệ thống ngôn ngữ hợp đồng thông minh Kardia (KSML)

KSML được thiết kế để trở thành một công cụ đặc lực cho các nhà lập trình xây dựng các hợp đồng thông minh trên hệ thống Kardia mà không yêu cầu mức độ hiểu biết rộng hay kinh nghiệm chuyên sâu về lập trình. Bằng cách đưa ra một bộ hướng dẫn lập trình tổng hợp cấu tạo từ các hệ ngôn ngữ căn bản (như là JSON và YAML), các nhà lập trình có thể dễ dàng xây dựng ý tưởng của họ mà không cần sử dụng một ngôn ngữ cụ thể để viết chỉ dẫn cho một chuỗi khối nhất định nào (Ví dụ như Ethereum yêu cầu Solidity hay Neo yêu cầu C#, Java hoặc Python và nhiều hệ ngôn ngữ khác).

Phát hành song song với bộ ngôn ngữ KSML là ứng dụng kiểm tra giúp các nhà lập trình có thể nhanh chóng kiểm tra và xác nhận hợp đồng thông minh mà họ mới xây dựng là chính xác và hoạt động tốt trên nền Kardia. KSML và bộ công cụ sẽ được tích hợp vào SDK nhằm cung cấp cho các nhà lập trình một bộ công cụ đầy đủ để họ tự do xây dựng sản phẩm trên nền Kardia.

Trong tương lai, chúng tôi hướng tới việc hỗ trợ không những các hệ thống ngôn ngữ Hợp đồng thông minh Kardia mà còn cho phép các nhà phát triển cài đặt các phương thức lập trình cụ thể ứng dụng cho từng chuỗi khối (ví dụ như Solidity cho Hợp đồng thông minh của Ethereum). Phát triển này sẽ loại bỏ các rào cản và cho phép nhà lập trình xây dựng các giải pháp bằng tất cả các hệ thống ngôn ngữ và logic ngoài những gì mà KSML đã cung cấp.

c) Mô-đun Máy Học liên chuỗi (CMNR)

Mô-đun Máy học liên chuỗi sử dụng thuật toán chọn lựa dựa trên hệ SON để tìm ra những chuỗi khối thích hợp nhất để tham gia vào quá trình giao dịch liên chuỗi. Lựa chọn được dựa trên nhiều yếu tố, trong đó có chi phí, thời gian xác nhận, lượng giao dịch trên từng chuỗi. Mô-đun này sử dụng thuật toán chấm điểm linh hoạt, được xây dựng từ một cấu trúc phân tích ưu việt nhất, nhằm xác định tổng điểm của một chuỗi khối X ở thời điểm t cho một giao dịch R như sau:



$$\text{ScoreXt} = f(h, f, v, d)$$

h: độ cao của khối

f: chi phí cho giao dịch gần nhất được ghi lại

v: thời gian hình thành một khối của X

d: chỉ số độ khó được tính toán từ sự khác nhau giữa độ khó của các hợp đồng thông minh

Với lượng dữ liệu được lấy trực tiếp và liên tục từ EcoKnow như miêu tả ở trên, Mô-đun Máy Học liên chuỗi có thể đưa ra những quyết định hiệu quả trong việc định hướng các hợp đồng thông minh, từ đó đạt được Hiệu suất hoạt động tối đa cùng chi phí vận hành cạnh tranh. Nhờ có khả năng tự động hóa quản lý và tự động tối ưu hóa, tất cả những thay đổi và nâng cấp cho thuật toán chủ đạo của SON có thể được áp dụng một cách tự động mà không cần tới sự can thiệp của con người.

Mô-đun Máy học liên chuỗi sẽ có hai lớp bề mặt: bề mặt nội là một bề mặt lập trình ứng dụng JSON-RPC cung cấp khả năng định hướng cho các Nút để chỉ dẫn các giao dịch từ Kardia, bề mặt ngoại hay gọi là bề mặt lập trình ứng dụng RESTful cho phép nhà lập trình nhận được chỉ dẫn về hướng đi hiệu quả nhất cho hợp đồng thông minh của họ.

d) Mô-đun xử lý

Mô-đun xử lý chịu trách nhiệm cho phần việc ít tính toán nhất đó là đăng tải bộ biên dịch mã byte của hợp đồng thông minh, theo hướng dẫn chi tiết từ CMNR, tới chuỗi khối đích thông qua các JSON-RPC tương ứng.

3. Các Mạch Ven

Các Ven có trách nhiệm thu thập cập nhật từ hệ sinh thái, xử lý chúng một cách hiệu quả và gửi chúng tới sổ cái một cách an toàn. Các ven có những bộ phận như:

a) Mô-đun hấp thụ

Mô-đun hấp thụ lấy các khối mới từ một hệ chuỗi cụ thể nơi mà các nút mạng kép gửi thông tin tới. Các cập nhật liên quan sẽ được cô đọng và gửi tới Mô-đun Tổng Hợp trong thời gian thực.

b) Mô-đun tổng hợp

Mô-đun tổng hợp nhận được những cập nhật trực tuyến từ Mô-đun hấp thụ và sẽ:

- (1) Khớp những giao dịch đã được định hướng với đúng các dãy số nhận dạng từ chuỗi ngoài
- (2) Tổng hợp một loạt các giao dịch có khả năng tích hợp với nhau thành một giao dịch mới trên Kardia và gửi giao dịch này tới bề tổng hợp giao dịch



d) Tổng hợp nhóm và Sổ cái nhóm

Bể tổng hợp giao dịch là nơi mà Nút Kép thu thập các giao dịch đã được định hướng để xử lý ở khối tiếp theo. Sổ cái nhóm giữ một bản ghi chú về những giao dịch này. Đọc lại phần Cấu tạo khối để hiểu rõ thêm làm thế nào Sổ cái nhóm có thể kết nối với Sổ cái chính

