**Báo cáo app bgri-dự án bkc lab**

**Chương 1: Mở đầu**

* 1. **Vấn đề thực phẩm hiện nay.**

Xã hội phát triển, cùng với đời sống ngày càng được nâng cao. Các nhu cầu thiết yếu của con người ngày càng được cải thiện và nâng cao. Trong đó nhu cầu ăn uống luôn là nhu cầu được con người quan tâm nhất. Giờ đây không chỉ còn là ăn no, mà ăn sao phải thật ngon, thật bổ dưỡng. Nhu cầu ăn uống tăng cao thì vấn đề vệ sinh an toàn thực phẩm hiện nay lại càng trở lên báo động hơn bao giờ hết. Trong những năm gần đây, vấn đề an toàn thực phẩm của Việt Nam đang trở lên đáng báo động hơn bao giờ hết đặc biệt là tại các khu vự đô thị.

Trong cuộc sống, sức khỏe là thứ tài sản quý giá nhất của mỗi con người. Mỗi người sinh ra đều có riêng trong mình những mục đích, lý tưởng sống khác nhau. Nhưng bất cứ mục đích hay lý tưởng gì, chúng ta đều cần có một sức khỏe tốt để hiện thực hóa chúng. Đó là lý do sức khỏe luôn là thứ quan trọng nhất của mỗi con người. Do đó vấn đề ATTP ngày trở thành các vấn đề nóng được nhiều người quan tâm. Thực phẩm không an toàn, không rõ nguồn gốc đang trực tiếp đe dọa đến sức khỏe của người tiêu dùng. Việc sử dụng các thực phẩm độc hại, người tiêu dùng phải trả giá quá đắt bằng chính sức khỏe, thậm chí cả tính mạng của mình. Theo báo cáo từ cơ quan chức năng trình báo lên chính phủ, sau hai năm thực hiện chỉ thị 13 từ năm 2017, tiêu chí đảm bảo an toàn thực phẩm đã được đưa vào một trong các tiêu chí xây dựng nông thôn mới đã tập trung giải quyết dứt điểm các vấn đề nóng gây bức xúc trong xã hội. Tư năm 2017 đã không còn xuất hiện các mẫu thịt nhiễm Salbutamol, các thực phẩm vi phạm các tiêu chí về kháng sinh giảm mạnh. Năm 2019 toàn quốc ghi nhận 76 vụ ngộ độc thực phẩm làm gần 2000 người mắc, hơn 1918 người nhập viện và 9 trường hợp tử vong. So với năm 2008 số vụ giảm 32 vụ, số mắc giảm 1478 người. Số đi viện 1335 người, số tử vong giảm 9 người. Các thực phẩm không đảm bảo về chất lượng cũng như nguồn gốc không dõ dàng khiến cho người dùng hoang mang, khó có thể chọ những sản phẩm đảm bảo chất lượng. Hiện nay Việt Nam có trên 8 triệu hộ sản xuất nông nghiệp và hàng triệu hộ chế biến thực phẩm nhỏ lẻ. Mỗi hộ gia đình sản xuất một cách nhỏ lẻ tự phát. Tạo lên một ma trận trong việc cung cấp và chết biến thực phẩm. Để đạt được lợi nhuận tối đa, các hộ gia đình đã sử dụng thuốc kích thích trong trồng trọt, thức ăn tăng trọng trong chăn nuôi. Những hóa chất độc hại thuộc trong danh mục cấm cũng được đưa vào chế biến nông thủy sản và sử dụng nhiều loại chất tẩy trắng khử mùi nguy hiểm để biến thực phẩm ôi thui trở thành thực phẩm tiêu thụ ngoài thị trường. Ngoài ra quy trình chết biến không được quy định dõ dàng. Việc sản xuất tự phát dẫn đến môi trường không đảm bảo vệ sinh, sử dụng trực tiếp nước thải sinh hoạt trong trồng trọt và chế biến. Nước thải chăn nuôi chưa qua xử lý được mang trực tiếp để tưới rau, điều này khiến cho hàm lượng độc tố, kim loại nặng cùng với các vi sinh vật gây bệnh trong rau củ cao hơn so với quy định. Việc quy trình sản xuất không dõ dàng dẫn đến ảnh hưởng xấu đến hàng hóa của ta không thể xuất khẩu sang các nước có tính cạnh tranh cao như Mỹ, Nhật, Hàn…

