

ỨNG DỤNG CÂY PATRICIA ĐỂ GIẢM THIỂU THỜI GIAN XỬ LÝ GIAO DỊCH TRONG HỆ THỐNG QUẢN LÝ CHUỖI CUNG ỨNG TRÁI CÂY

*Nguyễn Đức Tuấn**, *Nguyễn Xuân Dương†*

Ngày tòa soạn nhận được bài báo: 02/12/2022
Ngày nhận kết quả phản biện đánh giá: 02/06/2023
Ngày bài báo được duyệt đăng: 28/06/2023

DOI: 10.59266/houjs.2023.271

Tóm tắt: Công nghệ chuỗi khối (blockchain) hiện nay đang nhận được rất nhiều sự quan tâm và nghiên cứu của các nhà khoa học trên thế giới. Công nghệ này cũng đã được ứng dụng vào rất nhiều lĩnh vực khác nhau, từ kinh tế cho đến nông nghiệp, đặc biệt là ứng dụng trong các chuỗi cung ứng, cho phép người tiêu dùng có thể truy xuất nguồn gốc của các sản phẩm. Thông thường, số lượng các giao dịch trong các hệ thống quản lý các chuỗi cung ứng là rất lớn. Vì vậy, đã có nhiều giải pháp được đề xuất để giảm thiểu thời gian lưu trữ và xác thực các giao dịch. Trong bài báo này, nhóm tác giả đề xuất một giải pháp sử dụng cây Patricia để giảm thiểu thời gian lưu trữ và xác thực các giao dịch trong một hệ thống quản lý chuỗi cung ứng nông sản. Các kết quả thực nghiệm cho thấy, việc sử dụng cây Patricia giúp giảm thời gian cần thiết để xác thực các giao dịch.

Từ khóa: công nghệ chuỗi khối, cơ chế đồng thuận, chuỗi cung ứng hoa quả, hệ thống quản lý, cây patricia, kết nối điểm đến điểm, giao dịch.

I. Đặt vấn đề

Hiện nay, công nghệ chuỗi khối đang được sử dụng trong rất nhiều lĩnh vực của đời sống, chẳng hạn như tiền điện tử, chứng khoán và giao dịch tài chính, quản lý các chuỗi cung ứng, bảo hiểm, sức khỏe và y tế, bỏ phiếu điện tử, và nhiều lĩnh vực khác. Trong các hệ thống quản lý chuỗi cung ứng, chuỗi khối được ứng dụng để giúp cải thiện tính minh bạch và tin cậy, giúp người tiêu dùng có thể truy xuất được nguồn gốc của các sản phẩm.

Theo thực tiễn hoạt động, trong các hệ thống quản lý chuỗi cung ứng, số lượng các giao dịch giữa các thành viên trong hệ thống được tạo ra là rất lớn và các thông tin trong giao dịch này có thể bị giả mạo. Vì thế, đã có rất nhiều hệ thống quản lý chuỗi cung ứng sử dụng công nghệ chuỗi khối được xây dựng [1], [2] để giải quyết các vấn đề trên. Tuy nhiên, việc chỉ ứng dụng công nghệ chuỗi khối vào các hệ thống quản lý chuỗi cung ứng không đảm bảo sự giảm thiểu thời gian một cách hiệu quả cho

* Khoa Công nghệ Thông tin, Trường Đại học Mở Hà Nội

† Sinh viên Khoa Công nghệ Thông tin, Trường Đại học Mở Hà Nội

việc truy xuất nguồn gốc sản phẩm trong các hệ thống này.

II. Cơ sở lý thuyết

2.1. Công nghệ chuỗi khối

2.1.1. Chuỗi khối và cách thức hoạt động

Satoshi Nakamoto, một cá nhân chưa rõ danh tính, đã gửi thiêu ý tưởng về Bitcoin trong bài báo “BitCoin: A Peer-to-Peer Electronic Cash System” [3], nhằm giảm thiểu thời gian xác nhận các giao dịch giữa hai bên và loại bỏ sự phụ thuộc vào bên thứ ba. Bitcoin được tạo ra như một đồng tiền mật mã.

Hiện nay với sự phát triển của công nghệ, có nhiều blockchain được tạo ra với nhiều mục đích khác nhau nhưng chúng đều có các thành phần sau [4]:

- *Sổ cái được sao lập (Replicated ledger)*: là một thành phần quan trọng trong chuỗi khối. Nó được sử dụng để lưu trữ thông tin giao dịch, đồng bộ hoá dữ liệu giữa các nút trong mạng, đảm bảo tính toàn vẹn dữ liệu và xác nhận tính hợp lệ của các giao dịch và giúp ngăn chặn các hoạt động gian lận trên mạng chuỗi khối. Sổ cái sao lập chứa toàn bộ chuỗi khối và được lưu trữ trên tất cả các nút trong mạng chuỗi khối.

