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

MỤC TIÊU

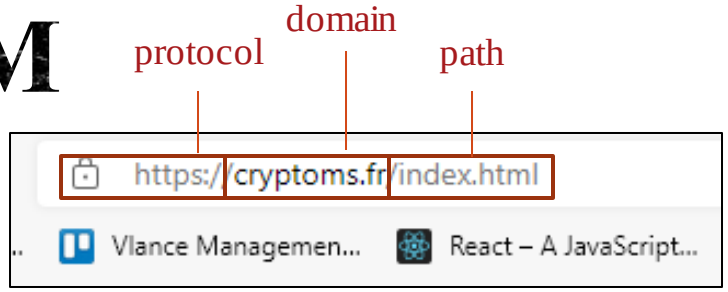
Lý thuyết

- Tìm hiểu cơ chế hoạt động của DNS truyền thống. 3
- Tìm hiểu các ưu và nhược điểm của DNS truyền thống. 5
- Tìm hiểu tổng quan về công nghệ Blockchain và giao thức đồng thuận PoW, PoS. 7
- Một số phần mềm DNS dựa trên blockchain hiện có. 8
- Xây dựng cơ chế hoạt động của DNS dựa trên blockchain. 9

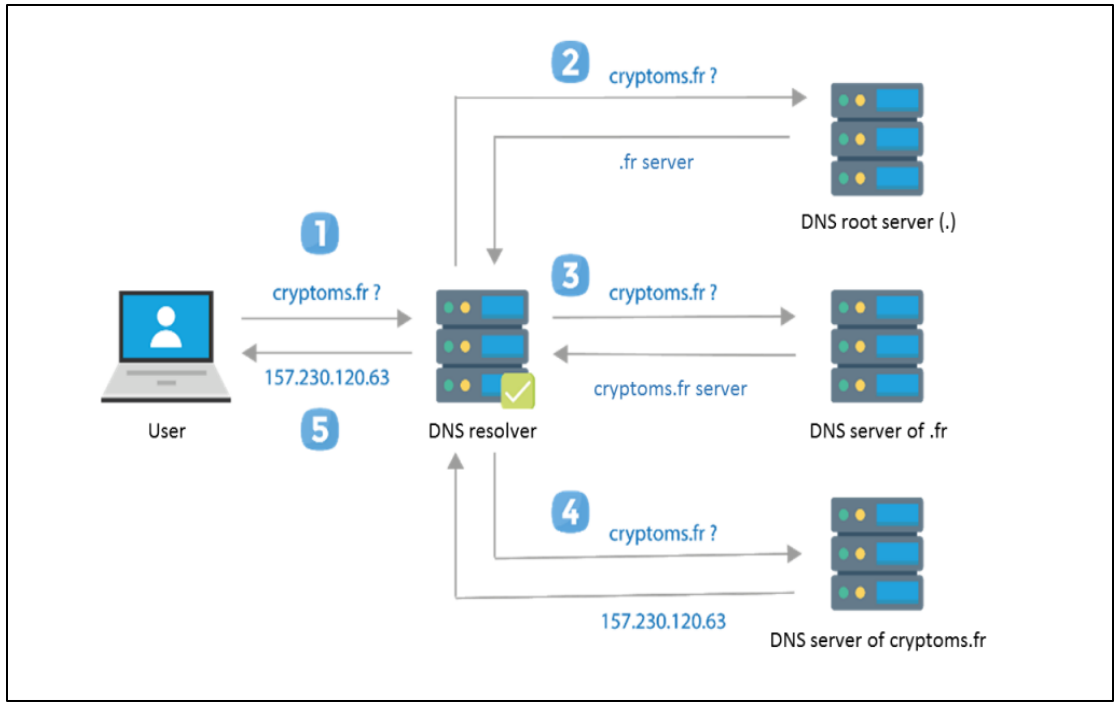
Thực hành

- Xây dựng một hệ và triển khai DNS trên một private blockchain với giao thức đồng thuận PoW. 10
- Xây dựng các kịch bản thử nghiệm cho giải pháp. 11

DNS - DOMAIN NAME SYSTEM



DNS truyền thống hoạt động như thế nào ?