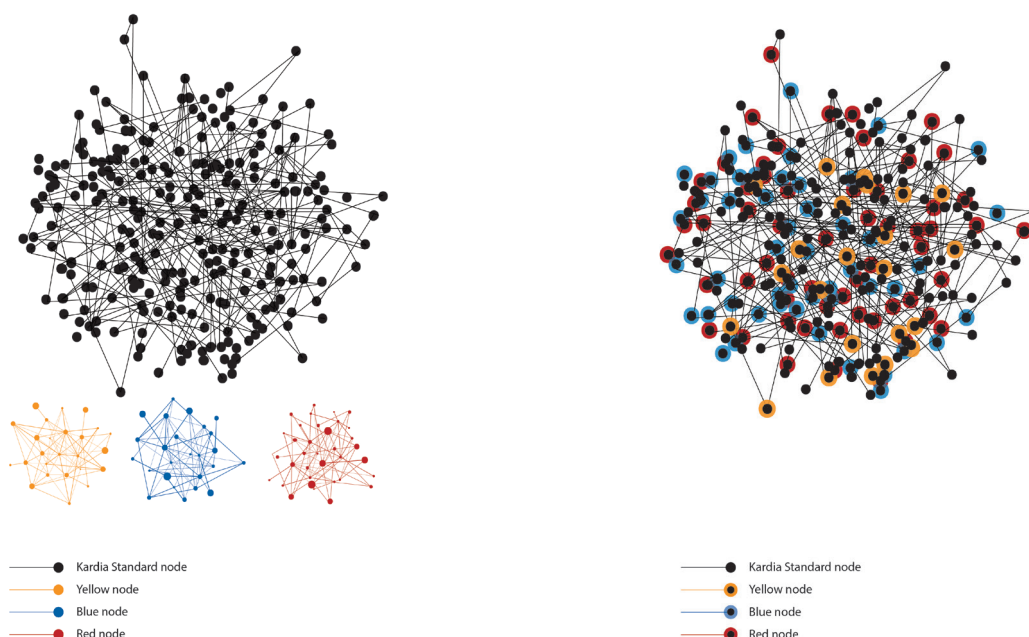
B. Cấu trúc hệ thống

Biểu đồ 6a. Tất cả các Nút khởi đầu là một nút Tiêu Chuẩn

Tất cả các Nút mới tham gia vào hệ thống sẽ được mặc định là một Nút Tiêu Chuẩn. Chúng có thể đặt cọc đồng tiền chính để trở thành một Nút Kép và tùy chọn một chuỗi ngoài để hỗ trợ. Nút Kép hoạt động theo nhóm được tạo ra bao gồm các Nút Kép hỗ trợ một chuỗi khối giống nhau. Có một lưu ý là ở từng thời điểm, Nút Kép chỉ gắn với một chuỗi khối cụ thể. Điều này là vì, đối với một nút đơn, hiệu suất xử lý giao dịch trên nhiều chuỗi ngoài cùng lúc là không hiệu quả và chưa khả thi. Sẽ cần tới các nghiên cứu thêm trong tương lai về sự khả thi của Nút Đa Chuỗi.

Biểu đồ.7a. Phân chia căn bản của Nhóm Nút Kép

Hình vẽ dưới cho thấy các Nút Kép trong cùng một nhóm có khoảng cách kết nối xa nhau, vì mỗi Nút chọn một chuỗi khối để hỗ trợ một cách tùy ý, hệ thống tổng sẽ chạy thuật toán tối ưu một cách định kỳ (một phần của Cơ chế phân luồng theo lợi ích của các bên tham gia) để đảm bảo liên kết tối đa giữa các Nút với nhau



Giai đoạn ban đầu - Tất cả các nút là các nút bình thường.

Giai đoạn chuyển tiếp - Các nút có thể chuyển sang các mạng được hỗ trợ.



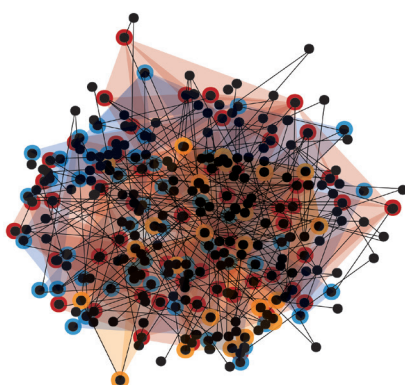
C. Cơ chế phân luồng theo lợi ích của các bên tham gia (ESWIM)

Biểu đồ 8. Chi phí giao dịch trên chuỗi Xanh và chuỗi Đỏ theo thời gian

Các Nút Kép được khuyến khích khi nhận được một phần lớn trong tổng số tiền thưởng của việc hình thành khối và tổng chi phí giao dịch để bù lại cho tần suất hoạt động phức tạp của chúng. Cơ chế Phân luồng theo lợi ích của các bên tham gia (ESWIM) có mục tiêu là đảm bảo hệ thống hoạt động ở trạng thái tốt nhất thông qua việc duy trì một số lượng Nút Kép phù hợp trong từng nhóm, và đảm bảo an ninh của hệ thống qua việc phân chia mức ảnh hưởng của các Người xác minh trong các nhóm và trong toàn hệ thống.

