

Lời cam đoan

Em xin cam đoan các nội dung trong báo cáo đồ án với đề tài “Ứng dụng công nghệ Blockchain trong truy xuất nguồn gốc thực phẩm” là công trình nghiên cứu của bản thân dưới sự hướng dẫn của TS. Lê Chí Ngọc. Các số liệu, hình ảnh, trích dẫn có nguồn gốc rõ ràng và tuân thủ nguyên tắc. Báo cáo không có sự sao chép từ các công trình, nghiên cứu của người khác mà không ghi rõ trong tài liệu tham khảo. Em xin chịu trách nhiệm về lời cam đoan này.

Hà Nội, ngày 07 tháng 01 năm 2021

Sinh viên

Nguyễn Công Thịnh

Mục lục

Lời cam đoan	1
Lời nói đầu	7
Chương 1. Công nghệ Blockchain	10
1 Lịch sử hình thành	10
1.1 Sự ra đời của Blockchain	10
1.2 Ý tưởng ra đời của Blockchain	11
2 Giới thiệu công nghệ Blockchain	12
2.1 Sổ cái phân tán - Nền tảng của công nghệ Blockchain	12
2.2 Định nghĩa Blockchain	13
2.3 Hàm băm	15
2.4 Đơn vị cấu thành blockchain - khối (block)	16
2.5 Quy trình của Blockchain	17
2.6 Các cơ chế đồng thuận	20
2.7 Phân loại Blockchain	24
2.8 Hợp đồng thông minh (Smart Contract)	28
2.9 Đặc điểm của blockchain	30
3 Ứng dụng của Blockchain	30
3.1 Bitcoin - Ứng dụng đầu tiên của blockchain	30
3.2 Truy xuất nguồn gốc	31
3.3 Xây dựng chính phủ điện tử	32
4 Truy xuất nguồn gốc	33
4.1 Khái niệm truy xuất nguồn gốc	33
4.2 Đặc điểm của truy xuất nguồn gốc	34

4.3	Bản chất của việc xây dựng một hệ thống truy xuất nguồn gốc . . .	35
4.4	Các cấp độ truy xuất nguồn gốc	35
4.5	Quy trình xây dựng hệ thống	36
4.6	Hệ thống truy xuất nguồn gốc hiệu quả	37
4.7	Lợi ích và thách thức của hệ thống truy xuất nguồn gốc	38
Chương 2. Bài toán truy xuất nguồn gốc thực phẩm		39
1	Nền tảng Hyperledger Fabric	39
1.1	Giới thiệu về Hyperledger Fabric	39
1.2	Thuật toán đồng thuận trong Hyperledger Fabric	40
1.3	Mô hình Hyperledger Fabric	41
1.4	Luồng giao dịch	42
1.5	Hệ thống mạng Hyperledger Fabric	46
2	Thực nghiệm xây dựng hệ thống	47
2.1	Phân tích và thiết kế hệ thống	47
2.2	Xây dựng mạng Hyperledger Fabric	51
2.3	Xây dựng chức năng và giao diện hệ thống	53
3	Kiểm thử và đánh giá kết quả	60
3.1	Kiểm thử và đánh giá chức năng đăng nhập	60
3.2	Kiểm thử và đánh giá chức năng thêm thông tin sản phẩm	60
3.3	Kiểm thử và đánh giá chức năng sửa thông tin sản phẩm	62
Kết luận		64
Tài liệu tham khảo		67

Danh sách hình vẽ

1.1	Minh họa bài toán các vị tướng Byzantine.	11
2.1	Mô hình mạng công nghệ sổ cái phân tán	12
2.2	Lược đồ về quy trình giao dịch trong mạng blockchain	18
2.3	Minh họa quá trình giao dịch trên mạng.	18
2.4	Trường hợp giá trị hàm băm thay đổi làm đứt liên kết.	19
2.5	Mô hình cơ chế hoạt động của PoW	21
2.6	Minh họa mô hình mạng Blockchain công khai.	25
2.7	Minh họa mô hình mạng Blockchain riêng tư.	26
2.8	Minh họa mô hình mạng Blockchain kết hợp.	27
2.9	Minh họa mô hình mạng Blockchain lai.	28
4.1	Mô hình cơ bản của hệ thống truy xuất nguồn gốc sản phẩm và luồng thông tin	34
4.2	Minh họa hai cấp độ truy xuất nguồn gốc: truy xuất toàn cục và truy xuất nội bộ	35
1.1	Kiến trúc Hyperledger Fabric [9].	41
1.2	Yêu cầu giao dịch [9].	43
1.3	Phản hồi yêu cầu [9].	43
1.4	Giao dịch đặt hàng [9].	44
1.5	Chuyển giao dịch [9].	44
1.6	Chuyển giao dịch [9].	45
1.7	Chuyển giao dịch [9].	45
1.8	Hệ thống mạng Hyperledger Fabric.	46
2.1	Sơ đồ tổng quát của hệ thống blockchain	48
2.2	Kiến trúc hệ thống mạng blockchain	49

2.3	Biểu đồ use-case tổng quát.	51
2.4	Cấu trúc mạng Hyperledger Fabric.	52
2.5	Quá trình thiết lập mô hình mạng và kết quả chạy thực tế.	52
2.6	Giao diện trang chủ hệ thống truy xuất nguồn gốc thực phẩm.	53
2.7	Giao diện chức năng đăng nhập.	54
2.8	Giao diện thêm thông tin sản phẩm.	55
2.9	Giao diện sửa đổi thông tin sản phẩm.	58
2.10	Truy xuất thông tin bằng mã sản phẩm.	58
2.11	Truy xuất thông tin bằng tên sản phẩm.	59
3.1	Thao tác đăng nhập hệ thống.	60
3.2	Thao tác thêm sản phẩm vào mạng.	61
3.3	Kết quả thực tế khi ghi nhận thông tin sản phẩm truy vấn qua API.	62
3.4	Thao tác sửa thông tin sản phẩm trên mạng.	63

Danh sách bảng

2.1	So sánh công nghệ sổ cái phân tán và công nghệ blockchain	14
2.2	So sánh hợp đồng thông minh và hợp đồng truyền thống.	29
3.1	Thông tin cơ bản về Bitcoin (tính đến ngày 11/05/2020)	31
2.1	Các tác nhân tham gia vào hệ thống	47
2.2	Thiết kế cơ sở dữ liệu (Commodity) của sản phẩm.	50
2.3	Thiết kế cơ sở dữ liệu (HistoryItem) của sản phẩm.	50
2.4	Bảng mô tả chi tiết các use-case.	51
2.5	Các sự kiện của chức năng đăng nhập.	54
2.6	Các sự kiện của chức năng thêm thông tin sản phẩm.	56
2.7	Các sự kiện của chức năng sửa thông tin sản phẩm.	57
2.8	Các sự kiện của chức năng tra cứu thông tin.	59
3.1	Mẫu nhập liệu thông tin sản phẩm	61

Lời nói đầu

1. Cơ sở khoa học và thực tiễn của đề tài

Năm 2020 vừa qua chứng kiến những biến động lớn của thế giới do ảnh hưởng của đại dịch Covid-19. Dịch bệnh làm thay đổi xu hướng tiêu dùng thông minh, đồng thời như một cú hích đẩy mạnh việc chuyển đổi số và tạo ra xu hướng đầu tư vào các loại tiền điện tử. Phải nói rằng năm 2020 là một năm bùng nổ của thị trường tiền điện tử với sự phát triển mạnh của các đồng tiền điện tử, chẳng hạn như Bitcoin, liên tục lập kỷ lục về giá trị của đồng tiền này. Những khái niệm về tiền điện tử, truy xuất nguồn gốc thực phẩm trong tiêu dùng hay chính phủ điện tử nêu trên đều xoay quanh một khái niệm đang nhận được sự quan tâm rất lớn đến từ cộng đồng thế giới, đó chính là công nghệ Blockchain. Từ các chính phủ, ngân hàng cho đến doanh nghiệp đang thực sự coi đây là một công nghệ tiềm năng và hoàn toàn có khả năng lớn mạnh trong thời gian tới. Với những tính năng hữu ích mà nói mạng lại, công nghệ này sẽ mở ra một xu hướng ứng dụng tiềm năng cho nhiều lĩnh vực như tài chính ngân hàng, bán lẻ, vận chuyển hàng hóa, sản xuất, v.v.

Cùng với xu thế ứng dụng công nghệ blockchain, những mối lo về bệnh dịch, về thực phẩm bẩn, thực phẩm nhiễm hóa chất độc hại cũng được người dân hết sức quan tâm. Do đó, việc áp dụng công nghệ blockchain là việc làm cần thiết. Chính vì vậy, em đã chọn đề tài: ***“Ứng dụng công nghệ blockchain trong truy xuất nguồn gốc thực phẩm”*** để làm hướng nghiên cứu cho bản thân mình. Đồng thời áp dụng nền tảng Hyperledger Fabric - một trong những nền tảng blockchain phổ biến hiện nay làm cơ sở để phát triển hệ thống. Blockchain có tiềm năng làm thay đổi xu hướng tiêu dùng của người dân, nhưng có lẽ sự ảnh hưởng lớn nhất là tạo ra một mức độ minh bạch mới. Việc áp dụng blockchain rộng rãi sẽ tạo ra sự minh bạch đáng kể ở mọi cấp độ, tạo được niềm tin của người tiêu dùng.

Trên quy mô lớn, mỗi khi một sản phẩm thực phẩm được sản xuất ra, được vận chuyển, chế biến hay mua bán, giao dịch sẽ được ghi chép lại trên một sổ cái kỹ thuật số, nhằm để lại dấu vết. Như vậy, hàng chục triệu giao dịch liên quan đến thực phẩm hàng năm sẽ được hiển thị công khai và có thể kiểm soát nhờ cơ sở dữ liệu được tạo ra bởi công nghệ blockchain.

Mặc dù đã có những chuyển biến tích cực trong việc áp dụng hệ thống công nghệ thông tin để hỗ trợ công tác truy xuất, song các hệ thống phần mềm vẫn không tránh khỏi một số vấn đề. Ví dụ như hệ thống phần mềm chưa được tích hợp, liên kết chặt chẽ, chưa có một mô hình dữ liệu chuẩn, việc chia sẻ, trao đổi dữ liệu còn khó khăn làm cho việc tổng hợp dữ liệu phục vụ quản lý, điều hành mất nhiều thời gian chuyển đổi, thiếu chính xác. Việc thiết kế cơ sở dữ liệu còn chưa linh động, dẫn tới khi các tiêu chuẩn về thực phẩm thay đổi, nhiều chương trình còn gặp khó khăn trong việc cấu trúc lại cơ sở dữ liệu để phù hợp với tiêu chuẩn đó. Đặc biệt trong quá trình sản xuất và chế biến sản phẩm vẫn còn một số điểm hạn chế của hệ thống phần mềm cho tới nay còn chưa đáp ứng được tối đa nhu cầu của khách hàng. Có thể kể đến đó là yêu cầu của người tiêu dùng, muốn nắm bắt thông tin về nguồn nguyên liệu, quá trình sản xuất, phương pháp lưu trữ và bảo quản của sản phẩm một cách rõ ràng, công khai minh bạch. Do vậy, việc nghiên cứu và áp dụng công nghệ blockchain hỗ trợ hoạt động truy xuất nguồn gốc thực phẩm sẽ trở thành một ứng dụng thiết thực và đem lại hiệu quả cao, khi mà nó có thể cung cấp cho các đối tượng từ người tiêu dùng cho đến các đơn vị tham gia vào quá trình sản xuất sản phẩm, các cấp chức năng có thể khai thác được dữ liệu, đảm bảo dữ liệu được truy vấn không bị thay đổi, tiết kiệm chi phí vận hành các hệ thống cơ sở dữ liệu truyền thống, đồng thời kiểm soát tránh xảy ra trường hợp thực phẩm không đạt yêu cầu tuần ra thị trường.

2. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu: bao gồm khái niệm về blockchain và các khái niệm liên quan đồng thời cũng nghiên cứu về công tác truy xuất nguồn gốc thực phẩm và việc ứng dụng công nghệ blockchain trong vận hành hệ thống truy xuất nguồn gốc thực phẩm.

Phạm vi nghiên cứu:

- Nghiên cứu vấn đề truy xuất nguồn gốc trong phạm vi giải quyết của blockchain.
- Giới hạn trong nghiệp vụ truy xuất nguồn gốc thực phẩm.

3. Kết cấu của báo cáo

Nội dung báo cáo được chia làm 3 phần như sau:

Chương 1. Giới thiệu tổng quan về blockchain, hợp đồng thông minh và các ứng dụng của blockchain.

Chương 2. Khái niệm, đặc điểm, bản chất của truy xuất nguồn gốc. Quy trình xây dựng một hệ thống truy xuất nguồn gốc.

Chương 3. Trình bày về nền tảng Hyperledger Fabric. Áp dụng blockchain để xây dựng ứng dụng truy xuất nguồn gốc thực phẩm. Trình bày về quá trình thực nghiệm, kiểm thử và đánh giá, các kết quả thực hiện được.

Cuối cùng, em xin gửi lời cảm ơn đặc biệt và sâu sắc tới thầy TS. Lê Chí Ngọc, giảng viên thuộc Bộ môn Toán Tin, Viện Toán ứng dụng và Tin học, Trường Đại học Bách Khoa Hà Nội đã trực tiếp hướng dẫn và chỉ bảo em tận tình, đồng thời đưa ra những kinh nghiệm quý báu để em có thể hoàn thành được báo cáo này. Em cũng xin trân trọng cảm ơn các thầy cô giảng viên viện Toán ứng dụng và Tin học đã giảng dạy truyền đạt cho em những kiến thức trong suốt những năm tháng học tại trường. Những kiến thức không những giúp em nâng cao kỹ năng bản thân mà còn giúp ích cho em trong cả công việc sau này. Mặc dù đã cố gắng hết sức, tuy nhiên trong quá trình thực hiện em không tránh khỏi được những thiếu sót, em rất mong nhận được sự thông cảm và đánh giá chân tình của thầy cô để báo cáo của em được hoàn thiện hơn nữa!

Hà Nội, ngày 07 tháng 01 năm 2021

Sinh viên

Nguyễn Công Thịnh

Chương 1

Công nghệ Blockchain

Trong những năm trở lại đây, công nghệ ngày càng phát triển vượt bậc với sự ra đời của hàng loạt những công nghệ mới và những ứng dụng tuyệt vời mà chúng đem lại. Một trong số những công nghệ mới đó được ứng dụng một cách rộng rãi trong nhiều lĩnh vực cuộc sống như tiền điện tử, bảo hiểm, chuỗi cung ứng và logistics, v.v. mà chắc hẳn có nhiều người biết tới, đó chính là công nghệ blockchain. Vậy blockchain là gì?

1 Lịch sử hình thành

1.1 Sự ra đời của Blockchain

Blockchain ra đời từ sau cuộc khủng hoảng tài chính năm 2008, hệ thống tài chính Mỹ sụp đổ hoàn toàn khiến người dân đánh mất niềm tin vào đồng tiền của một bên thứ ba đáng tin cậy. Ý tưởng về Bitcoin – một đồng tiền phân cấp ngang hàng trên mạng máy tính lần đầu tiên được Satoshi Nakamoto đưa ra thông qua bài báo có tiêu đề “Bitcoin: A Peer-to-Peer Electronic Cash System” [15]. Thông qua bài báo, ông đã xác lập Bitcoin là một đồng tiền điện tử và phát minh ra cơ sở dữ liệu blockchain đầu tiên.

Năm 2014, công nghệ blockchain được tách khỏi tiền điện tử và có tiềm năng rất lớn với các giao dịch tài chính, liên tổ chức [10]. Kể từ đây, công nghệ blockchain chuyển sang giai đoạn phát triển thứ hai với nhiều ứng dụng ngoài tiền tệ xuất hiện. Hệ thống blockchain Ethereum đưa các chương trình máy tính vào các khối, đại diện cho các công

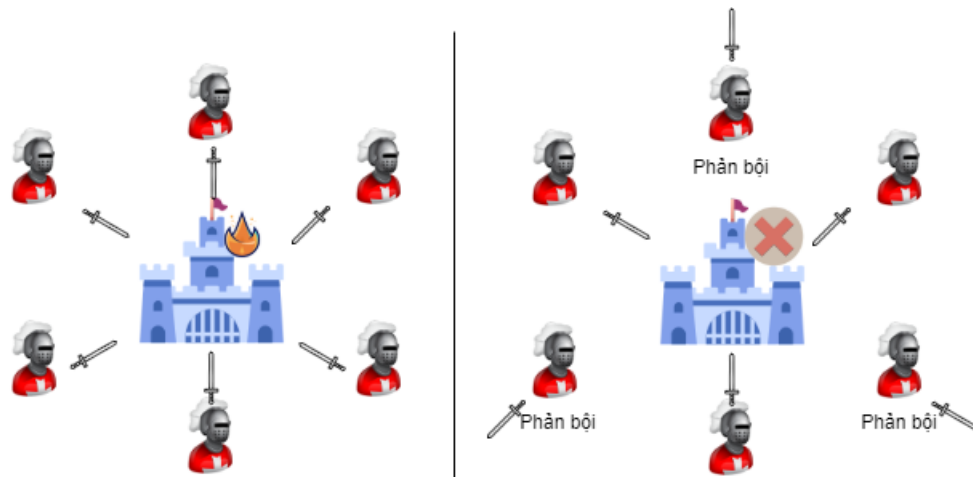
cụ tài chính như trái phiếu. Chúng được gọi là hợp đồng thông minh (smart contract).

“Blockchain là một sổ cái phân tán duy trì một danh sách dữ liệu liên tục phát triển các bản ghi được xác nhận bởi tất cả các nút tham gia ”.