Máy tính tìm kiếm tên miền *cryptoms.fr*

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".

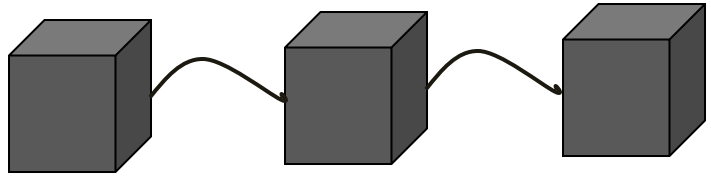
3) DR gửi yêu cầu đến máy chủ quản lý tên miền Pháp ".fr" tìm tên miền cryptoms.fr.

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".

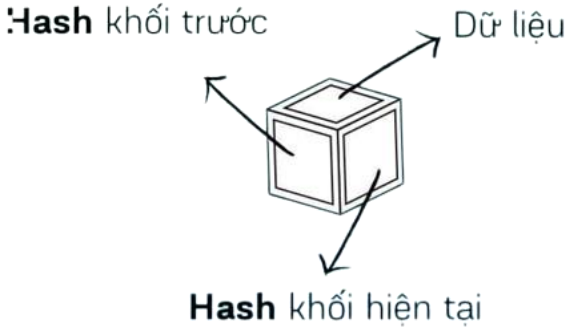
* DNS resolver – DR – Máy chủ phân giải tên miền cục bộ

BLOCKCHAIN

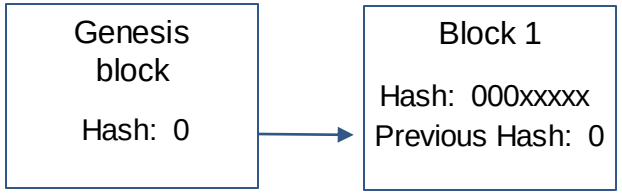


Công nghệ Blockchain

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



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



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

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.

Mạng ngang hàng

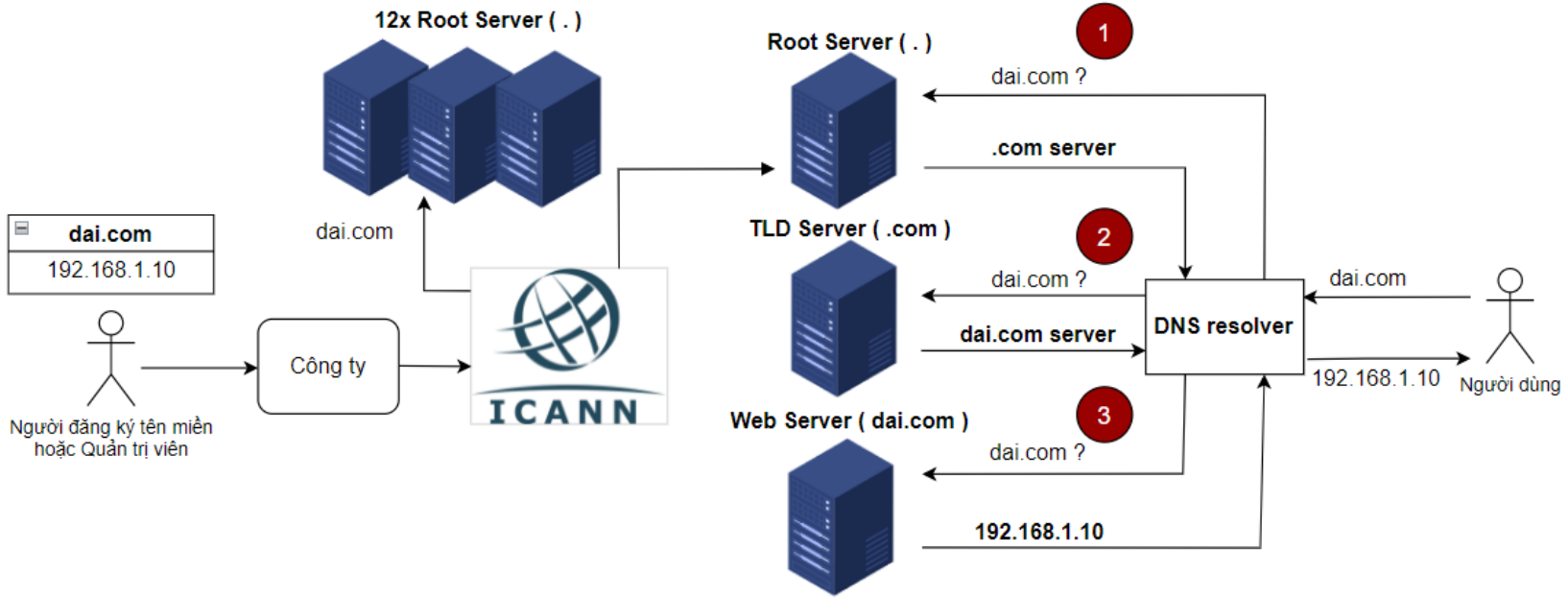
Minh bạch: Ai cũng có thể theo dõi dữ liệu Blockchain đi từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

