

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN TOÁN ỨNG DỤNG VÀ TIN HỌC



ỨNG DỤNG BLOCKCHAIN TRONG HỆ THỐNG
TRUY XUẤT NGUỒN GỐC CHUỖI CUNG ỨNG

ĐỒ ÁN II

Chuyên ngành: TOÁN TIN

Chuyên sâu: TIN HỌC

Giảng viên hướng dẫn:

ThS. Lê Quang Hòa

Sinh viên thực hiện:

Nguyễn Trọng Tuấn

Lớp:

CTTN Toán Tin K62

HÀ NỘI-2020

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

1. Mục đích và nội dung của đồ án:

2. Kết quả đạt được:

3. Ý thức làm việc của sinh viên:

Hà Nội, ngày ... tháng ... năm ...

Giảng viên hướng dẫn

(Ký và ghi rõ họ tên)

Mục Lục

1	Phần Mở Đầu	6
2	Cơ sở lý thuyết	7
2.1	Truy xuất nguồn gốc	7
2.1.1	Định nghĩa	7
2.1.2	Ứng dụng	8
2.1.3	Lợi ích của truy xuất nguồn gốc đối với chuỗi cung ứng	8
2.1.4	Các vấn đề với hệ thống truy xuất nguồn gốc hiện tại	9
2.1.5	Đặc điểm của một hệ thống truy xuất nguồn gốc hiệu quả . . .	10
2.2	Blockchain	11
2.2.1	Định nghĩa	11
2.2.2	Cơ chế hoạt động	12
2.2.3	Lợi ích của việc áp dụng blockchain vào hệ thống truy xuất nguồn gốc	13
2.2.4	Các nghiên cứu về hệ thống truy xuất nguồn gốc dựa trên blockchain	14
3	Đặc tả và thiết kế hệ thống	16
3.1	Giả thuyết hệ thống	16
3.2	Tiến trình	16
3.3	Đặc tả	16
3.3.1	Hệ thống truy xuất nguồn gốc	16
3.3.2	Doanh nghiệp	18
3.4	Nền tảng blockchain	19
3.4.1	Các nền tảng hiện tại	19
3.5	Mạng công khai hay mạng riêng tư	19
3.5.1	Tính năng	19

3.5.2	Lựa chọn	20
3.6	Hyperledger	20
3.6.1	Định danh	20
3.6.2	Cơ chế đồng thuận	21
3.6.3	Quyền truy cập và tính riêng tư	21
3.7	Mô hình mạng chuỗi cung ứng	22
3.8	Phương pháp xây dựng	24
3.9	Sản phẩm khả dụng tối thiểu	24
3.10	Hoàn thành phần còn lại của hệ thống	25
3.10.1	Mô hình mạng	25
3.10.2	Mô hình dữ liệu	25
4	Cài đặt hệ thống	26
4.1	Ảnh xạ thiết kế tới các bộ phận	26
4.2	Ảnh xạ mô hình mạng vào mô hình mạng Fabric	26
4.2.1	Docker	26
4.2.2	Mô hình hóa	27
4.2.3	Thêm thành viên cho mạng chuỗi cung ứng	27
4.3	Ảnh xạ sơ đồ thực thể liên kết vào CouchDB	28
4.3.1	Tài sản	28
4.3.2	Các mô hình giao dịch	28
4.4	Logic nghiệp vụ trong các hàm giao dịch	29
4.5	Cơ chế đồng thuận	31
4.5.1	Chứng thực	31
4.5.2	Ordering	32
4.5.3	Thẩm định	32
4.6	Giao diện người dùng	32
5	Thảo luận	33
5.1	Đánh giá phần mềm	33
5.2	Truy xuất nguồn gốc	33
5.3	Đánh giá dự án	34
5.3.1	Các tài liệu tham khảo	34
5.3.2	Nắm bắt các yêu cầu	34

5.3.3	Thiết kế	35
5.3.4	Các nghiên cứu tiếp theo	35
6	Phần Kết Luận	36

1 Phần Mở Đầu

Truy xuất nguồn gốc chuỗi cung ứng đang là một vấn đề ngày càng quan trọng bởi các quan ngại của các nhà hành pháp, chính phủ về an toàn thực phẩm cũng như nhu cầu của người tiêu dùng về một sản phẩm chất lượng cao.

Hiện tại đã có một số hệ thống truy xuất nguồn gốc đang hoạt động theo dạng trao đổi thông tin chỉ giữa hai tổ chức với nhau tạo ra sự thiếu tin tưởng lẫn nhau. Bởi vì các ưu đãi về kinh tế và pháp lý, các doanh nghiệp hiện nay đang tìm kiếm một nước đi đột phá để giải quyết vấn đề này.

Blockchain được nhắc tới như là một công nghệ có thể cách mạng hóa mô hình chuỗi cung ứng hiện tại, hứa hẹn sẽ giải quyết được thách thức trong sự thiếu tin cậy trong thông tin giữa các tổ chức trong chuỗi cung ứng.

Báo cáo này sẽ triển khai một hệ thống truy xuất nguồn gốc dựa trên blockchain từ các mô hình mạng lưới chuỗi cung ứng, và cho thấy rằng công nghệ blockchain là một công nghệ lý tưởng để thay thế cho hệ thống truy xuất nguồn gốc hiện tại trong thời gian sắp tới.

Báo cáo được hoàn thành dưới sự hướng dẫn tận tình của ThS. Lê Quang Hòa cùng các thầy cô là giảng viên của Viện Toán Ứng dụng và Tin học. Tôi xin được gửi lời cảm ơn chân thành nhất đến các thầy cô cùng các bạn sinh viên của lớp CTTN Toán Tin K62 đã đóng góp những ý kiến quý báu cho bài báo cáo. Tuy nhiên, dù đã cố gắng hết sức nhưng chắc chắn báo cáo vẫn còn những sai sót. Tôi mong nhận được những góp ý để bài báo cáo được hoàn thiện hơn. Xin chân thành cảm ơn!

2 Cơ sở lý thuyết

2.1 Truy xuất nguồn gốc

2.1.1 Định nghĩa

Có rất nhiều các nghiên cứu khoa học đề cập tới việc truy xuất nguồn gốc, đặc biệt là trong lĩnh vực công nghiệp thực phẩm. Ta cần phải biết hệ thống đang xây dựng chính xác sẽ truy vết cái gì.

Moe [21] định nghĩa hai loại của truy xuất nguồn gốc :

1. *Sản phẩm: Truy vết về vật liệu, nguồn gốc, quá trình sản xuất tiêu thụ và lịch sử phân phối.*
2. *Dữ liệu: Truy vết về các tính toán và dữ liệu được tạo ra trong suốt vòng chất lượng, đôi khi nó truy vết các yêu cầu về chất lượng.*

Theo tiêu chuẩn ISO [1] định nghĩa truy vết nguồn gốc sản phẩm là việc theo dõi các thông tin của sản phẩm tiêu dùng như là nguồn gốc, vật liệu, quá trình sản xuất, quá trình phân phối của sản phẩm trước khi tới tay người tiêu dùng.

Việc truy xuất nguồn gốc không chỉ được giới hạn trong ngành công nghiệp thực phẩm mà còn được ứng dụng rộng rãi trong nhiều lĩnh vực khác như nghệ thuật [29] hoặc dược phẩm [24]. Golan và đồng nghiệp [11] đưa ra một định nghĩa khái quát hơn là truy xuất nguồn gốc là một công cụ để có thể đạt được một số mục tiêu khác nhau”.

Trong báo cáo này, truy xuất nguồn gốc sẽ được hiểu như việc theo dõi quá trình biến đổi của sản phẩm hoặc quá trình di chuyển của sản phẩm trước khi tới được tay người dùng.

2.1.2 Ứng dụng

Để tránh việc làm giả phô mai Parmesan, một nhóm các nhà cung cấp phô mai Ý đã triển khai hệ thống truy xuất nguồn gốc để có thể xác định được phô mai chính hãng. Sữa bò được làm thành sữa tươi rồi sau đó mới được làm thành phô mai; phô mai sau đó được theo dõi suốt quá trình ủ và phân phối tới các nhà bán lẻ.

Các thông tin về sản phẩm được lưu lại ở nhiều trạng thái trong chuỗi cung ứng, ví dụ như ở trạng thái sữa tươi sẽ có các thông tin như nhiệt độ và mã chú bò được lấy sữa. Sau đó, với mỗi một lô hàng phô mai sẽ được gắn một chip RFID để có thể theo dõi thông tin. Sau quá trình chế biến, phô mai được ủ trong nhà kho và có thêm các thông tin như nhiệt độ, độ ẩm. Trước khi được đưa tới các siêu thị, phô mai trong từng lô được cắt nhỏ và được in thêm mã định danh trên bao bì sản phẩm.

