Hydro Raindrop

Xác thực công khai trên Blockchain

Tháng 01/2018

Tổng quan:

HYDRO: Nguyên thuỷ từ tiếng Hy Lạp cổ đại – nghĩa là Nước.

Hydro cho phép các hệ thống riêng mới và hiện có tích hợp liền mạch và thúc đẩy các giao dịch bất biến và minh bạch của một blockchain công cộng nhằm nâng cao tính bảo mật, quản lý định danh, giao dịch và trí tuệ nhân tạo của các ứng dụng và tài liệu.

Trong tài liệu này, sẽ mô tả cụ thể cho các hệ thống riêng, chẳng hạn như các API, sử dụng Hydro blockchain công cộng nhằm nâng cao tính bảo mật thông qua xác thực công cộng.

Công nghệ được đề xuất được gọi là "Hạt mưa" - một giao dịch được thực hiện thông qua hợp đồng thông minh xác thực quyền truy cập hệ thống riêng tư công khai và có thể bổ sung các phương thức xác thực riêng đã tồn tại. Công nghệ này được dự định để cung cấp bảo mật bổ sung cho dữ liệu tài chính nhạy cảm ngày càng có nguy cơ bị vi phạm và ăn cắp.

Việc cài đặt ban đầu cho Hydro Raindrop được thực hiện trên nền tảng Hydrogen API. Tập hợp các module API này đã có sẵn cho các doanh nghiệp và nhà phát triển trên toàn cầu để thử nghiệm, xây dựng, kiểm thử và triển khai trên các nền tảng công nghệ và sản phẩm tài chính giả lập.

Hydro Raindrop sẽ được cung cấp cho cộng đồng nhà phát triển thế giới dưới dạng phần mềm nguồn mở, cho phép các nhà phát triển tích hợp Hydro Raindrop với bất kỳ REST API.

Blockchain & Ethereum

Hydro được thực hiện trên mạng Ethereum. Trước khi cung cấp thêm chi tiết về dự án, điều quan trọng là phải hiểu một số ý tưởng cơ bản về blockchain và Ethereum.

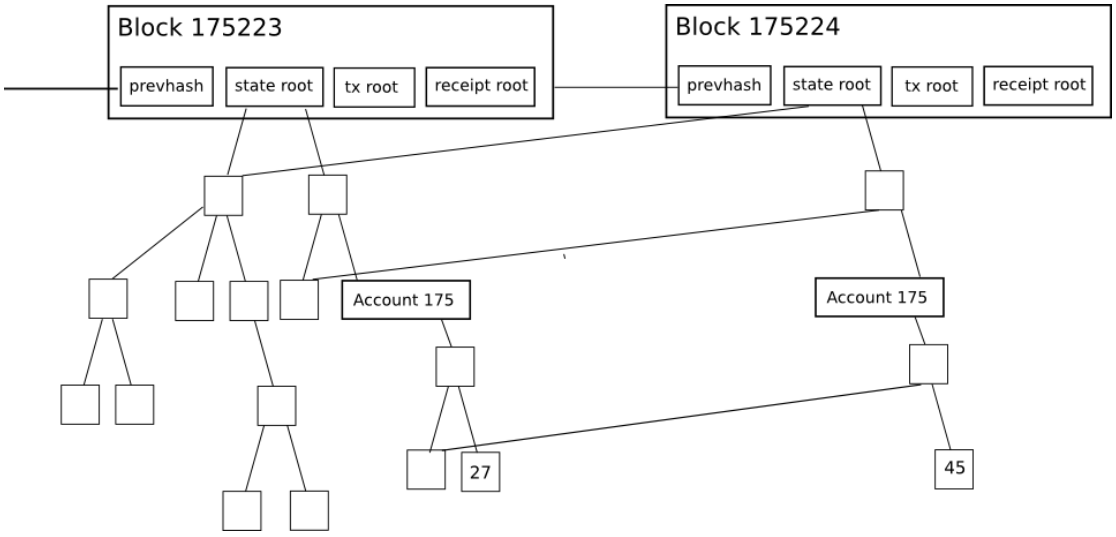
Xây dựng trên Ethereum

Nhiều ứng dụng như Snapchat được xây dựng bằng Swift và các công cụ khác được cung cấp ở trên cùng của nền tảng iOS của Apple, do đó, các ứng dụng blockchain cũng có thể được xây dựng ở trên cùng của Ethereum. Snap Inc. không cần phải xây dựng iOS, họ sử dụng nó làm cơ sở hạ tầng
để khởi chạy một ứng dụng truyền thông làm thay đổi mạng xã hội.

Dự án Hydro cũng tương tự. Nó dựa trên hàng nghìn nhà phát triển trên toàn cầu đang làm việc để làm cho công nghệ blockchain cơ bản nhanh hơn, mạnh hơn và hiệu quả hơn. Hydro tận dụng cơ sở hạ tầng liên tục được cải tiến này bằng cách phát triển sản phẩm tập trung vào các tương tác xung quanh công nghệ blockchain để có thể cung cấp các lợi ích hữu hình cho các ứng dụng dịch vụ tài chính.

Cây Merkle

Cây Merkle được sử dụng trong các hệ thống phân tán nhằm xác minh dữ liệu một cách hiệu quả. Chúng hiệu quả bởi vì chúng sử dụng phương thức băm thay vì các tệp đầy đủ. Băm là cách mã hóa các tệp nhỏ hơn nhiều so với tệp thực tế. Mỗi tiêu đề khối trong Ethereum chứa ba cây Merkle đại diện cho Các giao dịch, Biên nhận và Quốc gia:



Nguồn: [Merkling in Ethereum] ; Vitalik Buterin, Ethereum Founder

Điều này giúp khách hàng dễ dàng nhận được câu trả lời chính xác cho các câu hỏi như là:

- Tài khoản này có tồn tại không?
- Số dư hiện tại là bao nhiêu?
- Giao dịch này có được bao gồm trong một khối cụ thể không?