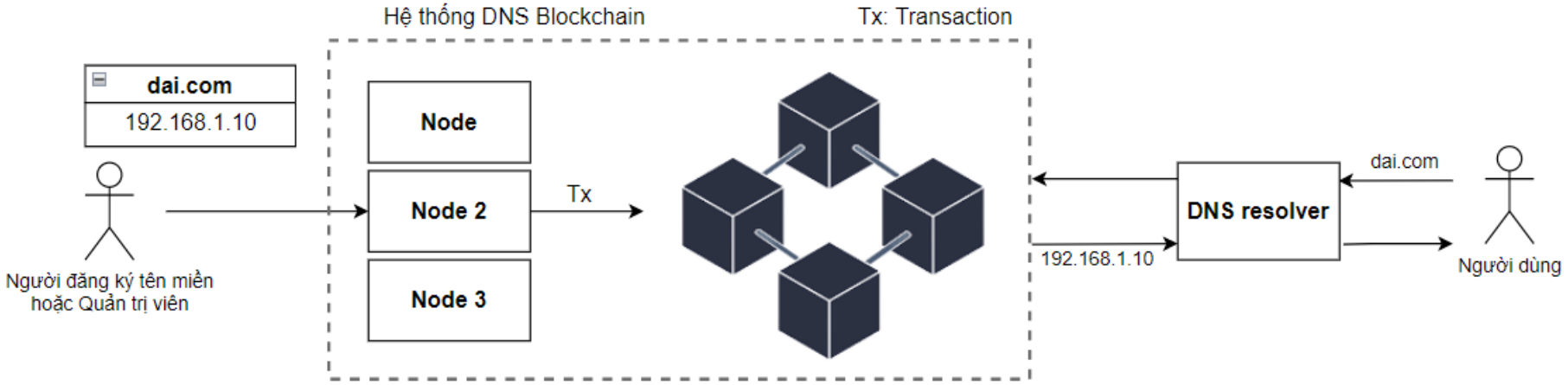
Lý thuyết trò chơi Pow, PoS

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.

→ **Bảo mật:** Các thông tin, dữ liệu trong Blockchain được phân tán và an toàn tuyệt đối.

SO SÁNH 2 MÔ HÌNH





TẠI SAO LÀ BLOCKCHAIN DNS ?

Điểm mạnh của DNS truyền thống
Hệ thống quản lý dữ liệu quy mô vừa và lớn hiệu quả.
Linh hoạt và nhất quán về hệ thống phân loại bản ghi tên miền (**NS, SOA, A, CNAME, AAAA,**...).
Phân giải IP nhanh và hiệu quả do kết nối liên tục giữa DNS và Web Server.
Có tổ chức phi lợi nhuận ICANN[1] kiểm tra tính hợp lệ sẵn.