Các thông tin được theo dõi trong suốt quá trình từ sữa bò đến các siêu thị giúp người dùng có thể chắc chắn rằng phô mai đang sử dụng là phô mai Parmesan chính hãng [26]

2.1.3 Lợi ích của truy xuất nguồn gốc đối với chuỗi cung ứng

Trong ngành công nghiệp thực phẩm, có rất nhiều đề tài nghiên cứu về chủ đề truy xuất nguồn gốc do có lợi ích lớn về kinh tế. Trong một báo cáo của Bộ Nông nghiệp Hoa Kỳ (USDA) về truy vết nguồn gốc nói rằng các hệ thống truy xuất nguồn gốc có xu hướng được thúc đẩy bởi các động lực kinh tế, chứ không phải quy định về truy xuất nguồn gốc của chính phủ” và ”khi các tác động tiêu cực của phân phối thực phẩm không an toàn tăng cao, lợi ích của các hệ thống truy xuất nguồn gốc là không thể bàn cãi”. [11]

Một số lợi ích kinh tế đối với các doanh nghiệp áp dụng hệ thống truy xuất nguồn gốc: [11]

- *Quản lý chuỗi cung ứng - các doanh nghiệp có thể cải thiện hiệu suất của các hoạt động logistics khi sử dụng các dữ liệu thu thập được trong hệ thống truy xuất.*
- *Chất lượng và an toàn - dựa vào hệ thống truy xuất nguồn gốc, việc thu hồi các sản phẩm trở nên dễ dàng và ít chi phí hơn vì tính chính xác của thông tin. Ngoài ra, trách nhiệm pháp lý của các cá nhân và tổ chức cũng có thể dễ dàng xác định.*

- *Doanh số cao hơn nhờ tính chính xác của thông tin của hệ thống truy xuất nguồn gốc.*

Ở một số quốc gia, việc truy xuất nguồn gốc của thông tin được thực hiện ở các mức độ khác nhau do bộ luật yêu cầu để có thể cải thiện sức khỏe cộng đồng. Ví dụ như ở Thụy Điển, sau đợt bùng phát của vi khuẩn salmonella, chính phủ Thụy Điển đã phải kiểm tra nghiêm ngặt việc nhập khẩu đối với thịt tươi và trứng. [9]

Khả năng có thể truy xuất nguồn gốc còn có thể áp dụng trong việc chứng minh quyền sở hữu. Đặc biệt là đối với các tài sản có giá trị cao như kim cương [27] hoặc tranh vẽ [29].

Trong các tình huống mà sai sót có thể dẫn đến hậu quả lớn cũng rất phù hợp với một hệ thống truy xuất nguồn gốc. Ví dụ như trong y tế, việc xác định được chính xác nguồn gốc của máu và nội tạng là việc tối quan trọng [22].

Một lợi ích khác của hệ thống truy xuất nguồn gốc đó là chống hàng giả - một trong những vũ khí tối thượng để chống lại nạn thuốc giả đó là theo dõi hoàn toàn và hệ thống quản lý truy vết có khả năng xác thực thuốc và nguồn gốc của nó”[19].

2.1.4 Các vấn đề với hệ thống truy xuất nguồn gốc hiện tại

Golan và các cộng sự [11] cho rằng nhiều công ty đã có sẵn hệ thống truy xuất nguồn gốc hoạt động hiệu quả của riêng họ. Tuy nhiên, trong nhiều trường hợp các hệ thống đó vẫn khó có thể truy xuất được sản phẩm trong chuỗi cung ứng.

Giải pháp cho vấn đề này chính là khả năng tương tác giữa các tác nhân trong chuỗi cung ứng. [2] Bechini và các cộng sự [4] khẳng định rằng ”ví dụ, với nhà bán lẻ không nên buộc phải tương tác với một số lượng lớn các hệ thống riêng biệt chỉ để đáp ứng các yêu cầu về truy xuất nguồn gốc... tốt hơn là truy cập vào một hệ thống duy nhất để có thể cung cấp tất cả thông tin được yêu cầu”.

Để thực hiện điều đó thì ta cần một hệ thống tập trung, nhưng Golan và các cộng sự [11] cho rằng điều đó có thể rất khó hoặc thậm chí là không thể, ngay cả khi có các quy định mới:

Chính phủ cũng có thể xem xét việc ủy quyền truy xuất nguồn gốc để tăng cường an toàn thực phẩm, nhưng việc ủy quyền như vậy có thể gây ra sự kém hiệu quả đối với các hệ thống truy xuất nguồn gốc tư nhân đã hiệu quả. Việc sử dụng tự nguyện rộng rãi truy xuất nguồn gốc làm phức tạp việc áp dụng hệ thống tập trung vì các công ty đã phát triển rất nhiều cách tiếp cận và hệ thống theo dõi

khác nhau. Nếu các hệ thống bắt buộc không cho phép các thay đổi trong hệ thống xác định nguồn gốc, chúng có thể sẽ buộc các công ty phải điều chỉnh các hệ thống đã hiệu quả hoặc tạo ra các hệ thống song song.”

2.1.5 Đặc điểm của một hệ thống truy xuất nguồn gốc hiệu quả

Sau đây là một số đặc điểm của một hệ thống truy xuất nguồn gốc hiệu quả đã được đúc kết lại trong quá trình nghiên cứu. Những đặc điểm này sẽ giúp ích rất nhiều cho việc xây dựng hệ thống truy xuất nguồn gốc dựa vào blockchain trong báo cáo này. Golan và các cộng sự [11] cho rằng Các đặc tính của hệ thống truy xuất nguồn gốc tốt rất khác nhau và không thể xác định được nếu không tham chiếu đến các yêu cầu của hệ thống”. Mặc khác, Storøy và cộng sự [28] lại cho rằng Có một số phương pháp và nguyên tắc được thiết lập chặt chẽ để làm cơ sở cho việc xây dựng hệ thống truy xuất nguồn gốc hiệu quả trong ngành công nghiệp thực phẩm; chúng được đề cập trong các nghiên cứu trước đây”.

Trong báo cáo này, việc truy xuất nguồn gốc được tập trung vào chuỗi cung ứng cho phép ta xây dựng hệ thống truy xuất nguồn gốc mang đặc thù riêng.

Ta bắt đầu với định nghĩa của McKean [20]:

Hệ thống truy xuất nguồn gốc sản phẩm đòi hỏi một chuỗi hành trình minh bạch để đạt được uy tín của nó và để hoàn thành các chức năng truy xuất và truyền tải thông tin mong muốn. Truy vết nguồn gốc sản phẩm có hai thành phần như sau:

- *Hệ thống định danh sản phẩm hoặc động vật độc nhất*
- *Một chuỗi hành trình minh bạch hoặc định danh có thể xác thực được*

Regattieri và các cộng sự [26] đi vào chi tiết hơn:

Hệ thống truy xuất nguồn gốc sản phẩm và đặc biệt là hệ thống truy xuất thực phẩm cơ bản dựa vào 4 yếu tố chính: định danh sản phẩm, dữ liệu để truy xuất, định tuyến sản phẩm và các công cụ truy xuất nguồn gốc.

Điều này đặt ra một số câu hỏi cần được xem xét khi thiết kế một hệ thống truy xuất nguồn gốc:

- Định danh sản phẩm - Làm thế nào để sản phẩm có mã định danh duy nhất?

- Dữ liệu để truy xuất - Nhưng dữ liệu nào cần thu thập? Nó được lưu trữ thế nào? Ai có quyền truy cập vào dữ liệu đó?
- Định tuyến sản phẩm - Dữ liệu được thu thập ở giai đoạn nào trong chuỗi cung ứng?
- Công cụ truy xuất nguồn gốc - Cần những công cụ bổ sung nào để có thể tích hợp hệ thống truy xuất nguồn gốc với quy trình hiện tại của chuỗi cung ứng?

Các yếu tố "dữ liệu để truy xuất" và "định tuyến sản phẩm" có thể được kết hợp lại thành thu thập dữ liệu truy xuất nguồn gốc". Do đó mà định nghĩa của Regattieri và của McKean trở nên tương đồng với hai yếu tố chính của một hệ thống truy xuất sản phẩm hiệu quả - mã định danh duy nhất và các bản ghi dữ liệu về các thay đổi của sản phẩm.

Hai yếu tố này có thể đủ cho một hệ thống truy xuất nguồn gốc trong nội bộ của một tổ chức. Tuy nhiên, để có thể truy xuất nguồn gốc một các hiệu quả nhất, các hệ thống nội bộ này cần phải có khả năng giao tiếp với nhau giữa các tổ chức. Do đó, hệ thống xác định nguồn gốc hiệu quả cần phải có thành phần thứ ba là sự giao tiếp giữa các tổ chức trong chuỗi cung ứng.

Tổng kết lại, một hệ thống truy xuất nguồn gốc tốt cần phải có ba yếu tố chính:

1. Mã định danh duy nhất cho từng đơn vị sản phẩm
2. Bản ghi dữ liệu về các thay đổi của sản phẩm
3. Sự trao đổi thông tin giữa các tác nhân của chuỗi cung ứng

2.2 Blockchain

2.2.1 Định nghĩa

Blockchain có thể được hiểu như một nhóm các công nghệ có những đặc điểm tương tự nhau. Jansson và Peterson [25] cung cấp một bản tóm tắt về các định nghĩa của blockchain.

