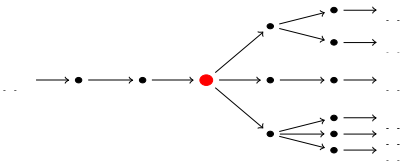
Bản thể luận cho hợp đồng thông minh

Darryl McAdams
Input Ouyput Hong Kong
Email: darryl.mcadams@iohk.io

I. GIỚI THIỆU

Bài viết này giới thiệu một bản thể luận cơ bản cố gắng nắm bắt các tính năng thiết yếu của nhiều hợp đồng thông minh, nhằm hỗ trợ lập luận chính thức về hành vi của chúng. Phần II cung cấp tổng quan chung về bản thể luận được đề xuất và Phần III đưa ra các phân tích về một số hợp đồng thông minh thú vị từ tài liệu, thông qua lăng kính của bản thể luận này. Các đề xuất ở đây không nhằm mục đích trở thành Một bản thể luận đúng duy nhất, mà là một bản thể luận hữu ích. Một Blockchain được thiết kế tốt sẽ có thể hỗ trợ các bản thể luận tùy ý như vậy.



Hình 1. Mối quan hệ giữa các trạng thái. Hiện tại là chấm lớn hơn màu đỏ. Mũi tên đại diện cho các sự kiện chuyển trạng thái này sang trạng thái khác, tạo ra khái niệm về thời gian.

II. BẢN THỂ LUẬN

Bản thể luận là một tập hợp khái niệm (hoặc loại, kiểu) được coi là cách cơ bản nhất để xem một tập hợp vấn đề và các mối quan hệ giữa chúng. Trong bối cảnh vật lý hạt nhân, bản thể luận là Mô hình Chuẩn của các hạt và các trường liên kết khác nhau.

Trong bối cảnh hợp đồng thông minh, một số khái niệm phát sinh lặp đi lặp lại, tạo thành bản thể luận của lĩnh vực này. Bài nghiên cứu này giả định rằng các hợp đồng thông minh về cơ bản là các phép tính trạng thái bao gồm một số giá trị trạng thái thay đổi theo thời gian và một hàm chuyển đổi cố định, không thay đổi. Chính xác những gì cấu thành một trạng thái và có bao nhiêu trạng thái, hoàn toàn phụ thuộc vào hợp đồng thông minh và có thể đơn giản như một Token đại diện cho một trạng thái trong một máy trạng thái hữu hạn (ví dụ: q_3) hoặc nó có thể là một phần dữ liệu tượng trưng phong phú hơn.

Bản thể luận cung cấp các khái niệm để suy nghĩ về các hợp đồng như vậy, được trừu tượng hóa qua các chi tiết dành riêng cho hợp đồng hoặc trực giao với hành vi vĩ mô và như sau:

Đại lý Đại lý là người tham gia hợp đồng, cho dù điều đó có nghĩa là một người, một tổ chức, một phần mềm hay thứ gì khác. Đại lý thực hiện các hành động ảnh hưởng đến trạng thái của hợp đồng.

Sự kiện Sự kiện là sự chuyển tiếp từ trạng thái này sang trạng thái khác. Các sự kiện được đưa ra bởi các Đại lý gọi chức năng chuyển tiếp ở trạng thái gần đây nhất.

Đối tượng Đối tượng là thứ được điều khiển bởi hợp đồng thông minh và có thể được chuyển giao giữa các Đại lý. Ai có thể điều khiển nó và làm thế nào được xác định bởi hợp đồng. Một số Đối tượng có thể có các ràng buộc về việc sử dụng, chẳng hạn như đối tượng có thể chuyển giao chúng (ví dụ: "thẻ quà tặng" chỉ có thể được chi tiêu tại một số nhà bán lẻ nhất định).

Thời gian Thời gian là khái niệm về thời gian ngoài đời thực, trôi qua với tốc độ độc lập với Blockchain. Nó khác với trật tự trước-sau nội bộ mà các Blockchain tồn tại để tạo ra. Thời gian là thời gian dương lịch.