Từ những phân tích trên, để nâng cao an toàn thực phẩm chúng ta cần có một quy trình dõ dàng từ khâu sản xuất đến khâu tiêu thụ. Các mô hình hợp tác xã đã được ra đời với quy trình kiểm soát khắt khe. Các nông sản sẽ được theo dõi ghi nhật kí từ lúc bắt đầu trồng cho đến lúc thu hoạch và đem đi tiêu thụ. Việc ghi chép hiện nay ở các hợp tác xã chủ yếu vẫn là ghi chép bằng tay. Điều này làm cho chi phí tăng lên rất cao. Khối lượng ghi chép lớn. Sự minh bạch tính chính xác là không thể chứng minh. Việc quản lí truy xuất nguồn gốc không thể thực hiện và vô cùng khó khăn. Từ đó bài toán số hóa quá trình sản xuất đã được đặt ra. Từ những nghiên cứu, để đảm bảo tính minh bạch chính xác của thông tin, dễ dàng truy xuất nguồn gốc cũng như trong việc quản lí truy vết nguồn gốc khi có vấn đề. Chúng tôi quyết định sử dụng công nghệ blockchain để giải quyết bài toán này.

* 1. **Mục tiêu của đề tài**

Mục tiêu xây dựng ứng dụng BKGri

1. Nghiên cứu công nghệ blockchain, nghiên cứu tiêu chuẩn VietGAP.
2. Xây dựng một quy trình sản xuất nông sản sạch hiệu quả, tối ưu nhất.
3. Áp dụng blockchain vào bài toán thực tế trong quy trình sản xuất nông sản sạch
4. Phân tích thiết kế hệ thống, cài đặt và triển khai hệ thống
5. Chạy thử nghiệm, đánh giá hệ thống, tối ưu hệ thống.
6. Định hướng phát triển sau này
   1. **Công nghệ sử dụng**
      1. **Thuật toán băm**

Trong môi trường mạng, chúng ta không còn xa lại gì với các mã hash. Vậy mã

hash là gì.

<hình>

Hash là thuật toán trong đó với mỗi đầu vào có độ dài, kích thước bất kì. Ta luôn

luôn nhận được đầu ra có độ dài xác định. Đó gọi làm hàm băm.

Một số hàm băm nổi tiếng hay dùng đó là MD5,SHA-1, SHA-2…

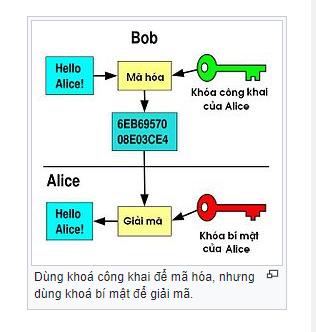
Hàm băm có tác dụng kiểm tra sự toàn vẹn của thông tin. Như chúng ta đã biết với cùng đầu vào có nội dung như nhau. Ta luôn nhận được một mã hash như nhau. Như vậy để tránh khi chúng ta tải các phần mềm mà chúng ta không biết nó có cài virut trong đó hay không. Ta sẽ băm phần mềm đó và so sánh với mã băm mà nhà sản xuất đưa ra. Nếu giống nhau thì ứng dụng đó đúng là từ nhà sản xuất và không bị thay đổi gì. Còn không đã có kẻ nào đó cố gắng cài hay thôi đổi gì đó trong ứng dụng.

* + 1. **Thuật toán mã hóa bất đối xứng.**

Trong mật mã học, chúng ta không còn xa lạ với thuật toán mã hóa bất đối xứng.

Trong đó người dùng sẽ có một cặp khóa gọi là khóa bí mật và khóa công khai. Người dùng có thể trao đổi thông tin mật với nhau mà không cần trao đổi khóa mật. Chúng ta có thể dùng khóa mật hoặc khóa công khai để mã hóa thông tin, và chúng ta cần khóa còn lại để giải mã.

<Hình>



Như trên hình trên ta thấy, giải sử người dùng Bob muốn gửi một thông điệp cho Alice. Hai người Bob và Alice sẽ trao đổi khóa công khai của mình. Sau đó người dùng Bob sẽ thực hiện mã hóa nội dung của mình bằng khóa công khai của Alice và gửi cho Alice. Alice nhận được bản mã sẽ sử dụng khóa bí mật của mình để giải mã đọc được nội dung Bob muốn gửi cho mình. Ngược lại nếu như Alice muốn gửi thông điệp cho Bob thì Alice sẽ mã hóa văn bản của mình với khóa công khai của Bob và gửi ngược lại cho Bob.

