*This translation has been made by* [QuangTV](https://forum.cardano.org/u/quangtvpc3/summary) *from the original document published by*[Prof Aggelos Kiayias](https://iohk.io/en/blog/authors/aggelos-kiayias/page-1/) *at* *https://iohk.io/en/blog/posts/2020/03/26/enter-the-hydra-scaling-distributed-ledgers-the-evidence-based-way.*

Chuyển sang Hydra: mở rộng sổ cái phân tán, cách tiếp cận dựa trên bằng chứng

### Tìm hiểu về Hydra: giao thức sổ cái nhiều đầu

26/3/2020,[Prof Aggelos Kiayias](https://iohk.io/en/blog/authors/aggelos-kiayias/page-1/) (10 phút)



Khả năng mở rộng là thách thức lớn nhất giúp blockchain phát triển. Bằng cách áp dụng phương pháp tiếp cận dựa trên bằng chứng, có nguyên tắc, chúng tôi đã đưa ra một giải pháp cho Cardano và các mạng lưới tương tự khác, đó là: Hydra. Hydra là đỉnh cao của nghiên cứu học thuật sâu rộng và là bước quyết định cho phép mở rộng mạng lưới phi tập trung quy mô phạm vi toàn cầu một cách an toàn.

## **Khả năng mở rộng là gì và cách thức đo lường?**

Mở rộng quy mô hệ thống sổ cái phân tán đề cập đến khả năng cung cấp thông lượng giao dịch cao, độ trễ thấp với dung lượng lưu trữ tối thiểu cho mỗi nút. Những đặc điểm này luôn được nhắc đến là 1 phần quan trọng đối với việc triển khai ứng dụng thành công giao thức blockchain trong thế giới thực. Về mặt thông lượng, mạng VISA với khả năng xử lý trung bình 1.736 giao dịch thanh toán mỗi giây (TPS) và tốc độ xử lý tối đa lên đến 24.000 TPS, được xem là cơ sở khi so sánh với các mạng lưới khác. Dĩ nhiên là độ trễ giao dịch mong muốn càng thấp càng tốt, với mục tiêu cuối cùng là thông tin được hiển thị tức thời cho người sử dụng. Mỗi ứng dụng sổ cái phân tán yêu cầu thông số này khác nhau. Khi thiết kế một sổ cái phân tán nói chung, điều tất nhiên là phải cố gắng đạt được cả ba thông số này.

Việc triển khai một hệ thống đảm bảo khả năng mở rộng cho một ứng dụng cụ thể đòi hỏi sự kết hợp xét trên hai phương diện: áp dụng thuật toán thiết kế đúng đắn và triển khai trên nền tảng phần cứng và hạ tầng mạng phù hợp.

Khi đánh giá một thiết kế thuật toán cụ thể, chúng ta thường nhầm lẫn khi chú ý đến giá trị tuyệt đối của các thông số này. Bởi các đại lượng tuyệt đối đó sẽ liên quan mật thiết với cấu hình mạng và phần cứng cụ thể, có thể ảnh hưởng đến việc đánh giá ưu nhược điểm của các thuật toán cụ thể. Thật vậy, một giao thức được thiết kế kém vẫn có thể hoạt động đủ tốt khi được triển khai trên phần cứng và hạ tầng mạng vượt trội.

Vì lý do này mà chúng ta cần phải cẩn thận xem xét khi đánh giá năng lực xử lý của giao thức dựa trên yêu cầu cấu hình phần cứng và hạ tầng mạng tối thiểu đi kèm. Điều này có thể đạt được bằng cách so sánh nó với các giao thức thô thuần tuý, trong đó loại bỏ tất cả các yếu tố về thiết kế. Chẳng hạn: nếu chúng ta muốn đánh giá phần mào đầu của một thuật toán mã hóa, chúng ta có thể so sánh hiệu suất truyền nhận giữa hai đầu cuối với bản tin được mã hoá và bản tin thuần tuý không mã hóa. Với thử nghiệm này thì việc xét tỷ lệ số bản tin trao đổi trên 1 giây không quan trọng, mà quan trọng là ở phần mào đầu được thuật toán mã hóa thêm vào. Hơn nữa, trong một số trường hợp cấu hình thử nghiệm thiết lập phần mào đầu gần bằng 0, chúng ta có thể kết luận rằng thuật toán tiệm cận với khả năng truyền nhận của cấu hình mạng tối thiểu nào đó và đây chính là ý nghĩa của việc tối ưu.

