**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

PHAN ĐẠI MSSV: N17DCAT013 CHUYÊN NGÀNH: An toàn thông tin 2017 -2022 Lớp: D17CQAT01-N

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

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



**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**

TP. HCM 2021

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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

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



**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**

# GIAO NHIỆM VỤ ĐỀ TÀI

# LỜI CẢM ƠN

*Kính thưa quý thầy cô!*

Đồ án tốt nghiệp chuyên ngành An toàn thông tin với đề tài **“XÂY DỰNG HỆ THỐNG DNS DỰA TRÊN CÔNG NGHỆ BLOCKCHAIN”** là kết quả của quá trình cố gắng không ngừng nghỉ của bản thân và nhận được sự hướng dẫn tận tình của thầy cô cùng các anh chị và bạn bè. Qua đây, em xin gửi lời cảm ơn chân thành tới những người đã giúp đỡ em hoàn thành được đồ án này.

Em xin tỏ lòng kính trọng và biết ơn sâu sắc đến thầy Huỳnh Thanh Tâm là người trực tiếp hướng dẫn đồ án. Thầy đã cung cấp cho em những tài liệu cần thiết cho đồ án của em.

Em xin chân thành cảm ơn nhà trường ban lãnh đạo khoa Công nghệ thông tin 2 đã tạo điều kiện để cho em có thể hoàn thành tốt được đồ án của mình.

Em xin chân thành cảm ơn!

TP. Hồ Chí Minh, ngày tháng năm 2021

**Sinh viên thực hiện**

**Phan Đại**

# 

# MỤC LỤC

[GIAO NHIỆM VỤ ĐỀ TÀI i](#_Toc9619)

[LỜI CẢM ƠN ii](#_Toc29525)

[MỤC LỤC iii](#_Toc19934)

[DANH MỤC KÝ HIỆU VÀ CHỮ VIẾT TẮT vi](#_Toc2307)

[DANH MỤC CÁC BẢNG VẼ vii](#_Toc29890)

[DANH MỤC CÁC HÌNH VẼ viii](#_Toc8620)

[LỜI MỞ ĐẦU 1](#_Toc13165)

[CHƯƠNG I : TỔNG QUAN 2](#_Toc14811)

[1.1. LÝ DO CHỌN ĐỀ TÀI 2](#_Toc9197)

[1.2. MỤC TIÊU XÂY DỰNG ĐỀ TÀI 2](#_Toc7251)

[1.2.1. CÁC CHỨC NĂNG CHÍNH 2](#_Toc17213)

[1.2.2. HOẠT ĐỘNG 3](#_Toc16990)

[1.3. HƯỚNG TIẾP CẬN ĐỀ TÀI 3](#_Toc15569)

[1.4. TÓM TẮT KẾT QUẢ ĐẠT ĐƯỢC 3](#_Toc11174)

[CHƯƠNG II : CƠ SỞ LÝ THUYẾT 4](#_Toc13195)

[2.1. ĐỊNH NGHĨA NGÔN NGỮ LẬP TRÌNH PYTHON 4](#_Toc4579)

[2.1.1. NGÔN NGỮ PYTHON 4](#_Toc31541)

[2.1.2. LỊCH SỬ 4](#_Toc16094)

[2.1.3. CÁC TÍNH NĂNG RIÊNG CỦA PYTHON 4](#_Toc3833)

[2.1.4. CÁC LĨNH VỰC CẦN PYTHON 5](#_Toc16276)

[2.2. ĐỊNH NGHĨA CỦA DOMAIN NAME SYSTEM 6](#_Toc13423)

[2.2.1. KHÁI NIỆM 6](#_Toc17800)

[2.2.2. LỊCH SỬ RA ĐỜI 6](#_Toc30771)

[2.2.3. CHỨC NĂNG 6](#_Toc20350)

[2.2.4. CÁCH HOẠT ĐỘNG 6](#_Toc22569)

[2.2.5. ƯU ĐIỂM 7](#_Toc15670)

[2.2.6. KHUYẾT ĐIỂM 8](#_Toc20691)

[2.2.7. DANH SÁCH CÁC BẢN GHI DNS ĐƯỢC DÙNG NHIỀU NHẤT 8](#_Toc19940)

[2.3. ĐỊNH NGHĨA CỦA BLOCKCHAIN 9](#_Toc28261)

[2.3.1. KHÁI NIỆM 9](#_Toc18292)

[2.3.2. LỊCH SỬ RA ĐỜI 9](#_Toc18306)

[2.3.3. MỤC ĐÍCH 10](#_Toc13529)

[2.3.4. CẤU TRÚC 10](#_Toc14015)

[2.3.5. ĐẶC ĐIỂM 11](#_Toc23549)

[2.3.6. PHÂN LOẠI 11](#_Toc4448)

[2.3.7. ƯU ĐIỂM 12](#_Toc20494)

[2.3.8. NHƯỢC ĐIỂM 12](#_Toc19698)

[2.4. CÁCH BLOCKCHAIN HOẠT ĐỘNG VÀ CÁC GIAO THỨC 13](#_Toc27439)