Các thuật toán bất đối xứng nổi tiếng hiện nay đang dùng là RSA và ECC. Các thuật toán được áp dụng rất nhiều trong đời sống như mã hóa, chữ kí số, truyền khóa bí mật … Mặc dù vậy mật mã khóa bất đối xứng có một nhược điểm lớn đó là kẻ tấn công có thể sửa đổi bản tin của Alice và Bob mà hai người không hề hay biết. Đó là hình thức tấn công kinh điển Man-in-the-middle.

<Hình>

Giả sử tình huống xảy ra, Alice muốn Bob trả tiền mình và chuyển vào số tài khoản viettinbank. Lúc này Alice sẽ gửi một thông báo mã hóa bằng thuật toán bất đối xứng RSA với nội dung như sau “Alice viettinbank 123456789”. Bằng một cách nào đó JAME là kẻ tấn công đã bắt được gói tin Alice chuyển cho Bob và không chuyển cho Bob nữa. JAME sẽ thay đổi nội dung gói tin là “Alice viettinbank 987654321”, mã hóa bằng khóa công khai của Bob và gửi gói tin đó cho Bob. Do không có cơ chế nào có thể biết gói tin đó có phải đến từ Alice hay không, Bob chỉ có thể giải mã bằng khóa bí mật của mình và thực hiện theo nội dung JAME đã thay đổi. Lúc này Bob đã bị lừa.

Để giải quyết vấn đề này chúng ta có thể sử dụng chữ kí điện tử được xây dựng dựa trên thuật toán bất đối xứng. Nội dung sau khi bị mã hóa, Alice sẽ đem đi hash nội dung mã hóa đó và mã hóa lại bằng khóa bí mật của mình. Khi gửi Alice sẽ gửi kèm bản mã và dãy chữ kí số đó. Bob sẽ dùng khóa công khai của Alice để giải mã chữ kí nhận được mã hash. Sau đó đem hash nội dung bản mã và so sánh với nhau. Nếu hai mã hash bằng nhau chứng tỏ nội dung chưa bị thay đổi.

* + 1. **Merkle tree**

Trong khoa học máy tính, chúng ta đều biết dạng cấu trúc dữ liệu cây. Vậy cây

merkle tree có gì đặc biệt. Chúng ta cùng theo dõi hình dưới đây.

<Hình>

Trong cây merkle tre, các nút lá T1,T2,T3,T4 đại diện cho dữ liệu cần lưu trữ. Các nút H1,H2.H3,H4 là các mã hash của các nút lá. Các nút cha là mã hash của các nút con của nó gộp vào. Mã hash cuối cùng ta được gọi là gốc của cây merkle tree.

Cây merkle tree có lợi ích lớn cho phép chứng minh tính toàn vẹn và hợp lệ của dữ liệu. Giúp ta có thể kiểm tra sự thay đổi dù nhỏ nhất một cách dễ dàng. Giả sử ta có T1 thay đổi, như vậy mã hash H1 cũng thay đổi và H(H1|| H2) cũng thay đổi. Và cuối cùng hash root cũng thay đổi.

* + 1. **Công nghệ máy chủ**

Năm 2020 chúng ta không còn xa lại với nodejs. Nodejs được xây dựng dựa trên

ngôn ngữ mà bất kì lập trình viên nào cũng đều biết đó là javascript. Từ đó chúng ta có thể dễ dàng xây dựng ứng dụng web một cách đơn giản và dễ dàng mở rộng. Ngoài ra nodejs có các thư viện web3js được phát triển rất tốt để tương tác với blockchain. Ngoài ra nodejs dễ dàng giúp cho chúng ta có thể xử lý bất đồng bộ một cách dễ dàng.

Framework sử dụng là express. Đây là web framework phổ biến nhất được viết bằng javascript và chạy trên môi trường nodejs. Nó rất linh hoạt, cung cấp đầy đủ các tính năng mạnh mẽ để phát triển mọi nền tảng từ web đến app mobie. Express có một cộng đồng hỗ trợ rộng lớn và vô số các thư viện đã được xây dựng rất hoàn chỉnh và đầy đủ. Ngoài ra tuy là một framework nhẹ nhưng performance của nó rất cao. Không thua kém các framework khác.

* + 1. **Công nghệ máy khách**

Với việc bùng nổ các thiết bị di động. Cùng sự tiện lợi gọn nhẹ dễ sử dụng. Rất phù

hợp với việc ghi nhất kí, kiểm tra nguồn gốc … Chúng tôi quyết định xây dựng ứng dụng trên thiết bị di động. Điều này giúp cho người dùng dễ dàng thao tác mọi lúc mọi nơi mà không cần cầm theo chiếc máy tính cồng kềnh. Công nghệ sử dụng ở đây chúng tôi chọn react native.