- *Mạng ngang hàng (Peer-to-Peer network)*: tất cả các nút cùng chia sẻ một sổ cái công khai mà không cần có tác nhân kiểm soát tập trung. Nói cách khác, tất cả các nút được kết nối với nhau thông qua mạng ngang hàng. Các giao dịch và khối được đồng bộ thông qua mạng này.

- *Cơ chế đồng thuận (Consensus)*: Các cơ chế đồng thuận được sử dụng để xác nhận tính hợp lệ của các khối trước khi chúng được thêm vào chuỗi khối. Một khi một giao dịch được tạo ra, nó sẽ được đưa vào khối và khối sẽ được gửi đến tất cả các nút trong mạng để nhận được sự đồng thuận về tính hợp lệ. Các thuật toán đồng thuận phổ biến được sử

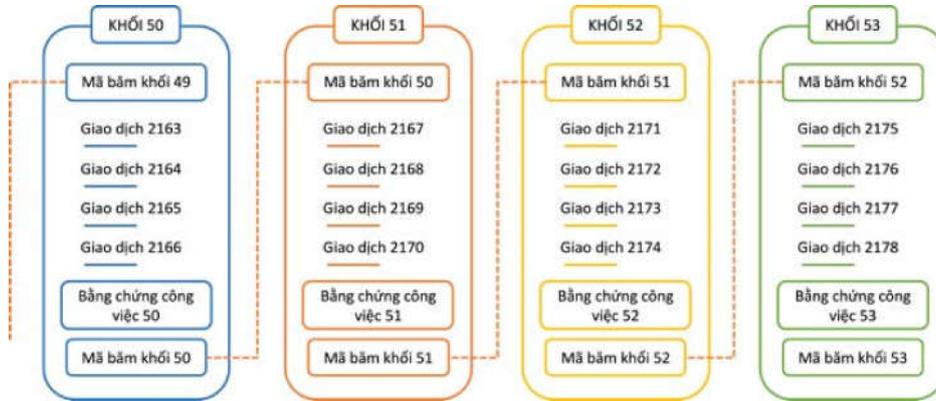
dụng là Proof-Of-Work (POW), Proof of Stake (POS), Practical Byzantine Fault Tolerance (PBFT),... Tùy vào từng mục đích, từng hệ thống thì thuật toán đồng thuận phù hợp sẽ được sử dụng .

- *Mật mã (Cryptography)*: An ninh của một hệ thống blockchain dựa trên các thuật toán mật mã. Trong một mạng blockchain, tính toàn vẹn của các giao dịch hỗ trợ chữ ký số và cấu trúc dữ liệu độc quyền (cây Merkle, Merkle Patricia, ...). Bên cạnh đó, hoạt động xác thực của các giao dịch được hỗ trợ bởi các chữ ký số. Tính toàn vẹn của các giao dịch được hỗ trợ bởi các thuật toán mật mã bất đối xứng là các thuật toán băm, được sử dụng để tạo ra một mã băm duy nhất cho mỗi khối dựa trên dữ liệu trong khối đó. Nếu có bất kỳ sự thay đổi nào xảy ra đối với dữ liệu của khối thì mã băm của khối đó cũng sẽ thay đổi.

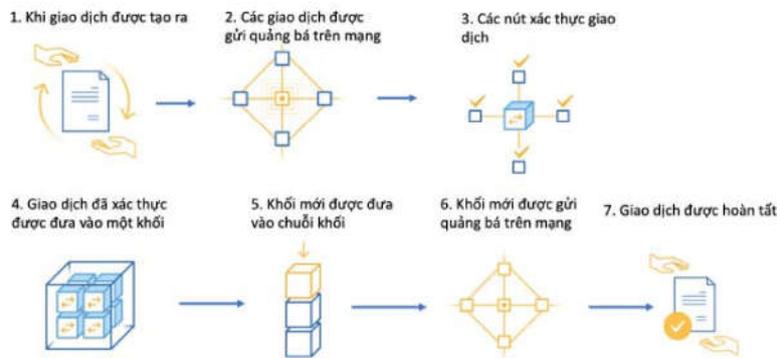
Thành phần cơ bản nhất của một blockchain là giao dịch (transaction). Các giao dịch thể hiện các hoạt động được thực hiện trong các hệ thống ứng dụng chuỗi khối và thường được tổ chức dưới dạng một cấu trúc dữ liệu. Các giao dịch được lưu trữ trong một khối (block). Kích thước của khối sẽ phụ thuộc vào số lượng các thành phần của giao dịch cũng như giao thức chuỗi khối. Các khối trong chuỗi đến được liên kết (nối) với nhau bằng các mã băm. Đây là dữ liệu băm được tạo ra với các dữ liệu đầu vào là dữ liệu của các khối. Mỗi khối sẽ lưu hai mã băm, một mã băm được tạo ra dựa trên dữ liệu của chính nó và một mã băm của khối trước nó. Ví dụ khối thứ n sẽ chứa mã băm của khối $n - 1$. Điều này giúp tạo nên sự liên kết và sự bền vững của chuỗi khối. Nếu kẻ tấn công muốn thay đổi dữ liệu trong một khối nào đó của chuỗi thì cần phải chỉnh sửa dữ liệu của tất cả các khối đứng trước nó. Vì vậy, khả năng thực hiện thành công hoạt động gian lận trong chuỗi khối là rất thấp khi mà số lượng khối trong chuỗi sẽ ngày càng nhiều hơn khi các hệ thống vận hành,