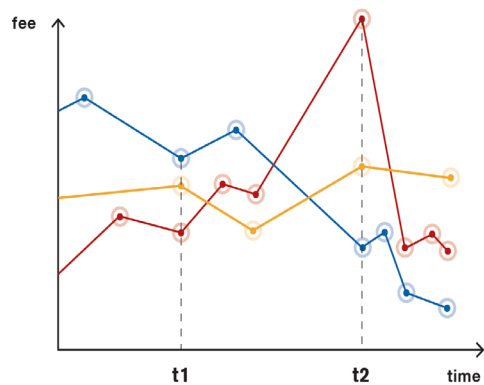
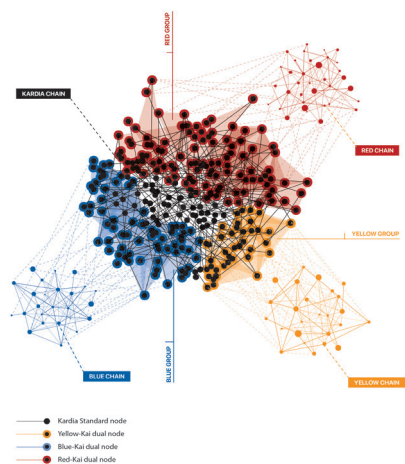
Cơ chế ESWIM khuyến khích các Nút chuyển đổi linh hoạt giữa Nút Tiêu Chuẩn và Nút Kép trong một nhóm thông qua một số công thức như: thay đổi sự phân chia tiền thưởng của khối, chi phí giao dịch và thay đổi những yêu cầu cụ thể với Nút cho từng chuỗi. Ví dụ, mức đặt cọc tối thiểu được tăng lên sẽ giúp chuyển bớt các Nút ra khỏi một nhóm quá đã quá tải, trong khi giảm thiểu mức này có thể thu hút nhiều Nút hơn tham gia vào một nhóm còn thiếu

Như thể hiện qua hình vẽ, sự thay đổi trong chi phí thực hiện giao dịch trên chuỗi Xanh và chuỗi Đỏ giữa khoảng thời gian t1 và t2 dẫn tới sự chuyển đổi trong nhóm Nút Kép của Kardia. Vì chi phí hoạt động trên chuỗi Đỏ trở nên đắt đỏ hơn, nên nhu cầu định hướng các giao dịch đến chuỗi Đỏ sẽ giảm đi, và ngược lại với chuỗi xanh. Cơ chế mà Kardia sử dụng sẽ điều chỉnh số lượng Nút Kép ở trong nhóm A và B một cách hợp lý dựa trên dự kiến số lượng giao dịch được hướng tới hai chuỗi này. Lưu ý rằng, chi phí thực hiện giao dịch chỉ là một trong nhiều yếu tố được Cơ chế Phân Luồng theo lợi ích các bên tham gia tính toán để thay đổi cho phù hợp.



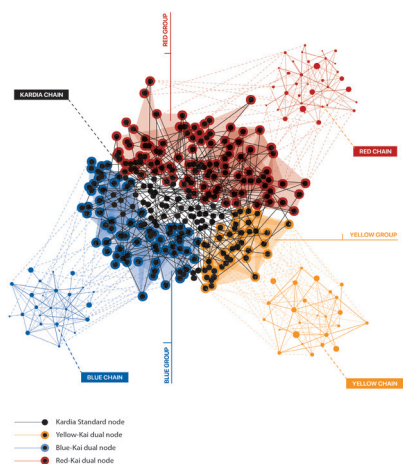
- Kardia Standard node
- Yellow-Kardia dual node
- Blue-Kardia dual node
- Red-Kardia dual node

Phân phối ban đầu của các nhóm kép

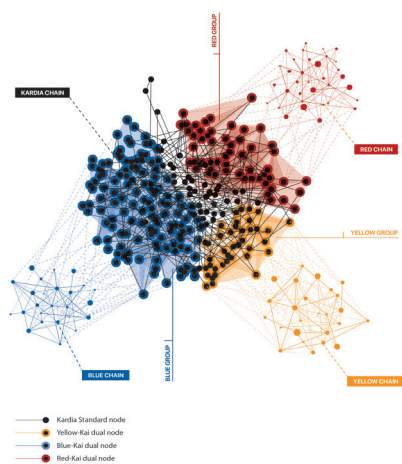


Tối ưu hóa phân phối nhóm kép

Thay đổi phí giao dịch cho chuỗi màu xanh và đỏ theo thời gian



Phân phối nhóm tại thời điểm t1



Phân phối nhóm tại thời điểm t2



D. Cơ chế đồng thuận

Biểu đồ 8. Chi phí giao dịch trên chuỗi Xanh và chuỗi Đỏ theo thời gian

KardiaChain sử dụng hai cơ chế đồng thuận BFT DPoS: Cơ chế đồng thuận chính (MCon) và cơ chế đồng thuận nhóm (GCon). Thành viên của cơ chế đồng thuận chính được gọi là Người xác minh chính (Mvals), là những người có trách nhiệm duy trì sổ cái chính của Kardia. Thành viên của cơ chế đồng thuận nhóm được gọi là Người xác minh nhóm (Gvals), là những người chịu trách nhiệm phê duyệt những giao dịch liên chuỗi và thêm chúng vào những nhóm sổ cái tương ứng.