Được phát triển bởi gã khổng lồ facebook, react native là một framework hướng đến phát triển các ứng dụng di động. Với react native, chúng ta không cần quan tâm ứng dụng của ta chạy trên thiết bị android hay IOS. Chỉ cần viết một lần và dễ dàng chạy trên hai nền tảng.

React native hoạt động nhờ tích hợp 2 thread là Main Thread và JS Thread cho ứng dụng mobie. Trong đó:

* Main Thread : cập nhật giao diện người dùng(UI) và xử lý tương tác người dùng
* JS Thread: thực thi và xử lý code javascript

Hai luồng main thread và js thread hoạt động độc lập với nhau. Hai thread sẽ tương tác với nhau nhờ một bridge( cầu nối). Chiếc cầu này sẽ chuyển đổi qua lại giữa các thread.

Ưu điểm:

* Việc có thể build và chạy trên 2 nền tảng android và ios. Các developer có thể dễ dàng tái sử dụng code.
* Thay vì phải thuê 2 developer IOS và Android thì ta chỉ cần 1 developer. Từ đó giúp cho chi phí phát triển giảm xuống. Tận dụng nguồn nhân lực tốt hơn.
* Có một cộng đồng lớn, theo như khảo sát trên toàn thế giới. React native được đánh giá là một trong những framework được yêu thích nhất.
* Được ông lớn facebook phát triển, react native có tính ổn định khá cao. Việc viết mã code đơn giản.
* Rất phù hợp với các app gọn nhẹ.
  + 1. **Công nghệ lưu trữ.**

**1.3.7 Mạng ngang hàng peer-to-peer**

**1.3.8 Công nghệ chuỗi khối**

Năm 2020 là năm của sự bùng nổ công nghệ với sự ra đời của 5G, trí tuệ nhân tạo… Chúng ta không còn xa lạ với công nghệ chuỗi khối(blockchain) với các dự án đầy tham vọng của các quốc gia tổ chức trên khắp thế giới như tiền điện tử nhân dân tệ của Trung Quốc, hay Libra của facebook…Blockchain là công nghệ lưu trữ dữ liệu phi tập chung, trong đó dữ liệu sẽ được lưu trữ trong các khối có kích thước cố định. Mỗi khối được sinh ra sẽ chứa thông tin về khối trước nó. Từ đó việc thay đổi dữ liệu một khối cần thay đổi toàn bộ các khối trước nó, điều này khiến cho dữ liệu lưu trữ trên blockchain không dễ thay đổi. Blockchain được xây dựng để đảm bảo chống lại việc thay đổi dữ liệu. Khi một khối được tạo ra sẽ cần sự chấp thuận của toàn mạng bằng thuật toán đồng thuận. Điều này khiến cho một khối khi đã được chấp thuận thêm vào chuỗi, sẽ không thể thay đổi. Blockchain gồm các phần chính sau:

* Khối (block)
* Chuỗi khối (block chain)
* Thuật toán đồng thuận
* Mạng blockchain
  + - 1. **Khối (block)**

Mỗi khối sẽ có kích thước nhất định. Trong mỗi khối sẽ gồm 2 phần chính là block header và danh sách các giao dịch.

Diagram

Description automatically generated

Block header: chứa thông tin của một block. Trong đó gồm 4 giá trị:

* Prev\_hash : Giá trị hash của block trước nó
* Timestamp: Thời gian tạo block
* Nonce: Là giá trị được thêm khối băm, đây là giá trị thể hiện độ khó mà các thợ đào bitcoin cần tìm ra.
* Tx\_root: Giá trị root của cây merkle tree

Danh sách các giao dịch (transaction)

* Trong blockchain, dữ liệu được lưu trữ và tổ chức theo cấu trúc cây merkle tree. Mỗi giao dịch sẽ là một nút lá của cây merkle tree. Các giao dịch sẽ được băm bằng một thuật toán hash. Các nút cha sẽ là mã hash của 2 node con gộp vào.

Diagram

Description automatically generated

**1.3.8.2 Chuỗi khối**

Trong blockchain, khi kích thước một khối đạt đến kích thước tối đa. Thì một block mới sẽ được tạo ra. Khối được tạo ra sẽ liên kết với khối trước đó bằng một hàm băm. Khối trước đó sẽ được băm bằng thuật toán băm và gắn vào block mới được tạo ra. Lúc này ra sẽ có một liên kết tạo thành một chuỗi. Nếu một khối thay đổi, giá trị băm sẽ thay đổi. Từ đó chúng ta sẽ có thể biết được rằng khối nào thay đổi.