1.2 Ý tưởng ra đời của Blockchain

Blockchain được tạo ra với ưu điểm là giải quyết được **bài toán các vị tướng Byzantine** (Byzantine Generals Problem) [12]. Byzantine Generals Problem là một bài toán kinh điển trong khoa học máy tính về đường truyền tin cậy, bộ xử lý lỗi trong một hệ phân tán.

Bài toán các vị tướng Byzantine: Một binh đoàn đánh chiếm một thành phố bằng cách chia thành nhiều đạo quân nhỏ vây hãm thành. Do đó phải liên lạc thông qua người đưa tin bằng ngựa làm trung gian. Để chiến thắng, tất cả các đạo quân phải cùng tiến công, nếu không sẽ không đủ sức mạnh và dẫn đến thất bại [12].



Hình 1.1: Minh họa bài toán các vị tướng Byzantine.

Có nhiều trường hợp xảy ra, chẳng hạn: người đưa tin bị địch tóm giữa đường, quân địch giả làm người đưa tin, hoặc trong số các tướng có nội gián, cố ý không xuất quân cùng lúc.

Câu hỏi đặt ra: “Làm thế nào để có thể tin tưởng lẫn nhau mà không phụ thuộc vào một bên thứ ba nào làm trung gian?”. Đây là ý tưởng mở đầu cho một hệ thống Blockchain có thể giúp các bên giao dịch tin tưởng nhau hơn.

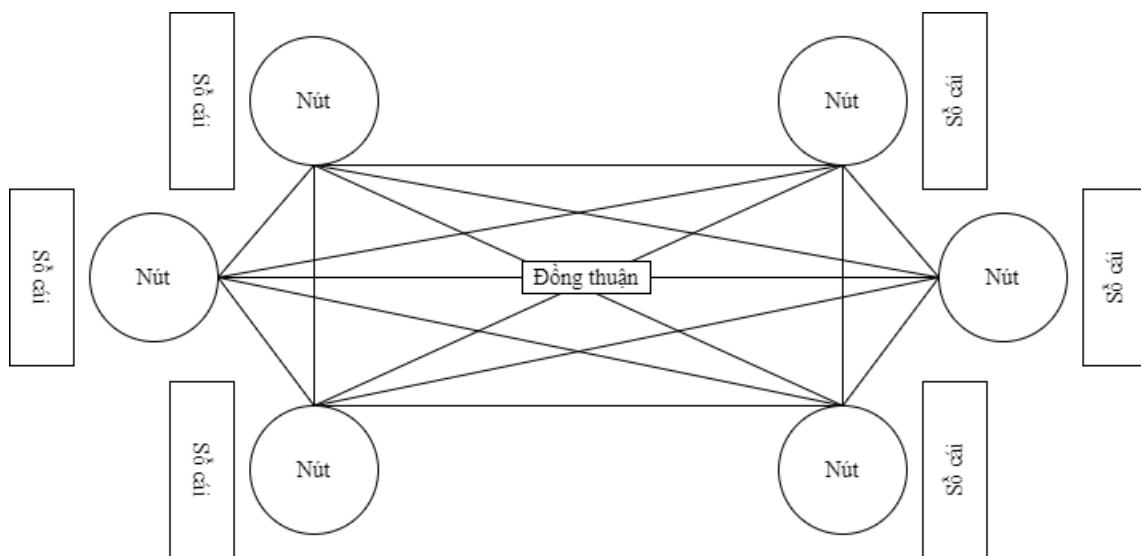
2 Giới thiệu công nghệ Blockchain

Blockchain là một công nghệ tiềm năng, những ứng dụng của nó hiện tại đã và đang đem lại hiệu quả rất lớn từ kỹ thuật đến cải thiện xã hội và kinh tế [20, 22]. Nội dung sau đây sẽ cung cấp những thông tin cốt lõi của công nghệ này.

2.1 Sổ cái phân tán - Nền tảng của công nghệ Blockchain

2.1.1 Khái niệm sổ cái phân tán

Định nghĩa 1.1. Công nghệ sổ cái phân tán (Distributed Ledger Technology - DLT) là thuật ngữ đề cập đến cơ sở hạ tầng công nghệ sử dụng máy tính độc lập - gọi là nút để ghi chép, chia sẻ và đồng bộ hóa các giao dịch trong sổ cái điện tử, thay vì lưu trữ dữ liệu tập trung như trong sổ cái truyền thống [17].



Hình 2.1: Mô hình mạng công nghệ sổ cái phân tán

DLT có tất cả các nút được kết nối với nhau, mỗi nút có một bản sao của sổ cái phân tán. Thuật ngữ “đồng thuận” ở trung tâm của mạng thể hiện cơ chế đồng thuận trong đó các nút đồng ý về các giao dịch mới và việc cập nhật sổ cái. DLT dùng thuật toán để mã hóa dữ liệu, đảm bảo chỉ người có quyền tham gia mới được sử dụng dữ liệu

DLT có khả năng hỗ trợ xử lý các hợp đồng thông minh (smart contracts) [5], các chương trình máy tính tự thực hiện dựa trên các điều khoản và điều kiện được qui định trước bởi các bên tham gia hợp đồng.

2.1.2 Ứng dụng của sổ cái phân tán

Tiền điện tử (Cryptocurrencies): là loại tiền không tồn tại dưới dạng tiền mặt, cho phép thực hiện giao dịch mà không cần các bên trung gian (ví dụ: ngân hàng,...), được phát hành bởi các cá nhân, công ty và tổ chức. Tiền mã hóa không được chính phủ công nhận.

Token hóa (Tokenization): là quá trình thể hiện quyền sở hữu tài sản vật chất trên sổ cái phân tán, DLT sẽ tạo một bản ghi kỹ thuật số duy nhất để xác minh quyền sở hữu và tính xác thực, bao gồm tất cả hoạt động trong quá khứ.

Bù trừ và thanh toán giao dịch chứng khoán (Post-trade clearing and settlement): cung cấp thông tin có độ trễ về thời gian rất nhỏ, do đó giảm độ phức tạp, giảm thời gian và chi phí liên quan đến xử lý giao dịch; đồng thời, loại bỏ gần như hoàn toàn sự trùng lặp thông tin ghi chép giữa các bên, giảm thiểu rủi ro, tăng tính thanh khoản của tài sản và tiền.

2.1.3 Những khó khăn khi triển khai công nghệ sổ cái phân tán tại Việt Nam

Chưa có một bộ khung pháp lý rõ ràng để triển khai công nghệ vào các hệ thống lớn tại Việt Nam. Việc tích hợp công nghệ này vào các hệ thống cũ gặp khó khăn do phần lớn các hệ thống hiện nay vẫn sử dụng mô hình quản lý dữ liệu tập trung.

Để duy trì hệ thống đòi hỏi một lượng lớn máy tính, do đó, chi phí điện, duy trì và bảo dưỡng hệ thống khá cao.

2.2 Định nghĩa Blockchain

Định nghĩa 1.2. Blockchain là một sổ cái phân tán bất biến, dữ liệu sau khi nhập vào sẽ được đóng gói thành các khối (block), được nối chuỗi với nhau bằng cách sử dụng các hàm băm và không thể bị đảo ngược [2, 19].

Bản chất của việc liên kết trong blockchain: liên kết giữa hàm băm của khối hiện tại và hàm băm của khối trước đó, giải thích ý nghĩa của chuỗi khối được liên kết bằng mật

mã thông qua các hàm băm này. Nếu ai đó giả mạo dữ liệu, giá trị của hàm băm này sẽ bị thay đổi và kết quả là chuỗi không hợp lệ. Các loại thông tin khác nhau có thể được lưu trữ trên blockchain nhưng việc sử dụng phổ biến nhất cho đến nay là sổ cái cho các giao dịch.

Có nhiều khái niệm có liên quan đến blockchain, chẳng hạn như: mạng ngang hàng phân tán (distributed peer-to-peer network) [13, 23], sổ cái đồng thuận (consensus ledgers), hàm băm mật mã (cryptographic hashes) [6],...

Điểm khác biệt của Blockchain và sổ cái phân tán (Distributed Ledger) Mặc dù bản thân blockchain cũng được biết đến như là một sổ cái phân tán, nhưng giữa chúng vẫn có sự khác biệt.

Bảng 2.1: So sánh công nghệ sổ cái phân tán và công nghệ blockchain

	Sổ cái phân tán	Blockchain
Công nghệ	Công nghệ gốc	Một nhánh của sổ cái phân tán
Tính công khai	Thường không công khai.	Bất kỳ ai cũng có thể sử dụng.
	Hạn chế những người có thể sử dụng và truy cập.	Bất cứ ai cũng có thể đóng vai trò là nút xác thực.
	Hạn chế những người có thể hoạt động như một nút (Trong nhiều trường hợp, các quyết định quản trị giao cho một cơ quan tập trung duy nhất)	Khi trở thành nút đều có thể hành động như một phần của cơ chế quản trị của blockchain đó.
Cấu trúc dữ liệu	Không yêu cầu dạng khối	Chuỗi khối dữ liệu liên kết chặt chẽ
Cơ chế đồng thuận	Không yêu cầu	Sử dụng các cơ chế đồng thuận để tạo niềm tin
Khả năng mở rộng	Gần như vô hạn	Giới hạn bởi năng lực của hệ thống

2.3 Hàm băm

2.3.1 Sơ lược về hàm băm

Định nghĩa 1.3. Hàm băm (hash function) là giải thuật nhằm sinh ra các giá trị băm (hash value) tương ứng với một khối dữ liệu (có thể là một chuỗi ký tự, một đối tượng,...). Giá trị băm này đóng vai trò như một khóa để phân biệt các khối dữ liệu, tuy nhiên, hiện tượng trùng khóa (hay còn gọi là đụng độ) vẫn có thể xảy ra và mục tiêu hướng tới là cải tiến giải thuật hàm băm để giảm thiểu đụng độ [19].

Hàm băm thường được sử dụng trong bảng băm nhằm giảm chi phí tính toán khi tìm một khối dữ liệu trong một tập hợp. Đa số các ngôn ngữ lập trình ngày nay đều cung cấp thư viện ứng dụng bảng băm dưới các dạng: tập hợp (collection), danh sách (list), bảng (table), ánh xạ (mapping), từ điển (dictionary),...

Hàm băm là viết tắt của dấu vân tay kỹ thuật số của một lượng dữ liệu nằm trong khối. Hàm băm được sử dụng để ánh xạ dữ liệu với kích thước tùy ý thành các giá trị băm có kích thước cố định.

Một hàm băm được đánh giá hiệu quả khi nó thỏa mãn các điều kiện như: khả năng tính toán nhanh; các khóa được phân bố đều trong bảng băm; ít xảy ra đụng độ và xử lý được các khóa có kiểu dữ liệu khác nhau.

2.3.2 Đặc trưng của hàm băm

Hàm băm có những đặc trưng như sau:

- Tính xác định, nghĩa là dữ liệu đầu vào giống nhau thì có cùng giá trị của hàm băm
- Tốc độ tính toán nhanh
- Không thể tạo lại dữ liệu, tức là từ một giá trị băm không thể tái tạo lại dữ liệu ban đầu.
- Tính không tương quan, chỉ cần thay đổi một chút về dữ liệu đầu vào cũng gây ra sự thay đổi đáng kể về giá trị hàm băm.

2.3.3 Ứng dụng

Hàm băm mật mã (cryptographic hash function) là một hàm băm một chiều [6, 21], tức là không có phương pháp thực tiễn nào để tìm ra bộ dữ liệu ứng với một giá trị băm đã biết và việc tấn công vào hàm băm để lấy dữ liệu là không thể.

Bảng băm cũng là một ứng dụng quan trọng và phổ biến trong thực tế, cho phép tra cứu nhanh một bản ghi dữ liệu nếu cho trước khóa của bản ghi đó (các khóa trong trường hợp này không phải là một chiều như hàm băm mật mã).

Thuật toán phổ biến được sử dụng để mã hóa bất kỳ nguồn dữ liệu kỹ thuật số nào là hàm băm SHA256 (Secure Hash Algorithm 256 bits) [14]. Đặc điểm của SHA256 có : giải mã một chiều, tính xác định, tính toán nhanh, tính không tương quan , và chịu được đụng độ

2.3.4 Ý nghĩa của hàm băm đối với công nghệ Blockchain

Quá trình xác nhận giao dịch dựa trên dữ liệu được mã hóa bằng thuật toán băm. Giá trị băm là một chuỗi các số và chữ cái không giống với dữ liệu gốc. Hàm băm xử lý dữ liệu từ một khối thông qua hàm toán học, kết quả đầu ra có độ dài cố định.

Việc giải quyết các hàm băm để mã hóa các khối mới đòi hỏi sức mạnh tính toán đáng kể. Giải quyết hàm băm về cơ bản là giải quyết một vấn đề toán học phức tạp và bắt đầu với dữ liệu có sẵn trong tiêu đề khối. Nếu giải quyết được hàm băm thì nó được chấp nhận làm giải pháp, và khối được thêm vào blockchain.

2.4 Đơn vị cấu thành blockchain - khối (block)

Định nghĩa 1.4. Một khối (block) là một bản ghi gồm dữ liệu bên trong nó, đồng thời chứa giá trị băm của khối trước đó và giá trị băm của chính nó [15].

Lý do sử dụng thuật toán băm là vì hàm băm là hàm một chiều nên các kỹ thuật dịch ngược không khả dụng, do đó, việc bỏ khóa nó là hoàn toàn không thể.

Blockchain là một sổ cái kỹ thuật số bất biến, bất cứ ai cố tình thay đổi dữ liệu của một khối sẽ làm thay đổi giá trị băm của khối này. Việc này dẫn đến liên kết giữa khối với khối tiếp theo bị phá vỡ, khiến tất cả các khối sau đó sẽ không còn hợp lệ. Do đó, dữ liệu sau khi nhập vào thì không thể thay đổi.

Trong trường hợp liên kết mật mã bị phá vỡ và gây ra lỗi lưu trữ dữ liệu như trên, vấn đề khôi phục lại hệ thống được giải quyết thông qua việc triển khai hệ thống mạng ngang hàng phân tán (P2P) [13, 23]. Đây là một thành phần quan trọng của công nghệ blockchain và là một cải tiến đáng kể trong công nghệ lưu trữ dữ liệu so với các công nghệ lưu trữ tập trung truyền thống.

Các thành phần cơ bản của một khối [15, 19]:

- Mã số khối
- Giá trị của hàm băm của khối trước đó (Previous block's hash value)
- Dữ liệu được đóng gói trong khối (Data)
- Hàm băm của khối hiện tại (Own hash)

Ngoài ra, còn một thành phần khác là nonce (number used only once - số chỉ dùng một lần), cung cấp khả năng kiểm soát bổ sung và tính linh hoạt giúp xác định chính xác giá trị của hàm băm.

Đầu vào của một hàm băm gồm các thành phần: mã số khối, giá trị hàm băm khối trước, dữ liệu, và nonce [15].

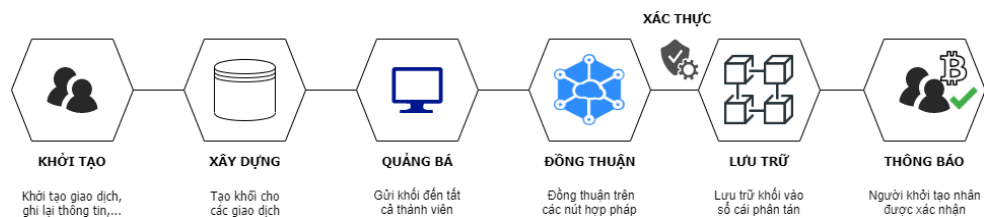
2.5 Quy trình của Blockchain

2.5.1 Lược đồ chung

Một giao dịch trong mạng blockchain để thực hiện thành công phải trải qua 6 bước, trong đó:

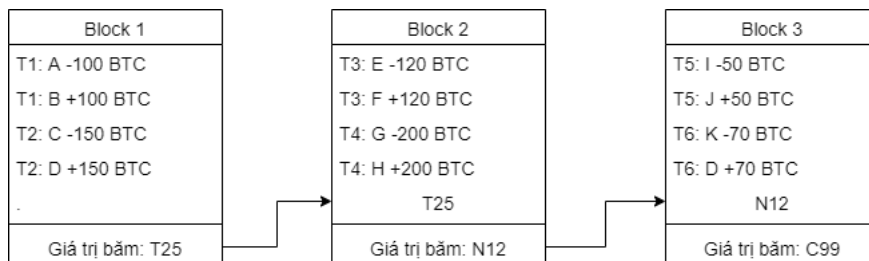
- Bước 1: **Khởi tạo** - Các bên tham gia giao dịch, chi tiết thông tin giao dịch được ghi lại.
- Bước 2: **Xây dựng khối** - Một hoặc nhiều giao dịch được đóng gói chung vào trong một khối.
- Bước 3: **Quảng bá** - Khối được tạo sẽ được gửi đến cho tất cả thành viên trong mạng.

- Bước 4: **Đồng thuận** - Các nút hợp pháp trên mạng tiến hành xác thực giao dịch trên khối bằng cách khai thác khối này dựa trên cơ chế đồng thuận.
- Bước 5: **Lưu trữ** - Khối sau khi được xác thực sẽ được nối chuỗi và lưu trữ vào sổ cái phân tán blockchain.
- Bước 6: **Thông báo** - Giao dịch được thực hiện, các bên liên quan sẽ được nhận thông báo về giao dịch.