1) Quá trình: Quá trình 5 bước trong cơ chế đồng thuận nhóm như sau:

- **Bầu cử:** Người xác minh lựa chọn ra giữa họ những Người đề xuất của nhóm.
- **Đề xuất:** Người đề xuất nhóm cấu tạo một khối và gửi khối này tới các Nút khác trong nhóm. Trong trường hợp Người đề xuất thất bại trong việc tạo ra một khối trong thời gian cho phép, hệ thống sẽ chuyển sang bước tiếp theo mà không quan tâm đến kết quả của việc tạo khối. Thêm vào đó, Người đề xuất sẽ dòi những giao dịch này đến khối tiếp theo (1)
- **Xác minh:** Người xác minh nhận được khối đề xuất, bắt đầu quá trình bầu cử với các lựa chọn là <Chấp thuận/Từ chối/Không bầu> để quyết định sự hợp lệ của khối, sau đó gửi phiếu bầu của họ thông qua nghi thức trao đổi.
- **Chấp thuận:** Khi mà Người đề xuất của nhóm nhận được 2/3 tổng số phiếu, họ sẽ gửi khối này tới Người đề xuất chính (2). Tất cả các Nút Kép sẽ chấp thuận khối này sau khi Khối Chính chấp thuận nó
- **Tổng kết:** Nếu khối mới được chấp thuận trên hệ thống, độ cao của khối sẽ tăng thêm 1 đơn vị để hiển thị khối mới này đã được hoàn toàn chấp thuận. Quá trình đồng thuận chính diễn ra theo các bước tương tự với một số điểm khác biệt nhỏ như:

Các bước tương tự được thực hiện trong cơ chế đồng thuận chính:

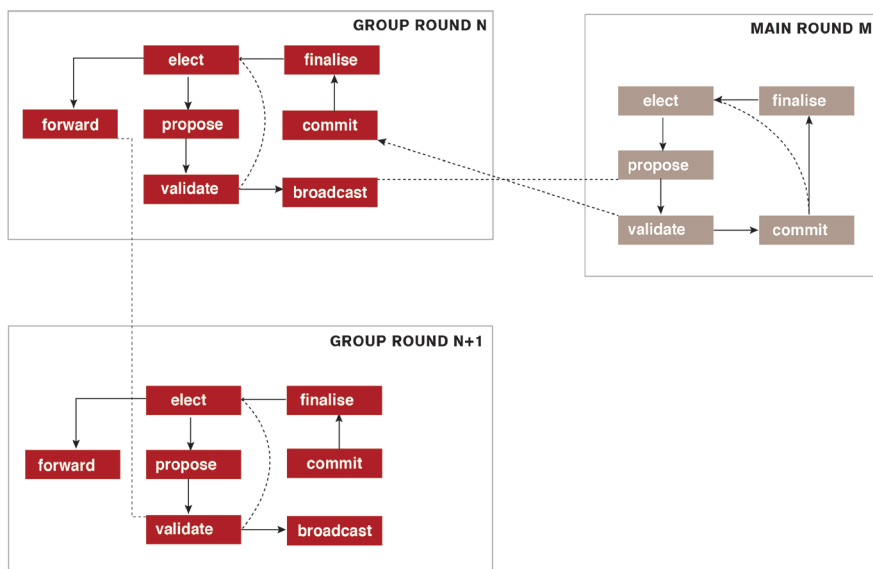
- **Bầu cử:** Những Người xác minh sẽ chọn trong số họ một Người đề xuất chính
- **Đề xuất:** Những người đề xuất chính sẽ cấu tạo một khối chính từ Nhóm khối mà họ nhận được và hợp lệ hóa
- **Chấp thuận:** Khi khối được đề xuất nhận đủ phiếu bầu chấp thuận, tất cả các Nút sẽ bắt đầu chấp nhận khối đó

(1) Chuyển tiếp các giao dịch: Người đề xuất của nhóm có kết nối với bể tổng hợp các giao dịch có thể định hướng và xử lý các giao dịch đã định hướng đang trong chế độ chờ và đã có chuỗi mục tiêu phù hợp với chuỗi hiện tại của các giao dịch này. Sau khi được cho phép



chuyển tiếp, Người đề xuất sẽ chuyển những giao dịch RTXs này tới bể tổng hợp Nút Kép, nơi mà các Nút Kép sẽ lưu lại và cập nhật những giao dịch này trong chuỗi khối tiếp theo được hình thành.

(2) Hiện thị những khối được chấp thuận: Sau khi các khối được đề xuất nhận đủ 2/3 số phiếu chấp thuận, các Nhà đề xuất nhóm sẽ gửi những khối này tới các Nút khác, tập trung hướng tới các Nhà đề xuất chính nhằm đưa những chuỗi này vào đề xuất của họ.



Nghị định thư thỏa thuận

2) Cấu trúc khối

Cấu trúc của một khối đôi có thể thấy như trên. Khối kép từ các nhóm khác nhau sẽ được đánh dấu bởi các danh tính riêng, ví dụ như EK cho Eth-Kardia, NK cho Neo-Kardia (*cách đánh dấu này có thể được thay đổi)

Người đề xuất chính sẽ tổng hợp các giao dịch đã được tích hợp TX(u) từ tất cả các Nút Kép với các giao dịch đã được tích hợp TX(n) từ các Nút tiêu chuẩn để hình thành tổng hợp dữ liệu của các giao dịch. Người Đề xuất chính sẽ xác nhận các giao dịch này với dữ liệu Chữ Ký thu thập được từ Khối Kép và những Nút tiêu chuẩn đã gửi giao dịch đến. Người đề xuất chính ghi lại những giao dịch này trên hệ thống gốc. Các Khối Chính sẽ được hình thành từ những dữ liệu cần thiết và các chữ ký có được từ Người đề xuất Chính.