Diagram

Description automatically generated

**1.3.8.3 Thuật toán đồng thuận**

Trong công nghệ blockchain, thuật toán đồng thuận là linh hồn của mạng blockchain. Nó giúp cho mạng blockchain đạt được sự đồng thuận trong quá trình tạo ra block và thêm vào chuỗi. Các thuật toán đồng thuận phổ biến hiện nay như proof of work (POS), proof of stake (POS)…

**1.3.8.3.1 Thuật toán POW**

POW là thuật toán đầu tiên được áp dụng vào công nghệ blockchain, và vẫn được rất nhiều mạng sử dụng. Nổi tiếng nhất phải kể đến mạng bitcoin. Trong đó những người tham gia vào mạng blockchain được gọi là miner. Các miner cần giải một bài toán có độ khó nhất định để có thể tạo khối và thêm vào chuỗi. Để giải được bài toán và nhận được phần thưởng, các miner cần sử dụng tài nguyên như phần cứng, tiền điện … để có thể tạo ra block. Khi có nhiều người tham gia làm miner, thời gian giải bài toán sẽ nhanh hơn. Khi đó độ khó bài toán dành cho miner sẽ được tăng lên, điều này đảm bảo tạo ra một block luôn trong khoảng 10 phút. Độ khó của thuật toán sẽ thay đổi sau mỗi 2016 block, thời gian ước lượng khoảng 2 tuần. Thuật toán POW đã chạy từ năm 2009, nó có những ưu nhược điểm sau.

* Ưu điểm: Là một thuật toán đồng thuật đầu tiên được áp dụng trong blockchain và nó vẫn chạy rất tốt cho đến bây giờ
* Nhược điểm: POW có thời gian tạo ra block khá chậm (khoảng10 phút). Điều này không phù hợp với sự phát triển ứng dụng DApp chạy trên blockchain. Chi phí để tạo ra một block quá tốn kém, tiêu tốn tài nguyên thiên nhiên.

**1.3.8.3.2. Thuật toán POS**

Từ hạn chế của thuật toán POW, thuật toán POS đã được ra đời. Thay vì các miner phải cạnh tranh nhau để tạo ra block và được chấp nhận thêm vào chuỗi. POS sẽ giúp cho chúng ta không cần quá tốn kém trong cuộc chạy đua tạo ra block đó. Thay vì ai cũng có thể trở thành miner, POS yêu cầu mỗi miner cần đóng góp số coin để trở thành miner. Ai nắm giữ lượng cổ phần cao nhất sẽ có khả năng trở thành miner. Khi đó những miner được chọn sẽ trở thành validator cùng nhau tham gia vào quá trình tạo ra block. Khi bắt đầu tạo block, hệ thống sẽ chọn validator nắm cổ phần cao nhất để làm người tạo ra block. Sau khi block được tạo ra, block sẽ được gửi cho tất cả các validator để confirm và vote. Nếu như block được chấp nhận và gắn vào chuỗi. Một phần thưởng sẽ được trao cho người tạo block. Validator tạo block sẽ chia phần thưởng cho những người vote cho mình. Ngược lại , nếu như block bị loại, hay validator cố tình tạo ra block rác. Block đó sẽ được hủy bỏ ra khỏi mạng, validator sẽ mất lượng coin đóng góp( cổ phần). POS có ưu và nhược điểm như sau.

* Ưu điểm: Tiết kiệm năng lương, chi phí. Tốn nhiều chi phí để tấn công hơn.
* Nhược điểm: Hiện tại không có nhược điểm gì. Các mạng đang chạy thuật toán này phổ biết nhất là Ethereum, Peercoin,…

**1.3.8.3.3 Thuật toán đồng thuận Delegated Proof Of Stake.**

Thuật toán Delegated proof of stake( DPOS) là một thuật toán có thể nói mới nhất và tốt nhất hiện nay. Nó gần giống với DPOS nhưng nó thể hiện tính dân chủ hơn. Với POS người nào đóng góp nhiều cổ phần nhất sẽ trở thành validator. Điều này làm cho quyền lực tạo ra block luôn luôn nằm trong tay một số cá nhân. Hay nói cách khác quyền lực luôn làm trong tay người giàu. Để giải quyết vấn đề này DPOS đã ra đời với hệ thống bầu cử dân chủ hơn. Đầu tiên hệ thống sẽ bầu lên 21 người tạo khối. Hai mươi người đầu tiên được chọn từ 20 người có số phiếu bầu cao nhất, một người còn lại sẽ được chọn ngẫu nhiên bởi hệ thống. Người tạo ra block lúc này phải đủ 2 yếu tố:

* Người có số phiếu cao thuộc trong top 20
* Phải có số token đủ lớn

Hai mươi một người được bầu lên sẽ thay phiên nhau tạo ra block sau mỗi 3 giây theo một vòng tròn.