Đúc kết lại, công nghệ blockchain có các thuộc tính cơ bản:

- Mạng phân tán ngang hàng - Các nút mạng là tác nhân của chuỗi cung ứng
- Sổ cái - Một bản ghi các giao dịch trong mạng mà các tác nhân trong mạng đều có một bản giống nhau.
- Hợp đồng thông minh - Các logic có thể lập trình được và gắn với các giao dịch

Lưu ý rằng trong hợp đồng thông minh, logic được gắn với chính giao dịch, không giống như logic nghiệp vụ được gắn với cơ sở dữ liệu của ứng dụng và có các quy tắc (như kiểm soát quyền truy cập) thường được đặt ở toàn bộ ở cấp cơ sở dữ liệu hoặc trong ứng dụng, chứ không phải trong giao dịch. [14] Nhiều hệ thống blockchain có một số đặc tính hữu ích khác ngoài những đặc tính được liệt kê bên trên, ví dụ như có thể dễ dàng phát hiện hành vi gian lận. [14]

2.2.2 Cơ chế hoạt động

Theo một cách đơn giản, người tham gia mạng blockchain sẽ gửi đi các giao dịch để có thể cập nhật vào sổ cái. Sau đó, những người tham gia sẽ thông qua một cơ chế đồng thuận để chấp thuận và bác bỏ việc thêm các giao dịch đó vào sổ cái.

Mạng công khai và mạng riêng tư

Các công nghệ blockchain có thể chia ra làm loại chính là công khai và riêng tư.

Trong mạng blockchain công khai, bất kỳ ai cũng đều có thể tham gia. Hệ quả là những mạng công khai có thể có nhiều người dùng giả mạo và cần phải có một cơ chế đồng thuận chặt chẽ để tránh việc bị thao túng sổ cái của mạng. Các mạng blockchain công khai nổi tiếng như Bitcoin, Ethereum và nhiều loại tiền điện tử khác. [3]

Trong mạng blockchain riêng tư, chỉ có những cá nhân hoặc tổ chức được cấp quyền tham gia mới có thể cập nhật thông tin cho sổ cái. Điều này có nghĩa là mạng riêng tư có thể sử dụng cơ chế đồng thuận ít nghiêm ngặt hơn (ít tốn tài nguyên hơn) có thể được sử dụng. [14] Các mạng blockchain riêng tư hay được biết đến như Hyperledger Fabric, MultiChain và Corda. [13]

Byzantine Fault Tolerance

Byzantine Fault Tolerance (BFT) hay còn gọi là hệ thống chịu lỗi Byzantine lần đầu tiên được nhắc đến trong bài báo khoa học có tên là The Byzantine Generals Pro-

blem”[18], trong đó các thành viên trong mạng là các vị tướng lĩnh cần phải tìm ra phương thức để có thể đồng ý kế hoạch chiến đấu chung:

”Hệ thống máy tính đáng tin cậy là một hệ thống có khả năng xử lý các thành phần bị trục trặc mà gửi thông tin gây xung đột cho các thành phần khác nhau của hệ thống. Tình huống này có thể diễn đạt một cách trêu tượng khi một nhóm tướng lĩnh của quân đội Byzantine đóng quân xung quanh một thành phố của đối phương. Họ chỉ có thể giao tiếp với nhau bằng các sứ giả, các tướng lĩnh phải thống nhất được kế hoạch chiến đấu chung cho toàn quân. Tuy nhiên, có thể xuất hiện một số kẻ phản bội cố gắng truyền đi thông tin gây mâu thuẫn. Bài toán là tìm ra một thuật toán để cho các vị tướng trung thành có thể đồng thuận được một kế hoạch chung.”

Một mạng với Byzantine Fault Tolerant đảm bảo rằng các giao dịch trong sổ cái là đúng nếu phần lớn các thành viên hoạt động chính xác, ngay cả khi có một số thành viên gây ra lỗi”. [7]

Cơ chế đồng thuận

Trong một mạng blockchain công khai, cơ chế đồng thuận thường được dùng là Byzantine Fault Tolerant, ví dụ như cơ chế Proof of Work (PoW) của Bitcoin. [23] Điểm yếu của cơ chế này là nó cần rất nhiều tài nguyên tính toán và thông lượng giao dịch thấp. [10] Trong các mạng blockchain riêng tư, do chỉ cho phép các thành viên đáng tin cậy tham gia nên có thể sử dụng cơ chế đồng thuận đơn giản hơn dựa trên biểu quyết, cho phép thông lượng giao dịch cao hơn và chi phí tài nguyên thấp hơn. [16]

2.2.3 Lợi ích của việc áp dụng blockchain vào hệ thống truy xuất nguồn gốc

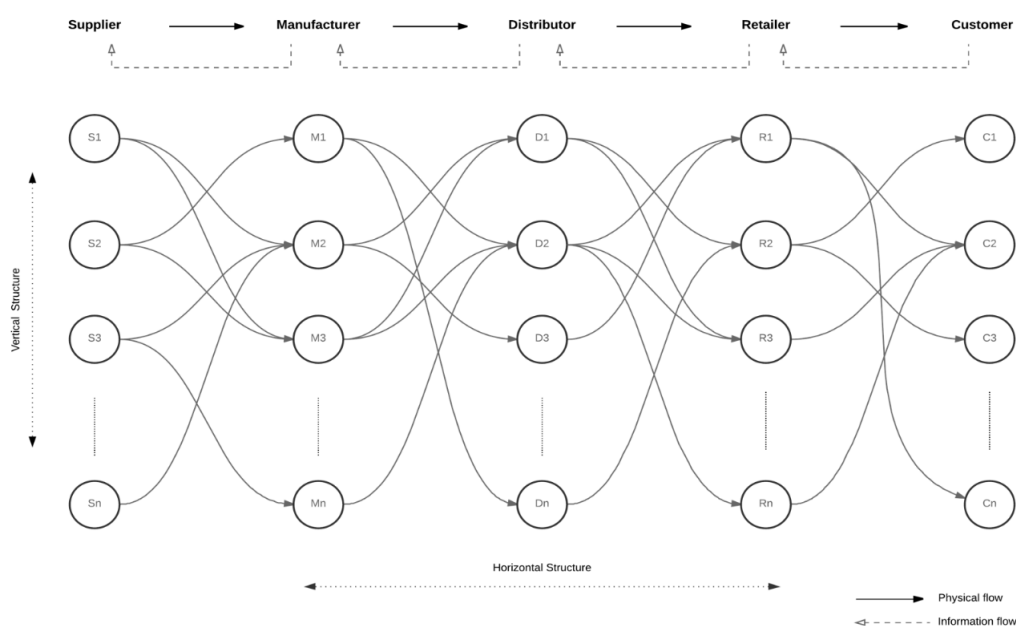
Một trong những khó khăn của hệ thống truy xuất nguồn gốc là các thành viên tham gia khó có thể giao tiếp với nhau. Việc sử dụng các định dạng dữ liệu được chuẩn hóa với một hệ thống tập trung đã đạt được một số cải thiện nhất định, nhưng khó có thể thực hiện được trên toàn bộ chuỗi cung ứng do chi phí lớn.

Các hệ thống blockchain được thiết kế phù hợp với hệ thống phân tán, trong đó các thành viên trao đổi thông tin với nhau thông qua sổ cái. Do đó mà blockchain có thể là một nền tảng công nghệ phù hợp để triển khai một hệ thống truy xuất nguồn gốc.

2.2.4 Các nghiên cứu về hệ thống truy xuất nguồn gốc dựa trên blockchain

Chen

Chen [8] đã cài đặt một chuỗi cung ứng với một ý tưởng chung về hàng hóa và những thành viên tham gia bằng cách sử dụng Hyperledger. Mô hình mạng của Chen được biểu thị qua Hình 2.1

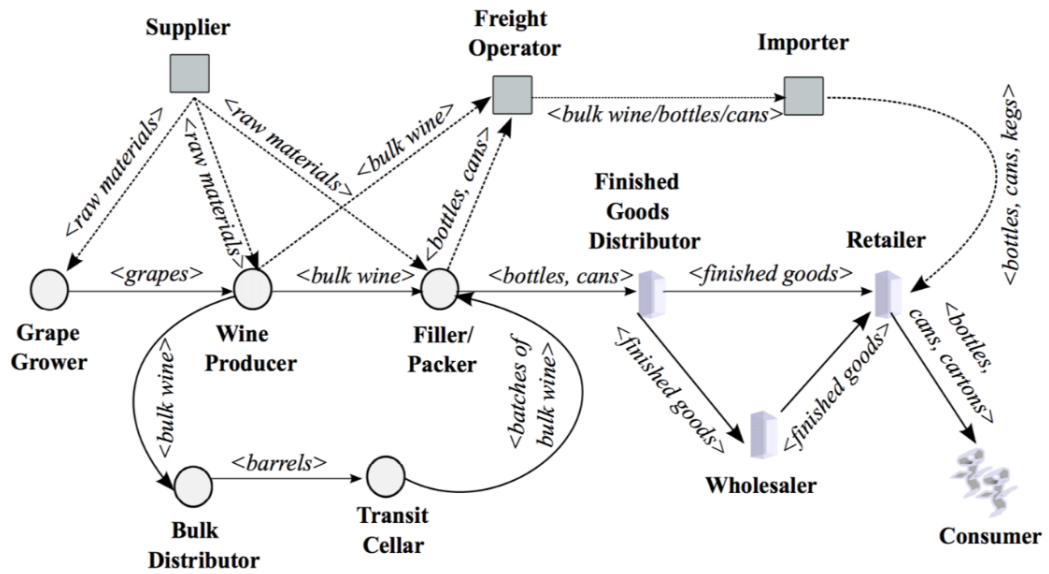


Hình 2.1: Mô hình mạng lưới chuỗi cung ứng của Chen

Cách cài đặt này khó có thể được áp dụng vào thực tế vì nó quá tổng quát và sẽ không phù hợp với những yêu cầu của hệ thống truy xuất nguồn gốc dựa trên blockchain sẽ được nêu trong Chương 3.