E. Mô hình Đặt Cọc

1) Một nhà điều hành Nút cần khóa tất cả các đồng Kardia (KAI) trong ví của mình sử dụng giao dịch khóa tài khoản (lockBalance) nhằm trở thành một Người xác minh. Lượng đặt cọc được yêu cầu từ Người xác minh của Nút chính là $s(M)$, của Nút Kép chính là $s(M+D)$. Chúng tôi sử dụng khái niệm 'độ tuổi của đồng tiền' để đánh giá mức tín nhiệm của lượng tiền đặt



cọc, có nghĩa là số tiền đặt cọc phải được giữ ở trong tài khoản

qua một

số lượng khối nhất định (ký hiệu `mature_time`) trước khi sẵn sàng để dùng cho `lockBalance`. Mô hình này bao gồm nhiều điểm bảo vệ hệ thống khỏi sự tấn công. Một mặt, `mature_time` giúp kéo dài thời gian cần thiết cho một cuộc tấn công khi những đồng tiền mới được giao dịch sẽ không được phép dùng cho việc đặt cọc. Mặt khác, trong thời gian `mature_time`, tổng lượng tiền đặt cọc có thể thay đổi, do đó lượng tiền đặt cọc cần thiết để đạt được đa số có thể sẽ phải tăng lên. Ví dụ, tổng lượng đặt cọc hiện tại là 1,000,000 KAI, một hacker phải sở hữu 2,000,001 KAI để đạt được trên 66% tổng phiếu bầu dựa trên cơ chế đồng thuận BFT miêu tả ở trên. Sau khi trải qua `Mature_time`, một số tài khoản mới tham gia vào hệ thống như những Người xác minh mới và nâng tổng số dự trữ lên thêm 100,000 KAI. Nghĩa là hacker sẽ cần thêm 200,000 KAI và chờ đợi thêm một lượt `mature_time` nữa để có khả năng tấn công hệ thống. Vì vậy, không có gì đảm bảo một cuộc tấn công vào hệ thống có thể thành công, khiến chúng trở nên khó khăn cho người dùng có ý định tấn công hệ thống.

Một sự tấn công vào Nhóm Nút Kép cũng yêu cầu phải đạt được sự kiểm soát của hệ thống chính vì những cập nhật từ chuỗi ngoài cần phải được xác nhận bởi Người xác minh chính trước khi được ghi lại tại Sổ Cái Chính. Như miêu tả ở biểu đồ 13, để chiếm quyền kiểm soát của một nhóm có 10% lượng đặt cọc sẽ cần 7% tổng lượng đặt cọc, ví dụ như, đưa ra một cập nhật giả từ chuỗi Vàng. Tuy nhiên, để cập nhật này được ghi lại trên sổ cái của Kardia, nó sẽ cần được xác minh bởi các Nhà xác minh chính. Điều này có nghĩa là cần thêm một lượng đặt cọc 60% nữa để có cơ hội thực hiện một cuộc tấn công. Trong trường hợp cuộc tấn công thất bại, lượng đặt cọc trên tất cả các Nút đã chấp thuận giao dịch này hoặc khối có hại này sẽ bị hủy (lượng tiền này sẽ được đốt đi), làm cho bất cứ một cuộc tấn công vào Kardia nào trở nên đắt đỏ hơn.

2) Chức năng của đồng tiền chính

Đồng tiền tiện ích mã hóa của KardiaChain (KAI) là một bộ phận quan trọng của hệ sinh thái mà KardiaChain xây dựng, nó được thiết kế với chức năng là đồng tiền duy nhất trong hệ thống. KAI là đồng tiền tiện ích không có khả năng được hoàn trả, chỉ được sử dụng làm đơn vị trao đổi giữa những thành viên tham gia trong hệ sinh thái KardiaChain. Sự ra đời của KAI nhằm cung cấp một phương thức thanh toán thuận tiện, an toàn và đơn giản cho hoạt động trao đổi giữa các thành viên khi tương tác với hệ sinh thái KardiaChain. KAI không đại diện cho bất cứ sự sở hữu (shareholding), sự tham dự (participation), quyền lợi (right), chức danh (title) hay lợi ích (interest) nào của người sở hữu KAI đối với Tổ chức (Foundation), nhà Phân phối (the Distributor), hay bất cứ đơn vị trực thuộc (its affiliates), doanh nghiệp hoặc bên đại diện nào, đồng KAI cũng không có giá trị đại diện hay cung cấp cho người sở hữu chúng bất cứ ràng buộc hay cam kết nào về phí (fee), cổ tức (dividends),



doanh thu (revenue), lợi nhuận (profits) hay lợi ích đầu tư nào (investment returns), và cũng không cấu thành, không là một phần của bất cứ một loại bảo chứng (securities) nào ở Singapore hay bất kỳ một vùng lãnh thổ có liên quan nào. KAI chỉ có thể được sử dụng trong hệ sinh thái của KardiaChain, sự sở hữu KAI không đi cùng với quyền hạn hay khả năng đưa ra ý kiến nào ngoại trừ khả năng được sử dụng KAI như một công cụ cho việc tương tác với KardiaChain.