Điểm yếu của DNS truyền thống
DNS là mục tiêu mà các hacker nhắm gây ra thiệt hại nặng cho các doanh nghiệp/ tổ chức. [2]
Nhiều bước trung gian, người dùng có nguy cơ bị phát tán thông tin.
Root Server được nắm bởi tổ chức nên có nguy cơ bị thao túng.
Khó bảo dưỡng và nếu có lỗi dữ liệu trong hệ thống thì khó tìm ra và cần chi phí lớn để thực hiện.

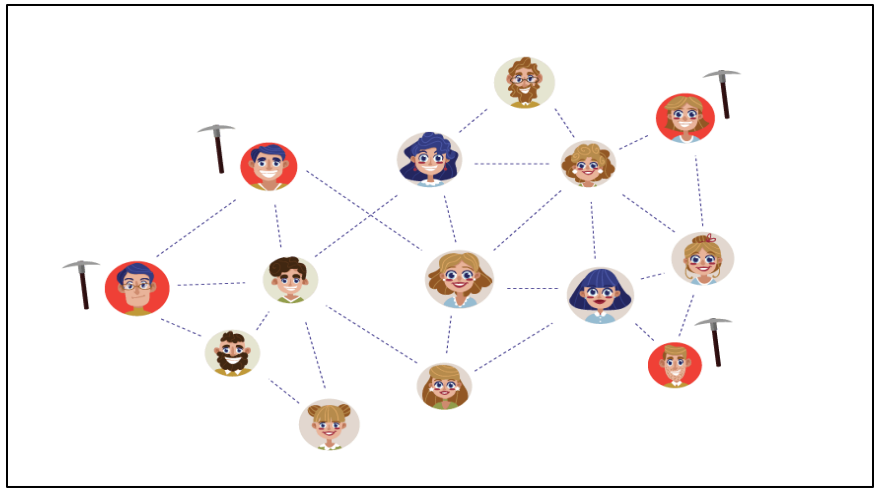
https://101blockchains.com/disadvantages-of-blockchain/

[1]: Internet Corporation for Assigned Names and Numbers (Tập đoàn cấp tên miền và số)

[2]: https://www.continuitycentral.com/index.php/news/technology/6621-2021-global-dns-threat-report-reveals-the-extent-and-impacts-of-dns-attacks

THUẬT TOÁN ĐỒNG THUẬN

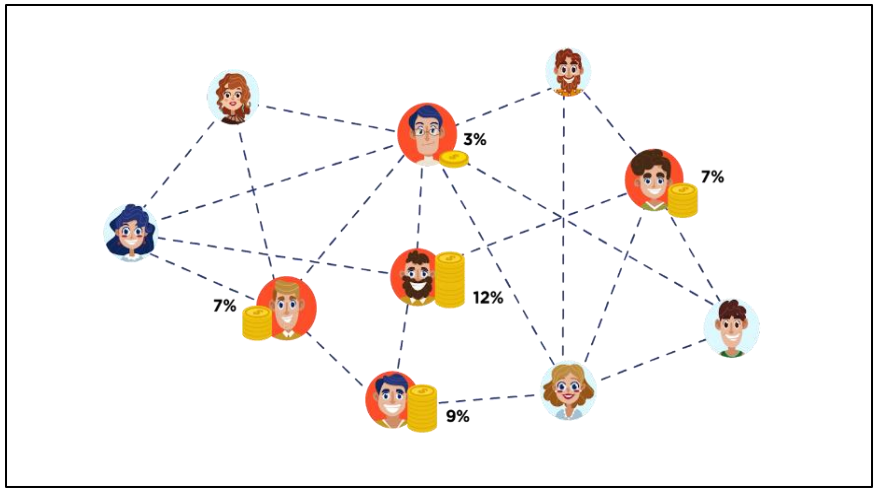
Proof of work và Proof of stake



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



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 [1]

