BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC ĐÀ LẠT

KỶ YẾU
HỘI NGHỊ NGHIÊN CỨU KHOA HỌC SINH VIÊN
TRƯỜNG ĐẠI HỌC ĐÀ LẠT NĂM 2020

Tiểu ban 1: Công nghệ thông tin

Lâm Đồng, tháng 08 năm 2020

DANH SÁCH TRÌNH BÀY BÁO CÁO TẠI HỘI NGHỊ NGHIÊN CỨU KHOAHỌC SINH VIÊN TRƯỜNG ĐẠI HỌC ĐÀ LẠT NĂM 2020

Số TT	Tên đề tài	Họ và tên sinh viên	Lớp/ Khoa	Họ tên Giáo viên hướng dẫn	Trang
Tiểu ban CNTT (01 đề tài CNTT, 01 đề tài Viễn thông)					
1.	Xây dựng ứng dụng truy xuất nguồn gốc nông sản dựa trên công nghệ blockchain	La Quốc Thắng ***(Chủ nhiệm)*** Trần Trọng Hiệp Nguyễn Thành Quốc	CTK40/ Khoa Công nghệ Thông tin	TS. Trần Ngô Như Khánh	3
2.	Ổ cắm điện thông minh điều khiển qua mạng Intenet	Trần Thanh Dương ***(Chủ nhiệm)*** Đào Trọng Khôi Ksor Bớt Nguyễn Cao Đức Đào Trọng Khôi	VTK40/ Khoa Vật lý	KS. Võ Minh Phụng	81

BỘ GIÁO DỤC ĐÀO TẠO

TRƯỜNG ĐẠI HỌC ĐÀ LẠT

BÁO CÁO TỔNG KẾT

ĐỀ TÀI KHOA HỌC SINH VIÊN NĂM 2020

XÂY DỰNG ỨNG DỤNG TRUY XUẤT NGUỒN GỐC NÔNG SẢN DỰA TRÊN CÔNG NGHỆ BLOCKCHAIN

Thuộc nhóm ngành khoa học: Công nghệ Thông tin

Lâm Đồng, tháng 6/2020

BỘ GIÁO DỤC ĐÀO TẠO

TRƯỜNG ĐẠI HỌC ĐÀ LẠT

BÁO CÁO TỔNG KẾT

ĐỀ TÀI KHOA HỌC SINH VIÊN NĂM 2020

XÂY DỰNG ỨNG DỤNG TRUY XUẤT NGUỒN GỐC NÔNG SẢN DỰA TRÊN CÔNG NGHỆ BLOCKCHAIN

Thuộc nhóm ngành khoa học: Công nghệ Thông tin

Sinh viên thực hiện: La Quốc Thắng Giới tính: Nam
Dân tộc: Kinh
Lớp, khoa: CTK40, Khoa CNTT Năm thứ: 4 /Số năm đào tạo: 4.5
Ngành học: Kỹ thuật Phần mềm

Giảng viên Hướng dẫn: TS. Trần Ngô Như Khánh

Lâm Đồng, tháng 6/2020

DANH SÁCH THÀNH VIÊN

Sinh viên thực hiện:

STT	Mã số sinh viên	Họ và tên	Email
1	1610207	La Quốc Thắng	1610207@dlu.edu.vn
2	1610121	Trần Trọng Hiệp	1610121@dlu.edu.vn
3	1610191	Nguyễn Thành Quốc	1610191@dlu.edu.vn

Giảng viên hướng dẫn: TS. Trần Ngô Như Khánh

MỤC LỤC

DANH SÁCH HÌNH ẢNH v
DANH SÁCH BẢNG BIỂU vi
DANH SÁCH CHỮ VIẾT TẮT vii
MỞ ĐẦU 1
1. Tổng quan tình hình nghiên cứu liên quan đến đề tài 1
2. Lý do chọn đề tài 1
3. Mục tiêu đề tài 6
3.1. Về lý thuyết 6
3.2. Về ứng dụng 6
4. Phương pháp nghiên cứu 6
5. Đối tượng nghiên cứu 7
6. Phạm vi nghiên cứu 7
CHƯƠNG I. TỔNG QUAN VỀ BLOCKCHAIN 8
I.1. Giới thiệu chung 8
I.2. Lịch sử ra đời 8
I.3. Phân loại Blockchain 9
I.3.1. Blockchain mở 9
I.3.2. Blockchain đóng 10
I.4. Kiến trúc Blockchain 11
I.4.1. Hàm băm mật mã 11
I.4.2. Giao dịch 13
I.4.3. Mật mã khóa bất đối xứng 15
I.4.4. Địa chỉ 16
I.4.5. Sổ cái 17
I.4.6. Khối 17
I.4.7. Chuỗi khối 20
I.5. Một số mô hình đồng thuận phổ biến 1
I.6. Một số nền tảng dựa trên Blockchain hiện nay 4
I.6.1. Ethereum 4
I.6.2. Hyperledger Fabric 5

I.6.3. IBM Blockchain 5
I.6.4. Multichain 6
I.6.5. Hydrachain 6
I.6.6. OpenChain 7
I.6.7. BigchainDB 7
CHƯƠNG II. TỔNG QUAN VỀ BIGCHAINDB 9
II.1. Giới thiệu về BigchainDB 9
II.2. Đặc điểm của BigchainDB 9
II.2.1. Tính phi tập trung và Byzantine Fault Tolerance 9
II.2.2. Tính bất biến 11
II.2.3. Tài sản do chủ sở hữu kiểm soát 11
II.2.4. Tốc độ giao dịch cao 12
II.2.5. Độ trễ thấp & Hoàn thành nhanh 12
II.2.6. Lập chỉ mục & Truy vấn dữ liệu có cấu trúc 12
II.2.7. Sybil Tolerance 12
II.3. Ứng dụng của BigchainDB 12
CHƯƠNG III. TRIỂN KHAI ỨNG DỤNG 17
III.1. Phân tích nghiệp vụ hệ thống 17
III.1.1. Phân tích chuỗi cung ứng nông sản 17
III.1.2. Danh sách Actor 17
III.1.3. Danh sách Use Case 18
III.1.4. Phân tích sơ đồ đối tượng 20
III.2. Mô hình triển khai 21
III.2.1. Khối BigchainDB 22
III.2.2. Khối ứng dựng web 24
III.2.3. Khối ứng dụng di động 27
III.3. Kết quả 28
III.3.1. Khối BigchainDB 28
III.3.2. Khối ứng dụng web 30
III.3.3. Khối ứng dụng di động 36
KẾT LUẬN VÀ KIẾN NGHỊ 40
1. Kết luận 40
2. Hướng phát triển 41

TÀI LIỆU THAM KHẢO.....43
PHỤ LỤC THUẬT NGỮ 45

DANH SÁCH HÌNH ẢNH

Hình 1. Sản lượng cây ăn quả phân bố tại Đà Lạt và toàn tỉnh Lâm Đồng 2
Hình 2. Diện tích thu hoạch cây ăn quả tại Đà Lạt và toàn tỉnh Lâm Đồng 3
Hình 3. Ví dụ về giao dịch tiền điện tử 14
Hình 4. Ví dụ về một chuỗi khối chung 20
Hình 5. Logo Ethereum 4
Hình 6. Logo Hyperledger Fabric 5
Hình 7. Logo IBM Blockchain 6
Hình 8. Logo MultiChain 6
Hình 9. Logo HydraChain 7
Hình 10. Logo OpenChain 7
Hình 11. Logo BigchainDB 8
Hình 12. Bốn nhóm ứng dụng chính của BigchainDB 13
Hình 13. Sở hữu truyền phát nhạc với Resonate 14
Hình 14. Các chứng chỉ giáo dục được xác thực với công nghệ Recruit 14
Hình 15. Với Innogy, mỗi sản phẩm có một câu chuyện 15
Hình 16. Công ty đăng ký đất đai Blockchain tại Ghana tên BenBen 16
Hình 17. Chuỗi cung ứng nông sản 17
Hình 18. Sơ đồ đối tượng trong hệ thống truy xuất nguồn gốc nông sản 20
Hình 19. Sơ đồ minh họa mô hình triển khai 22
Hình 20. Sơ đồ giao tiếp giữa các nút trong mạng 23
Hình 21. Mô hình MVC bao gồm Model, View và Controller 24
Hình 22. Ví dụ về lớp Person trong Models 25
Hình 23. Ví dụ về lớp PersonController trong Controllers 26
Hình 24. View với cú pháp Razor 27
Hình 25. Logo của Ionic 27
Hình 26. Từng bước để xây dựng các ứng dụng di động 28
Hình 27. BigchainDB cung cấp API dùng thử nghiệm https://test.ipdb.io/ 29
Hình 28. Thông tin khi được gửi lên https://test.ipdb.io/ 29
Hình 29. Mạng BigchainDB được triển khai trên máy ảo pcvn.vn 30
Hình 30. Giao diện trang chủ 31
Hình 31. Giao diện trang đăng nhập 31
Hình 32. Giao diện tạo sản phẩm cho người sản xuất 32
Hình 33. Giao diện để người dùng thêm thông tin cho các vai trò khác bằng cách nhập mã sản phẩm 33
Hình 34. Giao diện để người dùng thêm các thông tin vào sản phẩm 34
Hình 35. Giao diện quản lý hiển thị những sản phẩm mà người dùng đã nhập thông tin 34
Hình 36. Giao diện trang đăng nhập cho admin 35
Hình 37. Giao diện trang quản lý tài khoản của admin 35
Hình 38. Giao diện trang quản lý những sản mà người dùng đã thêm và đưa vào blockchain 36
Hình 39. Màn hình chính của ứng dụng 37
Hình 40. Xem thông tin người trồng 37
Hình 41. Xem thông tin người vận chuyển 38
Hình 42. Xem thông tin người bán 39

DANH SÁCH BẢNG BIỂU

Bảng 1. Sản lượng cây ăn quả của các địa phương ở tỉnh Lâm Đồng 5
Bảng 2. Ví dụ về đầu vào và đầu ra tương ứng của một số hàm băm.....13
Bảng 3. Minh họa một số kết quả mã QR 17
Bảng 4. Một số mô hình đồng thuận trong Blockchain 3
Bảng 5. Mục tiêu thiết kế của BigchainDB 2.0 9
Bảng 6. Danh sách Actor.....18
Bảng 7. Danh sách Use Case.....19
Bảng 8. Bảng vai trò của các thành phần trong chuỗi cung ứng.....21

DANH SÁCH CHỮ VIẾT TẮT

STT	Chữ viết tắt	Tên đầy đủ	Chú giải
1	API	Application Programming Interface	Giao diện lập trình ứng dụng
2	AWS	Amazon Web Services	Dịch vụ Web Amazon
3	BFT	Byzantine Fault Tolerance	Dung sai lỗi Byzantine
4	DNS	Domain Name System	Hệ thống phân giải tên miền
5	HTTP	Hypertext Transfer Protocol	Giao thức truyền tài siêu văn bản
6	IoT	Internet of Things	Internet Vạn vật
7	IP	Internet Protocol	Giao thức Internet
8	PoET	Proof of elapsed time	Bằng chứng thời gian trôi qua
9	PoS	Proof of Stake	Bằng chứng Cổ phần
10	PoW	Proof of Work	Bằng chứng Công việc
11	QR	Quick Response	Mã phản hồi nhanh, mã QR, mã vạch hai chiều
12	REST API	Representational State Transfer Application Programming Interface	Giao diện lập trình ứng dụng chuyển trạng thái đại diện
13	TCP	Transmission Control Protocol	Giao thức Điều khiển Truyền vận

MỞ ĐẦU

Tổng quan tình hình nghiên cứu liên quan đến đề tài

Ngày nay, các đồng tiền điện tử đã trở nên phổ biến, thông dụng trên thế giới. Một trong những đồng tiền điện tử thành công nhất không thể không kể đến đó là Bitcoin. Với cấu trúc lưu trữ dữ liệu được thiết kế đặc biệt, các giao dịch trong mạng Bitcoin có thể xảy ra mà không cần bất kỳ bên thứ ba, và cốt lõi công nghệ để xây dựng nên Bitcoin chính là Blockchain, được đề xuất vào năm 2008 và triển khai vào năm 2009 [1].

Blockchain – Công nghệ chuỗi khối – có thể được xem như một cuốn sổ cái công khai, chống giả mạo và tất cả các giao dịch được lưu trữ trong một danh sách các khối. Chuỗi này liên tục được phát triển khi các khối mới được thêm vào. Với hàm mật mã bất đối xứng và cơ chế đồng thuận phân tán đã làm cho Blockchain bảo mật, nhất quán hơn các cuốn sổ cái truyền thống.

Vì khả năng cho phép hoàn thành thanh toán mà không cần bất kỳ ngân hàng hay trung gian nào, Blockchain được dùng trong các dịch vụ tài chính khác nhau như tài sản kỹ thuật số, chuyển tiền hay thanh toán. Thêm vào đó, nó còn có thể áp dụng cho các lĩnh vực khác như hợp đồng thông minh, dịch vụ công cộng, Internet vạn vật, hệ thống danh tiếng và dịch vụ bảo mật [1].

Lý do chọn đề tài

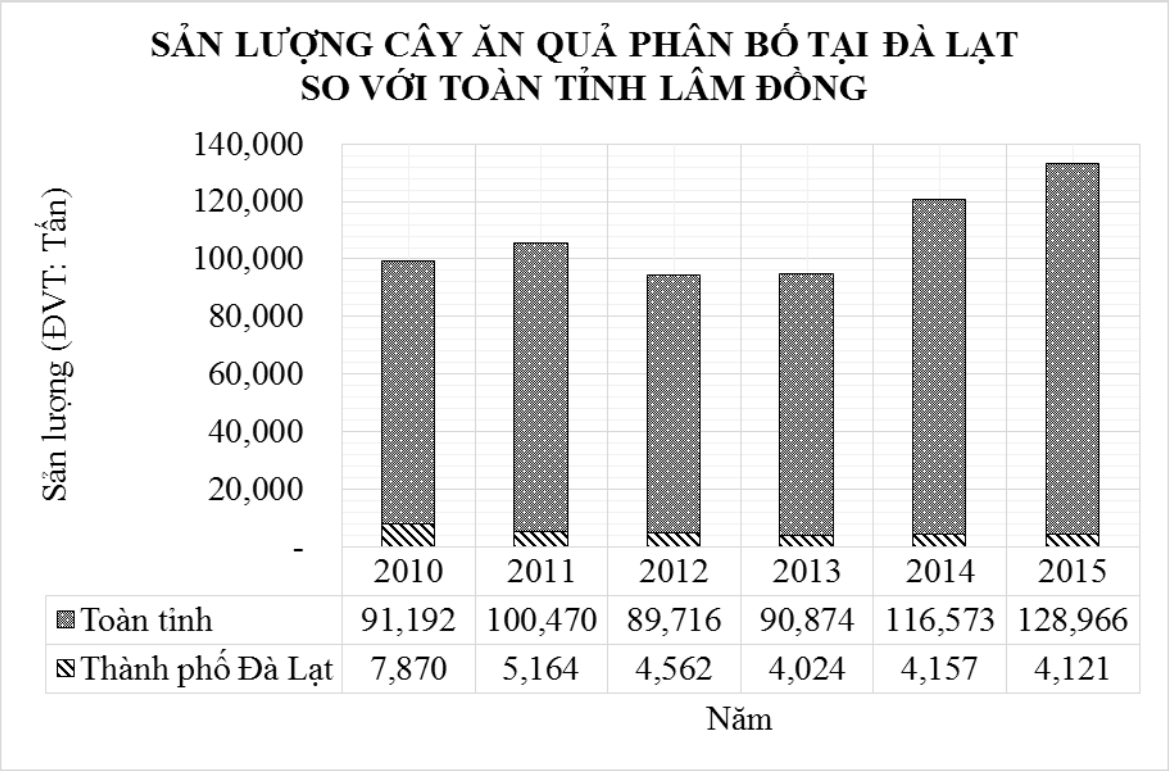
Do sự phát triển không ngừng của xã hội, các nhu cầu về cuộc sống con người được nâng cao. An toàn vệ sinh thực phẩm đang ngày càng trở thành vấn đề cấp bách không chỉ riêng Việt Nam mà còn là mối quan tâm hàng đầu của toàn thế giới. Bên cạnh đó, các thông tin nguồn gốc xuất xứ của thực phẩm cũng cần phải được minh bạch, rõ ràng.

Chính vì vậy mà giải pháp truy xuất nguồn gốc dựa trên nền tảng Blockchain đang rất được quan tâm vì nó mang lại sự minh bạch trong thông tin sản phẩm cũng như là khả năng phân tán nhằm hạn chế rủi ro xảy ra trên một địa điểm.

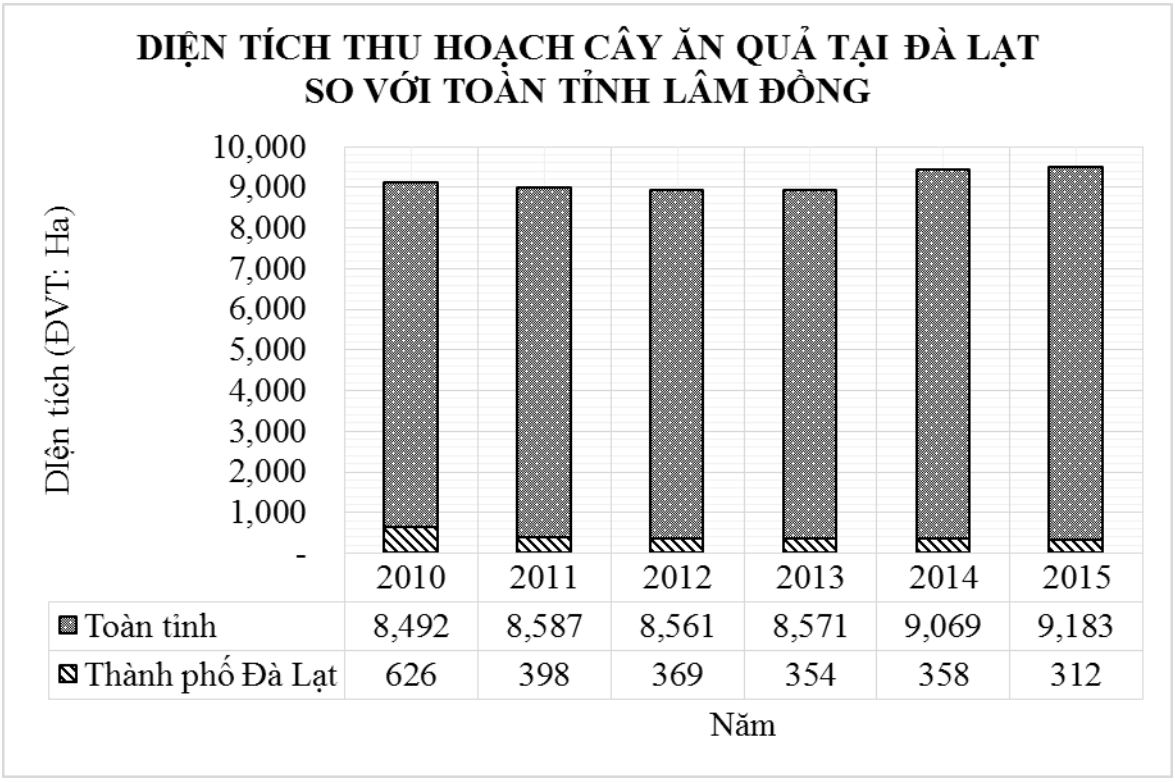
Đã có một số mô hình thử nghiệm dựa trên nền tảng Blockchain trong truy xuất nguồn như dự án "*Hỗ trợ Nông sản Việt Nam xây dựng nhận diện thương hiệu toàn cầu* [2]" với sự tài trợ của Đại sứ quán Úc tại Việt Nam đã được triển khai thí điểm trên chuỗi thanh long xuất khẩu sang thị trường Úc. Những lô hàng thanh long đầu tiên được cấp phép xuất khẩu sang Úc vào tháng 9/2017 [3] đã đánh dấu bước tiến

mới của ngành nông nghiệp Việt Nam trong việc mở rộng thị trường tiêu thụ. Ngoài quả thanh long, nông sản tiếp theo được áp dụng phổ biến là quả xoài của Hợp tác xã Mỹ Xương (Đồng Tháp) [4]. Như vậy, việc áp dụng Blockchain vào truy xuất nguồn gốc là hoàn toàn khả thi.

Để làm rõ hơn về nhu cầu truy xuất nguồn gốc nông sản ở địa phương hiện nay sẽ lấy ví dụ về tình hình nông sản ở Lâm Đồng nói chung và thành phố Đà Lạt nói riêng. Hai hình dưới đây thể hiện sản lượng và diện tích thu hoạch cây ăn quả tại thành phố Đà Lạt và một số địa phương khác thuộc tỉnh Lâm Đồng từ năm 2010 đến 2015 [5]:



Hình 1. Sản lượng cây ăn quả phân bố tại Đà Lạt và toàn tỉnh Lâm Đồng



Hình 2. Diện tích thu hoạch cây ăn quả tại Đà Lạt và toàn tỉnh Lâm Đồng

(ĐVT: Tấn)

Địa phương	2010	2011	2012	2013	2014	2015
1. Thành phố Đà Lạt	7,870	5,164	4,562	4,024	4,157	4,121
2. Thành phố Bảo Lộc	4,550	3,998	4,069	5,538	6,583	6,671
3. Huyện	1	1,	1	1	2,	2,

Đam Rông	,200	369	,785	,951	183	342
4. Huyện Lạc Dương	3,452	3,487	3,753	4,121	4,3444	4,5587
5. Huyện Lâm Hà	8,176	9,4177	7,986	6,461	8,7844	9,5211
6. Huyện Đơn Dương	26,160	25,702	19,687	15,401	15,6999	15,3188
7. Huyện Đức Trọng	8,500	13,679	11,297	14,156	16,8177	21,0888
8. Huyện Di Linh	3,57	6,652	6,36	6,82	7,3778	8,0177

	5		1	5		
9. Huyện Bảo Lâm	9,016	11,634	10,058	11,212	23,731	28,181
10. Huyện Đạ Huoai	13,573	14,645	13,533	14,044	19,182	20,177
11. Huyện Đạ Tẻh	2,720	2,295	3,221	3,553	3,968	4,686
12. Huyện Cát Tiên	2,400	2,429	3,405	3,587	3,747	4,257
Toàn tỉnh	**91,192**	**100,470**	**89,716**	**90,874**	**116,573**	**128,966**

Bảng 1. Sản lượng cây ăn quả của các địa phương ở tỉnh Lâm Đồng

Dựa vào Hình 1, Hình 2 và Bảng 1, có thể thấy sản lượng cây ăn quả toàn tỉnh có chiều hướng tăng lên khá rõ rệt. Đó là minh chứng cho thấy thị trường nông sản tại tỉnh Lâm Đồng phát triển theo chiều hướng tích cực. Nếu có thể áp dụng hệ thống truy xuất nguồn gốc này cho một số địa phương ở trên, bắt đầu từ phạm vi nhỏ trước, thì sau các năm, quy mô hệ thống có thể tăng lên cùng với sản lượng nông sản.

Mục tiêu đề tài

1.1. Về lý thuyết

Tìm hiểu lịch sử hình thành và phát triển của công nghệ chuỗi khối - Blockchain. Hiểu được kiến trúc và hoạt động cơ bản của nền tảng Blockchain, các cơ chế đồng thuận trong Blockchain. Khảo sát và phân tích ưu nhược điểm một số nền tảng điển hình của Blockchain hiện nay trong thực tiễn để chọn lựa nền tảng xây dựng ứng dụng truy xuất nguồn gốc nông sản.

1.2. Về ứng dụng

Xây dựng và triển khai ứng dụng truy xuất nguồn gốc nông sản dựa trên một nền tảng Blockchain mã nguồn mở (cụ thể là BigchainDB) để đáp ứng nhu cầu thực tế hiện tại. Hệ thống được phát triển trên nền tảng kết hợp các công nghệ phát triển ứng dụng web và di động mới nhất, cùng với công nghệ điện toán đám mây để thiết kế và phát triển hệ thống truy xuất nguồn gốc nông sản hướng tới việc minh bạch trong nguồn gốc xuất xứ sản phẩm, tạo niềm tin tiêu dùng. Người tiêu dùng chỉ cần quét mã QR được dán trên nông sản là có thể tiếp cận được thông tin chi tiết về nguồn gốc, xuất xứ và quá trình vận chuyển, cung cấp của nông sản.

Phương pháp nghiên cứu

Đề tài này sử dụng phương pháp nghiên cứu chủ yếu là phương pháp phân tích và tổng kết kinh nghiệm.

Phương pháp phân tích và tổng kết kinh nghiệm là phương pháp nghiên cứu xem xét lại những thành quả của hoạt động thực tiễn trong quá khứ để rút ra những kết luận bổ ích cho thực tiễn và cho khoa học. Tổng kết kinh nghiệm thường thường hướng vào nghiên cứu diễn biến và nguyên nhân của các sự kiện và nghiên cứu giải pháp thực tiễn đã áp dụng để tìm ra các giải pháp hoàn hảo nhất [6].

Chính vì vậy mà phương pháp này thường được sử dụng cho các mục đích sau:

- Tìm hiểu bản chất, nguồn gốc, nguyên nhân và cách giải quyết các vấn đề trong cuộc sống.
- Nghiên cứu con đường thực hiện có hiệu quả cách giải quyết trên.
- Tổng kết các sáng kiến của các những người đi trước.
- Tổng kết những nguyên nhân, để loại trừ những sai lầm, thất bại trong hoạt động.
- Tổng kết kinh nghiệm mang tính quần chúng rộng rãi.

Cụ thể, từ việc khảo sát và phân tích nhu cầu về ứng dụng quản lý truy xuất nguồn gốc nông sản cũng như các ứng dụng, công cụ hiện có, đề tài đề xuất mô hình hệ thống và xây dựng, phát triển ứng dụng.

Đối tượng nghiên cứu

Đối tượng nghiên cứu của đề này là công nghệ chuỗi khối - Blockchain, cụ thể là nền tảng mã nguồn mở BigchainDB và các công nghệ phát triển ứng dụng web, di động. Tận dụng các đặc trưng của Blockchain trong cơ sở dữ liệu để lưu trữ thông tin về nguồn gốc nông sản, sau đó áp dụng trên một số loại nông sản của thành phố Đà Lạt để thực nghiệm.

Phạm vi nghiên cứu

Phạm vi nghiên cứu của đề tài này ứng dụng truy xuất nguồn gốc nông sản trong khu vực thành phố Đà Lạt, tập trung chủ yếu ở các nông trại đang canh tác và quản lý theo cách truyền thống, chưa ứng dụng công nghệ thông tin trong việc quản lý quá trình sản xuất, vận chuyển và cung cấp nông sản đến người tiêu dùng.

Về chức năng, đề tài này chủ yếu tập trung thử nghiệm quy trình truy xuất nguồn gốc nông sản thực thông qua quét mã QR với các thông tin được lưu trữ trong cơ sở dữ liệu BigchainDB dựa trên công nghệ Blockchain.

CHƯƠNG I. TỔNG QUAN VỀ BLOCKCHAIN

I.1. Giới thiệu chung

Blockchain là cuốn sổ cái kỹ thuật số chống giả mạo[1] được triển khai theo mô hình phân tán (tức là không có kho lưu trữ trung tâm) và thường không cần một đơn vị đáng tin cậy chứng thực (như ngân hàng, công ty, chính phủ). Ở mức độ cơ bản, nó cho phép một cộng đồng người dùng ghi các giao dịch vào cuốn sổ cái chia sẻ, mà trong đó, với sự điều hành bình thường của mạng Blockchain thì không giao dịch nào có thể bị thay đổi sau khi xuất bản. Vào năm 2008, ý tưởng Blockchain được kết hợp với một vài công nghệ và khái niệm điện toán khác để tạo ra đồng tiền mã hóa hiện đại: tiền điện tử được bảo vệ bởi các cơ chế mật mã học thay vì nhờ vào bên chứng thực hoặc kho lưu trữ trung tâm.

Công nghệ này được biết đến rộng rãi vào năm 2009 với sự ra đời của mạng Bitcoin – một trong những đồng tiền mã hóa hiện đại đầu tiên. Ở hệ thống Bitcoin và các hệ thống tương tự, việc chuyển thông tin kỹ thuật số với đại diện là tiền điện tử diễn ra trong một hệ thống phân tán. Người dùng Bitcoin có thể ký chữ ký số và chuyển tài sản của mình sang người khác và Bitcoin ghi lại các giao dịch này công khai, cho phép những người tham gia mạng xác minh độc lập tính hợp lệ của giao dịch. Công nghệ Blockchain do đó được xem là giải pháp chung cho các đồng tiền mã hóa sau này.

Blockchain có thể được định nghĩa thông thường như sau:

"Blockchain là cuốn sổ cái kỹ thuật số của các giao dịch được ký bằng mật mã. Mỗi khối được liên kết mã hóa với khối trước nó sau khi được xác thực thì trải qua một quyết định đồng thuận. Khi một khối mới thêm vào, khối cũ hơn trở nên khó bị chỉnh sửa. Cuốn sổ cái sau đó được sao chép đến toàn bộ mạng và bất kỳ xung đột nào được giải quyết tự động thông qua các quy tắc được thiết lập."

I.2. Lịch sử ra đời

Ý tưởng chính đứng sau công nghệ Blockchain này nổi lên vào cuối những năm 1980, đầu năm 1990. Vào năm 1989, Leslie Lamport[2] đã phát triển giao thức Paxos.

[1] Nguyên văn tiếng Anh là "Blockchains are tamper evident and tamper resistant digital ledgers"

[2] Leslie B. Lamport là một nhà khoa học máy tính người Mỹ. Lamport được biết đến nhiều nhất với công việc tinh thần của mình trong các hệ thống phân tán.

Năm 1990, ông có bài báo *The Part-Time Parliament*[1] được gửi đến *ACM Transaction on Computer Systems*; bài báo được phát hành cuối cùng vào một số của năm 1998. Bài báo miêu tả một mô hình đồng thuận giúp đạt được thỏa thuận trên một kết quả của mạng lưới máy tính – nơi mà các máy tính hoặc bản thân mạng có thể không ổn định. Năm 1991, một chuỗi thông tin được ký đã được dùng như một cuốn sổ cái điện tử cho các tài liệu có chữ ký kỹ thuật số theo cách mà không dễ dàng để tài liệu được ký nào bị thay đổi. Các khái niệm này được kết hợp và áp dụng vào tiền điện tử năm 2008 và được miêu tả trong bài báo – *Bitcoin: A Peer to Peer Electronic Cash System*[2] – được xuất bản giả bởi Satoshi Nakamoto[3], và sau đó năm 2009 với sự ra đời của tiền điện tử Bitcoin [7].

Việc sử dụng Blockchain cho phép Bitcoin được triển khai theo kiểu phân tán, như vậy không có người dùng đơn lẻ điều khiển được tiền điện tử và không có khuyết điểm tồn tại đơn lẻ. Lợi ích chính là cho phép các giao dịch trực triếp giữa những người dùng mà không cần bên thứ ba đáng tin cậy. Nó cũng cho phép phát hành tiền mới theo cách được định nghĩa đến những người quản lý việc xuất bản các khối mới và duy trì bản sao của sổ cái, thì những đó được gọi là các *miner* ở Bitcoin. Bằng cách sử dụng cơ chế đồng thuận để duy trì và một cơ chế tự kiểm soát được tạo ra để đảm bảo rằng chỉ có các giao dịch và các khối hợp lệ mới được thêm vào Blockchain.

I.3. Phân loại Blockchain

Mạng Blockchain có thể phân loại dựa trên mô hình quyền hạn của nó mà xác định ai có thể duy trì chúng (chẳng hạn xuất bản các khối). Nếu bất kỳ ai có thể xuất bản một khối mới, gọi là *Blockchain mở*. Nếu chỉ có những người dùng cụ thể xuất bản các khối, gọi là *Blockchain đóng*. Hiểu đơn giản, một mạng Blockchain đóng giống như một mạng Intranet của tổ chức, trong khi đó Blockchain mở lại giống như mạng Internet công cộng vậy.

I.3.1. Blockchain mở

Mạng Blockchain mở là nền tảng sổ cái phi tập trung mở rộng đến bất kì ai muốn xuất bản các khối mà không cần quyền chứng thực nào cả. Nền tảng Blockchain mở thường là phần mềm mã nguồn mở, có sẵn miễn phí cho mọi người

[1] Chi tiết bài báo có thể xem ở đây: https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf
[2] Chi tiết bài báo có thể xem ở đây: https://bitcoin.org/bitcoin.pdf
[3] Satoshi Nakamoto (中本哲史) là một nhân vật hoặc tổ chức ẩn danh đã sáng tạo ra Bitcoin.

muốn tải xuống. Bởi vì bất kỳ ai đều có quyền xuất bản các khối, nên kết quả là bất kỳ ai cũng có thể đọc Blockchain cũng như là phát hành các giao dịch trên Blockchain (các giao dịch nằm trong các khối được xuất bản). Người dùng có ý đồ xấu có thể xuất bản các khối nhằm đánh sập hệ thống. Để ngăn chặn điều này, mạng Blockchain mở thường triển khai các thỏa thuận đa bên hay còn gọi là hệ thống "đồng thuận", yêu cầu người dùng chi tiêu hoặc duy trì tài nguyên khi muốn xuất bản các khối. Đồng thời, hệ thống "đồng thuận" thường thúc đẩy các hành vi đúng đắn thông qua việc trao thưởng cho các nhà xuất bản các khối tuân thủ giao thức với loại tiền điện tử tương ứng.

I.3.2. Blockchain đóng

Mạng Blockchain đóng là nền tảng sổ cái, nơi mà người dùng xuất bản các khối phải được chứng thực bởi cơ quan nào đó (làm cho nó tập trung hoặc phi tập trung). Bởi vì chỉ có người dùng được chứng thực là có thể duy trì Blockchain nên có có thể hạn chế quyền tiếp cận và hạn chế những ai có thể phát hành các giao dịch. Do đó, Blockchain đóng có thể quy định bất kỳ ai có thể đọc hoặc phải chứng thực để đọc được. Ngược lại, bất kỳ ai cũng có thể phát hành giao dịch hoặc hạn chế chỉ những cá nhân được chứng thực từ trước. Blockchain đóng có thể khởi tạo và duy trì bằng phần mềm mã nguồn mở hoặc đóng.