[2.4.1. KHÁI QUÁT CÁCH BLOCKCHAIN HOẠT ĐỘNG 13](#_Toc21159)

[2.4.2. CÁC QUY TẮC HOẠT ĐỘNG TRONG BLOCKCHAIN 13](#_Toc4840)

[2.4.3. THUẬT TOÁN ĐỒNG THUẬN 15](#_Toc30366)

[2.4.4. CÁC LÝ DO CHÍNH ẢNH HƯỞNG ĐẾN SỰ SỬA DỮ LIỆU TRÁI PHÉP CỦA BLOCKCHAIN LÀ BẤT KHẢ THI 17](#_Toc1213)

[2.5. DANH SÁCH CÁC PHẦN MỀM DNS DỰA TRÊN BLOCKCHAIN HIỆN CÓ 18](#_Toc31371)

[2.6. CƠ CHẾ HOẠT ĐỘNG CỦA DNS DỰA TRÊN BLOCKCHAIN 19](#_Toc5333)

[2.7. ỨNG DỤNG THỰC TIỄN CỦA CÔNG NGHỆ BLOCKCHAIN TRONG CUỘC SỐNG 21](#_Toc32329)

[CHƯƠNG III : PHÂN TÍCH VÀ XÂY DỰNG 22](#_Toc22180)

[3.1. PHÂN TÍCH CÁC YÊU CẦU CỦA ĐỀ TÀI 22](#_Toc5732)

[3.1.1. Ý TƯỞNG ĐỀ TÀI 22](#_Toc10209)

[3.1.2. ĐỐI TƯỢNG SỬ DỤNG 22](#_Toc16291)

[3.1.3. CÁC CHỨC NĂNG CHÍNH CẦN THIẾT 22](#_Toc6240)

[3.1.4. NGUYÊN LÝ HOẠT ĐỘNG 23](#_Toc24590)

[3.2. XÂY DỰNG ĐỀ TÀI 24](#_Toc15748)

[3.2.1. XÂY DỰNG ĐỊNH DẠNG LƯU TRỮ CHO DNS RECORD 24](#_Toc18702)

[3.2.2. XÂY DỰNG QUY TRÌNH THÊM NODE CHO HỆ THỐNG DNS BLOCKCHAIN 24](#_Toc13919)

[3.2.3. XÂY DỰNG QUY TRÌNH THÊM BLOCK CHO HỆ THỐNG DNS BLOCKCHAIN 27](#_Toc2960)

[3.2.4. XÂY DỰNG QUY TRÌNH PHÂN GIẢI TÊN MIỀN CHO HỆ THỐNG DNS BLOCKCHAIN 29](#_Toc3518)

[CHƯƠNG IV: THỰC NGHIỆM 31](#_Toc13917)

[4.1. GIỚI THIỆU KỊCH BẢN THỰC NGHIỆM 31](#_Toc20918)

[4.2. XÂY DỰNG KỊCH BẢN THỰC NGHIỆM 31](#_Toc6141)

[4.3. THỰC HÀNH 31](#_Toc13414)

[CHƯƠNG V: KẾT LUẬN 32](#_Toc10460)

[5.1. CÁC KẾT QUẢ ĐẠT ĐƯỢC 32](#_Toc26643)

[5.2. ĐÁNH GIÁ 32](#_Toc10136)

[5.3. MỞ RỘNG ĐỀ TÀI 32](#_Toc14528)

[TÀI LIỆU THAM KHẢO 33](#_Toc145)

[TIẾNG VIỆT 33](#_Toc14322)

[TIẾNG ANH 33](#_Toc9019)

[DANH MỤC CÁC WEBSITE THAM KHẢO 33](#_Toc13133)

# DANH MỤC KÝ HIỆU VÀ CHỮ VIẾT TẮT

BTC : Bitcoin Tiền ảo Bitcoin

CMD : Command Prompt Ứng dụng nhận lệnh của Windows

CMS : Content Management System Hệ thống quản trị nội dung

CNAME : Canonical Name Record Bản ghi bí danh cho domain

DNS : Domain Name System Hệ thống phân giải tên miền.

DNSSEC : Domain Name System Security Công nghệ an toàn mở rộng cho hệ thống DNS

DSC : Domain Name Service Center Trung tâm quản lý tên miền

ICANN : Internet Corporation for Assigned Names and Numbers Tổ chức quản lý tên miền trên toàn thế giới

IP : Internet Protocol Địa chỉ giao thức của internet

JSON : JavaScript Object Notation Ký hiệu đối tượng JavaScript

MX : Mail Exchange Record Record giúp xác định mail server

OOP : Object Oriented Programming Lập trình hướng đối tượng

PBS : Public Broadcasting Service Dịch vụ Truyền thông Công cộng

PKI : Public Key Infrastructure Hạ tầng khóa công khai

PoC : Proof of Concept Bằng chứng về khái niệm

TLD : Top level Domain Tên miền cấp cao nhất

TOR : The Onion Router Giao thức phân tuyến của Onion

TSC : TLD Service Centers Trung tâm quản lý TLD

VPN : Virtual Private Network Mạng riêng ảo

# 

# DANH MỤC CÁC BẢNG VẼ

[Bảng 1 . Bảng phân giải SRV record 9](#_Toc21502)