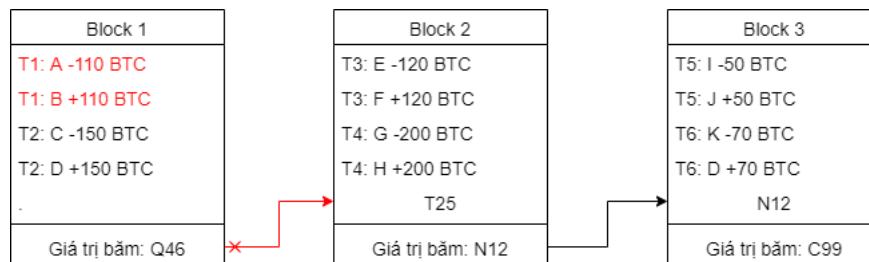
Hình 2.2: Lược đồ về quy trình giao dịch trong mạng blockchain

Ví dụ 1.1. Để minh họa một quá trình giao dịch trên mạng, ta xét ví dụ về một giao dịch Bitcoin: Giả sử có ba khối, mỗi khối đăng ký hai giao dịch. Khi được nối với nhau thì thuộc tính giá trị băm của khối trước sẽ được khối sau lưu lại tạo thành một chuỗi như Hình 2.3:



Hình 2.3: Minh họa quá trình giao dịch trên mạng.

Bất kỳ một thay đổi nào về dữ liệu của khối sẽ khiến giá trị băm thay đổi, làm đứt liên kết với khối phía sau (như Hình 2.4). Khi đó, cảnh báo sẽ được phát đi tới các nút khác trong mạng, đồng thời, trạng thái trước đó của khối được cập nhật lại dựa trên bản sao dữ liệu tại mỗi nút.



Hình 2.4: Trường hợp giá trị hàm băm thay đổi làm đứt liên kết.

Vì vậy, việc xác thực khối bản chất là việc xác định giá trị băm của khối bằng việc giải thuật toán băm SHA256 dựa trên hệ thống máy tính có khả năng tính toán lớn. Các khối sẽ được nối chuỗi nếu tìm ra được giá trị băm, khi đó, các bên tham gia giao dịch sẽ nhận được thông báo về giao dịch, chẳng hạn như ở giao dịch T1, A sẽ bị trừ 100 BTC và B nhận được 100 BTC.

2.5.2 Tính bảo mật của blockchain

Blockchain duy trì được tính bảo mật nhờ các cơ chế và kỹ thuật khác nhau:

- Hệ thống phân tán: các bản ghi dữ liệu được sao lưu và đồng bộ trên tất cả các nút trong mạng giúp hạn chế việc dữ liệu bị giả mạo và đảm bảo tính hồi phục của hệ thống [1, 15, 19].
- Mã hóa: dữ liệu mỗi khối được mã hóa bằng hàm băm, đóng vai trò đảm bảo tính bảo mật và tính bất biến của blockchain [15, 19].
- Kinh tế học mã hóa (Cryptoeconomics): xây dựng dựa trên lý thuyết trò chơi, sử dụng các nguyên lý kinh tế nhằm khuyến khích các nút trung thực hơn là thực hiện các hành vi độc hại hoặc gây lỗi. Các nút không trung thực sẽ bị trục xuất khỏi mạng blockchain, trong khi các nút đào trung thực có khả năng nhận được phần thưởng khối đáng kể.
- Hệ thống chịu lỗi Byzantine (Byzantine Fault Tolerance - BFT): cho phép một mạng lưới phân tán đạt được sự đồng thuận ngay cả khi một số nút trong mạng bị lỗi, bằng cách ra quyết định tập thể (bao gồm cả nút bình thường và nút bị lỗi) nhằm giảm ảnh hưởng của các nút bị lỗi [16].

2.6 Các cơ chế đồng thuận

2.6.1 Bằng chứng công việc (Proof of Work - PoW)

Định nghĩa 1.5. PoW là cơ chế nhằm ngăn chặn việc sử dụng năng lực điện toán độc hại như gửi email spam hoặc phát động các cuộc tấn công từ chối dịch vụ (DoS - Denial Of Service) [2].

Bản chất của cơ chế này là các nút đặc biệt (gọi là các thợ mỏ) cạnh tranh việc xác thực giao dịch (được đóng thành khối) để nhận phần thưởng. Họ thực hiện bằng cách sử dụng năng lực tính toán của hệ thống máy tính giải một câu đố chuyên sâu về tính toán (để xác minh) tìm ra số nonce, tìm ra được nonce tức là khai thác thành công khối đó.

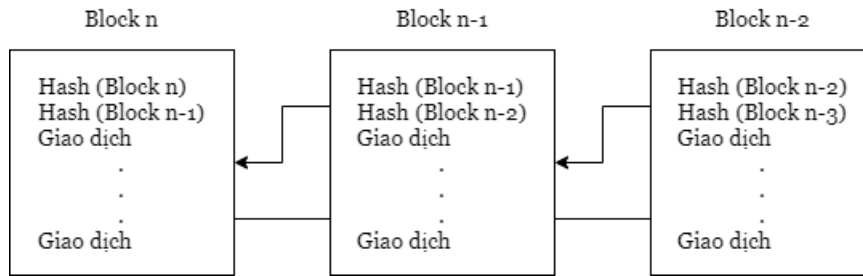
Cơ chế PoW tạo ra nhằm mục đích kiểm soát công việc, đảm bảo rằng các khối mới không được tạo ra quá nhanh. PoW áp đặt một số giới hạn về hành động trong mạng. Nếu muốn tấn công vào mạng đòi hỏi rất nhiều sức mạnh tính toán và rất nhiều thời gian để thực hiện các tính toán. Do đó, các cuộc tấn công trên lý thuyết vẫn có thể xảy ra nhưng chi phí quá cao. Đây chính là ưu điểm lớn nhất của PoW.

PoW có khả năng ngăn chặn chi tiêu kép [2, 7], được hầu hết các loại tiền mã hóa sử dụng như là thuật toán đồng thuận của chúng, được dùng như một phương pháp để bảo mật cho sổ cái của tiền mã hóa. Cơ chế này phổ biến trong Bitcoin, Ethereum, và hầu hết các loại tiền mã hóa khác.

Cơ chế hoạt động như sau:

- Các thợ mỏ giải quyết các câu đố, hình thành các khối mới và xác nhận các giao dịch. Băm của mỗi khối chứa băm của khối trước đó, làm tăng bảo mật và ngăn chặn bất kỳ vi phạm khối nào. Bất kỳ khối nào bao gồm một giao dịch không hợp lệ sẽ bị mạng tự động từ chối.
- Sau khi khối mới được hình thành thì các giao dịch trong khối này được coi là đã xác nhận.

Rào cản trong thực tiễn:



Hình 2.5: Mô hình cơ chế hoạt động của PoW

- Khả năng tiếp cận: đòi hỏi một lượng năng lượng đáng kể để duy trì, đồng thời phải mua, thiết lập và duy trì tất cả các phần cứng cần thiết để chạy hệ thống máy tính khai thác PoW.
- Tập trung: tập trung thành hai loại: các tập đoàn khai thác mỏ lớn hoạt động trong các khu vực có chi phí điện thấp và thời tiết lạnh (để giảm chi phí làm mát phần cứng khai thác) và các hồ khai thác mỏ.
- Khả năng mở rộng: khả năng mở rộng của mạng lưới bị giới hạn do phụ thuộc tốc độ khai thác khối.

2.6.2 Bằng chứng cổ phần (Proof of Stake - PoS)

Định nghĩa 1.6. PoS là cơ chế đồng thuận trong đó các nút của mạng blockchain phải cược một phần tài sản để được tham gia vào quá trình xác nhận các giao dịch trong một khối. Các nút tham gia được gọi là người xác thực (validator). Số tiền đặt cược được gọi là cổ phần (stake). Số tiền này sẽ bị hệ thống khóa lại, cho đến khi nút đó rút khỏi công việc xác thực [2].

Người xác thực được chọn ngẫu nhiên từ tập những người cược tiền. Nếu khối hợp lệ, nút tham gia xác thực sẽ nhận được phần thưởng là các khoản phí giao dịch, thường giao động từ 10 – 15% tiền cược. Chính vì vậy, cược càng nhiều thì phần thưởng càng lớn.

Cách thức chọn người xác nhận Người dùng khóa một số tiền nhất định vào mạng làm cổ phần. Số lượng cổ phần càng lớn, thì cơ hội được chọn làm người xác thực khối

kế tiếp càng lớn. Để tránh việc quá trình chỉ ưu tiên cho các nút giàu nhất trong mạng, hai phương pháp được sử dụng phổ biến nhất là:

- Lựa chọn khối ngẫu nhiên: tìm kiếm các nút có giá trị băm thấp nhất kết hợp với cổ phần lớn nhất. Vì độ lớn của cổ phần được công khai, nên có thể dự đoán người được chọn làm người xác thực kế tiếp.
- Lựa chọn độ tuổi tài sản: các nút được chọn dựa trên thời gian mà các token của họ đã được lưu giữ làm cổ phần gọi là độ tuổi tài sản. Độ tuổi của tài sản phải không dưới 30 ngày mới được xét chọn làm người xác thực.

Hiệu quả bảo mật: Người xác thực có thể phê duyệt một giao dịch gian lận, tuy nhiên, người đó sẽ mất một phần trong cổ phần và không được làm người xác thực trong tương lai. Vì vậy, khi cổ phần cao hơn phần thưởng, nếu gian lận thì người xác thực sẽ mất nhiều hơn số tiền thu lại được.

PoS giải quyết ba vấn đề của chuỗi PoW được thảo luận trước đó:

- Khả năng truy cập: không cần dùng nhiều năng lực tính toán, tuy nhiên, lại yêu cầu người xác thực phải đặt cược cổ phần với một lượng khá đáng kể.
- Tập trung hoá: việc chọn người xác thực không phụ thuộc vào số nút người đó kiểm soát, mà chỉ phụ thuộc vào số cổ phần người đó đang sở hữu hay độ tuổi của tài sản.
- Khả năng mở rộng: cho phép mở rộng bằng phương pháp sharding (phân mảnh) mà không làm giảm bảo mật.

PoS phổ biến trong Decred, Peercoin, Ethereum và trong tương lai là nhiều loại tiền mã hoá khác. Phân cấp hơn, tiêu hao ít năng lượng và không dễ gì bị đe dọa.

2.6.3 Bằng chứng cổ phần ủy quyền (Delegated Proof of Stake - DPoS)

Định nghĩa 1.7. DPoS là một cơ chế đồng thuận thay thế, đòi hỏi các cổ đông phải bỏ phiếu cho các "đại biểu", những người này sau đó chịu trách nhiệm xác nhận các giao dịch và duy trì chuỗi khối [2].

Những người nắm giữ tài sản sẽ bỏ phiếu cho một nhóm đại biểu được chọn để thực hiện vai trò xác nhận các giao dịch. Quyền biểu quyết nhiều hay ít phụ thuộc số lượng tài sản mà người đó nắm giữ.

Nó có thể được coi là giao thức đồng thuận ít tập trung nhất trong số các giao thức, cũng như có tính bao quát nhất. Một đại biểu thể hiện cam kết bằng cách cược tiền vào hệ thống (tài sản này sẽ bị tịch thu trong trường hợp người này thực hiện các hành vi gây hại cho hệ thống). Vai trò của các đại biểu: đảm bảo hoạt động của nút, xác thực giao dịch, chia phần thưởng cho cử tri.

Về bản chất, một mạng lưới DPoS được tự quản lí và điều chỉnh bởi tất cả những người tham gia của nó, việc đảm bảo lợi ích tốt nhất cho mạng vẫn là ưu tiên hàng đầu. DPoS được sử dụng ở nhiều đồng tiền mới sau này có thể kể đến như: Bitshares, EOS, LISH, ICON, Cybermiles,...

2.6.4 Bằng chứng ủy nhiệm (Proof of Authority - PoA)

Định nghĩa 1.8. PoA là một thuật toán đồng thuận dựa trên danh tiếng, trong đó những người xác thực khối được chọn không dựa trên số lượng tài sản mà dựa trên chính danh tiếng của mình [2].

Người xác thực là những người điều tiết của hệ thống được chọn dựa trên danh tiếng của họ.

Mô hình PoA có số lượng người xác thực khối giới hạn, phù hợp hơn cho các mạng blockchain riêng tư vì hiệu suất làm việc của nó cao hơn rất nhiều các hệ thống khác, đồng thời nó đề cao danh tính của người dùng thay vì số cổ phần của người dùng.

Các điều kiện cho đồng thuận PoA:

- Danh tính hợp lệ và đáng tin cậy: người xác thực cần xác nhận danh tính thực của mình.
- Khó khăn để trở thành người xác thực: ứng viên phải sẵn sàng đầu tư tiền và chấp nhận rủi ro với danh tiếng của mình.

Hạn chế của hệ thống PoA là danh tính của những người xác thực được công khai, việc này có thể tạo cơ hội cho các bên thứ ba khai thác.

Đây là mô hình tập trung thường thấy trong POA.Network, Ethereum Kovan Testnet với đặc điểm là hiệu suất cao, có khả năng mở rộng tốt.

2.7 Phân loại Blockchain

Nhu cầu cơ bản nhất hoặc ứng dụng của blockchain là thực hiện các giao dịch hoặc trao đổi thông tin thông qua một mạng an toàn. Tuy nhiên, có nhiều cách khác nhau để thiết lập mạng blockchain tùy thuộc vào việc sử dụng và yêu cầu.

Có chủ yếu là hai loại blockchain: Blockchain công khai (Public Blockchain) và Blockchain riêng tư (Private Blockchain). Tuy nhiên, cũng có một số biến thể, như Blockchain kết hợp (Consortium Blockchain) và Blockchain lai (Hybrid Blockchain).

2.7.1 Blockchain công khai (Permissionless Blockchain - Không phân quyền)

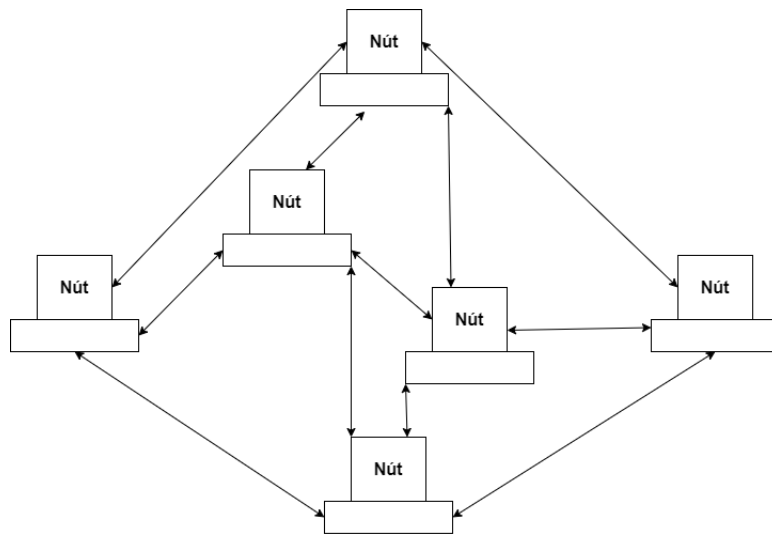
Định nghĩa 1.9. Blockchain công khai (Public Blockchain) là một hệ thống sổ cái phân tán không hạn chế, không phân quyền. Bất kỳ ai truy cập Internet đều có thể đăng nhập vào nền tảng blockchain để trở thành một nút của mạng blockchain. Một nút hoặc người dùng là một phần của blockchain công khai được phép truy cập các bản ghi hiện tại và quá khứ, xác minh các giao dịch hoặc làm bằng chứng công việc (PoW) cho một khối và thực hiện khai thác.

Ưu điểm:

- An toàn, đáng tin cậy.
- Cởi mở và minh bạch: blockchain công khai được mở và minh bạch dữ liệu cho tất cả các nút tham gia.

Nhược điểm:

- Tỷ lệ giao dịch mỗi giây (Transactions per second - TPS) trong một blockchain công khai là rất thấp.



Hình 2.6: Minh họa mô hình mạng Blockchain công khai.

- Các vấn đề về khả năng mở rộng: do tốc độ xử lý và hoàn thành giao dịch chậm nên khó mở rộng.
- Tiêu thụ năng lượng cao.

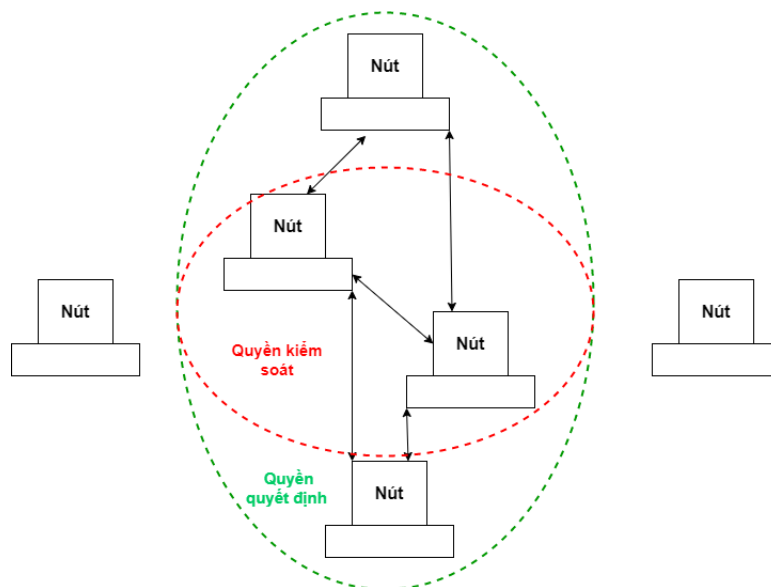
Ví dụ: Bitcoin, Ethereum, Litecoin,...

2.7.2 Blockchain riêng tư (Permissioned Blockchain - Phân quyền)

Định nghĩa 1.10. Blockchain riêng tư (Private Blockchain) là một blockchain hạn chế hoặc chỉ hoạt động trong một mạng khép kín. Các blockchain riêng tư thường được sử dụng trong một tổ chức hoặc doanh nghiệp mà chỉ có các thành viên được chọn là những người tham gia vào một mạng lưới blockchain (như Hình 2.7).