Mạng Blockchain đóng và Blockchain mở có thể giống nhau ở các đặc điểm: khả năng truy xuất tài sản kỹ thuật số trên Blockchain; hệ thống phân tán; phục hồi và lưu trữ dữ liệu dự phòng; các mô hình đồng thuận; có hoặc không có chi tiêu và duy trì tài nguyên. Trong mạng Blockchain đóng, có sự phân loại mức độ tin tưởng và thu hồi chứng thực nếu làm sai.

Mạng Blockchain đóng có lẽ được sử dụng bởi tổ chức muốn kiểm soát chặt chẽ hơn và bảo vệ Blockchain của họ. Tuy nhiên, nếu một thực thể kiểm soát những ai có thể xuất bản các khối, thì những người dùng sẽ cần phải tin tưởng vào thực thể đó. Một mạng Blockchain đóng của tổ chức này muốn làm việc với tổ chức khác nhưng có thể không hoàn toàn tin tưởng lẫn nhau. Họ có thể thành lập mạng và mời các đối tác kinh doanh ghi lại các giao dịch trên một cuốn sổ cái phân tán chia sẻ. Các tổ chức này có thể xác định mô hình đồng thuận sẽ được dùng dựa trên mức độ tin tưởng lẫn nhau. Bên cạnh đó, mạng cung cấp sự minh bạch và hiểu biết mà có

thể giúp thông báo các quyết định kinh doanh tốt hơn và buộc những bên làm sai chịu trách nhiệm.

Một vài mạng Blockchain đóng hỗ trợ khả năng tiết lộ giao dịch có chọn lọc dựa trên danh tính của người dùng. Với tính năng này, một vài mức độ riêng tư của giao dịch có thể được áp dụng. Ví dụ, mọi người có thể biết được có một giao dịch giữa hai người dùng được diễn ra, nhưng nội dung thật sự của giao dịch thì chỉ có những người liên quan mới có thể tiếp cận.

I.4. Kiến trúc Blockchain

I.4.1. Hàm băm mật mã

Một thành phần quan trọng của công nghệ Blockchain là sử dụng các hàm băm mật mã cho các hoạt động. *Băm* là một phương pháp áp dụng hàm băm mật mã vào dữ liệu nhằm tạo ra một đầu ra tương ứng duy nhất (được gọi là *tóm tắt thông điệp – message digest*, hoặc *tóm tắt – digest*) từ một đầu vào của bất kỳ kích thước (chẳng hạn một tập tin, văn bản hoặc hình ảnh). Nó cho phép các cá nhân chứng minh không có sự thay đổi dữ liệu, kể cả khi chỉ là một sự thay đổi nhỏ của đầu vào (chẳng hạn thay đổi một bit) sẽ dẫn đến kết quả hoàn toàn khác.

Hàm băm mật mã có các thuộc tính bảo mật quan trọng sau:

- *Preimage resistant (Chống nghịch ảnh)*: Có nghĩa là các giá trị từ hàm băm là một chiều; không thể tính toán chính xác giá trị đầu vào dựa vào giá trị đầu ra.

  Ví dụ: Cho giá trị hàm băm h, tìm thông điệp m sao cho $h = \text{hash}(m)$ là rất khó.

- *Second preimage resistant (Chống nghịch ảnh thứ hai)*: Có nghĩa là không thể tìm một đầu vào mà giống với đầu ra cụ thể được. Cụ thể hơn, hàm băm mật mã được thiết kế để từ một đầu vào cụ thể, không thể tính toán để tìm một đầu vào thứ hai mà cả hai đều có cùng một đầu ra.

  Ví dụ: Cho thông điệp m_1, việc tìm một thông điệp $m_2 \neq m_1$ sao cho $\text{hash}(m_1) = \text{hash}(m_2)$ là rất khó.

  Cách tiếp cận duy nhất là vét cạn toàn bộ các giá trị từ không gian đầu vào nhưng cơ hội thành công là không có.

- *Collision resistant (Chống xung đột)*: Có nghĩa là không thể tìm hai đầu vào mà băm thành một đầu ra giống nhau. Cụ thể hơn, không thể tính toán để tìm hai đầu vào mà tạo ra tóm tắt giống nhau.

  Ví dụ: Việc tìm hai thông điệp $m_1 \neq m_2$ sao cho hash(m_1) = hash(m_2) là rất khó.

Một hàm băm mật mã cụ thể được dùng trong triển khai Blockchain là Secure Hash Algorithm (SHA) với một đầu ra có kích thước 256 bits (SHA-256). Một vài máy vi tính hỗ trợ thuật toán này trong phần cứng, làm nó thực hiện tính toán nhanh hơn. SHA-256 có một đầu ra 32 bytes (32 bytes = 256 bits), được thể hiện bởi một chuỗi 64 ký tự cơ số 16.

Điều đó có nghĩa là có $2^{256} \approx 10^{77}$, hoặc 115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 913 129 639 936 các giá trị tóm tắt có thể. Thuật toán cho SHA-256 cũng như các thuật toán khác, được chỉ định bởi Tiêu chuẩn Xử lý Thông tin Liên bang - Federal Information Processing Standard (FIPS) 180-4[1]. Trang web NIST Secure Hashing[2] chứa thông số kỹ thuật FIPS cho tất cả các thuật toán được chứng nhận NIST[3].

Đầu vào	**Hàm băm**	**Đầu ra từ hàm băm**
1	MD5	c4ca4238a0b923820dcc509a6f75849b
	SHA-1	356a192b7913b04c54574d18c28d46e6395428ab
	SHA-256	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
Hello World	MD5	b10a8db164e0754105b7a99be72e3fe5
	SHA-1	0a4d55a8d778e5022fab701977c5d840bbc486d0
	SHA-256	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
Hello World!	MD5	ed076287532e86365e841e92bfc50d8c
	SHA-	2ef7bde608ce5404e97d5f042f95f89f1c232871

[1] Xem chi tiết tại: https://csrc.nist.gov/publications/detail/fips/180/4/final
[2] Trang web cụ thể: https://www.nist.gov/publications/secure-hash-standard
[3] Xem chi tiết tại: https://csrc.nist.gov/projects/hash-functions

	1	
	SHA-256	7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069

Bảng 2. Ví dụ về đầu vào và đầu ra tương ứng của một số hàm băm[1]

Có thể nhận thấy rằng có vô hạn các giá trị đầu vào và hữu hạn các giá trị đầu ra, có thể nhưng cũng khó xảy ra xung đột hash(x) = hash(y). SHA-256 được cho là có khả năng chống xung đột, bởi vì việc tìm xung đột xảy ra ở SHA-256, khi thực thi thuật toán, theo trung bình thì khoảng 2^{128} lần (340 282 366 920 938 463 463 374 607 431 768 211 456; xấp xỉ $3{,}402 \times 10^{38}$).

1.1.1.1. Cryptographic nonce

Số mật mã được dùng một lần (Cryptographic nonce) là một số tùy ý và chỉ được sử dụng một lần. Nó kết hợp với dữ liệu để tạo ra một tóm tắt mã băm khác nhau cho mỗi nonce:

$$\text{hash}\ (data + nonce) = digest$$

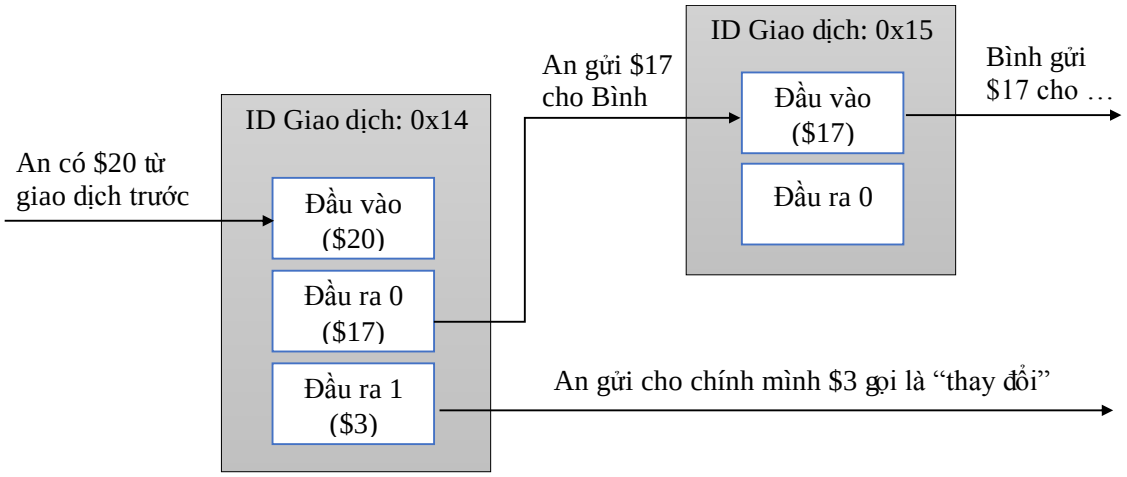
Thay đổi giá trị nonce cung cấp một cơ chế thu về các giá trị tóm tắt khác nhau trong khi giữ được cùng một dữ liệu. Kỹ thuật này được triển khai trong mô hình đồng thuận bằng chứng công việc (xem phần tiếp theo).

I.4.2. Giao dịch

Một giao dịch đại diện một sự tương tác giữa các bên tham gia. Với các đồng tiền mã hóa, một giao dịch đại diện cho việc chuyển tiền giữa những người dùng Blockchain. Đối với môi trường kinh doanh, một giao dịch có thể là một cách ghi lại các hoạt động xảy ra trên tài sản kỹ thuật số hoặc vật lý. Hình 3 cho thấy một ví dụ đáng chú ý của một giao dịch tiền điện tử. Mỗi một khối trong Blockchain có thể không chứa hoặc chứa nhiều giao dịch. Trong một vài triển khai Blockchain, việc cung cấp liên tục các khối mới (kể cả với giao dịch không) là quan trọng cho việc duy trì bảo mật mạng Blockchain: nó ngăn chặn những người dùng xấu xa khỏi "bắt được" và tạo một chuỗi khác thay thế.

[1] Công cụ được sử dụng: https://www.fileformat.info/tool/hash.htm

Một người dùng gửi thông tin đến mạng Blockchain. Thông tin được gửi có thể bao gồm địa chỉ người gửi (hoặc số nhận dạng có liên quan khác), khóa công khai



của người gửi, chữ ký số, đầu vào và đầu ra giao dịch.

Hình 3. Ví dụ về giao dịch tiền điện tử

Mỗi giao dịch đơn lẻ của tiền điện tử điển hình yêu cầu ít nhất các thông tin sau, có thể nhiều hơn:

- **Các đầu vào**: Các đầu vào thường là một danh sách các tài sản kỹ thuật số cần được chuyển. Một giao dịch sẽ tham chiếu đến nguồn của tài sản kỹ thuật số (bằng việc cung cấp nguồn gốc), có thể là giao dịch trước đó của người gửi hay sự kiện gốc nếu là trường hợp đầu tiên. Các giao dịch tham chiếu đến sự kiện trước đó mà không làm ảnh hưởng tới dữ liệu, vì vậy mà các giá trị của giao dịch không thể được thêm vào hoặc loại bỏ khỏi tài sản đã tồn tại trong Blockchain. Một tài sản đơn có thể chia thành nhiều tài sản mới với giá trị nhỏ hơn hoặc nhiều tài sản có thể kết hợp thành các tài sản với giá trị cao hơn. Việc chia hoặc kết hợp các tài sản sẽ được chỉ định ở đầu ra của giao dịch.

  Người gửi phải chứng minh được họ có quyền tiếp cận các đầu vào được tham chiếu, thường bằng cách ký chữ ký số vào giao dịch, chứng minh thông qua khóa riêng.
- **Các đầu ra**: Các đầu ra thường là các tài khoản người nhận tài sản kỹ thuật số cùng với số tài sản mà họ sẽ nhận. Mỗi đầu ra chỉ định số tài sản có thể chuyển cho người chủ mới và một tập các điều kiện mà người chủ mới phải

đáp ứng để chi tiêu giá trị đó. Nếu tài sản ở đầu ra nhiều hơn yêu cầu thì phần dư phải được gửi lại rõ ràng đến người gửi ban đầu (cơ chế "tạo thay đổi").

Trong khi mục đích chính là chuyển tài sản thì các giao dịch vẫn thường được sử dụng để chuyển dữ liệu. Trường hợp đơn giản, một ai đó muốn gửi dữ liệu vĩnh viễn và công khai trên Blockchain. Trong hợp đồng thông minh, các giao dịch có thể được dùng để gửi dữ liệu, xử lý dữ liệu và lưu trữ kết quả trên Blockchain.
Các giao dịch thường được ký bằng khóa riêng của người gửi và có thể được xác minh bất kỳ lúc nào bằng khóa chung được liên kết.

I.4.3. Mật mã khóa bất đối xứng

Công nghệ Blockchain sử dụng mật mã khóa bất đối xứng[1] (hay còn gọi là mật mã khóa công khai). Mật mã khóa bất đối xứng sử dụng một cặp khóa: một khóa chung và một khóa riêng có quan hệ toán học với nhau. Khóa công khai được phổ biến công khai mà không làm giảm tính bảo mật của quy trình nhưng khóa riêng phải được giữ bí mật nếu muốn mã hóa bảo vệ dữ liệu. Khóa riêng không thể xác định hiệu quả dựa trên tri thức về khóa công khai. Một khóa có nhiệm vụ là mã hóa thì khóa còn lại sẽ giải mã.

Mật mã khóa công khai cho phép một mối quan hệ tin tưởng giữa những người dùng không quen biết tin một ai đó, bằng cách cung cấp một cơ chế để xác minh tính ràng buộc và tính xác thực của giao dịch trong khi vẫn cho phép các giao dịch được công khai. Khóa riêng sẽ được dùng để mã hóa giao dịch và những ai có khóa công khai thì có thể giải mã được nó. Bởi vì khóa công khai có sẵn miễn phí, nên mã hóa giao dịch bằng khóa riêng chứng minh được người ký giao dịch có quyền truy cập khóa riêng hay không. Thay vào đó, nếu một ai đó mã hóa bằng khóa công khai của một người thì chỉ có người dùng có khóa riêng tương ứng thì có thể giải mã. Nhược điểm là mật mã khóa công khai thường xử lý tính toán chậm.

Khóa đối xứng thì trái ngược với những điều trên ở chỗ chỉ có một khóa riêng được sử dụng cho việc mã hóa và giải mã. Với mật mã khóa đối xứng, người dùng phải hoàn toàn tin tưởng vào người khác nếu muốn trao đổi khóa chia sẻ trước. Trong hệ thống đối xứng, bất kỳ dữ liệu được mã hóa thì có thể được giải mã bằng

[1] Trong FIPS Publication 186-4, Digital Signature Standard (DSS) chỉ ra một thuật toán cho ký chữ ký số được dùng trong công nghệ Blockchain là Hệ mật dựa trên đường cong Elliptic - Elliptic Curve Digital Signature Algorithm (ECDSA), xem chi tiết tại: https://csrc.nist.gov/publications/detail/fips/186/4/final

khóa chia sẻ trước này, xác nhận nó được gửi bởi một người khác cũng có quyền truy cập vào khóa chia sẻ trước; người dùng mà không tiếp cận được khóa chia sẻ trước thì không thể xem được dữ liệu giải mã. So với mật mã khóa bất đối xứng , mật mã khóa đối xứng thực thi nhanh hơn. Chính vì vậy, dữ liệu được mã hóa bằng mật mã khóa đối xứng, khóa đối xứng được mã hóa bằng mật mã khóa bất đối xứng, "thủ thuật" này có thể làm tăng tốc độ của mật mã khóa bất đối xứng lên nhiều.

I.4.4. Địa chỉ

Một vài mạng Blockchain sử dụng một *địa chỉ*, nó là một chuỗi ký tự trong bảng chữ cái và các số, ngắn, được lấy từ khóa công khai của người dùng bằng cách sử dụng một hàm băm mật mã, thêm vào là một vài dữ liệu (chẳng hạn số phiên bản, checksums). Các địa chỉ này là địa chỉ "đích đến" và địa chỉ "xuất phát" trong giao dịch. Địa chỉ ngắn hơn khóa công khai và không bí mật. Một phương pháp để tạo địa chỉ là sử dụng một khóa công khai, áp dụng hàm băm mật mã cho nó, và chuyển nó thành chuỗi băm:

khóa công khai → hàm băm mật mã học → địa chỉ

Mỗi triển khai Blockchain có thể thực hiện một phương thức tạo địa chỉ khác nhau. Các địa chỉ có thể đóng vài trò là người định danh công khai cho người dùng và thỉnh thoảng một địa chỉ được chuyển đổi thành một mã QR chứa dữ liệu tùy ý cho việc sử dụng dễ dàng hơn trên thiết bị di động.

Nội dung	Mã QR tương ứng
1	

Hello World	
Hello World!	

Bảng 3. Minh họa một số kết quả mã QR[1]

I.4.5. Sổ cái

Một quyển sổ cái truyền thống bao gồm danh sách các giao dịch. Trong suốt lịch sử, bút và giấy được dùng để ghi lại các hoạt động trao đổi hàng hóa và dịch vụ. Ngày nay, sổ cái đã được lưu trữ bằng kỹ thuật số, thường nằm trong một cơ sở dữ liệu lớn, được sở hữu và vận hành bởi một bên thứ ba tin cậy tập trung dựa, thay mặt cho cộng đồng người dùng. Sổ cái với quyền sở hữu tập trung thì có thể được triển khai theo mô hình tập trung hoặc phân tán (chẳng hạn, chỉ một máy chủ hoặc nhiều máy chủ).

Trong công nghệ Blockchain, cách tiếp cận là sử dụng cả quyền sở hữu phân tán và kiến trúc vật lý phân tán. Kiến trúc vật lý phân tán của mạng Blockchain liên quan đến một số lượng lớn các máy tính, nhiều hơn so với mạng có kiến trúc vật lý tập trung. Nhu cầu cần các sổ cái mà quyền sở hữu phân tán nhiều lên là bởi vì các sổ cái phải đảm bảo có thể tin tưởng, bảo mật và tin cậy.

I.4.6. Khối

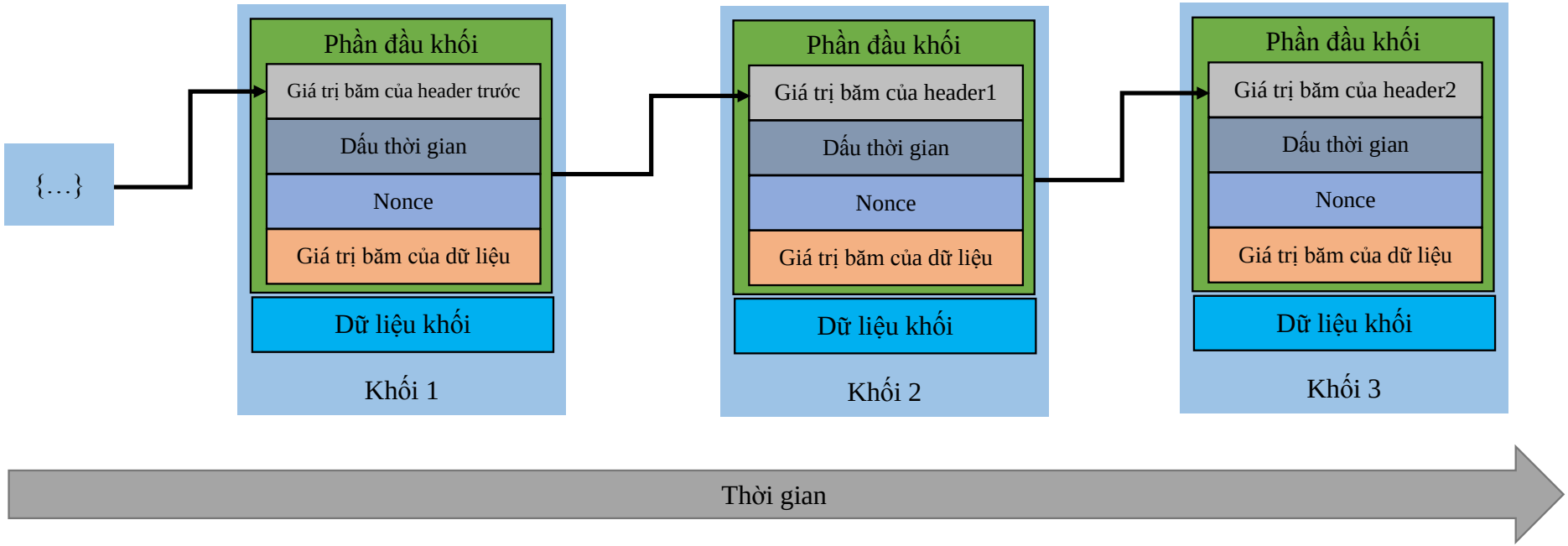
[1] Công cụ được sử dụng: https://www.the-qrcode-generator.com/

Người dùng gửi các giao dịch ứng viên lên mạng Blockchain thông qua phần mềm (ứng dụng desktop, ứng dụng di động, ví điện tử, dịch vụ web,…). Phần mềm gửi các giao dịch này tới một nút hoặc các nút trong mạng. Các giao dịch sau đó được gửi đến các nút khác trong mạng, nhưng lúc này vẫn chưa nằm trong Blockchain. Một khi giao dịch được gửi đến các nút, nó nằm trong hàng đợi cho đến khi được thêm vào Blockchain bởi một nút xuất bản.

Các giao dịch được thêm vào Blockchain khi có một nút xuất bản nó thành một khối. Một khối bao gồm phần đầu (block header) và phần dữ liệu (block data). Phần đầu chứa siêu dữ liệu của khối, còn phần dữ liệu chứa một danh sách các giao dịch được xác minh tính hợp lệ và tính xác thực được gửi đến mạng Blockchain. Tính hợp lệ và tính xác thực được đảm bảo bằng cách kiểm tra đúng định dạng và người gửi phải ký vào giao dịch chữ ký mật mã (đã đề cập ở phần trước).

I.4.7. Chuỗi khối

Các khối được nối với nhau thành chuỗi, trong đó mỗi khối chứa mã băm của phần đầu khối trước đó, do đó được gọi là chuỗi khối. nếu một khối được xuất bản trước đó bị thay đổi, nó sẽ có mã băm khác, gây ra vấn đề là khối còn lại có mã băm khác với khối trước. Điều này giúp cho việc phát hiện trở nên dễ dàng hơn và từ chối các khối thay thế. Hình 4 cho thấy một chuỗi khối chung (a generic chain of blocks).



Hình 4. Ví dụ về một chuỗi khối chung

Có thể tóm tắt quá trình diễn ra bên trong Blockchain như sau:

- Mỗi một hoạt động sẽ tương ứng với một giao dịch được tạo thành, có đầu vào và đầu ra. Ngoài ra còn phải có chữ ký kỹ thuật số (khóa riêng của người gửi) ký vào bên trong giao dịch để khẳng định chủ quyền sở hữu.
- Giao dịch được gửi đến mạng Blockchain và nằm trong hàng đợi để chờ được xuất bản. Có thể xác minh tính hợp lệ bằng cách sử dụng khóa chung của người gửi để kiểm tra. Nút xuất bản sẽ đảm nhiệm xuất bản giao dịch đó thành khối.
- Khối phải nắm được giá trị băm của header khối liền trước nó và của header mà nó đang nắm giữ. Giờ đây, khối có thể được thêm vào Blockchain.

Sau khi khối thêm vào trong Blockchain (nói cách khác, nó được ghi vào sổ cái mà nút đó đang giữ), thì nút đó gửi bản sao của sổ cái đến toàn bộ mạng.

I.5. Một số mô hình đồng thuận phổ biến

Tên mô hình	Mục tiêu	Ưu điểm	Nhược điểm	Phạm vi áp dụng	Ví dụ về triển khai
Bằng chứng Công việc (PoW)	Cung cấp một rào cản xuất bản các khối dưới dạng một câu đố tính toán chuyên sâu để cho phép các giao dịch giữa những người tham gia chưa đáng tin cậy.	• Khó khăn khi thực hiện tấn công từ chối dịch vụ với các khối xấu. • Bất kỳ ai có phần cứng thích hợp đều có thể tham gia giải đố.	• Tính toán chuyên sâu, tiêu thụ năng lượng, cạnh tranh phần cứng. • Nguy cơ tấn công 51% nếu có đủ năng lực tính toán.	Tiền điện tử mở	Bitcoin, Ethereum,…

Bằng chứng Cổ phần (PoS)	Cho phép rào cản ít tính toán chuyên sâu trong việc xuất bản các khối nhưng vẫn cho phép các giao dịch giữa những người tham gia chưa đáng tin cậy.	• Ít phải tính toán chuyên sâu như PoW. • Mở cho mọi người muốn có cổ phần tiền điện tử. • Các cổ đông điều khiển hệ thống.	• Các cổ đông điều khiển hệ thống. • Không có gì để ngăn chặn các nút tập trung quyền lực thành một nhóm. • Nguy cơ tấn công 51% nếu có đủ năng lực tài chính.	Tiền điện tử mở	Ethereum, Casper, Krypton
Round Robin	Cung cấp một hệ thống cho việc xuất bản các khối dựa trên các nút xuất bản được chứng thực/tin tưởng.	• Công suất tính toán thấp. • Đơn giản để hiểu.	Yêu cầu sự tin tưởng cao giữa các nút xuất bản.	Hệ thống đóng	MultiChain
Bằng chứng Thẩm quyền/ Danh tính	Tạo một quá trình đồng thuận tập trung để tối thiểu hóa quá trình tạo khối và tỷ lệ xác nhận.	• Thời gian xác nhận nhanh. • Cho phép tỷ	• Dựa vào giả định nút xác minh hiện tại không bị xâm	• Hệ thống đóng • Hệ thống Hybrid (sidechain)	Ethereum Kovan testnet, POA Chain, Các hệ thống đóng khác sử

		lệ tạo khối linh động. • Có thể được sử dụng trong một mô hình đồng thuận khác.	phạm. • Nguy cơ thất bại ở điểm tập trung. • Danh tiếng tiềm ẩn nguy cơ rủi ro cao và có thể bị xâm phạm bất ký lúc nào.		dụng Parity
Bằng chứng Thời gian trôi qua (PoET)	Cho phép một mô hình đồng thuận kinh tế hơn cho mạng Blockchain, chẳng hạn các chi phí cho đảm bảo bảo mật sâu hơn ở PoW.	Ít tính toán chuyên sâu như PoW	• Yêu cầu phần cứng chuyên dụng. • Giả sử phần cứng đó không bị xâm phạm. • Không thể đồng bộ trong hệ thống phân tán vì hạn chế về tốc độ trễ.	Mạng đóng	Hyperledger Sawtooth

Bảng 4. Một số mô hình đồng thuận trong Blockchain

I.6. Một số nền tảng dựa trên Blockchain hiện nay

I.6.1. Ethereum

Sau sự thành công của Bitcoin, một loại tiền điện tử khác cũng gây tiếng vang trong thị trường số hiện nay là Ethereum. Ethereum cho phép mọi người xây dựng và sử dụng các ứng dụng phi tập trung dựa trên công nghệ Blockchain. Nó là dự án mã nguồn mở, có thể chuyển đổi và linh hoạt hơn Bitcoin.

Ethereum có các đặc điểm sau:

- Là mạng mở;
- Sử dụng mô hình đồng thuận bằng chứng công việc;
- Có lượng người theo dõi trên Github cao;
- Hỗ trợ các ngôn ngữ như C++, Go và Python [8] [9].



Hình 5. Logo Ethereum

I.6.2. Hyperledger Fabric

Đây là một trong những nền tảng Blockchain phát triển gần đây nhất và được biết đến như là cuốn siêu sổ cái vào năm 2016, do Linux Foundation tạo ra. Mục tiêu của nó là đẩy nhanh sử dụng công nghệ Blockchain trong các ngành công nghiệp khác nhau như tài chính ngân hàng, IoT, chuỗi cung ứng…

Hyperledger Fabric có các đặc điểm sau:

- Có thể sử dụng cho mục đích mở hoặc đóng;
- Tích cực cập nhật trên Github;
- Sử dụng mô hình đồng thuận Pluggable;
- Hỗ trợ ngôn ngữ Python.



Hình 6. Logo Hyperledger Fabric

I.6.3. IBM Blockchain

Là công ty tiên phong liên doanh Blockchain vì vậy mà nó có thể tạo một nền tảng điều hành kinh doanh minh bạch. IBM tự hào về một cơ chế đồng thuận hiệu quả hơn, tạo sự chú ý cho nhiều người.

IBM Blockchain có các đặc điểm sau:

- Nó thuộc về mạng Blockchain đóng, do đó có sự bảo mật cao;
- Phổ biến ở mức trung bình nhưng tích cực cập nhật trên Github;
- Phiên bản miễn phí hạn chế, có thể nâng cấp lên gói Doanh nghiệp;
- Hỗ trợ các ngôn ngữ như Go và Javascript.



Hình 7. Logo IBM Blockchain

I.6.4. Multichain

Multichain là nền tảng Blockchain mã nguồn mở, được dùng trong mạng Blockchain đóng. Nó được sử dụng trong các doanh nghiệp khác nhau. Bằng cách cung cấp quyền riêng tư và sự kiểm soát mạng ngang hàng, nó như là sự cải thiện của Bitcoin cho các giao dịch tài chính riêng tư.

Multichain có các đặc điểm sau:

- Là mạng mang tính chất đóng;
- Phổ biến ở mức trung bình nhưng tích cực cập nhật trên Github;
- Miễn phí và mã nguồn mở;
- Hỗ trợ các ngôn ngữ như Python, C#, JavaScript , PHP, Ruby



Hình 8. Logo MultiChain

I.6.5. Hydrachain

Hydrachain là một sáng kiến hợp tác giữa Ethereum và công nghệ brainbot. Nó được dùng để tạo một sổ cái riêng tư hữu ích cho doanh nghiệp mặc dù nó không được phổ biến.

Hydrachain có các đặc điểm sau:

- Sử dụng giao thức Ethereum;
- Là mạng đóng.
- Ít phổ biến hơn nhưng tích cực cập nhật trên Github;

- Hỗ trợ ngôn ngữ Python.



Hình 9. Logo HydraChain

I.6.6. OpenChain

Openhain là một nền tảng mã nguồn mở, cực kỳ hữu ích cho các công ty đang tìm kiếm giải pháp quản lý tài sản kỹ thuật số. Nó còn cho phép tùy biến quyền theo các mức độ khác nhau.

OpenChain có các đặc điểm sau:

- Dùng cho mạng đóng;
- Phổ biến ở mức trung bình nhưng tích cực cập nhật trên Github;
- Hỗ trợ ngôn ngữ JavaScript;
- Sử dụng mô hình đồng thuận phân vùng.



Hình 10. Logo OpenChain

I.6.7. BigchainDB

BigchainDB là một nền tảng mã nguồn mở. Là một cơ sở dữ liệu nhưng mang các tính chất của Blockchain.

BigchainDB có các đặc điểm sau:

- Tùy biến tài sản;
- Không tích hợp sẵn tiền ảo;
- Có thể dùng cho cả mạng đóng và mở;
- Hỗ trợ các ngôn ngữ như Java, Python, Javascript và các ngôn ngữ khác do cộng đồng hỗ trợ.



Hình 11. Logo BigchainDB

BigchainDB mang bản chất của cơ sở dữ liệu và các đặc trưng của Blockchain nên xét về tổng thể thì BigchainDB phù hợp nhất để áp dụng trong đề tài này.

CHƯƠNG II. TỔNG QUAN VỀ BIGCHAINDB

II.1. Giới thiệu về BigchainDB

BigchainDB là sự kết hợp giữa công nghệ Blockchain (tính phi tập trung, tính bất biến và tài sản do chủ sở hữu kiểm soát) với cơ sở dữ liệu (tốc độ giao dịch cao, độ trễ thấp, lập chỉ mục và truy vấn dữ liệu có cấu trúc).

BigchainDB được phát hành lần đầu tiên vào tháng 2 năm 2016 và liên tục được cải tiến đến bây giờ. BigchainDB 2.0 có sự cải tiến đáng kể so với phiên bản trước. Cụ thể là có BFT vì vậy mà 1/3 các nút nếu có bị lỗi thì hệ thống vẫn sẽ tiếp tục hoạt động bình thường.

Bảng dưới đây cho thấy các mục tiêu thiết kế của BigchainDB 2.0:

	Blockchain điển hình	**Cơ sở dữ liệu phân tán điển hình**	**BigchainDB**
Tính phi tập trung	✓		✓
Byzantine Fault Tolerant	✓		✓
Tính bất biến	✓		✓
Tài sản do chủ sở hữu kiểm soát	✓		✓
Tốc độ giao dịch cao		✓	✓
Độ trễ thấp		✓	✓
Lập chỉ mục & truy vấn dữ liệu có cấu trúc		✓	✓

Bảng 5. Mục tiêu thiết kế của BigchainDB 2.0

II.2. Đặc điểm của BigchainDB

II.2.1. Tính phi tập trung và Byzantine Fault Tolerance

BigchainDB 2.0 sử dụng Tendermint cho toàn bộ mạng và đồng thuận. Mỗi một nút có cơ sở dữ liệu MongoDB riêng và tất cả giao tiếp giữa các nút là nhờ vào giao thức Tendermint[12]. Một khi tin tặc lấy quyền quản trị của một cơ sở dữ liệu Mongodb, trường

[12] Xem chi tiết tại https://tendermint.com/

hợp tệ nhất là họ có thể làm sụp đổ hệ thống hoặc xóa dữ liệu cục bộ; các cơ sở dữ liệu MongoDB ở các nút khác không bị ảnh hưởng là nhờ vào BFT và Tendermint chính là BFT[13].