đòi hỏi nhiều tài nguyên tính toán hơn nếu muốn sửa đổi dữ liệu. Ngoài ra, tất cả các nút (các máy tính) tham gia vào mạng lưới đều lưu trữ bản sao của chuỗi khối nên nếu

có sự thay đổi trên một khối nào đó thì khi đồng bộ, quá trình xác nhận sẽ được thực hiện để đảm bảo các khối bị sửa đổi ở một nút nào đó không thể được chấp nhận.



Hình 1. Khối và chuỗi các khối



Hình 2. Khối và chuỗi các khối

Hoạt động của chuỗi khối được thực hiện với các bước sau:

Bước 1. Khi có một giao dịch thể hiện một hoạt động trong hệ thống được tạo ra nó sẽ được thêm vào một khối.

Bước 2. Khối mới sẽ được gửi quảng bá lên một mạng ngang hàng (Peer-to-Peer) với các máy tính được biết đến như là các nút.

Bước 3. Các nút trong mạng sẽ xác thực tính hợp lệ của khối mới dựa trên các thuật toán đồng thuận như Proof of Work (PoW – Bảng chứng công việc), hoặc Proof of Stake (PoS – Bảng chứng cổ phần). Nút giành được quyền và thực hiện thành công việc xác thực một khối sẽ nhận được phần thưởng. Tuỳ thuộc vào từng hệ thống mà

phần thưởng có thể khác nhau. Trong các hệ thống liên quan đến tiền mật mã thì phần thưởng chính là loại tiền đó. Trong một số hệ thống thì phần thưởng thường chỉ mang tính chất tượng trưng để giúp các nút gia tăng khả năng xác thực được khối.

Bước 4. Các khối được xác thực tính hợp lệ sẽ được thêm vào chuỗi. Ngược lại, nó sẽ bị loại bỏ.

Bước 5. Chuỗi với khối mới sau đó sẽ được phân tán đến tất cả các nút trong mạng.

Bước 6. Giao dịch được hoàn tất.

Các nút trong mạng sẽ lưu giữ bản sao của toàn bộ chuỗi khối. Vì vậy, nếu xảy ra hỏng hóc hay mất mát dữ liệu tại một nút thì nút đó có thể lấy lại dữ liệu từ các nút khác. Và để có thể đảm bảo tính riêng tư của các

giao dịch/khối, chữ ký số sẽ được ký vào các khối này. Nên chỉ có những ai là chủ sở hữu của các giao dịch bên trong các khối mới có thể xem được nội dung của khối.

Khi một khối được tạo ra, chủ sở hữu khối sẽ ký vào đó bằng khoá riêng tư (bí mật). Chữ ký này sau đó sẽ được xác nhận bằng khoá công khai của chủ sở hữu khi các khối được gửi quảng bá lên mạng.

2.1.2. Các cơ chế đồng thuận

Các cơ chế đồng thuận (Consensus mechanisms) đã được tích hợp trong công nghệ chuỗi khối như một cơ chế chịu lỗi để xác minh các giao dịch trong mạng lưới [5]. Cơ chế này được sử dụng để đảm bảo tính đúng đắn của các khối mới được thêm vào chuỗi do toàn bộ hoạt động của chuỗi khối là hoàn toàn tự động nên cơ chế xác nhận khối mới cũng phải được thực hiện một cách tự động. Các khối mới này cần phải đạt được sự đồng thuận của ít nhất 51% số nút trong khối thì mới được thêm vào chuỗi.

