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

MÔ HÌNH HÓA TOÁN HỌC (CO2011)

Đề bài tập lớn

"Đặt tả Smart Contract bằng Linear Logic"

GVHD: Nguyễn An Khương
Huỳnh Tường Nguyên
Trần Văn Hoài
Lê Hồng Trang
Trần Tuấn Anh

Trợ Giảng: Nguyễn Trung Việt

SVTH: Đặng Đinh Hiển - 1611089

TP. HỒ CHÍ MINH, THÁNG 06/2018

Mục lục

1 Giới thiệu

1.1 Giới thiệu về Smart Contract

1.1.1 Lịch sử Smart Contract

- Cụm từ "Smart Contract" đã được đưa ra bởi nhà khoa học máy tính Nick Szabo vào năm 1994 và liên tục được ông tìm hiểu và phát triển trong nhiều năm liền. Ông đã cho ra mắt 2 cuốn sách là "Smart Contract" và "Formalizing and Securing Relationships on Public Networks". Các cuốn sách của ông miêu tả cách hoạt động cũng như cách thiết lập và xây dựng nên hợp đồng thông minh trong giao dịch điện tử được thực hiện thông qua Internet. Szabo lấy cảm hứng từ nhà nghiên cứu David Chaum, ông kì vọng vào việc hợp đồng thông minh sẽ rõ ràng hơn hợp đồng hợp đồng truyền thống với các đặc tả logic. Việc xác nhận và thực thi hợp đồng sẽ thông qua các giao thức máy tính. Tuy nhiên tại thời điểm này do chưa có điều kiện về môi trường và phương tiện vẫn chưa cho phép việc phát triển Smart Contract một cách hoàn thiện. Đến khi công nghệ BlockChain và Ethereum ra đời đã tạo một bước nhảy cho smart contract. Đưa smart contract vào ứng dụng trong nhiều lĩnh vực và ngày càng hoàn thiện.

1.1.2 Ứng dụng của Smart Contract

Smart Contract có thể được ứng dụng trong nhiều lĩnh vực. Sau đây là một số lĩnh vực đã và đang nghiên cứu sử dụng smart contract.

- Ứng dụng trong bảo hiểm: Các yêu cầu bảo hiểm thường rất nhiều và mất thời gian để xác thực bồi thường khách hàng. Với smart contract ta có thể thiết lập giao kèo giữa các bên tham gia để khi có sự kiện xảy ra thì việc bồi thường bảo hiểm sẽ tự động xảy ra chứ ko phải chờ làm thủ tục và duyệt bảo hiểm nữa.

- Ứng dụng trong bản quyền: người sở hữu bản quyền sẽ công khai thông tin bản quyền của người đó lên mạng blockchain, chính sách sử dụng bản quyền tác phẩm sẽ được thiết lập trong smart contract và mỗi khi tác phẩm của họ được sử dụng thì chính sách sử dụng sẽ được tuân thủ và thực hiện tức thời.

- Ứng dụng trong logistics: chuỗi cung ứng mà một hệ thống phức tạp gồm nhiều mối liên kết kế tiếp khác nhau. Mỗi liên kết cần phải nhận được xác nhận bởi cái ở trước để đủ điều kiện thực hiện phần việc của mình theo như hợp đồng. Ứng dụng 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 (Internet of Things).

1.2 Giới thiệu về Linear Logic

1.2.1 Lịch sử Linear Logic

- Linear Logic được giới thiệu bởi J.-Y Girard trong năm 1987, và gây nhiều sự chú ý tới các nhà khoa học máy tính bởi ý tưởng kiểm soát tài nguyên. Ý tưởng của Linear Logic sự tái phát triển của Logic cổ điển ở chỗ nó đưa thêm các khái niệm như nguồn lực, tài nguyên. Điều này đã khiến Linear Logic thu hút nhiều sự chú ý từ các nhà khoa học máy tính, vì nó là một cách hợp lý để xử lý và kiểm soát các tài nguyên, nguồn lực.

1.2.2 Ứng dụng của Linear Logic

Do tính kiểm soát tài nguyên là cực kì quan trọng trong ngành Khoa học máy tính, mà Linear Logic lại đáp ứng được nhu cầu đó nên nó đã được áp dụng vào một số lĩnh vực như :

- Functional programming.
- Logic programming.
- General theories of concurrency.
- Syntactic and semantic theories of natural language.
- Artificial intelligence planning.