**1.3.8.4 Smart contract (hợp đồng thông minh)**

Trong blockchain, smart contract là một hợp đồng được tạo cho phép thực hiện giao dịch giữa hai người một cách tự động mà không cần thông qua bên trung gian. Trong đời sống, để tăng tính tin cậy giữa giao dịch của hai bên. Chúng ta cần có một bên trung gian đáng tin cậy đứng ra thu xếp và chứng minh giao dịch của hai bên A và B là hợp lệ. Ví dụ khi một ông A cần mua một căn nhà của ông B. Ông B yêu cầu ông A đặt cọc trước một khoản tiền, để tránh bị lừa. Ông A sẽ sử dụng một bên trung gian có pháp lí, quyền lực như ngân hàng . Ông A sẽ gửi tiền vào tài khoản ông B. Ngân hàng sẽ tạm khóa giao dịch với khoản tiền đó, ông B chỉ có thể tiêu khi đã hoàn thành toàn bộ giấy tờ với ông A. Trong thế giới blockchain cũng vậy, do việc giao dịch trong mạng blockchain là ẩn danh. Để tăng tính tin cậy thì smart contract đã ra đời. Ông B chỉ có thể sử dụng số tiền khi thỏa mãn được các điều kiện đưa ra trong smart contract.

Smart contract được đưa ra lần đầu tiên bởi Nick Szabo vào năm 1993. Mặc dù các khái niệm và nguyên lí của nó đã được ông đưa ra vào năm 1993 nhưng tại thời điểm đó thế giới không đủ công nghệ và điều kiện để thực hiện nó. Mọi chuyện đã thay đổi khi công nghệ blokchain ra đời. Nó được phát triển mạnh mẽ khi mạng Ethereum xuất hiện và phổ biến với tất cả mọi người. Smart contract là một ứng dụng đã tận dụng toàn bộ điểm mạnh của blockchain lên nó có rất nhiều ưu điểm như.

* Mọi hợp đồng giao dịch đều thực hiện một cách tự động. Chúng ta không cần bên trung gian như ngân hàng , luật sư…
* Smart contract được xây dựng chạy trên blockchain, từ đó mọi dữ liệu của bạn không thể bị mất. Tăng sự minh bạch và chính xác của giao dịch. Mọi dữ liệu của bạn đều được an toàn, không một kẻ xấu nào có thể đánh cắp dữ liệu của bạn.
* Smart contract được viết bởi các ngôn ngữ lập trình. Mọi thứ đều được tự động hóa các điều kiện thỏa mã trong hợp đồng. Tiết kiệm công sức tiền bạc hàng nghìn tỉ đồng cho các công việc thủ công.
* Smart contract còn tránh sự sai sót lỗi do đánh máy của con người.
* Smart contract được ứng dụng rất nhiều trong lĩnh vực trong tương lai như tài chính ngân hàng, tiền điện tử, bầu cử, nhà đất…
* Mọi thứ rất minh bạch và không bị quản lí bởi bất kì bên thứ 3 nào.

* 1. **Tiêu chuẩn VietGAP**

**Chương 2: Phân tích thiết kế hệ thống**

**2.1 Đặc tả yêu cầu**

BKgri gồm 4 tác nhân:

* Quản lí liên nhóm
* Quản lí nhóm
* Nông dân
* Khách

|  |  |
| --- | --- |
| Tên | Vai trò |
| Quản lí liên nhóm | Người dùng quản lí liên nhóm sẽ có chức năng như sau:   * Quản lí các nhóm * Thêm nhóm * Xóa nhóm * Chấp nhận yêu cầu thiết lập mùa vụ của quản lí nhóm gửi lên * Chấp nhận kết thúc mùa vụ của quản lí nhóm gửi lên * Theo dõi nhật kí * Truy xuất nguồn gốc của sản phẩm |
| Quản lí nhóm | Người dùng quản lí nhóm có các chức năng sau:   * Thêm, xóa hộ dân * Thiết lập thông số nhật kí mùa vụ * Tạo hành động nhật kí * Kết thúc mùa vụ * Theo dõi nhật kí * Truy xuất nguồn gốc của sản phẩm |
| Nông dân | Người dùng nông dân có chức năng sau   * Thực hiện hành động theo yêu cầu của quản lí nhóm * Truy xuất nguồn gốc của sản phẩm |
| Khách | Người dùng khách có chức năng sau   * Truy xuất nguồn gốc sản phẩm |