Nếu mỗi một nút trong mạng BigchainDB được sở hữu và điều hành bởi một người khác nhau, thì nó được gọi là mạng phi tập trung, bởi vì nó không có một người dùng sở hữu toàn bộ, không một điểm tập trung và không có điểm thất bại. Lí tưởng nhất là các nút nên đặt ở nhiều quốc gia, với sự ràng buộc pháp lý và nhà cung cấp, vì vậy mà một vấn đề xảy ra không ảnh hưởng đến tất cả. Nếu một nút bị hư hỏng thì mạng vẫn tiếp tục hoạt động. Trên thực tế là nếu có tới 1/3 các nút bị tấn công[14] thì phần còn lại của mạng sẽ tiếp tục làm việc, BigchainDB sẽ cô lập những thay đổi đó nhờ vào Tendermint.

Tóm tại, để việc tấn công các nút trở nên khó khăn hơn (hạn chế 1/3 các nút bị "kiểm soát") thì có vài cách có thể tham khảo:

- **Đa dạng thẩm quyền**: Các nút phải được kiểm soát bởi những thực thể nằm trong vùng thẩm quyền pháp lý và sử dụng các phương tiện pháp lý để bắt buộc mọi người tuân theo.
- **Đa dạng địa lý**: Các máy chủ phải được đặt tại các vị trí vật lý trên nhiều vùng địa lý khác nhau, nhằm tránh các thảm họa tự nhiên (lũ lụt hoặc động đất) làm tổn hại đến mạng.
- **Đa dạng hosting**: Các máy chủ (kể cả các nút) nên được sử dụng từ các nhà cung cấp dịch vụ khác nhau (chẳng hạn Amazon Web Services, Microsoft Azure, Digital Ocean, Rackspace).
- **Đa dạng nói chung**: Sự đa dạng thẩm quyền mang nhiều lợi thế hơn. Nhờ vào đó, mà các biện pháp lý tưởng khác có thể được triển khai.

Một điều lưu ý: Nếu các nút có cùng triển khai (cùng sử dụng ngôn ngữ và các đoạn mã xây dựng BigchainDB) thì nếu có một lỗi nào đó xuất phát từ chính BigchainDB, các nút khác có thể bị lỗi giống như vậy, kẻ xấu có thể lợi dùng từ đó. Vậy nên nếu triển khai được BigchainDB bằng các ngôn ngữ khác, chẳng hạn Python và Go thì có thể gọi đây là đa dạng triển khai.

[13] Xem chi tiết tại https://en.wikipedia.org/wiki/Byzantine_fault
[14] Về mặt kỹ thuật, hơn 1/3 quyền biểu quyết (voting power) có thể bị tấn công (hay thất bại). Nhưng trong BigchainDB, thường là các nút có quyền biểu quyết giống nhau, vì vậy 1/3 quyền biểu quyết giống với 1/3 số nút.

II.2.2. Tính bất biến

Một khi dữ liệu được lưu trữ ở mạng BigchainDB thì nó không thể bị thay đổi hoặc tẩy xóa, hoặc ít nhất là rất khó khăn. Nếu một dữ liệu bị thay đổi hoặc tẩy xóa thì nó có thể phát hiện được. Mặc dù trong thế giới thực, mọi sự vật đều biến đổi, không hoàn toàn bất biến. Ví dụ các thiết bị bị hỏng do thiên tai, dữ liệu có thể bị mất. Nhưng trong thế giới lập trình, thì đây có thể được gọi là bất biến.

Dữ liệu blockchain chống lại sự thay đổi ngẫu nhiên xảy ra mà không có bất ký ý định nào (hành động vô ý), chẳng hạn trong trường hợp ổ cứng hư hỏng dẫn đến dữ liệu cũng bị ảnh hưởng.

BigchainDB có nhiều chiến lược để đạt được sự bất biến, có thể kể đến như sau:

- **Không tạo ra API trong BigchainDB cho phép thay đổi hoặc xóa dữ liệu.** Và BigchainDB không có các API như vậy. Tuy nhiên, nó không ngăn được các cách thay đổi khác, bởi vì nó là một trong những chiến lược phòng thủ.
- **Mỗi một nút giữ một bản sao của tất cả dữ liệu trong mạng BigchainDB**. Kể cả khi một nút bị sập hoặc phá hủy, các nút khác sẽ không bị ảnh hưởng vì vẫn còn lưu trữ bản sao của dữ liệu. Như vậy, càng nhiều bản sao lưu trữ tại các nút, thì càng khó khăn hơn cho sự thay đổi hoặc xóa.
- **Giám sát từ nội bộ và bên ngoài**. Thiết lập cơ chế theo dõi tất cả sự thay đổi tại mỗi nút, nếu một thay đổi không hợp lệ xảy ra, một hành động thích hợp có thể được thực hiện. Với các dự án có quy mô lớn, có thể nhờ bên thứ ba đáng tin cậy theo dõi, hoặc nhờ mọi người giám sát như kiểm toán viên.
- Có thể lưu trữ dữ liệu bằng các kỹ thuật khác nhau.
- **Tất cả giao dịch phải được ký chữ ký số** để khi có thay đổi gì thì dựa vào chữ ký để phát hiện.
- **Thực hiện các chính sách bảo mật mạnh mẽ nhất.**

II.2.3. Tài sản do chủ sở hữu kiểm soát

Như các Blockchain khác, BigchainDB có khái niệm tài sản do chủ sở hữu kiểm soát. Chỉ có chủ (một hoặc nhiều người nắm giữ khóa riêng) của tài sản thì có thể chuyển tài sản. Thậm chí người điều hành nút không thể chuyển tài sản.

Nếu như trong Bitcoin hoặc Ether thì chỉ có một tài sản tích hợp sẵn (là tiền điện tử) thì BigchainDB cho phép người dùng tạo bao nhiêu tài sản tùy thích, nhưng không thể tạo cái mà đã được tạo bởi người khác.

Ví dụ, ban đầu An có 100 token, anh ấy chuyển 37 token đến cho Bình bằng cách tạo giao dịch CHUYỂN với hai đầu ra:

- Chuyển 37 token đến Bình;
- Các token còn lại (100 – 37 = 63 token) quay về An.

BigchainDB kiểm tra mỗi giao dịch để đảm bảo không có giao dịch bị trùng.

II.2.4. Tốc độ giao dịch cao

Một trong những mục tiêu của BigchainDB là khả năng xử lý một lượng lớn giao dịch trong một giây và BigchainDB 2.0 vẫn đáp ứng như thế.

II.2.5. Độ trễ thấp & Hoàn thành nhanh

Mạng dựa trên Tendermint chỉ mất vài giây (hoặc ít hơn) cho một giao dịch để thêm vào khối. Sau đó, không còn cách nào khác để hoàn tác hoặc loại bỏ.

II.2.6. Lập chỉ mục & Truy vấn dữ liệu có cấu trúc

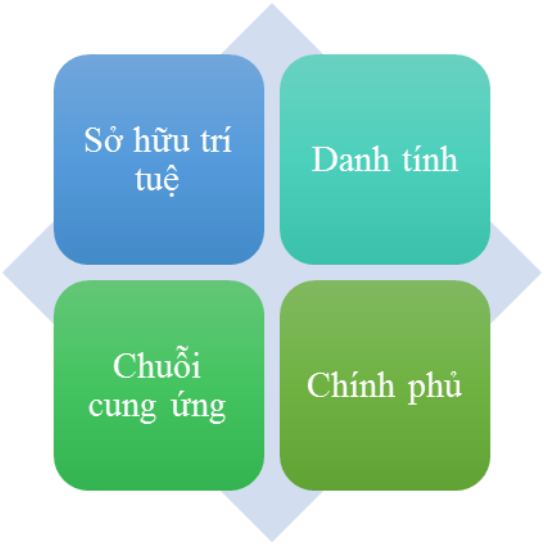
Một một người điều hành nút có toàn quyền lập chỉ mục và truy vấn dữ liệu có cấu trúc (giao dịch, tài sản, siêu dữ liệu, khối, tất cả đều là chuỗi JSON). Ngoài ra còn có thể quyết định lập chỉ mục dữ liệu không gian địa lí và cung cấp sự tối ưu về các truy vấn thực hiện tại vị trí ấy thông qua REST API.

II.2.7. Sybil Tolerance

Một vài mạng Blockchain (kể cả Bitcoin) cho phép người dùng thêm nút của họ vào mạng. Điều này tạo nên mối lo lắng về một ai đó có thể điều khiển hệ thống bằng cách thêm một vài nút vào mạng, gọi là cuộc tấn công Sybil. Bitcoin khiến chúng trở nên đắt đỏ khi thêm các nút vào mạng. Tuy nhiên, ở mạng BigchainDB, tổ chức đứng sau mạng BigchainDB quản lý danh sách thành viên, vì vậy mà tấn công BigchainDB không phải là vấn đề nguy hiểm.

II.3. Ứng dụng của BigchainDB

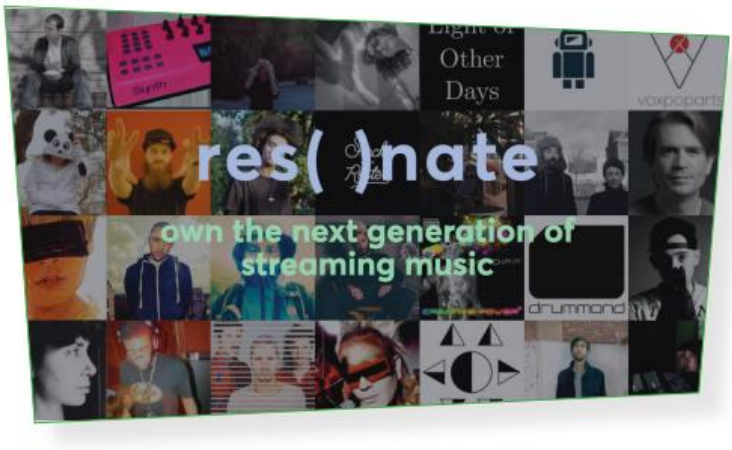
BigchainDB dành cho các nhà phát triển và tổ chức đang tìm kiếm một cơ sở dữ liệu có thể truy vấn với các đặc điểm của Blockchain như phân cấp, bất biến và khả năng tuỳ biến bất kỳ thứ gì được lưu trữ trong cơ sở dữ liệu như một tài sản [10].



Hình 12. Bốn nhóm ứng dụng chính của BigchainDB

- **Sở hữu trí tuệ**: Công nghệ Blockchain giúp bảo mật quyền tác giả. Nó cũng giúp dễ dàng cấp phép làm việc, theo dõi việc sử dụng và cung cấp các bản kiểm toán minh bạch cho tất cả các bên liên quan.

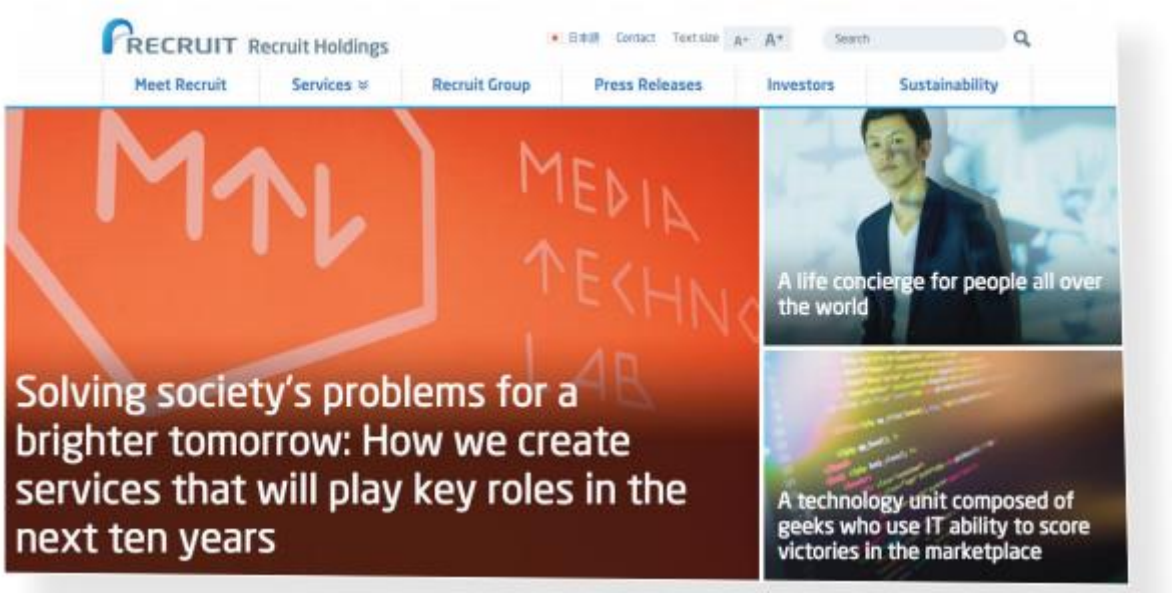
  Ví dụ thực tế: Điều gì sẽ xảy ra nếu người dùng trả tiền để phát nhạc trực tuyến và muốn biết số tiền thu được có chuyển đến các nghệ sĩ? Resonate là một dịch vụ truyền phát nhạc cho phép người nghe trả tiền để nghe nhạc trực tuyến và sở hữu bài hát [11].



Hình 13. Sở hữu truyền phát nhạc với Resonate

- **Danh tính**: Công nghệ Blockchain mang lại quyền kiểm soát cho phép dữ liệu cá nhân có chủ quyền – một cách mới để quản lý danh tính, hồ sơ y tế và thông tin đăng nhập.

  Ví dụ thực tế: Làm sao mà các công ty có thể dễ dàng xác minh thông tin chứng chỉ từ rất nhiều ứng viên? Làm sao để chống giả mạo, thay đổi, gian lận, làm sai lệch các tài liệu đó? Nền tảng Recruit sử dụng công nghệ Blockchain được tích hợp trong BigchainDB, giúp lưu trữ các hồ sơ chứng chỉ đã được xác minh và chia sẻ liền mạch cho nhiều bên, tăng niềm tin và giảm rủi ro cho mọi người [12].



Hình 14. Các chứng chỉ giáo dục được xác thực với công nghệ Recruit

- **Chuỗi cung ứng**: Công nghệ Blockchain tin cậy và minh bạch. Đây là một tính năng đang thiếu trong chuỗi cung ứng toàn cầu. Công nghệ này mang đến sự hứa hẹn về tính minh bạch và xuất xứ cho chuỗi cung ứng toàn cầu. Trong tương lai, mỗi sản phẩm sẽ có một hồ sơ rõ ràng về lịch sử và tính xác thực có thể kiểm chứng được.

  Ví dụ thực tế: Thông tin được sinh ra theo thời gian thực, với kết nối internet toàn cầu và công nghệ cảm biến tiến bộ nhanh chóng, không có lý do gì lại theo dõi từng sản phẩm một cách riêng lẻ từ khi bắt đầu cho đến tay người tiêu dùng.



Hình 15. Với Innogy, mỗi sản phẩm có một câu chuyện

Sử dụng công nghệ Blockchain do BigchainDB cung cấp có thể xây dựng cơ sở dữ liệu lưu trữ toàn bộ lịch sử của sản phẩm để có thể xác minh nguồn gốc, tính xác thực và quyền sở hữu [13].

- **Chính phủ**: Công nghệ Blockchain có thể được áp dụng trong mọi lĩnh vực của chính phủ như dịch vụ nhận dạng, doanh thu nội địa, quá trình hình thành công ty và đăng ký đất đai. Có sự minh bạch trong các dịch vụ của chính phủ hứa hẹn sẽ giảm tham nhũng, quyền đất đai và tài sản mạnh hơn, quản lý thuế hiệu quả và chủ quyền của cá nhân.

  Ví dụ thực tế:



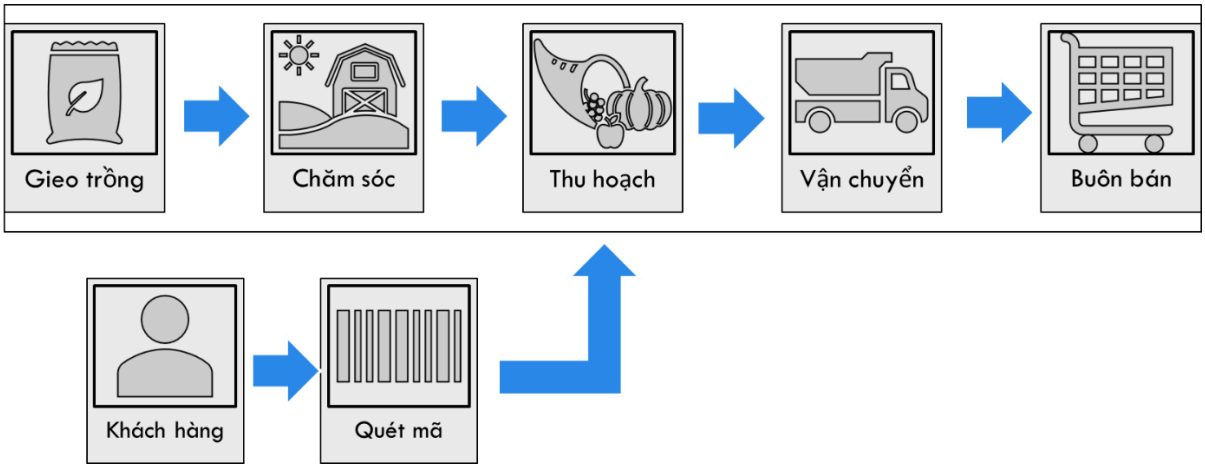
Hình 16. Công ty đăng ký đất đai Blockchain tại Ghana tên BenBen

Sử dụng công nghệ blockchain do BigchainDB cung cấp, có thể xây dựng sổ đăng ký đất đai và lịch sử giao dịch được xác minh. BigchainDB củng cố cơ quan đăng ký đất đai BenBen theo nhiều cách. BigchainDB tạo điều kiện cho sự phát triển nhanh của sản phẩm tại BenBen - cung cấp tất cả các công cụ phát triển và công nghệ để xây dựng nền tảng [14].

CHƯƠNG III. TRIỂN KHAI ỨNG DỤNG

III.1. Phân tích nghiệp vụ hệ thống

III.1.1. Phân tích chuỗi cung ứng nông sản



Hình 17. Chuỗi cung ứng nông sản

Ở giai đoạn đầu của chuỗi cung ứng, đối tượng chính là các loại hạt giống và cây trồng, chưa có khả năng thu hoạch ngay tại thời điểm đó. Trải qua thời gian chăm sóc, chúng trở thành nông sản bán thành phẩm. Để đến với tay người tiêu dùng, nông sản cần phải trải qua các giai đoạn như thu hoạch, vận chuyển và buôn bán mới chính thức trở thành sản phẩm tiêu dùng. Toàn bộ quá trình trong chuỗi cung ứng được ghi lại và tổ chức theo từng giai đoạn, do đó, khách hàng, chính là người tiêu dùng có thể nắm bắt được thông tin đó bằng việc quét mã được dán trên nông sản.

III.1.2. Danh sách Actor

ID	Tên Actor	Mô tả
A1	Quản trị viên	Là một thành viên có nhiệm vụ tạo và cấp quyền cho tài khoản mới, bảo trì hệ thống
A2	Người tiêu dùng	Là người đến các cửa hàng và truy xuất thông tin nông sản bằng điện thoại
A3	Thành viên	Có thể là cá nhân hoặc nhiều người có nhiệm vụ nào đó trong chuỗi cung ứng nông sản, đóng góp thông tin vào blockchain

A4	Nông sản	Nông sản mà thành viên quản lý

Bảng 6. Danh sách Actor

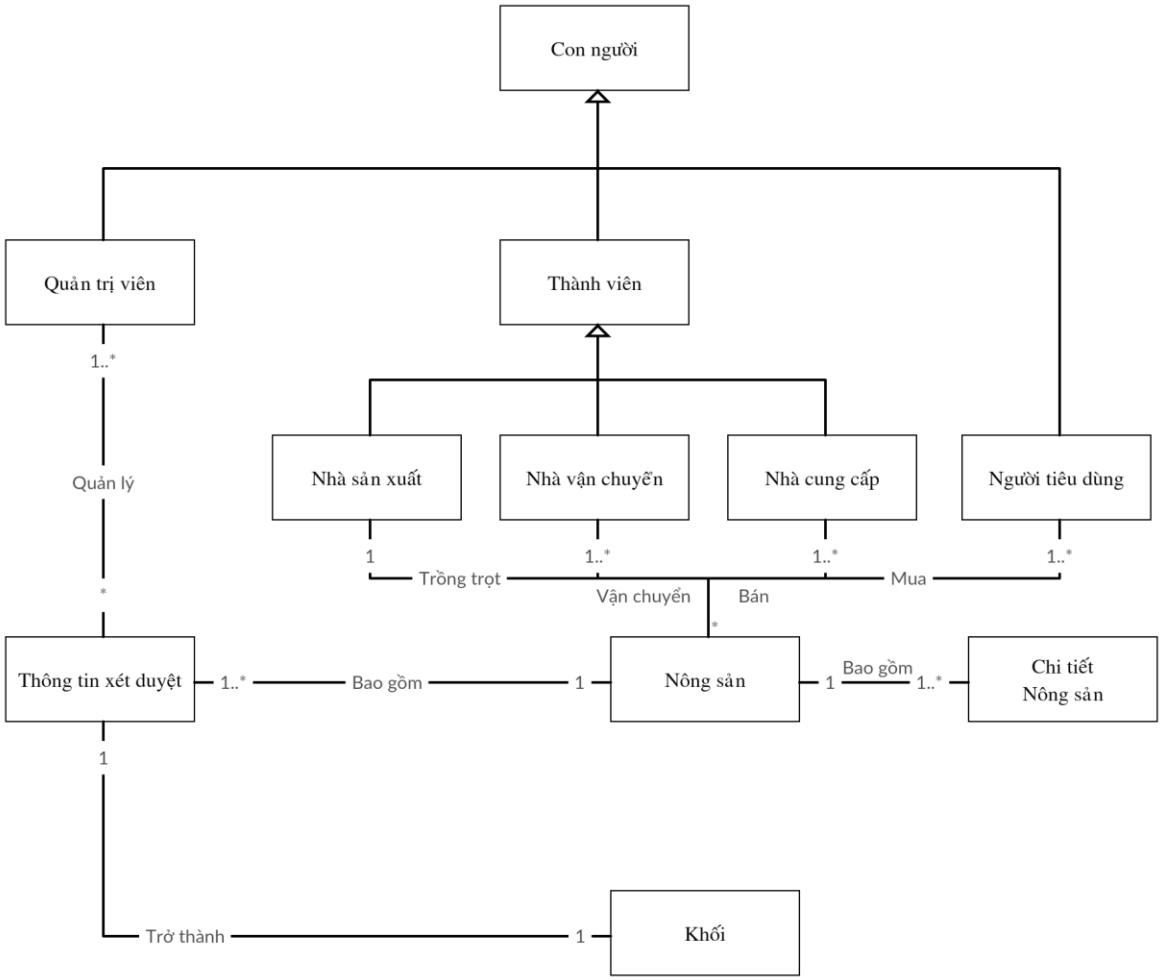
III.1.3. Danh sách Use Case

STT	ID	Tên Use Case	Mô tả	Yêu cầu nghiệp vụ
1	U1	Đăng nhập	Đăng nhập vào hệ thống để xác thực người dùng	Được mở rộng bởi tất cả
2	U2	Đăng xuất	Thoát ra khỏi hệ thống	Mở rộng U1
3	U3	Đổi mật khẩu	Đổi mật khẩu tài khoản thành viên	
4	U4	Xem danh sách nông sản đã đăng ký	Xem danh sách nông sản lưu trên hệ thống	Bao gồm U6
5	U5	Xem danh sách thành viên đã đăng ký	Xem danh sách thành viên lưu trên hệ thống	Bao gồm U7
6	U6	Xem kết quả tìm kiếm nông sản	Các kết quả tìm kiếm được hiển thị	Được bao gồm bởi U4 và U9, được mở rộng bởi U10
7	U7	Xem kết quả tìm kiếm thành viên	Các kết quả tìm kiếm được hiển thị	Được bao gồm bởi U5 và U8, được mở rộng bởi U11
8	U8	Tìm kiếm thành viên	Tìm kiếm thành viên theo yêu cầu	Bao gồm U7
9	U9	Tìm kiếm nông sản	Tìm kiếm thành viên theo yêu cầu	Bao gồm U6
10	U10	Xem chi tiết nông sản	Tìm và hiển thị chi tiết nông sản	Mở rộng U6
11	U11	Xem chi tiết thành	Tìm và hiển thị chi tiết các	Mở rộng U7

		viên	nông sản liên quan đến thành viên đó	
12	U12	Xem danh sách các thông tin phê duyệt	Xem danh sách các tin đang chờ phê duyệt	Được mở rộng bởi U13
13	U13	Xử lý thông tin đang phê duyệt	Phê duyệt hoặc gỡ bỏ thông tin	Mở rộng U12, bao gồm U14
14	U14	Thông báo đến thành viên	Thông báo kết quả của U14	Được bao gồm bởi U13
15	U15	Thêm thông tin nông sản	Các thông tin mới được cập nhật	Được mở rộng bởi U16
16	U16	Xuất QR	Thông tin liên quan đến nông sản cụ thể dành cho người dùng	Mở rộng U16

Bảng 7. Danh sách Use Case

III.1.4. Phân tích sơ đồ đối tượng



Hình 18. Sơ đồ đối tượng trong hệ thống truy xuất nguồn gốc nông sản

Giải thích sơ đồ trên như sau:

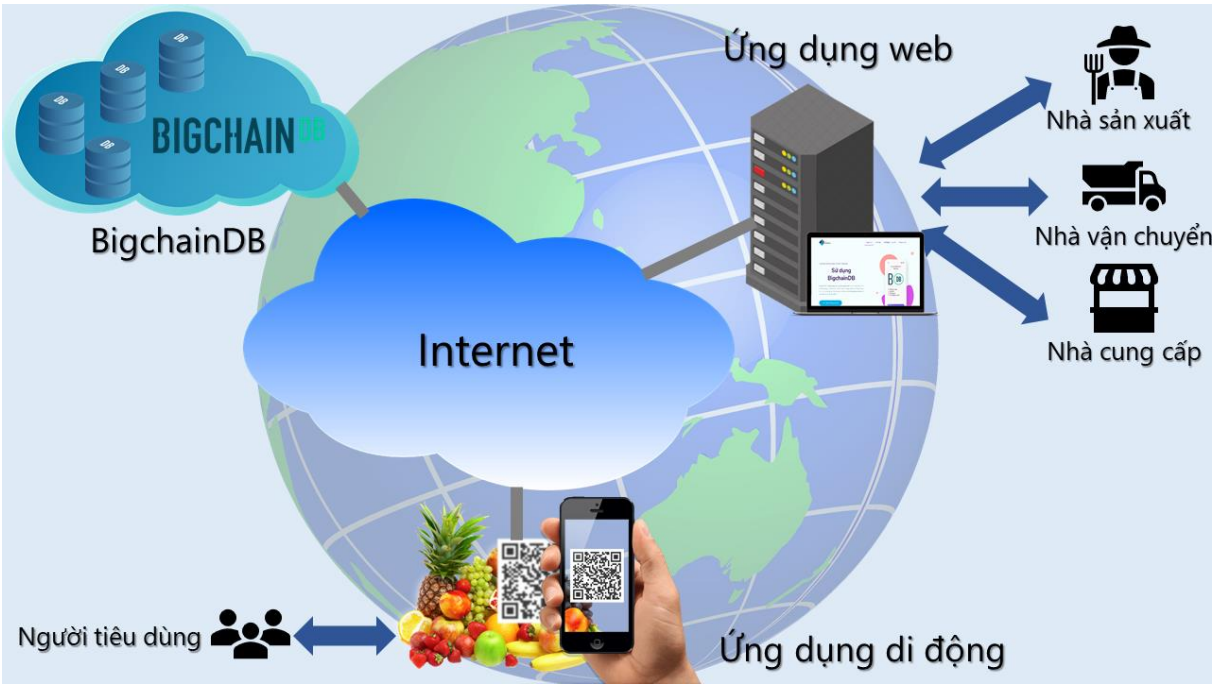
- Chia người sử dụng hệ thống bao gồm hai nhóm: thành viên (đã đăng nhập thành công) và người tiêu dùng (không cần đăng nhập vào hệ thống).
- Ở nhóm thành viên, tiếp tục phân ra thành Nhà sản xuất, Nhà vận chuyển và Nhà cung cấp. Cả thành viên và người tiêu dùng là những đối tượng được kế thừa từ Người.
- Bên cạnh Thành viên thì còn có Quản trị viên, là những người quản lý hệ thống.
- Nhà sản xuất có nhiệm vụ trồng trọt, chăm sóc, thu hoạch nông sản. Nhà vận chuyển có nhiệm vụ phân phối nông sản đến nơi khác. Còn nhà cung cấp sẽ đưa nông sản trưng bày trên kệ và bán ra thị trường. Người tiêu dùng (người mua) sẽ mua những nông sản nếu nông sản đó đã trải qua các giai đoạn kể trên.

- Vì một loại nông sản sẽ có nhiều thông tin khác nhau lưu trữ nên sẽ tách thêm Chi tiết nông sản.
- Các thông tin chi tiết của nông sản phải được xét duyệt trước khi chính thức đưa vào BigchainDB để trở thành khối, quản trị viên sẽ đảm nhận công việc đó.

STT	Tên vai trò	Ví dụ	Vai trò trong chuỗi cung ứng	Vai trò trong hệ thống
1	Nhà sản xuất	Người nông dân	- Trồng trọt - Chăm sóc - Thu hoạch	- Tạo thông tin nông sản - Bổ sung thêm thông tin trong từng hoạt động
2	Nhà vận chuyển	Các bên trung gian, đại lý phân phối	Vận chuyển hàng hóa đến các nhà cung cấp	Bổ sung thêm thông tin trong từng hoạt động
3	Nhà cung cấp	Nhà bán lẻ, siêu thị, chợ, tạp hóa	- Lựa chọn nhà sản xuất phù hợp để lấy hàng hóa - Trưng bày hàng hóa trên kệ và bán cho người tiêu dùng	Bổ sung thêm thông tin trong từng hoạt động
4	Người tiêu dùng	Khách hàng	Mua hàng hóa	Xem thông tin nguồn gốc hàng hóa
5	Quản trị viên	Nhân viên quản lý hoặc người có vai trò quyết định trong hệ thống này		Xét duyệt các thông tin trước khi đưa vào BigchainDB.

Bảng 8. Bảng vai trò của các thành phần trong chuỗi cung ứng

III.2. Mô hình triển khai



Hình 19. Sơ đồ minh họa mô hình triển khai

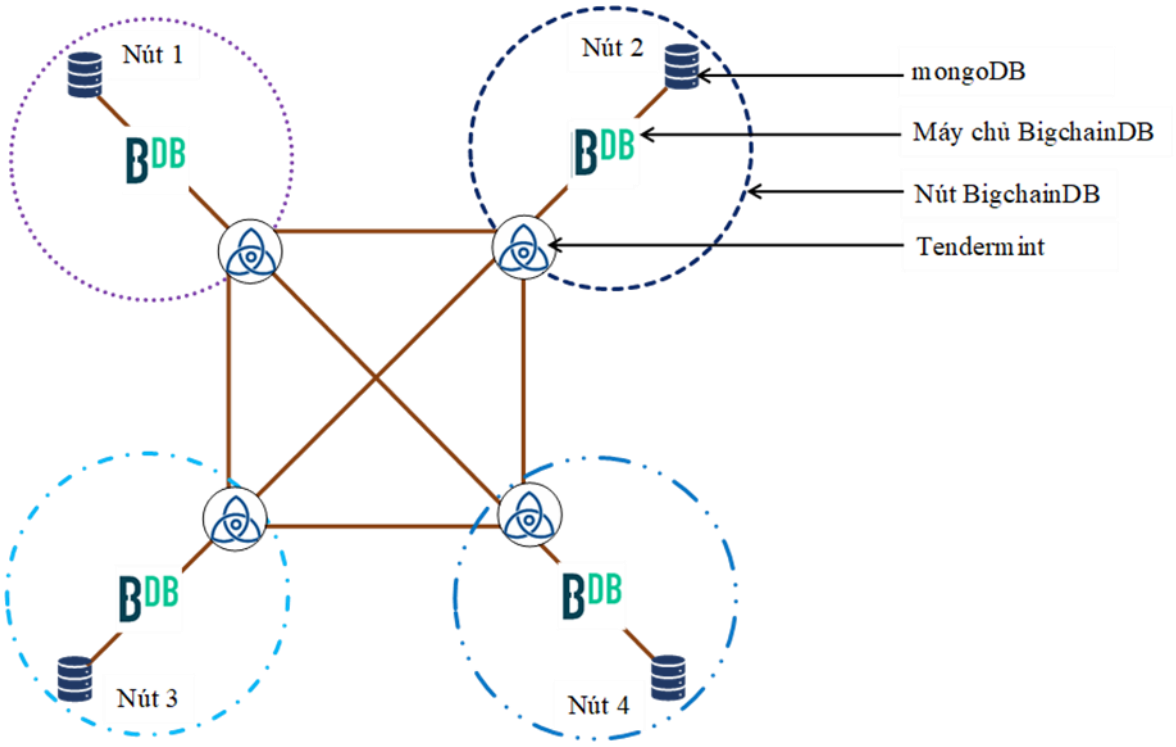
III.2.1. Khối BigchainDB

Trong khối BigchainDB là một tập các nút BigchainDB (các máy tính đã được cài đặt BigchainDB) kết nối với nhau và được quản lý bởi một tổ chức. Tổ chức này có thể là một công ty, một hợp tác xã nông nghiệp và có vai trò đưa ra các quyết định có liên quan đến toàn bộ hệ thống. Chẳng hạn, ai sẽ là đối tác được sử dụng hệ thống này, ai có thể đọc được dữ liệu được lưu tại đây, có cần phải mở rộng mạng BigchainDB hay không,…

Một quy trình quản trị hệ thống được yêu cầu để đưa ra các quyết định như trên, do đó khi triển khai thực tế, tổ chức đó phải thiết lập một quy trình quản trị có vai trò như vậy (nếu chưa có).