Tài nguyên mạng (computational resources) được sử dụng trong quá trình xác minh một khối mới/các thông tin trên hệ thống chuỗi khối, vì vậy, nhà cung cấp nguồn tài nguyên mạng sẽ thu phí từ những hoạt động sử dụng tài nguyên mạng (ví dụ như: “mining” trên KardiaChain) nhằm duy trì sự công bằng và minh bạch của hệ thống, KAI sẽ được sử dụng như một đơn vị thanh toán trong quá trình chi trả sau khi sử dụng tài nguyên mạng. KardiaChain yêu cầu các miners đặt cọc một số lượng KAI nhất định trước khi được phép tham gia vào quá trình mining. KAI là một phần không thể tách rời của KardiaChain, vì khi không có sự xuất hiện của KAI, sẽ không có lợi ích nào cho người dùng để sử dụng tài nguyên mạng để thực hiện các hoạt động hay cung cấp dịch vụ đóng góp vào sự phát triển của cả hệ sinh thái KardiaChain.

Những người dùng của KardiaChain và người sở hữu KAI sẽ không nhận được lợi ích từ KAI nếu không tích cực tham gia vào các hoạt động trên KardiaChain. Cụ thể, KAI được hiểu và chấp nhận là:

- Không có khả năng được hoàn trả và không được quy đổi thành tiền mặt (hoặc bất cứ giá trị tương đương nào đối với các đồng tiền mã hóa khác) hay bất cứ phương thức thanh toán nào từ Tổ chức, nhà Phân phối hay các đơn vị trực thuộc nào;
- Không đại diện hay cho phép người sở hữu KAI có bất cứ quyền hạn nào đối với Tổ chức, nhà Phân phối (hoặc bất cứ đơn vị trực thuộc nào), hay đối với doanh thu (revenue), tài sản (assets), bao gồm bất cứ quyền hạn nào để được nhận cổ tức (dividends), doanh thu (revenue), cổ phiếu (shares), quyền sở hữu (ownership), cổ phiếu (shares) hay bảo chứng (security), quyền bỏ phiếu, phân phối, mua lại, thanh toán, quyền sở hữu (bao gồm tất cả các hình thức liên quan tới tài sản trí tuệ), hay các quyền hạn về tài chính và luật pháp khác bao gồm quyền sở hữu trí tuệ hay bất cứ hình thức tham gia vào các vấn đề liên quan tới KardiaChain, Tổ chức, nhà Phân phối hay các nhà cung cấp dịch vụ cho các đơn vị nêu trên;
- Không đại diện cho bất cứ quyền hạn nào dưới dạng hợp đồng khác biệt, hay hợp đồng với mục đích đảm bảo lợi nhuận hoặc tránh thua lỗ;
- Không phải một hình thức tiền tệ (hoặc tiền điện tử), bảo chứng (security), hàng hóa (commodity), trái phiếu (bond), các công cụ nợ (debt instrument) hay bất cứ hình thức nào liên quan tới các công cụ tài chính (financial instrument) hoặc đầu tư;



- Không phải một khoản vay của Tổ chức, nhà Phân phối hay các đơn vị trực thuộc, không đại diện cho khoản vay của Tổ chức, nhà Phân phối hay các đơn vị trực thuộc, sẽ không có mong đợi về lãi suất;
- Không cung cấp cho người sở hữu KAI bất cứ quyền sở hữu hay lợi ích nào trong Tổ chức, nhà Phân phối hoặc bất cứ đơn vị trực thuộc nào.

Những đóng góp trong quá trình token sale sẽ được lưu trữ bởi nhà Phân phối (hoặc các đơn vị trực thuộc nhà phân phối) sau quá trình token sale. Những người tham gia trong quá trình sale sẽ không có quyền lợi về kinh tế, luật pháp, hay lợi ích nào từ khoản đóng góp nêu trên hoặc tài sản đã đóng góp của bên đóng góp sau quá trình token sale.

Trong trường hợp có những bước phát triển trong thị trường thứ cấp (secondary market) trao đổi KAI, thị trường này sẽ được duy trì và quản lý bởi một đơn vị riêng biệt, không có liên quan đến Tổ chức, nhà Phân phối, hay quá trình sale của KAI và Kardiachain. Tổ chức và nhà Phân phối sẽ không tạo ra một thị trường thứ cấp nếu trên, cũng như sẽ không trở thành một đơn vị trao đổi KAI.

V. LỢI THẾ CỦA KARDIACHAIN

Chúng tôi đề ra nhiệm vụ phải đơn giản hóa công việc cho các nhà lập trình khỏi sự giới hạn khi hoạt động trong một chuỗi đơn. Kardia cho phép các nhà lập trình tạo ra các ứng dụng phi tập trung có khả năng chạy trên nhiều chuỗi khối cùng lúc mà không yêu cầu họ phải viết các hợp đồng thông minh khác nhau cho từng chuỗi. Kardia hướng tới việc tạo ra một hệ thống bao quát gồm cả những chuỗi tư nhân và chuỗi mở. Trong hệ thống này, một chuỗi có thể tương tác với bất kỳ một chuỗi nào khác trong hệ thống mà không cần phải thay đổi cách thức liên lạc nào từ mỗi chuỗi. Vì vậy, chúng ta có thể dễ dàng tăng khả năng mở rộng, khả năng liên kết và khả năng thay đổi linh hoạt.