Mức độ bảo mật, ủy quyền, quyền, khả năng tiếp cận nằm trong tay của tổ chức kiểm soát. Do đó, các blockchain riêng tư cũng tương tự được sử dụng như một blockchain công cộng nhưng có một mạng lưới nhỏ và hạn chế. Các mạng blockchain riêng tư được triển khai để bỏ phiếu, quản lý chuỗi cung ứng, nhận dạng kỹ thuật số, sở hữu tài sản, v.v.

Ưu điểm:



Hình 2.7: Minh họa mô hình mạng Blockchain riêng tư.

- TPS cao: các blockchain riêng tư có thể tạo điều kiện thuận lợi cho các giao dịch với tốc độ lên đến hàng ngàn hoặc hàng trăm nghìn TPS cùng một lúc.
- Khả năng mở rộng: có thể chọn kích thước của blockchain riêng tư tùy theo nhu cầu của mạng.

Nhược điểm:

- Tập trung: một hệ thống quản lý truy cập có quyền giám sát toàn bộ hệ thống.
- Bảo mật thấp: do có số lượng nút hoặc người tham gia ít, dễ bị tấn công.

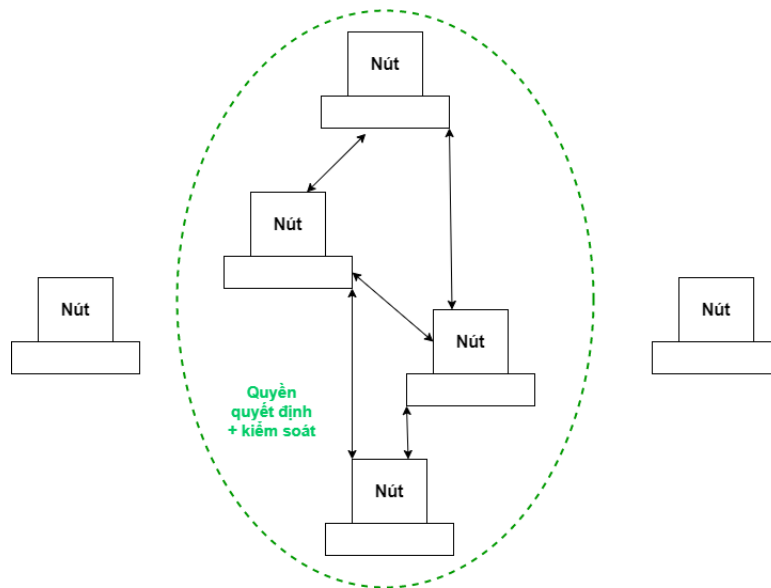
2.7.3 Blockchain kết hợp (Consortium Blockchain)

Định nghĩa 1.11. Blockchain kết hợp là một loại mạng bán phi tập trung, một biến thể của Blockchain riêng tư, trong đó, sẽ có nhiều tổ chức cùng quản lý một mạng [2].

Cách tổ chức quản lý trong mạng này trái ngược với những gì chúng ta đã thấy trong một Blockchain riêng tư, được quản lý bởi chỉ một tổ chức duy nhất. Nhiều tổ chức có thể hoạt động như một nút trong loại blockchain này và trao đổi thông tin hoặc khai thác. Hình 2.8 minh họa một mạng Blockchain kết hợp.

Thường được sử dụng bởi các ngân hàng, tổ chức chính phủ, v.v.

Một số ví dụ về hệ thống trên thực tế: Energy Web Foundation, R3, v.v.



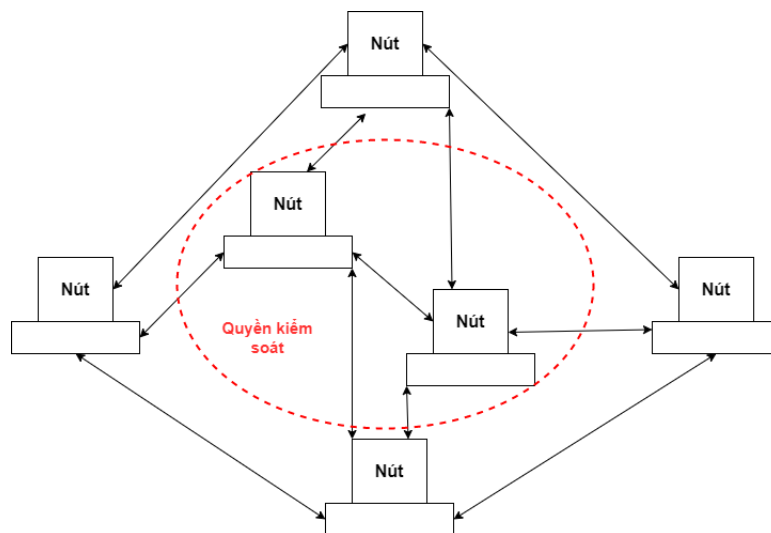
Hình 2.8: Minh họa mô hình mạng Blockchain kết hợp.

2.7.4 Blockchain lai (Hybrid Blockchain)

Định nghĩa 1.12. Blockchain lai là sự kết hợp nhằm sử dụng ưu điểm của cả hai giải pháp Blockchain công khai và Blockchain riêng tư. Nó sử dụng các tính năng của cả hai loại blockchain, tức là cho phép một hệ thống sẽ có quyền truy cập và quyền tự do được kiểm soát cùng một lúc. Người dùng có thể kiểm soát ai có quyền truy cập vào dữ liệu được lưu trữ trong blockchain. Chỉ một phần dữ liệu hoặc hồ sơ được chọn từ blockchain mới có thể được phép công khai giữ bí mật phần còn lại trong mạng riêng (xem Hình 2.9).

Lợi ích của Blockchain lai

- Tạo ra một hệ sinh thái khép kín trong doanh nghiệp.
- Bảo vệ quyền riêng tư trong khi vẫn kết nối với thế giới bên ngoài.
- Chi phí giao dịch thấp.



Hình 2.9: Minh họa mô hình mạng Blockchain lai.

Ví dụ về hệ thống sử dụng Blockchain lai: Dragonchain.

2.8 Hợp đồng thông minh (Smart Contract)

Năm 1998, nhà khoa học máy tính Nick Szabo công bố làm việc trên “bit vàng”, một loại tiền tệ kỹ thuật số phi tập trung. Đồng thời, ông cũng lần đầu tiên phát biểu khái niệm về hợp đồng thông minh.

Định nghĩa 1.13. Hợp đồng thông minh là một thuật ngữ mô tả một bộ giao thức đặc biệt có khả năng tự động thực hiện các điều khoản, các thỏa thuận giữa các bên trong hợp đồng (ở trường hợp này là các hệ thống máy tính) [5].

Toàn bộ hoạt động của hợp đồng thông minh được thực hiện một cách tự động mà không có sự can thiệp từ bên ngoài, hay thông qua một bên thứ ba trung gian. Các điều khoản trong hợp đồng thông minh tương đương với một hợp đồng có pháp lý và được ghi lại dưới ngôn ngữ của lập trình [1, 5].

Điểm nổi bật nhất của hợp đồng thông minh là cho phép hai bên tham gia thực hiện hợp đồng một cách chính xác, an toàn và nhanh chóng mà không cần gặp trực tiếp, hay một bên trung gian thứ ba mà chỉ cần có kết nối Internet.

Các bước thực hiện hợp đồng thông minh

1. Mã hóa (Encoding)
2. Hợp đồng thông minh được gửi thông qua sổ cái phân tán
3. Thực hiện hợp đồng

So sánh hợp đồng thông minh và hợp đồng truyền thống

Bảng 2.2: So sánh hợp đồng thông minh và hợp đồng truyền thống.

	Hợp đồng thông minh	Hợp đồng truyền thống
Phương thức giao dịch	Được xây dựng dựa trên các ngôn ngữ lập trình máy tính. Được ký bởi chữ ký điện tử.	Được xây dựng bởi các chuyên gia pháp lý
Thời gian xác lập	Nhanh gọn, không tốn thời gian	Mất thời gian để hoàn thiện khung pháp lý cho hợp đồng
Tính pháp lý	Các quy định và chính sách mang tính pháp lý vẫn chưa đầy đủ và rõ ràng.	Được quy định đầy đủ bởi hệ thống pháp luật
Tính minh bạch	Thực hiện tự động, đảm bảo được tính minh bạch	Được thực hiện bởi các bên có liên quan, kém minh bạch hơn.
Rủi ro bảo mật	Có nguy cơ bị tin tặc tấn công	Được đảm bảo thực hiện bởi pháp luật.

Thách thức khi ứng dụng hợp đồng thông minh

- Bảo mật: nhiều lỗ hổng được gây ra bởi sự hiểu lầm trong việc chuyển đổi các điều khoản trên thực tế sang ngôn ngữ lập trình, vì vậy vấn đề cải thiện mức độ bảo mật và ngôn ngữ hợp đồng thông minh là một trong những mối quan tâm chính của bất kỳ hệ thống nào.
- Thiếu tính pháp lý: nhiều quốc gia vẫn chưa công nhận hợp đồng thông minh.

2.9 Đặc điểm của blockchain

Là một sổ cái phân tán Thông tin được chia sẻ trên blockchain tồn tại dưới dạng cơ sở dữ liệu được chia sẻ, nhân rộng và đồng bộ liên tục. Mọi dữ liệu không được lưu trữ tập trung ở duy nhất một vị trí nào trên mạng, các bản ghi được lưu trữ một cách công khai, để kiểm chứng [1, 15, 19].

Tính bất biến Dữ liệu khi đã được đóng gói thành các khối và đưa lên blockchain thì không thể sửa đổi, can thiệp vào [1, 15].

Tính bền vững Các khối trong blockchain không thể bị hỏng. Nếu bất cứ khối tại một nút nào bị lỗi, ngay lập tức hệ thống sẽ phát đi cảnh báo tới các nút trên mạng, đồng thời, thay thế khối tại nút đó dựa trên bản sao sổ cái tại các nút khác trên mạng.

Tính minh bạch Mọi giao dịch trên mạng blockchain đều được công khai. Bất cứ người dùng nào cũng có thể xem được.

Tăng cường bảo mật Do dữ liệu được lưu trữ phân tán nên blockchain loại bỏ những rủi ro đi kèm với dữ liệu được tổ chức tập trung. Mạng blockchain không có những điểm dễ bị tổn thương.

3 Ứng dụng của Blockchain

3.1 Bitcoin - Ứng dụng đầu tiên của blockchain

Bitcoin là một loại tiền mã hoá, được phát hành năm 2009 thông qua một bài báo mang tựa đề “Bitcoin: A Peer-to-Peer Electronic Cash System” bởi Satoshi Nakamoto [15]. Giao dịch được thực hiện mà không cần thông qua bên trung gian. Do đó không có phí giao dịch và không cần phải cung cấp tên thật.

Bitcoin chính là ví dụ điển hình cho tiền điện tử (cryptocurrency) [15], với đặc điểm hấp dẫn người dùng bởi tính ẩn danh và không bị kiểm soát bởi chính phủ, được dự đoán như một loại tiền tệ tiềm năng có khả năng thay thế tiền giấy.

Công nghệ Blockchain cung cấp một sổ cái công khai Bitcoin, là một danh sách sắp xếp theo trình tự thời gian của các giao dịch. Hệ thống này được dùng để chống lại chi tiêu kép và những hành động sửa bản ghi trái phép. Mỗi nút trong mạng Bitcoin đều giữ một bản sao Blockchain đã được phân tán và có chứa những khối được xác thực bởi nút đó. Các nút phải tuân theo các cơ chế đồng thuận để duy trì sự đồng thuận trên toàn bộ mạng.

Bảng 3.1 liệt kê những thông tin cơ bản về Bitcoin (tính đến ngày 11/05/2020).

Bảng 3.1: Thông tin cơ bản về Bitcoin (tính đến ngày 11/05/2020)

Số lượng Bitcoin (BTC) tối đa	21,000,000
Số lượng đào được hiện tại	18,573,413
Thuật toán hàm băm	SHA256
Cơ chế đồng thuận	PoW
Giá trị Bitcoin	\$23,220 / 1 BTC
Phần thưởng cho mỗi block	6.25 BTC
Thời gian trung bình tạo ra 1 khối	10 phút
Số lần xảy ra sự kiện Bitcoin Halving	3

Bitcoin được thiết kế như một loại tiền tệ giảm phát. Theo thời gian, việc phát hành Bitcoin sẽ giảm và do đó trở nên khan hiếm hơn. Khi Bitcoin trở nên khan hiếm hơn và nếu nhu cầu đối với chúng tăng theo thời gian, Bitcoin có thể chống lạm phát, và giá trị đồng Bitcoin tăng lên. Giá trị đồng tiền này lần đầu ấn định trên sàn giao dịch ngày 5 tháng 10 năm 2009 là 0.00076 USD / 1 BTC, và hiện tại, giá trị đồng tiền này đã tăng kỷ lục lên mức 23,000 USD/ 1 BTC.

3.2 Truy xuất nguồn gốc

Hiện nay công nghệ blockchain đã được ứng dụng trong nông nghiệp cụ thể là truy xuất nguồn gốc trên toàn bộ chuỗi cung ứng. Blockchain hứa hẹn cải thiện truy xuất nguồn gốc và minh bạch trong chuỗi giá trị nông nghiệp thông qua các tiêu chí:

- Cập nhật thông tin nhanh chóng theo thời gian thực và kết nối thông tin.

- Dữ liệu được bảo mật và đáng tin cậy.
- Khả năng truy cập dữ liệu nhanh chóng.

Việc ứng dụng blockchain trong truy xuất nguồn gốc cho phép dữ liệu đã được chia sẻ trên hệ thống có thể truy cập nhanh chóng trong thời gian thực. Chính vì vậy cho phép việc truy xuất thông tin nhanh chóng về dữ liệu nguồn gốc của sản phẩm đến từng công đoạn của quá trình sản xuất, kinh doanh mà các mắt xích đã đưa lên mạng lưới dữ liệu chung. Việc truy lại chính xác, xác định nguyên nhân mất an toàn và thu hồi sản phẩm cũng dễ dàng hơn khi áp dụng công nghệ blockchain.

Phần 4 và Chương 2 sẽ đưa ra những kiến thức cơ bản về truy xuất nguồn gốc và xây dựng ứng dụng truy xuất nguồn gốc dựa trên công nghệ blockchain.

3.3 Xây dựng chính phủ điện tử

Trong số những công nghệ nền tảng phát triển chính phủ điện tử, blockchain thu hút được nhiều sự quan tâm nhờ vào tính minh bạch, tin cậy và bảo mật dữ liệu, đặc biệt nó phù hợp trong việc cung cấp dịch vụ công trực tuyến cho người dân, doanh nghiệp. Blockchain sẽ cho phép lưu trữ toàn bộ tương tác giữa người dân, doanh nghiệp với các cơ quan nhà nước. Quan trọng hơn, với mô hình như vậy, dữ liệu sẽ được liên thông, lưu trữ bởi tất cả đối tượng sử dụng hệ thống, tự động cập nhật khi có thay đổi.

Để áp dụng thực tế vào chính phủ điện tử, có thể xem xét một số nguyên tắc triển khai chính phủ điện tử từ tính chất vốn có của blockchain như sau:

1. Nguyên tắc luật hoá: bảo đảm tính áp buộc, cho phép thực thi luật thông qua cơ chế hợp đồng thông minh.
2. Nguyên tắc công khai, minh bạch (hoặc chiến lược mã nguồn mở): cho phép mọi người kiểm tra các luật lệ gắn với mã lệnh, giúp phần mềm an toàn bảo mật hơn, thúc đẩy sự phát triển của hệ sinh thái các phần mềm chính phủ điện tử.
3. Nguyên tắc tự động quy trình: xây dựng hệ thống chính phủ điện tử nhanh hơn và hiệu quả hơn; giúp nâng cao sự tham gia của cộng đồng vào công việc chung, dẫn đến các hoạt động tự quản trị của xã hội, tạo ra một hệ thống chính quyền dân chủ.

4 Truy xuất nguồn gốc

An toàn thực phẩm đang là mối quan tâm hàng đầu hiện nay của người dân nhiều nước, do việc sử dụng các hóa chất vượt quá giới hạn cho phép cho thực phẩm, đe dọa chất lượng và độ an toàn của sản phẩm, ảnh hưởng trực tiếp đến sức khỏe của con người. Vấn đề thu hồi các sản phẩm được xác định là thực phẩm bẩn, không an toàn đã trở nên cần thiết. Truy xuất nguồn gốc là một công cụ cho phép các đơn vị sản xuất, cung ứng thực phẩm hoặc cơ quan chức năng cùng tham gia để đáp ứng yêu cầu đó. Nó là nền tảng để xây dựng chính sách an toàn thực phẩm của bất kỳ quốc gia nào.

4.1 Khái niệm truy xuất nguồn gốc

Truy xuất nguồn gốc là khả năng lưu trữ và thu thập lại tất cả thông tin về nguồn gốc, nguyên liệu làm ra của một sản phẩm, đặc biệt là khi sản phẩm đó bị lỗi. Hệ thống xác định nguồn gốc cho phép xác định chất lượng một sản phẩm thông qua các giai đoạn và hoạt động liên quan đến sản xuất, chế biến, phân phối và xử lý thực phẩm, từ nơi sản xuất đến người tiêu dùng. Do đó, nó có thể tạo điều kiện thuận lợi cho việc xác định nguyên nhân của sản phẩm không đạt yêu cầu, thu hồi sản phẩm đó nếu cần thiết và ngăn chặn các sản phẩm không an toàn đến tay khách hàng.

Khái niệm truy xuất nguồn gốc định nghĩa bởi ISO (International Organization for Standardization - Tổ chức Tiêu chuẩn hóa Quốc tế) ISO đưa ra định nghĩa: “Truy xuất nguồn gốc là khả năng theo dõi chuyển động của thực phẩm qua (các) giai đoạn cụ thể của sản xuất, chế biến và phân phối” [11].