Ở một vài ngữ cảnh, quy trình quản trị hệ thống quyết định tính phi tập trung của mạng BigchainDB và các vấn đề bảo mật liên quan.

Về mạng BigchainDB, nó có thể cài đặt chỉ với một nút BigchainDB. Tuy nhiên, điều này không thật sự khuyến khích, và theo BigchainDB thì nhà phát triển nên cài đặt với số nút tối thiểu là 4. Sau khi thiết đặt, ta có thể loại bỏ hoặc thêm vào các nút.



Hình 20. Sơ đồ giao tiếp giữa các nút trong mạng

Trước khi cài đặt BigchainDB trên máy tính cần phải chuẩn bị các công việc sau:

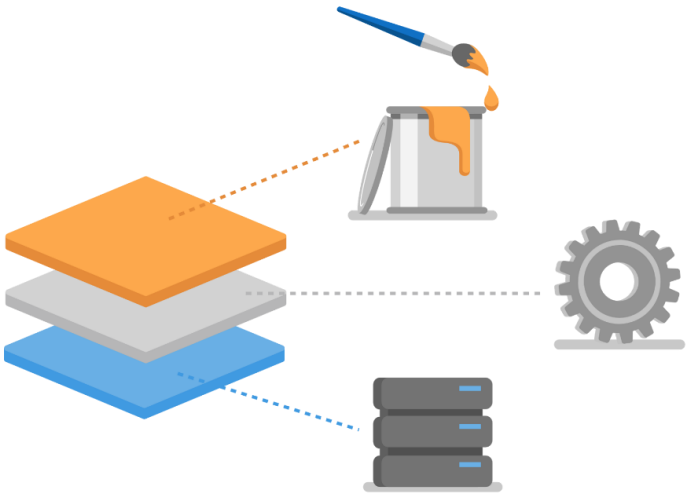
- Biết được địa chỉ IP công khai (nếu triển khai bên ngoài) hoặc IP riêng tư (nếu triển khai trên cùng mạng).
- Hệ điều hành được khuyến nghị là Ubuntu hoặc Ubuntu Server phiên bản từ 18.04 trở lên, sau đó cài đặt các cập nhật cho hệ điều hành
- Khi cài đặt trên máy thật hay ở trên các hệ thống như AWS, Azure, BigchainDB sẽ sử dụng các cổng sau cho lưu lượng vào và ra:
    - TCP ở cổng 22 (nếu dùng SSH để kết nối từ xa)
    - TCP ở cổng 9984 (cổng HTTP mặc định của BigchainDB, có thể chuyển qua cổng 80 hoặc 443)
    - Giao thức bất kỳ ở cổng 26656 (dùng cho Tenermint chia sẻ mạng ngang hàng)
- Cài đặt bảo mật tại nút đó
- Cài đặt DNS (nếu đã có đăng ký tên miền từ trước)

Chi tiết quá trình cài đặt BigchainDB và thiết lập mạng BigchainDB trên Ubuntu, có thể tham khảo thêm tại tài liệu chính thức này:

http://docs.bigchaindb.com/projects/server/en/latest/networks.html

III.2.2. Khối ứng dụng web

Trong đề tài này sẽ sử dụng mô hình MVC để xây dựng máy chủ web. Máy chủ web có vai trò quản lý thành viên và nông sản trong BigchainDB, đồng thời cho phép nhập thông tin nông sản. Mô hình Model – View – Controller (MVC) là mô hình thiết kế được sử dụng để phân tách giao diện người dùng (view), dữ liệu (model) và logic ứng dụng (controller). Mô hình này giúp đạt được sự tách biệt các thành phần của website.



Hình 21. Mô hình MVC bao gồm Model, View và Controller

Sử dụng mô hình này cho việc phát triển các website, định tuyến các yêu cầu gửi đến một Controller, Controller chịu trách nhiệm làm việc với Model để thực hiện các hành động và/hoặc nhận dữ liệu. Controller chọn View để hiển thị dữ liệu và cung cấp View cho Model. View xuất trang HTML dữ liệu dựa trên Model.

ASP.NET mang đến một cách thức mạnh mẽ, dựa trên mô hình MVC này để xây dựng một website động cho phép sự tách biệt ở các thành phần [15].

III.2.2.1. Model và Dữ liệu

Model bao gồm một tập các lớp mô hình rõ ràng và dễ dàng gắn kết chúng với cơ sở dữ liệu. Trong đó có thể định nghĩa các quy tắc xác thực dữ liệu bằng cách sử dụng các trạng thái (attributes) của C#, áp dụng được trên cả phía máy chủ và máy khách.

ASP.NET hỗ trợ nhiều cơ sở dữ liệu như SQLite, SQL Server, MySQL, DB2, PostgreSQL,… và các cơ sở dữ liệu phi quan hệ như MongoDB, Redis, Azure Cosmos DB.

Ví dụ về một lớp trong Model:

```
public class Person

{
 public int PersonId { get; set; }

 [Required]
 [MinLength(2)]
 public string Name { get; set; }

 [Phone]
 public string PhoneNumber { get; set; }

 [EmailAddress]
 public string Email { get; set; }
}
```

Hình 22. Ví dụ về lớp Person trong Models

III.2.2.2. Controller

Controller định tuyến một cách đơn giản các yêu cầu gửi đến các phương thức C# thông thường trong Controller. Dữ liệu từ các yêu cầu, chuỗi truy vấn và nội dung yêu cầu được gắn kết tự động đến các tham số trong phương thức.

Dưới đây là một ví dụ về Controller:

```
public class PeopleController : Controller
{
 private readonly AddressBookContext _context;

 public PeopleController(AddressBookContext context)
 {
 _context = context;
 }

 // GET: /people
 public async Task Index()
 {
 return View(await _context.People.ToListAsync());
 }

 // GET: /people/details/5
 public async Task Details(int id)
 {
 var person = await _context.People.Find(id);

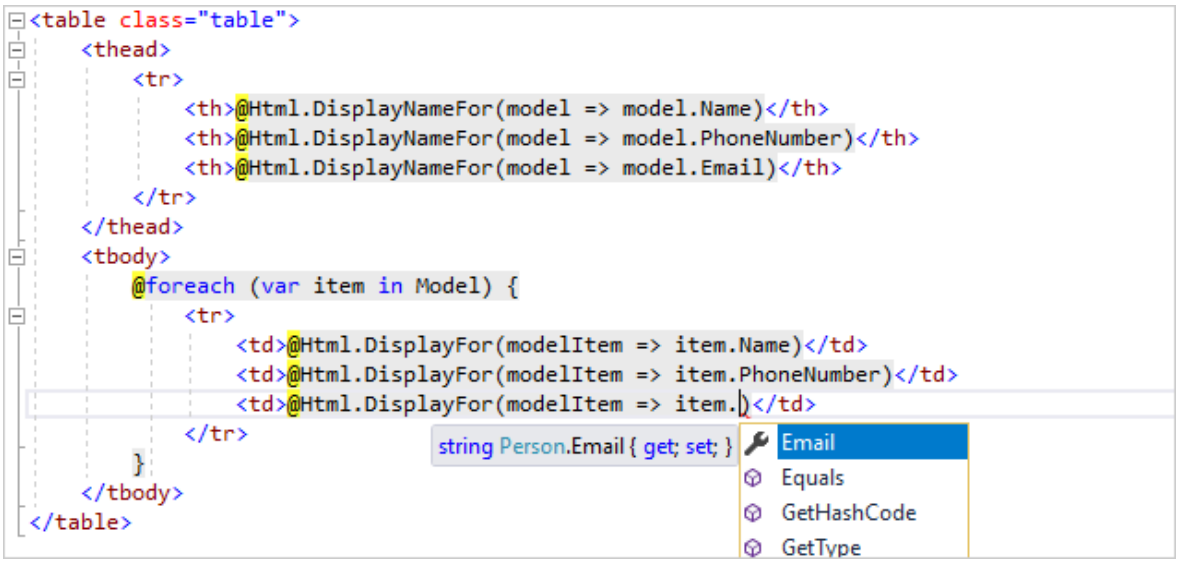
 if (person == null)
 {
 return NotFound();
 }

 return View(person);
 }
}
```

Hình 23. Ví dụ về lớp PersonController trong Controllers

III.2.2.3. View

View trong ASP.NET sử dụng Razor. Cú pháp Razor cung cấp một cách đơn giản, rõ ràng và nhẹ để tạo nội dung HTML cho View. Razor cho phép sử dụng C# trong View và tạo ra trang web HTML5 đầy đủ.



Hình 24. View với cú pháp Razor

III.2.3. Khối ứng dụng di động

Về phát triển ứng dụng di động để quét mã QR trên nông sản sẽ sử dụng Ionic. Khung làm việc Ionic là một bộ công cụ UI mã nguồn mở để xây dựng các ứng dụng desktop và di động có hiệu quả và chất lượng cao bằng việc sử dụng công nghệ web đó là HTML, CSS và Javascript – tích hợp với các khung làm việc phổ biến như Angular và React.



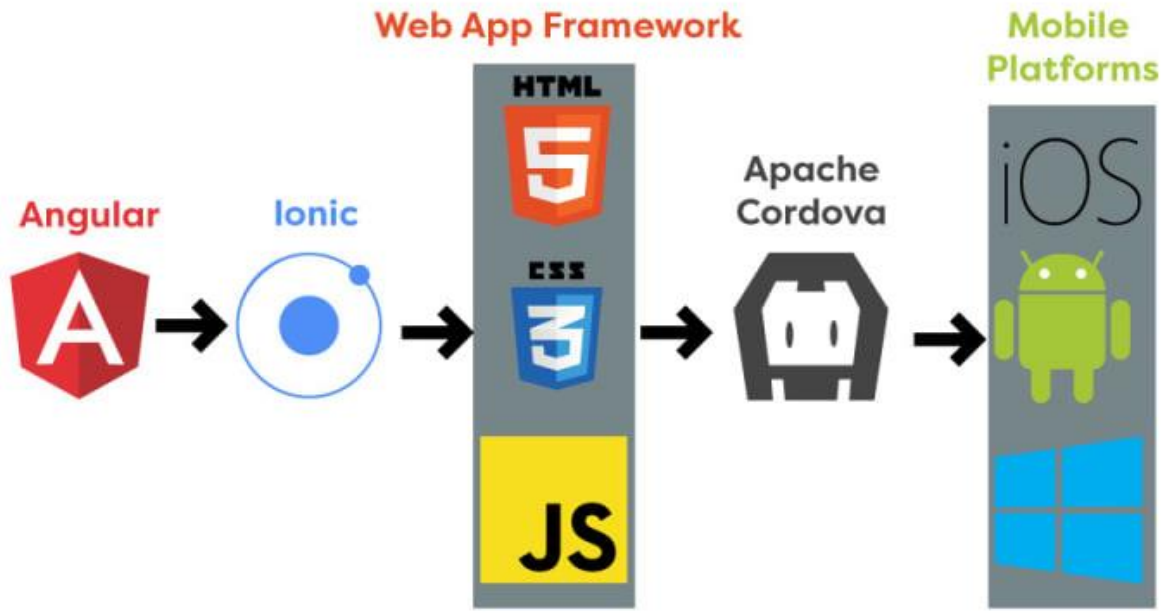
Hình 25. Logo của Ionic

Ionic tập trung vào sự tương tác giữa UI và UX trên một ứng dụng. Nó có thể xây dựng front-end mà không nhất thiết phải sử dụng các khung làm việc khác.

Đặc điểm của Ionic:

- **Viết một lần, chạy mọi nơi**: Ionic cho phép các nhà phát triển xây dựng các ứng dụng cho đa số các hệ điều hành cho thiết bị di động như Android, iOS và Windows Mobile.

- **Tập trung vào hiệu suất**: Các ứng dụng từ Ionic có thể hoạt động trên các thiết bị di động mới nhất với việc sử dụng hiệu quả các chuyển động tăng tốc phần cứng và các thao tác cử chỉ cảm ứng.
- **Thiết kế gọn gàng, đơn giản, nhiều tính năng**: Ionic được thiết kế để làm việc và hiển thị nội dung với phong cách đẹp như các thành phần tạo sẵn, các font chữ và giao diện chủ đề.
- **Tối ưu nguyên bản và web:** Ionic mang các chuẩn giao diện người dùng và tính năng giống như các ứng dụng được viết bằng ngôn ngữ native với hệ điều hành, đồng thời mang lại sức mạnh đầy đủ và tính linh hoạt đến từ web. Ionic sử dụng Cordova để triển khai thành ứng dụng nguyên bản [16].



Hình 26. Từng bước để xây dựng các ứng dụng di động

III.3. Kết quả

III.3.1. Khối BigchainDB

Để minh hoạt tính linh hoạt nền tảng BigchainDB, cũng như cung cấp cơ chế dự phòng, đề tài triển khai khối dữ liệu blockchain trên hai mạng BigchainDB khác nhau:

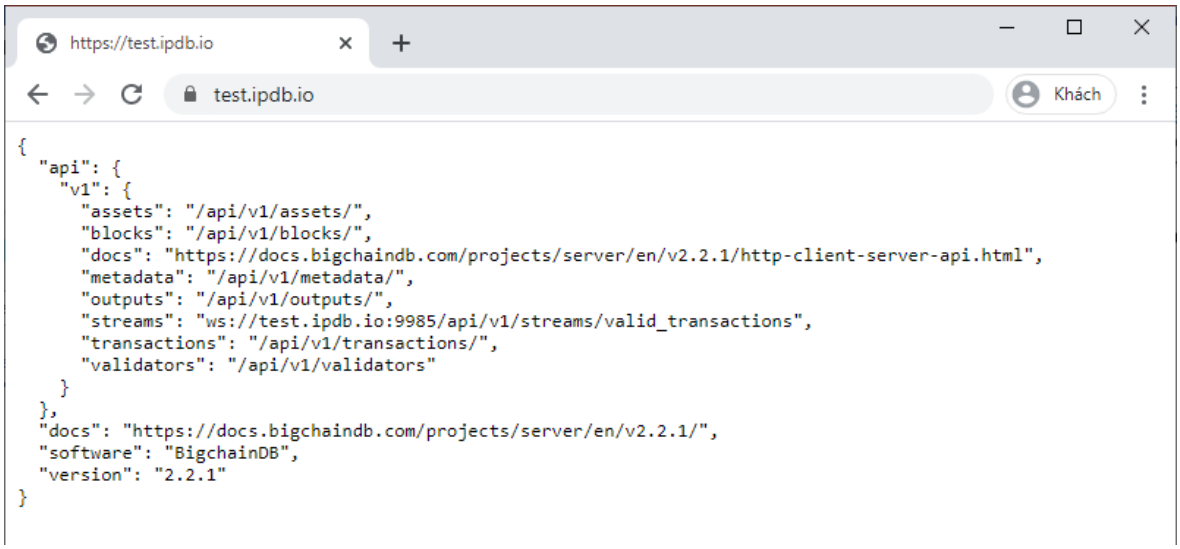
- Sử dụng hạ tầng có sẵn của BigchainDB là https://test.ipdb.io/ áp dụng cho website, gọi chung là Public Cloud

- Triển khai trên hệ thống máy ảo pcvn.vn:7000 của Khoa Công nghệ Thông tin, trường Đại học Đà Lạt áp dụng khi demo trên localhost, gọi chung là Private Cloud.

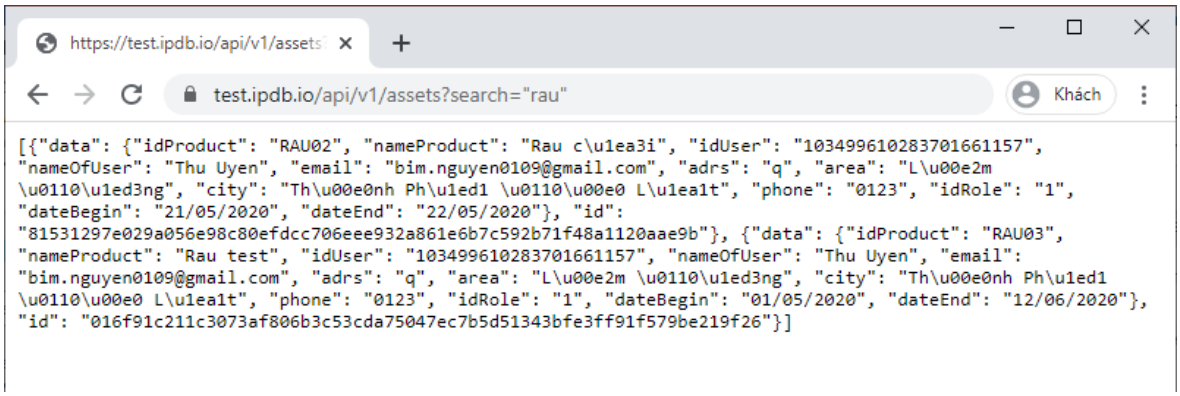
Chức năng chính của mạng BigchainDB này là lưu trữ dữ liệu (hay còn gọi là các giao dịch) theo cách phân tán, bất biến.

III.3.1.1. Mạng Public Cloud

Mạng https://test.ipdb.io/ được điều hành bởi IPDB Foundation, tự do sử dụng nó. Tuy nhiên, theo Quy định bảo vệ dữ liệu chung (General Data Protection Regulation – GDPR[15]), nó sẽ được đặt lại vào 4 giờ sáng mỗi ngày (theo múi giờ Trung Âu – CET) [17].



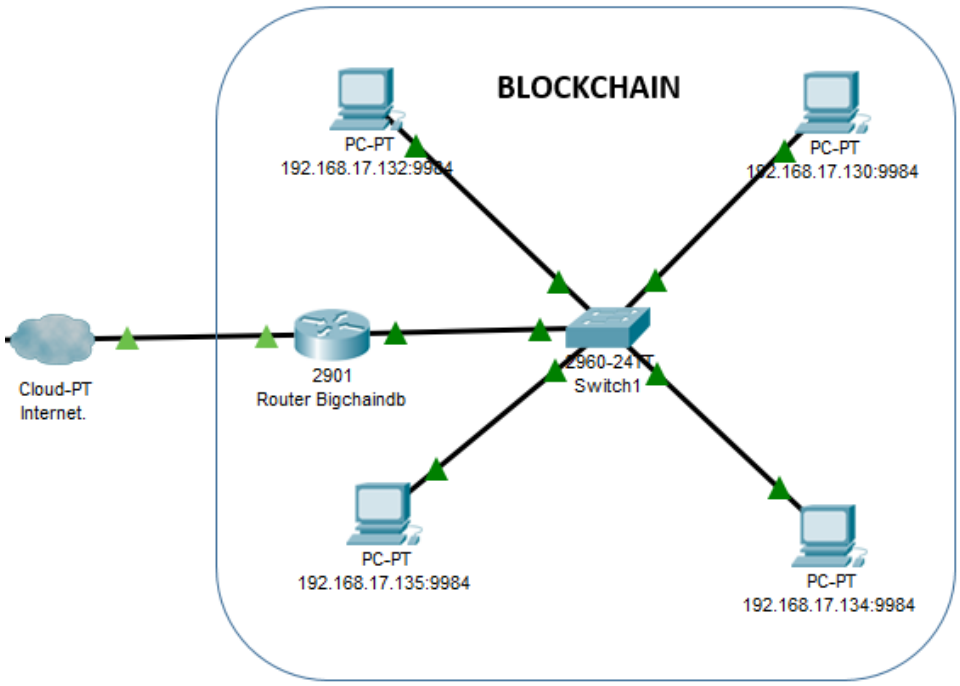
Hình 27. BigchainDB cung cấp API dùng thử nghiệm https://test.ipdb.io/



Hình 28. Thông tin khi được gửi lên https://test.ipdb.io/

[15] Xem chi tiết tại: https://gdpr-info.eu/

III.3.1.2. Mạng Private Cloud



Hình 29. Mạng BigchainDB được triển khai trên máy ảo pcvn.vn

Đặc điểm của mạng riêng tư này là khi gửi một giao dịch đến một nút trong mạng, giao dịch sau khi xác minh hợp lệ thì Tendermint sẽ gửi đến các nút khác trong mạng, đảm bảo dữ liệu được phân tán.

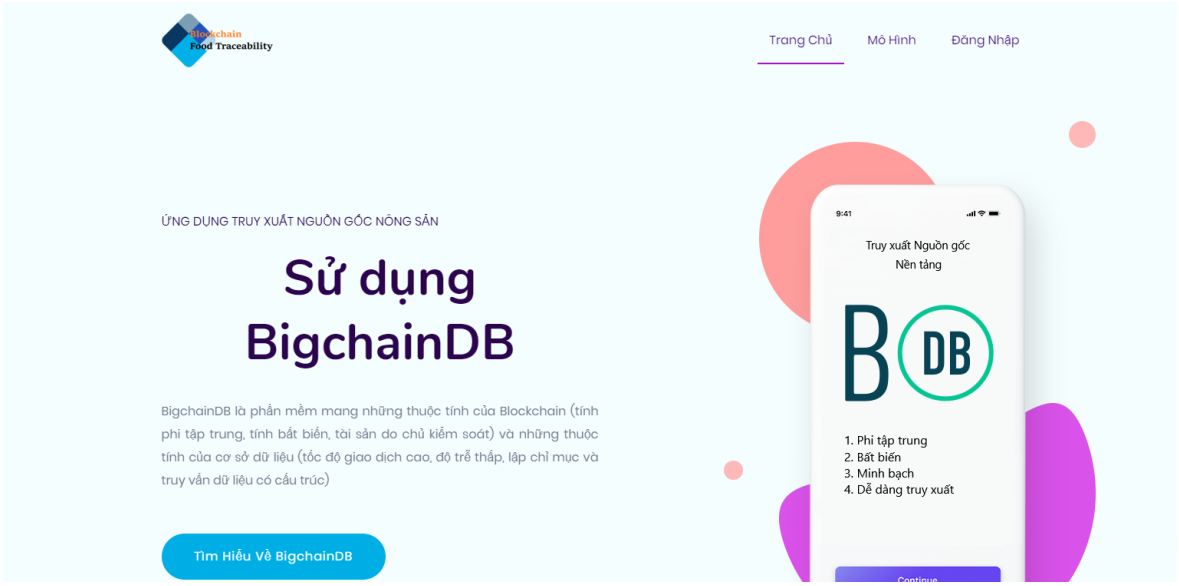
III.3.2. Khối ứng dụng web

III.3.2.1. Trang cho thành viên

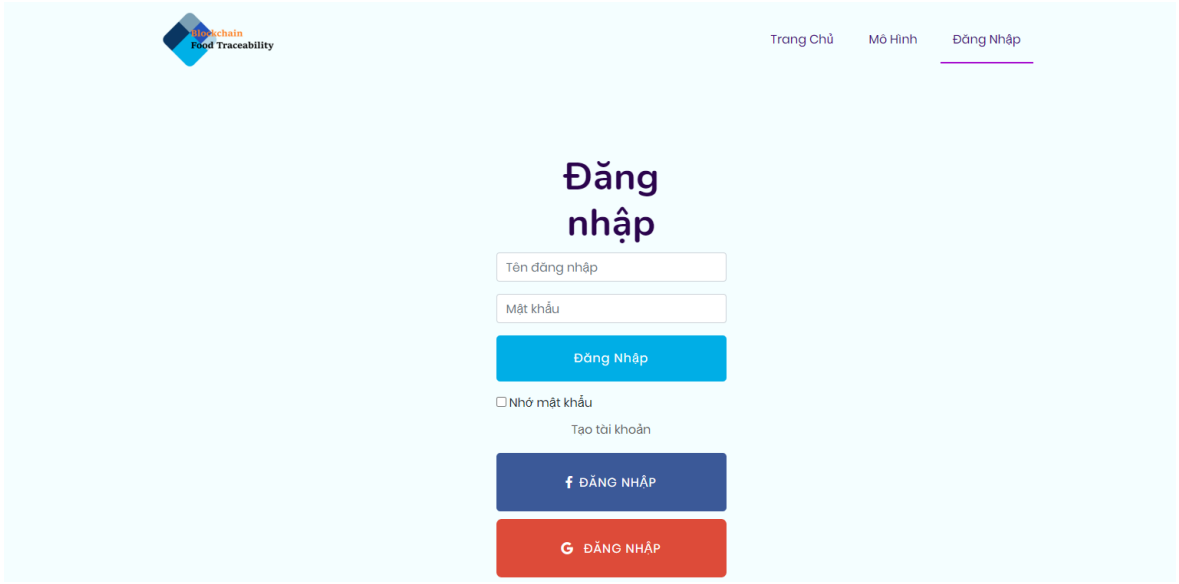
Website hiện đang được triển khai thử nghiệm tại địa chỉ sau http://foodtraceability.somee.com/.

Khi thành viên (không phải quản trị viên) đăng nhập vào hệ thống thì có thể thực hiện các công việc như tạo nông sản, cập nhật thông tin tương ứng với từng giai đoạn mà mình quản lý (nhà sản xuất, nhà vận chuyển và nhà buôn bán).

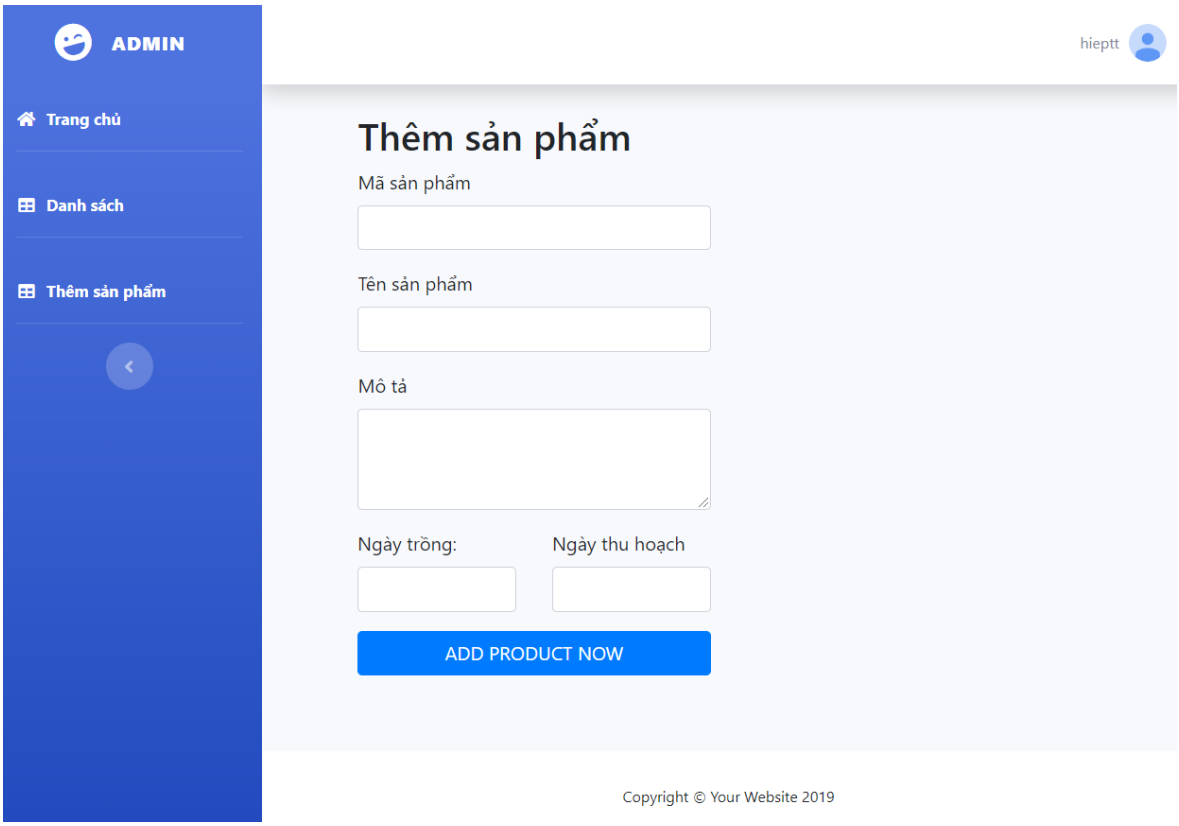
Một số hình ảnh chụp từ website:



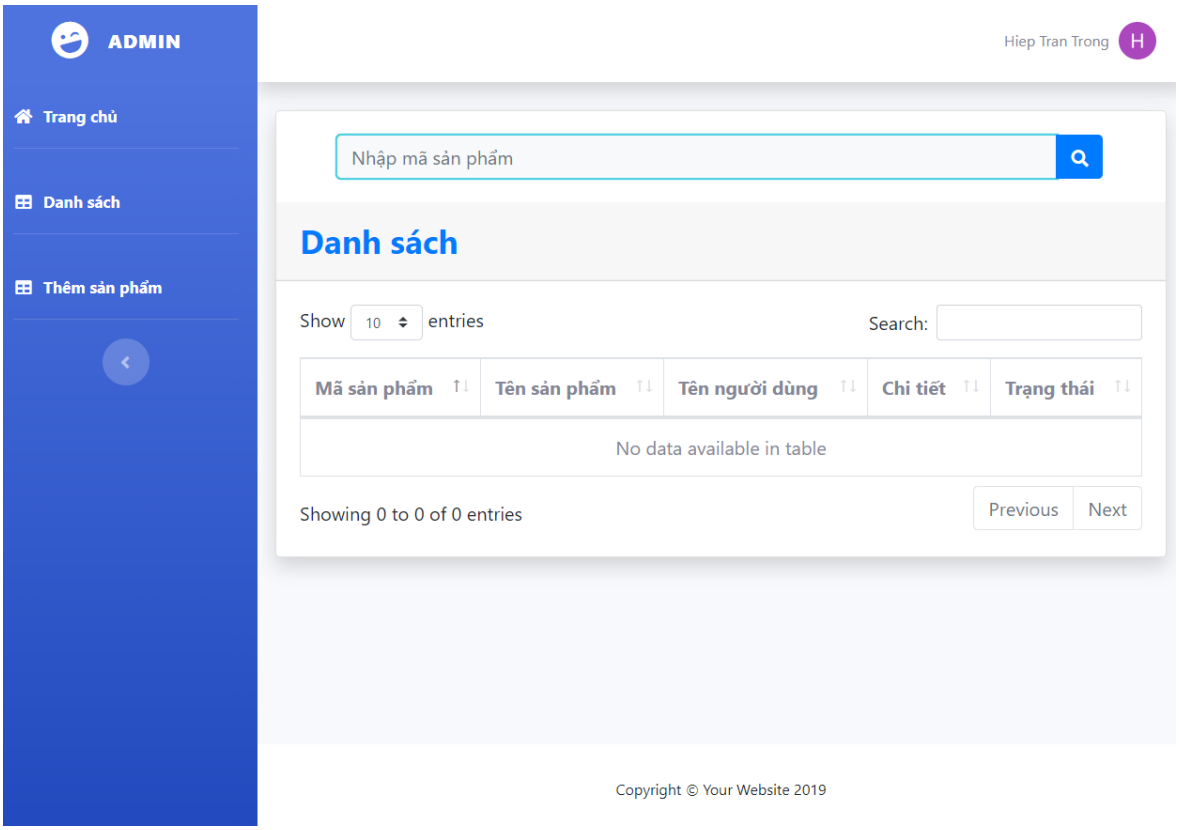
Hình 30. Giao diện trang chủ



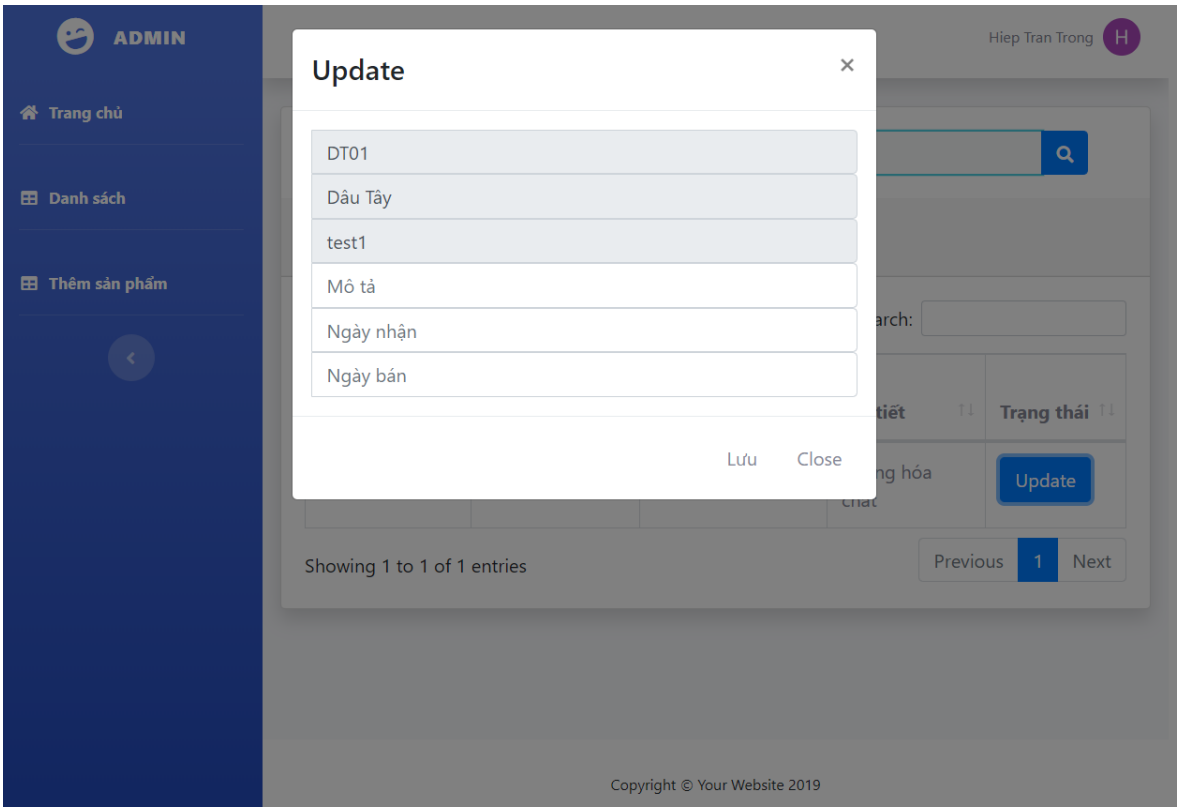
Hình 31. Giao diện trang đăng nhập



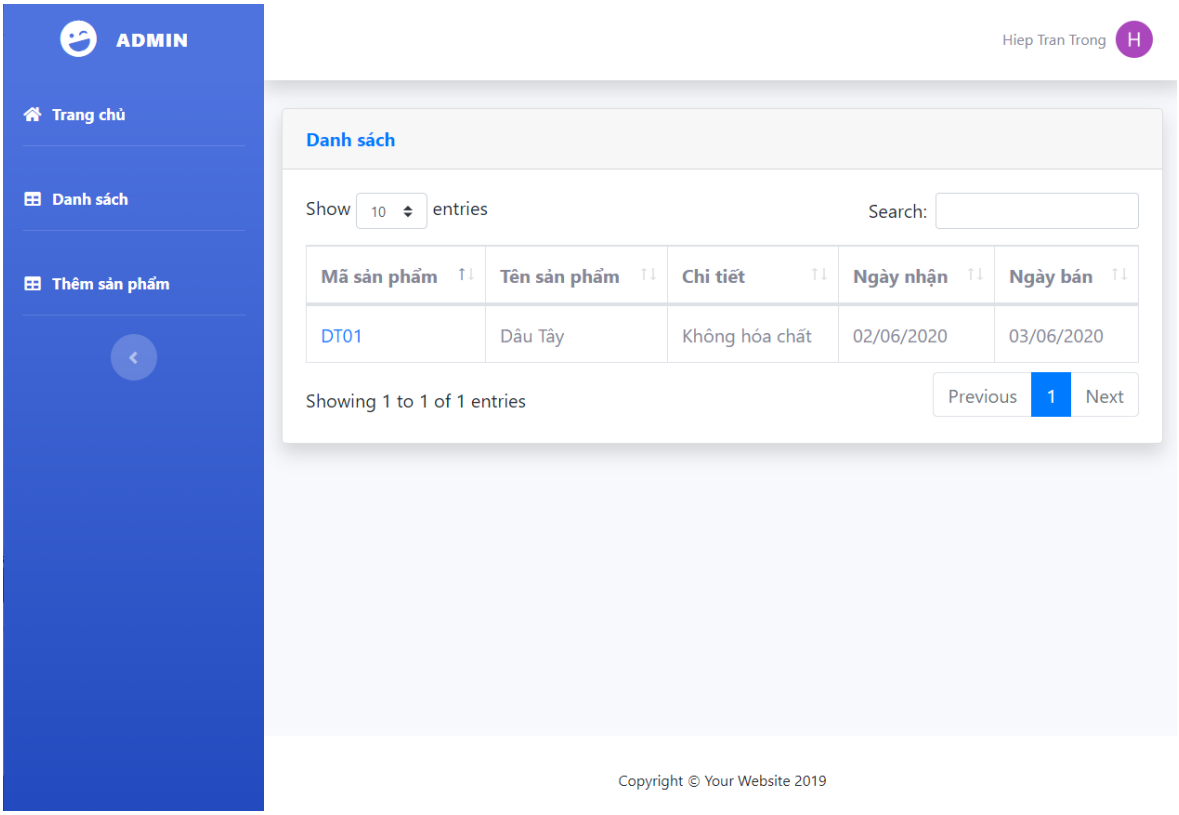
Hình 32. Giao diện tạo sản phẩm cho người sản xuất



