

ỨNG DỤNG BLOCKCHAIN TĂNG CƯỜNG ĐỘ TIN CẬY CHO HỆ THỐNG XÁC THỰC NGUỒN GỐC EZCHECK

**ThS. Hoàng Mạnh Thắng*, TS. Nguyễn Trung Kiên,
ThS. Nguyễn Kim Quang, KS. Hoàng Thị Thu**
Viện công nghệ Thông tin và Truyền thông CDIT
*Email: thanghm@ptit.edu.vn

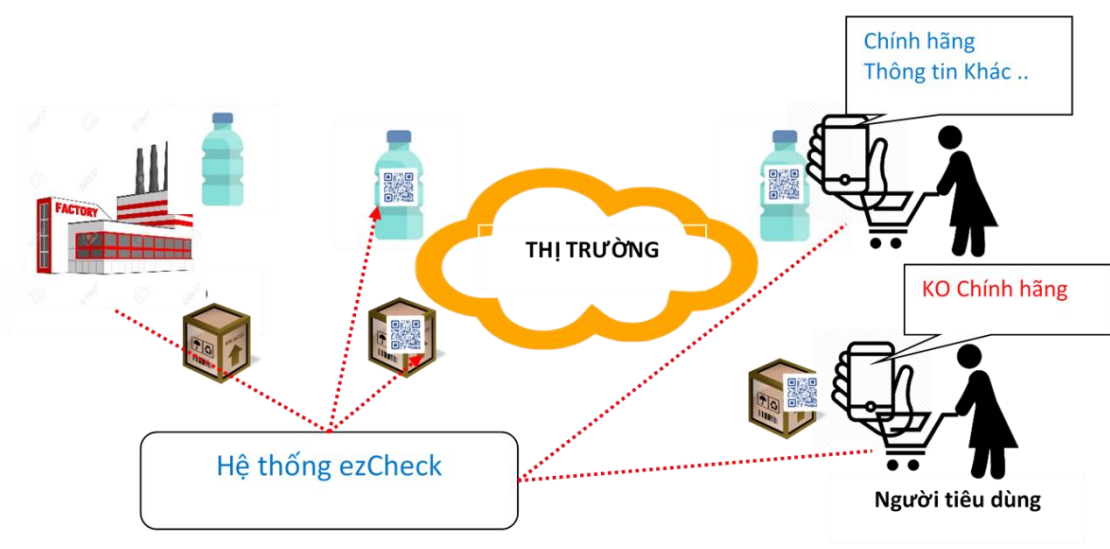
Tóm tắt: ezCheck là giải pháp sử dụng QR code và các kỹ thuật bảo mật để đảm bảo mỗi mã QRcode là định danh duy nhất cho từng đơn vị sản phẩm. Từ đó người tiêu dùng có thể kiểm tra nguồn gốc sản phẩm và nhận được nhiều thông tin khác về sản phẩm như Hướng dẫn sử dụng, chính sách khuyến mãi,... Doanh nghiệp có được giải pháp bảo vệ hàng hóa hiệu quả, cũng như tạo được sự gắn kết khách hàng thông qua việc nhận được các thông tin phản hồi từ khách hàng, chủ động quảng bá sản phẩm. Tuy nhiên, hiện nay dữ liệu của ezCheck được lưu trữ tập trung trên một nhóm server, các thông tin này có thể bị sửa xóa bởi người quản trị, bởi hacker; dẫn tới độ tin cậy của dữ liệu chưa cao. Bài báo này tập trung trình bày giải pháp tăng cường độ tin cậy của hệ thống ezCheck bằng cách ứng dụng công nghệ Blockchain thông qua một số kịch bản sử dụng trong thực tế.

Từ khóa: Blockchain, ezCheck, QRcode, chống giả, xác thực nguồn gốc.

1. GIỚI THIỆU EZCHECK VÀ VẤN ĐỀ CÒN TỒN TẠI

1.1. ezCheck

ezCheck là giải pháp xác thực nguồn gốc hàng hóa, chống hàng giả và gắn kết Người tiêu dùng (NTD) với Doanh nghiệp (DN)/Nhà sản xuất (NSX) trong thời đại số bằng cách tạo ra kênh thông tin 2 chiều thông suốt, minh bạch giữa DN và NTD cùng với một cơ chế xác thực thông minh.