- Có sự kiện cụ thể nào đã xảy ra trong địa chỉ này hôm nay không?

Hợp đồng thông minh

Một khái niệm chính được kích hoạt bởi Ethereum và các mạng dựa trên blockchain khác là hợp đồng thông minh. Đây là các khối mã tự thực thi mà nhiều thành phần có thể tương tác với nó, coi nó như là người trung gian đáng tin cậy. Đoạn mã trong một hợp đồng thông minh có thể được xem là tương tự như các điều khoản pháp lý trong hợp đồng giấy truyền thống, nhưng có nhiều chức năng mở rộng hơn. Hợp đồng có thể có các quy tắc, điều kiện, hình phạt cho việc không tuân thủ hoặc có thể bắt đầu các quá trình khác. Khi được kích hoạt, các hợp đồng thực hiện các điều khoản đã nêu tại thời điểm triển khai trên chuỗi công khai, cung cấp tính năng tích hợp sẵn các yếu tố bất biến và phân cấp.

Hợp đồng thông minh là một công cụ quan trọng để xây dựng trên cơ sở hạ tầng Ethereum. Chức năng cốt lõi của lớp Hydro blockchain đạt được thông qua tùy chỉnh
hợp đồng, sẽ được thảo luận ở phần sau.

Máy ảo Ethereum

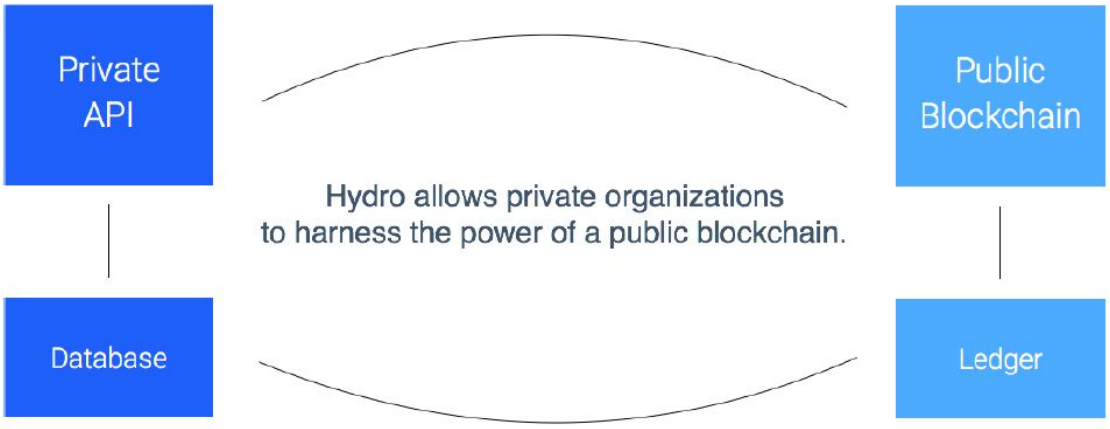
Máy ảo Ethereum (EVM) là môi trường thời gian thực cho hợp đồng thông minh trên Ethereum. EVM giúp ngăn chặn sự tấn công từ chối dịch vụ (DoS), đảm bảo các chương trình duy trì trạng thái ổn định, và cho phép các giao tiếp không thể bị gián đoạn. Các hành động trên EVM có chi phí liên quan đến chúng, được gọi là khí GAS, phụ thuộc vào các nguồn lực tính toán cần thiết. Mỗi giao dịch có lượng khí GAS tối đa được phân bổ cho nó, được gọi là giới hạn khí GAS. Nếu khí tiêu thụ bởi một giao dịch đạt đến giới hạn, nó sẽ chấm dứt việc tiếp tục xử lý.

Sổ cái công khai

<u>Một sổ cái công khai cho các hệ thống riêng</u>

Các hệ thống hỗ trợ nền tảng dịch vụ tài chính, trang web và ứng dụng thường có thể được mô tả dưới dạng phương tiện của luồng dữ liệu - chúng gửi, truy xuất, lưu trữ, cập nhật và xử lý dữ liệu cho các thực thể mà chúng giao tiếp. Bởi vì bản chất của dữ liệu nói riêng và các dịch vụ tài chính nói chung là các hệ thống này thường có những hoạt động phức tạp theo cả hướng độc lập và tập trung. Phụ thuộc vào cấu trúc riêng, thì việc bảo mật, tính minh bạch, và hiệu quả đạt được bằng cách kết hợp các lực lượng bên ngoài vượt quá tầm với của hệ thống nội bộ.

Trong trường hợp sử dụng nền tảng API của Hydrogen. Hydro hướng đến mục đích khai thác những lợi ích nói trên bằng cách cho phép người dùng Hydrogen giao tiếp với một blockchain theo những cách được tích hợp hoàn toàn vào hệ sinh thái riêng Hydrogen.