Biswas

Biswas và các cộng sự [5] lại sử dụng mạng MultiChain để truy xuất nguồn gốc trong chuỗi cung ứng rượu vang và cho ta một cái nhìn đầy đủ về mô hình mạng, cũng như những yêu cầu về dữ liệu tại mỗi giai đoạn trong chuỗi cung ứng. Mô hình mạng của Biswas được biểu thị trong Hình 2.2.



Hình 2.2: Mô hình mạng lưới chuỗi cung ứng rượu vang của Biswas và các cộng sự

3 Đặc tả và thiết kế hệ thống

3.1 Giả thuyết hệ thống

Hiện tại đã có nhiều tiêu chuẩn để có thể phân tích nghiệp vụ cho các hệ thống blockchain áp dụng cho chuỗi cung ứng [25]. Nếu các đánh giá cho kết quả tích cực thì làm thế nào để ta nên triển khai nó như thế nào?

Các doanh nghiệp cần có một nền tảng kỹ thuật để có thể tạo hệ thống blockchain cho chuỗi cung ứng và có thể tích hợp nó vào chuỗi cung ứng của họ.

Việc cài đặt một mô hình chuỗi cung ứng đủ phức tạp có thể là bằng chứng về khái niệm (proof of concepts) và là một nguồn tham khảo hữu ích cho các nhà phát triển tạo ra các hệ thống tương tự cho tổ chức của họ.

3.2 Tiến trình

Phần lớn các yêu cầu kỹ thuật trong báo cáo này được tôi lấy từ các tài liệu tham khảo. Từ đó, tôi khảo sát những yêu cầu của người dùng đối với một hệ thống truy xuất nguồn gốc và biến nó thành các tính năng trong hệ thống của chính mình.

3.3 Đặc tả

3.3.1 Hệ thống truy xuất nguồn gốc

Từ Mục 2.1.5, một hệ thống truy xuất nguồn gốc cần ba yếu tố chính:

1. Mã định danh duy nhất cho từng đơn vị sản phẩm
2. Bản ghi dữ liệu về các thay đổi của sản phẩm
3. Sự trao đổi thông tin giữa các tác nhân của chuỗi cung ứng

Mã định danh duy nhất cho từng đơn vị sản phẩm

Ta sẽ giả định rằng mỗi sản phẩm đều có một mã định danh duy nhất và được gắn trên bao bì của sản phẩm dưới dạng mã vạch.

Bản ghi dữ liệu về các thay đổi của sản phẩm

Yêu cầu.1 Ghi lại thông tin mỗi khi một sản phẩm được bán hoặc là biến đổi thành sản phẩm khác.

Các thông tin phải truy vấn được để có thể sử dụng thông tin này cho hệ thống truy xuất nguồn gốc.

Yêu cầu.2 Bản ghi các thông tin truy xuất nguồn gốc phải có thể truy vấn được và cho phép người dùng tìm kiếm toàn bộ lịch sử của một sản phẩm.

Bởi vì hệ thống được cài đặt trên toàn chuỗi cung ứng nên nó cũng phải có các logic nghiệp vụ ứng với các thay đổi của sản phẩm, do đó mà các thay đổi đó cần có thể lập trình được.

Yêu cầu.3 Hệ thống cần phải cung cấp các thay đổi của sản phẩm mà có thể lập trình được.

Sự trao đổi thông tin giữa các thành viên

Mỗi thành viên cần phải có khả năng đề xuất các giao dịch và truy vấn thông tin các giao dịch

Yêu cầu.4 Hệ thống phải có khả năng cấp và thu hồi thông tin đăng nhập mạng.

Ta cũng nên hạn chế quyền truy cập vào một số thông tin, chẳng hạn như các thành viên chỉ có thể sửa đổi những gì họ sở hữu.

Yêu cầu.5 Hệ thống phải hỗ trợ kiểm soát truy cập dựa trên danh tính của các thành viên để có thể hạn chế các hành động như truy cập và chỉnh sửa thông tin.

Các thành viên phải đồng thuận trên lịch sử giao dịch của chuỗi cung ứng, nếu không thì các thông tin truy xuất nguồn gốc sẽ không có được tính chính xác.

Yêu cầu.6 Hệ thống phải được cài đặt các cơ chế đồng thuận để có thể chắc chắn rằng là các thành viên đồng thuận với trạng thái hiện có của sổ cái.

3.3.2 Doanh nghiệp

Nền tảng công nghệ

Thông thường, nhiều tổ chức sẽ tham gia vào một hệ thống chuỗi cung ứng. [11] Nhiều tổ chức khác nhau lại tồn tại các nền tảng công nghệ khác nhau.

Yêu cầu.7 Hệ thống nên có khả năng hoạt động trên nhiều nền tảng phần cứng khác nhau như Google Cloud Platform (GCP) hoặc Amazon Web Service (AWS).

Các tổ chức không thể chuyển sang một chuỗi cung ứng mới ngay lập tức.

Yêu cầu.8 Hệ thống phải được tích hợp dần dần, tức là hệ thống phải được thiết kế để có thể tích hợp được với chuỗi cung ứng hiện có.

Việc cài đặt các logic nghiệp vụ trong chuỗi cung ứng sẽ rất khác nhau giữa các trường hợp sử dụng và các ngành.

Yêu cầu.9 Các nhà phát triển có thể dễ dàng hiểu được cách cài đặt hệ thống trong báo cáo này khi mà tạo ra hệ thống phù hợp với trường hợp sử dụng của riêng họ.

Các yêu cầu trong hoạt động hàng ngày

Một trong ba động lực chính để tạo ra một hệ thống chuỗi cung ứng mới là tăng cường hiệu quả trong chuỗi cung ứng.

Yêu cầu.10 Hệ thống phải có chi phí hoạt động thấp và có thông lượng giao dịch cao.

Các lịch sử giao dịch tồn tại lâu ngày nên được lưu trữ.

Yêu cầu.11 Hệ thống phải có khả năng cập nhật phần mềm và các logic nghiệp vụ trong khi mà mạng blockchain vẫn đang hoạt động mà không gây ra bất cứ thiệt hại gì về thông tin truy xuất nguồn gốc của sản phẩm.

Yêu cầu.12 Hệ thống phải có khả năng thêm thành viên vào trong mạng blockchain trong khi vẫn đang hoạt động.

3.4 Nền tảng blockchain

3.4.1 Các nền tảng hiện tại

Một trong những giai đoạn quan trọng nhất của dự án này là chọn được nền tảng phần mềm hợp lý để xây dựng mạng blockchain. Hiện tại có rất nhiều nền tảng blockchain như Hyperledger, Multichain, Corda hay kể cả là các nền tảng được xây dựng từ đầu. Sử dụng một nền tảng blockchain đã có sẵn là tốt hơn để xây dựng một mạng blockchain cho dự án này. Mục tiêu của dự án này là cung cấp một nguồn tham khảo để cài đặt hệ thống blockchain cho các doanh nghiệp, do đó việc chọn một nền tảng blockchain có sẵn và được biết đến rộng rãi là rất quan trọng để đáp ứng được *Yêu cầu.8*.

3.5 Mạng công khai hay mạng riêng tư

Yêu cầu.10: "Hệ thống phải có chi phí hoạt động thấp và có thông lượng giao dịch cao."

Hiện tại có một số nền tảng blockchain công khai được thiết kế cho thông lượng giao dịch cao [10], nhưng chỉ có mạng blockchain riêng tư mới có thể đáp ứng được chi phí hoạt động thấp và thông lượng cao do có thuật toán đồng thuận đơn giản hơn.

Với cơ chế đồng thuận đơn giản hơn đồng nghĩa với việc các thành phần xấu có thể dễ dàng làm gián đoạn lịch sử giao dịch của hệ thống. Tuy nhiên, đây không phải là vấn đề với mạng riêng tư vì chỉ có những thành viên được cho phép mới có thể được tham gia vào mạng.

