ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KĨ THUẬT MÁY TÍNH

MÔ HÌNH HÓA TOÁN HỌC (CO2011)

Đề bài tập lớn

Đặc tả Smart Contract bằng Linear Logic

Giáo viên hướng dẫn:	Nguyễn An Khương
	Huỳnh Tường Nguyên
	Trần Văn Hoài
	Lê Hồng Trang
	Trần Tuấn Anh
Trợ giảng:	Nguyễn Trung Việt
Sinh viên thực hiện:	1613575 - Trần Ngọc Tín
	1610852 - Huỳnh Sâm Hà
	1613535 - Nguyễn Văn Tiến
	161 - Thái Hoàng Nguyên
	161 - Huỳnh Song Anh Quân

Thành phố Hồ Chí Minh, Ngày 9 tháng 6 năm 2018

Mục lục

Danh sách hình vẽ

Danh sách bảng

1 Giới thiệu đề tài

2 Bài toán 1: Kiến thức ôn tập

2.1 Lịch sử và ứng dụng của Linear Logic

2.1.1 Lịch sử phát triển của Linear Logic

Linear Logic (Logic tuyến tính) là một dạng Substructural Logic (Logic thiếu mất 1 trong những quy luật cấu trúc) được đề xuất bởi Jean-Yves Girald vào năm 1987 như là một sự cải tiến của Classical Logic (Logic cổ điển) và Institutional Logic (Logic mang tính trực giác), kết hợp giữa luật đối tính của Classical Logic với các quy luật hình thành của Institutional Logic.

Mục tiêu của Linear Logic là cầu kết nối giữa logic và khoa học máy tính vì nó cho phép thể hiện và điều khiển những sự kiện của thế giới thực một cách tự nhiên. Một ví dụ điển hình là Law of Excluded Middle (LEM). LEM nói rằng "có A hoặc không có A", vốn là một điều hoàn toàn hợp lý trong cuộc sống cùa chúng ta. Đối với Classical Logic, LEM là một luật được chấp nhận, tuy nhiên điều đó lại ngược lại đối với Institutional Logic.

Linear Logic đã định nghĩa LEM theo 2 cách là $A \oplus \neg A$ và $Avchandngc(\&ngc)A$.

Cách thứ nhất tương đương với công thức của phép tuyển trong Institutional Logic và cách thứ hai tương đương với "A suy ra A" là điều luôn đúng. Cả 2 cách này đều được chấp nhận trong Institutional Logic. Từ đó, ta có thể thấy Linear Logic là một sự kết hợp hoàn hảo giữa Classical và Institutional.

2.1.2 Những ứng dụng của Linear Logic

Linear Logic có rất nhiều công dụng trên nhiều lĩnh vực khác nhau. Ví dụ:

• Diện toán lượng tử Khác với máy tính thông thường sử dụng bit để lưu trữ các trạng thái, máy tính lượng tử sử dụng qubit. Ở máy tính thông thường, chi phí tính toán một phép toán một lần hay nhiều lần là như nhau. Vì vậy mà ta có thể sử dụng logic cổ điển để thể hiện các phép toán trên máy tính thông thường. Tuy nhiên, đối với máy tính lượng tử, việc thực hiện một phép toán nhiều lần sẽ có chi phí tính toán cao hơn là thực hiện chỉ 1 lần. Sử dụng Linear Logic sẽ thích hợp hơn trong trường hợp này vì việc quản lý tài nguyên là một vấn đề cần được xem xét.

• Ngôn ngữ học Linear Logic có thể được dùng để kiểm tra và chứng minh ngữ pháp và ngữ nghĩa của một ngôn ngữ. Như việc kiểm tra xem ngữ pháp của một ngôn ngữ có cấu trúc nhất định hay ngữ nghĩa của một câu nói có thể hiện được một điều đúng đắn trong logic.

• Lập trình Vì Linear Logic cho phép quản lý tài nguyên một cách hiệu quả hơn, chúng ta có thể áp dụng nó vào việc lập trình để quản lý bộ nhớ hay việc thu gom rác một cách hiệu quả hơn. Ngoài ra, Linear Logic giúp thể hiện những hiện tượng trong thế giới thực một cách tự nhiên hơn, giúp cho việc lập trình trở nên đa dạng và dễ dàng hơn.