Tiêu chuẩn ISO 22005:2007 giải thích một cách toàn diện các nguyên tắc và yêu cầu đối với việc thiết kế và triển khai hệ thống truy xuất nguồn gốc thực phẩm. Tiêu chuẩn này cho phép các tổ chức hoạt động ở bất kỳ bước nào của chuỗi thực phẩm:

1. Theo dõi quá trình vận chuyển nguyên liệu (thức ăn, thực phẩm, thành phần của chúng và bao bì).
2. Xác định các văn bản, tài liệu có liên quan và theo dõi sát sao từng giai đoạn sản xuất.

3. Đảm bảo sự phối hợp đầy đủ giữa các bên liên quan.
4. Cải thiện khả năng trao đổi giữa các bên liên quan.
5. Nâng cao độ tin cậy của thông tin, tính hiệu quả và năng suất của tổ chức.

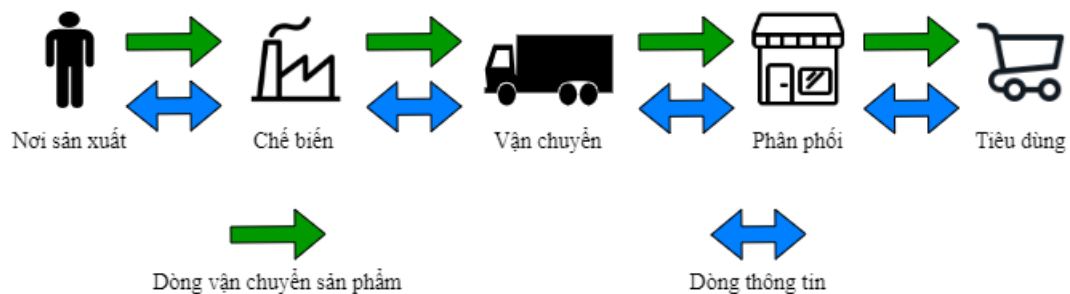
4.2 Đặc điểm của truy xuất nguồn gốc

Hệ thống truy xuất nguồn gốc là tổng hợp của dữ liệu và hoạt động có khả năng cung cấp thông tin về một sản phẩm và các thành phần của nó trên tất cả hoặc một phần của chuỗi sản xuất và sử dụng (ISO 2007). Hệ thống ghi lại dữ liệu và theo dõi sản phẩm và nguyên liệu từ nguồn cung, tới bước chế biến, phân phối sản phẩm và cuối cùng đến tay người tiêu dùng. Do đó, cơ sở của toàn bộ hệ thống được xây dựng dọc theo chuỗi cung ứng từ nơi sản xuất đến nơi tiêu thụ.

Những đặc điểm cơ bản của một hệ thống truy xuất nguồn gốc bao gồm:

- Xác định chi tiết từng đơn vị/ lô của tất cả các thành phần và sản phẩm;
- Thông tin về thời gian và địa điểm các đơn vị/ lô được chuyển đi, xử lý.
- Hệ thống sẽ liên kết những dữ liệu này và chuyển tất cả thông tin xác định nguồn gốc có liên quan tới sản phẩm đến công đoạn tiếp theo.

Trên thực tế, hệ thống xác định nguồn gốc lưu trữ hồ sơ dựa trên đường dẫn của một sản phẩm cụ thể từ nhà cung cấp thông qua các bước trung gian đến người tiêu dùng như Hình 4.1 sau:



Hình 4.1: Mô hình cơ bản của hệ thống truy xuất nguồn gốc sản phẩm và luồng thông tin

4.3 Bản chất của việc xây dựng một hệ thống truy xuất nguồn gốc

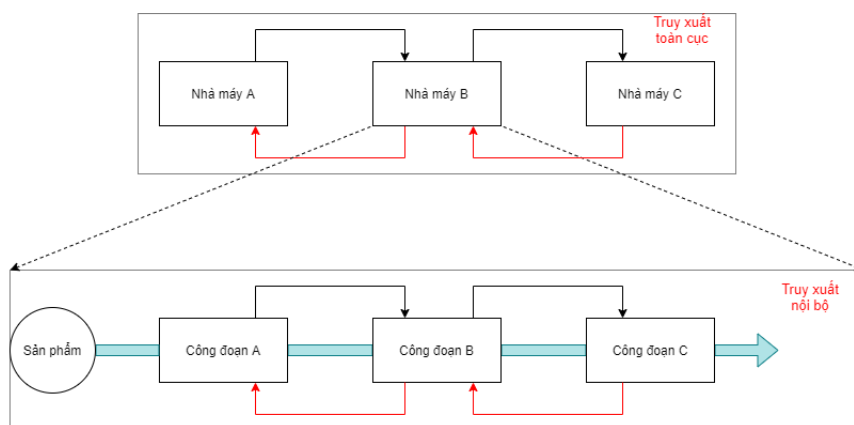
Hệ thống truy xuất nguồn gốc thực phẩm kiểm soát thông tin về thành phần thực phẩm, nguồn nguyên liệu, cách chế biến cũng như điều kiện vận chuyển và bảo quản. Vì vậy, một hệ thống truy xuất nguồn gốc lý tưởng sẽ chứa thông tin về cả định lượng và chất lượng của từng thành phần cấu tạo nên sản phẩm cuối cùng.

Để phát triển hệ thống truy xuất nguồn gốc hiệu quả, cần phải giải quyết những vấn đề sau [8]:

1. Xác định dữ liệu nào quan trọng và cần phải được thu thập.
2. Chủ sở hữu của thông tin trong mọi giai đoạn của chuỗi cung ứng.
3. Phương tiện, thiết bị để thu thập dữ liệu.
4. Cách quản lý dữ liệu sao cho luôn sẵn có và dễ hiểu với tất cả các bên liên quan và người tiêu dùng.

4.4 Các cấp độ truy xuất nguồn gốc

Theo các nghiên cứu của Corallo và Aung cùng các cộng sự, có hai cấp độ truy xuất nguồn gốc khác nhau [4, 8]:



Hình 4.2: Minh họa hai cấp độ truy xuất nguồn gốc: truy xuất toàn cục và truy xuất nội bộ

1. Truy xuất nội bộ (Internal traceability)

Truy xuất nguồn gốc nội bộ là quá trình truy xuất được duy trì trong nội bộ đơn vị doanh nghiệp để liên kết dữ liệu giữa các công đoạn, giữa các nguyên liệu và thành phẩm. Mỗi liên kết giữa sản phẩm và các nguyên liệu đầu vào của nó phải được duy trì (chẳng hạn như máy cày, phân bón, bao bì, ... và nhiều nguyên liệu đầu vào khác) để duy trì truy xuất nguồn gốc [4, 8].

2. Truy xuất toàn cục (External traceability)

Truy xuất toàn cục là quá trình truy xuất thông tin về sản phẩm giữa các đơn vị tham gia kênh phân phối sản phẩm [4]. Việc truy xuất nguồn gốc sản phẩm đòi hỏi xác định:

- Mã sản phẩm duy nhất.
- Mã lô hàng.

Để duy trì khả năng truy xuất nguồn gốc toàn cục, mã vật phẩm phải được gắn trên nhãn sản phẩm. Điều này liên kết các sản phẩm vật lý với các yêu cầu thông tin cần thiết để truy xuất nguồn gốc. Truy xuất nguồn gốc toàn cục cho phép: truy tìm trở lại (truy xuất nguồn gốc nhà cung cấp) và theo dõi chuyển tiếp (truy xuất nguồn gốc khách hàng).

Một thách thức chính đối với các hệ thống truy xuất này nằm ở sự phức tạp của chúng, vì mọi tác nhân có thể có các tiêu chuẩn và phương pháp riêng của họ để theo dõi và truy tìm sản phẩm, dẫn đến nhiều loại dữ liệu thu được. Do đó, việc tổ chức, quản lý và sử dụng các loại dữ liệu khác nhau đòi hỏi khả năng tùy biến của hệ thống [18].

4.5 Quy trình xây dựng hệ thống

Một quy trình xây dựng hệ thống truy xuất nguồn gốc thực phẩm hoàn thiện bao gồm những bước cơ bản sau:

Bước 1: Xác định vấn đề và mục tiêu.

Bước 2: Xác định cơ chế đồng thuận thích hợp nhất.

Bước 3: Xác định nền tảng phù hợp nhất.

Bước 4: Thiết kế cấu tạo.

Bước 5: Cấu hình ứng dụng.

Bước 6: Xây dựng các APIs.

Bước 7: Thiết kế giao diện người dùng.

Bước 8: Kiểm tra và xác định các vấn đề.

4.6 Hệ thống truy xuất nguồn gốc hiệu quả

Trong mọi trường hợp, khả năng xác định nguồn gốc phụ thuộc vào việc thu thập và ghi chép chính xác các dữ liệu, được điều phối bởi hệ thống quản lý. Hệ thống truy xuất nguồn gốc đạt hiệu quả khi các sản phẩm thực phẩm có thể dễ dàng được truy xuất toàn bộ thông tin trong chuỗi cung ứng thực phẩm.

Các yếu tố chính ảnh hưởng đến hiệu quả của truy xuất nguồn gốc như: cấu trúc và cách tổ chức chuỗi cung ứng (số lượng, mức độ tương tác, khả năng quản lý,...của thành viên); thời gian để truy xuất một sản phẩm; độ tin cậy của phương pháp; phương pháp thu thập và chuẩn hóa dữ liệu và phạm vi có thể truy xuất.

Một hệ thống truy xuất nguồn gốc thực phẩm bao gồm những thông tin về: các bên buôn bán sản phẩm (nhà cung cấp nguyên liệu, trang trại, nhà phân phối, đơn vị vận chuyển, khách hàng); các bên chế biến, xử lý và lưu trữ sản phẩm (nhà máy chế biến, đóng gói, kho bảo quản, cửa hàng phân phối,...); nguyên liệu tạo thành sản phẩm và ngày, giờ nhận- gửi sản phẩm của các bên.

Điểm mấu chốt để một chương trình xác định nguồn gốc thành công là khả năng nhận dạng chính xác. Hiện nay, công nghệ sử dụng mã vạch được ưa chuộng và phổ biến trong thực tế bởi tính tiện dụng và dễ dàng truy xuất bằng các thiết bị phổ biến như điện thoại

thông minh. Việc tận dụng công nghệ mã vạch giúp hệ thống trở nên dễ tiếp cận hơn với đa số người dùng.

4.7 Lợi ích và thách thức của hệ thống truy xuất nguồn gốc

Lợi ích

- Truy vấn và thực hiện thu hồi, xử lý nhanh chóng các sản phẩm kém chất lượng khi có vấn đề về an toàn thực phẩm.
- Kiểm soát nhanh dòng thông tin từ các khâu của chuỗi cung ứng, quản lý thông tin sản xuất nội bộ, phòng chống và phát hiện hàng giả, hàng nhái.
- Tăng sự tin tưởng của người tiêu dùng: các thông tin về nguồn gốc sản phẩm, quá trình hình thành sản phẩm đều được minh bạch với người tiêu dùng, giúp họ tin tưởng hơn về sản phẩm.
- Là phương tiện để kết nối trực tiếp với người tiêu dùng cuối cùng, thông qua đó quảng bá sản phẩm, xây dựng thương hiệu doanh nghiệp.

Thách thức

- Chi phí để xây dựng, duy trì hệ thống truy xuất nguồn gốc đánh trực tiếp vào chi phí sản xuất ra sản phẩm khiến giá thành sản phẩm bị đội lên cao.
- Quy trình thu thập dữ liệu và chuẩn hóa dữ liệu đòi hỏi hàm lượng công nghệ cao, đi kèm với chi phí lớn.
- Khả năng tiếp cận và ứng dụng công nghệ của các đơn vị trong chuỗi sản xuất chưa đáp ứng.

Chương 2

Bài toán truy xuất nguồn gốc thực phẩm

1 Nền tảng Hyperledger Fabric

1.1 Giới thiệu về Hyperledger Fabric

Hyperledger Fabric là một nền tảng cho các giải pháp sổ cái phân tán được xây dựng dựa trên kiến trúc mô-đun mang lại độ bảo mật cao, khả năng phục hồi, tính linh hoạt để tùy biến và khả năng mở rộng dễ dàng.

Fabric hỗ trợ các giao thức đồng thuận kết hợp, giúp cho hệ thống vẫn đạt được sự đồng thuận một cách chính xác cho dù các thành phần khác có thể bị lỗi [3].

Tính mô-đun Fabric được xây dựng gồm các mô-đun sau:

- Một dịch vụ cung cấp thành viên (Membership Service Provider): liên kết các thực thể trong mạng, có khả năng tích hợp.
- Dịch vụ đặt hàng (Ordering Service) cho phép tích hợp giao thức đồng thuận về thứ tự giao dịch và quảng bá cho các khối ngang hàng.
- Một dịch vụ nhắn tin ngang hàng.

- Sổ cái hỗ trợ nhiều hệ quản trị cơ sở dữ liệu.
- Hợp đồng thông minh chạy trong môi trường Docker.
- Một plugin có thể liên kết các chính sách xác thực.

Hợp đồng thông minh Hợp đồng thông minh trong Fabric được gọi là chaincode [3], có những đặc điểm chính là:

- Nhiều hợp đồng thông minh chạy đồng thời trong mạng.
- Có thể triển khai linh hoạt.

Fabric xây dựng một kiến trúc mới cho các giao dịch là: Thực thi - Đặt lệnh - Xác thực, trong đó:

- Thực thi một giao dịch và kiểm tra tính chính xác của nó, xác nhận nó.
- Đặt lệnh qua giao thức đồng thuận.
- Xác thực giao dịch dựa trên xác nhận ứng dụng cụ thể trước khi chốt với sổ cái.

1.2 Thuật toán đồng thuận trong Hyperledger Fabric

Trong Hyperledger Fabric, sự đồng thuận được tạo thành từ ba bước riêng biệt: chứng thực giao dịch, đặt hàng và xác nhận.

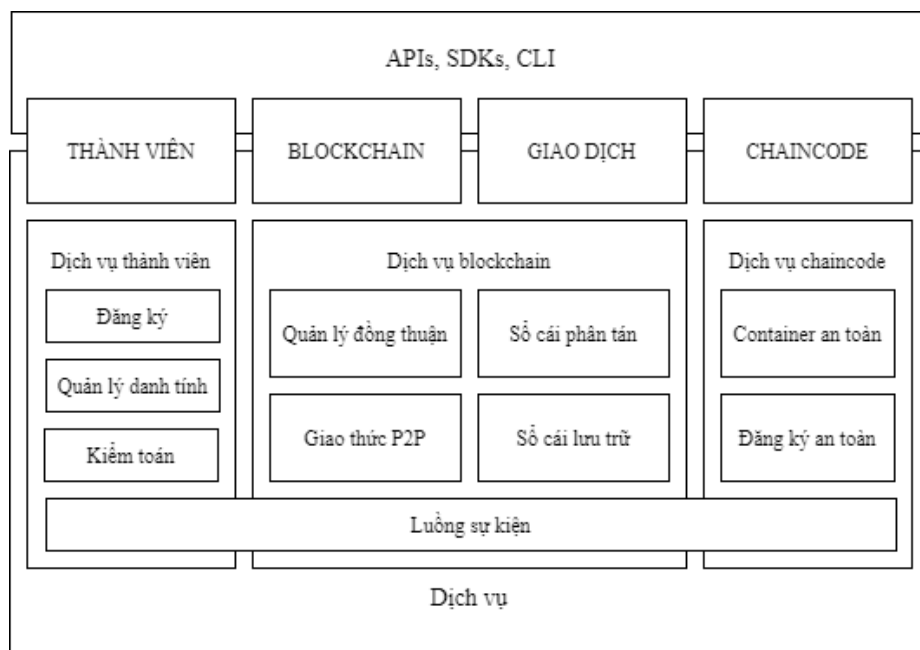
Hyperledger Fabric hoạt động ở chế độ Permissioned Blockchain (được cấp phép) với cơ chế kiểm soát truy cập và đồng thuận linh hoạt, giúp cải thiện hiệu năng và độ mở rộng của ứng dụng. Cơ chế đồng thuận của Fabric phủ khắp và bao gồm toàn bộ quá trình giao dịch. Thay vì là như nhau trong quá trình đồng thuận, các nút được phân bổ nhiệm vụ và vai trò khác nhau: khách (client), người đặt hàng (orderer) hay thành viên (peer) [3].

- Client là người dùng cuối, có quyền tạo và hủy giao dịch, giao tiếp với người đặt hàng và thành viên.

- Peer duy trì sổ cái của blockchain, nhận tín hiệu từ người đặt hàng, đưa giao dịch mới vào sổ cái. Người xác nhận là thành viên đặc biệt có khả năng xác nhận giao dịch bằng cách kiểm tra điều kiện, trạng thái, tính hợp lệ của giao dịch.
- Người đặt hàng cung cấp kênh giao tiếp giữa khách và thành viên, nó đảm bảo các tín hiệu giao dịch được phủ trên kênh giao tiếp.

Khách hàng gửi giao dịch tới những người xác nhận để khởi tạo quá trình thêm dữ liệu vào sổ cái. Giao dịch được đề xuất phải được sự đồng ý của những người xác nhận. Tiếp theo giao dịch được gửi đến những người đặt hàng, và chúng cần được đồng thuận. Sau đó, giao dịch này được chuyển tới đến các thành viên nắm giữ sổ cái để bắt đầu giao dịch.

1.3 Mô hình Hyperledger Fabric



Hình 1.1: Kiến trúc Hyperledger Fabric [9].

Thành viên Cung cấp các dịch vụ quản lý danh tính, quyền riêng tư, bảo mật và kiểm toán trên mạng.