3.5.1 Tính năng

Việc chọn nền tảng phù hợp cũng phải dựa vào các tính năng mà nền tảng đó cung cấp. Bảng tóm tắt các yêu cầu dưới đây được tôi chọn là những đặc điểm quan trọng nhất trong việc lựa chọn nền tảng blockchain. Tất nhiên là ta có thể thêm những tính năng mà một nền tảng không có trong trường hợp mà nó có những tính năng ưu việt khác. Dưới đây là các đánh giá về các tính năng của ba mạng blockchain riêng tư nổi tiếng nhất là Hyperledger, Multichain và Corda [13]

Yêu cầu	Hyperledger [16]	Corda [15]	MultiChain [12]
<i>Yêu cầu.2</i> Khả năng truy vấn sổ cái	Có (Có thể thay đổi)	Có (SQL)	Có (Dựa vào Bitcoin)
<i>Yêu cầu.5</i> Quyền truy cập	Có	Có	Có
<i>Yêu cầu.3</i> Hợp đồng thông minh	Có (Chaincode)	Có (CorDapps)	Không
<i>Yêu cầu.6</i> Cơ chế đồng thuận	Có (Có thể thay đổi)	Có (Có thể thay đổi)	Có (Round Robin)

3.5.2 Lựa chọn

Ta thấy rằng cả Hyperledger và Corda đều thỏa mãn tất cả các yêu cầu, nhưng khi nhìn vào mục đích của mỗi nền tảng ta sẽ biết được nên chọn nền tảng nào:

- **Hyperleger:** "Hyperledger khuyến khích việc tái sử dụng các khối xây dựng thông thường thông qua kiến trúc mô-đun"[16]
- **Corda:** Một sổ cái dùng chung cho các trường hợp sử dụng trong dịch vụ tài chính"[6]

Corda đã được điều chỉnh cho các trường hợp sử dụng không phải là các dịch vụ tài chính, nhưng vì Hyperledger được thiết kế theo kiến trúc mô-đun ngay từ đầu nên nó mang lại sự linh hoạt cho trường hợp sử dụng của chuỗi cung ứng.

3.6 Hyperledger

Trong mục này ta sẽ khám phá kiến trúc của Hyperledger

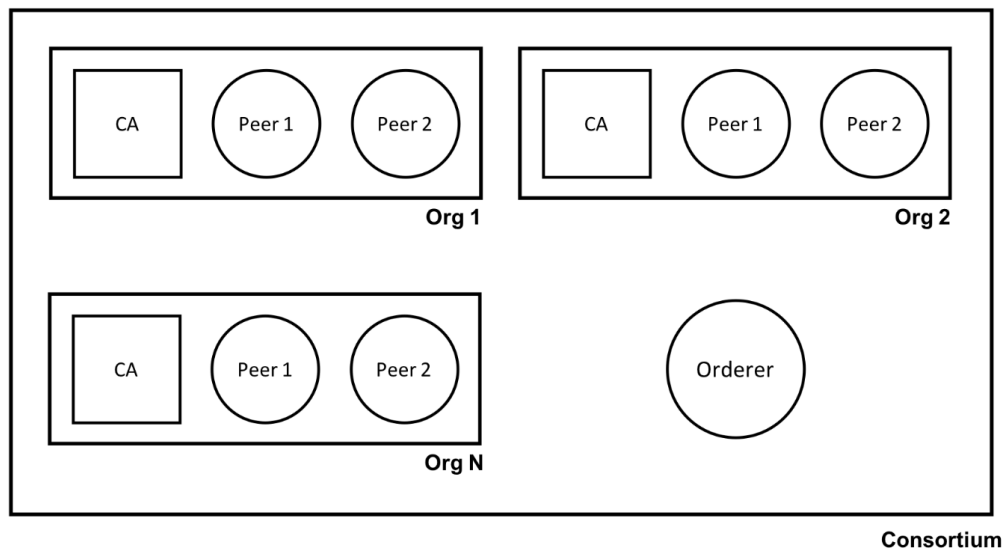
3.6.1 Định danh

Yêu cầu.4: "Hệ thống phải có khả năng cấp và thu hồi thông tin đăng nhập mạng."

Hyperledger cung cấp Fabric Certificate Authority (CA) để có thể thỏa mãn được yêu cầu này. Đây là một thành phần của kiến trúc mạng Hyperledger Fabric có khả năng: [17]

- Đăng ký định danh, hoặc kết nối tới một hệ thống xác thực có sẵn
- Cấp định danh
- Gia hạn hoặc thu hồi chứng chỉ

Trong Hình 3.1 , ta có thể thấy rằng mỗi tổ chức đều có một CA.



Hình 3.1: Kiến trúc mạng Blockchain Fabric

3.6.2 Cơ chế đồng thuận

Yêu cầu.6: "Hệ thống phải được cài đặt các cơ chế đồng thuận để có thể chắc chắn rằng là các thành viên đồng thuận với trạng thái hiện có của sổ cái."

Hyperledger Fabric hỗ trợ nhiều cơ chế đồng thuận trong mỗi giai đoạn của quá trình đồng thuận: [16]

- Các chứng thực được thực hiện bởi chính sách (ví dụ m trong số n chữ ký) mà những thành viên xác nhận giao dịch
- Ordering Service chấp nhận các giao dịch đã được xác nhận và đồng ý cho các giao dịch đó được cập nhật vào sổ cái
- Cơ chế xác thực thực hiện xác thực lại các khối giao dịch đã được xác nhận để kiểm tra tính đúng đắn của các giao dịch, bao gồm cả việc kiểm tra các chính sách xác thực

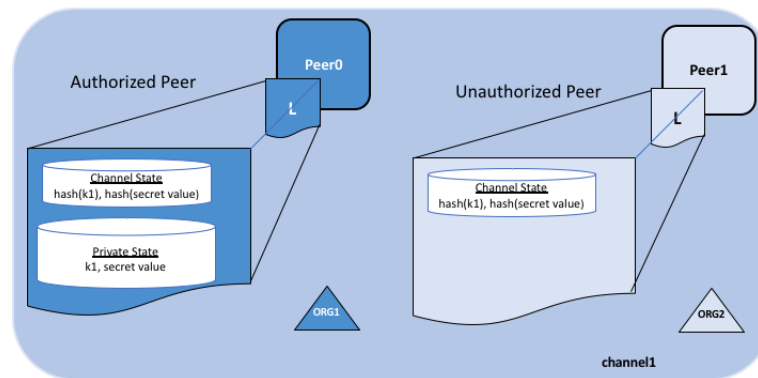
3.6.3 Quyền truy cập và tính riêng tư

Yêu cầu.5: "Hệ thống phải hỗ trợ kiểm soát truy cập dựa trên danh tính của các thành

viên để có thể hạn chế các hành động như truy cập và chỉnh sửa thông tin.”

Fabric hỗ trợ đóng gói các dữ liệu riêng tư giữa các thành viên thông qua hai cách:

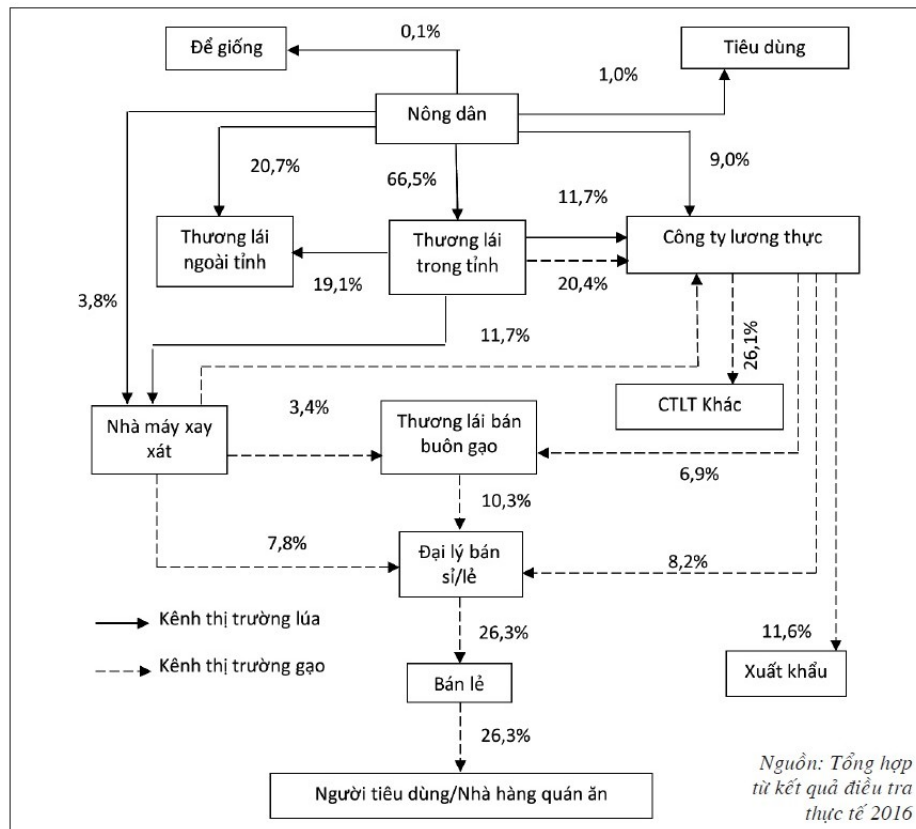
- **Các kênh riêng:** Tạo ra các kênh riêng tư gồm các tổ chức có quyền truy cập vào dữ liệu trên kênh đó
- **Collections:** Bao gồm dữ liệu riêng tư và mã băm của dữ liệu đó tồn tại như một bằng chứng của các giao dịch. Chỉ có các thành viên được phép mới được truy cập vào dữ liệu riêng tư đó như trong Hình 3.2