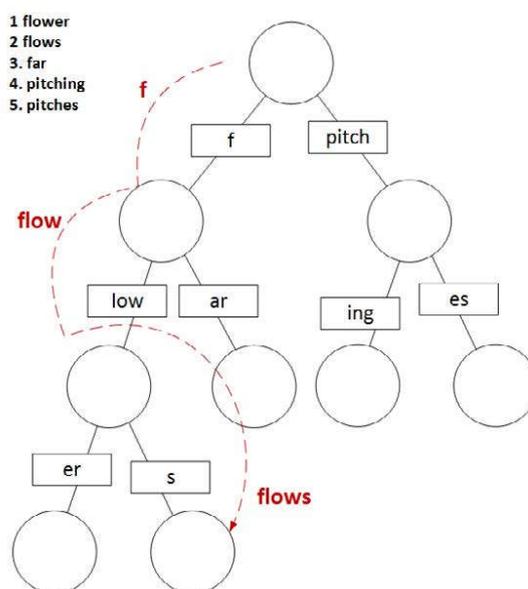
Hiện nay có rất nhiều thuật toán đồng thuận khác nhau nhưng phổ biến nhất là Proof of Work (PoW – Bằng chứng công việc). Bản chất của cơ chế này những người tham gia sẽ phải sử dụng tài nguyên tính toán để giải một bài toán được đặt ra nhằm giành quyền xác thực (công nhận) cho một khối mới trước khi khối này được thêm vào chuỗi. Người tham gia (nút) giành được quyền xác thực khối sẽ nhận được phần thưởng cho việc này. Đây cũng là điểm khó khi triển khai cơ chế PoW trong các hệ thống ứng dụng không liên quan đến tiền mặt mã. Bởi vì cần phải xác định phần thưởng mà nút tham gia xác thực khối mới sẽ nhận được là gì.

2.2. Cây Patricia và ứng dụng trong chuỗi khối

2.2.1. Cây Patricia trie

Cây Patricia, còn được biết đến thuật ngữ cây Radix hay Trie, là một cấu trúc dữ

liệu dạng cây thường được sử dụng để lưu trữ một tập hợp động hoặc mảng kết hợp, trong đó các khoá thường là các chuỗi. Khác với các cấu trúc dữ liệu cây được sử dụng phổ biến hiện nay như các cây nhị phân tìm kiếm, các nút trên các cây Radix không lưu trữ toàn bộ các khoá; thay vào đó, các nút trên Radix chỉ lưu trữ một phần của các Khoá. Và chỉ có đường dẫn đầy đủ từ gốc đến là mô tả một giá trị khoá hoàn chỉnh ứng với một giá trị [6].



Hình 2. Cây Patricia trie [7]

Ngoài ra, các hoạt động trên trên các cây Radix không phải là so sánh các khoá của các nút mà là tìm kiếm một từ khoá theo các nguyên tắc sau:

(1) Bắt đầu từ nút gốc, và với mỗi nút bên trong, một khoá thành phần (partial key) được trích xuất tại mỗi cấp độ.

(2) Khoá thành phần xác định nhánh dẫn đến nút con tiếp theo.

(3) Quá trình này lặp lại cho đến khi gặp một nút lá (khoá được tìm thấy) hoặc một nhánh rỗng (không tìm thấy khoá).

Dưới đây là một ví dụ về cây Patricia trie.

Như trong ví dụ trên 5 từ vựng được sử dụng để tạo chỉ mục cho việc tìm kiếm:

flower, flows, far, pitching, và pitches. Nếu người dùng nhập ký tự “f”, quá trình tìm kiếm sẽ thực hiện ở mức thứ hai, nếu từ “low” được nhập thì sẽ di chuyển xuống mức thứ ba. Và cuối cùng nếu ký tự “s” được nhập thì quá trình tìm kiếm sẽ chuyển xuống mức thứ tư.

Cây Patricia có thể được sử dụng để biểu diễn các cặp (key, value) – (khóa, giá trị). Chúng ta có thể có một danh sách các key và một giá trị gắn kết với mỗi khóa. Các key là các chuỗi ký tự được biểu diễn bởi trie và giá trị sẽ lưu trữ trong nút tại vị trí kết thúc của một key đường dẫn.

Trong một cây Patricia, có 3 loại nút:

- Nút nhánh (Branch node): một nút có nhiều hơn một nút con. Nó lưu trữ liên kết đến các nút con.

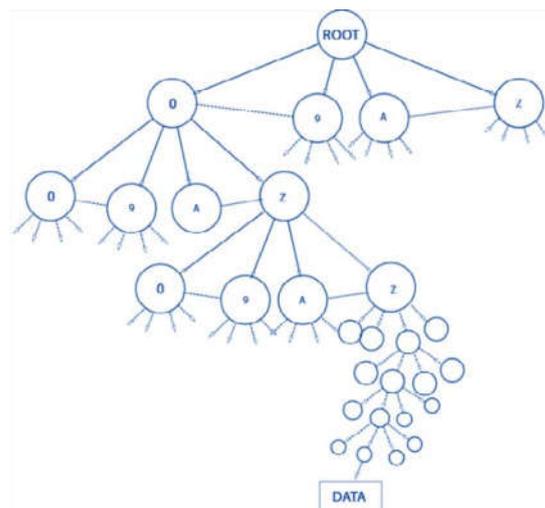
- Nút mở rộng (Extention node): Là một nút không phải nút lá đại diện cho một chuỗi các nút mà chỉ có một nút con. Nó lưu trữ một giá trị khóa biểu diễn cho các nút kết hợp, và một liên kết (link) đến nút kế tiếp.