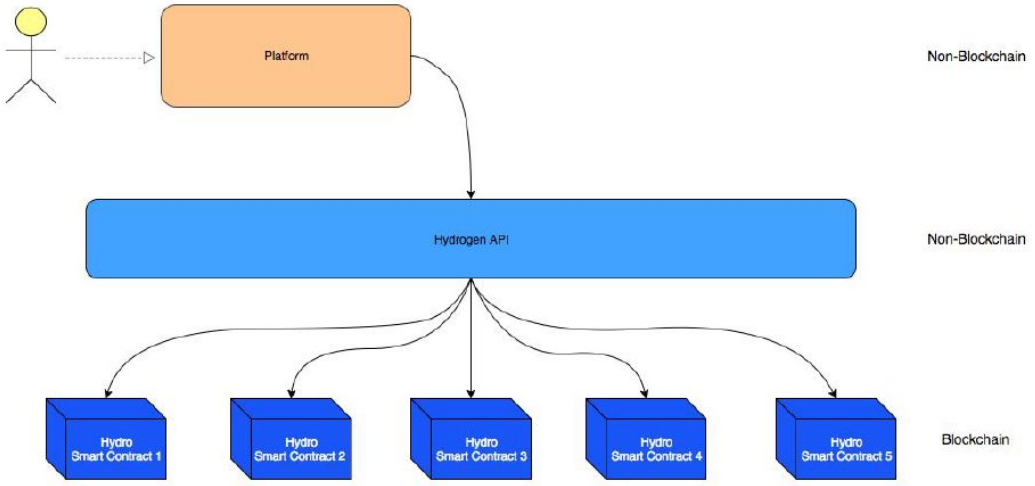


Các hoạt động công khai dựa trên blockchain có thể xảy ra trước, trong hoặc sau hoạt động riêng tư. Sự tương tác giữa các yếu tố riêng tư và công khai có thể phục vụ xác nhận, đóng dấu, ghi lại hoặc tăng cường các quy trình trong một hệ sinh thái.

Đặc tính của mô hình này đang làm cho các quy trình trở nên mạnh mẽ hơn bằng cách khai thác lợi ích của công nghệ blockchain đặc biệt nó có thể tạo ra nhiều nhất tác động tích cực. Mặc dù framework này có thể không áp dụng được cho tất cả nền tảng, vì vậy Hydro tập trung vào việc cung cấp giá trị cho các trường hợp trong đó.

Kiến trúc cho việc áp dụng

Hydro khác với nhiều sáng kiến blockchain hiện có, bởi vì nó có thể tồn tại độc lập và bọc xung quanh hệ thống mới hoặc hiện có mà không yêu cầu thay đổi hệ thống. Thay vì thay thế, Hydro hướng đến việc tăng thêm. Nền tảng và các tổ chức có sử dụng API Hydrogen có thể tự động truy cập vào blockchain.



Phạm vi của các nền tảng dịch vụ tài chính có thể tận dụng Hydro là rộng lớn. Những nền tảng này có thể cung cấp hầu hết mọi trải nghiệm, bất kỳ số lượng các dịch vụ độc quyền, thực hiện bất kỳ hoạt động dữ liệu riêng tư và triển khai trong bất kỳ môi trường. Điều này được kích hoạt bởi module hoá cấu trúc của Hydrogen và là
hiệp đồng với Hydro, hoạt động như việc đề nghị bổ sung trình điều khiển.

Raindrop

Được xây dựng trên sổ cái công khai Hydro làmột dịch vụ xác thực dựa trên blockchain, được gọi là "Hạt mưa". Điều này cung cấp một sự khác biệt, bất biến, lớp bảo mật toàn cầu có thể xem được để xác minh yêu cầu truy cập đến từ một nguồn được ủy quyền.

Giao thức xác thực riêng tư như OAuth 2.0 cung cấp các cấp độ khác nhau của sự mạnh mẽ và hữu ích cho trường hợp cụ thể đã tồn tại. Ở đây cần phải hoàn thiện thêm một chút nữa hoặc hoặc cố gắng thay thế các giao thức này - Hydro
cung cấp một cách để tăng cường chúng bằng cách kết hợp các cơ chế blockchain như một thành phần của một thủ tục xác thực. Điều này có thể thêm một lớp bảo mật hữu ích để giúp ngăn chặn các truy cập phạm pháp vào hệ thống nhằm đánh cắp dữ liệu. Trước khi xem xét các khía cạnh kỹ thuật của Raindrop, trước tiên hãy xem
vấn đề nó đang cố gắng giải quyết.

Tình trạng an ninh tài chính

Sự gia tăng của thời đại dữ liệu đã mang đến nỗi lo về việc mất cắp dữ liệu, điều này đặc biệt quan trọng đối với các dịch vụ tài chính. Nền tảng tài chính thường à cổng vào số lượng lớn dữ liệu riêng tư và nhạy cảm như Số ID, thông tin đăng nhập tài khoản và lịch sử giao dịch. Bởi vì những dữ liệu này rất quan trọng, các truy cập không được bảo vệ thường được để lại hậu quả thật nặng nề.

Công ty nghiên cứu công nghiệp Trend Micro đã công bố một báo cáo tìm thấy đường dây đánh cắp các mục Thông tin nhận dạng cá nhân (PII) được bán trên Deep Web với giá ít nhất là $ 1, quét các tài liệu như hộ chiếu với giá ít nhất là $ 10 và thông tin đăng nhập ngân hàng có giá là $ 200, làm cho việc phân phối các dữ liệu bị đánh cắp ngày càng bị phân mảnh và không thể truy cập được.

Thật không may, hệ thống tài chính hiện tại không có một hồ sơ theo dõi chi tiết khi nói đến việc ngăn chặn, chẩn đoán và truyền đạt các vi phạm dữ liệu với các bên liên quan của nó.