Khả năng mở rộng

Khi một hợp đồng thông minh được gửi tới KardiaChain, nó sẽ được tích hợp và gửi tới một chuỗi khối được chỉ định trong hệ thống. Chuỗi khối phù hợp nhất được bầu chọn để nhận và xử lý giao dịch này nhằm cung cấp khả năng xử lý giao dịch ở mức tối ưu nhất trong cả hệ thống tính ở thời điểm giao dịch được gửi tới. Đây còn được biết đến như một giải pháp giảm tải cho các chuỗi khối, tránh các trường hợp ùn tắc cục bộ ở một số thời điểm nhất định.



Khả năng tích hợp

Bất cứ một tổ chức hay cá nhân nào đều có thể có những trải nghiệm đầu tiên với ứng dụng của công nghệ chuỗi khối thông qua các hợp đồng thông minh APIs, cung cấp một bộ công cụ để sử dụng và hỗ trợ đầy đủ các hệ ngôn ngữ giúp nhà lập trình có thể xây dựng, kiểm định và áp dụng những hợp đồng thông minh đầu tiên mà họ xây dựng và không gặp phải khó khăn nào. Tất cả các bước đều có thể được thực hiện trên một nền tảng web đơn giản, không yêu cầu các cài đặt nâng cao.

Khả năng phát triển

Các nhà lập trình có thể dễ dàng tích hợp thêm các công nghệ chuỗi khối mới thông qua các giao diện lập trình hợp đồng thông minh của Kardia từ những công cụ và hệ ngôn ngữ quen thuộc với họ. KSML được thiết kế với ngôn ngữ dễ đọc, các hệ ngôn ngữ có sẵn để hỗ trợ hầu hết các hoạt động mà hợp đồng thông minh liên quan tới. Bằng cách thay đổi hợp đồng thông minh thông qua KSML, các nhà lập trình sẽ dễ dàng áp dụng giải pháp mà họ xây dựng trên tất cả các chuỗi khối được hỗ trợ.

Chi phí

Khi bạn hoạt động trong một hệ thống nhất định, bạn sẽ phải trả một lượng phí với tỷ lệ thay đổi liên tục. Với Kardia, người dùng sử dụng CMNR nhằm chọn ra chuỗi phù hợp nhất để xử lý giao dịch trong một khoảng thời gian nhất định. Kể cả cộng thêm phí giao dịch của Kardia, chi phí trung bình sẽ luôn luôn thấp hơn chi phí trung bình trên một chuỗi đơn

Khả năng liên kết

Thông qua Kardia, tất cả các chuỗi trong hệ thống đều có khả năng tương tác, sử dụng dữ liệu và tài sản trên các chuỗi khác. Chức năng liên chuỗi cho phép các ứng dụng phi tập trung có thể được ứng dụng trên nhiều chuỗi khác nhau, điều sẽ giúp giảm thiểu sự ùn tắc trên một chuỗi cụ thể ở một thời điểm nhất định



V. CHÂN TRỜI MỚI CHO ỨNG DỤNG PHI TẬP TRUNG

Mục này sẽ giới thiệu tổng quan về 3 đặc trưng tiêu biểu mà các ứng dụng phi tập trung có được khi chạy trên hệ thống của chúng tôi:

A. Các Dapp đơn giản với lượng truy cập lớn:

Bầu cử công khai là một ví dụ điển hình cho loại Dapp này. Trong một khoảng thời gian cố định, chúng ta dự tính sẽ nhận được một lượng phiếu bầu lớn tương ứng với dân số của cả một đất nước. Tuy nhiên, quá trình cài đặt rất đơn giản khi nhà tổ chức chỉ cần điều chỉnh một phần nhỏ trong biểu mẫu SMC có sẵn mà Kardia cung cấp, sau đó sử dụng lệnh `Vote_smart contract_ABC(K)` trên hệ thống Kardia. Trừ khi có những sửa đổi thêm, CMNR sẽ phân tích lệnh trên và đưa ra một danh sách những hệ thống chuỗi mà lệnh `Vote_smart contract_ABC(K)` có thể chạy trên. Sau đó, bộ phận này sẽ chuyển đổi mã code SMC để tích hợp với chuỗi được chọn, ví dụ như `Vote_smart contract_ABC(Eth)` tích hợp cho Ethereum.

Nhà tổ chức sau đây sẽ nhận được danh sách của một số địa chỉ lệnh `Vote_smart contract_ABC` trên nhiều chuỗi và có thể tùy chọn để sử dụng chúng một cách hợp lý. Những người bầu cử có thể gửi phiếu bầu của mình trên bất cứ một chuỗi nào mà lệnh `Vote_smart contract_ABC` được chạy trên. Tuy nhiên, chúng tôi có khuyến cáo gửi phiếu bầu qua hệ thống chuỗi gốc Kardia nhằm tối ưu hóa bộ dẫn thông minh đã được mã hóa làm giảm ùn tắc cho cả hệ thống.

Một ví dụ khiêm tốn đó là, Kardia hỗ trợ 2 hệ thống chuỗi (E và N) trong thời điểm diễn ra cuộc bầu cử. Chuỗi khối đầu tiên có khả năng xử lý 2000 giao dịch trong một giây với mỗi khối được hình thành trong 10 giây, trong khi chuỗi khối còn lại có thể thực hiện 1000 giao dịch trong một giây với thời gian hình thành khối là 5 giây. Bên cạnh đó, hệ thống chuỗi gốc của Kardia có thể xử lý thêm khoảng 3100 giao dịch trong 1 giây, tổng cộng, cả hệ thống có thể đảm bảo thu nhận đầy đủ phiếu bầu của 50 triệu dân (với điều kiện tất cả dân số gửi phiếu bầu của họ đi trong vòng 8 tiếng, ở cùng một ngày, dẫn tới nhu cầu sử dụng trung bình 1700 giao dịch trong vòng một giây).

