**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**------------------------------**



**TÓM TẮT ĐỒ ÁN**

**TỐT NGHIỆP ĐẠI HỌC**

***Đề tài :* “XÂY DỰNG HỆ THỐNG DNS DỰA TRÊN CÔNG NGHỆ BLOCKCHAIN”**

**Giáo viên hướng dẫn : HUỲNH THANH TÂM**

**Sinh viên thực hiện : PHAN ĐẠI**

**Mã số sinh viên : N17DCAT013**

**Lớp : D17CQAT01-N**

**Khóa : 2017**

**Hệ : ĐẠI HỌC CHÍNH QUY**

**TP. HỒ CHÍ MINH, năm 2021**

# MỤC LỤC

[MỤC LỤC 2](#_Toc91451766)

[MỤC TIÊU 3](#_Toc91451767)

[LÝ THUYẾT 3](#_Toc91451768)

[THỰC HÀNH 3](#_Toc91451769)

[DNS - DOMAIN NAME SYSTEM 4](#_Toc91451770)

[DNS TRUYỀN THỐNG HOẠT ĐỘNG NHƯ THẾ NÀO ? 4](#_Toc91451771)

[BLOCKCHAIN 5](#_Toc91451772)

[CÔNG NGHỆ BLOCKCHAIN 5](#_Toc91451773)

[SO SÁNH 2 MÔ HÌNH 6](#_Toc91451774)

[THUẬT TOÁN ĐỒNG THUẬN 7](#_Toc91451775)

[PROOF OF WORK 7](#_Toc91451776)

[PROOF OF STAKE 7](#_Toc91451777)

[PHẦN MỀM DNS BLOCKCHAIN HIỆN CÓ 8](#_Toc91451778)

[DANH SÁCH XẾP HẠNG 13 PHẦN MỀM DNS BLOCKCHAIN 8](#_Toc91451779)

[CƠ CHẾ CỦA DNS BLOCKCHAIN 9](#_Toc91451780)

[DNS BLOCKCHAIN HOÀN CHỈNH GỒM 9](#_Toc91451781)

[XÂY DỰNG DNS BLOCKCHAIN 10](#_Toc91451782)

[MÔ HÌNH HOẠT ĐỘNG CỦA HỆ THỐNG DNS BLOCKCHAIN 10](#_Toc91451783)

[XÂY DỰNG ĐỊNH DẠNG LƯU TRỮ CHUNG TRONG HỆ THỐNG 11](#_Toc91451784)

[XÂY DỰNG HỆ THỐNG BLOCKCHAIN VÀ GIAO DIỆN NGƯỜI DÙNG VỚI PYTHON FLASK 11](#_Toc91451785)

[XÂY DỰNG HỆ THỐNG DNS RESOLVER VỚI PYTHON SOCKET 12](#_Toc91451786)

[THỰC NGHIỆM 13](#_Toc91451787)

[KỊCH BẢN 1 13](#_Toc91451788)

[KỊCH BẢN 2 13](#_Toc91451789)

[Kịch bản 3 14](#_Toc91451790)

[KẾT LUẬN 15](#_Toc91451791)

[TÓM TẮT NHỮNG ĐIỀU MÀ ĐỀ TÀI ĐÃ ĐẠT ĐƯỢC 15](#_Toc91451792)

[GIẢI PHÁP, ĐỀ XUẤT 16](#_Toc91451793)

[HẠN CHẾ CỦA ĐỀ TÀI 16](#_Toc91451794)