Chaincode Chaincode được sử dụng trong Hyperledger là Golang. Có thể hiểu chaincode là một decentralized application (ứng dụng phân quyền), chạy trên các nút xác nhận hợp lệ và được đóng gói trong docker.

Dịch vụ blockchain Các dịch vụ Blockchain bao gồm ba thành phần chính: giao thức peer-to-peer (P2P), sổ cái phân tán và trình quản lý đồng thuận.

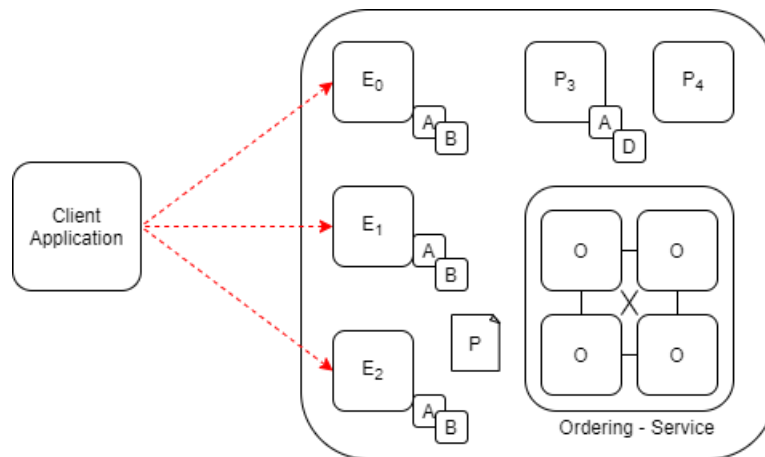
Giao dịch Các giao dịch được thực hiện và lưu trữ trên blockchain.

1.4 Luồng giao dịch

Các thành phần của luồng giao dịch bao gồm:

- Ứng dụng Client: các ứng dụng sử dụng SDK hoặc dịch vụ Web service Restfull để tương tác với mạng Hyperledger Fabric.
- E_0, E_1, E_2 : Người xác thực giao dịch (Endorser peer).
- P_3, P_4 : Người xác minh và xác nhận kết quả giao dịch (Committing peer).
- A, B, D : Hợp đồng thông minh (Chaincode).
- P : Chính sách chứng thực.
- **Sổ cái (Ledger)**.
- **World-state**: cơ sở dữ liệu chứa các giá trị hiện tại của một tập hợp các trạng thái sổ cái. Các trạng thái sổ cái mặc định được biểu thị dưới dạng cặp khóa-giá trị.

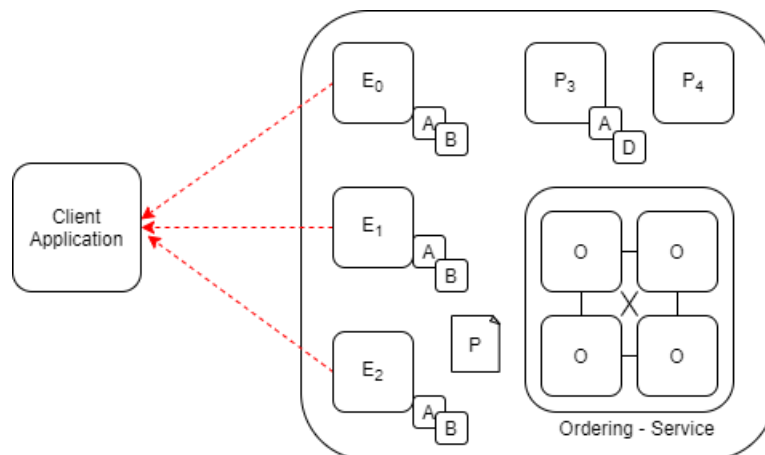
Bước 1: Yêu cầu giao dịch Ứng dụng Client sẽ gửi đi đề nghị giao dịch với hợp đồng thông minh A tới các thành phần chứng thực giao dịch E_0, E_1, E_2 .



Hình 1.2: Yêu cầu giao dịch [9].

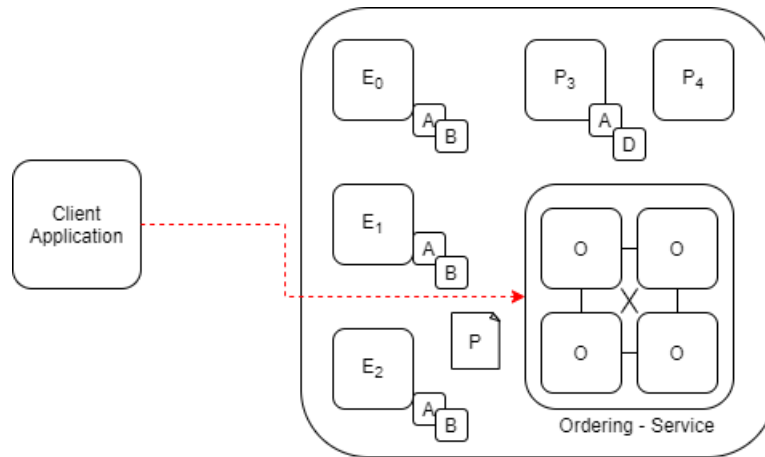
Bước 2: Thực hiện yêu cầu E0, E1, E2 sẽ thực hiện các đề nghị giao dịch bằng cách kiểm tra các chứng chỉ để xác thực giao dịch. Với mỗi một lệnh được thực hiện thì sẽ ghi lại trạng thái đọc và ghi của dữ liệu, gọi là tập ReadWrite (RW). Công đoạn này sẽ thực hiện Chaincode để trả về các phản hồi cho ứng dụng Client.

Bước 3: Phản hồi yêu cầu Tập RW được xác thực bởi các người xác thực sẽ được thực hiện đồng bộ trở lại với ứng dụng.



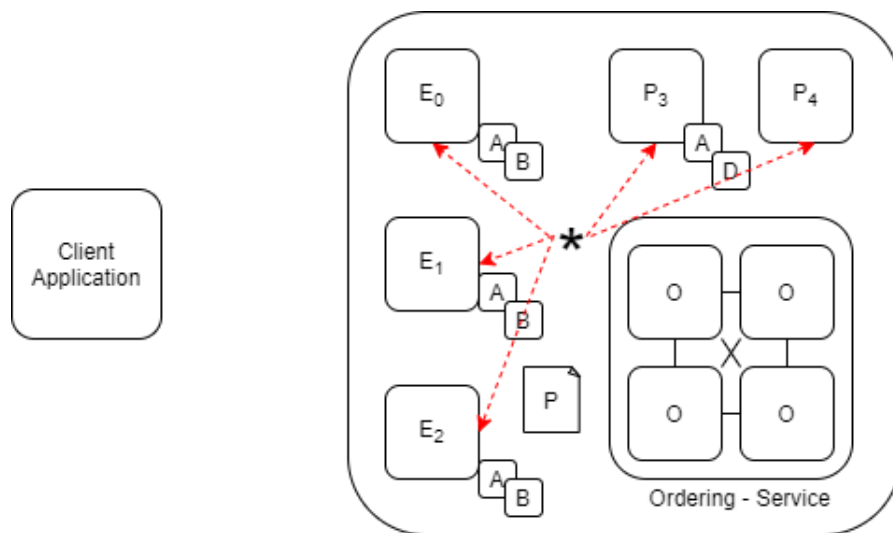
Hình 1.3: Phản hồi yêu cầu [9].

Bước 4: Giao dịch đặt hàng Ứng dụng Client tiếp tục gửi đi kết quả đã được phê duyệt như một giao dịch tối dịch vụ đặt hàng Ordering-Service.



Hình 1.4: Giao dịch đặt hàng [9].

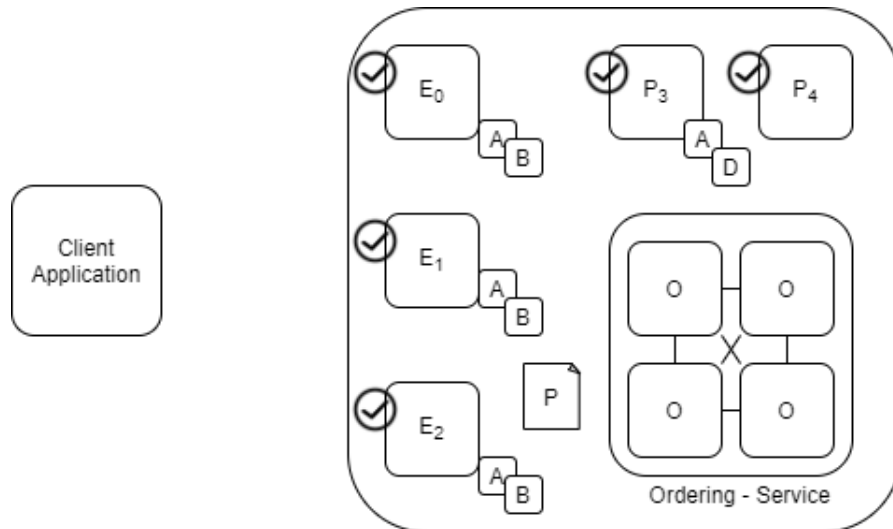
Bước 5: Chuyển giao dịch Dịch vụ đặt hàng Ordering-Service sẽ tập hợp các giao dịch trong một khối kết quả và gửi cho các nút trong mạng.



Hình 1.5: Chuyển giao dịch [9].

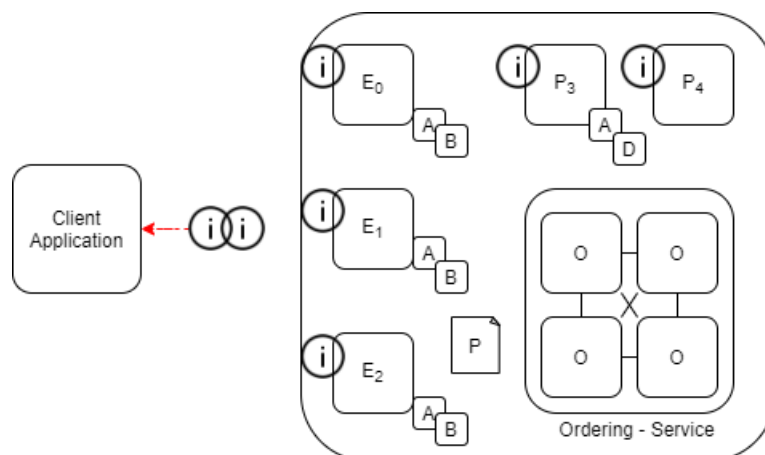
Bước 6: Xác nhận giao dịch Mọi người xác minh (Committing peer) sẽ xác nhận lại các chính sách xác thực một lần nữa. Đồng thời nó kiểm tra hiệu lực của tập RW. Việc

xác nhận giao dịch sẽ được lưu vào World-state, còn sổ cái sẽ lưu lại các giao dịch. Khi này, sổ cái được đồng bộ hóa.



Hình 1.6: Chuyển giao dịch [9].

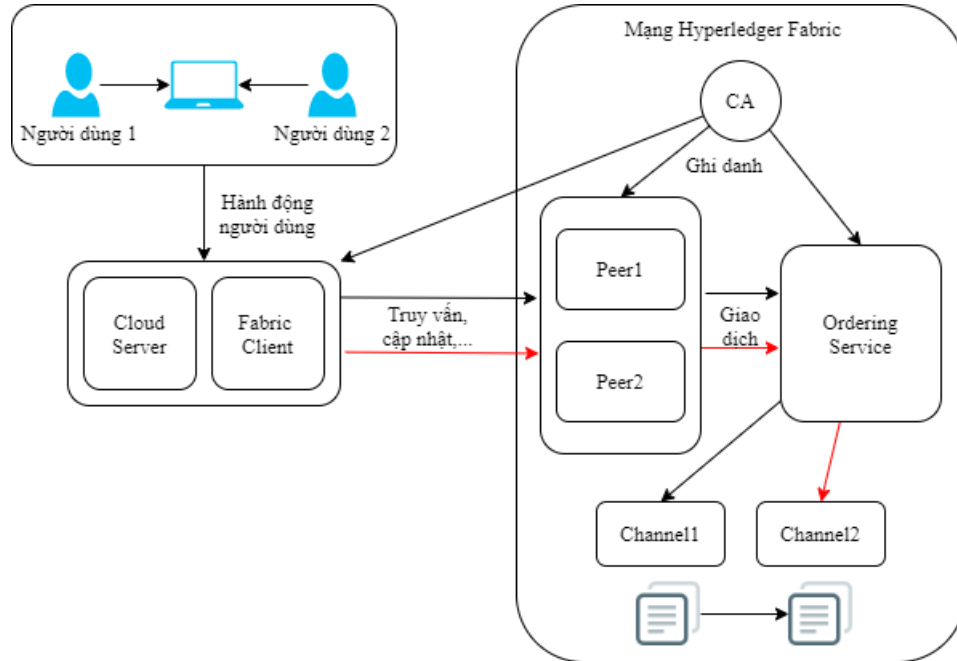
Bước 7: Thông báo Người xác minh sẽ thông báo lại cho ứng dụng rằng giao dịch có thành công hay không. Ứng dụng sẽ được thông báo bởi các nút mà nó kết nối tới.



Hình 1.7: Chuyển giao dịch [9].

1.5 Hệ thống mạng Hyperledger Fabric

Mạng Blockchain là một cơ sở hạ tầng kỹ thuật cung cấp sổ cái và hợp đồng thông minh cho các ứng dụng. Các hợp đồng thông minh được sử dụng để tạo ra các giao dịch sau đó phân phối cho các nút ngang hàng trong mạng.



Hình 1.8: Hệ thống mạng Hyperledger Fabric.

Ở mô hình biểu diễn ở Hình 1.8, Fabric CA là Fabric Certificate Authority cung cấp tính xác thực cho các người tham gia trong mạng Hyperledger. Bất kỳ người tham gia nào muốn tham gia mạng blockchain phải được đăng ký với CA trước. Quá trình này gọi là tuyển thành viên. Các Peer là các nút mạng, lưu trữ bản copy của blockchain và thực hiện quá trình đồng thuận. Dịch vụ đặt hàng Ordering Service kiểm tra quyền của client, xác thực các giao dịch đến từ client.

2 Thực nghiệm xây dựng hệ thống

2.1 Phân tích và thiết kế hệ thống

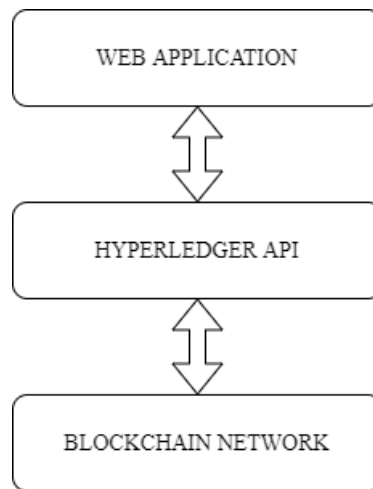
2.1.1 Các tác nhân tham gia vào hệ thống

Bảng 2.1: Các tác nhân tham gia vào hệ thống

Tác nhân		Vai trò/Quyền hạn	Mục đích
Khách hàng		<ul style="list-style-type: none">Đưa yêu cầu về những vấn đề liên quan tới sản phẩm. Quản lý hệ thống sẽ tiếp nhận yêu cầu và giải quyết.Tra cứu thông tin về sản phẩm bao gồm cả lịch sử của sản phẩm khi trải qua các công đoạn.	Thông tin chi tiết về sản phẩm.
Quản lý	Bộ phận ghi thông tin	<ul style="list-style-type: none">Thêm/sửa thông tin sản phẩm.Có quyền thao tác với dữ liệu sản phẩm trong phạm vi sản phẩm đang quản lý.	Ghi nhận thông tin sản phẩm.
	Bộ phận kiểm tra	Kiểm tra các thông tin theo yêu cầu khách hàng.	Thực hiện kiểm tra các thông tin của sản phẩm.

2.1.2 Sơ đồ tổng quan về hệ thống

Hệ thống blockchain trong báo cáo được xây dựng dựa trên 3 phần cơ bản như Hình 2.1:



Hình 2.1: Sơ đồ tổng quát của hệ thống blockchain

Application: Tầng này là giao diện chính để các tác nhân tham gia vào hệ thống tương tác với chương trình. Nó cung cấp các tính năng của phần mềm để người dùng thao tác.

Hyperledger API: Cung cấp các hàm API được tạo ra bởi mạng blockchain. Các API được thiết kế theo chuẩn Restful API gồm các phương thức *get*, *put*, *post*, *delete* các đối tượng tài nguyên trong mạng. Đồng thời nó cũng cung cấp hàm xử lý giao dịch trong mạng.

Blockchain network: Tầng này định nghĩa các đối tượng tham gia vào mạng, các tài nguyên để thao tác, quyền hạn với mỗi thành viên trong mạng và smartcontract.