- Nút lá (Leaf node) hay nút giá trị (Value node): giống với nút mở rộng nhưng thay vì lưu trữ liên kết, nó lưu trữ một giá trị.

2.2.2. Ứng dụng của cây Patricia trie trong công nghệ chuỗi khối

Cây Patricia có thể được sử dụng để lưu trữ các giao dịch (transaction) trong các chuỗi khối. Với các dữ liệu là các giao dịch hoặc các khối và các “unique strings” (các chuỗi duy nhất) có thể được sử dụng để lưu trữ dữ liệu trong trie (có thể là các mã băm của các giao dịch hoặc các khối).

Để lưu trữ các giao dịch sử dụng cây Patricia, cây sẽ có dạng sau:



Hình 3. Cây Patricia trie để lưu trữ các giao dịch

Mỗi mã băm của giao dịch sẽ có ký tự số hoặc ký tự văn bản (tùy thuộc vào thuật toán băm được sử dụng). Chẳng hạn, với sha256 chúng ta sẽ có mã băm dài 32 ký tự. Giả sử mã băm chỉ bao gồm các ký tự 0-9 và A-Z, thì mỗi nút trong patricia trie sẽ có 35 nút con. Việc duyệt sẽ bắt đầu từ nút gốc (root), di chuyển xuống dưới (các nút con) để khớp với từng ký tự của giá trị của nút cho đến nút cuối để có được đối tượng dữ liệu giao dịch.

Thuật toán:

- Với mỗi nút trong cây (trie), bản thân sẽ là một bảng băm với mỗi ký tự băm là một khóa và bảng băm khác là giá trị. Tất cả các hoạt động, chèn, xóa hoặc truy nhập đều có độ phức tạp là $O(h)$ với h là độ lớn của mã băm hay chiều cao của cây.

- Với định nghĩa trên, thuật toán để lưu trữ các giao dịch trong chuỗi khối như sau:

```
curr ← {}
for each character in data.has
  if curr[character] is null:
    curr[character] ← {}
  curr ← curr[character]
curr["DATA"] ← data
```

Trong thuật toán này, một đối tượng gồm một cặp key-value rỗng được tạo ra. Duyệt hết toàn bộ mã băm và với mỗi ký tự thì thiết lập một giá trị mới cho đối tượng cặp key-value rỗng. Đồng thời với mỗi ký tự, đối sánh **curr** hiện tại sẽ được thiết lập cho đối sánh tiếp theo. Và cuối cùng khi toàn bộ các nhánh của cây đã được tạo ra, các dữ liệu sẽ được gán vào các nút cuối cùng với nhãn là “DATA” [8].

III. Phương pháp nghiên cứu

Nhờ có thời gian duyệt các thành phần trong là $O(h)$ nên cây Patricia đang được sử dụng trong nhiều hệ thống ứng dụng chuỗi khối khác nhau. Đặc biệt là các hệ thống quản lý chuỗi cung ứng.

Trong bài báo này, cây Patricia sẽ được triển khai để lưu trữ các giao dịch về các hoạt động của chuỗi cung ứng trái cây. Một lượng lớn các giao dịch mô phỏng sẽ được tạo ra và thời gian thực hiện sẽ được ước lượng, tổng hợp, so sánh và đánh giá.

3.1. Hệ thống quản lý chuỗi cung ứng trái cây sử dụng công nghệ chuỗi khối

Hiện nay, đã có rất nhiều hệ thống quản lý chuỗi cung ứng trái cây được xây dựng [9]China”, ”event-title”: ”2022 International Conference on Cloud Computing, Big Data and Internet of Things (3CBIT). Các hệ thống này quản lý các quá trình sản xuất và trồng trọt, chế biến, vận chuyển, bảo quản và bán hàng, v.v. Dữ liệu thu thập trong mỗi quá trình sẽ được xác minh và tải lên hệ thống. Quá trình trồng trọt bao gồm các hoạt động trồng trọt, thu hoạch và giám sát trạng thái của nông sản. Các thông tin được tạo ra bao gồm lô sản phẩm, thông tin nguồn gốc, thời gian trồng, thời gian thu hoạch, thông tin nhiệt độ và độ ẩm. Quá trình chế biến bao gồm làm sạch và làm mát nông sản, lựa chọn và sắp xếp trái cây, đóng gói

vào các thùng,...

Với các thông tin có được từ các quá trình, người tiêu dùng hoàn toàn có thể truy xuất nhằm lựa chọn trái cây một cách phù hợp nhất.