2.2 Lịch sử và ứng dụng của Smart Contract

2.2.1 Lịch sử phát triển và cái nhìn tổng quan về Smart Contract

Theo dòng lịch sử chúng ta sẽ thấy công nghệ đã thay đổi rất nhiều thứ, kể cả nhận thức của mỗi chúng ta. Các công nghệ mới được sinh ra và dần dần thay thế các công nghệ đã trở nên lạc hậu. Bắt đầu kỉ nguyên của internet, niềm tin luôn là một thứ gì đó khá xa xỉ khi các tổ chức, cá nhân bắt tay, giao tiếp với nhau trên mạng internet. Đứng trước bài toán đó, vào những năm 1990, nhà mật mã học Nick Szabo đã đưa ra 1 khái niệm hoàn toàn mới là Smart Contract. Ông định nghĩa một smart contract là một giao thức máy tính tạo ra để số hóa, kiểm chứng và thực thi các thỏa thuận và nghĩa vụ được quy định trong một hợp đồng. Smart contract cho phép thực thi các giao dịch một cách đáng tin cậy mà không cần một bên thứ ba làm chứng. Các giao dịch đó có thể theo dấu và không thể đảo ngược được.

Một cách dễ hiểu để mô tả smart contract (dịch ra ngôn ngữ Việt là *hợp đồng thôngn minh*) là hình dung công nghệ này như một máy bán nước tự động. Thông thường, người làm hợp đồng sẽ phải tìm đến luật sư hay đem đi công chứng, trả tiền cho họ và chờ đợi để lấy giấy tờ tài liệu. Bằng cách sử dụng hợp đồng thông minh, ta chỉ cần thả một bitcoin (giả sử pháp luật Việt Nam cho phép ta sử dụng đồng tiền kĩ thuật số Bitcoin trong giao dịch mua bán như trong ví dụ này) vào máy bán hàng tự động, đã được phát triển trên nền tảng Blockchain và những gì bạn yêu cầu sẽ được trả lại trực tiếp vào tài khoản của bạn. Hơn nữa, hợp đồng thông minh không chỉ xác minh những quy định, quyền lợi và nghĩa vụ giống như hợp đồng truyền thống mà nó còn tự động thực thi những điều trên, không thông qua một bên thứ 3 trong môi trường thiếu niềm tin.

Công nghệ nguyên thủy của hợp đồng thông minh đã từng là một bài toán tư duy *"ngủ yên"* trong hơn một thập kỷ. Thế nhưng mọi thứ đã thay đổi với sự ra đời và phát triển của công nghệ Blockchain. Tuy Bitcoin đã đặt ra những nền tảng cơ bản cho việc thiết lập hợp đồng trên nền tảng Blockchain, nó vẫn còn chưa thể thõa mãn mọi nhu cầu trong đời sống xã hội hiện nay. Mãi cho đến khi Ethereum ra đời thì ý tưởng hợp đồng thông minh mới chính thức phổ biến, cung cấp phương thức mới để thiết lập hợp đồng. Ngày nay, số lượng các tổ chức, công ty nghiên cứu về các lĩnh vực trong công nghệ Blockchain và ứng dụng của smart contract đã và đang tăng lên đáng kể, cho thấy sự phát triển đầy tiềm năng của công nghệ này.

2.2.2 Những ứng dụng dựa trên Smart Contract

Smart contract kết hợp với blockchain có thể ứng dụng trong rất nhiều lĩnh vực, từ tài chính, bảo hiểm, ngân hàng cho đến các nhu cầu như giải trí, bầu cử (voiting), bình chọn,... Với mỗi lĩnh vực ta lại sử dụng một loại hợp đồng thông minh khác nhau, ví dụ hợp đồng vay tiền, hợp đồng đóng tiền định kỳ, hợp đồng mua bán, hợp đồng chuyển nhượng,...