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**

[1] : https://www.softwaretestinghelp.com/best-blockchain-dns-software/

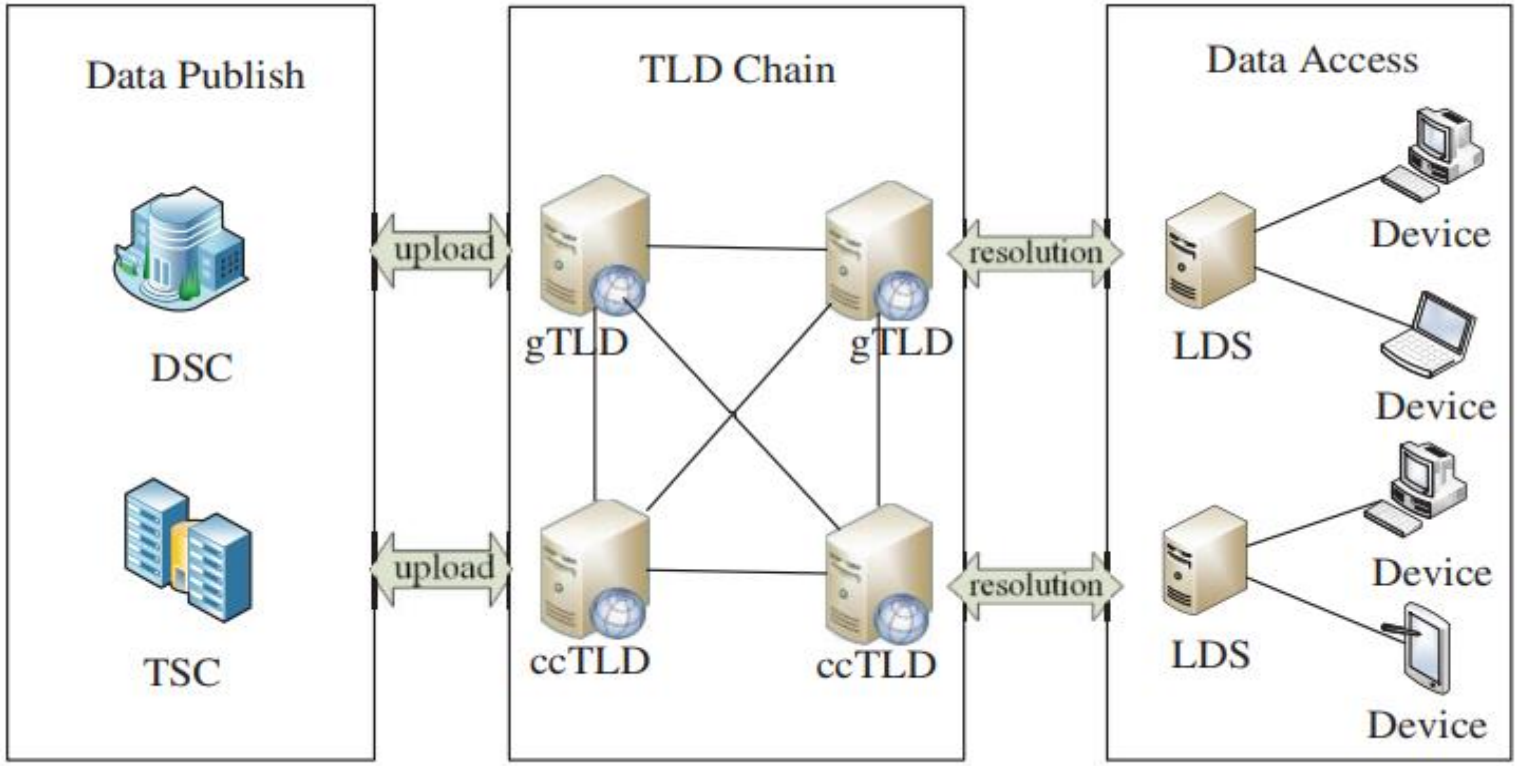
CƠ CHẾ CỦA DNS BLOCKCHAIN

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.