# MỤC TIÊU

## LÝ THUYẾT

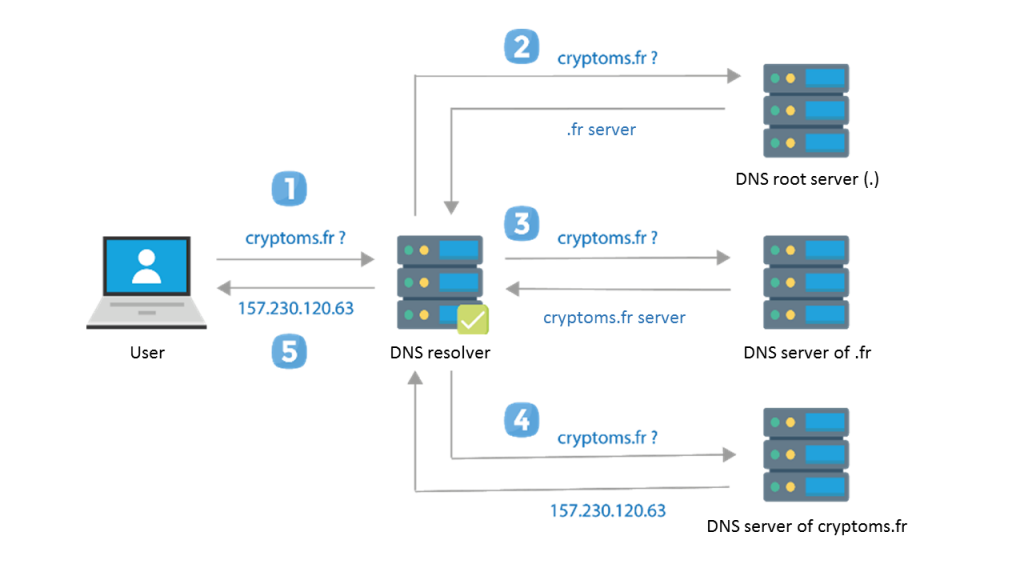
* Tìm hiểu cơ chế hoạt động của DNS truyền thống.
* Tìm hiểu các ưu và nhược điểm của DNS truyền thống.
* Tìm hiểu tổng quan về công nghệ Blockchain và giao thức đồng thuận PoW, PoS.
* Một số phần mềm DNS dựa trên blockchain hiện có.
* Xây dựng cơ chế hoạt động của DNS dựa trên blockchain.

## THỰC HÀNH

* Xây dựng một hệ và triển khai DNS trên một private blockchain với giao thức đồng thuận PoW.
* Xây dựng các kịch bản thử nghiệm cho giải pháp.

# DNS - DOMAIN NAME SYSTEM

## DNS TRUYỀN THỐNG HOẠT ĐỘNG NHƯ THẾ NÀO ?



Hình 1. Mô hình hoạt động cơ bản của DNS

\* DNS resolver – DR – Máy chủ phân giải tên miền cục bộ

Máy tính tìm kiếm tên miền *cryptoms.fr* theo các bước sau:

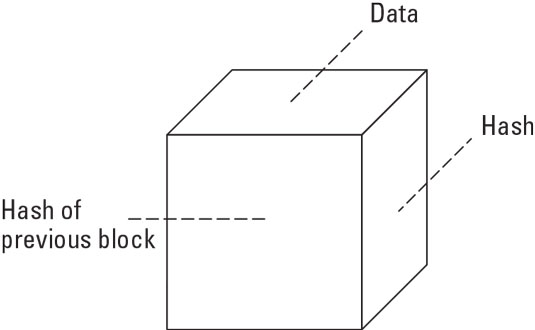
1. Máy tính trước khi gửi đi,DNS resolver sẽ kiểm tra domain trong Web cache hoặc DNS cache để trả lại kết quả.
2. Nếu không có kết quả, DR sẽ hỏi tên miền mức ROOT chỉ cho máy chủ tên miền cục bộ địa chỉ mà nó quản lý có đuôi “.fr”.
3. DR gửi yêu cầu đến máy chủ quản lý tên miền Pháp “.fr” tìm tên miền cryptoms.fr.
4. DR sẽ hỏi máy chủ quản lý tên miền “.fr” địa chỉ IP của tên miền “cryptoms.fr” và gửi trả lại cho DR, sau đó chuyển đến máy của người dùng.

**Người dùng sử dụng địa chỉ IP này kết nối đến server chứa website có địa chỉ “cryptoms.fr”.**

# BLOCKCHAIN

## CÔNG NGHỆ BLOCKCHAIN

Blockchain sẽ bao gồm nhiều block như hình bên phải, các block liên kết với nhau qua “Hash khối trước”.



**Mật mã học**

**Bất biến:** dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.

Hình 2. Cấu trúc của Block

Khi khởi tạo Blockchain sẽ cần 1 block gọi là genesis block có hash khối hiện tại và khối trước là 0 và dữ liệu là null.

Genesis

block

Hash: 0

Block 1

Previous Hash: 0

Hash: 000xxxxx

Hình 3. Block khởi tạo

Blockchain được tạo ra nhờ 3 loại công nghệ và từng loại công nghệ giúp Blockchain mang đặc điểm sau.