Hình 33. Giao diện để người dùng thêm thông tin cho các vai trò khác bằng cách nhập mã sản phẩm



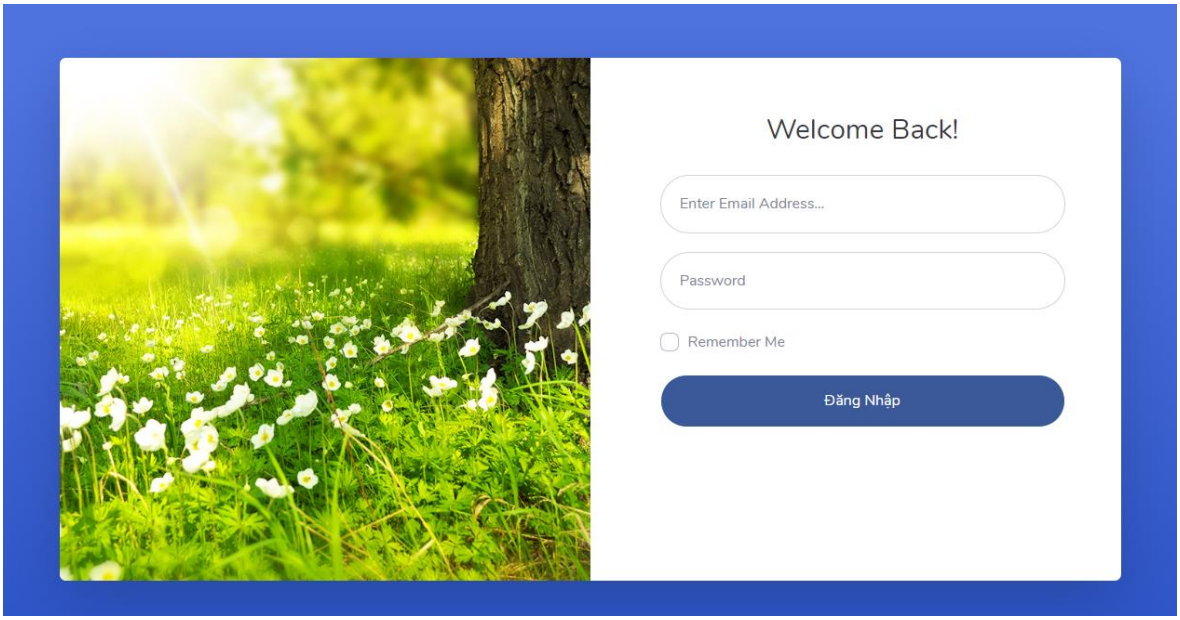
Hình 34. Giao diện để người dùng thêm các thông tin vào sản phẩm



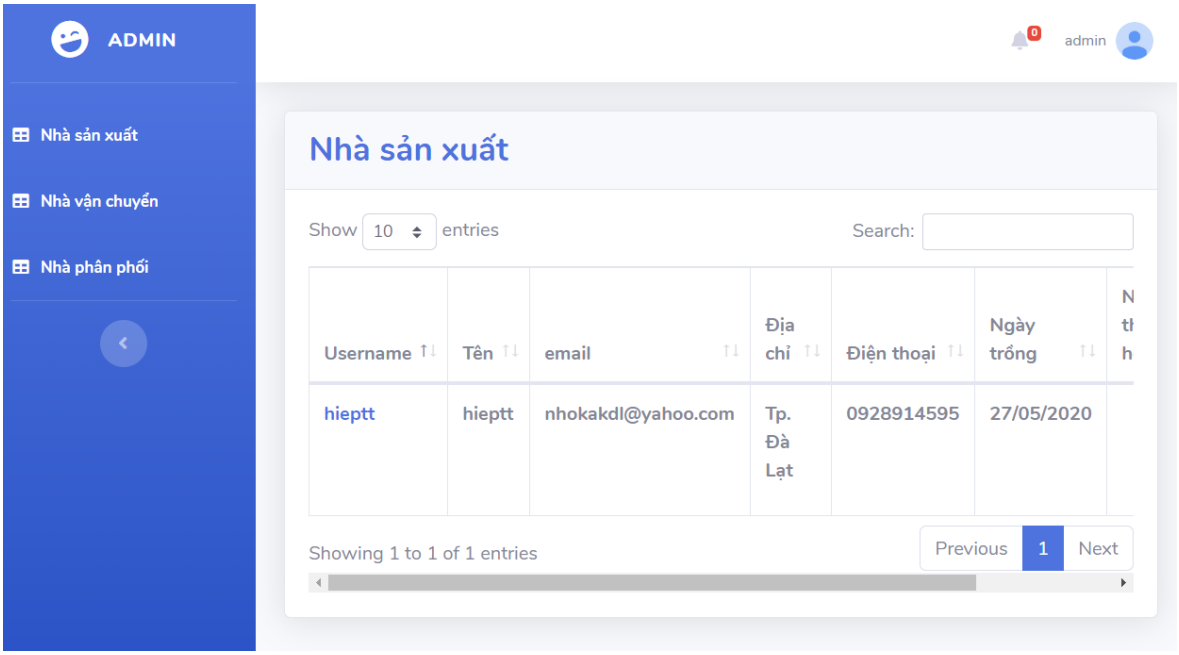
Hình 35. Giao diện quản lý hiển thị những sản phẩm mà người dùng đã nhập thông tin

III.3.2.2. Trang cho quản trị viên

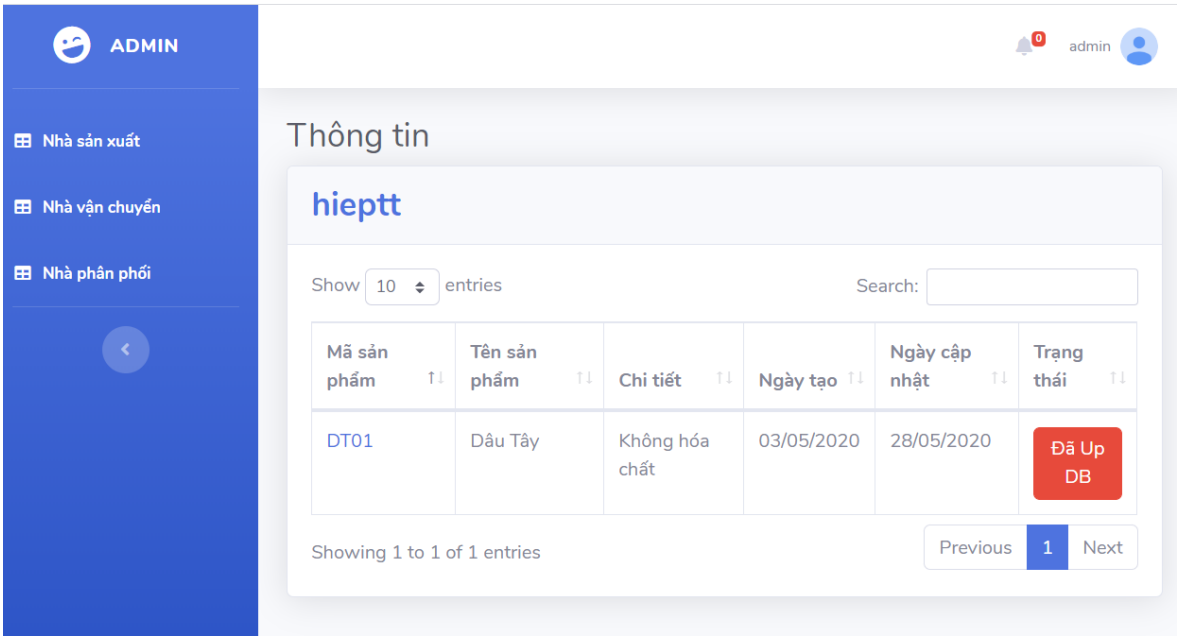
Mặc định trang đăng nhập dành cho quản trị viên sẽ tách riêng trang đăng nhập của thành viên. Đây không phải là vấn đề lớn vì có thể tích hợp cả hai trang lại với nhau. Khi quản trị viên đăng nhập thành công, quản trị viên sẽ phải phê duyệt các thông tin mà thành viên gửi lên trước khi chúng được thêm vào BigchainDB.



Hình 36. Giao diện trang đăng nhập cho admin



Hình 37. Giao diện trang quản lý tài khoản của admin



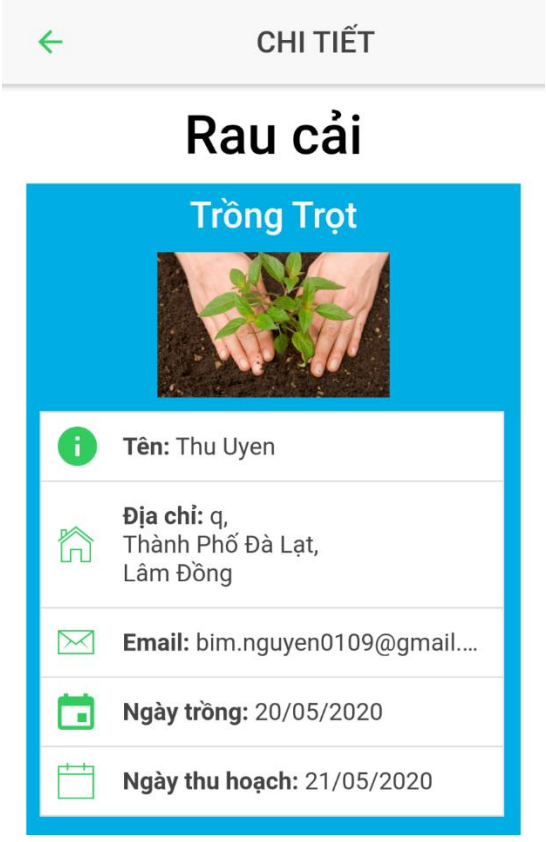
Hình 38. Giao diện trang quản lý những sản mà người dùng đã thêm và đưa vào blockchain

III.3.3. Khối ứng dụng di động

Chức năng chính của ứng dụng này là quét mã QR dán trên nông sản, sau đó lấy thông tin của nông sản đó từ BigchainDB rồi xuất lên màn hình cho người dùng xem. Yêu cầu cần phải có kết nối mạng Internet thông qua Wifi hoặc 3G/4G và có camera.



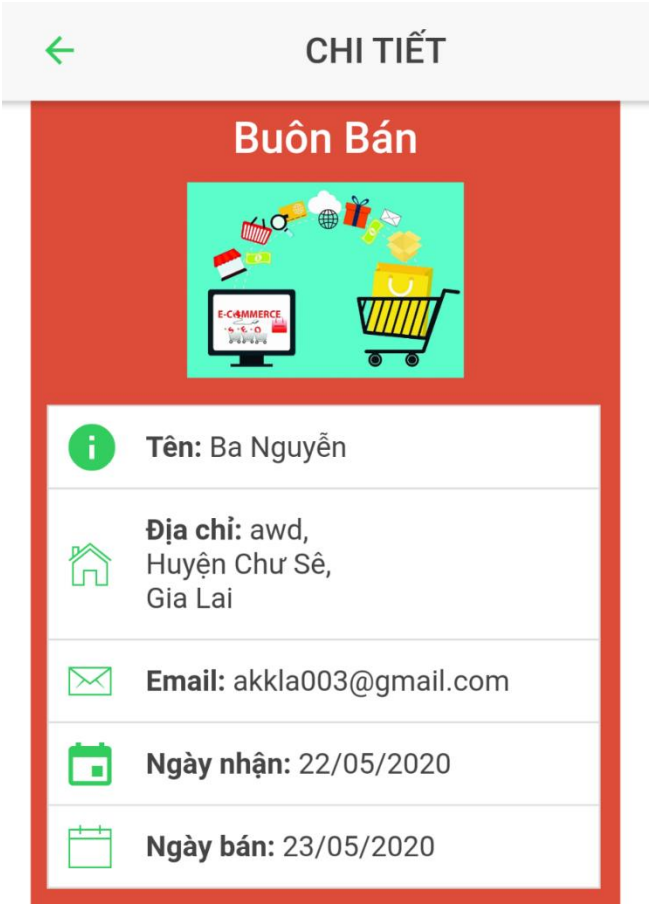
Hình 39. Màn hình chính của ứng dụng



Hình 40. Xem thông tin người trồng



Hình 41. Xem thông tin người vận chuyển



Hình 42. Xem thông tin người bán

Như vậy, thông qua ứng dụng này, người dùng nắm bắt được các thông tin cơ bản trong chuỗi cung ứng như giai đoạn trồng trọt, giai đoạn chăm sóc, giai đoạn vận chuyển, giai đoạn buôn bán.

KẾT LUẬN VÀ KIẾN NGHỊ

1. Kết luận

Công nghệ Blockchain đã cho thấy những tiềm năng to lớn, giúp các ngành công nghiệp và nông nghiệp truyền thống chuyển mình phát triển cùng với nền Công nghiệp 4.0 và mang trong mình các đặc trưng như: tính phi tập trung, tính bất biến, tính phân tán, tính minh bạch. Chính nhờ các đặc trưng này, các khung làm việc dựa trên Blockchain đang rất được cộng đồng quan tâm và áp dụng trên nhiều lĩnh vực như tài chính ngân hàng, kinh tế, chính trị - xã hội, y tế, giáo dục, hợp đồng thông minh,…

Chính nhờ đó mà việc ứng dụng công nghệ thông tin trong lĩnh vực nông nghiệp – vốn đã gắn liền với đời sống vật chất và tinh thần của người Việt Nam chúng ta từ hàng ngàn năm nay – đã sẽ từng bước không còn mang tiếng "lạc hậu" bởi vì không có gì mà các ngành khác áp dụng được Blockchain mà nông nghiệp lại không được cả nữa và tiến đến một nền nông nghiệp thông minh. Với định hướng trong tương lai tất cả mọi thứ đều có đặc trưng là minh bạch, phân tán, bất biến thì công nghệ Blockchain ở điểm hiện tại rất đáng được quan tâm để ứng dụng trong nông nghiệp cũng như nhiều các lĩnh vực khác.

Đề tài này đã áp dụng công nghệ Blockchain, cụ thể là nền tảng BigchainDB, để giải quyết bài toán truy xuất nguồn gốc nông sản. Kết quả của đề tài là đã xây dựng được hệ thống hỗ trợ quản lý, truy xuất nguồn gốc nông sản và thử nghiệm áp dụng trên một số nông sản của Đà Lạt. Cụ thể:

- **Về lý thuyết**: Hiểu được khái niệm công nghệ chuỗi khối Blockchain, kiến trúc và các mô hình đồng thuận cũng như quy trình xử lý trong chuỗi cung ứng nông sản hiện nay.
- **Về thực nghiệm**: Đã xây dựng và triển khai thử nghiệm thành công hệ thống gồm các phân hệ và chức năng khác nhau nhằm giải quyết vấn đề lớn "truy xuất nguồn gốc nông sản bằng công nghệ Blockchain". Hệ thống này có tính khả thi cao và có thể mở rộng, đặc biệt là có thể kết hợp với các thiết bị khác như cảm biến, camera,… để tạo thành hệ thống IoT hoàn chỉnh, tự động hóa các quy trình nhập liệu, kiểm tra thông tin đưa vào BigchainDB.

Hệ thống đã được phát triển gồm các phân hệ và chức năng sau:

- *Phân hệ Quản lý Hệ thống* bao gồm hệ thống các máy tính trong mạng BigchainDB do quản trị viên quản lý có chức năng lưu trữ thông tin dưới dạng chuỗi khối.
- *Phân hệ Quản lý Nông sản* bao gồm máy chủ web do quản trị viên quản lý, nhà sản xuất, nhà vận chuyển và nhà cung cấp có vai trò cung cấp thông tin liên quan đến nông sản ứng với nhiệm vụ của mình.
- *Phân hệ Người tiêu dùng* bao gồm ứng dụng quét mã và hiển thị thông tin nguồn gốc nông sản, người tiêu dùng sử dụng ứng dụng này để nắm được các thông tin của nông sản.

Tuy nhiên, kết quả của đề tài còn tồn tại một số khó khăn, hạn chế sau:

- Khó khăn:
    - Dịch bệnh Covid-19 xảy ra ngay khi bắt đầu học kỳ 2 năm học 2019-2020 dẫn đến một số hoạt động nghiên cứu bị đình trệ.
    - Do phạm vi nghiên cứu của đề tài (kinh phí, thời gian) nên chưa đi chuyên sâu vào triển khai thực tế nhiều trên một số nông sản trồng tại Đà Lạt.
- Hạn chế:
    - Liên quan đến BigchainDB
        - Phải cài đặt và cấu hình BigchainDB nhiều lần trên các máy ảo Ubuntu để chúng có thể hoạt động được như mong đợi.
        - Mạng BigchainDB chưa "thật sự" phân tán.
        - Tồn tại nhiều lỗi bảo mật.
    - Liên quan đến ứng dụng đã phát triển
        - Sự hạn chế về chuyên môn kỹ thuật của các thành viên trong nhóm.
        - Chưa có nhiều kinh phí, trang thiết bị để triển khai hệ thống này đầy đủ.

2. Hướng phát triển

Từ các khó khăn trên và các kết quả đạt được, đề tài dự kiến sẽ mở rộng phát triển ở các hướng sau:

- Áp dụng thực tế trên nhiều loại nông sản hiện có trên Đà Lạt. Đề tài này được hình thành nhằm giải quyết một trong những vấn đề quan tâm hiện nay là "truy xuất

nguồn gốc nông sản" thế nên nếu có điều kiện thì áp dụng thực tế vào các nông trại tại Đà Lạt, mời các bên liên quan trong chuỗi cung ứng nông sản tham gia vào hệ thống, như vậy tạo thành một "quy trình" đầy đủ của hệ thống, đạt hiệu quả cao và thông tin lưu trữ sẽ đầy đủ, đảm bảo hơn.

- Kêu gọi vốn đầu tư và trang thiết bị để đề tài có thể tiếp tục phát triển. Đề tài này có thể đáp ứng các tiêu chí của các cuộc thi Khoa học Kỹ thuật từ cấp Tỉnh lên đến Trung ương, các hội thảo Khoa học nếu đề tài này được triển khai thực tế. Mà để đề tài đi từ thực nghiệm sang thực tế thì cần phải có sự đầu tư về nhân lực, tiền bạc và máy móc.
- Khắc phục các lỗi bảo mật đang tồn tại. Mặc dù đề tài sử dụng BigchainDB được biết như một ứng dụng điển hình của Blockchain thế nhưng cũng như các hệ thống khác, đặc biệt là thuở sơ khai thì không thể không tránh khỏi các sai sót trong lập trình, cấu hình và bảo mật. Điểm yếu hiện tại của hệ thống là chưa có chứng thực các yêu cầu API gửi đến mạng BigchainDB nên hiện giờ, ai cũng có đọc và ghi lên đó được.
- Triển khai BigchainDB trên nhiều nền tảng như Azure, AWS, Digital Ocean. Để đảm bảo tính an toàn và tính phân tán thì mạng BigchainDB nên cài đặt trên nhiều nền tảng máy ảo, lý tưởng nhất là nên đặt tại nhiều quốc gia và có chính sách pháp lý ràng buộc rõ ràng, nghiêm ngặt nhằm tránh sự tấn công có chủ đích vào hệ thống và đảm bảo hệ thống hoạt động ổn định khi bị tấn công.
- "Chuyển giao công nghệ" hoặc "Đưa ra thị trường". Đề tài có thể bàn giao công nghệ như mã nguồn website, mã nguồn ứng dụng quét mã, mạng BigchainDB cho các công ty nếu họ muốn thực sự quan tâm, muốn sở hữu kỹ thuật được sử dụng trong đề tài. Ngoài ra, nhóm có thể tự phát triển, sử dụng kết quả của đề tài để kinh doanh và thu lợi nhuận.

TÀI LIỆU THAM KHẢO

[1] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *IEEE 6th International Congress on Big Data*, 2017.

[2] "Xây dựng thương hiệu nông sản Việt Nam ra toàn cầu," Báo Sài Gòn Giải phóng, 10 9 2018. [Online]. Available: https://www.sggp.org.vn/xay-dung-thuong-hieu-nong-san-viet-nam-ra-toan-cau-544678.html. [Accessed 21 6 2020].

[3] "Sau 9 năm đàm phán, thanh long Việt Nam lần đầu sang Úc," Báo Tuổi trẻ, 20 9 2017. [Online]. Available: https://tuoitre.vn/viet-nam-thanh-nuoc-dau-tien-dua-trai-thanh-long-vao-uc-2017092017171634.htm. [Accessed 21 6 2020].

[4] "Đồng Tháp: Hợp tác xã xoài Mỹ Xương thí điểm ứng dụng blockchain," Báo Công luận, 17 9 2018. [Online]. Available: https://congluan.vn/dong-thap-hop-tac-xa-xoai-my-xuong-thi-diem-ung-dung-blockchain-post44913.html. [Accessed 21 6 2020].

[5] "Niên giám thống kê năm 2015," Cục Thống kê Tỉnh Lâm Đồng, 2015. [Online]. Available: http://cucthongke.lamdong.gov.vn/Default.aspx?Act=10&IDNews=726. [Accessed 21 6 2020].

[6] V. T. N. Lan and N. V. Tuấn, Giáo trình Phương pháp Nghiên cứu khoa học giáo dục, Thành phố Hồ Chí Minh: Đại học Quốc gia Thành phố Hồ Chí Minh, 2012.

[7] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology, Gaithersburg, Maryland, USA, 2018.

[8] S. Purkayastha, "Compare eight Blockchain platform to kick start your next project," Radiostud, 6 9 2018. [Online]. Available: https://radiostud.io/eight-blockchain-platforms-comparison/. [Accessed 21 6 2020].

[9] "Top Blockchain platforms of 2020," LeewayHertz, [Online]. Available: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/.

[Accessed 21 6 2020].

[10] "BigchainDB: Features & Use Cases," BigchainDB GmbH, [Online]. Available: https://www.bigchaindb.com/features/. [Accessed 21 6 2020].

[11] "Own the Music You Stream with Resonate," [Online]. Available: https://www.bigchaindb.com/usecases/ip/resonate.pdf. [Accessed 24 6 2020].

[12] "Verified Educational Credentials with Recruit Technologies," [Online]. Available: https://www.bigchaindb.com/usecases/identity/recruit.pdf. [Accessed 24 6 2020].

[13] "Every Product Has a Story - innogy's Digital Product Memory," [Online]. Available: https://www.bigchaindb.com/usecases/supplychain/innogy.pdf. [Accessed 24 6 2020].

[14] "Blockchain Powered Land Registry in Ghana with BenBen," [Online]. Available: https://www.bigchaindb.com/usecases/government/benben.pdf. [Accessed 24 6 2020].

[15] "ASP.NET MVC Pattern," Microsoft, [Online]. Available: https://dotnet.microsoft.com/apps/aspnet/mvc. [Accessed 21 6 2020].

[16] "Ionic Framework," Ionic, 2 4 2020. [Online]. Available: https://ionicframework.com/docs. [Accessed 21 6 2020].

[17] T. McConaghy, "The Status of the BigchainDB Testnet," 12 6 2019. [Online]. Available: https://blog.bigchaindb.com/the-status-of-the-bigchaindb-testnet-90d446edd2b4. [Accessed 21 6 2020].

[18] BigchainDB GmbH, "BigchainDB 2.0 Whitepaper," 14 5 2018. [Online]. Available: https://www.bigchaindb.com/whitepaper/. [Accessed 21 6 2020].

[19] BigchainDB Contributors, "BigchainDB Networks," BigchainDB GmbH, [Online]. Available: http://docs.bigchaindb.com/projects/server/en/latest/networks.html. [Accessed 21 6 2020].

PHỤ LỤC THUẬT NGỮ

STT	Từ tiếng Anh	Nghĩa tiếng Việt	Chú giải
1	BigchainDB Consortium	Hiệp hội BigchainDB	Là những người hoặc tổ chức mà chạy các nút trong mạng BigChainDB này. Một hiệp hội phải có cấu trúc quản lý việc đưa ra các quyết định. Nếu một mạng BigChainDB được chạy bởi một công ty đơn lẻ thì thuật ngữ "hiệp hội" chính là công ty đó.
2	BigchainDB Network	Mạng BigchainDB	Một tập hợp các nút BigChainDB kết nối lẫn nhau tạo nên một mạng BigChainDB. Mỗi một nút trong mạng chạy cùng phần mềm và có thể có một máy làm công việc quản lý.
3	BigchainDB Node	Nút BigChainDB	Là một thiết bị (hoặc thiết bị logic) chạy BigChainDB Server và các phần mềm liên quan. Mỗi một nút được điều khiển bởi một người hoặc tổ chức.
4	Broadcast	Phát sóng	Cách thức truyền tin được gửi từ một điểm đến tất cả các điểm khác trong cùng một mạng.
5	Checksum	Giá trị tổng kiểm/ giá trị kiểm tra	Giá trị tính toán được gắn vào một gói dữ liệu, tập tin. Dùng để kiểm tra tính toàn vẹn của dữ liệu khi truyền qua mạng.
6	CheckTx	Kiểm tra Giao	Bước đầu tiên để kiểm tra một giao

		dịch	dịch, với Tx là chữ viết tắt của Transaction
7	Cryptocurrency	Tiền điện tử/ tiền mã hóa	Là một tài sản kỹ thuật số được thiết kế để làm việc như là một trung gian trao đổi mà sử dụng mật mã để đảm bảo các giao dịch của nó.
8	Digital Asset	Tài sản kỹ thuật số	Là bất cứ thứ gì tồn tại ở định dạng nhị phân và đi kèm với quyền sử dụng.
9	Distributed Consensus	Đồng thuận phân tán	Đảm bảo sự đồng thuận của dữ liệu giữa các nút trong một hệ thống phân tán hoặc đạt được thỏa thuận đề xuất.
10	Framework	Khung phần mềm	Là một sự trừu tượng trong đó phần mềm cung cấp chức năng chung có thể được thay đổi có chọn lọc bằng mã do người dùng viết thêm, do đó cung cấp phần mềm dành riêng cho ứng dụng.
11	KYC (Know Your Customer/ Know Your Client)	Biết khách hàng của bạn	Là quá trình một doanh nghiệp xác minh danh tính của khách hàng và đánh giá sự phù hợp của họ, cùng với những rủi ro tiềm ẩn của ý định bất hợp pháp đối với mối quan hệ kinh doanh.
12	Mempool	Vùng nhớ	Là nơi chứa các giao dịch đang chờ xử lý. Trong Bitcoin, đó là nơi tất cả các giao dịch Bitcoin chưa được xác nhận chờ đợi cho đến khi tất cả các xác nhận được phát hành.

13	Miner (Bitcoin)	Máy đào/ Người đào tiền ảo	Các máy tính có nhiệm vụ bảo mật mạng và thực hiện tính toán để chấp nhận các giao dịch hợp lệ thành các khối trong Blockchain .
14	Payment	Thanh toán	Là sự chuyển giao tài sản của một bên cho bên kia, thường được sử dụng khi trao đổi sản phẩm hoặc dịch vụ trong một giao dịch có ràng buộc pháp lý.
15	Prototype Model	Mô hình nguyên mẫu	Là một mô hình phát triển phần mềm được phát triển dựa trên các yêu cầu hệ thống, dựa vào bản nguyên mẫu mà khách hàng có cái nhìn tổng quan về hệ thống thực tế.
16	Record	Bản ghi/ ghi dữ liệu	Là quá trình ghi lại dữ liệu hoặc biến đổi thông tin sang một định dạng nào đó để lưu trữ trên một phương tiện lưu trữ.
17	Remittance	Kiều hối/ chuyển tiền	Là tiền bạc được di chuyển từ những người đang trú ngụ hay là lao động ở nước ngoài đến thân nhân của họ tại quê hương.
18	Repository	Kho lưu trữ/ kho chứa	Là một vị trí lưu trữ cho các gói phần mềm.
19	Reputation System	Hệ thống danh tiếng	Là các chương trình cho phép người dùng đánh giá lẫn nhau trong các cộng đồng trực tuyến nhằm tạo dựng niềm tin thông qua danh tiếng.
20	Smart Contract	Hợp đồng thông minh	Là một giao thức máy tính nhằm tạo điều kiện kỹ thuật số, xác minh hoặc

			thực thi đàm phán hoặc thực hiện hợp đồng. Hợp đồng thông minh cho phép thực hiện các giao dịch đáng tin cậy mà không cần bên thứ ba. Các giao dịch này có thể theo dõi và không thể đảo ngược.
21	Supply Chain	Chuỗi cung ứng	Là một hệ thống các tổ chức, con người, hoạt động, thông tin và các nguồn lực liên quan tới việc di chuyển sản phẩm hay dịch vụ từ nhà cung cấp hay nhà sản xuất đến người tiêu dùng.
22	Tamper Evident	Bằng chứng can thiệp	Là một thiết bị, nhãn, công cụ hoặc quá trình phát hiện sự truy cập, thay đổi, loại bỏ, gây tổn hại trái phép vào đối tượng được bảo vệ.
23	Tamper Resistance	Chống can thiệp	Là các nhãn hoặc quá trình đóng gói được thiết kế để ngăn cản một ai đó mở và tiếp cận nội dung bên trong một vật.
24	Timestamp	Dấu thời gian	Là một chuỗi các ký tự hoặc thông tin được mã hóa xác định khi một sự kiện nào đó xảy ra, thường đưa ra ngày và giờ trong ngày, đôi khi chính xác đến một phần nhỏ của một giây.
25	UI (User Interface)	Giao diện người dùng	UI bao gồm tất cả những gì người dùng có thể nhìn thấy trên giao diện phần mềm, website, hệ điều hành.
26	UX (User Experience)	Trải nghiệm người dùng	Là những đánh giá của người dùng hay những trải nghiệm khi sử dụng một phần mềm, website, hệ điều hành.

27	Voting Power	Quyền biểu quyết	Trong BigchainDB, mặc định mỗi một nút có cùng quyền biểu quyết ngang nhau. Nếu có nhiều hơn 2/3 số phiếu đồng ý, đề xuất thay đổi đó sẽ được chấp nhận.
28	Waterfall Model	Mô hình thác nước	Là một mô hình của quy trình phát triển phần mềm, trong đó quy trình phát triển trông giống như một dòng chảy, với các pha được thực hiện theo trật tự nghiêm ngặt và không có sự quay lui hay nhảy vượt pha là: phân tích yêu cầu, thiết kế, triển khai thực hiện, kiểm thử,...