- Theo một nghiên cứu gần đây của Javelin Strategy & Research – Nghiên cứu gian lận danh tính 2017 - 16 tỷ đô la đã bị đánh cắp từ 15,4 triệu người tiêu dùng Mỹ trong năm 2016 do thất bại của hệ thống tài chính để bảo vệ Thông tin nhận dạng cá nhân (PII).
- Vào tháng 4 năm 2017, Symantec đã công bố Báo cáo về mối đe dọa bảo mật Internet của mình, ước tính 1,1 tỷ phần PII đã bị truy cập trái phép ở nhiều mức độ khác nhau trong suốt năm 2016.
- Trong tài liệu Vi phạm dữ liệu cuối năm 2016 của Risk Based Security cho biết có 4.149 vụ vi phạm dữ liệu xảy ra trong các doanh nghiệp toàn cầu vào năm 2016, phơi bày hơn 4,2 tỷ bản ghi.
- Báo cáo Thales Data Threat năm 2017 - Phiên bản dịch vụ tài chính, khảo sát các chuyên gia CNTT toàn cầu trong các dịch vụ chuyên nghiệp, thấy rằng 49% các tổ chức dịch vụ tài chính đã bị vi phạm an ninh trong quá khứ, 78%

đang chi tiêu nhiều hơn để tự bảo vệ mình, nhưng 73% là tung ra các sáng kiến mới liên quan đến công nghệ AI, IoT và đám mây trước khi chuẩn bị các giải pháp bảo mật thích hợp.

Vi phạm Equifax

Vào ngày 29 tháng 7 năm 2017, Equifax, một cơ quan báo cáo tín dụng Hoa Kỳ - thành lập được 118 năm, đã bị tấn công. Dữ liệu của 143 triệu người tiêu dùng có PII đã bị rò rỉ, bao gồm cả Số An Sinh Xã Hội. 209.000 khách hàng đã bị xâm phạm dữ liệu thẻ tín dụng.

Nguyên nhân của sự vi phạm này là gì?

Bắt đầu với một trong những công nghệ phụ trợ được sử dụng bởi Equifax. Struts là một framwork nguồn mở để phát triển các ứng dụng web bằng ngôn ngữ lập trình Java, được xây dựng bởi Apache Software Foundation. CVE-2017-9805 là một lỗ hổng trong Apache Struts liên quan đến việc sử dụng plugin Struts REST với trình xử lý XStream để xử lý các payload XML. Nếu bị khai thác, nó cho phép những kẻ tấn công điều khiển từ xa không cần xác thực để chạy mã độc trên máy chủ ứng dụng đến hoặc là khởi động thêm các cuộc tấn công từ nó. Bản vá bởi Apache được đưa ra hai tháng trước cuộc tấn công Equifax.

Apache Struts chứa một lỗ hổng trong XStream của REST Plugin được kích hoạt như
chương trình không tuần tự hóa tuần tự đầu vào do người dùng cung cấp trong các yêu cầu XML. Cụ thể hơn, sự cố xảy ra trong phương thức toObject () của XStreamHandler không áp đặt bất kỳ hạn chế nào đối với giá trị đầu vào khi sử dụng Xstream deserialization vào một đối tượng, dẫn đến lỗ hổng thực thi mã tùy ý.

Ngay cả khi REST plugin này đã bị xâm nhập, nó có quan trọng không? Có phải là có một cách sử dụng công nghệ blockchain để bảo mật thông tin tài chính của 143 triệu khách hàng trong khi vẫn dựa vào REST API hiện tại và các hệ thống dựa trên Java?

Thêm một lớp Blockchain

Rõ ràng là tính toàn vẹn của các cổng dữ liệu tài chính có thể được cải thiện.
Hãy xem xét làm thế nào để có thêm một lớp bảo mật thông qua Hydro.

Các cơ chế đồng thuận cơ bản của mạng Ethereum đảm bảo tính hiệu lực giao dịch vì người tham gia thu thập xử lý các giao dịch chung được xác nhận. Thực tế này dẫn đến phân cấp và bất biến, nhưng, quan trọng hơn, nó cung cấp một vector để giảm thiểu truy cập trái phép vào một cổng xử lý dữ liệu nhạy cảm.

Với Hydro, xác thực có thể được xác định dựa trên các hoạt động giao dịch trên blockchain. Ví dụ, một API có thể chọn xác thực nhà phát triển và ứng dụng bằng cách yêu cầu họ bắt đầu các giao dịch cụ thể, với các tải trọng dữ liệu cụ thể, giữa các địa chỉ cụ thể trên blockchain, như một điều kiện tiên quyết khởi động một giao thức xác thực tiêu chuẩn.

Hydro Raindrop

Mưa chứa các gói nước ngưng tụ có đường kính từ 0,0001 đến 0,005 cm. Trong một cơn mưa bình thường, có hàng tỷ các gói dữ liệu, mỗi kích thước, vận tốc và hình dạng ngẫu nhiên. Do đó, người ta không thể dự đoán chính xác bản chất của mưa. Tương tự, mọi giao dịch xác thực Hydro là duy nhất và hầu như không thể xảy ra
tình cờ - đó là lý do tại sao chúng tôi gọi chúng là hạt mưa.

Các nền tảng dịch vụ tài chính thường sử dụng công cụ xác minh tiền gửi vi mô để xác nhận tài khoản khách hàng. Khái niệm rất đơn giản: nền tảng chia khoản tiền gởi ngẫu nhiên vào tài khoản ngân hàng được xác nhận quyền sở hữu của người dùng. Để chứng minh người dùng thực sự sở hữu tài khoản đã nói, họ phải chuyển tiếp khoản tiền gửi số tiền trở lại nền tảng, tại đó chúng được xác thực. Cách duy nhất người dùng có thể biết số tiền hợp lệ (ngoài việc đoán) là bằng cách truy cập vào tài khoản ngân hàng.