Phương thức Các phương thức là hiện tượng bậc cao mô tả mối quan hệ giữa các trạng thái trong tổng thể của những gì có thể về mặt logic. Các phương thức định lượng các trạng thái trong quá khứ hoặc tương lai liên quan đến một trạng thái hiện tại nhất định và cho phép các khái niệm về khả năng, sự cần thiết, v.v. Các 2 loại phương thức chính:

Dọc Phương thức dọc định lượng trên các tương lai thay thế tương thích với trạng thái nhất định ở hiện tại. Các khái niệm như “phải” và “có thể” về cơ bản là theo phương thức dọc vì chúng chỉ mô tả sự tồn tại hoặc không tồn tại của một số loại sự kiện. Một điều “phải” xảy ra nếu mọi tương lai đều có điều đó xảy ra, trong khi nó “có thể” xảy ra nếu ít nhất một tương lai nó xảy ra.

Ngang Phương thức Ngang, cũng có thể được gọi là Phương thức Thời gian, định lượng theo trình tự các trạng thái. Các khái niệm như “cuối cùng” và “không bao giờ” về cơ bản là phương thức ngang vì chúng mô tả cấu trúc bên trong của các hợp đồng tượng lai thay thế. Một điều gì đó “cuối cùng” sẽ xảy ra nếu nó xảy ra trong một tương lai nào đó, nhưng có thể chỉ sau khi nhiều sự kiện đã diễn ra. Một cái gì đó "không bao giờ" xảy ra nếu không có một số sự kiện mà sau đó nó xảy ra.

Thuật ngữ “Dọc” và “Ngang” xuất phát từ trực quan hóa. Chúng ta có thể tưởng tượng rằng một chuỗi các chuyển đổi trạng thái giống như một dòng thời gian được sắp xếp từ trái sang phải, như trong Hình 1. Tại bất kỳ trạng thái cụ thể nào, có một quá khứ kéo dài sang trái và nhiều loại tương lai kéo dài sang phải. Mỗi tương lai có liên quan về mặt hình học với trạng thái đó bằng cách bù theo chiều ngang từ nó, nhưng được bù theo chiều dọc so với các tương lai khác của trạng thái đó. Thậm chí có thể xảy ra trường hợp một trạng thái có nhiều quá khứ, vì có thể có nhiều cách để đến trạng thái đó.

Một số thứ khác có liên quan đến bản thể luận, nhưng được coi là cơ bản hơn trong bài nghiên cứu này, là các khái niệm như thông tin, kiến thức, danh tính, bí mật và xác minh. Đây là tất cả các khái niệm liên quan đến lý thuyết thông tin và giao thức mật mã, và lý luận về chúng là vô cùng khó khăn. Ngoài ra còn có một tài liệu đáng kể về chủ đề đó, có thể cung cấp một bộ công cụ tốt hơn so với bài nghiên cứu này.

III. PHÂN TÍCH HỢP ĐỒNG THÔNG MINH

Phần này phân tích một số hợp đồng thông minh từ tài liệu. Đây không phải là một tổng quan toàn diện về đầy đủ các cách để áp dụng bản thể luận này, cũng như các hợp đồng thông minh. Thay vào đó, nó nhằm mục đích đưa ra một số trực giác về cách áp dụng bản thể luận và cách nó có thể được sử dụng để mô tả các thuộc tính dẫn đến lỗi khi chúng không giữ được.

A. Giao dịch đơn giản

Trong giao dịch đơn giản, Người gửi chuyển quyền kiểm soát một Vật phẩm, thường là một dạng tiền nào đó, cho một người tham gia khác, Người nhận đã biết trước khi gửi. Theo cách hiểu thông thường của Giao dịch, điều này liên quan đến việc Người gửi cấp cho Người nhận khả năng tiếp tục xử lý vật phẩm theo ý muốn của họ.

Sử dụng bản thể luận, chúng ta có thể xác định Người gửi và Người nhận là Đại lý, Vật phẩm là Đối tượng, và Giao dịch là Sự kiện, giúp chuyển hệ thống sang trạng thái mà Người nhận có khả năng độc quyền để tiếp tục chuyển tiếp Vật phẩm.