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC ĐÀ LẠT

BÁO CÁO TỔNG KẾT
ĐỀ TÀI KHOA HỌC SINH VIÊN NĂM 2020

Ổ CẮM ĐIỆN THÔNG MINH ĐIỀU KHIỂN QUA MẠNG INTERNET

Thuộc nhóm ngành khoa học: Kỹ thuật



Lâm Đồng, tháng 7 năm 2020

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC ĐÀ LẠT

BÁO CÁO TỔNG KẾT
ĐỀ TÀI KHOA HỌC SINH VIÊN NĂM 2020

Ổ CẮM ĐIỆN THÔNG MINH ĐIỀU KHIỂN QUA MẠNG INTERNET

Thuộc nhóm ngành khoa học: Kỹ thuật

Sinh viên thực hiện: Trần Thanh Dương Nam

Dân tộc: Kinh

Lớp: VTK40 - Khoa Vật lý và kỹ thuật hạt nhân

Ngành học:Điện Tử Viễn Thông Năm thứ: 4 /Số năm đào tạo: 4.5

Người hướng dẫn: Thạc sĩ. Võ Minh Phụng.

Lâm Đồng, tháng 7 năm 2020

DANH MỤC TỪ VIẾT TẮT

IoT	Internet of Things	Internet kết nối vạn vật
IDE	Intergrated Development Environment	Môi trường tích hợp dùng để viết code để phát triển ứng dụng.
ID	Identification	Thẻ nhận dạng
IP	Internet Protocol	Giao thức Internet
Vin	Voltage Input	Điện áp vào
Vout	Voltage Output	Điện áp ra
GND	Ground	Tiếp điểm đất
IFTTT	If This, Then That	Trợ lý ảo giúp tự động hoá các công việc hàng ngày

NHÓM SINH VIÊN THỰC HIỆN ĐỀ TÀI

Trần Thanh Dương	Nam	Dân tộc: Kinh
Ksor Bớt	Nam	Dân tộc: Jrai
Nguyễn Duy Khang	Nam	Dân tộc: Kinh
Đào Trọng Khôi	Nam	Dân tộc: Kinh
Nguyễn Cao Đức	Nam	Dân tộc: Kinh

Lớp VTK40

Khoa Vật Lý và Kỹ Thuật Hạt Nhân

Năm thứ: 4 - Số năm đào tạo: 4.5 năm

Ngành học: Điện Tử Viễn Thông

MỤC LỤC

LỜI NÓI ĐẦU **56**

I. MỤC ĐÍCH 57

II. NỀN TẢNG 57

III. SẢN PHẨM VÀ KẾT QUẢ 57

IV. KẾT LUẬN 57

CHƯƠNG1. TỔNG QUAN **59**

1.1. Giới Thiệu Tổng Quan Về IoT. 59

1.1.1. Thực tiễn và ứng dụng: 59

1.1.2. Kiến trúc hệ thống IoT 61

1.2. Giới Thiệu Tổng Quan Về "Chiếc Ổ Cắm Thông Minh" Và Tính Thực Tiễn Của Đề Tài. 63

1.2.1. Ổ Cắm Điện Thông Minh Là gì? 63

1.2.2. Ưu điểm của ổ cắm điện thông minh so với ổ cắm thường. 64

1.2.3. Tính phổ biến của ổ cắm thông minh trên thị trường và thách thức. 64

1.2.4. Tính ứng dụng thực tiễn của đề tài với hoàn cảnh thực tế. 65

CHƯƠNG 2. QUY TRÌNH CÔNG NGHỆ CHẾ TẠOTHIẾT KẾ PHẦN CỨNG **66**

2.1. Đặc điểm cấu tạo của thiết bị 66

2.2. Thiết kế chi tiết các khối 68

2.2.1. Thiết kế khối nguồn 68

2.2.2. Khối điều khiển trung tâm – vi điều khiển esp8266. 70

2.2.3. Khối đóng cắt dùng relay 72

3.1. Cài đặt app BLYNK 73

Tạo tài khoản Blynk 75

3.2. Điều khiển các thiết bị trong gia đình bằng giọng nói 78

1.Bên cạnh việc điều khiển bằng nút nhấn, chúng ta có thể điều khiển bật tắt các thiết bị trong ngôi nhà của mình thông qua giọng nói. 78

3.2.1.Google Assistant 79

3.2.2. IFTTT 79

Chương 4. KẾT QUẢ ĐẠT ĐƯỢC **88**

4.1. Sơ đồ nguyên lý ..... **Error! Bookmark not defined.**

4.2. Sơ đồ mạch in ..... **Error! Bookmark not defined.**

4.3. Mạch đồng sau khi hoàn tất 88
KẾT LUẬN **89**
TÀI LIỆU THAM KHẢO **91**
PHỤ LỤC **92**

LỜI NÓI ĐẦU

Ngày nay với sự phát triển vượt bậc của khoa học kỹ thuật đã làm cho cuộc sống của con người ngày càng trở nên văn minh và hiện đại hơn. Sự phát triển của kỹ thuật điện tử đã tạo ra hàng loạt những thiết bị với đặc điểm nổi bật như sự chính xác cao, tốc độ truyền tải nhanh, gọn nhẹ là những yếu tố rất cần thiết cho hoạt động của con người đạt hiệu quả cao.

Một trong những ứng dụng quan trọng trong công nghệ điện tử là kỹ thuật điều khiển từ xa. Nó đã góp phần lớn trong việc điều khiển các thiết bị từ xa hay những thiết bị mà con người không thể trực tiếp trạm vào để vận hành điều khiển. Bên cạnh đó Thuật ngữ "Internet of Things" viết tắt là IoT gần đây xuất hiện khá nhiều và thu hút không ít sự quan tâm chú ý của thế giới công nghệ.

Internet of Things được mô tả là một mạng lưới vạn vật kết nối Internet hoặc là mạng lưới thiết bị kết nối Internet, khi mà mỗi đồ vật, con người được cung cấp một định danh của riêng mình, và tất cả có khả năng truyền tải, trao đổi thông tin, dữ liệu qua một mạng duy nhất mà không cần đến sự tương tác trực tiếp giữa người với người, hay người với máy tính. Nói đơn giản IoT là một tập hợp các thiết bị có khả năng kết nối với nhau, với Internet và với thế giới bên ngoài để thực hiện một công việc nào đó. Việc kết nối thì có thể thực hiện qua Wi-Fi, mạng viễn thông băng rộng (3G, 4G), Bluetooth, ZigBee, hồng ngoại…) .

Không những vậy, kèm với sự phát triển không ngừng của điện thoại thông minh. Với một chiếc Smartphone có kết nối Internet bạn dễ dàng điều khiển được hệ thống toàn bộ thiết bị trong gia đình bạn. Việc sử dụng các phần mềm chạy trên các thiết bị di động để bạn dễ dàng quản lý các thiết bị điện trong nhà qua mạng Internet.

Con người chúng ta thường hay quên tắt các thiết bị điện khi ra khỏi nhà, thay vì phải quay trở lại nhà để tắt chúng, thì nay có thể sử dụng điện thoại thông minh với vài thao tác điều khiển là có thể tắt các thiết bị điện trong nhà.

Và ý tưởng "Ổ cắm điện thông minh điều khiển qua mạng Internet" cũng xuất phát từ nhu cầu thực tiễn như vậy. Ổ cắm thông minh là loại ổ cắm điện có khả năng thay thế ổ cắm thông thường, giúp kết nối đồ điện tử với nguồn điện. Tuy nhiên, chúng có thể bật tắt các thiết bị điện dễ dàng, thông qua kết nối Internet với smartphone, tự ngắt điện khi quá tải hay cài đặt kịch bản khởi động hoặc tắt thiết bị khi kết hợp với các cảm biến.

TÓM TẮT NỘI DUNG ĐỀ TÀI

I. MỤC ĐÍCH

- Thiết kế, phát triển sản phẩm ổ cắm điện thông minh, online dựa trên cơ sở IoT cụ thể là điều khiển từ xa bằng wifi, hoặc bất cứ nơi nào smart phone của bạn có kết nối Internet. Sản phẩm đảm bảo các tiêu chí
    - Hoạt động chính xác, ổn định, ngay cả khi các điều kiện của sản phẩm thay đổi như nhiệt độ, độ ẩm.
    - Có giao diện phần mềm giao tiếp trực quan với người dùng.
- Đưa ra một thiết kế mô hình, mà các thiết bị trong mô hình này liên kết chặt chẽ với nhau và liên kết với trung tâm điều khiển. Chỉ cần kết nối với trung tâm điều kiển này, người dùng có khả năng điều khiển toàn bộ các thiết bị mong muốn trong ngôi nhà của mình.
- Điều đặc biệt trong dự án này là khối điều khiển trung tâm sẽ kết nối với Điện thoại cầm tay thông qua wifi để điều khiển toàn bộ các thiết bị mong muốn trong ngôi nhà.

II. NỀN TẢNG

- Điện tử: Vi điều khiển ESP8266 NodeMCU lua CP2102.
- Phần mềm lập trình: Adruino IDE và thư viện đi kèm.
- Phần mềm thiết kế mạch: Proteus.
- Phần mềm kết nối điện thoại: App Blynk.

III. SẢN PHẨM VÀ KẾT QUẢ

- Thiết kế "Ổ cắm điện thông minh điều khiển qua mạng Internet" được trình bày dưới dạng một sản phẩm hoàn thiện. Toàn bộ hệ thống được điều khiển bằng Điện thoại cầm tay, thông qua app Blynk. Sản phẩm thay thế cho ổ cắm điện thông thường, mang lại các giải pháp thiết thực và giá thành phù hợp cho mỗi tổ ấm người dân Việt Nam. Giúp con người có một cuộc sống đầy đủ, hiện đại, tiện nghi và an toàn.

IV. KẾT LUẬN

- Với nền tảng nguồn mở Adruino có tính tương thích cao với nhiều thiết bị hiện nay cũng có nhiều sự linh hoạt trong lập trình, dự án "Ổ cắm điện thông minh điều khiển qua mạng Internet" có khả năng nâng cấp hiện đại nhiều hơn nữa trong tương lai gần.
- Sản phẩm có tính thực tiễn cao, vừa đơn giản, hiệu quả phù hợp với số đông người dân Việt Nam hiện nay.

CHƯƠNG1. TỔNG QUAN

1.1. Giới Thiệu Tổng Quan Về IoT.

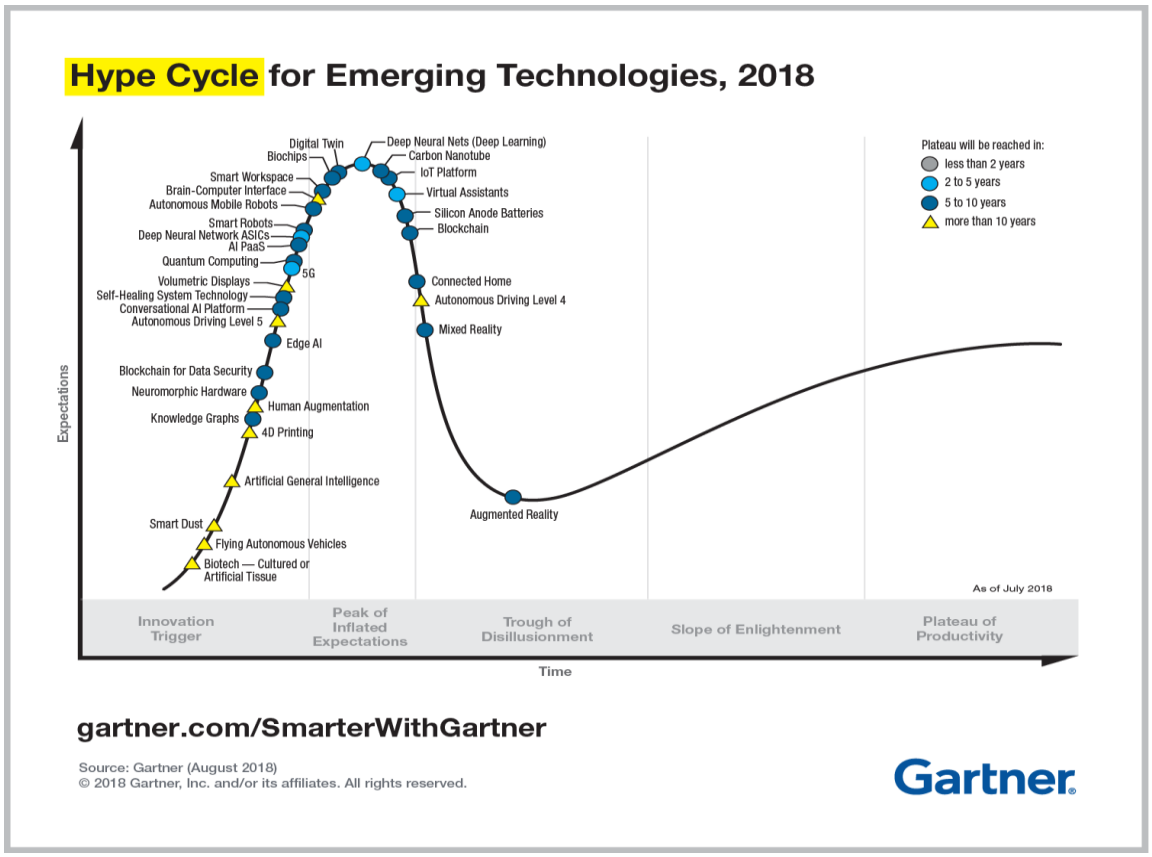
1.1.1. Thực tiễn và ứng dụng:

- Thời đại vạn vật kết nối Internet of Things (IoT) là một mạng lưới các vật thể được gắn cảm biến hoặc hệ thống điện tử đặc biệt cho phép chúng kết nối với nhau để thu thập và trao đổi dữ liệu. Các vật thể trong mạng lưới này có thể được kết nối với mạng Internet cho mục đích điều khiển từ xa.
- Xét về mặt vật chất, làm thế nào để chất lượng cuộc sống chúng ta được nâng cao, đó là khi các nhu cầu của chúng ta được đáp ứng nhiều hơn trước. Nhu cầu ở đây có thể là có đầy đủ thức ăn, có quần áo đẹp, không kẹt xe, giảm bớt những lo lắng, không phải nhớ nhiều thứ linh tinh trong đầu, … Những điều này đều sẽ được đáp ứng bởi IoT. Hiện tại, IoT ảnh hưởng lớn nhất đến 5 khía cạnh trong đời sống.

IoT có ứng dụng rộng vô cùng, có thể kể ra một số thư như sau:

- Quản lý chất thải
- Quản lý và lập kế hoạch quản lí đô thị
- Quản lý môi trường
- Phản hồi trong các tinh huống khẩn cấp
- Mua sắm thông minh
- Quản lý các thiết bị cá nhân
- Tự động hóa ngôi nhà

Theo báo cáo hàng năm của hãng Gartner về xu hướng công nghệ sẽ thay đổi thế giới trong năm 2018 thì IoT đang xếp ở mức đỉnh cao của kỳ vọng và ứng dụng của IoT trong vòng 5 năm đến 10 năm nữa sẽ ứng dụng nhiều trong đời sống thực tế.



Hình 1.1. Biểu đồ Hype Cycle của hãng Gartner

Theo một số dự đoán khảo sát được đưa ra

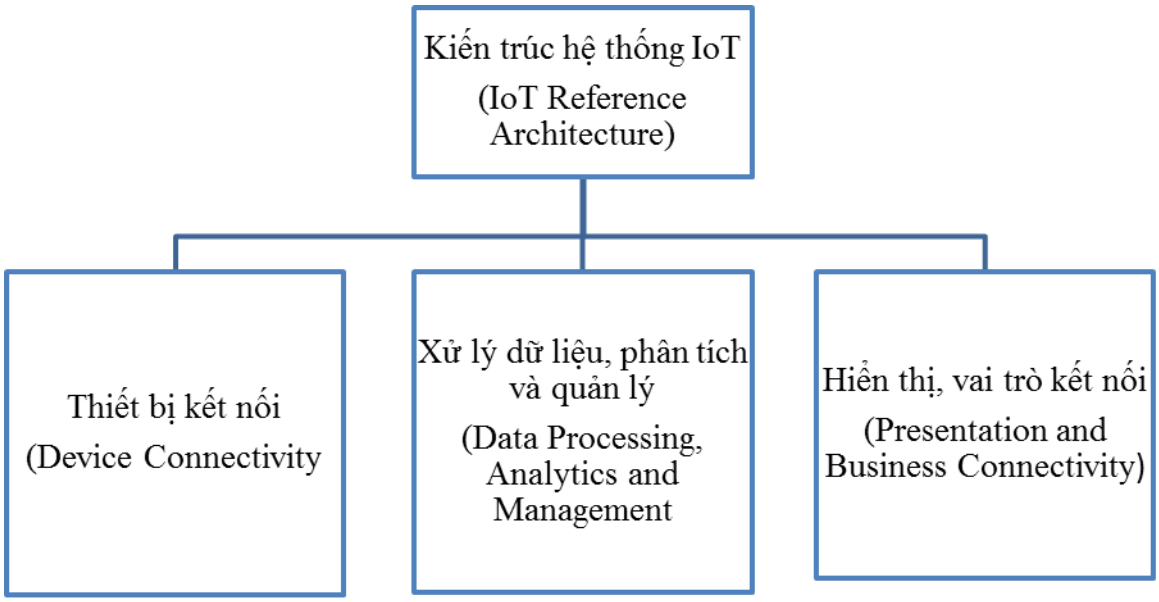


Hình 1.2. Một số dự đoán khảo sát

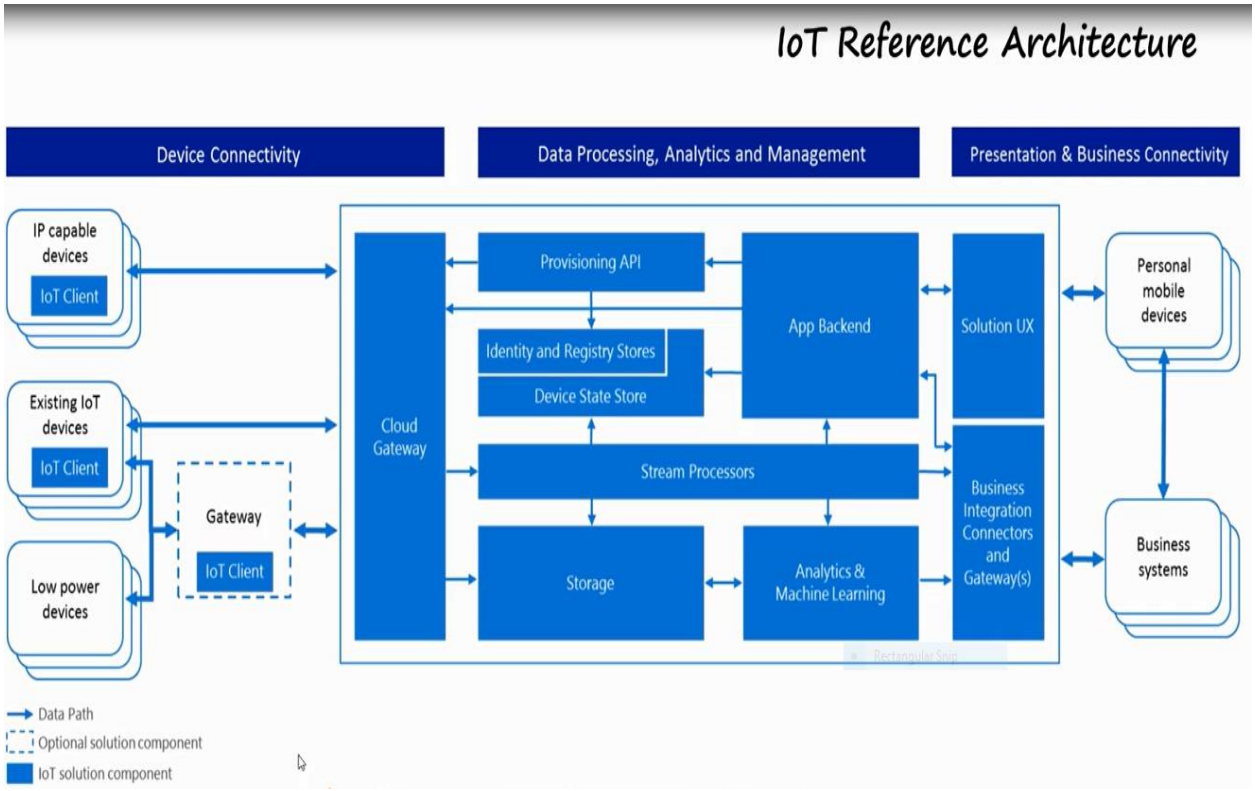
Năm 2003 với 6.3 tỷ người có 500 triệu kết nối internet, với mỗi người sở hữu 0.08 thiết bị kết nối.

Năm 2020 với 7.6 tỷ người đã lên đến 50 tỷ kết nối với 1 người sở hữu 6.58 thiết bị kết nối internet.

1.1.2. Kiến trúc hệ thống IoT



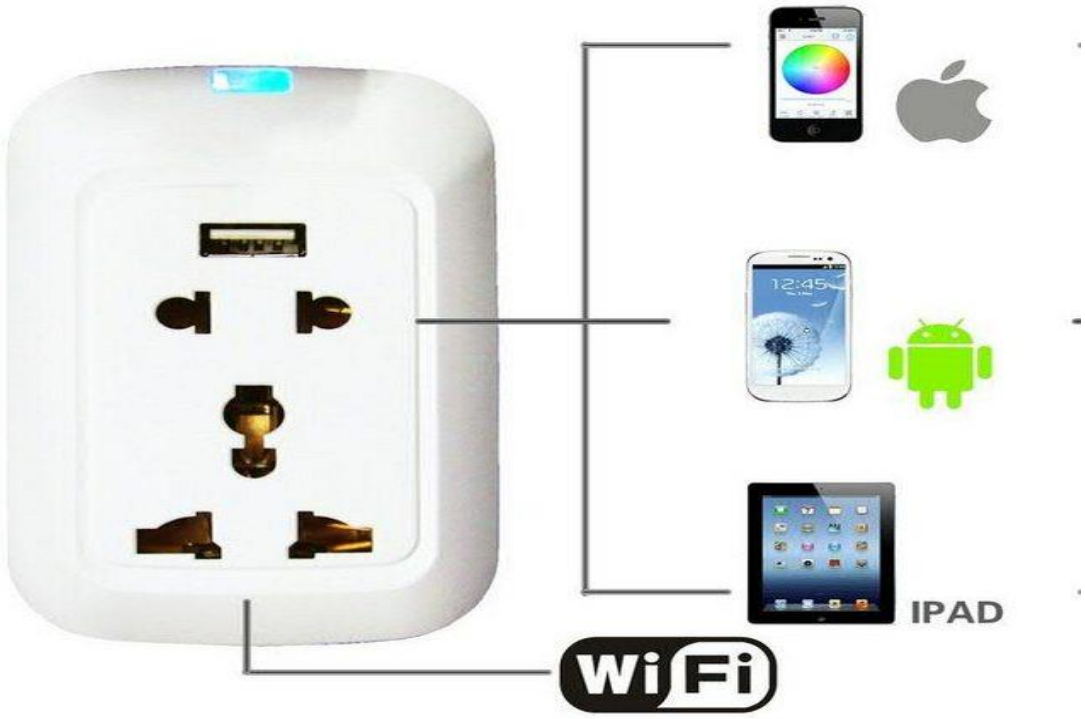
Hình 1.3. Kiến trúc một hệ thống IoT(ảnh sưu tầm từ Google)



Hình 1.4. Tổng quan về một hệ thống IoT (ảnh sưu tầm từ Google)

1.2. Giới Thiệu Tổng Quan Về "Chiếc Ổ Cắm Thông Minh" Và Tính Thực Tiễn Của Đề Tài.

1.2.1. Ổ Cắm Điện Thông Minh Là gì?



Hình 1.5: Mô hình ổ cắm thông minh.(Ảnh sưu tầm từ Google)

Ổ cắm điện thông minh là ổ cắm có khả năng tương tác với các thiết bị kết nối wifi trong nhà. Phụ kiện thông minh này được hiển thị hầu hết trên các ứng dụng của Google Assistant, Amazon Alexa, Apple HomeKit,…. để hỗ trợ tính năng điều khiển không dây đối với các thiết bị trong nhà, như bóng đèn, máy sưởi, máy giặt, máy điều hoà,... cũng như các thiết bị điện tử nói chung.

Ổ cắm thông minh là loại ổ cắm điện có khả năng thay thế ổ cắm thông thường, giúp kết nối đồ điện tử với nguồn điện. Tuy nhiên, chúng có thể bật tắt các thiết bị điện dễ dàng, thông qua kết nối Wi-Fi với smartphone, tự ngắt điện khi quá tải hay cài đặt kịch bản khởi động hoặc tắt thiết bị khi kết hợp với các cảm biến.

1.2.2. Ưu điểm của ổ cắm điện thông minh so với ổ cắm thường.

- Thứ nhất: Bật/ tắt được các thiết bị từ xa một cách dễ dàng, thay thế các công tắc cơ ở một ổ cắm bình thường bằng các relay đóng ngắt tự động.
- Thứ hai: Ít tiếp xúc vật lý nên tăng tính an toàn cho người sử dụng.
- Thứ ba: Là cứu tinh trong một số trường hợp cấp bách.

Chúng ta có thể hình dung một tình huống cụ thể như sau:

Mỗi buổi sáng bạn đều ủi quần áo tươm tất để đi làm. Một hôm bạn đã xuống dưới nhà giữ xe và chợt nhớ ra là chưa rút ổ cắm bàn ủi. Nhà bạn lại ở căn hộ tầng 50 của Vin Group, phải đợi thang máy và đi lên lại ư – chắn chắn là không. Với chiếc ổ cắm thông minh đã kết nối với chiếc smartphone của bạn rất đơn giản khi chỉ cần mở app điện thoại, chọn vào biểu tượng ổ cắm thông minh và bấm nút tắt là xong. Đối với chiếc ổ cắm thông thường thì bạn đã có cơ hội tập thể dục nâng cao sức khỏe rồi đấy.

- Thứ tư: Giúp tiết kiệm tiền điện hiệu quả .

Rất nhiều người có thói quen ra khỏi nhà thường quên không tắt thiết bị điện hoặc để chúng ở chế độ chờ .Có nhiều thiết bị khi ở chế độ chờ vẫn ngốn không ít tiền điện như là Tivi, máy tính, Wifi, các cục sạc pin, lò vi sóng, máy nướng, máy xay sinh tố…Chúng ta chỉ cần bật chế độ vắng nhà với thiết lập cài đặt sẵn, Ổ cắm điện thông minh sẽ kiểm soát toàn bộ mọi thiết bị điện trong nhà, đảm bảo mọi thiết bị sẽ được tắt khi không có người ở nhà để tiết kiệm tối đa chi phí.

1.2.3. Tính phổ biến của ổ cắm thông minh trên thị trường và thách thức.

- Được sử dụng rộng rải trong các căn hộ cao cấp, nhà hàng, khách sạn, villa..là những nơi sang trọng dành cho giới thượng lưu.
- Do giá thành sản phẩm còn cao nên khó tiếp cận đến người tiêu dùng bình dân, do vậy mà tính phổ biến của ổ cắm thông minh thực tế vẫn còn rất eo hẹp và ít người biết đến. Song người dân Việt Nam vẫn chưa thay đổi thói quen với chiếc ổ cắm thông thường.
- Khả năng hiểu biết công nghệ của người tiêu dung Việt Nam còn hạn chế, còn e ngại khi sử dụng các thiết bị công nghệ. Vì vậy cần phổ cập kiến thức công nghệ đến người sử dụng một cách thiết thực và gần gũi từ đó mới hướng người tiêu dùng đến với sản phẩm một cách nhanh chóng và hiệu quả nhất. Song song đó cũng là một thách thức chonhà sản xuất.

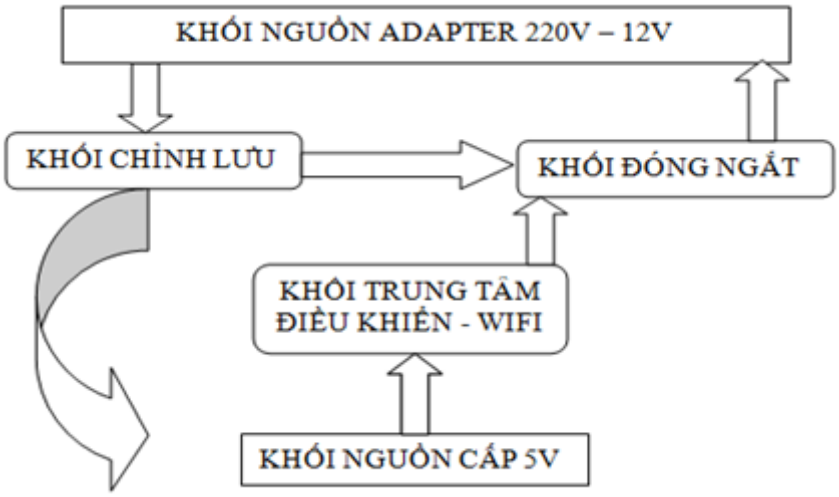
1.2.4. Tính ứng dụng thực tiễn của đề tài với hoàn cảnh thực tế.

Theo xu hướng phát triển của thế giới nhận thấy giải pháp cho một chiếc ổ cắm thông minh thực sự rất thiết yếu và là một hướng đề tài ứng dụng rất hay. Hiện nay chiếc ổ cắm thông minh đang rất phổ biến ở các nước lớn trên thế giới, tuy nhiên ở Việt Nam thì còn chưa phổ biến.Với xu hướng hiện nay, đời sống con người ngày càng phát triển và hiện đại hơn, thì nhu cầu cài đặt nhiều thiết bị điện thông minh trong nhà đặc biệt là chiếc ổ cắm sẽ mang lại sự tiện nghi bất ngờ nhờ được điều khiển tự động và ngày càng cần thiết. Do đó, tính thực tiễn của đề tài "Ổ cắm thông minh điều khiển quan mạng internet" là rất lớn.

CHƯƠNG 2. QUY TRÌNH CÔNG NGHỆ CHẾ TẠO THIẾT KẾ PHẦN CỨNG

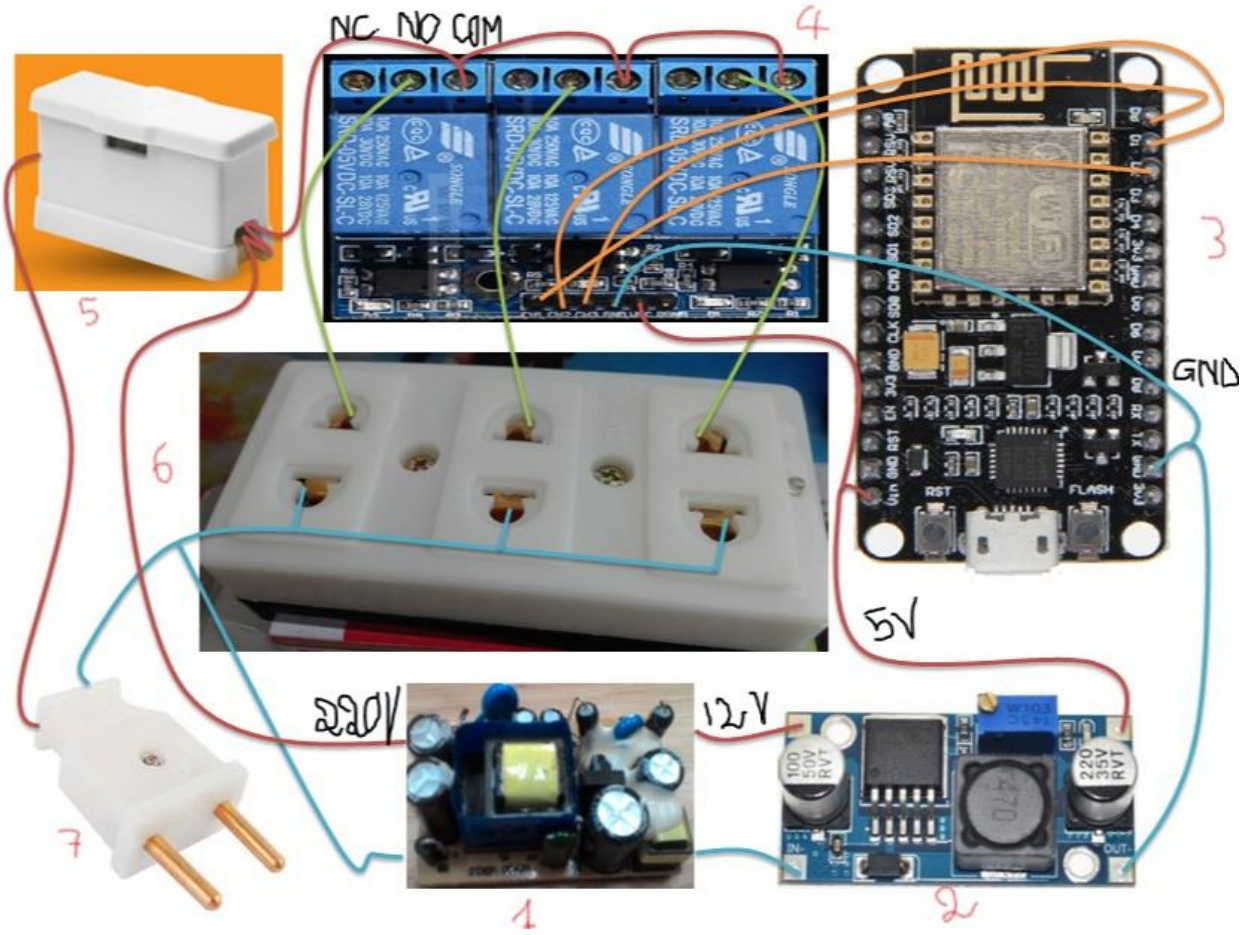
2.1. Đặc điểm cấu tạo của thiết bị

2.1.1. Sơ đồ nguyên lý



2.1.2. Sơ đồ thực tế

Thiết bị được xây dựng theo mô hình được thể hiện trong sơ đồ dưới đây.