Xác minh dựa trên Raindrop với Hydro tương tự. Thay vì gửi người sử dụng một số tiền và chờ phản hồi chuyển tiếp trở lại, chúng tôi xác định một giao dịch và người sử dụng phải thực thi nó từ một chiếc ví có sẵn. Cách duy nhất để người dùng có thể tiến hành giao dịch hợp lệ là bằng cách truy cập vào ví.

Bằng cách sử dụng Raindrops, cả hệ thống và người truy cập đều có thể theo các truy cập xác thực trên sổ cái công khai bất biến. Giao dịch dựa trên blockchain này là
tách rời khỏi các hoạt động hệ thống cơ bản, xảy ra trên một mạng phân tán, và tùy thuộc vào quyền sở hữu khóa riêng tư. Do đó, nó phục vụ như một công cụ xác thực hữu ích.

Góc nhìn chi tiết

Có bốn thực thể tham gia vào quá trình xác thực Hydro:

1. *Accessor* - Bên cố gắng truy cập vào một hệ thống. Trong trường hợp của Hydrogen, người truy cập là một tổ chức tài chính hoặc ứng dụng sử dụng API Hydrogen cho cơ sở hạ tầng kỹ thuật số cốt lõi của nó.
2. *System* - Hệ thống hoặc cổng giao tiếp đang được Accessor truy cập. Đối với Hydrogen, hệ thống là chính Hydrogen API.
3. *Hydro* - Các mô-đun được sử dụng bởi hệ thống để giao tiếp với blockchain.
4. *Blockchain* - Sổ cái công khai phân tán xử lý các giao dịch HYDRO và chứa các hợp đồng thông minh Hydro, qua đó thông tin có thể được đẩy, kéo hoặc hoạt động theo cách khác.

Mỗi Raindrop, là một thực thể gồm năm thông số giao dịch:

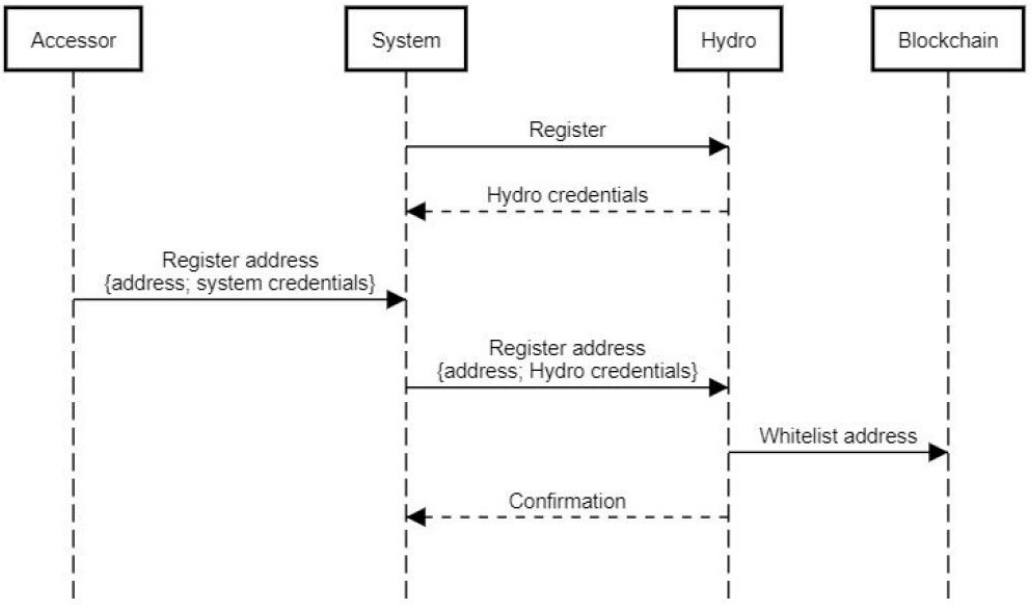
1. *Sender* - Địa chỉ khởi tạo giao dịch.
2. *Receiver* - Đích đến của giao dịch. Điều này tương ứng với việc gọi một phương thức trong hợp đồng thông minh Hydro.
3. *ID* - Mã định danh được liên kết với Hệ thống.
4. *Quantity* - Số lượng HYDRO cần gửi.
5. *Challenge* - Chuỗi ký tự chữ và số được tạo ngẫu nhiên.

Dưới đây là một phác thảo về quy trình xác thực, nói chung được phân thành ba giai đoạn:

1. Khởi tạo
2. Raindrop
3. Tính hợp lệ

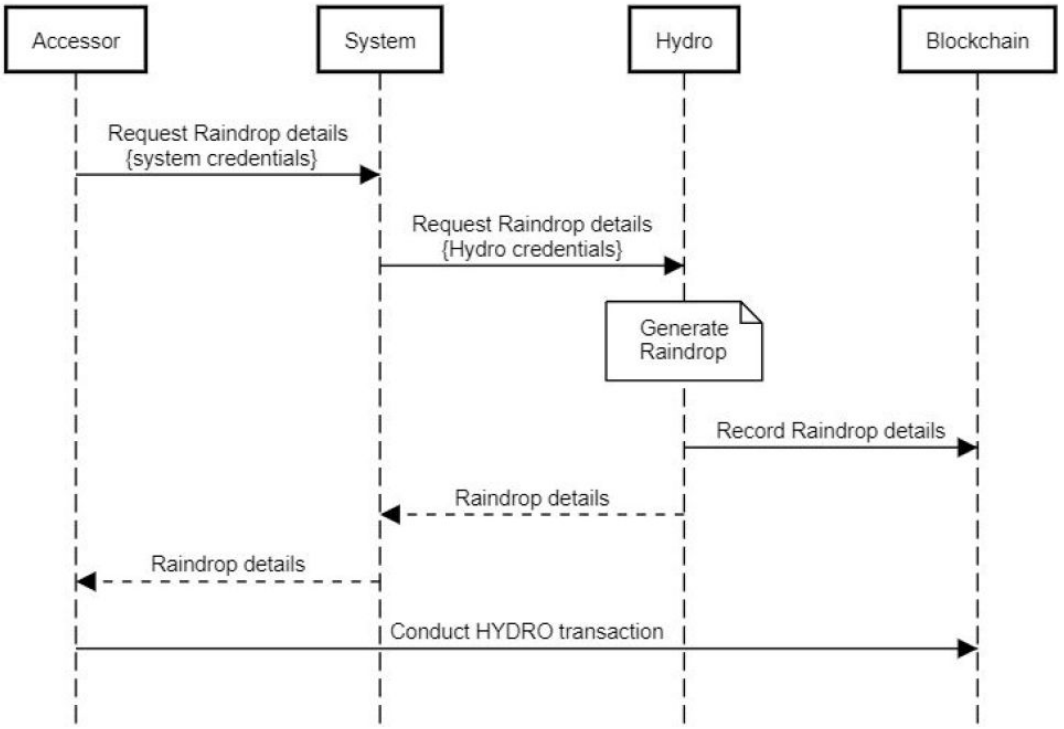
Bắt đầu khởi tạo với System (ví dụ: Hydrogen) đăng ký sử dụng Hydro và lấy thông tin xác thực, cho phép hệ thống giao tiếp với blockchain qua mô-đun Hydro. System tích hợp một Accessor (ví dụ: tổ chức tài chính) đăng ký địa chỉ công cộng và sau đó chuyển địa chỉ đã đăng ký với Hydro. Địa chỉ này được ghi vào blockchain tới một danh sách trắng được lưu trữ trong một hợp đồng thông minh Hydro. Hệ thống nhận được xác nhận rằng địa chỉ đã được đưa vào danh sách trắng, cũng có thể được xác minh là một sự kiện có thể xem công khai. Chỉ cần đăng ký hệ thống một lần, trong khi danh sách trắng Accessor chỉ xuất hiện một lần cho mỗi Accessor.

Xác thực với Hydro: Khởi tạo



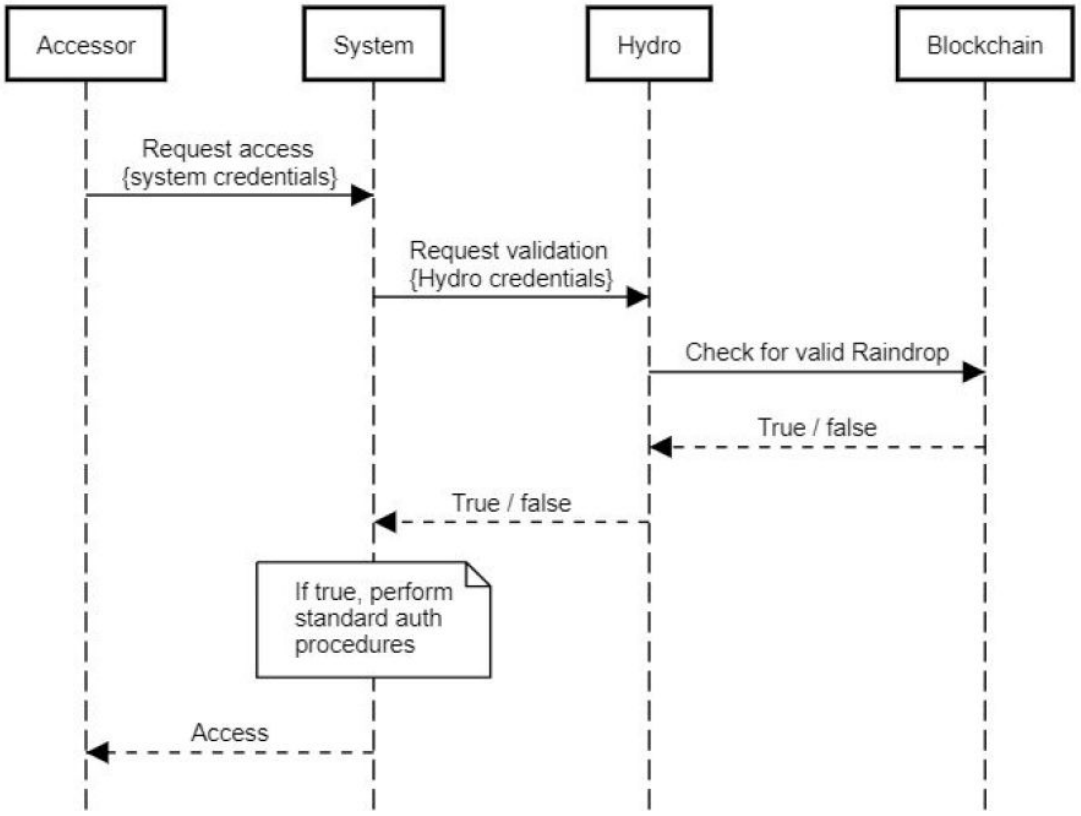
Sau khi khởi tạo xong, cốt lõi của quá trình xác thực Hydro có thể bắt đầu. Các Accessor, người phải thực hiện một giao dịch Raindrop, nhảy đến quá trình này bằng cách yêu cầu chi tiết Raindrop từ System và System định tuyến yêu cầu tới Hydro. Hydro tạo ra một Raindrop mới, lưu trữ một số chi tiết bất biến trên blockchain và trả về chi tiết đầy đủ cho Accessor thông qua System. Accessor, được trang bị tất cả thông tin bắt buộc, tiến hành giao dịch từ địa chỉ đã đăng ký tới một phương thức trong hợp đồng thông minh Hydro. Nếu địa chỉ không có trong danh sách trắng, hành động bị từ chối - còn không, nó được ghi lại trong hợp đồng thông minh. Điều quan trọng cần lưu ý là giao dịch này sẽ xảy ra bên ngoài System, trực tiếp từ Accessor đến Blockchain, vì nó phải được ký với khóa riêng của Accessor (mà chỉ có Accessor mới có thể có được).