1.2.3 Các phép toán Linear Logic

- Phép $\perp$ được gọi là phép linear negation ("Phủ định tuyến tính"). Biểu thức $A^{\perp}$ được gọi là "không A hay phủ định A". Ví dụ bên dưới sẽ minh họa cho điều này:
  Ví dụ 1: Giả sử A là mệnh đề "Tôi có \$10" thì $A^{\perp}$ là mệnh đề "Tôi không có \$10".
- Phép $\top$ là true ("Đúng đắn").
- Một số tính chất đặc biệt của Linear Logic được biểu diễn thông qua 2 toán tử được gọi là "exponentials".
  - Toán tử "!" thể hiện tính chất vô hạn của tài nguyên, nguồn lực. !A còn được gọi là Of course A.

    Ví dụ 2: Với phép toán logic thông thường $A \longrightarrow B$. Trong logic thông thường khi ta có A và $A \longrightarrow B$ thì ta có thể thực hiện phép suy luận $A \longrightarrow B$ một cách nhiều lần như một chân lý. Trong linear logic để thực hiện phép biểu diễn này do chúng ta có thêm một số khái niệm về tài nguyên, nguồn lực nên ta phải biểu diễn lại với linear logic như sau: $!A \multimap B$ Vậy với tính chất của phép "!" ta có thể định nghĩa lại $A \longrightarrow B$ thành $!A \multimap B$ trong linear logic.
  - Toán tử "?" thể hiện tính chất thực tế (actuality)của của nguồn lực, tài nguyên vô tận(potential resource inexhaustibility). Nguồn lực, tài nguyên vô tận(potential unexhaustibility) này bị phụ thuộc vào sự bổ sung thực tế (actual replenishment) ?A còn được gọi là Why not A. ?A có thể được định nghĩa lại như sau $(!A)^{\perp}$.

    Ví dụ 3: Gọi tài nguyên A là một phần của bộ nhớ máy tính, chúng ta có thể chỉ ra được dung lượng máy tính cần thiết cần mở rộng thêm (actual replenishment) để đáp ứng cho nhu cầu sử dụng của máy tính.

2 Xây dựng và mô tả ngữ cảnh cho một smart contract

2.1 Mô tả ngữ cảnh mua bán Website cho smart contract

Công Ty A muốn có một Website bán hàng để phục vụ dịp tết 2019 âm lịch, nên công ty A muốn có một Website trước ngày 31/12/2018. Doanh nghiệp B muốn đứng ra viết một Website đáp ứng cho Công Ty A. Hai bên quyết định lập một smart contract với nội dung cụ thể như sau:

- Trị giá của website là \$2000
- Để đảm bảo doanh nghiệp B thực hiện đúng hạn và hiệu quả , công ty A yêu cầu doanh nghiệp B phải bỏ ra 20% số tiền hợp đồng (\$400) làm tiền cọc, phòng trường hợp đúng ngày kết thúc hợp đồng mà chưa có website thì \$400 là chi phí bồi thường cho doanh nghiệp A, còn nếu có đầy đủ Website + \$2000(tiền của bên A) + \$400(tiền cọc của bên B) thì sẽ tiến hành giao website cho bên A, hoàn trả \$400 cho bên B và trả thêm cho bên B \$2000 giá trị website.

2.2 Chuyển ngữ cảnh mua bán Website dưới dạng các điều khoản

Hợp đồng sẽ gồm 2 giai đoạn:

- Giai đoạn 1: 11h30 AM - 8/8/2018 là thời điểm hai bên sẽ gửi tiền website và tiền cọc đến smart contract (Bên A gửi $2000 ,bên B gửi $400).
  - Article 1. Bên A gửi $2000 đến smart contract trước 11h30 AM - 8/8/2018, số tiền này sẽ được smart contract giữ lại.
  - Article 2. Bên B gửi $400 đến smart contract trước 11h30 AM - 8/8/2018, số tiền này sẽ được smart contract giữ lại.
  - Article 3. 11h30 AM - 8/8/2018 nếu có đủ $2000 (của bên A) và $400 (của bên B) thì tiến hành giai đoạn 2 của hợp đồng.
  - Article 4. 11h30 AM - 8/8/2018 Bên A gửi $2000 nhưng bên B vẫn chưa gửi $400 thì hoàn trả lại $2000 cho bên A, kết thúc hợp đồng (không chuyển qua giai đoạn 2).
  - Article 5. 11h30 AM - 8/8/2018 Bên B gửi $400 nhưng bên A vẫn chưa gửi $2000 thì hoàn trả $400 cho bên B và kết thúc hợp đồng.
- Giai đoạn 2: 11h30 AM - 31/12/2018 bên B phải gửi website đến smart contract.
  - Article 6. Bên B gửi website đến smart contract trước 11h30 AM - 31/12/2018 và được smart contract giữ lại.
  - Article 7. 11h30 AM - 31/12/2018 nếu đã có website thì chuyển website cho bên A, chuyển $2000 (tiền website) và $400 (tiền cọc) cho bên B.
  - Article 8. 11h30 AM - 31/12/2018 nếu chưa có website thì hoàn trả $2000 cho bên A, cộng thêm $400 (tiền bồi thường) cho bên A.