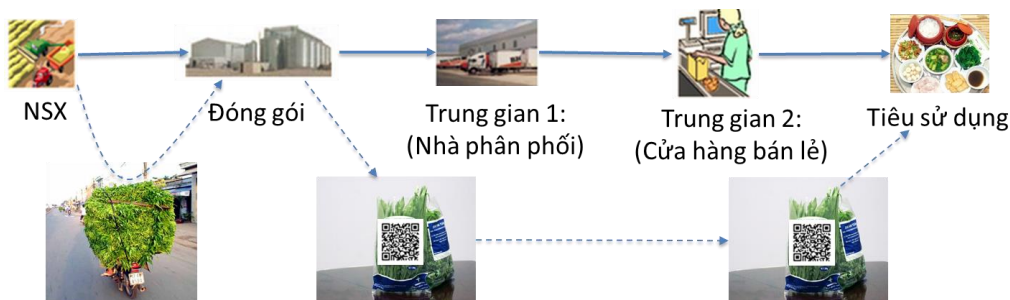
Hình 1: Mô hình hệ thống ezCheck

Hai chức năng cơ bản của ezCheck là:

- Xác thực nguồn gốc sản phẩm,
- Kênh thông tin 2 chiều giữa DN và NTD.

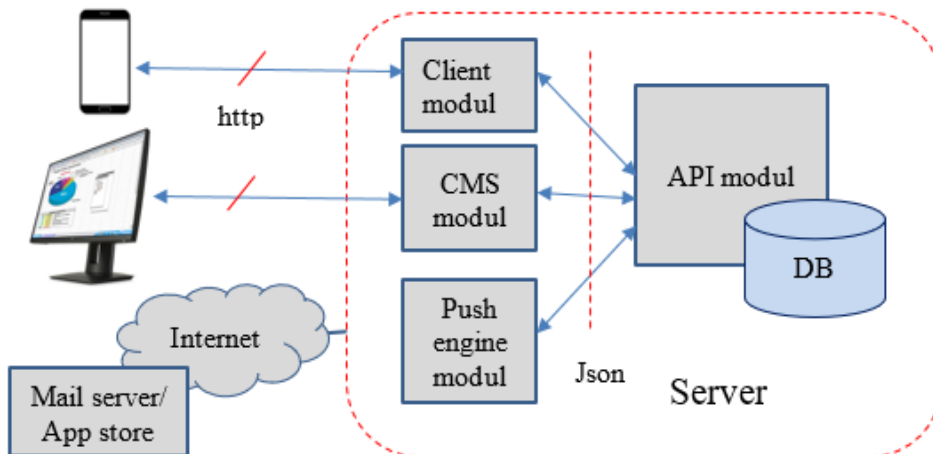
Khi DN sử dụng Tem/Nhãn có chứa mã của ezCheck, NTD có thể quét mã các sản phẩm đó để xác thực nguồn gốc sản phẩm hàng hóa. Mỗi đơn vị sản phẩm sẽ được gán một mã duy nhất, thể hiện dạng QR code:

- Nhà sản xuất sẽ thu thập và cung cấp thông tin ban đầu trên hệ thống thông qua giao diện Web (CMS module)
- Người sử dụng dùng smartphone quét QR code để truy xuất và xác thực thông tin của sản phẩm (Client module).



Hình 2: Quy trình nghiệp vụ hệ thống

Hệ thống ezCheck được thiết kế thành các module con, các module này có thể triển khai cùng trên một máy tính với mô hình nhỏ hoặc có thể triển khai trên nhiều máy tính với mô hình lớn:



Hình 3: Mô hình kết nối hệ thống ezCheck

1.2. Vấn đề còn tồn tại

Tuy hệ thống ezCheck đã được thiết kế thành nhiều module con để dễ dàng nâng cấp và mở rộng khi cần dung lượng lớn nhưng nhìn tổng thể, mô hình hệ thống ezCheck cũng như mô hình của các hệ thống xác thực nguồn gốc khác hiện nay vẫn là mô hình tập trung. Các thành phần của hệ thống được tập trung trên một hoặc một

nhóm nhỏ các server, do một hoặc một nhóm người quản trị, điều này dẫn tới những nguy cơ như:

- Thông tin lưu trữ trên server có thể bị chỉnh sửa một cách đơn giản, dễ dàng bởi Hacker hoặc chính người quản trị hệ thống;
- Dữ liệu lưu trữ tập trung, có thể có backup dự phòng nhưng rất dễ bị xóa với những cuộc tấn công có chủ đích;
- Thông tin về sản phẩm, hàng hoá tập trung ở từng bộ phận, chưa có mối liên hệ giữa các khâu trong chuỗi cung ứng với nhau.