Khả năng độc quyền của Người nhận để tiếp tục sử dụng Vật phẩm tạo thành chất lượng phương thức của hệ thống. Cụ thể, chúng ta muốn Người nhận *có thể* sử dụng Vật phẩm là sự thật. Vì vậy, chúng ta muốn đúng là đối với bất kỳ loại Sự kiện nào có thể do Người nhận khởi xướng và liên quan đến Vật phẩm đều có thể được khởi tạo từ trạng thái kết quả đó. Hơn nữa, tính độc quyền của khả năng này có nghĩa là chúng ta muốn đúng là không có Tác nhân nào khác có thể bắt đầu bất kỳ loại Sự kiện nào liên quan đến Vật phẩm từ trạng thái kết quả đó.

B. Giao dịch có nhiều người gửi

Giao dịch nhiều người gửi giống như Giao dịch đơn giản, ngoại trừ việc có nhiều người gửi tham gia. Mỗi Người gửi phải ủy quyền Giao dịch, điều này thường xảy ra thông qua một chuỗi Sự kiện thu thập các ủy quyền riêng lẻ thành một trạng thái tổng hợp. Do đó, chúng ta có một cặp thuộc tính phương thức được yêu cầu.

Đối với bất kỳ trạng thái không phải là cuối cùng nào của hệ thống, bất kỳ Người gửi nào cũng có thể bắt đầu Sự kiện bổ sung quyền của họ vào trạng thái (có thể thừa) và chỉ Người gửi mới có thể thực hiện việc này. Theo một nghĩa nào đó, đây giống như ví dụ về nhiều người nhận ngoại trừ ở đây chúng ta có nhiều hành động theo trình tự, thay vì nhiều hành động thay thế.

Thuộc tính phương thức thứ hai giống như ví dụ đối với một người nhận duy nhất, cụ thể là Người nhận và chỉ Người nhận mới có thể bắt đầu bất kỳ loại Sự kiện nào từ trạng thái kết quả của toàn bộ Giao dịch.

C. Giao dịch có nhiều người nhận

Giao dịch nhiều người nhận giống như Giao dịch đơn giản, ngoại trừ việc có nhiều Người nhận tham gia có khả năng chuyển thêm Vật phẩm. Do đó, chất lượng phương thức mà chúng ta muốn giữ nguyên là bất kỳ Người nhận nào cũng có thể bắt đầu Sự kiện, nhưng không có Đại lý nào ngoài một trong số họ có thể làm như vậy.

Cả Giao dịch nhiều người gửi và nhiều người nhận có thể được coi là các phiên bản khác nhau của mẫu M-of-N chung. Chúng được phân biệt ở đây chỉ vì mục đích làm nổi bật các khía cạnh khác nhau của nội dung phương thức.

D. Giao dịch phụ thuộc vào thời hạn

Giao dịch phụ thuộc vào thời hạn (được mô tả trong [1] phần 2.3 làm ví dụ về hoán đổi tài chính) giống như Giao dịch nhiều người nhận ngoại trừ việc Người nhận có quyền sở hữu trong các khoảng thời gian khác nhau. Đặc biệt, trước một số thời hạn (có thể là thời gian, hoặc một sự kiện hoặc một số điều kiện khác), chỉ Người nhận 1 mới có thể chuyển Vật phẩm và sau thời hạn, chỉ Người nhận 2 mới có thể chuyển Vật phẩm.

Một cách sử dụng điển hình là để đảm bảo rằng một hợp đồng thông minh, chẳng hạn như trong một trò chơi mà luồng thông tin là quan trọng, luôn tồn tại theo một nghĩa nào đó. Điều đó có nghĩa là không hành động nào của người tham gia có thể làm tắc nghẽn hợp đồng và khiến những người khác mất tiền vĩnh viễn. Nội dung phương thức được quan tâm là tuyên bố rằng sẽ luôn có trạng thái trong đó ai đó hoàn toàn kiểm soát Vật phẩm. Mọi trạng thái có thể xảy ra trong tương lai, và cả trạng thái hiện tại, sao cho luôn có chủ sở hữu xác định của Vật phẩm sau khi kết thúc thời hạn.