Khi một lĩnh vực được áp dụng hợp đồng thông minh hay còn gọi là smart contract,

mọi quyết định hoặc giao dịch thuận theo hợp đồng đều được xử lý tự động khi thỏa điều kiện đã đưa ra. Ví dụ:

- Hợp đồng vay tiền có lãi suất:
  Giả sử rằng bạn vay một số tiền có lãi suất và ký hợp đồng này, khi đến một ngày nhất định, hợp đồng thông minh sẽ tự trừ tiền trong tài khoản của bạn và gửi (cộng thêm) cho người cho vay theo tỉ lệ đúng như đã ký kết.

- Hợp đồng chuyển nhượng:
  Giả sử nếu bạn trả 50% số tiền bạn sẽ được giữ cọc món hàng, nếu bạn trả đủ 100% bạn sẽ được nhận món hàng đó, nếu bạn trả 50% nhưng không thanh toán đủ trong thời gian quy định thì bạn sẽ mất cọc, tất cả đều được tự động xử lý với hợp đồng thông minh.

- Bầu cử:
  Giả sử ta đang xét trong một quá trình bầu cử cần sự minh bạch, rõ ràng và không xảy ra gian lận giữa người tổ chức và các ứng cử viên. Nếu ta thực hiện theo cách truyền thống, ví dụ như bỏ phiếu hoặc bình chọn bằng tin nhắn, có thể thấy còn thiếu sự minh bạch, và có thể xảy ra gian lận. Cụ thể người chơi (ứng cử viên) không thể biết được những ai đã bầu cho các người chơi khác, và những người bầu cử cũng không biết được thực sự những ai đã bầu cho những người nào. Do đó thiếu đi sự minh bạch trong phương thức truyền thống. Nếu ta sử dụng nền tảng công nghệ Blockchain với smart contract, mọi thứ sẽ được giải quyết ổn thỏa. Kết quả bỏ phiếu sẽ được chuyển vào Blockchain, do smart contract quản lý và phân phối về các node trong mạng lưới. Toàn bộ dữ liệu sẽ được mã hóa và hoàn toàn ẩn danh, mọi người cũng có thể biết chính xác có bao nhiêu phiếu đã bầu cử cho những người nào.

- Logistics
  Chúng ta đều biết rằng chuỗi cung ứng là một hệ thống kéo dài và gồm nhiều liên kết khác nhau. Mỗi liên kết cần phải nhận được xác nhận bởi một mắt xích (xem như một node) ở trước đó để đủ điều kiện thực hiện phần việc của mình theo như hợp đồng.

  Đây là một quá trình kéo dài, lãng phí và kém năng suất, nhưng với smart contract thì mỗi bộ phận tham gia đều có thể theo dõi tiến trình công việc để từ đó hoàn thành nhiệm vụ đúng hạn. Smart contract bảo đảm tính minh bạch trong điều khoản hợp đồng, chống gian lận.

  Nó còn có thể cung cấp cho ta khả năng giám sát quá trình cung ứng nếu như được tích hợp chung với mạng lưới vạn vật kết nối Internet (hay còn gọi là Internet of Things). Có thể nói hai công nghệ này kết hợp với nhau tạo ra một nền công nghệ 4.0 hoàn thiện.

- ICO
  Một ứng dụng rộng rãi của hợp đồng thông minh trong lĩnh vực tiền mã hóa đó là phát hành ICO. Một hợp đồng thông minh được viết ra để khi nhà đầu tư gửi

vào địa chỉ của hợp đồng một số tiền, họ sẽ nhận lại được một số token tương ứng với số tiền họ đã bỏ ra. Hợp đồng thông minh đó có thể bổ sung một số điều kiện như đóng băng số tiền nhận được trong một khoản thời gian quy định hoặc hủy các token không bán được.

Việc ứng dụng hợp đồng thông minh và blockchain trong ICO giúp các nhà đầu tư có thể theo dõi dự án đã gọi được bao nhiêu tiền, có đạt được mục tiêu hay không, và nhiều thông tin khác nữa.

Ngoài ra, smart contract còn có rất nhiều những ứng dụng khác trong đời sống xã hội cũng như kinh tế chính trị, lĩnh vực tài chính,...