2.1.3 Sơ đồ chi tiết hệ thống

Go Web (Client Application): cung cấp giao diện các chức năng cho người dùng tương tác

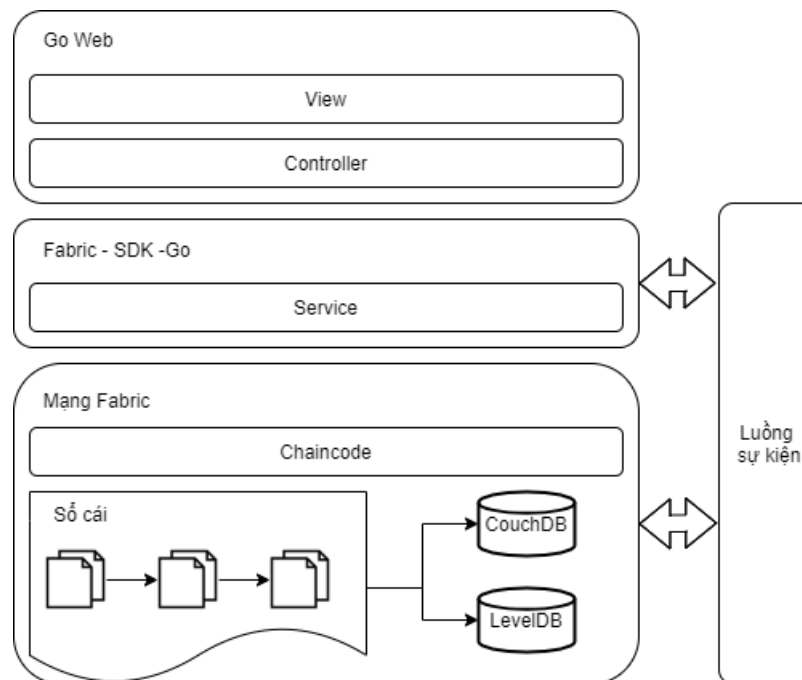
- Chức năng Đăng nhập: người quản lý sẽ dùng tài khoản được cung cấp vào chương trình. Quản lý có nhiệm vụ sử dụng các chức năng để thêm, sửa thông tin về sản phẩm.
- Chức năng Thêm thông tin sản phẩm.
- Chức năng Sửa thông tin sản phẩm.

- Chức năng Tra cứu thông tin khách hàng: cho phép người dùng hoặc quản lý truy cập thông tin sản phẩm để tra cứu.

Fabric-SDK-Go: cung cấp các hàm tương tác với mạng Hyperledger Fabric

- Thêm, sửa thông tin sản phẩm.
- Tra cứu thông tin sản phẩm.

Hyperledger Fabric: mạng blockchain lưu trữ thông tin các đối tượng và tài nguyên.



Hình 2.2: Kiến trúc hệ thống mạng blockchain

2.1.4 Thiết kế cơ sở dữ liệu

Cơ sở dữ liệu của sản phẩm được thiết kế như Bảng 2.2:

Bảng 2.2: Thiết kế cơ sở dữ liệu (Commodity) của sản phẩm.

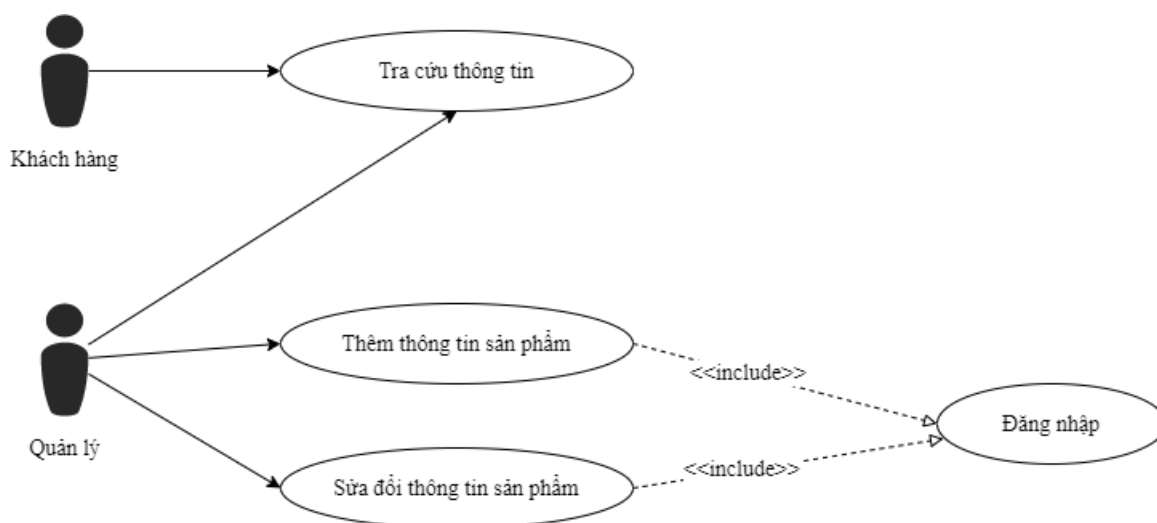
Tên	Kiểu dữ liệu	Mô tả
ObjectType	string	
Type	string	Loại sản phẩm
Primarykey	string	Mã sản phẩm
Name	string	Tên
Des	string	Mô tả
Specification	string	Khối lượng
Source	string	Nguồn gốc
Machining	string	Phương pháp xử lý
Remarks	string	Ghi chú
Principal	string	Chủ sở hữu
PhoneNumber	string	Số điện thoại
Photo	string	Ảnh
ShelfLife	string	Hạn sử dụng
StorageMethod	string	Phương pháp bảo quản
Brand	string	Nhãn hiệu
Vendor	string	Nhà phân phối
PlaceOfProduction	string	Nơi sản xuất
ExecutiveStandard	string	Tiêu chuẩn chất lượng
Historys	[]HistoryItem	Lịch sử chi tiết của sản phẩm
Time	string	Thời gian

Trong Bảng 2.2, thuộc tính Historys được thiết kế là một danh sách lưu trữ lịch sử chi tiết thông tin sản phẩm. Mỗi một bản ghi trong Historys sẽ bao gồm: số giao dịch TxId và thuộc tính Commodity (định nghĩa trong Bảng 2.2) giúp lưu trữ chi tiết thông tin sản phẩm (xem Bảng 2.3).

Bảng 2.3: Thiết kế cơ sở dữ liệu (HistoryItem) của sản phẩm.

Tên	Kiểu dữ liệu	Mô tả
TxId	string	Số giao dịch
Commodity	Commodity	Chi tiết về lịch sử

2.1.5 Biểu đồ use-case tổng quát



Hình 2.3: Biểu đồ use-case tổng quát.

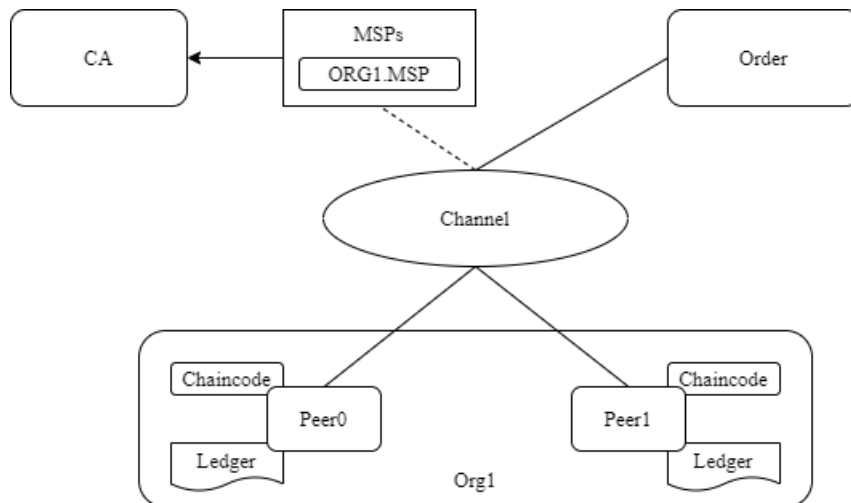
Bảng 2.4 mô tả chi tiết các use-case:

Bảng 2.4: Bảng mô tả chi tiết các use-case.

Tên usecase	Tác nhân	Đầu vào (Input)	Đầu ra (Output)
Tra cứu thông tin	Khách hàng, Quản lý	Mã sản phẩm cần tìm	Thông tin chi tiết về sản phẩm
Đăng nhập	Quản lý	Tên tài khoản và mật khẩu	Thông tin đăng nhập
Thêm thông tin sản phẩm	Quản lý	Toàn bộ thông tin về sản phẩm cần nhập	Sản phẩm được lưu thành bản ghi trong blockchain
Sửa đổi thông tin sản phẩm	Quản lý	Sản phẩm cần sửa đổi	Sản phẩm sau khi sửa được lưu thành bản ghi mới (có dấu thời gian)

2.2 Xây dựng mạng Hyperledger Fabric

Do quy mô đề tài ở mức cá nhân, nên cấu trúc của mạng bao gồm: 1 tổ chức (organization) chứa 2 nút (peer); 1 order và 1 kênh (channel) (như Hình 2.4).



Hình 2.4: Cấu trúc mạng Hyperledger Fabric.

Quá trình thiết lập mô hình mạng và kết quả chạy thực tế được biểu diễn như Hình 2.5 dưới đây:

<pre>channels: # name of the channel kevinkongyixueyuan: peers: peer0.org1.kevin.kongyixueyuan.com: endorsingPeer: true ledgerQuery: true eventSource: true peer1.org1.kevin.kongyixueyuan.com: endorsingPeer: true chaincodeQuery: true ledgerQuery: true eventSource: true policies: queryChannelConfig: minResponses: 1 #[Optional] channel config will be retrieved for these number of r maxTargets: 1 #[Optional] retry options for query config block retryOpts: #[Optional] number of retry attempts attempts: 5 #[Optional] the back off interval for the first retry attempt initialBackoff: 500ms #[Optional] the maximum back off interval for any retry attempt</pre>	<pre>Build ... # @dep ensure Build done Start environment ... Creating network "fixtures_default" with the default driver Creating orderer.kevin.kongyixueyuan.com ... Creating couchdb ... Creating ca.org1.kevin.kongyixueyuan.com ... Creating orderer.kevin.kongyixueyuan.com ... Creating couchdb ... Creating couchdb ... done Creating peer0.org1.kevin.kongyixueyuan.com ... Creating peer0.org1.kevin.kongyixueyuan.com ... Creating peer1.org1.kevin.kongyixueyuan.com ... Creating peer0.org1.kevin.kongyixueyuan.com ... done Environment up Start app ... Fabric SDK was successfully launched! Channel has been successfully created!, peers have successfully joined the channel. Start to install the chain code..... The specified chain code is installed successfully! Start instantiating chaincode.....</pre>
--	--

(a) Thiết lập mô hình mạng.

(b) Kết quả chạy thực tế.

Hình 2.5: Quá trình thiết lập mô hình mạng và kết quả chạy thực tế.

2.3 Xây dựng chức năng và giao diện hệ thống

2.3.1 Trang chủ và menu các chức năng

Giao diện trang chủ gồm phần mô tả thông tin ứng dụng và menu các chức năng thao tác trong chương trình. Menu gồm các chức năng:

- Trang chủ: màn hình chính.
- Đăng nhập.
- Tra cứu thông tin bằng mã sản phẩm.
- Tra cứu thông tin bằng tên sản phẩm.

HỆ THỐNG TRUY XUẤT NGUỒN GỐC THỰC PHẨM - No. block: 5	
<div><h3>Tiêu chí truy xuất</h3><p>Các tiêu chí truy xuất nguồn gốc sản phẩm</p><div><p>Yêu cầu</p><p>Thành phần</p><p>Nhà cung cấp</p><p>Hình ảnh</p></div><div>Xác minh trực tuyến Truy xuất nguồn gốc</div></div>	<div><h3>Truy xuất nguồn gốc</h3><p>Xác minh trực tuyến dựa trên tên sản phẩm hoặc mã sản phẩm để truy xuất nguồn gốc sản phẩm.</p><div><p>Truy xuất nguồn gốc theo:</p><p>1. Tên sản phẩm 2. Mã sản phẩm</p></div><div>Giới thiệu Đăng nhập</div></div>

Hình 2.6: Giao diện trang chủ hệ thống truy xuất nguồn gốc thực phẩm.

2.3.2 Chức năng đăng nhập

Chức năng đăng nhập dành cho đối tượng là quản lý. Quản lý trong hệ thống sử dụng các chức năng của chương trình để cập nhật thông tin về sản phẩm (thêm, sửa).

ĐĂNG NHẬP

Sử dụng tài khoản admin để đăng nhập

Hình 2.7: Giao diện chức năng đăng nhập.

Những sự kiện của chức năng đăng nhập được mô tả trong Bảng 2.5:


Bảng 2.5: Các sự kiện của chức năng đăng nhập.

Tên use-case	Đăng nhập
Tác nhân	Quản lý
Sự kiện chính	<ol style="list-style-type: none"> 1. Hiển thị giao diện đăng nhập. 2. Người dùng nhập tên đăng nhập và mật khẩu. 3. Kiểm tra và xác nhận thông tin đăng nhập. 4. Báo đăng nhập thành công. 5. Hiển thị giao diện chính của hệ thống.
Sự kiện ngoại lệ	<ol style="list-style-type: none"> 1. Thông báo thông tin đăng nhập sai. 2. Người dùng nhập lại tên đăng nhập và mật khẩu.

2.3.3 Chức năng thêm thông tin sản phẩm

Chức năng thêm thông tin sản phẩm bị giới hạn ở đối tượng quản lý, chỉ những đối tượng này mới có quyền thêm thông tin sản phẩm (xem Hình 2.8).

Thêm sản phẩm [Về trang chủ](#)

Loại sản phẩm:	<input type="text" value="Loại sản phẩm"/>	Ghi chú:	<input type="text" value="Ghi chú"/>	 Kích thước (120*160px)
Mã sản phẩm:	<input type="text" value="Mã sản phẩm"/>	Chủ sở hữu:	<input type="text" value="Chủ sở hữu"/>	
Tên sản phẩm:	<input type="text" value="Tên sản phẩm"/>	Điện thoại:	<input type="text" value="Điện thoại"/>	
Nhãn hiệu:	<input type="text" value="Nhãn hiệu"/>	Hạn sử dụng:	<input type="text" value="Hạn sử dụng"/>	
Mô tả:	<input type="text" value="Mô tả"/>	Bảo quản:	<input type="text" value="Bảo quản"/>	
Thông số:	<input type="text" value="Thông số"/>	Nhà sản xuất:	<input type="text" value="Nhà sản xuất"/>	
Nguồn:	<input type="text" value="Nguồn"/>	Nơi sản xuất:	<input type="text" value="Nơi sản xuất"/>	
Xử lý:	<input type="text" value="Phương pháp xử lý"/>	Tiêu chuẩn:	<input type="text" value="Tiêu chuẩn"/>	

Hình 2.8: Giao diện thêm thông tin sản phẩm.

Một số thuộc tính của sản phẩm được đưa ra như Hình 2.8, chẳng hạn:

- | | | | |
|-----------------|------------|---------------|----------------|
| • Loại sản phẩm | • Mô tả | • Ghi chú | • Bảo quản |
| • Mã sản phẩm | • Thông số | • Chủ sở hữu | • Nhà sản xuất |
| • Tên sản phẩm | • Nguồn | • Điện thoại | • Nơi sản xuất |
| • Nhãn hiệu | • Xử lý | • Hạn sử dụng | • Tiêu chuẩn |

trong đó, lưu ý một số thuộc tính như: mô tả (thông tin về chất lượng, nguyên liệu và hình thức sản xuất sản phẩm), thông số (khối lượng, thể tích), xử lý (phương pháp xử lý, chế biến), ghi chú (quá trình vận chuyển,...), bảo quản (phương pháp lưu trữ, thời gian,...), tiêu chuẩn (tiêu chuẩn chất lượng sản phẩm thỏa mãn).

Ngoài ra, chức năng thêm sản phẩm bao gồm cả thuộc tính hình ảnh (góc trên bên phải Hình 2.8). Dữ liệu đầu vào của thuộc tính là hình ảnh có kích thước lớn hơn hoặc bằng $120 \times 160px$ (định dạng jpg, jpeg, png).

Các sự kiện của chức năng thêm thông tin sản phẩm được mô tả như Bảng 2.6:

Bảng 2.6: Các sự kiện của chức năng thêm thông tin sản phẩm.

Tên use-case	Thêm thông tin sản phẩm
Tác nhân	Quản lý
Sự kiện chính	<ol style="list-style-type: none"> 1. Hiển thị giao diện điền thông tin sản phẩm. 2. Người dùng nhập toàn bộ dữ liệu đầu vào của sản phẩm. 3. Kiểm tra và xác nhận thông tin đầu vào. 4. Trả về kết quả sau khi thêm sản phẩm vào bản ghi trong blockchain.
Sự kiện ngoại lệ	<ol style="list-style-type: none"> 1. Báo lỗi khi mã sản phẩm nhập vào bị trùng. 2. Nhập sai định dạng dữ liệu. 3. Hình ảnh tải lên không đúng định dạng hoặc kích thước. 4. Người dùng nhập lại dữ liệu đầu vào.

2.3.4 Chức năng sửa thông tin sản phẩm

Chức năng sửa thông tin sản phẩm cũng bị giới hạn ở đối tượng quản lý, chỉ những đối tượng này mới có quyền sửa thông tin sản phẩm.

Thông tin của sản phẩm trước khi sửa không bị mất đi, thay vào đó, thông tin sau khi sửa đổi sẽ được lưu dưới dạng một bản ghi mới, sử dụng dấu thời gian (Timestamp) để phân biệt với thông tin cũ của sản phẩm.

Bảng 2.7 mô tả những sự kiện của chức năng sửa thông tin sản phẩm:


Bảng 2.7: Các sự kiện của chức năng sửa thông tin sản phẩm.

Tên use-case	Sửa thông tin sản phẩm
Tác nhân	Quản lý
Sự kiện chính	<ol style="list-style-type: none"> 1. Hiển thị giao diện sửa thông tin sản phẩm. 2. Người dùng chọn những thuộc tính cần thay đổi và nhập dữ liệu thay thế. 3. Kiểm tra và xác nhận thông tin đầu vào. 4. Trả về kết quả sau khi sửa thông tin sản phẩm dưới dạng bản ghi trong blockchain.
Sự kiện ngoại lệ	<ol style="list-style-type: none"> 1. Báo lỗi khi mã sản phẩm nhập vào bị trùng. 2. Dữ liệu đầu vào không đúng định dạng. 3. Hình ảnh tải lên không đúng định dạng hoặc kích thước. 4. Người dùng nhập lại dữ liệu đầu vào.