Hình 3.2: Collections giữa các thành viên được cấp quyền và không được cấp quyền

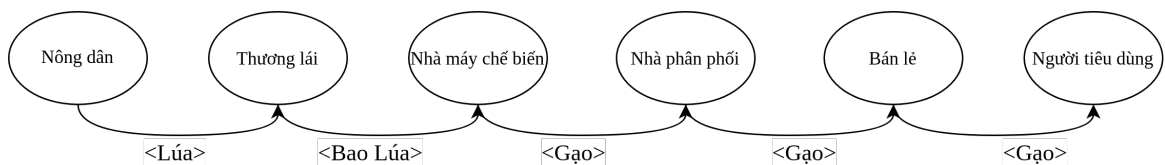
3.7 Mô hình mạng chuỗi cung ứng

Mô hình chuỗi cung ứng ở trong báo cáo này được lựa chọn thông qua một số chuỗi cung ứng hiện có trong thực tế như chuỗi cung ứng gạo tại tỉnh Kiên Giang, Việt Nam. Sơ đồ chuỗi cung ứng chi tiết trong Hình 3.3



Hình 3.3: Chuỗi cung ứng gạo tại tỉnh Kiên Giang, Việt Nam

Ta thấy rằng tại tỉnh Kiên Giang có rất nhiều kênh phân phối lúa gạo, ta sẽ chỉ thiết kế một kênh phân phối lúa gạo trong báo cáo này. Mô hình chuỗi cung ứng lúa gạo sẽ được đơn giản hóa như trong Hình 3.4



Hình 3.4: Mô hình chuỗi ứng lúa gạo trong báo cáo này

3.8 Phương pháp xây dựng

Sản phẩm khả dụng tối thiểu (Minium Viable Product) sẽ được tạo ra đầu tiên như một phiên bản rút gọn của hệ thống. Cách xây dựng này sẽ giúp ta có thể kiểm tra được các giả thiết đặt ra và tiếp tục phát triển sản phẩm đến hoàn thiện nếu khả thi.

Bởi vì Hyperledger Fabric chỉ hỗ trợ cơ sở dữ liệu đối tượng nên ta sẽ dùng sơ đồ thực thể liên kết để miêu tả dữ liệu của hệ thống.

3.9 Sản phẩm khả dụng tối thiểu

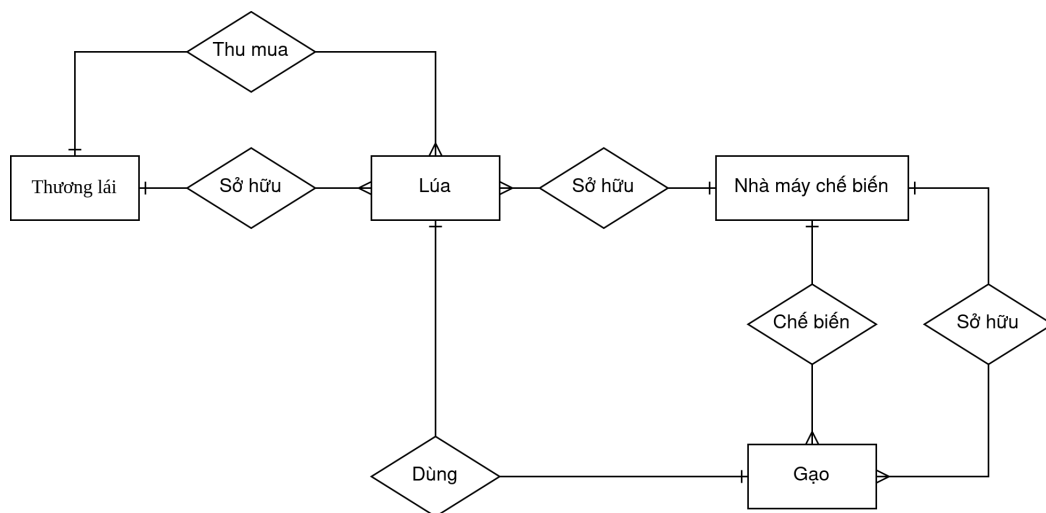
Ta sẽ chọn hai thành viên trong mạng chuỗi cung ứng là *Thương lái* và *Nhà máy chế biến* để thể hiện các giao dịch cũng như sự thay đổi của dữ liệu từ *Lúa* sang *Gạo*.

Sản phẩm khả dụng tối thiểu cần được cài đặt mô hình dữ liệu của hai thành viên này bao gồm cả dữ liệu giao dịch giữa hai bên.

Thành viên *Thương lái* cần phải lưu các thông tin như thông tin chi tiết của nông dân, ngày thu mua, đặc điểm của sản phẩm thu mua.

Thành viên *Nhà máy chế biến* cần phải lưu trữ các thông tin như thông tin chi tiết của thương lái, ngày nhận sản phẩm, đặc điểm của sản phẩm.

Sơ đồ thực thể liên kết được thể hiện chi tiết trong Hình 3.5



Hình 3.5: Sơ đồ thực thể liên kết cho sản phẩm khả dụng tối thiểu

3.10 Hoàn thành phần còn lại của hệ thống

3.10.1 Mô hình mạng

Từ Hình 3.4, hệ thống tối thiểu cần thêm những yêu cầu sau

- Thêm các thành viên còn lại
- Tạo các giao dịch giữa chúng

3.10.2 Mô hình dữ liệu

Thêm vào mô hình thực thể liên kết các thực thể của mạng cũng như dữ liệu đi theo chúng. Lưu ý rằng, có nhiều dữ liệu được chia sẻ giữa các thực thể để có thể thực hiện được chức năng truy xuất nguồn gốc.

4 Cài đặt hệ thống

4.1 Ánh xạ thiết kế tới các bộ phận

Các thành phần của bản thiết kế hệ thống cần phải được ánh xạ vào các bộ phận phần mềm.

- Mô hình mạng sẽ được ánh xạ tới các nút được thể hiện bằng các Docker container.
- Sơ đồ thực thể liên kết được ánh xạ vào cơ sở dữ liệu CouchDB của hệ thống.

4.2 Ánh xạ mô hình mạng vào mô hình mạng Fabric

4.2.1 Docker

Yêu cầu.7: "Hệ thống nên có khả năng hoạt động trên nhiều nền tảng phần cứng khác nhau như Google Cloud Platform (GCP) hoặc Amazon Web Service (AWS)."

Fabric cung cấp các Docker container image cho mỗi loại nút trong mạng. Xem Hình 4.2

IMAGE	PORTS	NAMES
hyperledger/fabric-peer	0.0.0.0:8051->7051/tcp, 0.0.0.0:8053->7053/tcp	peer1.grower.biswas.com
hyperledger/fabric-peer	0.0.0.0:7051->7051/tcp, 0.0.0.0:7053->7053/tcp	peer0.grower.biswas.com
hyperledger/fabric-couchdb	4369/tcp, 5984/tcp, 9100/tcp	peer1-db.grower.biswas.com
hyperledger/fabric-couchdb	4369/tcp, 5984/tcp, 9100/tcp	peer0-db.grower.biswas.com
hyperledger/fabric-ca	0.0.0.0:7054->7054/tcp	ca.grower.biswas.com

Hình 4.1: Docker container cho một tổ chức duy nhất

4.2.2 Mô hình hóa

Mỗi thành viên trong mạng lưới chuỗi cung ứng (xem Hình 3.4) được mô hình hóa thành các tổ chức riêng biệt và có các cơ sở dữ liệu riêng. Mỗi tổ chức đều có một Certificate Authority riêng.

Các Docker container có thể được triển khai chạy trên các dịch vụ đám mây bất kỳ. Khi các container chạy trên một máy thì nó sẽ được ánh xạ vào các cổng khác nhau trên máy đó, còn khi ở trên các dịch vụ đám mây chúng sẽ được thay bằng các địa chỉ URL hoặc IPv4.

Cấu hình của các Docker container được viết chi tiết trong các tệp *Docker Compose* tương tự như Hình 4.2

```
11  services:
12
13    ca_producer:
14      image: hyperledger/fabric-ca:$IMAGE_TAG
15      environment:
16        - FABRIC_CA_HOME=/etc/hyperledger/fabric-ca-server
17        - FABRIC_CA_SERVER_CA_NAME=ca-producer
18        - FABRIC_CA_SERVER_TLS_ENABLED=true
19        - FABRIC_CA_SERVER_PORT=7054
20      ports:
21        - "7054:7054"
22      command: sh -c 'fabric-ca-server start -b admin:adminpw -d'
23      volumes:
24        - ../organizations/fabric-ca/producer:/etc/hyperledger/fabric-ca-server
25      container_name: ca_producer
26      networks:
27        - test
```

Hình 4.2: Tệp Docker Compose cho một tổ chức duy nhất

4.2.3 Thêm thành viên cho mạng chuỗi cung ứng

Yêu cầu.12: "Hệ thống phải có khả năng thêm thành viên vào trong mạng blockchain trong khi vẫn đang hoạt động."

Ta có thể thêm nhiều tổ chức khác nhau cho mỗi loại thành viên (ví dụ như thêm nhiều Nông dân) tham gia vào mạng lưới chuỗi cung ứng bằng cách cài đặt các Docker container cần thiết vào hệ thống của tổ chức đó. Sau đó quản trị mạng lưới sẽ thêm tổ chức mới vào kênh phân phối để có thể thực hiện các giao dịch với thành viên trong kênh.