**Mạng ngang hàng**

**Mật mã học**

**Lý thuyết trò chơi**

**Bất biến:** dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.

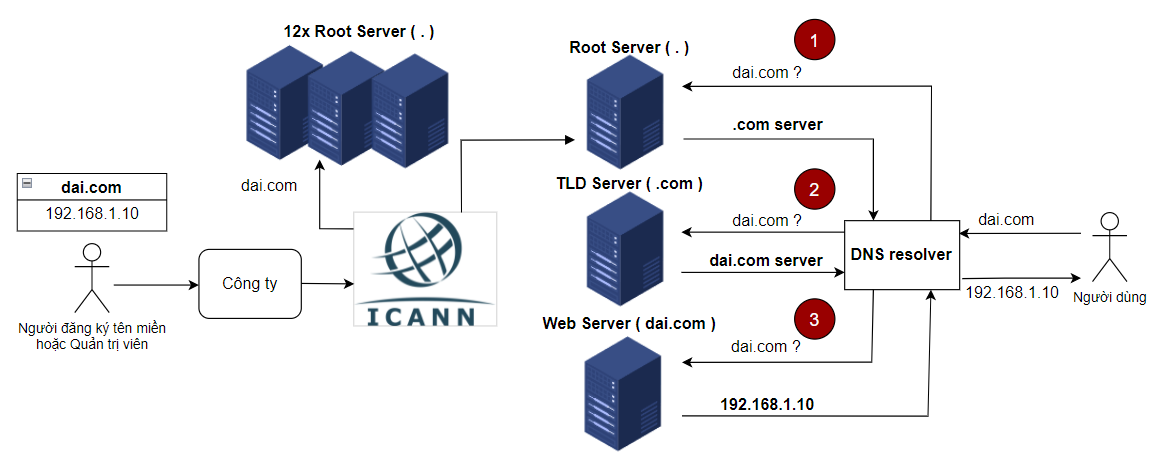
**Minh bạch:** Ai cũng có thể theo dõi dữ liệu Blockchain đi từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

**Hợp đồng thông minh:** là hợp đồng kỹ thuật số được nhúng vào đoạn code if-this-then-that (IFTTT), cho phép chúng tự thực thi mà không cần bên thứ ba.