3.2. Ứng dụng cây Patricia trong hệ thống quản lý chuỗi cung ứng trái cây sử dụng chuỗi khối

Đối với khách hàng, điều quan trọng nhất là sự phản hồi một cách nhanh chóng của hệ thống về nguồn gốc của các nông sản mà họ đang tìm hiểu. Một số khách hàng khó tính còn muốn biết sản phẩm mà họ đang quan tâm đã được trồng ở đâu, đã được thu hoạch khi nào, vận chuyển ra sao, có đảm bảo các tiêu chí về an toàn hay không. Vì vậy, để có thể giảm thiểu được thời gian truy xuất thông tin nguồn gốc của các nông sản, cây Patricia đã được sử dụng để lưu trữ các giao dịch:

- đơn vị thu hoạch thực hiện thu hoạch nông sản.
- đơn vị đóng gói thực hiện đóng gói các nông sản đã được thu hoạch theo các tiêu chuẩn.
- đơn vị vận chuyển vận chuyển nông sản đến nhà phân phối.
- đơn vị thu mua thực hiện thu mua nông sản.

Với một lượng lớn các nhà sản xuất (người nông dân) và rất nhiều hoạt động sẽ được thực hiện trước khi các nông sản đến tay người tiêu dùng. Do đó sẽ mất rất nhiều thời gian để có thể truy xuất được quá trình nông sản được xử lý nếu không có cơ chế lưu trữ phù hợp và hiệu quả. Và mất nhiều thời gian, chẳng hạn lớn hơn 5 giây để có được thông tin về nguồn gốc của nông sản thì khả năng người tiêu dùng quyết định mua sẽ giảm đi đáng kể. Một khi số lượng giao dịch tăng lên theo thời

gian thì thời gian cần để có thể truy xuất được thông tin cũng sẽ tăng lên. Vì vậy, với phương pháp sử dụng cây Patricia để lưu trữ giao dịch sẽ giúp giảm thiểu thời gian cần thiết để có thể truy xuất được các thông tin.

IV. Kết quả và thảo luận

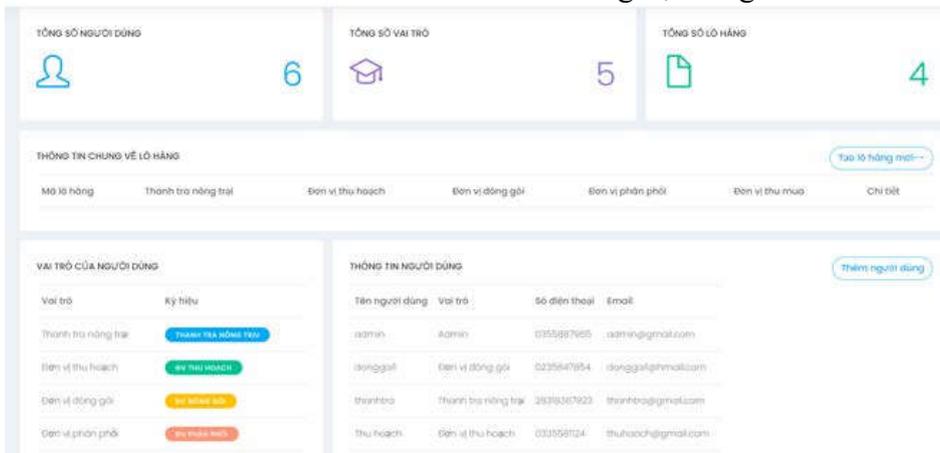
Trong phần này, hệ thống quản lý chuỗi cung ứng có ứng dụng công nghệ chuỗi khối và cây Patricia được trình bày với các chức năng hỗ trợ người dùng và các kết quả thực nghiệm về thời gian thực thi các giao dịch cũng được thu thập, phân tích.

4.1. Các cài đặt môi trường triển khai

Hệ thống được triển khai sử dụng Hệ quản trị cơ sở dữ liệu Microsoft SQL Server để lưu trữ các thông tin về người dùng, nhà sản xuất, phân phối,... Các chức năng của hệ thống quản lý được xây dựng trên nền tảng Asp.net và JS.

4.2. Xây dựng hệ thống quản lý chuỗi cung ứng trái cây dựa trên chuỗi khối

Để thực nghiệm hiệu năng của cây Patricia trong các hệ thống quản lý chuỗi cung ứng dựa trên chuỗi khối, trong bài báo này giới thiệu một hệ thống quản lý chuỗi cung ứng trái cây sử dụng cây Patricia để lưu trữ các giao dịch được tạo ra trong hệ thống.



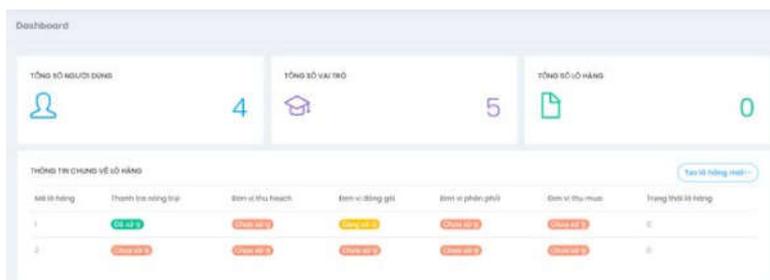
Hình 4. Hệ thống quản lý chuỗi cung ứng trái cây

Tại giao diện này, người quản lý có thể có được các thông tin tổng quan về số người dùng, số vai trò của người dùng: thanh tra nông trại, đơn vị thu hoạch, đơn vị đóng gói, đơn vị phân phối, đơn vị thu mua, người sản xuất, số lô hàng.