Hình 2.1. (Hình chỉ mang tính chất mô tả)

1) Khối nguồn Adapter: Cấp điện áp xoay chiều 220VAC từ lưới, từ đây điện áp được chuyển đổi thành 12V ngỏ ra , sau đó đưa về khối tiếp theo là khối chỉnh lưu.

2) Khối giảm áp: Sử dụng module LM2596 với chức năng giảm điện áp đầu vào 12V xuống còn 5V cấp cho vi điều khiển và relay.

3) Khối wifi: Sử dụng Modul wifi ESP8266 để nhận tín hiệu thu về từ vi xử lý, gửi dữ liệu nhận được lên web sever để ta có thể theo dõi online qua wifi internet.

4) Khối đóng cắt: Sử dụng relay 5V-10A để đóng cắt mạch điện khi nhận được tín hiệu điều khiển từ người sử dụng

5) Khối cầu chì để bảo vệ mạch không bị hư hỏng khi xảy ra chập điện hoặc cháy nổ.

6) Ổ cắm kết nối các thiết bị trong nhà.

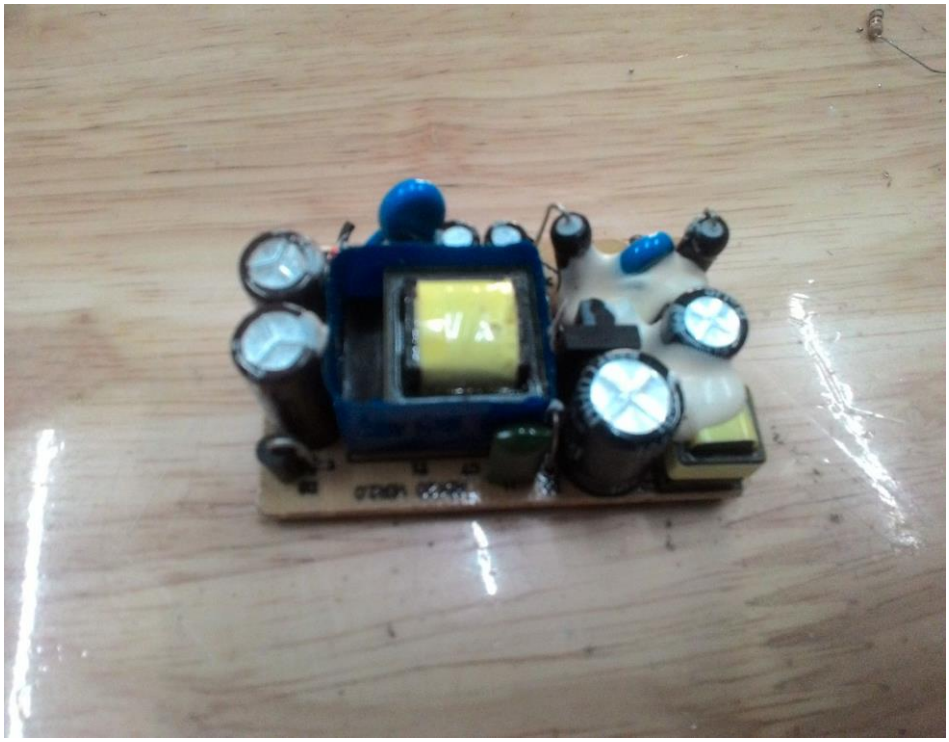
7) Phích cắm

2.2. Thiết kế chi tiết các khối

2.2.1. Thiết kế khối nguồn

Thiết bị sử dụng các cấp điện áp Mạch Adapter 220V – 12V, 5VDC, 3.3VDC

2.2.1.1. Khối nguồn Adapter.



Hình 2.2. Mạch nguồn Adapter 12V

Tận dụng nguồn Adapter sẵn có, sinh viên tháo rời mạch, mạch có chức năng chuyển đổi điện áp 220V ngỏ vào thành điện áp 12V ngỏ ra, sau đó điện áp 12V này được cấp cho module LM2596.

2.2.1.2. Khối chinh lưu và nguồn 5VDC

Ta sử dụng Module nguồn LM2596 với:

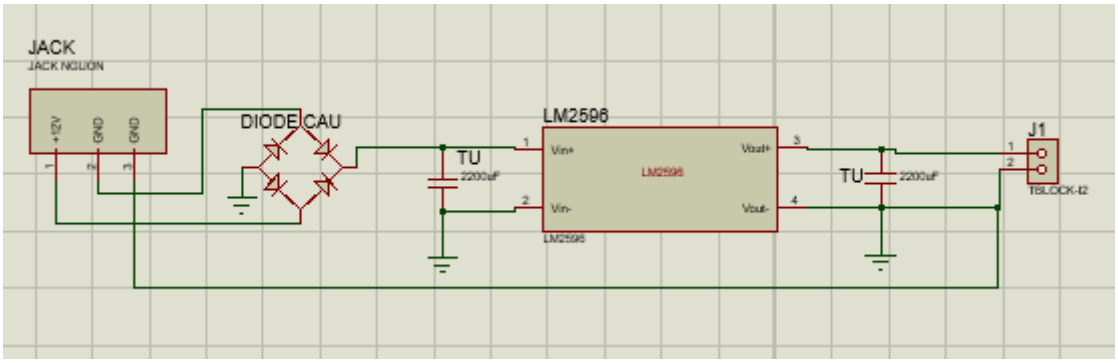
Input: Điện áp 12V được đưa từ Adapter

Output: 5VDC/3W



Hình 2.3. Mạch nguồn giảm áp 5VDC

2.2.1.2. Sơ đồ nguyên lý.

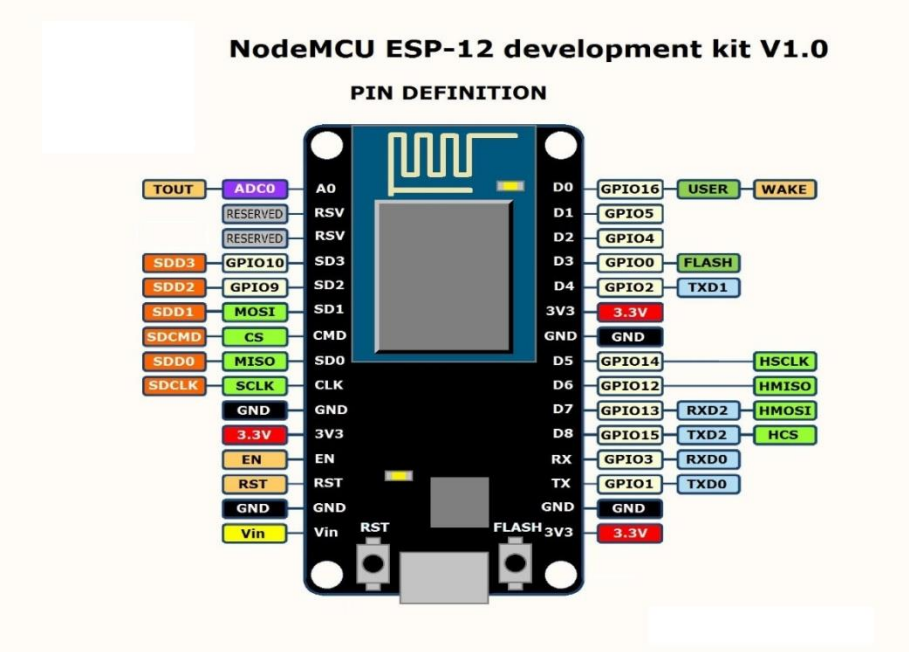


Điện áp 12V từ Adapter sẽ được đưa qua khối chỉnh lưu để chuyển đổi điện áp một chiều thành điện áp xoay chiều, sau đó đưa tín hiệu vào tụ 2200uF để làm mượt lần thứ nhất trước khi đưa vào khối module giảm áp LM2596. Module LM2596 với thành phần chủ chốt là IC LM2596 và một số linh kiên khác, sẽ chuyển đổi mức điện áp 12V thành điện áp 5V xoay chiều và ta có thể tùy chỉnh điện áp bằng cách xoay biến trở trên module. Điện áp 5V ngỏ ra cho qua tụ điện 2200uF để làm mượt trước khi cấp cho vi điều khiển Node MCU và module relay.

2.2.2. Khối điều khiển trung tâm – vi điều khiển esp8266.

▪ Khối điều khiển trung tâm đóng vai trò như một bộ não có khả năng điều khiển tất cả các thiết bị khác trong nhà như bóng đèn, cảm biến gas, cảm biến nhiệt độ, độ ẩm, đồng hồ hiển thị số…Có khả năng điều khiển mọi thiết bị trong gia đình bằng cách sử dụng điện thoại thông qua wifi.

▪ESP8266 là một chip tích hợp cao - System on Chip (SoC), có khả năng xử lý và lưu trữ tốt. ESP8266 còn cung cấp khả năng kết nối mạng wifi đầy đủ và khép kín.



Hình 2.4. ESP8266 PINOUT.

2.2.2.1. Thông tin về sản phẩm

- Chip: ESP8266EX
- Hỗ trợ kết nối WiFi: 2.4 GHz hỗ trợ chuẩn 802.11 b/g/n
- Điện áp hoạt động: 0V-3.3V
- Điện áp vào: 5V thông qua cổng USB
- Số chân I/O: 11 (tất cả các chân I/O đều có Interrupt/PWM/I2C/One-wire, trừ chân D0)
- Số chân Analog Input: 1 (điện áp vào tối đa 3.3V)
- Bộ nhớ Flash: 4MB
- Giao tiếp: Cable Micro USB
- Có thể lập trình được bằng C/C++, Arduino IDE, NodeMCU

- Nguồn 5V trực tiếp từ USB hoặc 5V qua Vin

2.2.2.2. Ứng dụng

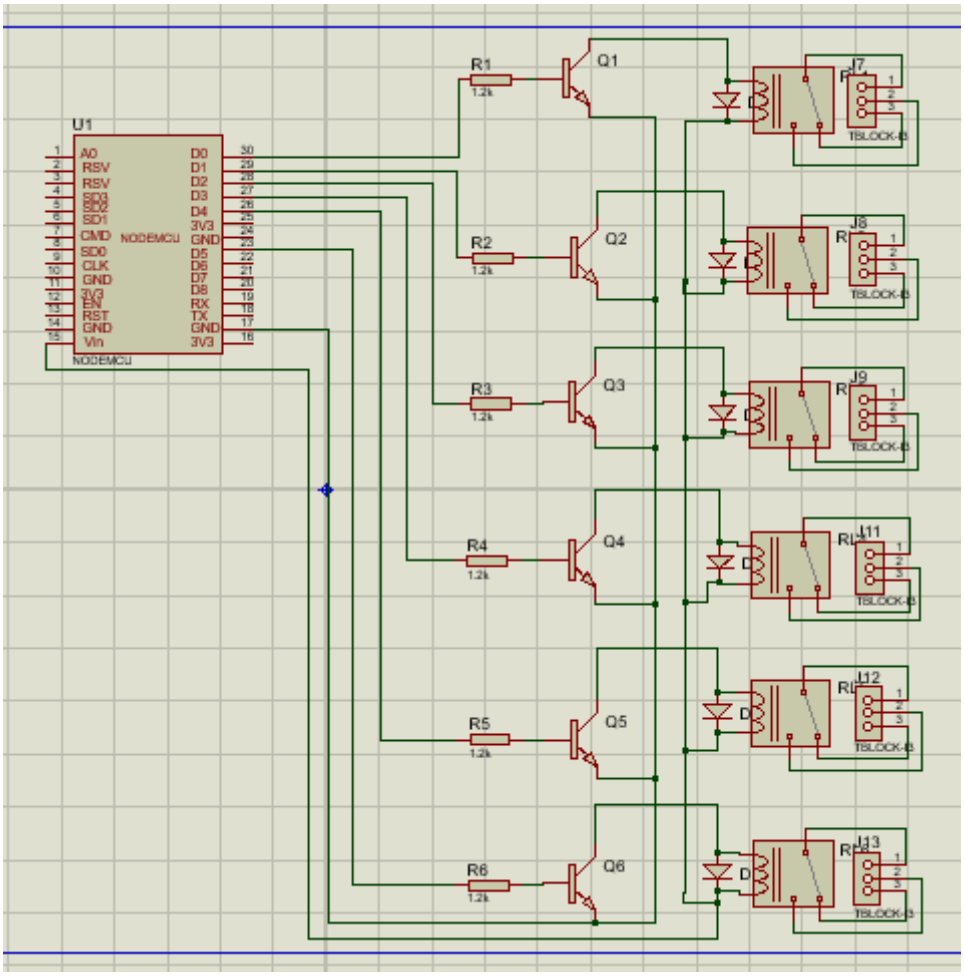
ESP8266 có thể ứng dụng trên nhiều lĩnh vực khác nhau như:

- Thiết bị dân dụng
- Tự động hoá nhà ở
- Điều khiển không dây trong công nghiệp
- Thiết bị nhận biết vị trí wifi
- Thẻ ID bảo mật
- Camera IP

2.2.2.3. Ưu điểm.

- Kết nối WiFi chính là điểm mạnh nhất của ESP8266.
- Giá thành rẻ, dễ dàng tìm kiếm trên thị trường.
- Nhỏ, gọn.

2.2.2.4. Sơ đồ nguyên lý.



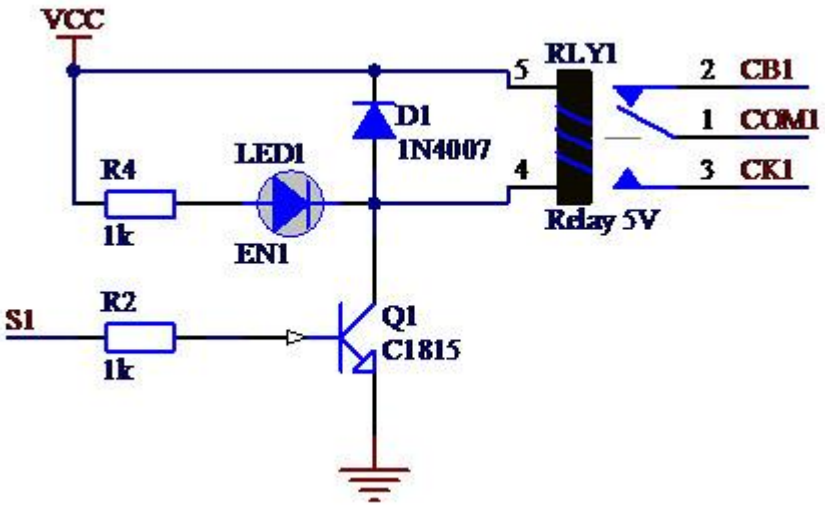
Cấp nguồn 5V vào chân Vin và nối với cực âm (Cathode) của diode 1N4007, các chân mass nối các chân E của transistor C1815 (Q1 đến Q6) và nối vào chân GND của vi điều khiển. Các chân tín hiệu kết nối với các chân digital (D0, D1, D2, D3, D4,D5) , nối lần lượt qua các điện trở (từ R1 đến R6) vào cực B của Transistor.

2.2.3. Khối đóng cắt dùng relay

+ Rơ-le là một loại linh kiện điện tử thụ động rất hay gặp trong các ứng dụng thực tế. Khi bạn gặp các vấn đề liên quan đến công suất và cần sự ổn định cao, ngoài ra có thể dễ dàng bảo trì, thì rơ-le chính là cái bạn cần tìm.

+ Nhiều rơ le sử dụng một nam châm điện để vận hành cơ khí công tắc, nhưng nguyên lý vận hành khác cũng được sử dụng, chẳng hạn như rơ le trạng thái rắn.

+ Rơ le được sử dụng khi cần kiểm soát một mạch điện bằng một tín hiệu công suất thấp (với đầy đủ cách điện giữa kiểm soát và mạch điều khiển), hoặc trong trường hợp một số mạch phải được kiểm soát bởi một tín hiệu.



Sơ đồ nguyên lý mô tả đóng ngắt một relay đơn giản

Ở đây sinh viên sử dụng Transistor NPN (C1815) để điều khiển.

Khi S1 = 1; Q1 thông, có dòng điện cấp cho cuộn hút của Relay. Tiếp điểm 1 nối với 3, đèn LED1 sáng, đồng nghĩa ổ cắm có điện, thiết bị kết nối với ổ cắm sẽ hoạt động. Ngược lại,Khi S1 = 0; Q1 tắt, không có dòng qua cuộn hút. Tiếp điểm 1 nối với 2, đèn LED1 tắt, ổ cắm không có dòng điện chạy qua, thiết bị ngắt kết nối.

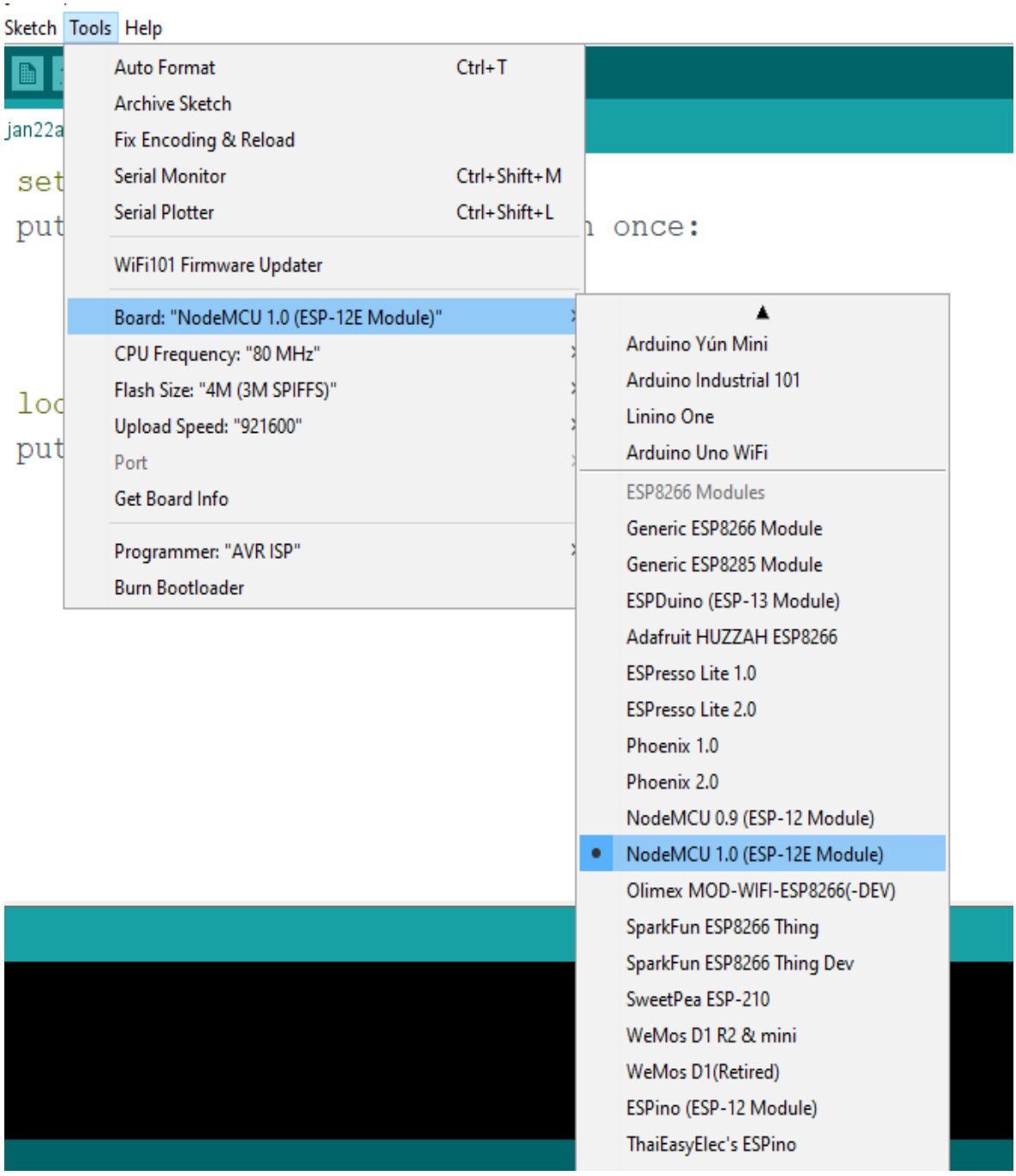
Với sơ đồ này ta có thể thay Relay 5V bằng 12V, 24V (Tương ứng VCC= 12V, 24V). Mặc dùng điện áp điều khiển S1 =0, 5V. Mạch vẫn hoạt động bình thường.

Chương 3. QUY TRÌNH CÀI ĐẶT VÀ THIẾT KẾ GIAO DIỆN PHẦN MỀM.

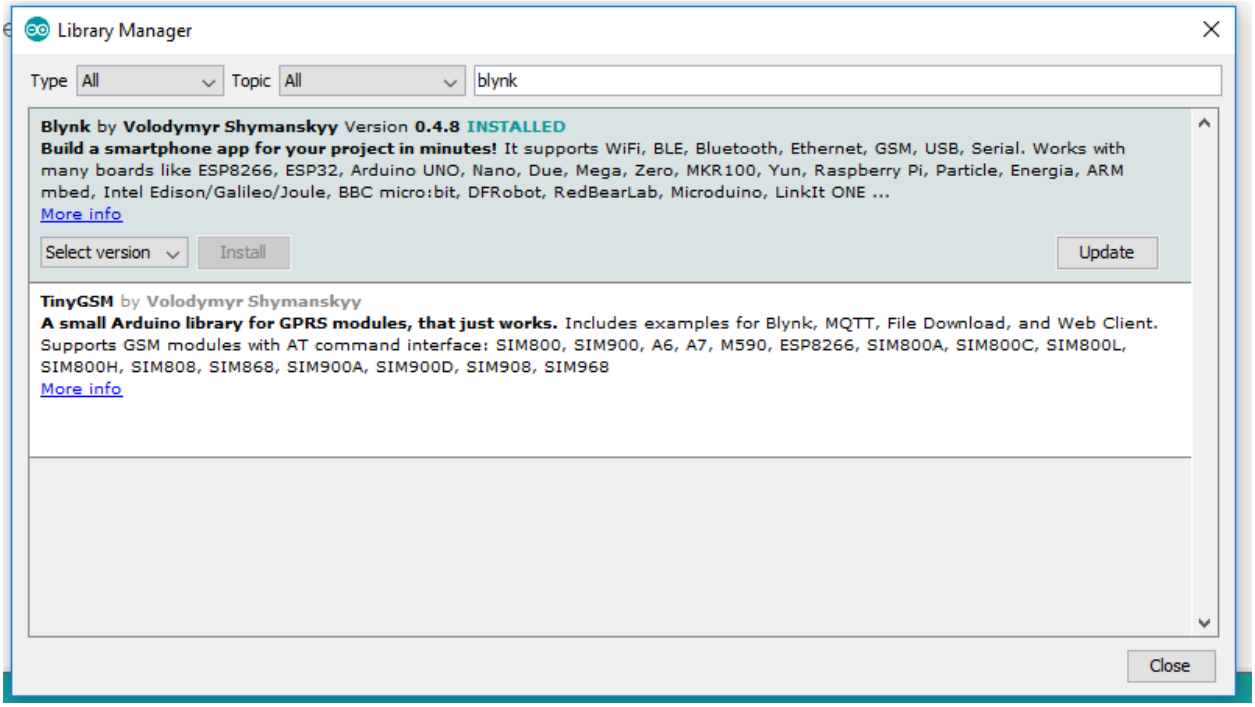
3.1. Cài đặt app BLYNK

Blynk là một ứng dụng chạy trên nền tảng iOS và Android để điều khiển và giám sát thiết bị thông qua internet. Blynk không bị ràng buộc với những phần cứng cụ thể nào cả, thay vào đó, nó hỗ trợ phần cứng cho bạn lựa chọn như Arduino, Raspberry Pi, ESP8266 và nhiều module phần cứng phổ biến khác.

Đề tài này sử dụng Blynk với NodeMCU (ESP8266). Trước khi bắt đầu cần mở Arduino IDE và chọn đúng module mình đang sử dụng, ở đây là Node MCU.



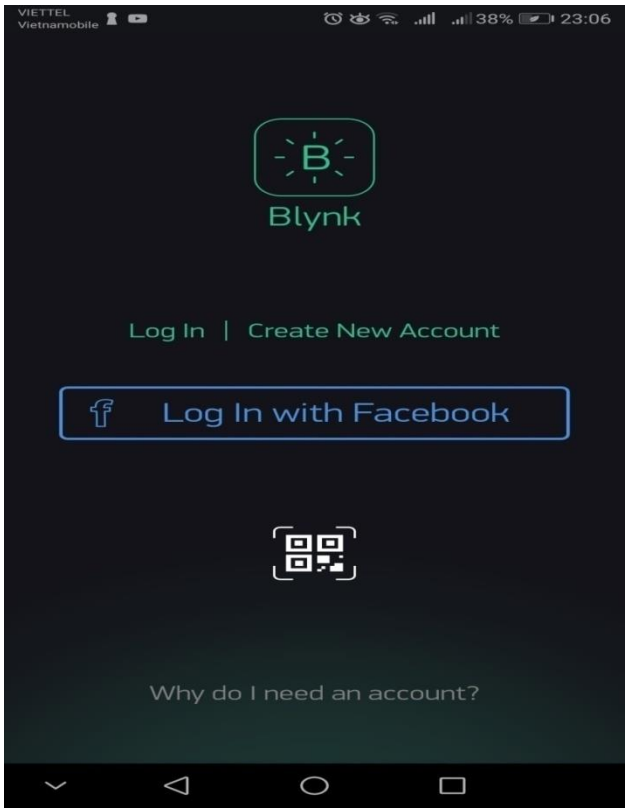
Để dùng được Blynk, ta cần cài thư viện này vào Arduino IDE:



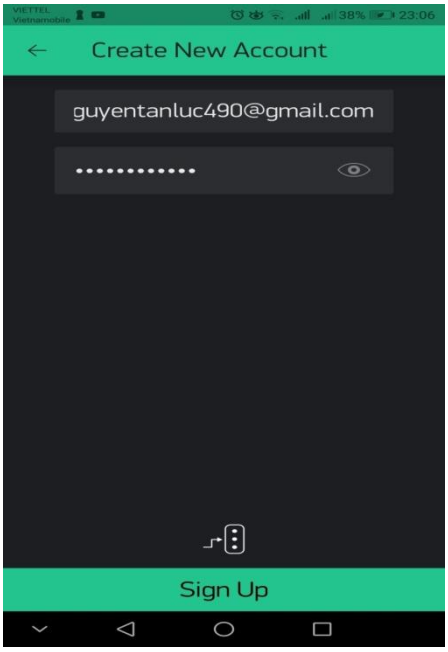
Tạo tài khoản Blynk

Để có thể sử dụng App Blynk chúng ta cần phải đăng ký một tài khoản mới. Ở đây có 2 cách đăng ký bằng Facebook hoặc tạo một tài khoản mới (Create New Account).

Dưới đây là cách đăng ký bằng **Account**.



Nhập thông tin tài khoản Gmail của các bạn. Rồi nhấn **Sign Up** để tiến hành đăng ký.

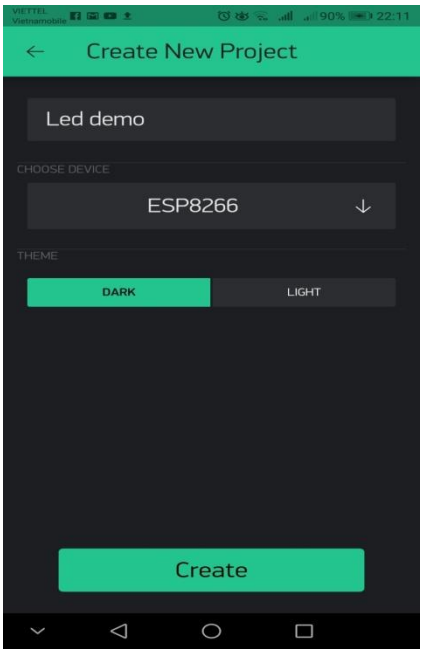


Sau khi đăng ký hoàn thành, chúng ta sẽ tiến hành tạo một Project mới.

Mình sẽ hướng dẫn các bạn tạo một dự án Bật/Tắt LED trên Blynk.

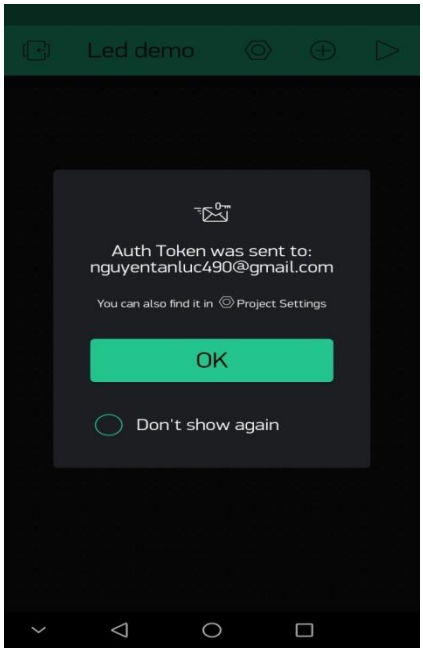
Các bạn Click vào **dấu cộng (+)** trên thanh công cụ để tiến hành tạo Project mới.

Click vào **Create** để hoàn tất việc tạo mới.

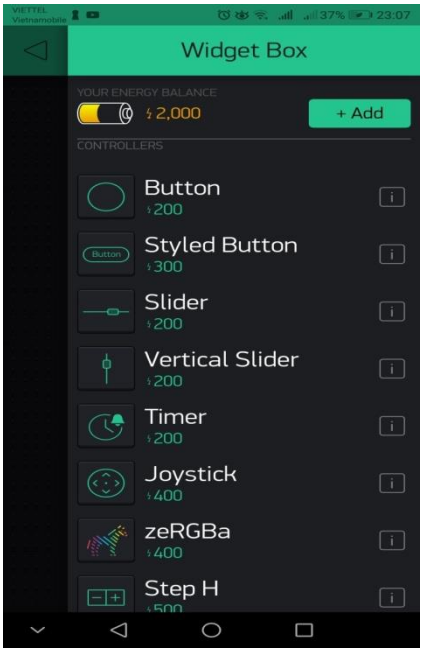


Blynk sẽ cấp cho các bạn một **mã Token**, mã này sẽ gửi trực tiếp vào Gmail mà lúc nãy bạn đăng ký.

Mã Token này dùng để chèn vào code Example của Blynk.



Để Bật/Tắt Led chúng ta cần có một nút bấm để điều khiển. **Vào Widget Box (+) > Click vào Button** để lấy nút nhấn ra.

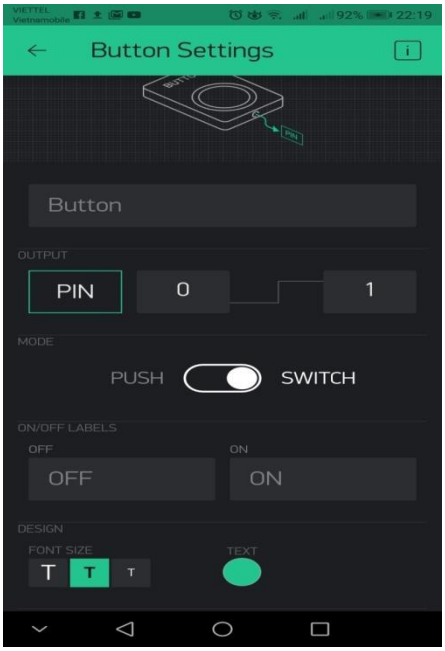


Click vào Button để tiến hành cài đặt thông số.

- Ở mục Button: Đặt tên cho nút nhấn.
- OUTPUT: Cấu hình cho PIN cần kết nối, ở đây mình chọn Digital > gp16 (chân này có LED được tích hợp trên board mạch sẵn).
- MODE: có 2 chế độ PUSH (nhấn thả) và SWITCH (nhấn giữ).

• ON/OFF LABELS: Thay đổi chế đọ hiển thị cho nút nhấn (Vd: Các bạn không thích để ON/OFF có thể thay bằng BẬT/TẮT hoặc một cái tên nào mà bạn muốn).

• DESIGN: Ở phần này các bạn có thể điều chỉnh màu sắc của nút nhấn.

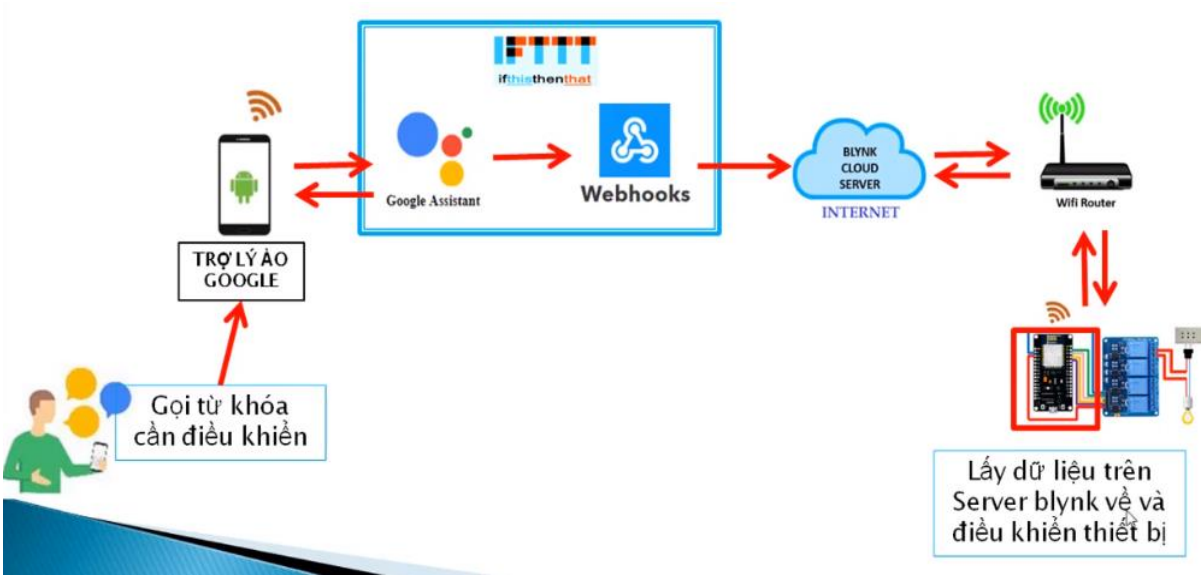


3.2. Điều khiển các thiết bị trong gia đình bằng giọng nói

1.Bên cạnh việc điều khiển bằng nút nhấn, chúng ta có thể điều khiển bật tắt các thiết bị trong ngôi nhà của mình thông qua giọng nói.