E. Trò chơi "Oẳn tù tì"

Trong trò chơi "Oẳn tù tì" dựa trên Blockchain (như được mô tả trong [1] phần 4) với hai người chơi, Người chơi 1 và Người chơi 2, mỗi người đưa ra lựa chọn của mình (kéo, búa, hoặc bao) cùng với một số Vật phẩm, sau khi trò chơi chuyển sang trạng thái mà một Người chơi có thể sở hữu Vật phẩm bằng cách được phép chuyển chúng.

Thông qua lăng kính của bản thể luận, trò chơi bao gồm hai Đại lý, Người chơi 1 và Người chơi 2, mỗi người phải bắt đầu một Sự kiện đóng góp một số Đối tượng cho trò chơi trước khi trò chơi chính thức diễn ra. Đây là một cặp thuộc tính phương thức, bao gồm khả năng một Tác nhân tùy ý khởi tạo Sự kiện đầu tiên như vậy và sau đó ở trạng thái kết quả, khả năng một Tác nhân tùy ý khác khởi tạo Sự kiện thứ hai như vậy. Ở trạng thái thứ ba này, có một khả năng phân biệt, đó là chỉ có Người chơi 1 hoặc Người chơi 2 mới có thể bắt đầu một số Sự kiện.

IV. LÝ LUẬN NHƯ THẾ NÀO VÀ VỀ ĐIỀU GÌ

Bản thể luận được mô tả ở trên là một tập hợp các khái niệm nguyên thủy cơ bản có thể được sử dụng để suy luận về hợp đồng thông minh, nhưng tất nhiên chúng ta cũng phải có các công cụ chính thức thực tế để suy luận về hợp đồng thông minh và chúng ta phải có một số hệ thống thực tế có thể được sử dụng để thực hiện các hợp đồng thông minh.

Bản chất phương thức của bản thể luận gợi ý rõ ràng là chúng ta nên sử dụng các mô hình kết hợp của ngữ nghĩa ngôn ngữ lập trình. Ví dụ, các kỹ thuật được mô tả trong [2] có thể tạo thành cơ sở của một khuôn khổ như vậy. Chúng ta cũng có thể sử dụng các công cụ lý thuyết bằng chứng, chẳng hạn như lý thuyết loại thời gian và lý thuyết loại mờ Lax [3], như một khuôn khổ lý luận về hợp đồng thông minh. Nghiên cứu về lý thuyết loại nhận thức tuyến tính [4] [5] cũng có thể phù hợp, vì nó là lý thuyết loại cho các hệ thống ủy quyền phân tán, đây là một mô tả khá chính xác về hợp đồng thông minh dựa trên Blockchain.

Đối với bản chất của một hợp đồng thông minh, có rất nhiều lựa chọn khả thi. Cách đơn giản nhất là xác định rõ ràng thông tin tổng hợp trong ngôn ngữ lập trình thông thường. Ví dụ: giả sử trạng thái chỉ là Token cho một máy trạng thái hữu hạn. Chúng ta sẽ cần xác định loại Token trạng thái, loại tương tác mà những người tham gia hợp đồng thông minh có thể tham gia,

trạng thái ban đầu để hệ thống chạy từ đó và chức năng chuyển tiếp xác định cách tính toán tiến hành để đáp ứng với tương tác. Sau đó, trong Haskell, chúng ta có thể chỉ cần khai báo

```
data StateToken = ...
data Interaction = ...

initState :: StateToken
initState = ...

transition :: Interaction
                -> StateToken -> StateToken
transition = ...
```

Với điều kiện là chúng ta có một mô hình tốt về hành vi của ngôn ngữ chủ, điều này là đủ. Điều này đặc biệt tốt nếu ngôn ngữ chủ được đảm bảo chấm dứt, bởi vì khi đó chúng ta có thể chắc chắn rằng mỗi quá trình chuyển đổi riêng lẻ sẽ diễn ra trong thời gian hữu hạn, ngay cả khi toàn bộ hợp đồng thông minh có thể tiến hành vô thời hạn trong tương lai. Một ví dụ điển hình của chương trình như vậy là một máy chủ web, nơi bạn muốn mọi yêu cầu chấm dứt và trả lời (trang web), nhưng bạn muốn toàn bộ máy chủ tiếp tục chạy vô thời hạn.