Như vậy, do tính chất tập trung, phụ thuộc vào con người mà các giải pháp hiện nay có độ tin cậy, tính minh bạch chưa cao. Để khắc phục vấn đề này, một trong những giải pháp hiện nay là chuyển mô hình hệ thống sang mô hình phân tán. Dữ liệu sẽ được phân tán ra các server vật lý khác nhau, không thể thêm, bớt, sửa, xóa dữ liệu khi chưa có sự đồng thuận của các bên tham gia. Đây cũng là đặc tính cơ bản của công nghệ tiên tiến hiện nay - công nghệ Blockchain. Bài báo này trình bày về việc ứng dụng công nghệ Blockchain để tăng cường độ tin cậy của giải pháp xác thực nguồn gốc sản phẩm, hàng hóa ezCheck của CDIT.

2. ỨNG DỤNG BLOCKCHAIN TĂNG CƯỜNG ĐỘ TIN CẬY CỦA EZCHECK

2.1. Sự phù hợp của Blockchain trong việc tăng cường độ tin cậy

Blockchain là công nghệ lưu trữ dữ liệu theo chuỗi. Mỗi khối dữ liệu được móc nối với nhau thông qua các thuật toán phức tạp nhằm đảm bảo khi khối dữ liệu đã được thêm vào chuỗi thì không thể sửa, xóa, thay đổi thứ tự với các công nghệ tính toán hiện nay trong khoảng thời gian cho phép được (hay còn gọi là độ phức tạp tính toán cao). Với kỹ thuật này, công nghệ Blockchain mang những đặc điểm như:

- ***Không thể làm giả, không thể phá hủy các chuỗi Blockchain:*** chỉ có máy tính lượng tử mới có thể can thiệp vào và giải mã chuỗi Blockchain và nó chỉ bị phá hủy hoàn toàn khi không có internet trên toàn cầu.
- ***Tính minh bạch:*** Blockchain cung cấp nhiều bước tiến to lớn trong việc cải tiến tính minh bạch khi so sánh với cách thức ghi chép hồ sơ và sổ cái hiện hành trong các ngành công nghiệp.
- ***Loại bỏ đơn vị trung gian:*** các hệ thống được xây dựng dựa trên công nghệ Blockchain cho phép loại bỏ các đơn vị trung gian liên quan đến hoạt động lập hồ sơ và chuyển giao tài sản.
- ***Tính bất biến:*** khi giao dịch hoặc dữ liệu đã được ghi bởi người nắm giữ khóa bí mật, chỉ riêng người khởi tạo Blockchain mới có, dữ liệu đó không thể sửa chữa, nó sẽ lưu lại mãi mãi.

- **Tính phi tập trung:** các hệ thống xây dựng dựa trên công nghệ Blockchain có thể hoạt động trên mạng lưới máy tính phi tập trung, nhằm giảm thiểu rủi ro bị tấn công, thời gian chết máy chủ và thất thoát dữ liệu.
- **Độ tin cậy:** các hệ thống xây dựng dựa trên công nghệ Blockchain gia tăng độ tin cậy giữa các bên giao dịch nhờ tính minh bạch được cải thiện và mạng lưới phi tập trung. Đồng thời loại bỏ các đơn vị trung gian tại các quốc gia nơi con người khó có lòng tin vào đơn vị trung gian trong giao dịch.