2. Chỉ với vài câu nói ra lệnh để bật hay tắt thiết bị thông qua Google Assistant có trên điện thoại chúng ta có thể điều khiển dễ dàng các thiết bị mà mình mong muốn.

3. Sơ đồ quy trình điều khiển các thiết bị bằng giọng nói diễn ra như sau:



3.2.1.Google Assistant

- Là một trợ lý cá nhân ảo được phát triển bởi Google và được giới thiệu tại hội nghị nhà phát triển của hãngvào tháng 5 năm 2016. Google Assistant có thể tham gia các cuộc trò chuyện hai chiều. Google Assistantlà công cụ để kết nối giữa Smartphone và dịch vụ IFTTT.



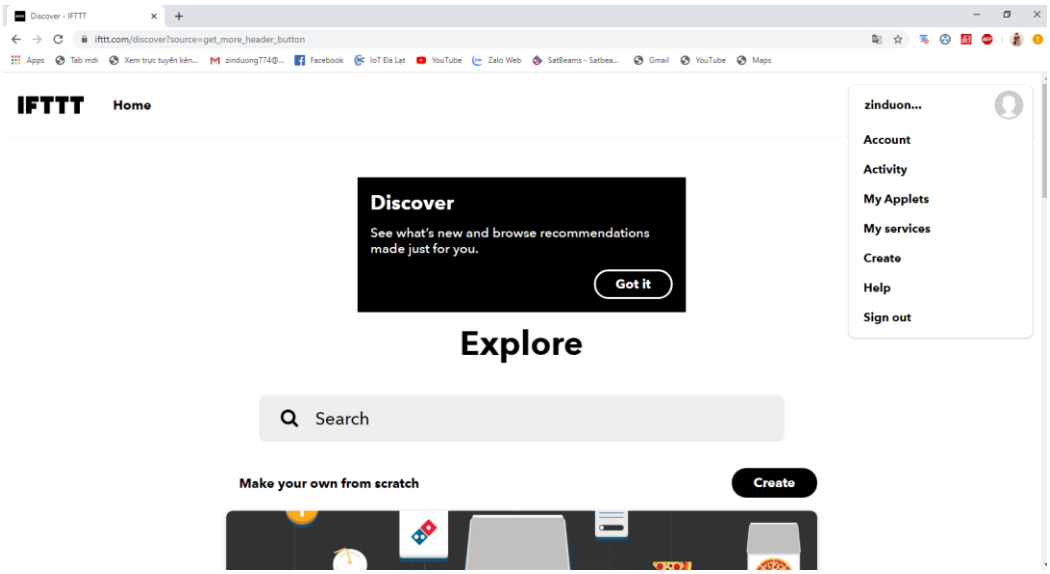
3.2.2. IFTTT

- Đây là một dịch vụ web trung gian. Nó đứng giữa hai dịch vụ để thực hiện một tác vụ khi một điều kiện nào đó xảy ra, bởi vậy mới có cái tên If this (nếu điều này xảy ra) then that (thì làm việc kia). Toàn bộ hoạt động của IFTTT dựa hết vào nguyên lý này. IFTTT giúp kết nối giữa Google Assistant và Webhook làm cho mọi thứ hoạt động cùng với nhau một cách suôn sẻ.

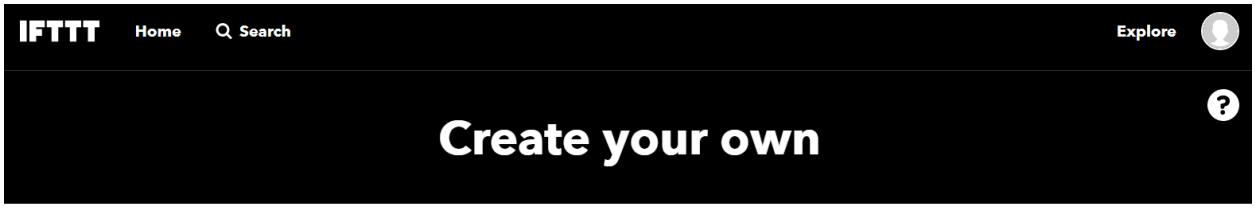


► Đăng nhập và setup trên IFTTT:

Đăng nhập bằng tài khoản của Google Assistant như trên điện thoại hoặc là đăng nhập bằng Gmail của Google.



Click Create để tạo applet mới. Ở đây chúng ta sẽ tạo 2 Applet, 1 cái cho lệnh ON, 1 cái cho lệnh OFF.





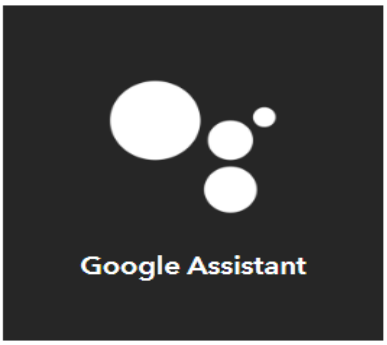
Build your own service

Với mục **THIS** thì chúng ta sẽ chọn Google Assistant như hình sau:

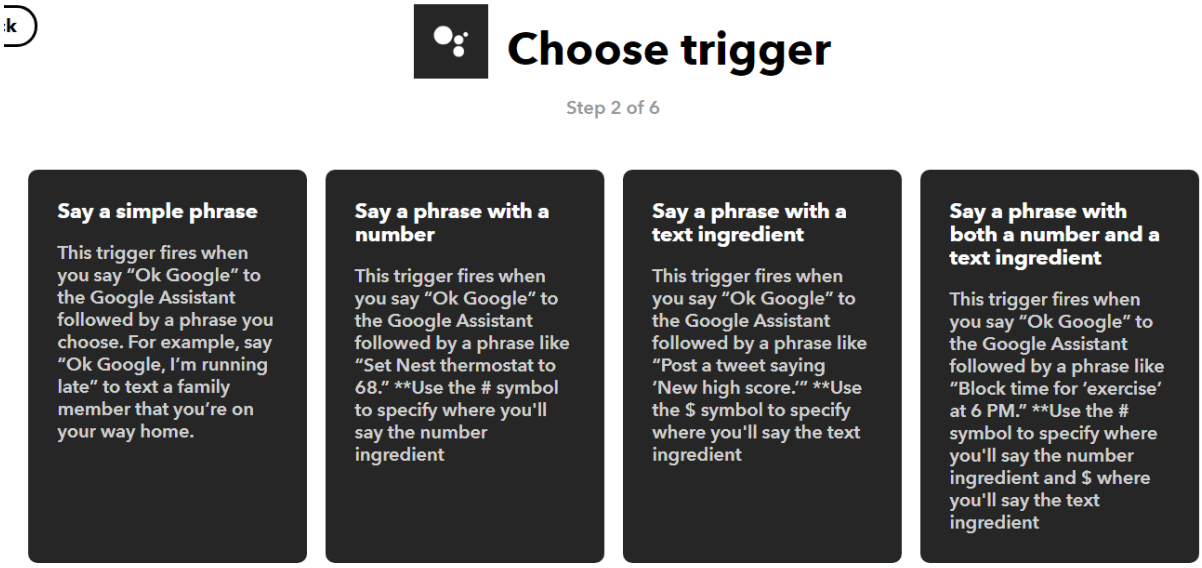
Choose a service

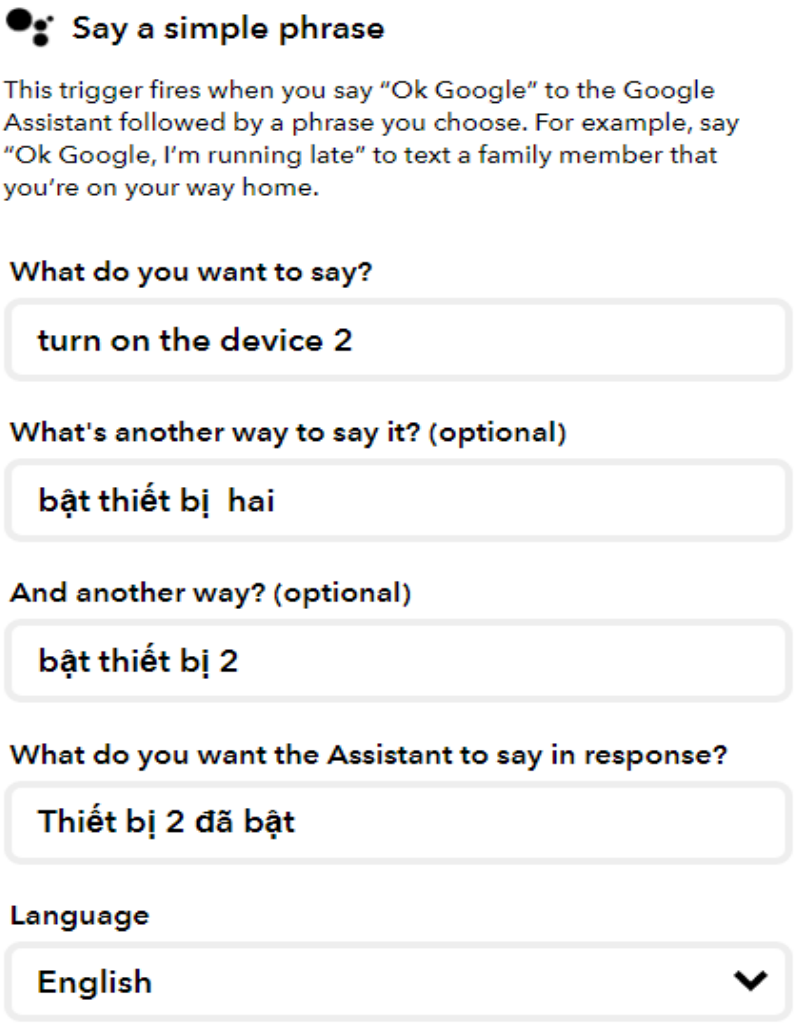
Step 1 of 6

google Assistant



Chọn "*Say a simple phrase*"

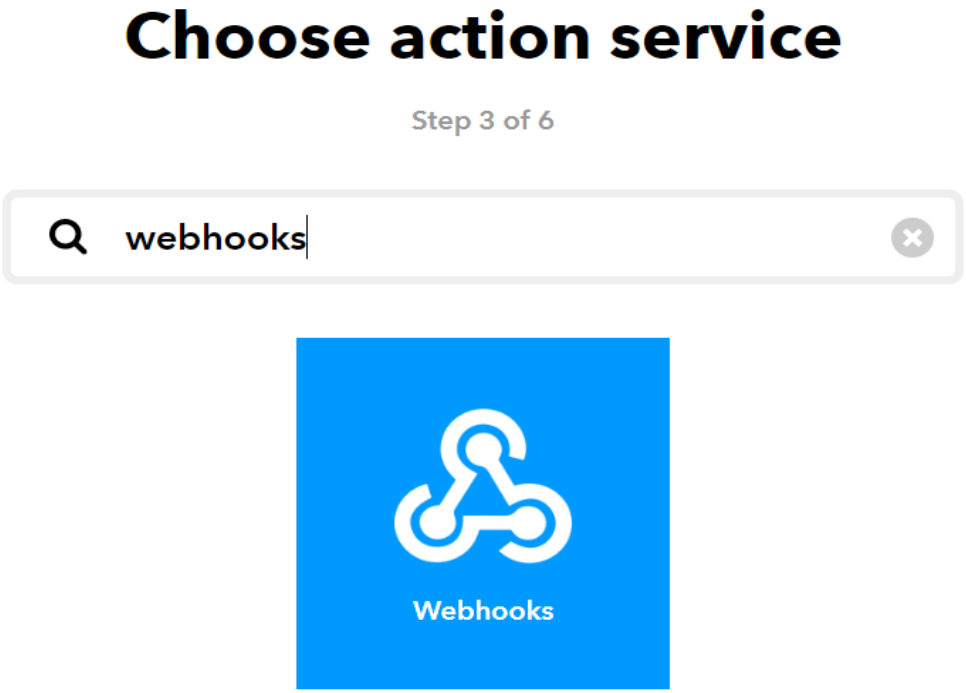




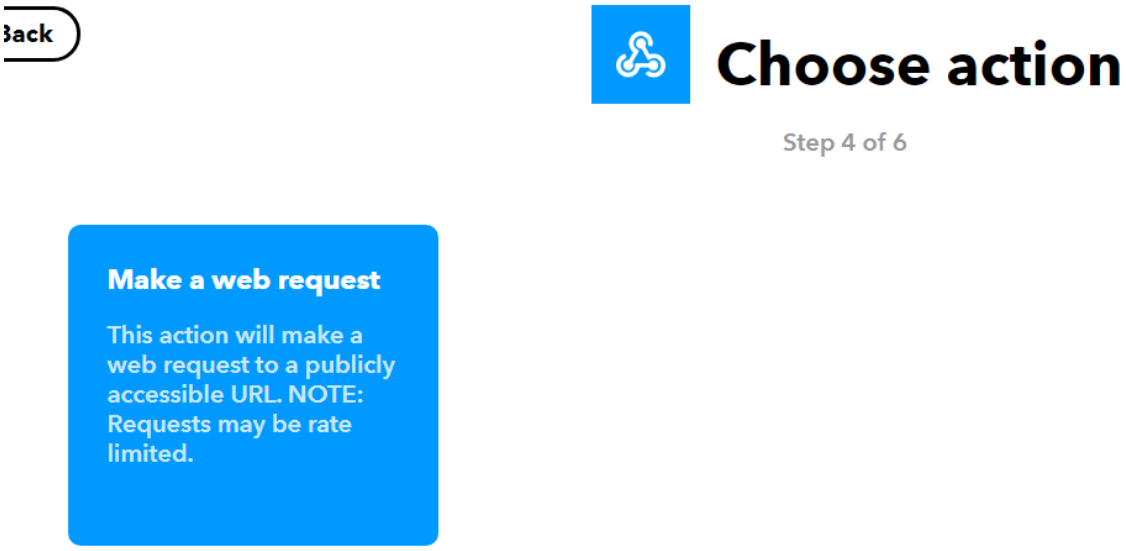
Điền câu lệnh muốn nói như thế nào thì tùy, ví dụ "turn on the light". Điền xong thì *Create Trigger*.

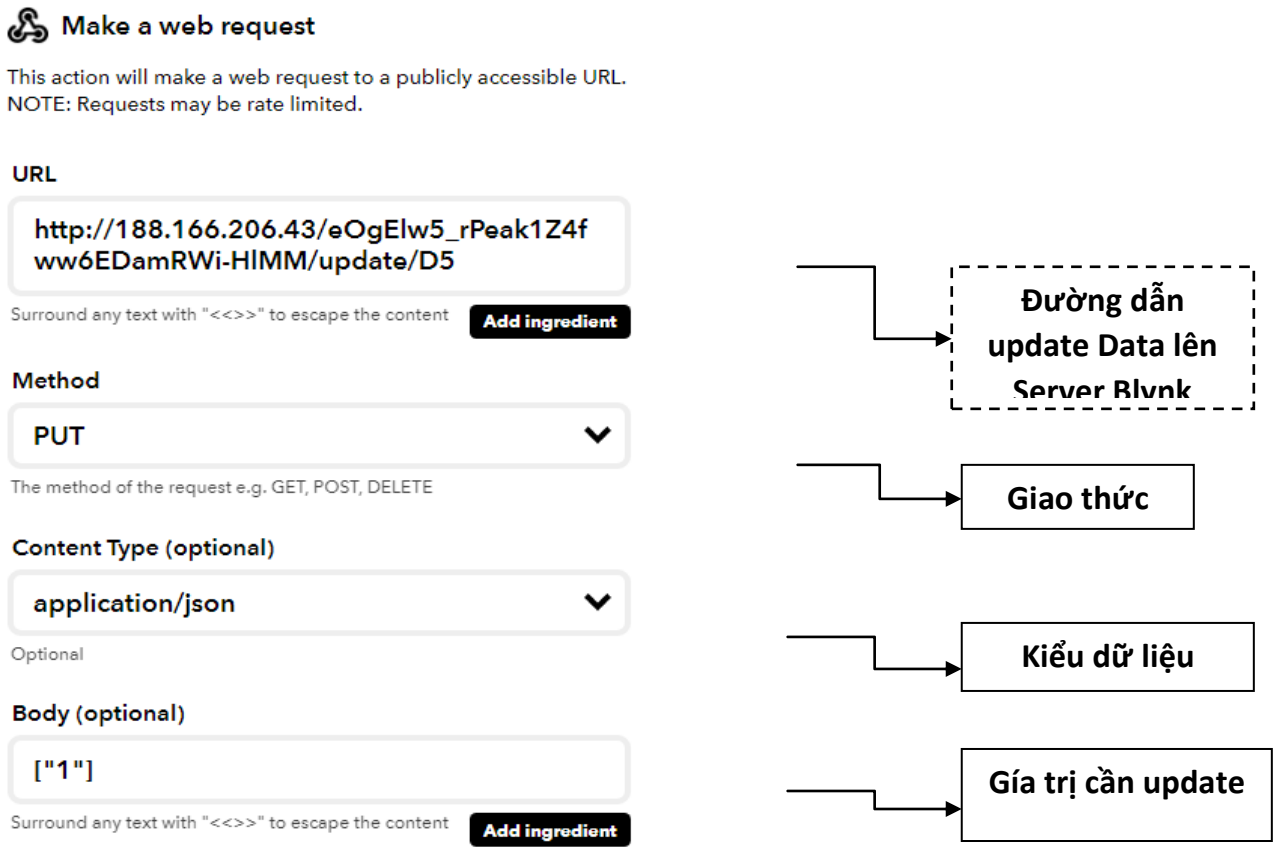


Với mục **THAT** thì chọn "**Webhook**".

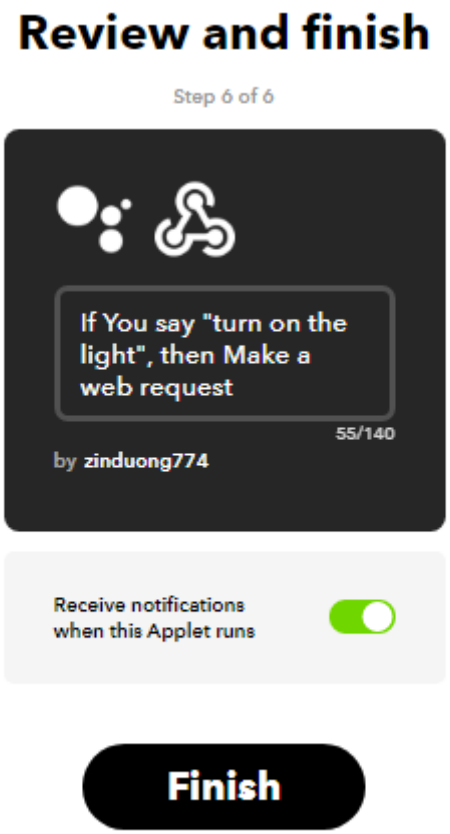


Chọn "*Make a web request*"

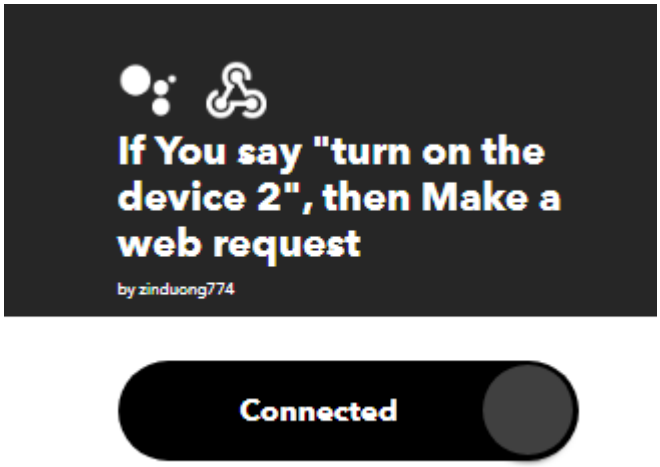


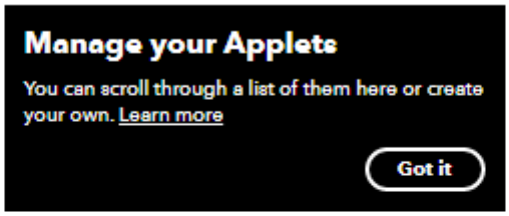


Nhấn Create action

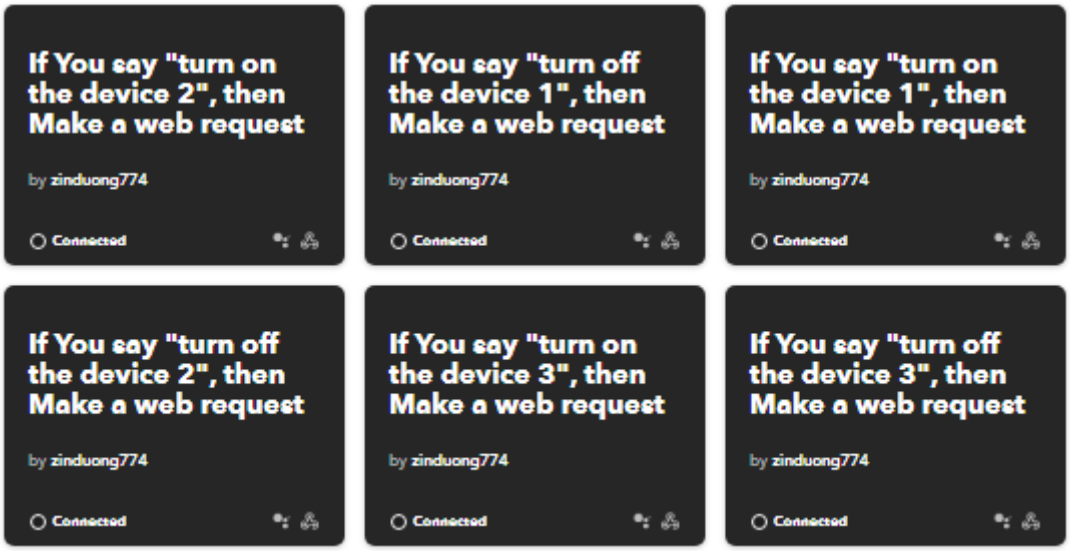


Nhấn Finish ta tạo được applet như sau



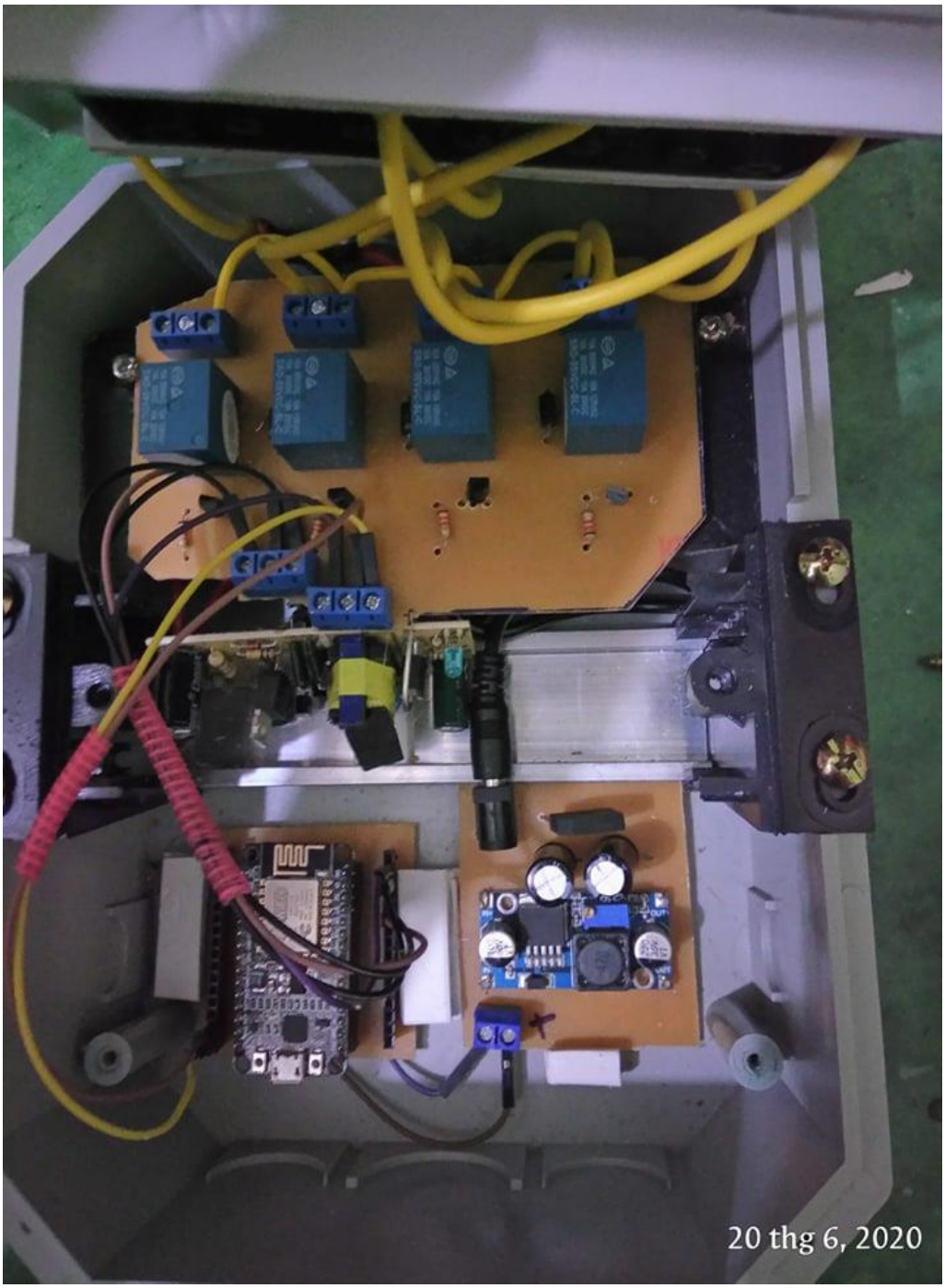

Manage your Applets
You can scroll through a list of them here or create your own. Learn more
Got it

My Applets


If You say "turn on the device 2", then Make a web request
by zinduong774
Connected
If You say "turn off the device 1", then Make a web request
by zinduong774
Connected
If You say "turn on the device 1", then Make a web request
by zinduong774
Connected
If You say "turn off the device 2", then Make a web request
by zinduong774
Connected
If You say "turn on the device 3", then Make a web request
by zinduong774
Connected
If You say "turn off the device 3", then Make a web request
by zinduong774
Connected

Chương 4. KẾT QUẢ ĐẠT ĐƯỢC

4.3. Mạch đồng sau khi hoàn tất



KẾT LUẬN

Đề tài *"Ổ cắm điện thông minh điều khiển qua mạng internet"* của chúng em còn rất nhiều thiếu sót và khiếm khuyết, mặc dù đã rất cố gắng tìm hiểu và tìm tòi, cũng như được sự chỉ bảo của GVHD thầy Võ Minh Phụng, nhưng do kinh nghiệm và kiến thức còn hạn chế nên hệ thống cũng chưa thực sự hoàn hảo. Em mong nhận được nhiều ý kiến đóng góp của quý thầy, cô cũng như các bạn để hệ thống ngày càng hoàn thiện hơn, giúp các chúng em ngày càng hiểu rõ hơn về hệ thống điều khiển tự động từ xa và nắm bắt được xu thế chung của xã hội về mô hình ngôi nhà thông minh nói riêng cũng như hệ thống điều khiển thông minh nói chung. Góp phần giúp đất nước tiến vào cuộc cách mạng công nghiệp 4.0 đang rất phổ biến ở các nước trên thế giới.

● **Kết quả thựchiện**:

Sau thời gian nghiên cứu và thực hiện đề tài này cùng với sự hướng dẫn tận tình của thầy Võ Minh Phụng chúng em đã hoàn thành đúng, đủ theo mục tiêu đề tài đã đề ra. Kết quả đạt được như sau:

- Củng cố các kiến thức đã thu nhận được trong suốt quá trình học tập
- Thiết kế xây dựng mạch và viết chương trình điềukhiển.
- Hoàn thiện báo cáo lý thuyết về đề tài.
- Xây dựng được mô hình điều khiển thiết bị bằng điện thoại di động.

● **Ưu điểm và hạn chế:**

➢ Ưu điểm

Sau quá trình làm đề tài và sản phẩm mạch thực tế, em nhận thấy đề tài của mình có một số ưu điểm như sau:

- Sử dụng điện thoại di động có chức năng wifi mang tính hiện đại và tiện nghi.
- Phần cứng được thiết kế đơn giản, sử dụng số linh kiên tối thiểu, kết nối chân ra đáp ứng nhu cầu phát triển đề tài sau này.

➢ Nhượcđiểm

Sau quá trình làm đồ án và sản phẩm mạch thực tế, em nhận thấy đề tài của mình có một số nhược điểm, hạn chế như sau:

- Hệ thống không hoạt động được ở vùng không có wifi (ví dụ như khi mất điện).

● **Hướng pháttriển:**

Đề tài *"Ổ cắm điện thông minh điều khiển qua mạng internet"* đã được chúng em xây dựng tương đối hoàn chỉnh, song chúng em tự nhận thấy rằng đề tài của mình còn nhiều thiếu sót vì vậy để đề tài này thêm phần phong phú, mang tính áp dụng trong thực tế hơn, có khả năng làm việc cao hơn thì đề tài của em cần phải có thêm các tính năng thiết thực như sau:

- Có thêm nhiều ổ cắm đa năng hơn.
-Có thêm công tắc cho thuận tiện khi ở gần thiết bị.
- Lắp đặt thêm bàn phím, màn hình LCD để hiển thị nội dung thông báo trên ổ cắm.
- Thay đổi được tên và mật khẩu wifi mà không cần nạp lại code.
- Giảm kích thước và thiết kế mẫu mã đẹp hơn.

● **Giá thành của sản phẩm: 5 triệu đồng**

TÀI LIỆU THAM KHẢO

[1] Felix Wortmann & Kristina Flüchter, "Internet of Things", *College of Information and Communication Engineering*, 2017.

[2] Zhenxing Wang, "The SmartHome Controller Based on Zigbee", *International Conference on Mechanical and Electronics Engineering (ICMEE)*, 2010.

[3] Mr.Rohit Kadam, Mr.Pranav Mahamuni, Mr.Yash Parikh, "Smart Home System", *International Journal of Innovative Research in Advanced Engineering (IJIRAE*), 2015.

[4] T.D.P. Mendes, G.J. Osorio, E.M.G. Rodrigues, J.P.S. Catalao, "Energy Management in SmartHomes using an Experimental Setup with Wireless Technologies", *International Conference on Engineering (ICE)*, 2013.

[5] Andrej Souvent, "Concept of SmartHome and SmartGrids integration", *International Conference on Engineering (ICE)*, 2013.

[6]Ths.LêHoàngAnh,*Giáotrìnhthiếtkếmạchin*,NXBTrườngđạihọc*Lạc Hồng*, 2014.

[7]Kiều Xuân Thực, Vũ Thị Thu Hương, Vũ Trung Kiên, *Vi điều khiển cấu trúc –lập trình và ứng dụng*, NXB Giáo dục,2008.

PHỤ LỤC

Code toàn mạch:

```
1.#define BLYNK_PRINT Serial
2.#include <ESP8266WiFi.h>
3.#include <BlynkSimpleEsp8266.h>

4.char auth[] = "eOgElw5_rPeak1Z4fww6EDamRWi-HlMM";
5.char ssid[] = "DuongVT";
6.char pass[] = "camonbandatruycap";

7.WidgetLED led1(V0);
8.WidgetLED led2(V1);
9. WidgetLED led3(V2);
10. WidgetLED led4(V3);
11. BlynkTimer timer;

12. void blinkLedWidget()
13. {if (led1.getValue()) {
14.   led1.off();
15.  Serial.println("LED on V0: off");
16. } else {
17.   led1.on();
18. Serial.println("LED on V0: on");
19.   }
20. }

21. BLYNK_WRITE(V1)
22. {
```

```
23.   int pinValue = param.asInt();
24.   Serial.println(pinValue);
25.   digitalWrite(D1, pinValue);
26.   if (digitalRead(D1)) {
27.    led2.off();
28.  } else {
29.     led2.on();
30.  }
31. }
32. BLYNK_WRITE(V2)
33. {
34.  int pinValue = param.asInt();
35.   Serial.println(pinValue);
36.  digitalWrite(D2, pinValue);
37.  if (digitalRead(D2)) {
38.    led3.off();
39.   } else {
40.     led3.on();
41.   }
42. }
43. BLYNK_WRITE(V3)
44. {
45.   int pinValue = param.asInt();
46.   Serial.println(pinValue);
47.   digitalWrite(D5, pinValue);
48.  if (digitalRead(D5)) {
49.     led4.off();
50.   } else {
51.     led4.on();
52.   }
```

```
53. }
54. void setup()
55. {  Serial.begin(9600);
56. Blynk.begin(auth, ssid, pass);
57.   timer.setInterval(1000L, blinkLedWidget);
58.   pinMode(D1, OUTPUT);
59.  digitalWrite(D1, HIGH);
60. pinMode(D2, OUTPUT);
61.   digitalWrite(D2, HIGH);
62.   pinMode(D5, OUTPUT);
63.   digitalWrite(D5, HIGH);
64. }
65. void loop()
66. {
67.   Blynk.run();
68.   timer.run();
69. }
```