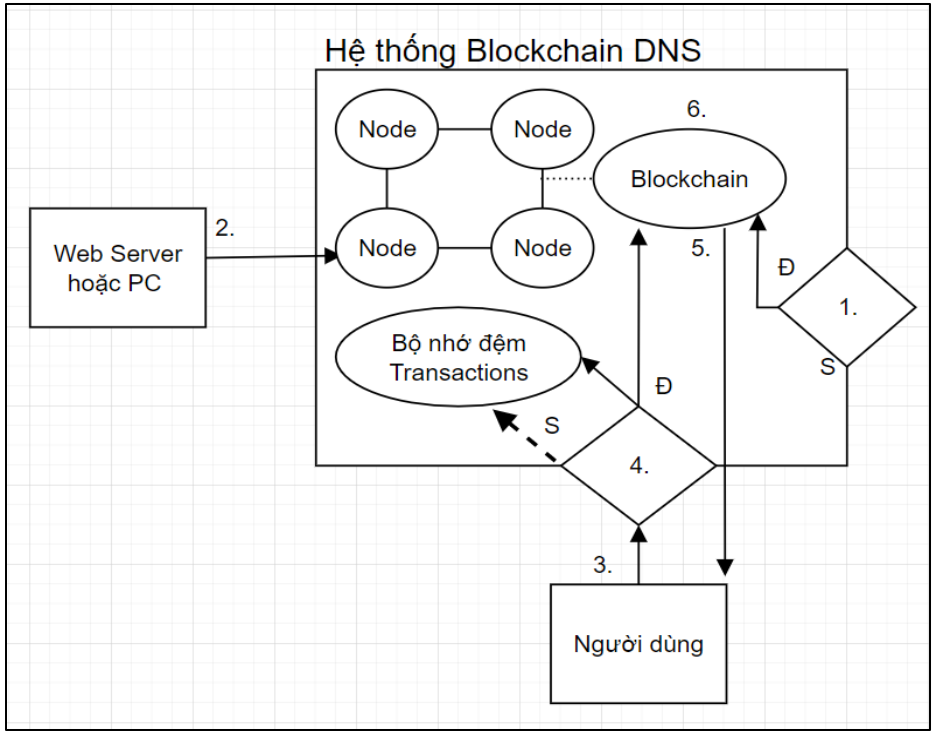
XÂY DỰNG DNS BLOCKCHAIN

Mô hình hoạt động

1. Hệ thống DNS Blockchain trực tiếp kiểm tra dãy Blocks hiện tại có đáp ứng điều kiện hay không theo 2 trường hợp như sau:
   - Đúng (Đ): Sử dụng các khối Blocks đó để khởi tạo Blockchain và tiếp tục mở rộng nhằm tạo blockchain dài nhất.
   - Sai (S): Khởi tạo Blockchain rỗng.

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

3. Người dùng có thể gửi yêu cầu phân giải cho hệ thống Blockchain DNS kèm theo tên miền thông qua input của giao diện Python Flask Web.



7. Hệ thống trước khi tắt sẽ tính toán blockchain dài nhất, xác thực blockchain và gửi lên cho các nodes để cập nhật.

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) : Thêm vào bộ nhớ đệm Transaction và phát động thuật toán Proof of Work cho các nodes tạo số Nonce cho Block mới.
   - Sai (S) : Chỉ thêm vào bộ nhớ đệm Transaction.

5. Hệ thống gửi kết quả sau khi phân giải cho người dùng thông qua hệ thống phân giải DNS.

6. Hệ thống ghi nhận lần kiểm duyệt giao dịch và gửi cho node thực hiện thành công, giao dịch sẽ được thêm vào block trong Blockchain.

XÂY DỰNG DNS BLOCKCHAIN

XÂY DỰNG ĐỊNH DẠNG LƯU TRỮ CHUNG TRONG HỆ THỐNG

Quan trọng nhất là DNS Record

- 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

=> Vì nếu thiếu, hệ thống DNS sẽ không phân giải được

XÂY DỰNG HỆ THỐNG BLOCKCHAIN VÀ GIAO DIỆN NGƯỜI DÙNG

Viết bằng 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

Viết bằng 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.