3 Đặt tả ngữ cảnh mua bán Website bằng linear logic

- Công ty A bỏ ra $2000 để nhờ doanh nghiệp B viết sản phẩm website (“website”).

$$\$2000 \multimap website$$

- Doanh Nghiệp B muốn hợp đồng với bên Công ty A phải bỏ ra $400 làm tiền đặt cọc để đảm bảo đúng hạn hợp đồng (contract).

$$\$400 \multimap contract$$

Giai đoạn 1:

- 11h30 AM ngày 8/8/2018 (“times” thời gian giao dịch đầu tiên) nếu bên công ty A gửi $2000 và $400 tiền cọc của công ty B thì chờ đến thời điểm thực hiện giai đoạn 2(“check_s1true”) 11h30 AM - 31/12/2018 (“times2”), nghĩa là đã thực hiện thành công giai đoạn 1.

$$times \otimes \$400 \otimes \$2000 \multimap check\_s1true \otimes \$400 \otimes \$2000$$

- Nếu 11h30 AM ngày 8/8/2018 (“times” thời gian giao dịch đầu tiên) chưa có $400 từ công ty A hoặc $2000 từ công ty B thì sẽ hủy hợp đồng, không chuyển qua giai đoạn 2, trả tiền cọc cho doanh nghiệp B (returnWalletB) hoặc trả tiền cho công ty A (returnWalletA).

$$times \otimes (\$400 \oplus \$2000) \multimap returnWalletA \vee returnWalletB$$

Giai đoạn 2:

- 11h30 AM ngày 31/12/2018 ("times2" thời gian giao dịch lần 2) nếu bên B tiến hành gửi website thì sẽ tiến hành giao dịch: bên công ty A nhận website (rcWebsite) và trả $2000 tiền cho bên doanh nghiệp B (sendWalletB) và hoàn trả $400 tiền cọc ban đầu (returnWalletB).

$$times2 \otimes website \otimes check\_s1true \otimes \$400 \otimes \$2000$$

$$\multimap rcWebsite \otimes sendWalletB \otimes returnWalletB$$

- 11h30 AM ngày 31/12/2018 ("times2" thời gian giao dịch lần 2) nếu bên B chưa gửi website thì sẽ phải đền bù cho bên công ty A $400 tiền cọc ban đầu coi như tiền bồi thường (sendWalletA) và trả $2000 về cho công ty A.

$$times2 \otimes website^{\perp} \otimes check\_s1true \otimes \$400 \otimes \$2000 \multimap sendWalletA \otimes returnWalletA$$

- Nếu trước 11h30 AM ngày 31/12/2018 ("times2" thời gian giao dịch lần 2), công ty B gửi website thì sẽ được smart contract giữ lại và chờ đến stage2 để thực hiện hợp đồng.

$$times2^{\perp} \otimes website \otimes check\_s1true \otimes \$400 \otimes \$2000$$

$$\multimap rcWebsite^{\perp} \otimes sendWalletB^{\perp} \otimes returnWalletB^{\perp}$$

4 Dùng mã giả xây dựng một smart contract cho ngữ cảnh mua bán Website

```
input: CtyA , DnB , tien_website, tien_coc ,website, time_s1, time_s2
output:
if Converting system time to timestamp >= time_s1 then
|   if tien_coc > 0 & tien_website > 0 then
|   |   if Converting system time to timestamp = time_s2 then
|   |   |   if exists(website) then
|   |   |   |   Transfer tien_coc to DnB;
|   |   |   |   Transfer tien_website to DnB;
|   |   |   |   Transfer website to ctyA;
|   |   |   end
|   |   |   else
|   |   |   |   Transfer tien_coc to CtyA;
|   |   |   |   Transfer tien_website to CtyA;
|   |   |   end
|   |   end
|   |   else if Converting system time to timestamp < time_s2 then
|   |   |   Do not anything, waiting...;
|   |   end
|   end
|   else
|   |   if tien_coc > 0 then
|   |   |   Transfer tien_coc to DnB;
|   |   end
|   |   else if tien_website > 0 then
|   |   |   Transfer tien_website to CtyA;
|   |   end
|   end
end
else
|   Do not anything, waiting...;
end
```