**2.2. Phân tích chi tiết hệ thống**

**2.2.1 Danh sách các ca sử dụng**

Hệ thống có tổng cộng 11 ca sử dụng. Toàn bộ chi tiết được thể hiện bảng \_\_\_ dưới đây.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Tên ca sử dụng** | **Mô tả** | **Tác nhân tham gia** |
| UC-01 | Đăng ký | Người dùng sẽ đăng ký tài khoản của mình | Người dùng |
| UC-02 | Đăng nhập | Người dùng sử dụng tài khoản của mình để đăng kí vào hệ thống | Người dùng |
| UC-03 | Truy xuất nguồn gốc | Người dùng sau khi đăng nhập, sử dụng app để quét mã Qrcode để xem thông tin về sản phẩm | Người dùng |
| UC-04 | Thêm quản lí nhóm | Quản lí liên nhóm sẽ tạo nhóm, và lựa chọn một quản lí nhóm | Quản lí liên nhóm |
| UC-05 | Xóa quản lí nhóm | Quản lí liên nhóm sẽ xóa quản lí nhóm | Quản lí liên nhóm |
| UC-06 | Thêm hộ dân | Quản lí nhóm sẽ thêm hộ dân vào một mùa vụ. | Quản lí nhóm |
| UC-07 | Xóa hộ dân | Hộ dân sẽ bị xóa ra khỏi mùa vụ | Quản lí nhóm |
| UC-08 | Tạo mới một mùa vụ | Khi bắt đầu một mùa mới, quản lí nhóm sẽ tạo mới một mùa vụ | Quản lí nhóm |
| UC-09 | Ghi nhật kí | Quản lí nhóm sẽ tạo công việc và yêu cầu nông dân thực hiện | Quản lí nhóm |
| UC-10 | Kết thúc mùa vụ | Quản lí liên nhóm sẽ thực hiện kết thúc mùa vụ và xuất ra mã QRcode | Quản lí liên nhóm |
| UC-11 | Đăng xuất | Người dùng đăng xuất khỏi hệ thống | Người dùng |

**2.2.2 Đặc tả ca sử dụng**

Biểu đồ ca sử dụng tổng quan của hệ thống

<hình ca sử dụng tổng quan>

Có tất cả bốn tác nhân tham gia vào hệ thống là khách, nông dân, quản lí liên nhóm, quả lí nhóm. Trong đó khách là người dùng chưa đăng nhập vào hệ thống. Các chức năng mà khách có thể sử dụng là đăng nhập và truy xuất nguồn gốc. Tác nhân thứ 2 là nông dân. Nông dân có thể sử dụng các chứ năng là đăng nhập, truy xuất nguồn gốc và thực hiện hành động mà quản lí nhóm yêu cầu. Tác nhân thứ ba là quản lí nhóm. Quản lí nhóm có các chức năng đăng nhập, thêm mới nông dân vào mùa vụ, tạo mới mùa vụ , ghi nhật kí, truy xuất nguồn gốc. Tác nhân thứ bốn là quản lí liên nhóm, quản lí liên nhóm có các chức năng là đăng nhập, đăng xuất. Thêm một người làm quản lí nhóm, xóa quản lí nhóm, phê duyệt các thiết lập mùa vụ mà quản lí nhóm trình lên, kết thúc mùa vụ.

<Hình ca sử dụng đăng kí>

|  |  |
| --- | --- |
| Use case ID | UC-01 |
| Tên Use Case | Đăng ký |
| Tạo bởi | Trần Cảnh Tuấn |
| Ngày tạo | 25/12/2020 |

|  |  |
| --- | --- |
| Tên tác nhân | Khách |
| Mô tả | Ca sử dụng cho phép khách có thể tạo một tài khoản để sử dụng ứng dụng |
| Tiền điều kiện | Người dùng ấn vào nút tạo mới tài khoản |
| Hậu điều kiện | Ứng dụng hiển thị màn hình đăng kí |
| Luồng thực hiện | 1. Người dùng bật app 2. Một màn hình hiển thị yêu cầu đăng nhập 3. Người dùng ấn vào nút đăng kí 4. Một màn hình đăng kí được hiển thị 5. Người dùng nhập thông tin cần thiết 6. Sau khi nhập thông tin đầy đủ, người dùng ấn vào nút tạo mới tài khoản |
| Ngoại lệ | Thông tin điền không đúng theo quy định hoặc đăng kí thất bại. Hệ thống sẽ hiển thị lỗi cho người dùng |
| Tần số sử dụng | Trung bình |
| Quy tắc nghiệp vụ | Không có |
| Yêu cầu đặc biệt | Không có |
| Ghi chú | Không có |