2.3 Làm rõ mấy cái phép toán trong ass

2.4 Hai phép toán kia - ghi vô

2.5 Exponentials connectives

Trong linear logic, ngoài các connectives (dịch là phép tuyển) *multiplicatives* và *additives* như trên đã trình bày, còn một loại connective khác là *exponentials* (dịch ra là số mũ, ý chỉ cấp số mũ, tăng nhanh chóng hay vô hạn), trong đó bao gồm 2 loại connectives là ! và ?. Chi tiết của hai loại connectives này sẽ được trình bày trong section này.

2.5.1 Connective !

Đây là một connective trong linear logic, được đọc là *"of course"* (dịch ra là *tất nhiên*) hay *"bang"*. Connective này diễn tả một tài nguyên có tiềm năng vô tận, ý nghĩa là dùng để chỉ sự sản sinh, hay có được một số lượng không giới hạn của một yếu tố nào đó. Cụ thể:

!A: *có nghĩa là tạo ra một lượng không giới hạn yếu tố A.*

Ví dụ 1

Trong thực đơn menu của một nhà hàng nêu rõ một phần ăn giá \$5 dành cho một người gồm các phần ăn như sau:

+ Hamburger
+ Fries or Wedges
+ Unlimited Pepsi
+ Ice-cream or Sorbet

Ta có thể chuyển bài toán trên thành linear logic với các connectives đã học. Cụ thể kí hiệu Hamburger (H), Fries (F), Wedges (W), Pepsi (P), Ice-cream (I) và Sorbet (S), khi đó ta có:

$$\$1 \otimes \$1 \otimes \$1 \otimes \$1 \otimes \$1 \multimap H \otimes (F \& W) \otimes !P \otimes (I \oplus S)$$

Ta thấy trong ví dụ này, ta sử dụng connective ! cho trường hợp ta tạo ra một lượng không giới hạng pepsi.

Ví dụ 2

Xét một ví dụ khác liên quan đến *Constraint Handling Rules (CHR)*. Xét bài toán tung đồng xu ta luôn có một trong hai kết quả là mặt ngửa và mặt xấp mỗi khi tung đồng xu. Cụ thể trong logic cổ điển ta có thể diễn tả như sau

$$(throw(Coin) \Leftrightarrow Coin = head) \wedge (throw(Coin) \Leftrightarrow Coin = tail)$$

Có nghĩa khi tung đồng xu, không phải mặt ngửa thì là mặt xấp. Còn trong linear logic, chúng ta có thể dùng biểu thức sau để nhấn mạnh tính đúng đắn của định luật trên bằng connective ! (dịch ra là *tất nhiên*) như sau:

$$!(throw(Coin) \multimap ((Coin = head)\&(Coin = tail))$$

Biểu thức trên sử dụng connective ! để chỉ ra việc ta có một tiềm năng vô hạn về việc khi chi tiêu A (tung đồng xu), ta sẽ có được B (không ngửa thì là xấp). Cũng có thể đọc là *"Tất nhiên khi tung đồng xu, không phải mặt ngửa thì là mặt xấp"*.

2.5.2 Connective ?

Tiếp theo, ta sẽ nói về connective còn lại trong Exponentials connective trong linear logic, đó là connective ?, được đọc là *"why not"*.

Ngược lại với connective !, connective ? diễn tả một thực tế về tài nguyên hiện tại có tiềm năng vô tận, tức mang ý nghĩa chi tiêu (tiêu thụ) một lượng không giới hạn một yếu tố, cụ thể:

?A: *có nghĩa chi tiêu một lượng không giới hạn yếu tố A.*

Ví dụ

Trong thực tế, sẽ không có ví dụ nào minh họa được tính có sẵn nguồn lực vô hạn mà cụ thể, ta đều có thể ước tính được lượng cần sử dụng cần thiết để tạo ra một thứ gì đó. Lấy ví dụ như trong việc sử dụng các nguồn năng lượng tự nhiên như năng lượng gió, năng lượng mặt trời, năng lượng nước, băng các thực nghiệm và tính toán, ta đều có thể ước tính được lượng ta cần sử dụng để tạo ra một khối lượng sản phẩm đầu ra sau cùng.