Hình 4. Công nghệ tạo nên Blockchain

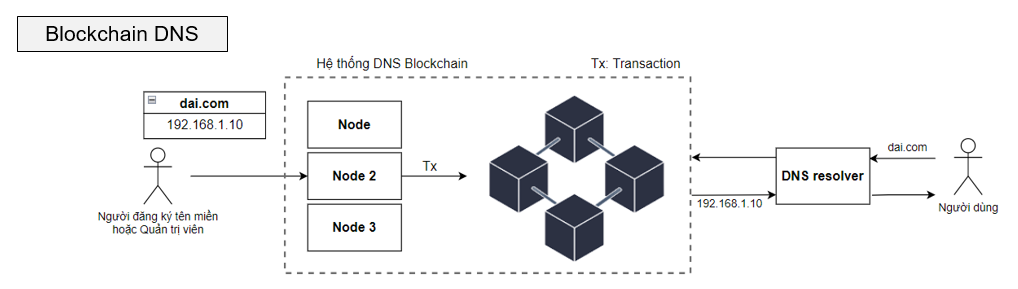
# SO SÁNH 2 MÔ HÌNH

Blockchain DNS

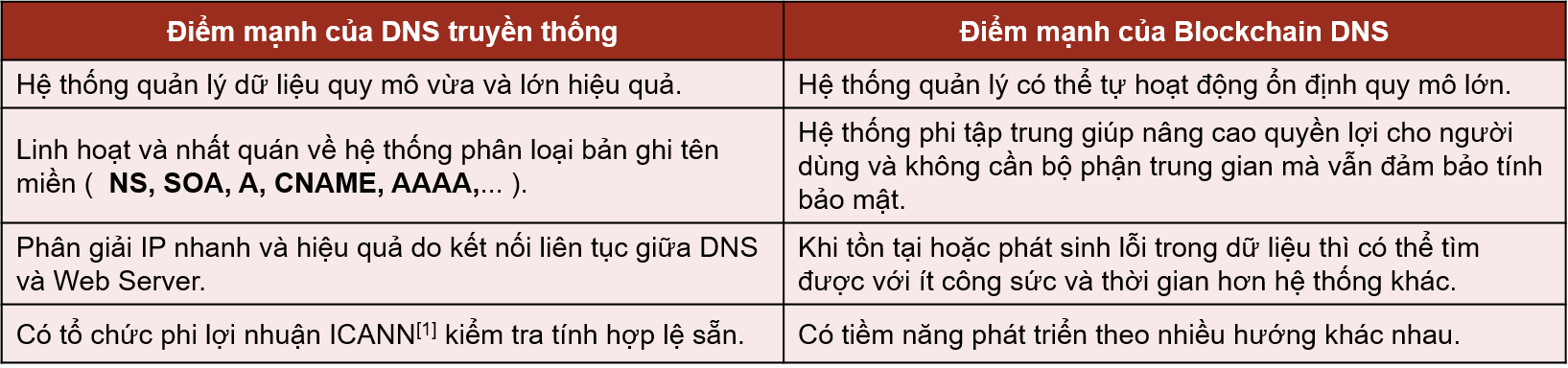


DNS truyền thống

Hình 5. Mô hình DNS truyền thống



Hình 6. Mô hình Blockchain DNS



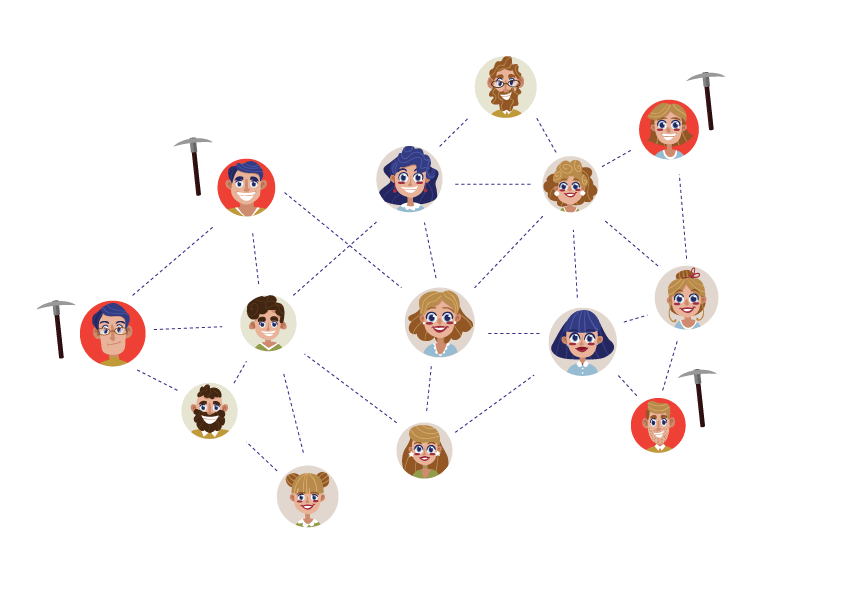
Bảng 1. Điểm mạnh của 2 hệ thống



Bảng 2. Điểm yếu của 2 hệ thống

# THUẬT TOÁN ĐỒNG THUẬN

## PROOF OF WORK

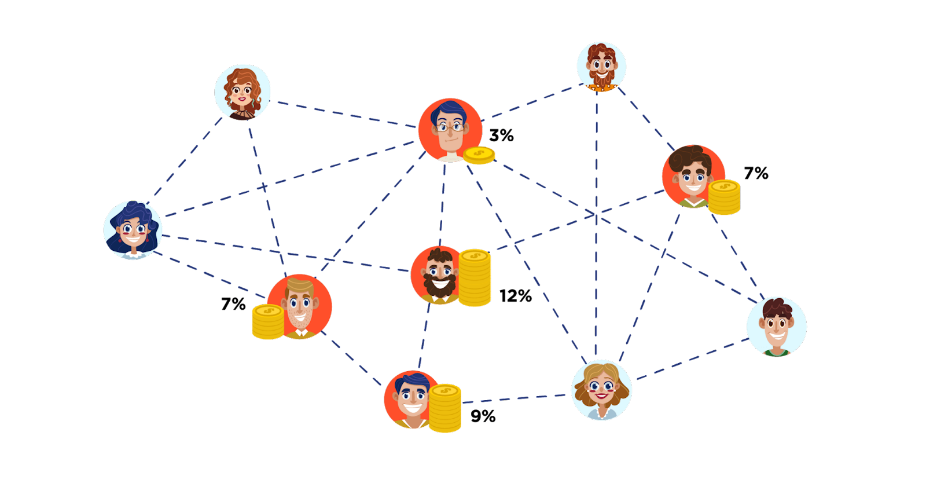


Mỗi node đóng vai trò như là Miner ( thợ mỏ ) cạnh tranh với nhau làm công việc tìm ra số Nonce đầu tiên ( số sử dụng 1 lần ), sao cho sau khi có số nonce, hash của khối sẽ bắt đầu với 0 x độ khó.

Khuyết điểm:

* Dễ bị tấn công 51%;
* Hao tổn nhiều điện năng tiêu thụ

## PROOF OF STAKE



Mỗi node sẽ đặt cọc một khoản tiền ảo nhất định vào lần giao dịch đó, hệ thống sẽ sử dụng thuật toán để đánh giá theo tiêu chí và lựa chọn để đảm bảo rằng người thợ đào phù hợp với lợi ích lâu dài của cả mạng lưới.