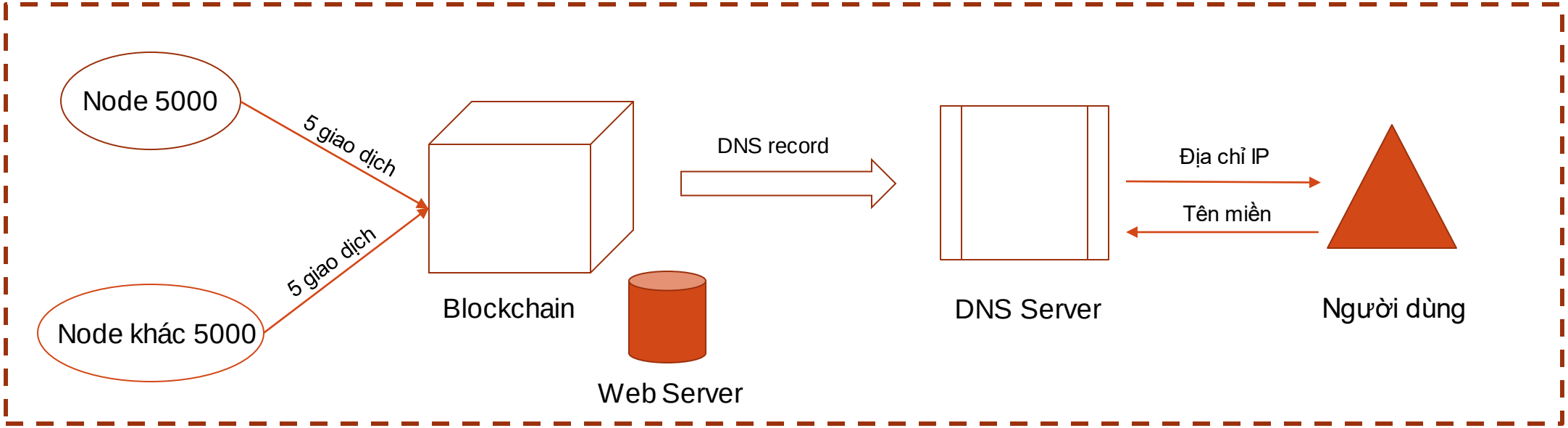
THỰC NGHIỆM

Kịch bản 1

Chạy DNS server, mở web server ở máy chính , mở 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 chính.

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

Môi trường máy chính



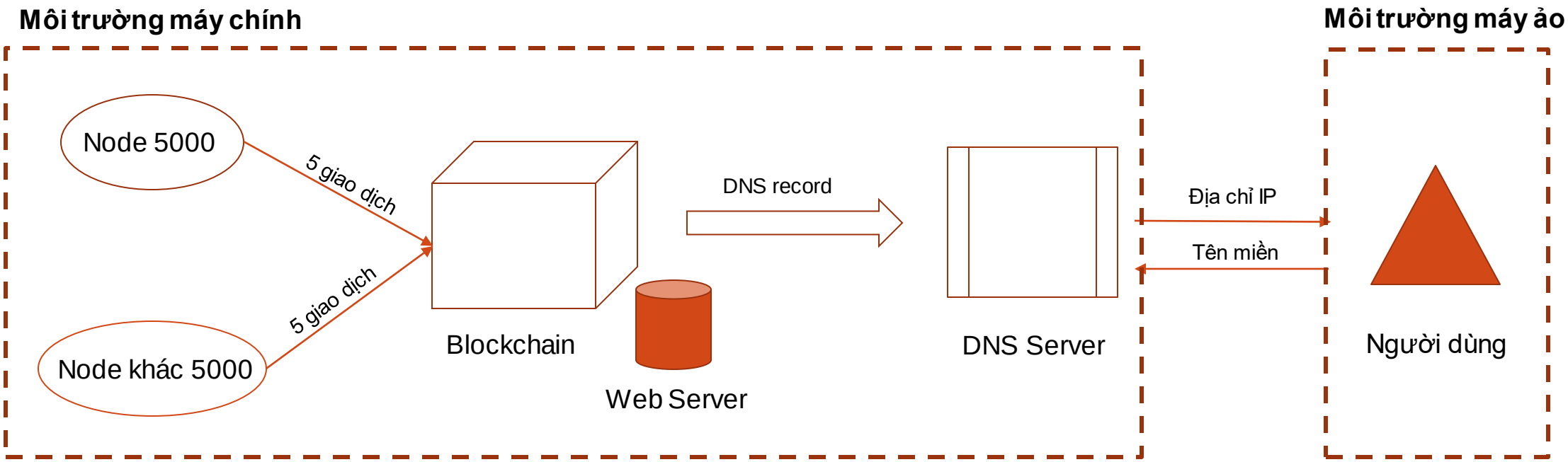
THỰC NGHIỆM

Kịch bản 2

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

Chạy DNS server, mở web server ở máy chính, mở 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 ảo.