Cụ thể, trong ngành năng lượng thủy điện, sử dụng nước để tạo ra điện, lấy ví dụ người ta cần dùng $500m^3$ nước để sản sinh ra $1kJ$ điện năng. Tuy nhiên ta có thể giả sử việc sử dụng lượng nước bao nhiêu là không tính trước được, hoặc ta cần một lượng vô hạng điện năng, ta có thể sử dụng linear logic để biểu diễn bài toán như sau:

$$?(hydro) \multimap 1kJ \text{ hay } ?(hydro) \multimap !(electric)$$

Lấy một ví dụ khác trong ngành điện gió, ta cần một lượng động năng sinh ra từ gió không giới hạn để tạo ra một lượng điện năng cho toàn bộ thành phố (cũng chưa biết):

$$?(wind) \multimap !(electric)$$

2.5.3 Liên hệ của ! và ? trong linear logic

Trong linear logic, ta có mối quan hệ sau

$$(?A)^{\perp} = !(A^{\perp}) \text{ và } (!A)^{\perp} = ?(A^{\perp})$$

Trong đó hai connectives này là dual của nhau.

2.5.4 Một số biểu thức liên quan

Biểu thức 1. $!(A\&B) \equiv !A \otimes !B$

Biểu thức này nói rằng có sự tương đường giữa hai yếu tố $!(A\&B)$ và $!A \otimes !B$. Ta có thể giải thích như sau:

+ $!(A\&B)$: có nghĩa là ta có được một lượng vô hạn các sự lựa chọn (mang tính chủ động, phụ thuộc cách chọn của ta) các yếu tố A, hoặc B. Do đó ở mỗi lần lựa chọn trong số vô hạn lần tạo ra, ta có thể tùy ý chọn A hoặc chọn B.

+ $!A \otimes !B$: còn công thức này có nghĩa là ta tạo ra được cả A lẫn B, trong đó không giới hạn số lượng A, hay B tạo ra. Có nghĩa ta có được vô hạn lần A cũng như vô hạn lần B.

Qua đó ta thấy có sự tương đương giữa 2 công thức, đều muốn đề cập đến việc có được vô hạn các yếu tố A và B.

Biểu thức 2. $A \otimes !(A \multimap B) \vdash B \otimes !(A \multimap B)$

Đây là một sequent chỉ ra rằng khi có A và "luôn có" tính chất "Chi tiêu A sẽ được B", thì ta sẽ có B, cũng như tính chất trên không thay đổi. Điều này hiển nhiên là đúng và ở đây ta thấy được việc sử dụng connective ! để chỉ một tính chất luôn đúng mà ta có được (ở đây là chi tiêu A sẽ được B).

3 Bài toán 2: Ngữ cảnh smart contract

3.1 Mô tả ngữ cảnh cho smart contract

3.1.1 Động cơ và mục tiêu

Trong các hoạt động kinh doanh, vận chuyển hàng hóa hiện nay, hợp đồng thông minh (smart contract) giúp giải quyết rất nhiều những khó khăn, rào cản mà việc xử lí thủ công mắc phải. Trước hết, bởi vì các smart contract sẽ thực hiện tự động những hoạt động mà trước đây thường phải thực hiện thủ công (như việc xác nhận đơn hàng) nên chúng có khả năng thúc đẩy tốc độ của quy trình kinh doanh. Ngoài ra, smart contract cũng đem lại sự đảm bảo về độ chính xác của giao dịch cao hơn, ít lỗi hơn, từ đó giảm thiểu đáng kể rủi ro khi thực hiện hợp đồng. Bên cạnh đó, một ưu điểm cần phải kể đến của ssmart contract đó là việc tối thiểu hóa sự tham gia của các bên thứ ba hay bên trung gian vào quá trình thực hiện hợp đồng. Sự tinh giản này giúp tiết kiệm đáng kể chi phí kinh doanh.

Đặt trong bối cảnh một doanh nghiệp phải thực hiện hàng ngày một lượng khổng lồ các thủ tục xác nhận đơn hàng logistics, lợi ích mà smart contract đem lại sẽ không chỉ kể hết trong một hai trang giấy. Như vậy, với lý tưởng đảm bảo sự công bằng, minh bạch và tiết kiệm tối đa chi phí cho các bên tham gia giao kết hợp đồng, smart contract thực sự đã cho thấy những tiềm năng ứng dụng của nó, không chỉ đơn thuần áp dụng vào các hoạt động thương mại, mà còn được kỳ vọng sẽ hoạt động hiệu quả trong việc bầu cử, tiếp cận dữ liệu về sức khỏe và dân số, hỗ trợ quy trình bồi thường bảo hiểm hoặc quản lý chính phủ.