Khuyết điểm:

* Khi gặp sự cố không mong muốn, sẽ mất phần đặt cọc ( Vd: mất wifi, cúp điện, ... );

# PHẦN MỀM DNS BLOCKCHAIN HIỆN CÓ

## DANH SÁCH XẾP HẠNG 13 PHẦN MỀM DNS BLOCKCHAIN

Dựa vào bảng xếp hạng trên trang Software Testing Help theo đường link

*https://www.softwaretestinghelp.com/best-blockchain-dns-software/*

1. Namecoin
2. Blockstack
3. Ethereum Name Service ( ENS )
4. Handshake
5. Nebulis
6. Dot BIT
7. Emercoin DNS
8. PeerName
9. Blockchain DNS for Firefox
10. FrigGate for Chrome and other browsers
11. NEM Blockchain DNS extension
12. Unstoppable Domains
13. Aloaha Blockchain DNS

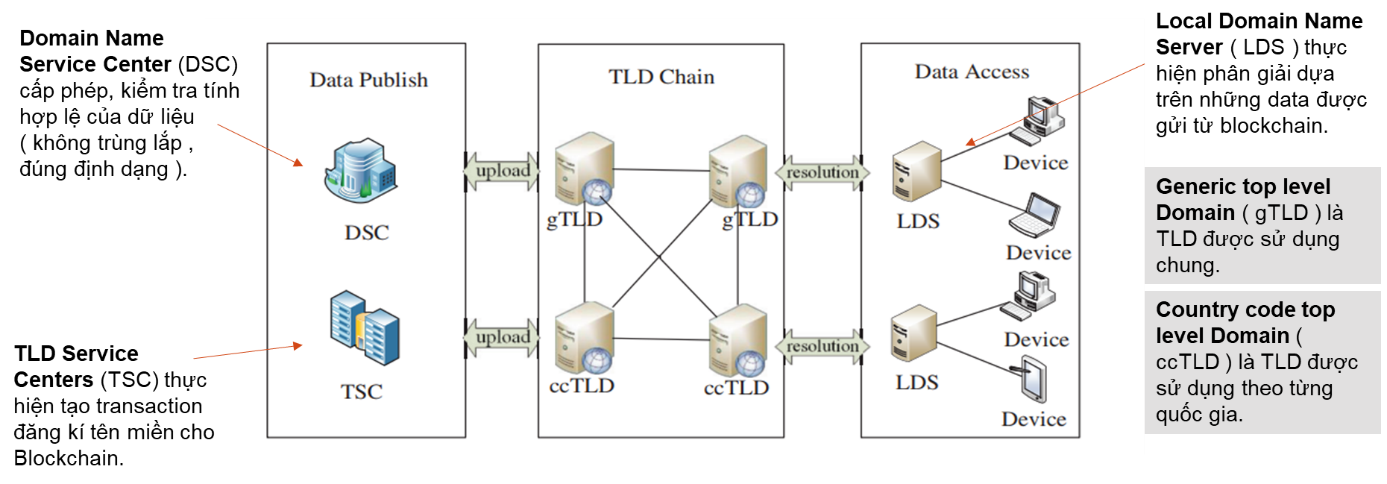
# CƠ CHẾ CỦA DNS BLOCKCHAIN

## DNS BLOCKCHAIN HOÀN CHỈNH GỒM

**Data Publish:** Chịu trách nhiệm cho việc upload dữ liệu tên miền và thực thi những yêu cầu với dữ liệu upload.

**TLD Chain:** Blockchain lưu trữ những dữ liệu tên miền đã được đồng bộ hóa.

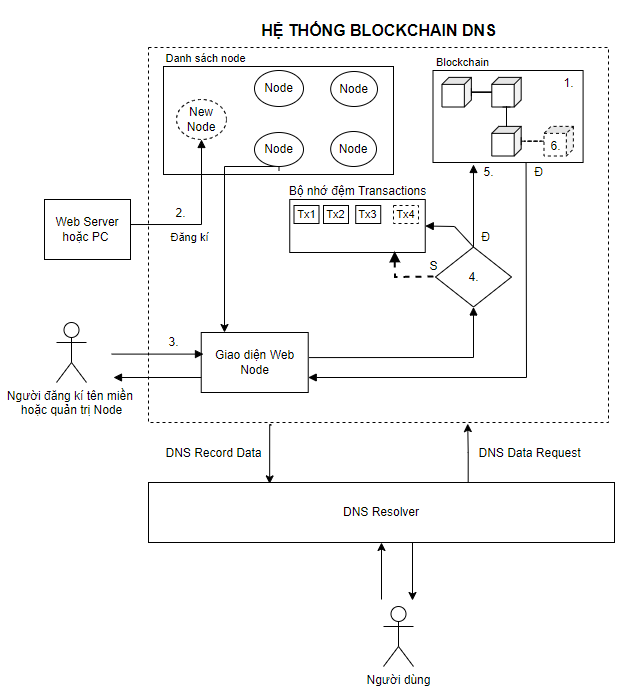
**Data Access:** Chịu trách nhiệm nhận yêu cầu và trả kết quả phân giải cho người yêu cầu.