B. Dapp đa công dụng:

Một ví dụ đơn giản đó là phần mềm trò chơi CryptoKitties, phần mềm này với mỗi thao tác mà người chơi sử dụng ví dụ như cho mèo ăn, thay đổi tên mèo sẽ sử dụng 1 giao dịch



trên hệ thống chuỗi Ethereum và tiêu tốn cả thời gian lẫn tiền bạc. Chúng ta có thể tiết kiệm được rất nhiều thời gian và chi phí nếu có thể chuyển những thao tác nhỏ này đến một hệ thống chuỗi đang có ít giao dịch hơn và yêu cầu chi phí thấp hơn. Những thao tác chính như mua/bán mèo sẽ được thực hiện trên những hệ thống chuỗi chính và đang tin cậy. Cách tiếp cận này sẽ mang lại lợi ích trong việc tận dụng sự chênh lệch trong tần suất thực hiện các thao tác. Ví dụ như, cho mèo ăn là thao tác sẽ được thực hiện nhiều, trong khi việc trao đổi các chú mèo giữa người chơi sẽ được thực hiện ở một tần suất thấp hơn nhiều. Vì vậy, tại sao cả hai thao tác này nhất thiết phải chạy trên cùng một hệ thống chuỗi? Trong việc thiết kế phần mềm, chúng ta biết việc sử dụng nhiều điểm dữ liệu với các thông số khác nhau (như tốc độ và tính liên tục) cho từng mục đích phù hợp là một phương pháp đáng được quan tâm và tạo ra nhiều lợi ích trong khi ứng dụng phần mềm này.

C. Các Dapps liên thông với nhau:

Kardia cung cấp một hệ thống hạ tầng cho Dapps để chúng có thể trao đổi dữ liệu và tương tác với nhau một cách an toàn, liền mạch. Biểu đồ dưới đây giúp chúng ta hiểu phương thức hoạt động của một Dapp trong mảng ngân hàng, khi Dapp này đã sử dụng dữ liệu KYC của một Dapp khác trong khi hai Dapp này được chạy trên hai hệ thống chuỗi khác nhau (KardiaChain và ChainX). Người dùng A đăng tải thông tin cá nhân KYC lên ChainX, người dùng A có thể cho phép ứng dụng Banking_Dapp sử dụng dữ liệu KYC_A từ điểm dữ liệu KYC_Dapp trên KardiaChain. Quá trình này được thực hiện một cách an toàn và phi tập trung nhằm giảm thiểu khối lượng công việc cho các kỹ sư phần mềm và nâng cao trải nghiệm cho người dùng.



VII. 참고문헌(References)

- [1] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, P. Saxena, "A secure sharding protocol for open blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016.
- [2] D. Beaver, S. Kumar, H. C. Li, J. Sobel, P. Vajgel, "Finding a needle in Haystack: Facebook's photo storage," in Proc. 9th USENIX Conf. Oper. Syst. Des. Implement. (OSDI), 2010.
- [3] Facebook Inc, "2018 Third Quarter Reports," 2018 [Online]. Available: <https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Third-Quarter-2018-Results>
- [4] <https://www.omnicoreagency.com/youtube-statistics/>
- [5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008 [Online]. Available: <http://bitcoin.org/bitcoin.pdf>.
- [6] M. Castro, B. Liskov, "Practical Byzantine Fault Tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, ser. OSDI '99. Berkeley, CA, USA: USENIX Association, 1999.
- [7] M.L. Abbott, M.T. Fisher, "The art of scalability: Scalable web architecture, processes, and organizations for the modern enterprise," Addison-Wesley, 2009.
- [8] "Ethereum Yellow Paper," 2014 [Online]. Available: <https://ethereum.github.io/yellowpaper/paper.pdf>
- [11] M. Al-Bassam, A. Sonnino, V. Buterin, "Fraud Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities," ArXiv:1809.09044. Available: <https://arxiv.org/abs/1809.09044>
- [12] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, P. Wuille, "Enabling Blockchain Innovations with Pegged Sidechains," [Online]. Available: <https://blockstream.com/sidechains.pdf>



- [13] G Verdian, P Tasca, C Paterson, G Mondelli, "Overledger White Paper," 2018. [Online]. Available <https://www.quant.network/press/overledger-white-paper>
- [14] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework" 2017. [Online]. Available: <https://polkadot.network/PolkaDotPaper.pdf>
- [15] N Chondros, K Kokordelis, M Roussopoulos, "On the practicality of practical Byzantine fault tolerance," in Proceedings of the 13th International Middleware Conference, Montreal, QC, Canada, Dec 2012.
- [16] C. Brunner, D. Flore, "Generation of Pathloss and Interference Maps as SON Enabler in Deployed UMTS Networks," in Proceedings of IEEE 69th Vehicular Technology Conference, Barcelona, Spain, 2009.
- [17] W. LiS'ebastien, A. BohliGhassan, G. Karame, "Securing Proof-of-Stake Blockchain Protocols," in Data Privacy Management, Cryptocurrencies and Blockchain Technology, DPM 2017, CBT 2017.s
- [18] N. Bowles, "CryptoKitties, Explained ... Mostly," in The New York Times, Dec. 28, 2017. Available: <https://www.nytimes.com/2017/12/28/style/cryptokitties-want-a-blockchain-snuggle.html>



KARDIACHAIN

hello@kardiachain.io
www.kardiachain.io