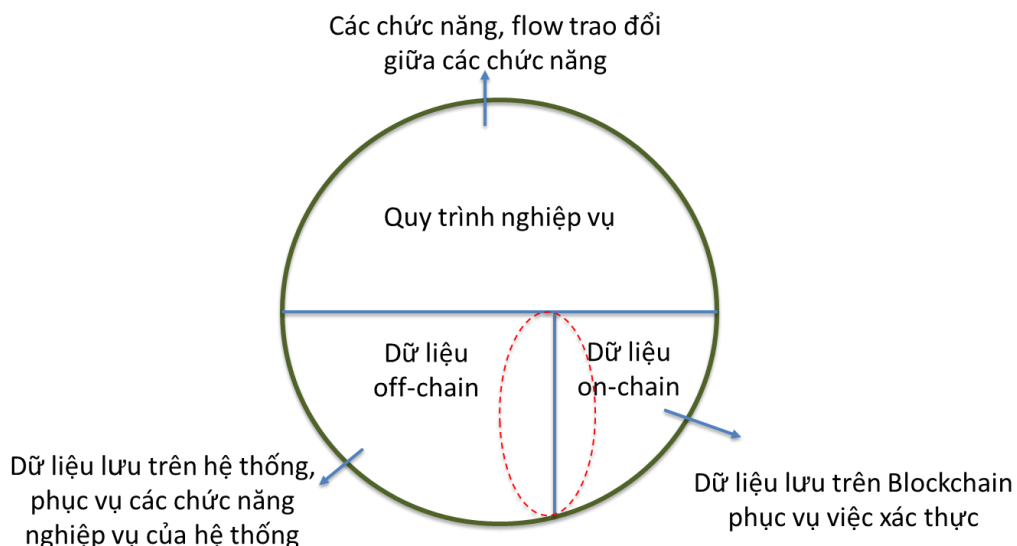
Như vậy, các ứng dụng dựa trên công nghệ Blockchain sẽ kế thừa các thuộc tính, đặc điểm Blockchain, đặc biệt là về độ tin cậy. Thực tế, các nghiên cứu trên thế giới và ở Việt Nam đều chỉ ra rằng, công nghệ Blockchain là ứng cử viên hàng đầu cho các giải pháp xác thực. Do đó, CDIT đã nghiên cứu, áp dụng Blockchain để cải tiến độ tin cậy của hệ thống ezCheck, nhằm mang đến cho xã hội một giải pháp an toàn hơn, minh bạch hơn, đáp ứng nhu cầu cao hơn của DN cũng như người sử dụng.

2.2. Mô hình ứng dụng công nghệ Blockchain vào sản phẩm ezCheck

Blockchain hoạt động theo mô hình mạng phân tán, mỗi khối dữ liệu được thêm vào chuỗi cần phải có sự đồng thuận của tất cả các node mạng, đồng thời các khối dữ liệu này cũng được thêm vào tất cả các node, số lượng node mạng càng lớn, độ tin cậy càng cao, dữ liệu được nhân bản nhiều hơn, số lượng cần đồng thuận cao hơn. Như vậy, để tăng cường độ tin cậy, Blockchain đã đánh đổi với không gian lưu trữ và tốc độ xử lý. Để tận dụng hiệu quả của Blockchain, dữ liệu ghi lên mạng Blockchain nên là những dữ liệu ngắn gọn, ý nghĩa (Ví dụ như các thông tin về giao dịch). Đó cũng là lý do mà Blockchain rất phù hợp với tiền điện tử và cũng đã phát triển rất mạnh cùng với tiền điện tử.

Do đó, để phát huy được ưu điểm của Blockchain thì các ứng dụng trên nền công nghệ Blockchain thường có hai loại dữ liệu là dữ liệu on-chain và dữ liệu off-chain:

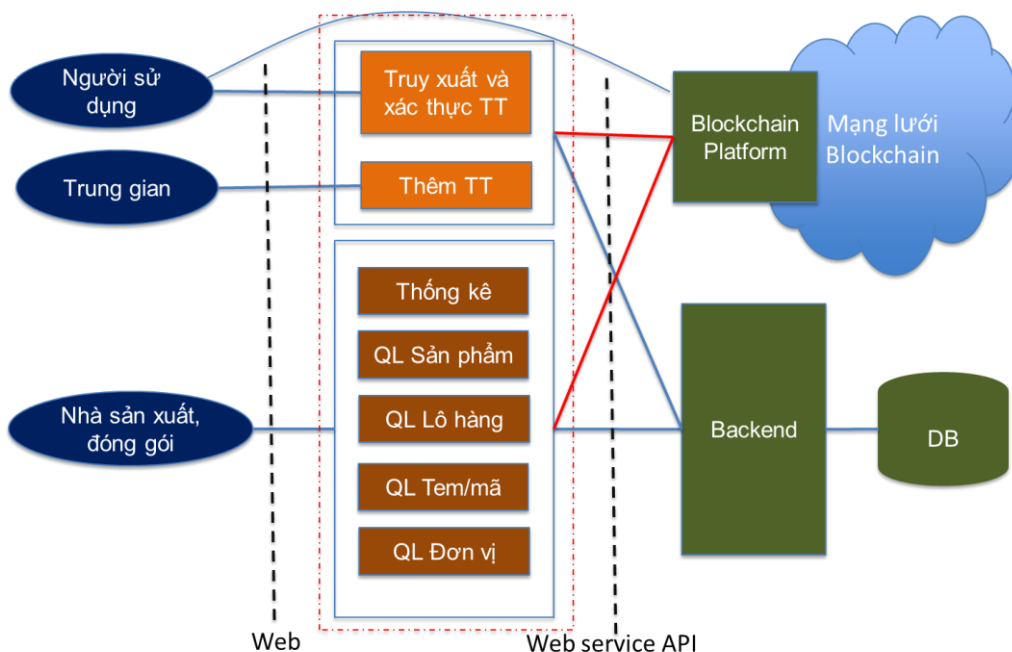
- **Dữ liệu on-chain:** là dữ liệu lưu trên mạng Blockchain, thường là các dữ liệu ngắn gọn, ý nghĩa như các mã băm, các sự kiện sinh ra trong quá trình thêm, bớt, sửa, xóa thông tin khi thực hiện quy trình nghiệp vụ của dịch vụ/ứng dụng.
- **Dữ liệu off-chain:** là dữ liệu multimedia có kích thước lớn, có thể thay đổi sinh ra trong quá trình thực hiện quy trình nghiệp vụ của dịch vụ/ứng dụng.



Hình 4: Mô hình ứng dụng Blockchain

Khi tích hợp Blockchain vào hệ thống ezCheck, những dữ liệu hiện tại của hệ thống được coi là dữ liệu off-chain, còn những dữ liệu on-chain là những dữ liệu sẽ được sử dụng để xác thực thông tin là đúng hay sai, có bị chỉnh sửa gì không như:

- Mã băm của các dữ liệu offchain (Text, hình ảnh, âm thanh, video về sản phẩm)
- Lịch sử của những giao dịch trong hệ thống ezCheck như kích hoạt mã, thêm/sửa/xóa thông tin về sản phẩm,...



Hình 5: Kiến trúc hệ thống xác thực nguồn gốc ứng dụng Blockchain

Các đối tượng (actor) của hệ thống:

- Nhà sản xuất/đóng gói,
- Nhà trung gian (vận chuyển, đóng gói lại, siêu thị, bán lẻ),
- Người tiêu dùng.

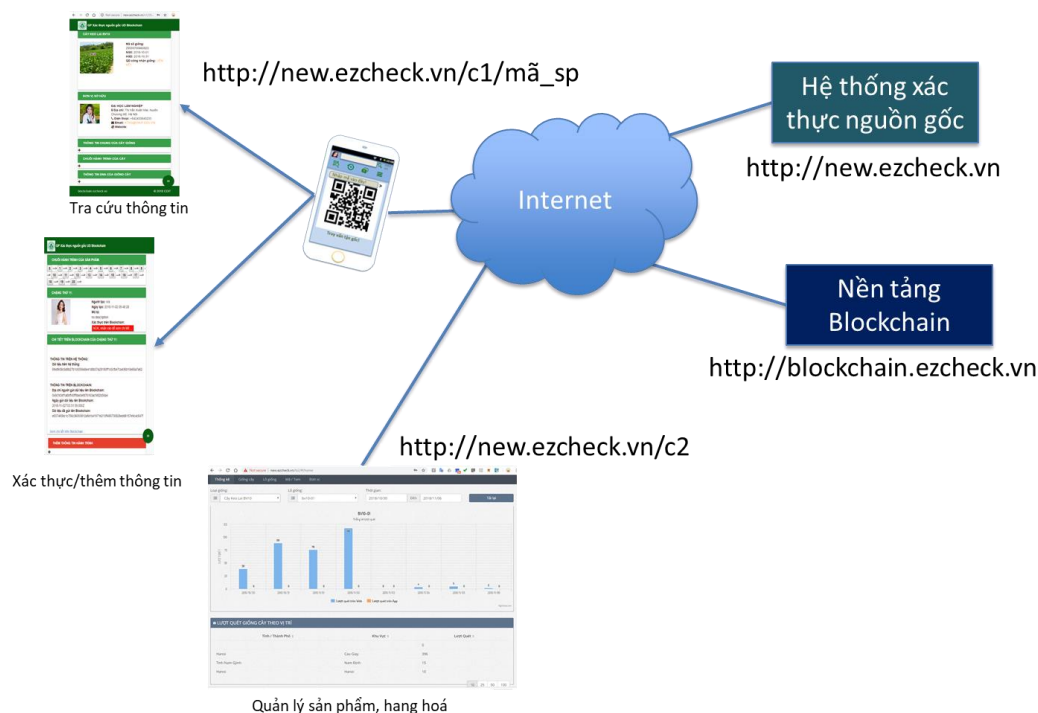
Các đối tượng tham gia giao dịch trong hệ thống đều được cấp một địa chỉ Blockchain, địa chỉ này được cấp khi đăng ký sử dụng hệ thống. Các đối tượng tham gia hệ thống có quyền thêm các thông tin trong hệ thống, mỗi hành động này là một giao dịch. Thông tin được tạo ra trong giao dịch này là hình ảnh, mô tả, ngày giờ,... được băm ra và gửi lên trên hệ thống Blockchain với FromID là địa chỉ Blockchain của các đối tượng tạo ra thông tin.