Hình 7. Mô hình Blockchain DNS hoàn chỉnh

# XÂY DỰNG DNS BLOCKCHAIN

## MÔ HÌNH HOẠT ĐỘNG CỦA HỆ THỐNG DNS BLOCKCHAIN



Hình 8. Mô hình Blockchain DNS đầy đủ của đề tài

Chú thích

1. Khởi tạo Blockchain bằng cách, mở Node ( máy chủ ) thuộc danh sách Node, đồng thời khởi tạo Blockchain cho hệ thống.

Blockchain khi khởi tạo sẽ kiểm tra tính hợp lệ của từng block bằng cách kiểm tra previous\_hash của khối hiện tại và hash của khối trước.

2. Web Server hoặc PC có thể đăng kí trở thành Node mới của hệ thống Blockchain.

3. Hệ quản trị ( Admin ) hay người đăng kí tên miền ( Hoster ) có thể dùng giao diện chạy bởi Node để đăng kí tên miền.

4. Hệ thống kiểm tra điều kiện tạo Block – số transaction ( giao dịch ) hiện tại phải lớn hơn hoặc bằng số transaction được quy định trong block như sau:

* Đúng ( Đ ) : Hệ thống tạo block
* Sai ( S ) : Chỉ thêm vào bộ nhớ đệm Transaction.

5. Khi tạo block, hệ thống phát động thuật toán Proof of Work cho các nodes và cho phép Node mà tìm ra số Nonce nhanh nhất được gắn Block vào chain.

6. Block sẽ mới sẽ được cập nhật vào Blockchain của từng Node trong danh sách. Xong sẽ gửi thông báo cho người dùng.

## XÂY DỰNG ĐỊNH DẠNG LƯU TRỮ CHUNG TRONG HỆ THỐNG

* Định dạng cho DNS record;
* Định dạng cho Transaction;
* Định dạng cho Block;
* Định dạng cho Node;
* Định dạng cho Account;

|  |  |
| --- | --- |
| $origin: ‘spec.com’ | Tên miền gốc |
| $ttl: 3600 | Quy định Thời gian tên miền tồn tại |
| Soa | Quy định thông tin xác nhận từ phía máy chủ tiếp nhận |
| Ns | Quy định các loại tên miền phụ |
| A | Bản ghi được sử dụng trỏ tên website tới một địa chỉ IP cụ thể |

## XÂY DỰNG HỆ THỐNG BLOCKCHAIN VÀ GIAO DIỆN NGƯỜI DÙNG VỚI PYTHON FLASK

* Xây dựng quy trình xử lý thông tin đăng kí node và account admin tham gia vào hệ thống Blockchain.
* Xây dựng quy trình thêm thông tin tên miền và tạo giao dịch trên hệ thống.
* Xây dựng giao thức đồng thuận và quy trình xử lý tạo block khi đạt đủ điều kiện giao dịch.
* Xây dựng xử lý phân quyền giữa các loại người dùng khác nhau ( Hoster, Admin, Client )

## XÂY DỰNG HỆ THỐNG DNS RESOLVER VỚI PYTHON SOCKET

* Xây dựng quy trình lấy tên miền từ hệ thống blockchain.
* Xây dựng quy trình phân giải tên miền cho hệ thống DNS.