3.1.2 Tình huống cụ thể

Với tình huống cụ thể là giao dịch liên quan đến vận tải đa phương thức (logistics) giữa công ty A và công ty B. Giả sử bên A (công ty A) có nhu cầu vận chuyển một lô hàng thủ công mỹ nghệ, và sử dụng dịch vụ vận tải của công ty B (gọi là bên B). Tuy nhiên bên A và bên B chưa có được niềm tin tưởng lẫn nhau. Cụ thể bên A băn khoăn rằng liệu bên B có bảo quản tốt hàng hóa, đảm bảo về chất lượng lẫn số lượng, cũng như thời gian chuyển hàng tới địa điểm chỉ định đúng hẹn hay không? Còn bên B thì đặt ra câu hỏi là liệu bên A có đảm bảo uy tín, không phải là công ty lừa đảo, hay hàng hóa của bên A là hợp pháp hay bất hợp pháp, cũng như việc thù lao khi bên B giao hàng đến nơi có được chuyển đúng hẹn? Để giải quyết những khúc mắc này, 2 bên phải giao kết một hợp đồng thỏa thuận về việc vận chuyển hàng hóa, dẫn đến những phát sinh về dịch vụ tư vấn luật như soạn thảo hợp đồng, phòng ngừa các rủi ro pháp lý,... Vậy cách nào để đơn giản hóa quy trình thỏa thuận giữa 2 bên A và B, khi mà không có niềm tin trong môi trường doanh nghiệp như trong tình huống này?

Lúc này, smart contract có thể giải quyết câu hỏi này. Khi hai bên tham gia vào mô hình này, bên A sẽ thanh toán phí vận chuyển cho bên B thông qua smart contract. Bên B cũng đảm bảo số tiền đặt cọc bảo đảm về hàng hóa khi vận chuyển vào smart contract. Smart contract này sẽ giữ lại số tiền của cả 2 bên và việc thanh toán này chỉ được thực hiện khi 2 bên hoàn thành yêu cầu của hợp đồng kèm theo sự xác nhận của 2 bên. Chi tiết cụ thể như sau: 2 bên cung cấp những thông tin về thời gian, địa điểm, hàng hóa, các quy định bồi thường vào smart contract, và smart contract public thông tin này cho 2 phía. Ngoài ra 2 bên cùng chuyển vào smart contract số tiền cần thiết của 2 bên để smart contract giữ số tiền này. Cụ thể bên A cần chuyển vào số tiền thù lao mà bên A sẽ phải chi trả cho bên B nếu bên B hoàn tất công việc. Còn bên B cần chuyển vào số tiền mà bên B có thể sẽ phải bồi thường trong quá trình smart contract hoạt động, số tiền này tối thiểu phải là lượng tiền bồi thường lớn nhất mà bên B gánh phải trong suốt quá trình hợp đồng xảy ra. Khi 2 bên thỏa thuận, smart contract chính thức có hiệu lực. Trong suốt quá trình nhận hàng, kiểm tra hàng, vận chuyển, tiếp nhận, kiểm tra lại hàng hóa của 2 phía, smart contract sẽ luôn thực thi khi một điều kiện nào đó kích hoạt nó, bao gồm việc bồi thường của 2 bên, hoặc hợp đồng bị hủy, hoặc hoàn tất.

Chi tiết của các điều kiện trong bản hợp đồng sẽ kích hoạt smart contract như sau: diễn ra ở các giai đoạn B đến nhận hàng từ A, B kiểm tra hàng hóa của A, A nhận hàng khi B vận chuyển và cuối cùng là A kiểm tra lại hàng hóa của mình.

- Khi B đến nhận hàng từ A

Gồm các quy định về thời gian nhận hàng, B cần phải đến sớm hoặc đúng hơn thời gian nhận hàng, nếu đến trễ hoặc không đến, B sẽ phải bồi thường hoặc hủy hợp đồng. Bên A cũng có trách nhiệm có hàng hóa để giao cho bên B. Nếu bên A không có hàng hóa, bên A cũng chịu trách nhiệm bồi thường hoặc hủy hợp đồng.