Tuy nhiên, viết một hợp đồng thông minh trong cài đặt này có thể không lý tưởng. Nó yêu cầu chương trình mã hóa hành vi của hợp đồng thành trạng thái và hàm chuyển tiếp, đây có thể không phải là biểu diễn dễ hiểu nhất, ngay cả khi nó có lợi cho tính toán. Và giải pháp thay thế sẽ là xác định một ngôn ngữ dành riêng cho miền nắm bắt trực tiếp hơn bản chất của hợp đồng thông minh dưới dạng nguyên gốc của ngôn ngữ và cho phép lập luận trực tiếp. Điều này sau đó có thể được biên dịch thành một ngôn ngữ giúp thực thi dễ dàng hoặc một môi trường thực thi có thể được phát triển riêng cho nó.

Một tùy chọn khác kết hợp cả hai là phát triển một ngôn ngữ dành riêng cho miền được nhúng. Nếu có một ngôn ngữ có mục đích chung chẳng hạn như Haskell để chúng ta có thể xác định các loại và chức năng tùy chỉnh, thì miền hợp đồng thông minh có thể được biểu diễn dưới dạng một tập hợp các ngôn ngữ đó. Đây là phương pháp thường được sử dụng cho EDSL trong Haskell, chẳng hạn như thư viện hình ảnh và âm thanh.

V. THẢO LUẬN

Từ các hợp đồng thông minh ví dụ này, việc sử dụng một bản thể luận phương thức trong đó các trạng thái được liên kết bởi các sự kiện có thể nắm bắt được nhiều thuộc tính quan trọng. Chúng ta không chỉ có thể thể hiện các quyền mà Tác nhân có bằng cách đưa ra yêu cầu theo phương thức về các sự kiện có thể xảy ra mà Tác nhân có thể bắt đầu, chúng ta còn có thể thể hiện nghĩa vụ bằng cách thể hiện rằng việc không hành động không bao giờ có thể gây ra tắc nghẽn. Chúng ta có thể sử dụng các kỹ thuật tương tự này để thể hiện các khái niệm phong phú hơn liên quan đến tính sống động để đảm bảo rằng một hợp đồng không bao giờ bị mắc kẹt trong các vòng lặp không thể thoát ra được do các cuộc tấn công.

Tuy nhiên, có những hạn chế quan trọng đối với những gì có thể được diễn đạt ở đây. Các hệ thống trạng thái như hợp đồng thông minh là máy tính hiệu quả và nếu không có những hạn chế nghiêm trọng đối với những gì cấu thành trạng thái của hợp đồng, chúng ta có thể không bao giờ chứng minh được một số điều nhất định. Chẳng hạn, một người có thể muốn chứng minh rằng một hợp đồng thông minh nhất định sẽ luôn đạt đến một số trạng thái cuối cùng khi các quyền theo hợp đồng kết thúc và tất cả các nghĩa vụ đã được thực hiện, nếu không thì hợp đồng đã kết thúc sớm. Tuy nhiên, nếu các trạng thái của hợp đồng bao gồm băng Turing Machine và các trạng thái điều khiển, thì có thể không chứng minh được. Vì chúng ta có thể nhúng Turing Machine vào hợp đồng, chúng ta gặp phải vấn đề tạm dừng.

Tuy nhiên, không nên giới hạn trạng thái hợp đồng. Thật khó để dự đoán những gì mọi người sẽ sử dụng và có lẽ chạy Turing Machine là hoàn toàn hợp lý. Tuy nhiên, một thư viện các mẫu hợp đồng có thể được xây dựng và các thuộc tính này có thể được chứng minh là chúng độc lập với các khởi tạo cụ thể, cho phép người dùng dễ dàng có được hành vi có thể kiểm chứng.