4.3 Ảnh xạ sơ đồ thực thể liên kết vào CouchDB

Các thành viên trong mô hình mạng lưới chuỗi ứng đã được mô hình hóa thành các thành viên của một kênh trong Fabric với đầy đủ chức năng. Bây giờ các thành viên cần được mô hình hóa thành các thực thể trong cơ sở dữ liệu gắn với các tài sản đi cùng như trong Hình 3.5

4.3.1 Tài sản

Hình 3.5 là một phần nhỏ của hệ thống. Hệ thống hoàn chỉnh cần các tài sản sau:

- Lúa
- Bó lúa
- Gạo
- Bao gạo

4.3.2 Các mô hình giao dịch

Các giao dịch trong mạng lưới cũng cần được mô hình hóa để có thể xác định được dữ liệu nào cần được yêu cầu trong các giao dịch. Hình 4.3 thể hiện các mô hình giao dịch trong mạng gồm:

- Chuyển đổi các lô (ví dụ như sản xuất các bao gạo từ các bó lúa)
- Chuyển đổi quyền sở hữu

```

1 abstract participant Actor identified by name {
2   o String name
3   o String email
4 }
5 abstract asset Batch identified by batchId {
6   o String batchId
7   o Integer quantity
8   --> Actor owner
9 }

```

Hình 4.3: Mô hình các giao dịch trong mạng

4.4 Logic nghiệp vụ trong các hàm giao dịch

Các logic nghiệp vụ được cài đặt vào mạng Fabric thông qua các hợp đồng thông minh và sau đó được đóng gói thành các chaincode.

Các chaincode có thể được cài đặt thông qua các ngôn ngữ như GoLang, Node.js hoặc JavaScript.

Hình 4.4 thể hiện một hàm giao dịch chuyển đổi các lô.

Hàm *transformBatch* lấy đầu một đầu vào là các dữ liệu giao dịch được nêu chi tiết trong Hình 4.3.

```

101 function transformBatch(tx) {
102     // check batch is owned by submitter
103     var oldBatch = tx.batch;
104     var factory = getFactory();
105
106     var submitter = getCurrentParticipant();
107     if (oldBatch.owner.$identifier !== submitter.$identifier) {
108         throw new Error('You do not own that batch');
109     }
110
111     var oldBatchNamespace = tx.batch.$namespace;
112     var oldBatchName = tx.batch.$type;
113     var oldFQBatchName = oldBatchNamespace + '.' + oldBatchName;
114
115     var newBatchDetails = transformations[oldBatchName];
116     var newFQBatchName = newBatchDetails.namespace + '.' + newBatchDetails.name;
117     var newBatch;
118
119     return getAssetRegistry(newFQBatchName)
120         .then(function(newBatchRegistry) {
121             // create a new batch for the new owner
122             var id = newBatchDetails.name + '_' + Date.now();
123             newBatch = factory.newResource(newBatchDetails.namespace, newBatchDetails.name, id);
124
125             newBatch.quantity = parseInt(oldBatch.quantity * newBatchDetails.scaleFactor);
126             newBatch.owner = factory.newRelationship(submitter.$namespace, submitter.$type, submitter.$identifier);
127             assignBatchProperties(oldBatch, newBatch, factory);
128
129             return newBatchRegistry.add(newBatch);
130         })
131         .then(function() {
132             return getAssetRegistry(oldFQBatchName);
133         })
134         .then(function(oldBatchRegistry) {
135             // Consume the original batch
136             oldBatch.quantity = 0;
137             return oldBatchRegistry.update(oldBatch);
138         })
139         .then(function() {
140             // emit an event
141             var event = factory.newEvent('biswas.base', 'BatchTransformed');
142             event.batchTypeConsumed = oldBatchName;
143             event.oldBatch = factory.newRelationship(oldBatchNamespace, oldBatchName, oldBatch.$identifier);
144             event.batchTypeCreated = newBatchDetails.name;
145             event.newBatch = factory.newRelationship(
146                 newBatchDetails.namespace,
147                 newBatchDetails.name,
148                 newBatch.$identifier
149             );
150             emit(event);
151         });
152 }

```

Hình 4.4: Mô hình các giao dịch trong mạng

4.5 Cơ chế đồng thuận

4.5.1 Chứng thực

Trong giai đoạn đầu tiên của cơ chế đồng thuận, các chính xác chứng thực sẽ yêu cầu chữ ký số của các thành viên cần phải có để có thể gửi yêu cầu giao dịch. Xem Hình 4.5 là chính xác chứng thực giữa nhà phân phối và nhà bán lẻ. Chính sách này nói rằng giao dịch phải có chữ ký số của một thành viên ở mỗi tổ chức để có thể được coi là tồn tại.

```
1 {
2     "identities": [
3         {
4             "role": {
5                 "name": "member",
6                 "mspId": "DistributorMSP"
7             }
8         },
9         {
10            "role": {
11                "name": "member",
12                "mspId": "RetailerMSP"
13            }
14        }
15    ],
16    "policy": {
17        "2-of": [
18            {
19                "signed-by": 0
20            },
21            {
22                "signed-by": 1
23            }
24        ]
25    }
26 }
```

Hình 4.5: Chính sách xác thực giữa nhà phân phối và nhà bán lẻ

4.5.2 Ordering

Trong giai đoạn thứ hai, Ordering Service sẽ kiểm tra các giao dịch được xác thực. Có hai loại Ordering Service:

- Solo - Duy nhất một nút ordering
- Kafka - Nhiều nút ordering thông qua nền tảng Apache Kafka để giao tiếp với nhau

4.5.3 Thẩm định

Sau khi các giao dịch đã được xác thực và thẩm định, giao dịch sẽ được tự động kiểm tra ở các nút thành viên bằng cách kiểm tra trạng thái của sổ cái. Điều này đảm bảo rằng các mục có liên quan trong sổ cái không được cập nhật kể từ khi gửi đi xác thực để tránh vấn đề double spending.

4.6 Giao diện người dùng

Các giao tiếp với mạng lưới Fabric sẽ được triển khai thành các REST API giao tiếp với ứng dụng web.

5 Thảo luận

5.1 Đánh giá phần mềm

Trong mục 3.1, sau khi xem xét một số nghiên cứu đã có, mục tiêu của dự án này là:

Các doanh nghiệp cần có một nền tảng kỹ thuật để có thể tạo hệ thống blockchain cho chuỗi cung ứng và có thể tích hợp nó vào chuỗi cung ứng của họ.

Việc cài đặt một mô hình chuỗi cung ứng đủ phức tạp có thể là bằng chứng về khái niệm (proof of concepts) và là một nguồn tham khảo hữu ích cho các nhà phát triển tạo ra các hệ thống tương tự cho tổ chức của họ.

Yêu cầu.9: Các nhà phát triển có thể dễ dàng hiểu được cách cài đặt hệ thống trong báo cáo này khi mà tạo ra hệ thống phù hợp với trường hợp sử dụng của riêng họ.”

Tôi tin rằng một hệ thống càng phức tạp thì càng gần với thực tế và có thể bao quát được các chuỗi cung ứng một cách dễ dàng. Trong báo cáo này, tôi đã trình bày chi tiết cách thiết kế một hệ thống truy xuất nguồn gốc cho đến cài đặt hệ thống đó.

Mạng lưới chuỗi cung ứng trong báo cáo này cũng đủ phức tạp khi được làm đơn giản hóa đi từ một chuỗi cung ứng trong thực tế. Ngoài ra, so với mạng của Chen [8] thì trong báo cáo này đã đi sâu vào quá trình phát triển hệ thống hơn như ánh xạ mô hình thực tế sang mô hình mạng Fabric, và ánh xạ sơ đồ thực thể liên kết vào cơ sở dữ liệu CouchDB.

5.2 Truy xuất nguồn gốc

Sau khi đã nghiên cứu các báo cáo khoa học trước đó, tôi đã tìm hiểu được các yếu tố chính để tạo lên một hệ thống truy xuất nguồn gốc hiệu quả. Trong báo cáo này, tôi đã sử dụng những yếu tố đó để xây dựng nên hệ thống truy xuất nguồn gốc lúa gạo.

Các yêu cầu chính của truy xuất nguồn gốc là *Yêu cầu.1:* ”Ghi lại thông tin mỗi khi một sản phẩm được bán hoặc là biến đổi thành sản phẩm khác.” và *Yêu cầu.2:* ”Bản

ghi các thông tin truy xuất nguồn gốc phải có thể truy vấn được và cho phép người dùng tìm kiếm toàn bộ lịch sử của một sản phẩm.”.

Hệ thống sẽ lưu trữ dữ liệu mỗi lần một giao dịch được gửi đi. Bên trong các hàm giao dịch, các sự kiện đi theo nó chứa nhiều thông tin hơn về giao dịch đó. Điều này làm thỏa mãn *Yêu cầu.1*, và kết hợp các dữ liệu được lưu trữ này với các chức năng truy vấn sẽ thỏa mãn *Yêu cầu.2*.

Cuối cùng, một hệ thống truy xuất nguồn gốc phải hỗ trợ trao đổi thông tin giữa các thành viên trong chuỗi cung ứng hay là thỏa mãn *Yêu cầu.8*. Điều này được thỏa mãn bởi chính sổ cái của mạng blockchain và thêm nữa là các API giao tiếp.

5.3 Đánh giá dự án

5.3.1 Các tài liệu tham khảo

Dự án này bắt đầu với mong muốn là tạo được ra một hệ thống truy xuất nguồn gốc chung cho mọi loại sản phẩm giống như mô hình của Chen [8], nhưng sau khi nghiên cứu các tài liệu tương tự tôi nhận thấy rằng vấn đề này đã được giải quyết tốt. Do đó mục tiêu của dự án là áp dụng vào các chuỗi cung ứng cụ thể hơn, phức tạp hơn.