3. THỬ NGHIỆM TRONG THỰC TẾ

3.1. Mô hình triển khai thử nghiệm

Xét về độ tin cậy, Public Blockchain được coi là có độ tin cậy cao nhất vì dữ liệu on-chain được public và lưu trữ phân tán trên toàn mạng, nhưng việc gửi dữ liệu lên chuỗi sẽ bị tính phí. Việc này phù hợp với những sản phẩm có giá trị cao, còn những sản phẩm khác có thể có những giải pháp khác phù hợp hơn như một nền tảng Private Blockchain chẳng hạn.

Trong phạm vi nghiên cứu, hướng tới một giải pháp có độ tin cậy cao nhất cũng như sẵn sàng làm chủ nền tảng Blockchain, nhóm thực hiện đã dựng một hệ thống Blockchain nội bộ dựa trên nền tảng opensource Ethereum, là một trong những nền tảng Public Blockchain V2.0 phổ biến nhất hiện nay.



Hình 6: Mô hình triển khai thử nghiệm của hệ thống

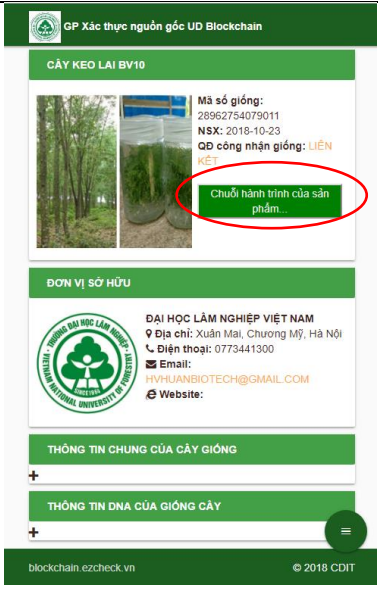
3.2. Case study: ứng dụng Blockchain phát hiện thay đổi thông tin về sản phẩm, hàng hóa