Cập nhật thông tin truy xuất nguồn gốc sản phẩm

[Thêm mới](#)
[Về trang chủ](#)

Loại sản phẩm:	Gạo	Ghi chú:	Không
Mã sản phẩm:	002	Chủ sở hữu:	Quốc Đạt
Tên sản phẩm:	Gạo tám Thái	Điện thoại:	123456789
Nhãn hiệu:	Quốc Đạt	Hạn sử dụng:	1 năm
Mô tả:	Trồng trên ruộng	Bảo quản:	Nơi khô ráo, nhiệt độ bình thường
Thông số:	1kg	Nhà sản xuất:	Nhà máy ở Nam Định
Nguồn:	Nam Định	Nơi sản xuất:	Việt Nam
Xử lý:	Thu hoạch bằng máy gặt	Tiêu chuẩn:	TCVN 11888:2017



Kích thước (120*160px)

Cập nhật

Hình 2.9: Giao diện sửa đổi thông tin sản phẩm.

2.3.5 Chức năng tra cứu thông tin sản phẩm

Có hai hình thức để tra cứu thông tin sản phẩm, bao gồm:

- Tra cứu thông tin bằng mã sản phẩm.
- Tra cứu thông tin bằng tên sản phẩm..

Truy xuất thông tin sản phẩm

Mã truy xuất:

Mã truy xuất

Xác nhận

[Truy xuất theo tên](#)
[Quay lại trang chủ](#)

Lưu ý

1. Nhấn để xem phạm vi truy xuất.
2. Không được đăng tải lại kết quả truy xuất.
3. Điện thoại: (+84) 705443301
Email: nguyencongthinh1999@gmail.com

Hình 2.10: Truy xuất thông tin bằng mã sản phẩm.

Truy xuất thông tin sản phẩm

Chứng nhận:

Tên sản phẩm:

Xác nhận

[Truy xuất theo mã](#) [Quay lại trang chủ](#)

Lưu ý

- Nhấn để xem phạm vi truy xuất.
- Không được đăng tải lại kết quả truy xuất.
- Điện thoại: (+84) 705443301
Email: nguyencongthinh1999@gmail.com

Hình 2.11: Truy xuất thông tin bằng tên sản phẩm.

Những sự kiện của chức năng tra cứu thông tin được mô tả trong Bảng 2.8:

Bảng 2.8: Các sự kiện của chức năng tra cứu thông tin.

Tên use-case	Tra cứu thông tin
Tác nhân	Khách hàng, Quản lý
Sự kiện chính	<ol style="list-style-type: none">Hiển thị giao diện tra cứu.Người dùng chọn phương thức tra cứu: mã sản phẩm hoặc tên sản phẩm.Nhập vào dữ liệu đầu vào (mã sản phẩm/tên sản phẩm) để tra cứu.Kiểm tra và xác nhận thông tin tra cứu.Hiển thị giao diện trả về kết quả truy xuất.
Sự kiện ngoại lệ	<ol style="list-style-type: none">Hiển thị trang trắng khi thông tin nhập vào không khớp.Người dùng nhập lại dữ liệu đầu vào.

3 Kiểm thử và đánh giá kết quả

3.1 Kiểm thử và đánh giá chức năng đăng nhập

Chức năng đăng nhập dành cho đối tượng quản lý. Kiểm thử chức năng đăng nhập nhằm đảm bảo nó hoạt động bình thường và đối tượng truy cập được vào hệ thống.

Điều kiện áp dụng: dành cho đối tượng quản lý đã được cấp tài khoản và mật khẩu.

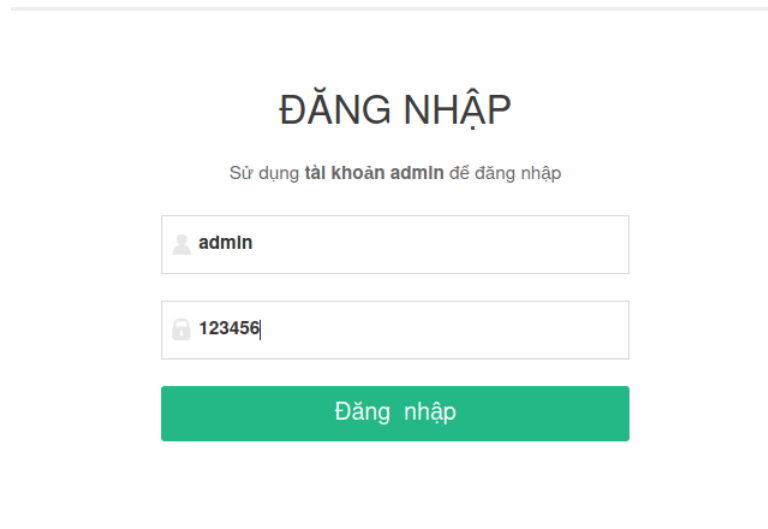
Các bước thực hiện:

Bước 1: Nhập đầy đủ thông tin đăng nhập trên giao diện gồm: tên đăng nhập, mật khẩu.

Bước 2: Nhấn “Đăng nhập”.

Kết quả mong đợi: truy cập bình thường vào hệ thống.

Kết quả thực tế: đăng nhập thành công.



The screenshot displays a login form with the following elements:

- Title:** ĐĂNG NHẬP
- Subtitle:** Sử dụng tài khoản admin để đăng nhập
- Username Field:** Contains the text 'admin'.
- Password Field:** Contains the text '123456'.
- Login Button:** A green button labeled 'Đăng nhập'.

Hình 3.1: Thao tác đăng nhập hệ thống.

3.2 Kiểm thử và đánh giá chức năng thêm thông tin sản phẩm

Kiểm thử chức năng thêm thông tin sản phẩm nhằm đảm bảo thông tin khi nhập vào được lưu vào blockchain.

Điều kiện áp dụng: đã đăng nhập thành công vào hệ thống và đã vào chức năng thêm thông tin sản phẩm.

Các bước thực hiện:

Bước 1: Nhập đầy đủ thông tin sản phẩm trên giao diện gồm: loại sản phẩm, mã sản phẩm, tên sản phẩm,...

Loại sản phẩm	Gạo	Ghi chú	Không
Mã sản phẩm	005	Chủ sở hữu	Việt Hương
Tên sản phẩm	Gạo lứt	Điện thoại	12345678
Nhãn hiệu	Việt Hương	Hạn sử dụng	1 năm
Mô tả	Trồng trên ruộng	Bảo quản	Nơi khô ráo, nhiệt độ bình thường
Thông số	1kg	Nhà sản xuất	Nhà máy Thái Bình
Nguồn	Thái Bình	Nơi sản xuất	Việt Nam
Xử lý	Thu hoạch bằng máy gặt	Tiêu chuẩn	TCVN 11888:2017

Bảng 3.1: Mẫu nhập liệu thông tin sản phẩm

Bước 2: Nhấn “Thêm”.

Thêm sản phẩm

[Về trang chủ](#)

Loại sản phẩm:

Ghi chú:

Mã sản phẩm:

Chủ sở hữu:

Tên sản phẩm:

Điện thoại:

Nhãn hiệu:

Hạn sử dụng:

Mô tả:

Bảo quản:

Thông số:


Nhà sản xuất:

Nguồn:

Nơi sản xuất:

Xử lý:

Tiêu chuẩn:



Kích thước (120*160px)

Thêm

Hình 3.2: Thao tác thêm sản phẩm vào mạng.

Kết quả mong đợi: thông tin sản phẩm được ghi vào blockchain.

Kết quả thực tế: thông tin được ghi vào blockchain và có thể truy cập thông qua API.

```
{
  Type: "Gạo",
  Primarykey: "005",
  Name: "Gạo lứt",
  Des: "Trồng trên ruộng",
  Specification: "1kg",
  Source: "Thái Bình",
  Machining: "Thu hoạch bằng máy gặt",
  Remarks: "Không",
  Principal: "Việt Hương",
  PhoneNumber: "123456789",
  Photo: "/static/photo/gaolut.jpg",
  ShelfLife: "1 năm",
  StorageMethod: "Nơi khô ráo, nhiệt độ bình thường",
  Brand: "Việt Hương",
  Vendor: "Nhà máy Thái Bình",
  PlaceOfProduction: "Việt Nam",
  ExecutiveStandard: "TCVN 11888:2017",
  Time: "2020-12-31 20:46:05"
}
```

Hình 3.3: Kết quả thực tế khi ghi nhận thông tin sản phẩm truy vấn qua API.

3.3 Kiểm thử và đánh giá chức năng sửa thông tin sản phẩm

Kiểm thử chức năng sửa thông tin sản phẩm nhằm đảm bảo thông tin sản phẩm sau khi sửa được lưu vào blockchain.

Điều kiện áp dụng: đã đăng nhập thành công vào hệ thống và đã vào chức năng sửa thông tin sản phẩm.

Các bước thực hiện:

Bước 1: Sửa dữ liệu các thuộc tính : loại sản phẩm, mã sản phẩm, tên sản phẩm,...

Bước 2: Nhấn “Sửa”.

Kết quả mong đợi: thông tin sản phẩm sau khi sửa được ghi vào blockchain.


Kết quả thực tế: thông tin sau khi sửa được ghi vào blockchain và có thể truy cập thông qua API.

Cập nhật thông tin truy xuất nguồn gốc sản phẩm

[Thêm mới](#) [Về trang chủ](#)

Loại sản phẩm:	Gạo	Ghi chú:	Đã sửa đổi
Mã sản phẩm:	005	Chủ sở hữu:	Việt Hương
Tên sản phẩm:	Gạo lứt	Điện thoại:	12345678
Nhãn hiệu:	Việt Hương	Hạn sử dụng:	1 năm
Mô tả:	Trồng trên ruộng	Bảo quản:	Nơi khô ráo, thoáng mát
Thông số:	1kg	Nhà sản xuất:	Nhà máy Thái Bình
Nguồn:	Thái Bình	Nơi sản xuất:	Thái Bình
Xử lý:	Thu hoạch bằng máy gặt	Tiêu chuẩn:	TCVN 11888:2017

Cập nhật



Kích thước (120*160px)

Hình 3.4: Thao tác sửa thông tin sản phẩm trên mạng.

Kết luận kiểm thử: các chức năng trong chương trình đã hoạt động đúng theo kịch bản đề ra, thông tin sản phẩm ghi nhận được vào blockchain và để khai thác dữ liệu các ứng dụng bên ngoài có thể sử dụng API được cung cấp để truy vấn.

Kết luận

Những kết quả đạt được của báo cáo

Đưa ra được bài toán thực tế và ứng dụng được những ưu điểm của công nghệ blockchain mang lại và áp dụng cho bài toán truy xuất nguồn gốc. Đồng thời nghiên cứu và áp dụng nền tảng Hyperledger Fabric để xây dựng mạng blockchain phục vụ công tác tra cứu thông tin sản phẩm của người tiêu dùng và công tác thêm, sửa thông tin sản phẩm của quản lý. Báo cáo đã thực hiện cài đặt mạng blockchain và triển khai ứng dụng web để cho quản lý cũng như khách hàng sử dụng.

Phần mềm đưa công nghệ blockchain vào giúp tăng cường tính công khai, minh bạch của dữ liệu chỉ số, giúp khách hàng có thể tra cứu và tin tưởng vào thông tin sản phẩm được cung cấp. Báo cáo đề mở khả năng phát triển trong tương lai, có thể giải quyết các bài toán khác trong truy xuất nguồn gốc ví dụ như: truy xuất nguồn gốc tới tận các nguyên liệu tạo thành giúp khách hàng có thể kiểm tra được xuất xứ và quá trình tạo ra sản phẩm từ nguyên liệu, v.v.

Hướng phát triển của báo cáo

Tiếp tục triển khai mở rộng, hoàn thiện các chức năng như thống kê, báo cáo, cảnh báo trường hợp sửa đổi thông tin sản phẩm bất thường. Hiệu chỉnh lại giao diện thân thiện, dễ sử dụng đối với người dùng.

Tiếp tục nghiên cứu mạng blockchain, cụ thể là Hyperledger để ứng dụng được nhiều tính năng của nền tảng này cung cấp như chia kênh, cài đặt các chứng chỉ cho các thành viên tham gia. Xây dựng ứng dụng di động để nhân viên dễ sử dụng và thao tác.

Chỉ mục

B

Bảng băm, 15
BFT, 19
Bitcoin, 18, 20
block, 16
Blockchain, 10, 30
Byzantine, 11

C

Chuỗi cung ứng, 10, 37
Client, 40
Cơ chế đồng thuận, 31
Committing peer, 44
Consortium Blockchain, 26
Cryptoeconomics, 19

D

DPoS, 22

E

Endorser peer, 42
Ethereum, 20

F

Fabric Certificate Authority, 46

G

Giá trị băm, 15

H

Hàm băm, 15
Hàm băm mật mã, 16
Hợp đồng thông minh, 11, 28
Hybrid Blockchain, 27
Hyperledger, 48

I

ISO, 33

L

Logistics, 10

M

Mã hóa, 29
Mã vạch, 37
Mạng ngang hàng phân tán, 14, 17
Membership Service Provider, 39

N

Ứng dụng phân quyền, 42
Nonce, 17
Nút, 12

O

Ordering Service, 39

P

P2P, 17

Peer, 41
PoA, 23
PoS, 21
PoW, 20
Private Blockchain, 25
Public Blockchain, 24

R

Resful API, 48

S

Sổ cái phân tán, 12
Satoshi Nakamoto, 10
SHA256, 16
Sharding, 22

T

Tiền điện tử, 13
Token hóa, 13
TPS, 24, 26
Truy xuất nguồn gốc, 33
Truy xuất nội bộ, 36
Truy xuất toàn cục, 36

U

Use-case, 51

W

World-state, 42

Tài liệu tham khảo

- [1] Abeyratne S.A., Monfared R.P., “Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger”, *International Journal of Research in Engineering and Technology*, Vol 05, 2016.
- [2] Alsunaidi S., Al-Haidari F., “A Survey of Consensus Algorithms for Blockchain Technology”, *2019 International Conference on Computer and Information Sciences (ICCIS)*, 2019, 1–6.
- [3] Androulaki E. , Barger A. , Bortnikov V. , Cachin C. , Christidis K. , Caro A. , Enyeart D. , Ferris C. , Laventman G. , Manevich Y. , Muralidharan S. , Murthy C. , Sethi M. , Singh G. , Smith K. , Sorniotti A. , Stathakopoulou C. , Vukolic M., Yellick J., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”, , 2018.
- [4] Aung M. M., Chang Y. S., “Traceability in a food supply chain: Safety and quality perspectives”, *Food Control*, Vol 39, 2014, 172–184.
- [5] Bartoletti M., Pompianu L., “An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns”, *In: Brenner M. et al. (eds) Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science*, Vol 10323, 2017, 494–509.
- [6] Bauspiess F., Damm F., “Requirements for cryptographic hash functions”, *Computers and Security*, Vol 11(5), 1992, 427–437.
- [7] Brown M., Peköz E., Ross S., “Blockchain double-spend attack duration”, *Probability in the Engineering and Informational Sciences*, 2020, 1–9.

- [8] Corallo A., Paiano R. , Guido A. L. ,Pandurino A., Latino M. E. , Menegoli M., “Intelligent monitoring Internet of Things based system for agri-food value chain traceability and transparency: A framework proposed”, *2018 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS)*, 2018, 1–6.
- [9] Feagan L., “Hyperledger Fabric Peer Design”, IBM China Research Lab, 2018.
- [10] Hughes L., Dwivedi Y.K., Misra.S.K, Rana N.P., Raghavan V., Akella V, “Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda”, *International Journal of Information Management*, Vol 49, 2019, 114–129.
- [11] ISO Technical Committee, “Traceability in the feed and food chain. General principles and basic requirements for system design and implementation, ISO 22005:2007”, ISO Technical Committee: Geneva,Switzerland.
- [12] Lamport L., Shostak R., Pease M., “The Byzantine Generals Problem”, *ACM Trans. Program. Lang. Syst.*, Vol 4(3), 1982, 382–401.
- [13] Li Z., Barenji A.V., Huang G.Q, “Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform”, *Robotics and Computer-Integrated Manufacturing*, Vol 54, 2018, 133–144.
- [14] Martino R., Cilaro A., “Designing a SHA-256 processor for blockchain-based IoT applications”, *Internet of Things*, Vol 11, 2020, 100254.
- [15] Nakamoto S., “A peer-to-peer electronic cash system”, In: Bitcoin, <https://nakamotoinstitute.org/bitcoin>.
- [16] Nasreen M.A., Ganesh A., Sunitha C., “A Study on Byzantine Fault Tolerance Methods in Distributed Networks”, *Procedia Computer Science*, Vol 87, 2016, 50–54.
- [17] Olnes S., Ubacht J., Janssen M., “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing”, *Government Information Quarterly*, Vol 34(3), 2017, 355–364.

- [18] Pappa I. C., Iliopoulos C., Massouras T., “What determines the acceptance and use of electronic traceability systems in agri-food supply chains?”, *Journal of Rural Studies*, Vol 58, 2018, 123–135.
- [19] Pierro M.D., “What Is the Blockchain?”, *Computing in Science Engineering*, Vol 19(5), 2017, 92–95.
- [20] Schuetz S., Venkatesh V, “Blockchain, adoption, and financial inclusion in India: Research opportunities”, *International Journal of Information Management*, Vol 52, 2020, 101936.
- [21] Sobti R., Ganesan G., “Cryptographic Hash Functions: A Review”, *International Journal of Computer Science Issues*, ISSN (Online): 1694-0814, Vol Vol 9, 2012, 461–479.
- [22] Ying W., Jia S., Du W., “Digital enablement of blockchain: Evidence from HNA group”, *International Journal of Information Management*, Vol 39, 2018, 1–4.
- [23] Yli-Huumo J., Ko D., Choi S., Park S., Smolander K., “Where Is Current Research on Blockchain Technology?—A Systematic Review”, *PLOS ONE*, Vol 11(10), 2016, 1–27.