4.2.1. Chức năng quản lý lô hàng

Chức năng cho phép người quản trị quản lý các lô hàng trái cây.

Việc thêm mới lô hàng có thể được thực hiện thông qua một giao diện của chức năng thêm lô hàng.



Hình 5. Chức năng quản lý lô hàng

Hình 6. Chức năng thêm lô hàng

4.2.2. Chức năng quản lý người dùng

Chức năng quản lý người dùng cho phép quản trị viên thêm mới, chỉnh sửa thông tin, phân quyền người dùng theo vai trò.

Hình 7. Chức năng quản lý người dùng

4.2.3. Chức năng nhập thông tin thông qua mã QR

Để tạo thuận tiện cho người sử dụng, hệ thống cung cấp chức năng nhập liệu cho các đối tượng, quá trình bằng cách quét các mã QR tương ứng.



Hình 8. Chức năng nhập thông tin thông qua mã QR

Chức năng này được xây dựng với giao diện đơn giản, cùng với đó là một số trường dữ liệu để triển khai thực nghiệm.

4.2.4. Chức năng hiển thị thông tin lô hàng

Chức năng này cho phép người tiêu dùng có thể tra cứu nguồn gốc của một nông sản cụ thể.

Tại mỗi bước đều thể hiện đầy đủ thông tin về nơi mà nông sản được trồng, được thu hoạch, được đóng gói:

- Thông tin lô hàng: do ai sản xuất, địa chỉ, đơn vị thu hoạch, đơn vị đóng gói.

Quản lý lô hàng [Print](#)

Mã lô: a44070283daf98cc070986b537449e2ectf80a5fee5812909d93e9bd4ffc567

Lô hàng

Mã nông dân: 565a2728 ✓

Tên nông dân: Nguyễn Xuân Cường ✓

Địa chỉ: 001 ✓

Đơn vị thu hoạch: 144 ✓

Đơn vị đóng gói: Công ty BSA ✓

Thành tra nông trại

Giống cây: Cây 1 ✓

Loại phân bón: phân nhón ✓

Loại phân bón: phân nhón ✓

Mùa vụ: vụ 1 ✓

Đơn vị thu hoạch

Loại sản phẩm: Quả 1 ✓

Sản lượng: 10 ✓

Đơn vị tính: Tấn ✓

Đơn vị đóng gói

Mã đơn vị: 0001 ✓

Địa chỉ: ✓

Ngày nhận: 12/12/2019 ✓

Số lượng: 1000 ✓

Đơn vị tính: Tấn ✓

Ngày đóng gói: 12/12/2019 ✓

Hiện sử dụng: 30/12/2019 ✓

Hình 9. Chức năng hiện thị thông tin lô hàng

- Thanh tra nông trại: xác nhận thông tin về giống cây, loại phân bón sử dụng, mùa vụ.

- Thông tin đóng gói: đơn vị đóng gói, ngày nhận, số lượng, đơn vị tính, ngày đóng gói, hạn sử dụng.

- Thông tin thu hoạch: đơn vị thu hoạch, sản lượng (tấn).

4.2.5. Thử nghiệm về tốc độ xử lý các giao dịch

Trong các thực nghiệm này, có hai phương án được triển khai: 1) Sử dụng cây Patricia và 2) không sử dụng cây Patricia để lưu trữ các giao dịch. Số lượng giao dịch được thử nghiệm nằm trong khoảng từ [1000 – 7.500.000], thời gian xử lý toàn bộ giao dịch để thêm giao dịch mới được đo bằng micro-giây. Các dữ liệu thu được từ thực nghiệm được thể hiện trong bảng 1.

Bảng 1. So sánh thời gian xử lý các giao dịch giữa phương án sử dụng cây Patricia và không sử dụng cây Patricia để lưu trữ các giao dịch

Số lượng giao dịch	Thời gian (micro giây)	
	Cây Patricia	Không sử dụng cây Patricia
1000	4,6	4,9
3000	4,9	5,2
5000	4,3	5,6
10.000	4,4	7,7
50.000	4,5	7,9
100.000	4,2	9,5
500.000	4,2	16,4
1.000.000	4,3	29
2.000.000	4,4	49,3
4.000.000	4,3	87,9
7.500.000	4,6	155,1

Như trong bảng 1, với số lượng giao dịch nằm trong khoảng [1000 – 5000] thì thời gian cần để xử lý toàn bộ các giao dịch giữa hai phương án sử dụng và không sử dụng cây Patricia là gần tương đương.