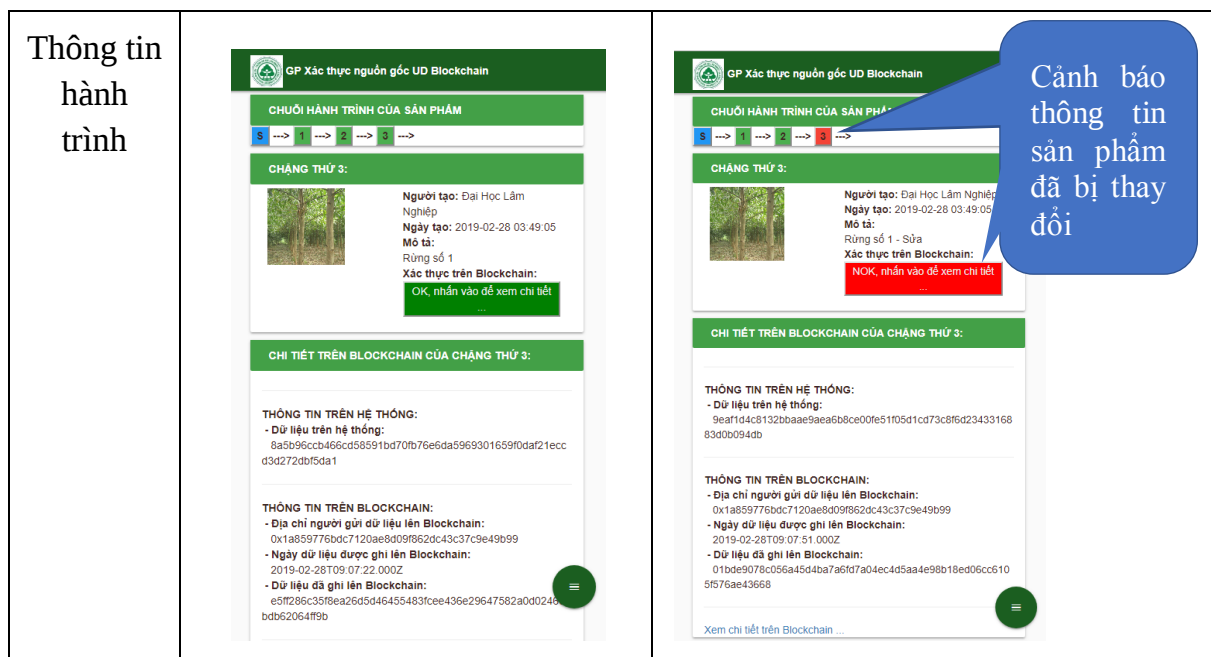
Trong quá trình thực hiện, nhóm nghiên cứu đã tiến hành thử nghiệm hệ thống xác thực nguồn gốc ứng dụng công nghệ Blockchain vào quản lý chuỗi hành trình và truy xuất nguồn gốc của giống cây trồng tại Viện Sinh thái rừng và Môi trường, Trường Đại học Lâm nghiệp Việt Nam, Hà Nội.

Với ý tưởng coi mỗi cây giống là một đối tượng với các thuộc tính riêng có các thông số cần theo dõi (vị trí trồng, điều kiện môi trường, kích thước cây, chế độ chăm sóc, các hoạt động của người chăm sóc tác động lên cây,...). Dữ liệu của đối tượng này được lưu tập trung trên server. Mỗi đối tượng (cây) được định danh bằng 1 ID duy nhất (dưới dạng đường link web) thông qua QR code. Người chăm sóc hàng ngày sẽ sử dụng smartphone với phần mềm SCAN QR code để cập nhật các thông số (trạng thái, số đo hay hình ảnh) tại thời điểm kiểm tra lên server. Phía server sẽ tự động phân tích dữ liệu tạo ra các báo cáo, các cảnh báo hay các sự kiện nhắc lịch cho người chăm sóc.

Hệ thống triển khai thử nghiệm được mô tả chi tiết ở bảng dưới đây

Giao diện sản phẩm trước khi bị sửa xóa thông tin

	Thông tin bình thường	Thông tin đã bị thay đổi
Thông tin chung		



4. KẾT LUẬN

Bài báo đã trình bày một ứng dụng của Blockchain trong việc tăng cường độ tin cậy của giải pháp xác thực nguồn gốc hàng hóa ezCheck. Việc sử dụng tem ezCheck và dịch vụ xác thực nguồn gốc của ezCheck có thể giúp đảm bảo các sản phẩm của DN khi ra thị trường luôn được xác thực nguồn gốc rõ ràng và có kênh kết nối trực tiếp tới NTD.

Hiện sản phẩm này của Viện CDIT đã được chuyển giao công nghệ cho Tập đoàn Bưu chính Viễn thông Việt nam VNPT để cung cấp dịch vụ trên cả nước với thương hiệu VNPT Check.

TÀI LIỆU THAM KHẢO

1. Báo cáo khoa học đề tài cấp Bộ Thông tin và Truyền thông “Nghiên cứu, xây dựng thử nghiệm hệ thống xác thực nguồn gốc sản phẩm, hàng hóa ứng dụng blockchain.”. Mã số 022.18
2. Website: ezcheck.vn
3. Website: vnptcheck.vn