**Hydra - tầm nhìn 30.000 feet**

Hydra là một kiến trúc mở rộng ngoài chuỗi cho sổ cái phân tán, giải quyết cả ba thách thức về khả năng mở rộng đã đề cập đó là: thông lượng giao dịch cao, độ trễ thấp với dung lượng lưu trữ trên mỗi nút là tối thiểu. Mặc dù Hydra được thiết kế trên cơ sở kết hợp giao thức Ouroboros với sổ cái Cardano, nhưng nó cũng có thể được sử dụng trên các hệ thống khác, miễn là chuỗi khối của nó có những đặc điểm tương đồng với Cardano.

Dù là một giải pháp tích hợp hệ thống nhằm giải quyết vấn đề về khả năng mở rộng - Hydra vẫn bao gồm một số giao thức phụ. Điều này là cần thiết vì bản thân Cardano không phải là hệ sinh thái hoàn chỉnh mà gồm nhiều mảnh ghép công nghệ khác nhau: hệ thống hỗ trợ các pool đóng block với các nhóm cổ phần liên quan, ví lưu trữ lưu lượng cao cho các sàn giao dịch và cho người dùng với nhiều tính năng và hiệu suất tính toán. Nếu kỳ vọng vào giải pháp một giao thức duy nhất có thể đảm bảo khả năng mở rộng cho đa dạng thành phần tham gia mạng lưới như vậy thì sẽ không thực tế.

Kiến trúc khả năng mở rộng Hydra có thể được chia thành bốn giao thức thành phần: phần đầu (head), phần đuôi (tail), truyền thông chéo giữa đầu và đuôi (cross), cùng một số giao thức hỗ trợ định tuyến, cấu hình và ảo hóa. Trong đó 'head' là giao thức trọng tâm, cho phép một tập hợp những người tham gia có hiệu suất và độ sẵn sàng cao (chẳng hạn như các nhóm cổ phần) xử lý rất nhanh một số lượng lớn các giao dịch với dung lượng lưu trữ tối thiểu thông qua kênh trạng thái đa bên – giống như cách triển khai kênh thanh toán hai bên trong mạng Lightning.

Thêm vào đó là là việc bổ sung giao thức 'tail', cho phép mở rộng số lượng lớn người dùng cuối, các bên tham gia cung cấp khả năng cho những người có thể sử dụng hệ thống từ các thiết bị tiêu thụ điện năng thấp, chẳng hạn như điện thoại di động và những người offline trong khoảng thời gian dài. Trong khi đầu và đuôi đã có thể giao tiếp thông qua chuỗi chính Cardano, giao thức chéo giữa đầu và đuôi cung cấp một biến thể ngoài chuỗi (off-chain) hiệu quả. Tất cả điều này được gắn với nhau bằng cách định tuyến và quản lý cấu hình, trong khi ảo hóa tạo điều kiện giao tiếp nhanh hơn, tổng quát hóa giao tiếp đầu và đuôi.

## **Giao thức head của Hydra**

Giao thức Head Hydra là thành phần đầu tiên của kiến trúc Hydra được phát hành công khai. Nó cho phép một nhóm người tham gia tạo ra một kênh trạng thái ngoài chuỗi (được gọi là một đầu), trong đó họ có thể chạy các hợp đồng thông minh (hoặc xử lý các giao dịch đơn giản hơn) với nhau mà không cần tương tác với lớp blockchain bên dưới trong trường hợp tích cực là tất cả bên tham gia đều tuân thủ giao thức. Kênh trạng thái không những giúp giải quyết rất nhanh và thông lượng giao dịch cao; mà còn tốn rất ít dung lượng lưu trữ, vì lịch sử giao dịch ngoài chuỗi có thể bị xóa ngay khi trạng thái kết quả của nó đã được xác minh bằng ‘ảnh chụp’ ngoài chuỗi.

Ngay cả trong trường hợp tệ nhất khi có bất kỳ người tham gia vi phạm, thì hệ thống vẫn được đảm bảo an toàn đầy đủ và nghiêm ngặt. Bất kỳ lúc nào, người tham gia cũng có thể bắt đầu 'đóng trạng thái” người đứng đầu với hiệu ứng là trạng thái của người đứng đầu được chuyển trở lại blockchain (kém hiệu quả hơn). Chúng tôi nhấn mạnh rằng việc thực hiện bất kỳ hợp đồng thông minh nào có thể được duy trì liên tục trên chuỗi. Tiền không được tạo ra và cũng không có người tham gia nào bị mất tiền ngoài chuỗi.