Tuy nhiên, khi số lượng giao dịch tăng lên thì thời gian của phương án không sử dụng cây Patricia tăng lên rất nhiều. Ngược lại, phương án sử dụng cây Patricia luôn ổn định trong khoảng [4.2 – 4.6] micro-giây. Như vậy, rất rõ ràng là việc sử dụng cây Patricia để lưu trữ các giao dịch trong chuỗi khối giúp giảm thiểu một cách hiệu quả thời gian cần thiết để thêm một giao dịch. Từ đó giúp tăng khả năng người tiêu dùng sẽ quyết định mua trái cây khi họ có thể mất ít thời gian hơn trong việc truy xuất nguồn gốc của trái cây mà họ đang quan tâm.

4.3. Thảo luận

Qua các thực nghiệm được thực hiện trong bài báo này, rõ ràng việc triển khai cây Patricia để lưu trữ các giao dịch trong chuỗi khối giúp giảm thiểu một cách đáng kể thời gian cần thiết xử lý các giao dịch. Đặc biệt là trong các hệ thống quản lý chuỗi cung ứng trái cây ứng dụng công nghệ chuỗi khối, thì thời gian phản hồi yêu cầu truy xuất nguồn gốc của người tiêu dùng là rất quan trọng. Từ kết quả đó, một hệ thống quản lý chuỗi cung ứng trái cây đã được xây dựng. Người quản lý có thể quản lý các công đoạn sản xuất, trồng trọt, thu hoạch, chế biến, vận chuyển, phân phối. Người tiêu dùng có thể sử dụng chức năng quét mã QR của trái cây để truy xuất nguồn gốc và toàn bộ thông tin về quá trình sản xuất nông sản.

Tài liệu tham khảo:

- [1]. R. Manzoor, B. S. Sahay, and S. K. Singh, "Blockchain technology in supply chain management: an organizational theoretic overview and research agenda," *Ann. Oper. Res.*, Nov. 2022, doi: 10.1007/s10479-022-05069-5.
- [2]. H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks," *IEEE Access*, vol. 7, pp. 41426–41444, 2019, doi: 10.1109/ACCESS.2019.2907695.
- [3]. S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," *Secur. Commun. Netw.*, vol. 2021, pp. 1–22, Jan. 2021, doi: 10.1155/2021/6693731.
- [4]. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," *IEEE Access*, vol. 7, pp. 134422–134433, 2019, doi: 10.1109/ACCESS.2019.2941905.
- [5]. B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021, doi: 10.1109/ACCESS.2021.3065880.
- [6]. V. Alvarez, S. Richter, X. Chen, and J. Dittrich, "A comparison of adaptive radix trees and hash tables," in *2015 IEEE 31st International Conference on Data Engineering*, Seoul, South Korea: IEEE, Apr. 2015, pp. 1227–1238. doi: 10.1109/ICDE.2015.7113370.
- [7]. "Radix Trie (aka PATRICIA trie)." <https://asecuritysite.com/blockchain/js09> (accessed Feb. 14, 2023).
- [8]. K. Khullar, "Implementing Merkle Tree and Patricia Trie," *Coinmonks*, Aug. 23, 2020. <https://medium.com/coinmonks/implementing-merkle-tree-and-patricia-trie-b8badd6d9591> (accessed Mar. 12, 2023).

- [9]. Y. Wang, X. Zhang, J. Leng, S. Cheng, and D. Wang, "Design of Fruit and Vegetable Produce Traceability System Based on Dual Chain and Dual Storage Blockchain," in *2022 International Conference on Cloud Computing, Big Data and Internet of Things (3CBIT)*, Wuhan, China: IEEE, Oct. 2022, pp. 130–134. doi: 10.1109/3CBIT57391.2022.00034.

EMPLOYING PATRICIA TREE TO OPTIMIZE THE CONSUMED TIME FOR TRANSACTION PROCESSING IN THE FRUIT SUPPLYING CHAIN MANAGEMENT SYSTEM

Nguyen Duc Tuan[‡], *Nguyen Xuan Duong*[§]
Email: nguyenductuan@hou.edu.vn

Abstract: *Blockchain technology is receiving much attention and research from scientists worldwide. This technology has also been applied in many fields, from economics to agriculture, especially in supply chains, allowing consumers to trace the origin of products. The number of transactions in supply chain management systems is generally very large. Therefore, many approaches have been proposed to reduce the time required to store and verify transactions. In this article, the authors offer a solution using Patricia trees to reduce the time required to keep and verify transactions in a supply chain management system for agricultural products. Experimental results show that using Patricia trees helps reduce the time required to verify transactions.*

Keywords: *blockchain, consensus mechanism, supplying chain for fruits, management system, patricia tree, peer-to-peer, transaction*

[‡] Faculty of Information technology, Hanoi Open University

[§] Student of Faculty of Information technology, Hanoi Open University