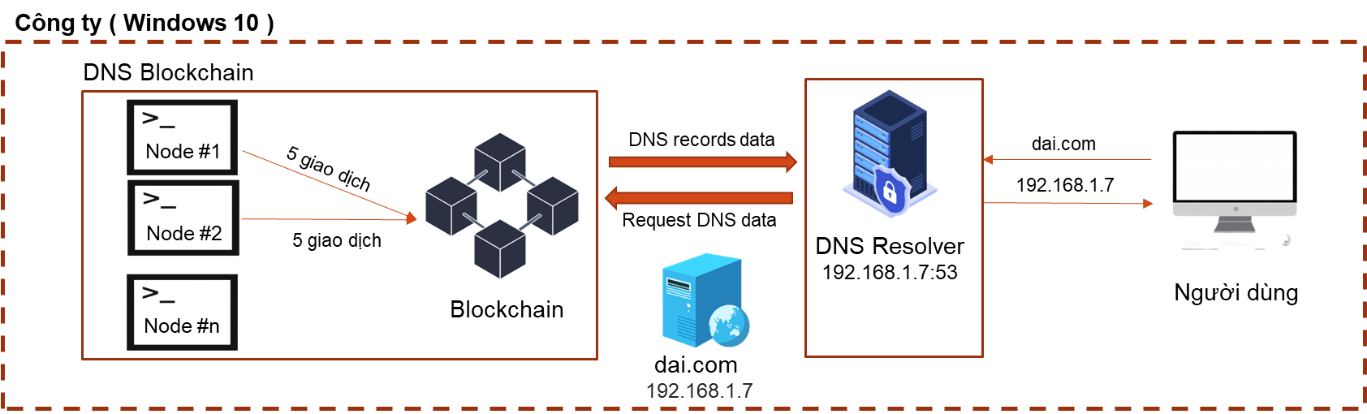
# THỰC NGHIỆM

## KỊCH BẢN 1

Công ty muốn kiểm tra DNS Server hoạt động cục bộ

- Chạy DNS server, mở web server ở máy công ty , mở CMD node có port là 5000, đăng nhập với vai trò là admin, thực hiện thêm 5 giao dịch tên miền, sau đó tiến hành phân giải trên máy công ty . ( 5 giao dịch trong đó có chứa 1 giao dịch dai.com )

- Mở CMD node với port bất kì, thực hiện thêm 5 giao dịch tên miền khác và phân giải tên miền thông qua máy công ty .

****

Hình 9. Kịch bản thử nghiệm thứ nhất

**Mục tiêu :** Người dùng truy cập thành công vào dai.com tại máy chủ mà vẫn vào được Internet.

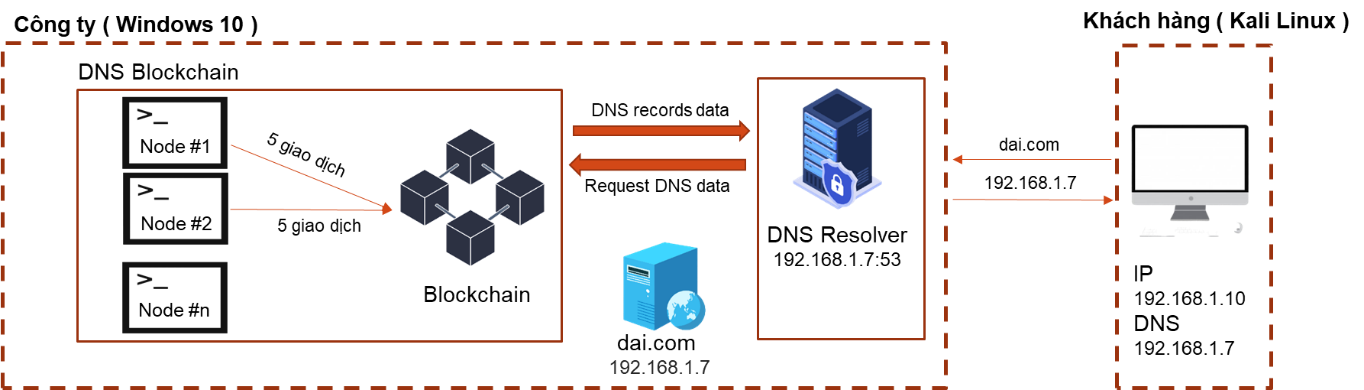
## KỊCH BẢN 2

Khách hàng muốn truy cập vào Web server của công ty

( giống với kịch bản 1 nhưng quá trình phân giải sẽ diễn ra ở máy ảo )

- Chạy DNS server, mở web server ở máy công ty, mở CMD node có port là 5000, đăng nhập với vai trò là admin, thực hiện thêm 5 giao dịch tên miền, sau đó tiến hành phân giải trên máy khách hàng. ( 5 giao dịch trong đó có chứa 1 giao dịch dai.com )

- Mở CMD node với port bất kì, thực hiện thêm 5 giao dịch tên miền khác và phân giải tên miền thông qua máy khách hàng.