Các kênh trạng thái trong Hydra được xem là đồng cấu trúc, chúng sử dụng định dạng giao dịch và mã hợp đồng giống như lớp blockchain bên dưới, điều này giúp cho các hợp đồng có thể được chuyển trực tiếp qua lại giữa các kênh và blockchain. Nhờ đó, các kênh trạng thái mang lại hiệu quả xử lý song song nhờ nhân bản sổ cái ngoài chuỗi. Cũng có thể ví như sổ cái có thể mọc ra nhiều đầu.

Việc xác nhận giao dịch trong một đầu sẽ được thực hiện cùng lúc bằng quy trình xác thực không đồng bộ ngoài chuỗi sử dụng đa chữ ký. Cơ chế xử lý song song tốc độ cao này được kích hoạt bằng cách sử dụng mô hình UTxO mở rộng ([EUTxO](https://github.com/hydra-supplementary-material/eutxo-spec/blob/master/extended-utxo-specification.pdf)). Trong mô hình EUTxO, các giao dịch sẽ tường minh hơn, cho phép cập nhật trạng thái mà không cần phải đợi từng giao dịch riêng lẻ thực hiện tuần tự.

**Thử nghiệm xác thực giao thức Head**

Ngay từ bước đầu tiên xác thực hiệu suất của giao thức Head bằng thực nghiệm, chúng tôi đã thực hiện một mô phỏng. Từng hành động riêng lẻ được yêu cầu mô phỏng theo thời gian (xác thực giao dịch, xác minh chữ ký, v.v.) và thực hiện mô phỏng thực tế và đúng thời gian của một nhóm các nút phân tán tạo thành phần đầu. Kết quả là tính được thời gian xác nhận giao dịch và thông lượng thực tế.

Chúng tôi thấy rằng một đầu Hydra có thể đạt được khoảng 1.000 TPS, vì vậy bằng cách chạy song song 1.000 đầu (ví dụ: một đầu cho mỗi nhóm cổ phần Shelley), chúng ta sẽ đạt được một triệu TPS. Điều đó thật ấn tượng và giúp chúng ta bỏ xa đối thủ, nhưng tại sao chúng ta phải dừng lại ở đó? 2.000 đầu sẽ cung cấp cho chúng ta 2 triệu TPS - và nếu cần đạt một tỷ TPS, thì chúng ta chỉ cần yêu cầu họ chạy một triệu đầu. Hơn nữa, nhiều cải tiến về hiệu suất trong quá trình triển khai có thể cải thiện phép đo đầu đơn lẻ 1.000 TPS, bổ sung thêm vào hiệu suất giả định của giao thức.

Vì vậy, chúng ta có thể đạt được bất kỳ số TPS nào mà chúng ta muốn không? Về lý thuyết, câu trả lời là chắc chắn có, và điều đó cho chúng ta thấy vấn đề trong việc sử dụng TPS làm thước đo khi so sánh các hệ thống. Mặc dù có xu hướng giảm độ phức tạp của việc đánh giá hiệu suất giao thức xuống một con số duy nhất, nhưng trên thực tế, điều này dẫn đến đơn giản hóa quá mức. Nếu không có bối cảnh khác, số TPS gần như vô nghĩa. Để giải thích nó một cách chính xác và thực hiện so sánh, ít nhất bạn nên yêu cầu kích thước của nhóm (ảnh hưởng đến chi phí giao tiếp); sự phân bố địa lý của nó (xác định lượng thời gian để thông tin chuyển qua hệ thống); chất lượng dịch vụ (thời gian xác nhận giao dịch, cung cấp dữ liệu cho người dùng cuối) bị ảnh hưởng như thế nào bởi tỷ lệ giao dịch cao; mức độ lớn và phức tạp của các giao dịch (có ảnh hưởng đến thời gian xác thực giao dịch, thời gian truyền thông điệp, yêu cầu đối với hệ thống lưu trữ cục bộ và thành phần của những người tham gia chính); loại phần cứng và kết nối mạng nào đã được sử dụng trong các thử nghiệm. Chỉ thay đổi mức độ phức tạp của các giao dịch có thể thay đổi TPS theo hệ số ba, như có thể thấy trong các số liệu trong [bài báo](https://eprint.iacr.org/2020/299) (tham khảo Phần 7 - Mô phỏng).