- Khi B kiểm tra hàng hóa của A
  Gồm các quy định về thông tin hàng hóa, bên A phải đảm bảo hàng hóa của mình đúng như thông tin hàng hóa quy định trong smart contract. Bên A sẽ phải chịu bồi thường hoặc hủy hợp đồng nếu vi phạm

- Khi bên A nhận hàng hóa từ bên B
  Gồm các quy định về thời gian, bên B phải giao hàng cho bên A đúng địa điểm thời gian trong smart contract. Nếu đến trễ hoặc không đến, bên B sẽ phải chịu bồi thường.

- Khi bên A kiểm tra lại hàng hóa
  Gồm các quy định về hàng hóa, bên B phải đảm bảo hàng hóa còn nguyên vẹn, đảm bảo về chất lượng lẫn số lượng, vẫn còn niên phong nếu có. Nếu vi phạm, bên B sẽ phải chịu bồi thường trong smart contract. Nếu không có gì xảy ra, smart contract xem như hoàn tất và trả lại số tiền cho 2 bên đúng như quy định của các điều khoản trong hợp đồng.

3.2 Mô tả các điều khoản cho ngữ cảnh smart contract

Trong ngữ cảnh của bài toán trên, ta có 2 đối tượng cần xem xét là bên thuê A và bên vận chuyển B. Giữa 2 đối tượng có những quan hệ và ràng buộc, cần được chuyển thành những điều khoản cụ thể được quy định trong smart contract. Smart contract đóng vai trò là bên thứ 3 quy định các điều khoản này, tạo nên niềm tin giữa 2 bên khi 2 bên không có niềm tin tưởng cho nhau. Cụ thể ta có thể cụ thể thành các điều khoản sau cho smart contract:

Article 1.

Bên A đưa ra thông tin về hàng hóa p_info cần bên B vận chuyển (gồm tính chất, chất lượng, số lượng, ...), các thông tin về thời gian (gồm các thời gian được nêu trong các điều khoản khác), địa điểm (gồm các địa điểm được nêu trong các điều khoản khác), tiền bạc (gồm các chi phí được nêu trong các điều khoản khác). Tất cả các thông tin được smart contract ghi lại và public cho 2 phía.

Article 2.

Bên B đưa ra các thông tin về thời gian (gồm các thời gian được nêu trong các điều khoản khác), tiền bạc (gồm các chi phí được nêu trong các điều khoản khác). Tất cả thông tin được smart contract ghi nhận lại và public cho 2 phía.

Article 3.

Bên A gửi toàn bộ số tiền m_A mà bên B sẽ được nhận nếu bên B hoàn thành đúng việc vận chuyển vào smart contract. Smart contract sẽ giữ số tiền này.

Article 4.

Bên B gửi số tiền sẽ phải tiền đặt cọc m_B tối thiểu phải là số tiền bồi thường tối đa mà B phải chịu trong suốt quá trình smart contract vận hành vào smart contract. Smart contract sẽ giữ số tiền này.

Article 5.

Bên B đưa phương tiện vận chuyển đến tại nơi bên A ký gửi hàng a_A_gui trước hoặc đúng thời gian ký gửi hàng t_B_nhan được quy định trước trong smart contract. Nếu đúng, smart contract tiếp tục vận hành.

Article 6.

Nếu bên B đến nơi nhận hàng a_A_gui trễ hơn thời gian t_B_nhan chưa quá $dt\_B\_tre\_nhan$ (tức trong hạn $(t\_B\_nhan; t\_B\_nhan + dt\_B\_tre\_nhan]$) được quy định trước trong smart contract, thì bên B có trách nhiệm bồi thường khoản thiệt hại m_B_tre được quy định trước trong smart contract. Lúc này smart contract gửi số tiền m_B_tre từ smart contract vào tài khoản của A.

Article 7.