Một khả năng thú vị khác là xem cấu trúc phương thức trạng thái thông qua lăng kính của máy ảo và thiết kế trình biên dịch. Có thể xây dựng các ngôn ngữ lập trình dễ dàng kiểm tra các điều kiện kết thúc để biên dịch thành các hệ thống chuyển tiếp thuộc loại này. Sau đó, các thuộc tính có thể dễ chứng minh hơn vì chúng có thể được áp dụng thay thế cho ngôn ngữ lập trình chứ không phải cho máy trạng thái thực sự thực hiện hợp đồng. Chính xác thì một ngôn ngữ như vậy sẽ trông như thế nào là một chủ đề nghiên cứu khả thi trong tương lai.

Công việc tiếp theo cũng có thể cần thiết để kết hợp lý luận về kiến thức. Bản thể luận được đưa ra ở trên giả định rằng kiến thức là một khái niệm nguyên thủy hơn những gì mà bản thể luận nhắm tới, nhưng điều này có thể không đúng. Nhiều hợp đồng thông minh dựa vào việc ẩn thông tin tạm thời để hoạt động và do đó, có thể mong muốn thể hiện khả năng của Đại lý bất kỳ lúc nào bằng cả phương thức và *cả* tuyên bố về mức độ họ biết so với yêu cầu của hệ thống. Làm việc trên logic nhận thức tuyến tính cho ủy quyền phân tán có thể có liên quan ở đây. Tuy nhiên, chủ đề này cũng rất rộng, vì kiến thức và bí mật có thể được hiểu là bao gồm bất kỳ loại rò rỉ thông tin nào. Chúng ta có nên thể hiện trong một hợp đồng thông minh rằng không có thông tin nào về tính chẵn lẻ của một số bị rò rỉ bởi một tập hợp các Sự kiện không? Có lẽ, nhưng điều này sẽ đòi hỏi rất nhiều bằng chứng về lý thuyết thông tin, hoặc một loại lý thuyết rất mạnh để tính toán an toàn. Cả hai điều này đều rất phức tạp. Bảo mật cũng là một vấn đề đối với các cấp độ Blockchain thấp hơn, không chỉ ở cấp độ logic của hợp đồng và do đó, đây có thể là phần sai của hệ thống khi đưa điều đó vào.

LỜI CẢM ƠN

Tôi muốn cảm ơn Lars Brunjes, Vitalik Buterin, Yoichi Hirai, Pablo Lamela, Alex McSherry và Simon Thompson vì những nhận xét và thảo luận của họ. Quan điểm của họ cực kỳ giá trị, đặc biệt là khi nó tiết lộ những giả định ẩn giấu về phía tôi về những gì người đọc biết.

TÀI LIỆU THAM KHẢO

[1] Delmolino, K và cộng sự. *Từng bước hướng tới tạo hợp đồng thông minh an toàn: Bài học và thông tin chi tiết từ phòng thí nghiệm Crypto*. https://eprint.iacr.org/2015/460.pdf

[2] Backhouse, R., Crole, R., và Gibbons, J. *Các phương pháp đại số và đại số trong toán học xây dựng chương trình*.

[3] Pfenning, F., và Davies, R. *Tái cấu trúc có nhận xét của logic phương thức*. https://www.cs.cmu.edu/ fp/papers/mscs00.pdf

[4] Garg, D., và Pfenning, F. *Logic ủy quyền của trạng thái – Lý thuyết bằng chứng và một nghiên cứu điển hình*. http://www.cs.cmu.edu/ fp/papers/jcs12.pdf

[5] DeYoung, H., và Pfenning, F. *Lý luận về hậu quả của các chính sách ủy quyền trong logic nhận thức tuyến tính*. http://www.cs.cmu.edu/ fp/papers/fcs09.pdf

Người dịch: Nguyễn Văn Tú

Telegram: https://t.me/Tulibra

Link gốc: https://iohk.io/en/research/library/papers/an-ontology-for-smart-contracts/