<Hình ca sử dụng đăng nhập>

|  |  |
| --- | --- |
| Use case ID | UC-02 |
| Tên Use Case | Đăng nhập |
| Tạo bởi | Trần Cảnh Tuấn |
| Ngày tạo | 25/12/2020 |

|  |  |
| --- | --- |
| Tên tác nhân | Khách |
| Mô tả | Ca sử dụng cho phép tác nhân có thể đăng nhập vào hệ thống để sử dụng các chức năng của hệ thống |
| Tiền điều kiện | Người dùng ấn vào nút đăng nhập và yêu cầu được đăng nhập vào hệ thống. |
| Hậu điều kiện | Ứng dụng hiển thị giao diện tương ứng với quyền mà tài khoản đó đang được chỉ định  Ứng dụng cấp toàn bộ quyền phù hợp với tài khoản đăng nhập |
| Luồng thực hiện | 1. Người dùng bật app 2. Một màn hình hiển thị yêu cầu đăng nhập 3. Người dùng điền thông tin đăng nhập email và password 4. Người dùng ấn vào nút đăng nhập |
| Ngoại lệ | - Hệ thống sẽ thông báo khi tác nhân nhập sai thông tin tài khỏan. - Hoặc không đúng định dạng thông tin nhập bắt buộc |
| Tần số sử dụng | Trung bình |
| Quy tắc nghiệp vụ | Không có |
| Yêu cầu đặc biệt | Người dùng cần tạo tài khoản trước đó |
| Ghi chú | Không có |

<Hình truy xuất nguồn gooscs>

|  |  |
| --- | --- |
| Use case ID | UC-03 |
| Tên Use Case | Truy xuất nguồn gốc sản phẩm |
| Tạo bởi | Trần Cảnh Tuấn |
| Ngày tạo | 25/12/2020 |

|  |  |
| --- | --- |
| Tên tác nhân | Khách |
| Mô tả | Ca sử dụng cho phép truy xuất nguồn gốc bằng cách quét mã QRcode |
| Tiền điều kiện | - Người dùng mở ứng dụng bkgri app.  - Đăng nhập vào hệ thống |
| Hậu điều kiện | Ứng dụng hiển thị toàn bộ thông tin về sản phẩm ứng với Qrcode đó |
| Luồng thực hiện | 1. Người dùng bật app và đã đăng nhập thành công 2. Sau đó người dùng sẽ vào phần truy xuất nguồn gốc 3. Người dùng tiến hành quét mã Qrcode của một sản phẩm 4. App sẽ gửi yêu cầu đến server 5. Server thực hiện tìm kiếm thông tin về sản phẩm trên blockchain 6. App sẽ hiển thị kết quả từ server trả về |
| Ngoại lệ | Không có |
| Tần số sử dụng | Cao |
| Quy tắc nghiệp vụ | Không có |
| Yêu cầu đặc biệt | Người dùng cần đăng nhập thành công |
| Ghi chú | Không có |

<Hình Thêm quản lí nhóm>

|  |  |
| --- | --- |
| Use case ID | UC-04 |
| Tên Use Case | Thêm quản lí nhóm |
| Tạo bởi | Trần Cảnh Tuấn |
| Ngày tạo | 25/12/2020 |

|  |  |
| --- | --- |
| Tên tác nhân | Quản lí liên nhóm |
| Mô tả | Ca sử dụng cho phép thêm một người dùng làm quản lí nhóm |
| Tiền điều kiện | - Người dùng đăng nhập với quyền là quản lí liên nhóm |
| Hậu điều kiện | Hệ thống sẽ thay đổi quyền của người dùng với quyền của một quản lí nhóm |
| Luồng thực hiện | 1. Người dùng bật app và đã đăng nhập thành công với quyền của quản lí liên nhóm 2. Sau đó người dùng sẽ vào phần truy xuất nguồn gốc 3. Người dùng tiến hành quét mã Qrcode của một sản phẩm 4. App sẽ gửi yêu cầu đến server 5. Server thực hiện tìm kiếm thông tin về sản phẩm trên blockchain 6. App sẽ hiển thị kết quả từ server trả về |
| Ngoại lệ | Không có |
| Tần số sử dụng | Cao |
| Quy tắc nghiệp vụ | Không có |
| Yêu cầu đặc biệt | Người dùng cần đăng nhập thành công |
| Ghi chú | Không có |