Nếu bên B đến nơi nhận hàng a_A_gui trễ hơn thời hạn tối đa cho phép trễ, tức sau $t\_B\_nhan + dt\_B\_tre\_nhan$, thì hợp đồng này coi như hủy bỏ, và bên B có trách nhiệm bồi thường với số tiền m_B_huy cho bên A. Lúc này smart contract sẽ trả lại số tiền m_A cho bên A, đồng thời gửi m_B_huy vào tài khoản A. Số tiền dư còn lại của bên B là $m\_B - m\_B\_huy$ sẽ được smart contract trả lại cho bên B

Article 8.

Nếu bên B đến nhận hàng đúng thời điểm t_B_nhan mà bên A chưa có hàng để giao không quá $dt\_A\_tre\_gui$ thì bên A có trách nhiệm bồi thường cho bên B về chi phí đi lại là $m\_A\_tre\_gui$ cho bên B. Lúc này smart contract sẽ gửi số tiền $m\_A\_tre\_gui$ từ smart contract cho bên B.

Article 9.

Nếu bên B đến nhận hàng trong thời gian quy định mà bên A không có hàng để giao quá thời gian trễ cho phép là $dt\_A\_tre\_gui$, smart contract coi như hủy bỏ và bên A phải bồi thường khoảng tiền $m\_A\_khong\_dung\_hen$ cho bên B. Lúc này smart contract sẽ gửi số tiền $m\_B + m\_A\_khong\_dung\_hen$ cho bên B và số tiền ban đầu còn lại của A $m\_A - m\_A\_khong\_dung\_hen$ cho bên A.

Article 10.

Nếu bên B đến nhận hàng trong thời gian quy định mà hàng p_nhan không đúng với bên A đề cập trong smart contract, tức $p\_nhan! = p\_info$, smart contract hủy bỏ và bên A chịu khoảng bồi thường là $mA\_khong\_dung\_hang$ cho bên B. Lúc này smart contract sẽ gửi số tiền $m\_B + mA\_khong\_dung\_hang$ cho bên B và số tiền ban đầu còn lại của A $m\_A - mA\_khong\_dung\_hang$ cho bên A.

Article 11.

Khi bên B đã hoàn tất thủ tục nhận hàng gửi, bên B phải đảm bảo giao đúng địa điểm a_A_nhan và đúng hẹn trước khoảng thời gian t_A_nhan trong smart contract. Nếu giao đúng hẹn, smart contract tiếp tục hoạt động.

Article 12.

Nếu bên B giao hàng trễ hơn so với thời gian quy định không quá $dt\_B\_tre\_gui$, bên B phải bồi thường thiệt hại cho bên A với khoảng tiền $m\_B\_tre\_gui$ cho bên A. Lúc này smart contract sẽ gửi số tiền $m\_B\_tre\_gui$ cho bên A.

Article 13.

Nếu bên B không có hàng để giao hoặc làm mất số hàng, smart contract xem như hủy bỏ và bên B bồi thường khoảng tiền $m\_B\_khong\_hang$ cho bên A. Lúc này smart contract sẽ gửi số tiền $m\_A + m\_B\_khong\_hang$ cho bên A và số tiền ban đầu còn lại của B $m\_B - m\_B\_khong\_hang$ cho bên B.

Article 14.

Bên B phải đảm bảo hàng p_nhan bên A còn nguyên vẹn, không hư hỏng và còn được niên phong nếu có (mệnh đề $hang\_on(p\_nhan)$ thỏa), nếu không bên B phải chịu bồi thường thiệt hại là $m\_B\_hang\_hong$ như trong smart contract. Lúc này smart contract sẽ gửi số tiền $m\_B\_hang\_hong$ cho A.

Article 15.

Sau khi bên B giao hàng đúng thời hạn và đúng địa điểm cho bên A, đồng thời không xảy ra bất cứ khiếu nại tranh chấp nào, smart contract coi như hoàn tất và số tiền thù lao cho B từ smart contract sau khi đã trừ các khoản bồi thường sẽ được chuyển vào tài khoản của B. Số tiền đặt cọc ban đầu của B sau khi đã trừ các khoản bồi thường nếu có cũng được trả lại cho B. Bên A lúc này không còn khoản tiền nào được nhận lại từ smart contract. Lúc này smart contract cũng không còn khoản tiền nào trong tài khoản.

Phụ lục