Rõ ràng, chúng ta cần một tiêu chuẩn tốt hơn. Thiết kế giao thức Head của Hydra có thực sự tốt không? Điều chúng ta cần hỏi là liệu nó có đạt đến giới hạn vật lý của hạ tầng mạng, không phải là một con số TPS đơn thuần. Do đó, đối với việc đánh giá giao thức Head trong vòng đầu, chúng tôi đã sử dụng cách tiếp cận sau để đảm bảo số liệu cung cấp có ý nghĩa hơn:

1. Chúng tôi liệt kê tất cả các tham số ảnh hưởng đến mô phỏng như: quy mô giao dịch, thời gian xác thực giao dịch, thời gian mã hoá, phân bổ băng thông cho mỗi nút, độ lớn của từng phân đoạn, phân bố về mặt địa lý và giới hạn xử lý cấp phát giao dịch song song. Nếu không ràng buộc về môi trường hoạt động, chúng ta sẽ không thể xác định được thông lượng giao dịch.
2. Chúng tôi so sánh hiệu suất của giao thức với các đường hiệu suất cơ sở được xây dựng dựa trên giới hạn chính xác tuyệt đối của nền tảng phần cứng và hạ tầng mạng. Việc xem xét yếu tố giới hạn giúp chúng ta nắm bắt được dư địa còn lại có thể cải tiến thêm. Điều này tuân theo phương pháp được giải thích ở trên bằng cách sử dụng ví dụ về thuật toán mã hóa.

Chúng tôi sử dụng hai đường hiệu suất cơ sở cho Hydra. Đầu tiên, và cũng phổ biến đó là Full Trust: áp dụng cho bất kỳ giao thức nào thực hiện giao dịch giữa các nút và khẳng định rằng mỗi nút lần lượt xác nhận các giao dịch - mà không cần đạt được đồng thuận. Điều này dẫn đến một giới hạn về TPS bằng cách chỉ cần thêm thời gian gửi và xác thực thông điệp. Cách tiếp cận giới hạn này tốt như thế nào cho chúng tôi biết mức giá mà chúng tôi đang trả cho sự đồng thuận, mà không dựa trên sự so sánh với các giao thức khác. Đường cơ sở thứ hai đó là Hydra Unlimited, đạt được ngưỡng TPS dành riêng cho giao thức head cũng như độ trễ và dung lượng lưu trữ lý tưởng. Chúng tôi đạt được ngưỡng đó với giả định có thể gửi đủ số giao dịch đồng thời để phân bổ hoàn toàn thời gian luân chuyển trên mạng và tất cả các hành động có thể được thực hiện khi cần thiết mà không có tranh chấp về tài nguyên. Đường cơ sở giúp chúng tôi trả lời câu hỏi về những gì có thể đạt được trong trường hợp lý tưởng với thiết kế của Hydra (cho một bộ giá trị nhất định của các tham số đầu vào) cũng như đánh giá độ trễ xác nhận và mào đầu lưu trữ so với bất kỳ giao thức nào khác. Có thể xem thêm chi tiết và biểu đồ cho những người quan tâm trong [bài báo](https://eprint.iacr.org/2020/299) của chúng tôi (vẫn là Phần 7 của Mô phỏng).

## **Điều kế tiếp sẽ là gì?**

Giải quyết vấn đề về khả năng mở rộng được xem là chén thánh cho lĩnh vực blockchain. Đã đến lúc phải áp dụng cách tiếp cận dựa trên bằng chứng, có nguyên tắc trong thiết kế các giải pháp kỹ thuật để mở rộng chuỗi khối. So với các giải pháp đề xuất mở rộng khác thì việc sử dụng đường cơ sở đã giúp ích quan trọng trong việc thiết kế giao thức. Nó củng cố cho việc lựa chọn thiết kế giao thức phù hợp cho sổ cái phân tán hiệu quả và cung cấp số liệu gần như tuyệt đối cho các ứng dụng thực tế. Trong khi triển khai thử nghiệm giao thức Head, chúng tôi cũng sẽ nhanh chóng phát hành các phần giao thức còn lại của Hydra với cùng nguyên tắc tiếp cận nói trên.

Điều cuối cùng muốn nói đến, tôi muốn gửi lời cảm ơn những nhà nghiên cứu đã nỗ lực cho Hydra. Đó là Manuel Chakravarty, Sandro Coretti, Matthias Fitzi, Peter Gaži, Philipp Kant và Alexander Russel. Chúng tôi cũng xin cảm ơn Dự án 780477 của EU, PRIVILEDGE đã góp phần hỗ trợ cho chúng tôi.

# Cardano.