Xác thực với Hydro: Raindrop



Bước cuối cùng của quy trình là Xác thực. Trong bước này, Accessor chính thức yêu cầu truy cập vào System thông qua hệ thống cơ chế đã được thiết lập. Trước khi triển khai bất kỳ giao thức xác thực chuẩn nào của nó, System hỏi Hydro rằng Accessor đã thực hiện giao dịch Raindrop hợp lệ hay không. Các giao tiếp Hydro với hợp đồng thông minh thực hiện kiểm tra tính hợp lệ và phản hồi với chỉ định đúng / sai. System có thể quyết định cách nó nên tiến hành dựa trên chỉ định này - nếu nó là sai, System có thể từ chối truy cập và nếu đúng, System có thể cấp quyền truy cập.

Xác thực với Hydro: Tính hợp lệ



Nếu chúng ta xem xét thông tin đăng nhập của System cơ bản - hoặc bất kỳ System hiện có nào mà giao thức được kết nối là một yếu tố xác thực, là quan trọng thì lớp Hydro cung cấp sẽ là một nhân tố quan trọng thứ hai. Bằng cách kiểm tra hai hướng ảnh hưởng chính này, chúng ta có thể dễ dàng xác nhận tính hữu dụng của nó:

- Hướng 1 - Kẻ tấn công đánh cắp thông tin xác thực hệ thống cơ sở của Accessor
    - Kẻ tấn công cố gắng truy cập vào Hệ thống với thông tin xác thực hợp lệ.
    - Kiểm tra hệ thống với Hydro để xác định xem có phải là một giao dịch hợp lệ được thực hiện trên blockchain hay không.
    - Hydro trả về false và hệ thống từ chối truy cập
- Hướng 2 - Kẻ tấn công đánh cắp (các) khóa riêng tư truy cập vào ví của Accessor
    - Kẻ tấn công cố gắng thực hiện giao dịch Hydro từ địa chỉ đã đăng ký, không cần chi tiết về Raindrop

- Kẻ tấn công không thể thực hiện một giao dịch blockchain hợp lệ
- Kẻ tấn công cũng không thể yêu cầu quyền truy cập vào Hệ thống mà không có thông tin đăng nhập hệ thống phù hợp

Rõ ràng là Kẻ tấn công phải ăn cắp cả thông tin đăng nhập hệ thống cơ bản và (các) khóa ví riêng của Accessor mới có thể truy cập vào Hệ thống. Về vấn đề này, Hydro đã thêm thành công một yếu tố xác thực bổ sung.

Mở Raindrop cho công đồng

Mặc dù dịch vụ xác thực dựa trên blockchain này được kiến trúc để trợ giúp an toàn hệ sinh thái Hydrogen API, nó được áp dụng rộng rãi cho các hệ thống khác nhau nền tảng và hệ thống. Bởi vì chúng tôi cảm thấy rằng những người khác có thể có lợi từ lớp xác minh này, chúng tôi đang mở công khai nó để mọi người sử dụng.

Cũng giống như Hydrogen sẽ tích hợp nó như một điều kiện tiên quyết để truy cập vào API của hệ sinh thái, vì vậy cũng có thể có bất kỳ hệ thống nào thêm nó vào các thủ tục và giao thức hiện có. Bất kỳ nền tảng nào - có thể là API, ứng dụng, phần mềm doanh nghiệp, nền tảng trò chơi, v.v. - có thể sử dụng Hydro cho mục đích xác thực. Tài liệu chính thức sẽ có sẵn trên GitHub cho những ai muốn kết hợp blockchain này đưa vào framework xác thực hoặc REST API.

Case Study - Raindrop với OAuth 2.0

Có rất nhiều cách mà bản phát hành Raindrop có thể được sử dụng bởi các tổ chức riêng. Các API, cơ sở dữ liệu và mạng riêng tư đã tạo ra các hệ thống thẻ, khóa, ứng dụng và giao thức phức tạp trong thập kỷ qua, trong việc cố gắng bảo mật dữ liệu nhạy cảm. Ví dụ như Google, đã trở thành một trong những các nhà cung cấp sản phẩm phổ biến trên thị trường với ứng dụng Google Authenticator. Như đã đề cập trước đó, có rất ít hoặc không có lý do để cạnh tranh với hoặc thay thế các giao thức hiện có này.
Như một nghiên cứu điển hình, đây là một tổng quan ngắn gọn về cách Hydrogen cài đặt xác thực Hydro như là lớp bảo mật tổng thể trong framework bảo mật API của nó:

1. Các đối tác API Hydrogen trước tiên phải có địa chỉ IP của các môi trường được đưa vào danh sách trắng.
2. Đối tác phải yêu cầu đưa một địa chỉ Hydro công khai vào danh sách trắng.
3. Tất cả các cuộc gọi đến API Hydrogen và chuyển dữ liệu được mã hóa và được truyền qua giao thức HTTPS.
4. Đối tác phải hoàn tất giao dịch raindrop Hydro hợp lệ từ địa chỉ Hydro đã đăng ký.
5. Đối tác phải sử dụng xác thực OAuth 2.0. OAuth (Open Authorization) là một tiêu chuẩn mở cho xác thực và ủy quyền dựa trên token. Hydrogen hỗ trợ “Resource Owner Password Credentials” và “Client Credentials” và mỗi người dùng API phải cung cấp thông tin xác thực cho một yêu cầu xác thực.
6. Nếu không có yếu tố nào ở trên bị vi phạm, thì đối tác Hydrogen được cấp một token duy nhất, nó sẽ được kiểm tra và xác minh với mỗi lệnh gọi API.

7. Token có giá trị trong 24 giờ, sau đó đối tác phải xác thực một lần nữa.

Nếu bất kỳ bước nào trong số này bị vi phạm, người dùng sẽ bị khóa quyền truy cập API ngay lập. Một hacker không thể bỏ qua các yếu tố bảo mật này bằng cách đoán ngẫu nhiên, bởi vì có hàng tỷ tỷ kết hợp độc đáo.

Hydro blockchain dựa trên xác thực là một thành phần quan trọng của giao thức bảo mật Hydrogen. Nhóm Hydrogen khuyến khích các đối tác thành lập ví đa chữ ký và lưu trữ khóa cá nhân ở nhiều vị trí an toàn độc lập với các thông tin khác, vì thế sẽ không có một điểm duy nhất thất bại. Ví đa chữ ký được bảo mật đúng cách không chỉ khó ăn cắp, mà bản chất công cộng của blockchain cũng cho phép nhanh chóng nhận ra bất kỳ hành vi trộm cắp nào vì nó liên quan đến sự an toàn của API.

Bất kỳ ai cũng có thể xem những cố gắng truy cập đến hợp đồng thông minh Hydro, có nghĩa là những ngày đầu của nền tảng bị xâm phạm trong nhiều tháng từ đầu đến cuối. Tin tặc API giờ đây có thể bị cản trở với tính năng nhanh hơn vì khả năng phát hiện các nỗ lực ủy quyền không mong muốn trong thời gian thực, từ mọi nơi trên thế giới.

Rủi ro

Giống như bất kỳ công nghệ mới, chẳng hạn như những ngày đầu của truyền thông xã hội, email và các ứng dụng phát trực tuyến (phụ thuộc vào kết nối quay số), điều quan trọng là nhóm phát triển cốt lõi theo dõi chặt chẽ những phát triển mới về tốc độ và khối lượng giao dịch bằng Ethereum. Bạn có thể tưởng tượng YouTube cố gắng khởi chạy vào năm 1995? Hoặc Instagram lần đầu tiên được cung cấp trên Blackberry?

Các nhà phát triển cốt lõi Ethereum như Vitalik Buterin và Joseph Poon đã đề xuất Plasma: Các hợp đồng thông minh tự trị có thể mở rộng nâng cấp lên giao thức Ethereum:

> Plasma là một framework được đề xuất cho việc khuyến khích thực thi bắt buộc của các hợp đồng thông minh mà có thể mở rộng đến một số lượng đáng kể trạng thái cập nhật mỗi giây (có thể là hàng tỷ) cho phép blockchain có thể trở thành đại diện cho một lượng đáng kể các ứng dụng tài chính phi tập trung trên toàn thế giới. Những hợp đồng thông minh này được khuyến khích tiếp tục hoạt động độc lập thông qua phí giao dịch mạng, là cuối cùng dựa vào blockchain cơ bản (ví dụ: Ethereum) để thực thi chuyển tiếp trạng thái giao dịch.

Những người khác, chẳng hạn như The Raiden Network, đã đề xuất một giải pháp mở rộng chuỗi được thiết kế để tạo sức mạnh cho các giao dịch nhanh hơn và chi phí thấp hơn. Tại thời điểm này, Raindrop không làm ảnh hưởng nhiều trên nền tảng Ethereuem, do đó khả năng mở rộng là một rủi ro rất nhỏ đối với sự thành công của công nghệ.

Kết luận

Tính bất biến của blockchain công cộng cung cấp những cách thức mới để tăng cường tính bảo mật của các hệ thống riêng như API.

Tài liệu này đã chỉ ra ba điều quan trọng:

1. Blockchains công cộng có thể tăng thêm giá trị trong các dịch vụ tài chính.
2. Hydro Raindrop có thể tăng cường an ninh cho hệ thống cá nhân.
3. Có các ứng dụng sẵn của Hydro Raindrop trong nền tảng API Hydro.

Nhóm Hydro tin rằng framework được đặt ra có thể là tiêu chuẩn bảo mật cơ sở hạ tầng cho một mô hình mới của hệ thống công cộng-riêng tư, sẽ đem lại lợi ích cho tất cả các bên liên quan trong ngành dịch vụ tài chính và hơn thế nữa.

Nguồn:
Ethereum; Merkling in Ethereum
Trend Micro; What Do Hackers Do With Your Stolen Identity?
Javelin Strategy & Research; The 2017 Identity Fraud Study
Symantec; Internet Security Threat Report
Risk Based Security; 2016 Data Breach Trends - Year in Review
Thales; 2017 Thales Data Threat Report – Financial Services Edition
Apache.org; Apache Struts 2 Documentation - S2-052
Joseph Poon and Vitalik Buterin; Plasma: Scalable Autonomous Smart Contracts