Mở node với port bất kì, thực hiện thêm 5 giao dịch tên miền khác và phân giải tên miền thông qua một máy ảo.

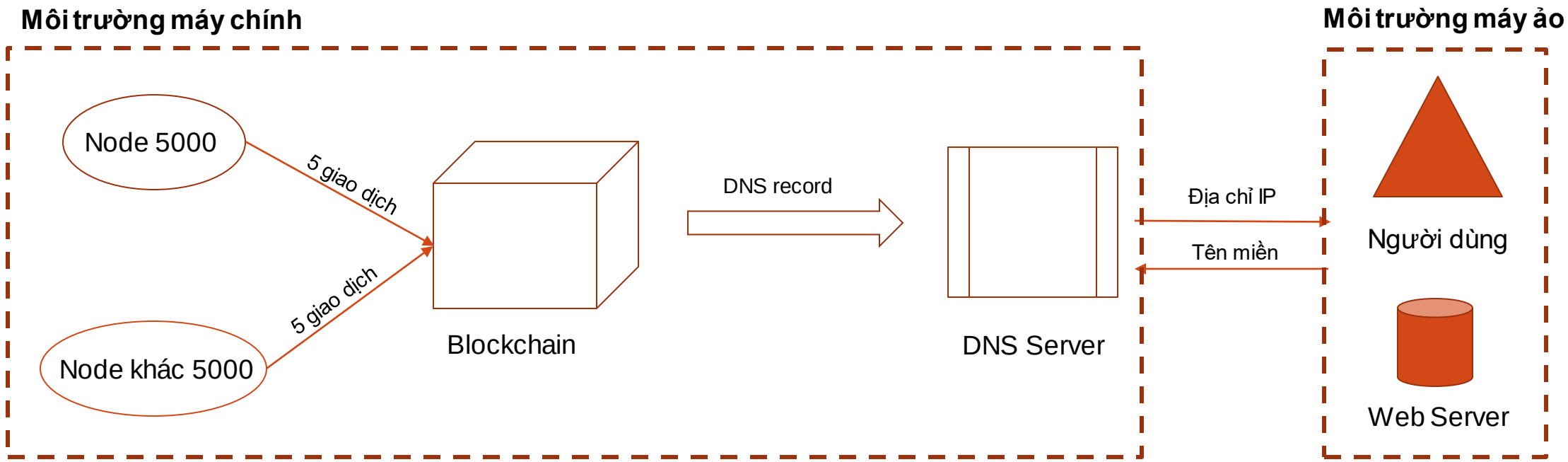


THỰC NGHIỆM

Kịch bản 3

Chạy DNS server, chạy web server trên máy ảo, mở 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 ảo.

Mở node có port khác, đăng nhập với vai trò là admin, thực hiện thêm 5 giao dịch tên miền cộng 1 giao dịch có tên miền trỏ vào địa chỉ của web server máy ảo và tiến hành phân giải trên máy ảo.



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 kiểu cũ giúp việc kế thừa và chuyển hóa công nghệ dễ dàng.
- Áp dụng DNS Server cho máy tính cá nhân có hệ điều hành không phải Windows Server.
- Phân giải tên miền cho các máy tính khác trong mạng có kết nối vào DNS Server.

⇨ **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

Trước khi đến giải pháp, đề tài còn có những hạn chế nhất định sau đây:

- 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 sẽ phần lớn nhắm vào hạn chế đã nêu trên như sau :

- 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.

Xin cảm ơn sự theo dõi của quý thầy cô

THANK YOU

Phan Đại