Khó khăn trong việc nghiên cứu các tài liệu tham khảo là tìm đúng tài liệu hữu ích. Bởi vì một số bài nghiên cứu về nguồn gốc sản phẩm là không cần thiết, vì các kỹ thuật tìm nguồn gốc dữ liệu và các vấn đề với truy xuất nguồn gốc dữ liệu rất khác so với chuỗi cung ứng thực tế.

Mặt khác, đọc một số nghiên cứu về truy xuất nguồn gốc đôi khi sẽ hữu ích hơn thay vì xem xét toàn bộ hệ thống chuỗi cung ứng blockchain. Các kiến thức về truy xuất nguồn gốc nói chung cho phép tổng hợp các thuộc tính của một hệ thống xác định nguồn gốc hiệu quả, và từ đó dẫn tới một hệ thống truy xuất nguồn gốc có thể khái quát một cách hiệu quả cho các loại sản phẩm khác nhau.

5.3.2 Nắm bắt các yêu cầu

Trong giai đoạn xác định các yêu cầu của hệ thống, việc đọc nhiều tài liệu truy xuất nguồn gốc hơn cho phép nắm bắt nhiều yêu cầu tập trung vào doanh nghiệp hơn, dẫn đến việc xem xét hệ thống từ góc độ người dùng thay vì chỉ tập trung vào công nghệ.

Tuy nhiên, nó sẽ làm tăng sự tin tưởng vào các yêu cầu này nếu được dẫn từ một số chuyên gia trong lĩnh vực truy xuất nguồn gốc.

5.3.3 Thiết kế

Lựa chọn công nghệ

Lựa chọn nền tảng công nghệ là một phần quan trọng của giai đoạn thiết kế, với quyết định cuối cùng là Hyperledger.

Lựa chọn mô hình mạng

Một lựa chọn quan trọng khác khi thiết kế hệ thống là lựa chọn mô hình mạng chuỗi cung ứng để có thể cài đặt vào hệ thống. Ta đã chọn sử dụng mô hình các kênh phân phối lúa gạo tại tỉnh Kiên Giang, Việt Nam với độ phức tạp vừa đủ để có thể khái quát các chuỗi cung ứng khác.

5.3.4 Các nghiên cứu tiếp theo

Việc ta cài đặt nhiều mô hình mạng có thể sẽ cải thiện tính tổng quát của hệ thống đối với các sản phẩm khác trong chuỗi cung ứng chung.

Một tính năng khác có thể được thêm vào dự án là quy trình để triển khai hệ thống trên các nền tảng đám mây như Amazon Web Services (AWS) hoặc Microsoft Azure. Điều này cho phép các nhà phát triển chạy phần mềm khi bị hạn chế về vấn đề phần cứng và một lần nữa cung cấp hệ thống hoàn chỉnh hơn cho doanh nghiệp.

Cuối cùng, cùng một mạng lưới chuỗi cung ứng có thể được triển khai trên các nền tảng blockchain khác như MultiChain. Điều này cho phép hai nền tảng được so sánh trực tiếp và ta sẽ thu được về các nhận xét hữu ích cho mỗi nền tảng.

6 Phần Kết Luận

Trong phần đầu của báo cáo này, ta đã xác định được các yếu tố của một hệ thống truy xuất nguồn gốc, cùng với các mô hình mạng lưới chuỗi cung ứng phức tạp từ các nghiên cứu khoa học trước đó. Sau đó, ta đã đánh giá một loạt các nền tảng blockchain khác nhau để có thể chọn được nền tảng tốt nhất phù hợp với các yêu cầu đặt ra của một hệ thống truy xuất nguồn gốc chuỗi cung ứng.

Phần tiếp theo, ta đã xác định được mô hình mạng chuỗi cung ứng lúa gạo để có thể cài đặt trên nền tảng Hyperledger Fabric bằng cách sử dụng phương pháp phát triển phần mềm khả dụng tối thiểu. Thông qua đó, ta biết được rằng một hệ thống truy xuất nguồn gốc dựa trên blockchain có thể giúp cải thiện được khả năng truy xuất nguồn gốc trong chuỗi cung ứng.

Báo cáo này có thể là nguồn tham khảo hữu ích về việc cài đặt một hệ thống truy xuất nguồn gốc cho chuỗi cung ứng trên nền tảng Hyperledger, và cũng có thể làm cơ sở để triển khai một hệ thống truy xuất nguồn gốc như vậy trong một doanh nghiệp

Tài Liệu Tham Khảo

- [1] ISO 9000:2015(En). *Quality Management Systems — Fundamentals and Vocabulary [2015]*. URL: <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en:term:3.6.13..>
- [2] M. M. Aung und Y. Chang. “Traceability in a food supply chain: Safety and quality perspectives”. In: *Food Control* 39 (2014), S. 172–184.
- [3] Nolan Bauerle. *What Are the Applications and Use Cases of Blockchains?* URL: <https://www.coindesk.com/learn/blockchain-101/how-does-blockchain-technology-work>.
- [4] A. Bechini u. a. “Patterns and technologies for enabling supply chain traceability through collaborative e-business”. In: *Inf. Softw. Technol.* 50 (2008), S. 342–359.
- [5] K. Biswas, V. Muthukkumarasamy und W. Tan. “Grape Grower Wine Producer Filler / Packer Bulk Distributor Transit Cellar Supplier Freight Operator Importer Finished Goods Distributor”. In: 2018.
- [6] R. Brown u. a. “Corda : An Introduction”. In: 2016.
- [7] C. Cachin, S. Schubert und M. Vukolic. “Non-determinism in Byzantine Fault-Tolerant Replication”. In: *OPODIS*. 2016.
- [8] Enbo Chen. ““An Approach for Improving Transparency and Traceability of Industrial Supply Chain with Blockchain Technology””. In: (2016).
- [9] European Commission. *Commission Regulation (EC) No 1688/2005*.
- [10] Thaddeus Dryja und Joseph Poon. “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”. In: 2016.
- [11] Elise H. Golan u. a. “Traceability in the US food supply: Economic theory and industry studies”. In: *Agricultural economic report* 830(3) (2004), S. 1–48.

- [12] Gideon Greenspan. *MultiChain Private Blockchain — White Paper*. URL: <https://www.multichain.com/download/MultiChain-White-Paper.pdf>.
- [13] Gideon Greenspan. *Where Have All the Private Blockchains Gone?* URL: <https://www.coindesk.com/private-blockchains-gone>.
- [14] M. Hancock und E. Vaizey. *Distributed Ledger Technology: Beyond block chain*. 2016. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
- [15] Mike Hearn. “Corda: A distributed ledger”. In: *Corda Technical White Paper* (2016).
- [16] *Hyperledger Architecture, Volume 1*. 2017. URL: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf.
- [17] *Hyperledger Fabric Documentation - Certificate Authorities*. 2020. URL: <https://hyperledger-fabric-ca.readthedocs.io/en/latest/users-guide.html>.
- [18] Leslie Lamport, Robert Shostak und Marshall Pease. “The Byzantine Generals Problem”. In: *ACM Trans. Program. Lang. Syst.* 4.3 (1982), S. 382–401.
- [19] C. Lovis. “Traceability in healthcare: crossing boundaries.” In: *Yearbook of medical informatics* (2008), S. 105–13.
- [20] J. Mckean. “The importance of traceability for public health and consumer protection.” In: *Revue scientifique et technique* 20 2 (2001), S. 363–71.
- [21] T. Moe. “Perspectives on traceability in food manufacture”. In: *Trends in Food Science & Technology* 9 (5) (1998), S. 211–214.
- [22] William G. Murphy, Louis M. Katz und Peter Flanagan. “Regulatory Aspects of Blood Transfusion”. In: *Practical Transfusion Medicine*. John Wiley & Sons, Ltd, 2017. Kap. 18, S. 184–192.
- [23] Satoshi Nakamoto. “Bitcoin : A Peer-to-Peer Electronic Cash System”. In: 2009.
- [24] M. Orcutt. “Who Will Build the Health-Care Blockchain?” In: *MIT Technology Review* (2017).

- [25] Oskar Petersen und Fredrik Jansson. “Blockchain Technology in Supply Chain Traceability Systems”. In: (2017). URL: <http://lup.lub.lu.se/luur/download?func=downloadFile%5C&recordId=8918347%5C&fileId=8919918>..
- [26] A. Regattieri, M. Gamberi und R. Manzini. “Traceability of food products: General framework and experimental evidence”. In: *Journal of Food Engineering* 81 (2007), S. 347–356.
- [27] J. Robert. *The Diamond Industry Is Obsessed With the Blockchain*. 2017. URL: <http://fortune.com/2017/09/12/diamond-blockchain-everledger/>.
- [28] Jostein Storøy, Maitri Thakur und P. Olsen. “The TraceFood Framework – Principles and guidelines for implementing traceability in food value chains”. In: *Journal of Food Engineering* 115 (2013), S. 41–48.
- [29] W. C. Tan. “Research problems in data provenance”. In: *IEEE Data Eng. Bull.* 27(4) (2004), S. 45–52.