Hình 10. Kịch bản thử nghiệm thứ hai

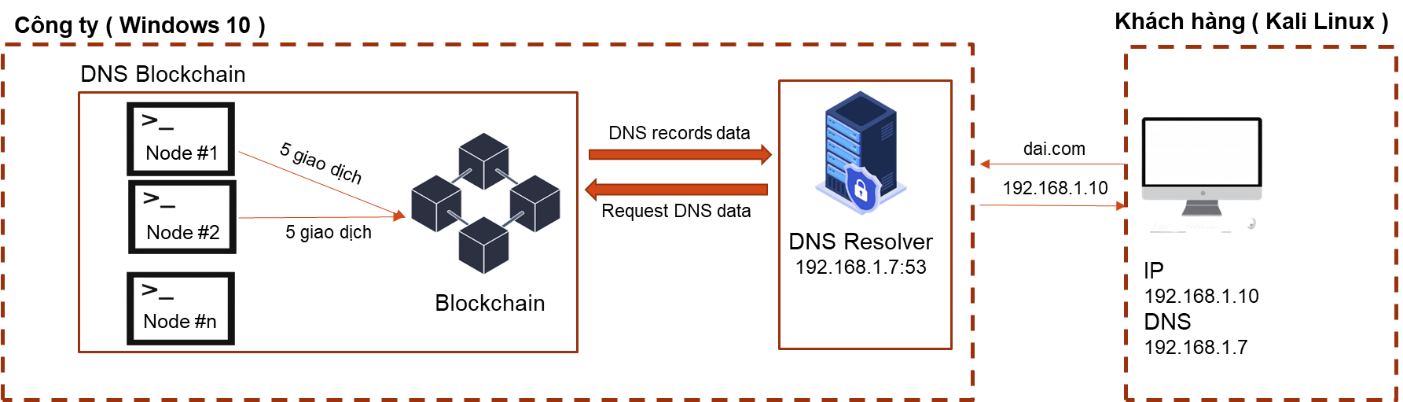
**Mục tiêu :** Khách hàng truy cập thành công vào dai.com từ máy khách hàng mà vẫn vào được Internet.

## Kịch bản 3

Khách hàng muốn truy cập vào Web server của khách hàng thông qua phân giải tên miền từ máy chủ

- Chạy DNS server, chạy web server trên máy khách hàng, mở CMD node có port là 5000, đăng nhập với vai trò là admin, thực hiện thêm 5 giao dịch tên miền, sau đó tiến hành phân giải trên máy khách hàng.

- Mở CMD node có port khác, đăng nhập với vai trò là admin, thực hiện thêm 5 giao dịch tên miền + 1 giao dịch dai.com và tiến hành phân giải trên máy khách hàng.



Hình 11. Kịch bản thử nghiệm thứ ba

**Mục tiêu :** Khách hàng truy cập thành công vào dai.com từ máy khách hàng mà vẫn vào được Internet.

# KẾT LUẬN

## TÓM TẮT NHỮNG ĐIỀU MÀ ĐỀ TÀI ĐÃ ĐẠT ĐƯỢC

* Nêu rõ khái niệm, điểm mạnh và yếu của DNS server và cách DNS server hiện tại hoạt động.
* Nêu rõ khái niệm, điểm mạnh và yếu của Blockchain và hiểu thêm về giải pháp DNS phát triển bằng công nghệ Blockchain.
* Xây dựng được và tái hiện hệ thống Blockchain DNS trên máy tính cá nhân.
* Phân giải tên miền và trả về kết quả thành công cho dù ở trên trình duyệt.
* Phần mềm tận dụng những DNS record lâu đời giúp việc kế thừa và chuyển hóa công nghệ dễ dàng.
* Áp dụng DNS Server cho máy tính cá nhân, không cần cài đặt DNS Server trên Windows Server.
* Phân giải tên miền cho các máy tính khác trong mạng có kết nối vào DNS Server mà vẫn giữ kết nối Internet.
* DNS Blockchain là một giải pháp khả thi hiện nay, vừa phần nào giải quyết được bài toán bảo mật, vừa mang lại cơ hội khai thác phát triển triệt để giá trị của tên miền.

# GIẢI PHÁP, ĐỀ XUẤT

## HẠN CHẾ CỦA ĐỀ TÀI

* Vì là máy tính cá nhân không thể làm việc ở thời gian liên tục và lâu dài cần phải bật tắt hàng ngày nên phải dùng đến PostgreSQL.
* Môi trường cần mạng wifi, không thể dùng hotspot trên điện thoại lâu dài để phát nên khó trong việc di chuyển đến những nơi xa hay thiếu wifi.
* Vì không phải là một Server tiêu chuẩn nên hiệu suất truyền dẫn có phần thấp hơn hệ thống DNS thông thường.
* Ở đề tài, mô hình này đã đạt được những điều cơ bản của hệ thống Blockchain thông thường nhưng thiếu một số bước kiểm soát tính chất hợp lệ của giao dịch.
* Chưa thể ngăn được các loại tấn công nghe lén hay truyền tin.

**CÁC HƯỚNG MỞ RỘNG**

* Phát triển thêm hệ thống Blockchain về mặt bảo mật giao dịch bằng chữ kí số hay các giải pháp bảo mật khác ở hiện tại.
* Đưa nhiều lựa chọn hơn trên giao diện giao tiếp người dùng, cho phép nhiều loại người dùng khác nhau trở thành Miner và trả công qua ví điện tử thật.
* Giao diện và ứng dụng được áp dụng ở nhiều môi trường khác nhau kể cả điện thoại.