[Bảng 2 . Bảng liệt kê các cơ chế ngăn việc sửa trái phép trên Blockchain 18](#_Toc25683)

[Bảng 3 . Bảng liệt kê các tham số của Node 25](#_Toc6856)

[Bảng 4 . Bảng liệt kê các trường hợp khi xử lý thông tin Node 26](#_Toc5260)

[Bảng 5 . Bảng liệt kê các thuộc tính của Block 27](#_Toc15840)

# 

# DANH MỤC CÁC HÌNH VẼ

[Hình 1 . Quy tắc phân giải tên miền 6](#_Toc11493)

[Hình 2 . Cách hoạt động của DNS 7](#_Toc5219)

[Hình 3 . Cấu trúc của khối Block 10](#_Toc8339)

[Hình 4 . Cấu trúc của Blockchain 11](#_Toc15265)

[Hình 5 . Phân loại blockchain 11](#_Toc14804)

[Hình 6 . Các lợi ích khi sử dụng công nghệ Blockchain 12](#_Toc4248)

[Hình 7 . Qthêm một giao dịch vào blockchain 13](#_Toc30391)

[Hình 8 . Cách xác định số dư của tài khoản 14](#_Toc16243)

[Hình 9 . Thuật toán đồng thuận Proof of Work 16](#_Toc3940)

[Hình 10 . Thuật toán đồng thuận Proof of Stake 17](#_Toc16706)

[Hình 11 . Sơ đồ cơ chế Blockchain DNS 20](#_Toc16899)

[Hình 12 . Sơ đồ nguyên lý hoạt động của Blockchain DNS 23](#_Toc9978)

[Hình 13 . Trường hợp xử lý thông tin node 1 26](#_Toc5593)

[Hình 14 . Trường hợp xử lý thông tin node 2 26](#_Toc5565)

[Hình 15 . Trường hợp xử lý thông tin node 3 27](#_Toc22964)

[Hình 16 . Trường hợp xử lý thông tin node 4 27](#_Toc22620)

[Hình 17 . Trường hợp xử lý thông tin node 5 27](#_Toc24970)

[Hình 18 . Xử lý thêm transactions trong quy trình tạo block 28](#_Toc10779)

[Hình 19 . Xử lý khi tiếp nhận yêu cầu mine Block 28](#_Toc18269)

[Hình 20 . Điều kiện để tạo block 29](#_Toc7860)

[Hình 21 . Xử lý chính khi tạo block 29](#_Toc13153)

[Hình 22 . Xử lý khi tiếp nhận yêu cầu phân giải tên miền 30](#_Toc19358)

[Hình 23 . Xử lý tìm kiếm tên miền 30](#_Toc28513)

# LỜI MỞ ĐẦU

Ngay từ những năm đầu thập niên 80 của thế kỷ trước, các nhà sáng chế đã cố gắng tìm cách giải quyết các vấn đề bảo mật, an ninh trên internet bằng các thuật toán mã hóa. Nhưng rất khó khăn để có thể giải quyết bài toán này, bởi các giao dịch trên mạng luôn có khả năng bị rò rỉ do sự tham gia hoặc cố tình can thiệp của bên thứ ba, bao gồm cả tội phạm mạng. Chẳng hạn như thanh toán bằng thẻ tín dụng qua internet là không an toàn, vì người dùng đã phải tiết lộ quá nhiều dữ liệu cá nhân, đồng thời chịu phí giao dịch cao dù chỉ là các khoản thanh toán nhỏ.

Năm 2008, Satoshi Nakamoto, người được biết đến là cha đẻ của Bitcoin, đã vạch ra một giao thức mới cho hệ thống tiền mặt điện tử ngang hàng (peer-to-peer) sử dụng các dạng mã hóa để tạo ra đồng tiền kỹ thuật số Bitcoin.

Dựa trên nền tảng này, Blockchain - công nghệ phân phối bảng kê, đã ra đời. Mỗi bảng kê tương đương hàng triệu dữ liệu số liên quan quá trình phát triển, chuyển giao,... của một giao dịch trên mạng. Có người gọi mỗi “block” như một cuốn sổ cái trong kế toán, và Blockchain là chuỗi thông tin của hàng loạt cuốn sổ cái như vậy liên kết lại, và mã hóa mà thành.

Với quy tắc hoạt động này, Blockchain đóng vai trò quan trọng trong việc giải quyết những vấn đề tồn động của hệ thống DNS truyền thống mà cả Internet đang phụ thuộc vào : hệ thống DNS hiện tại là chịu sự kiểm soát hay quy định của chính phủ, chính phủ có thể lấy một số lý do cấm các máy chủ nhất định nếu họ thấy nó ảnh hướng đến lợi ích của họ hay quốc gia họ. Chính phủ có thể yêu cầu tất cả các nhà cung cấp dịch vụ Internet ở quốc gia đó chặn một số tên miền nhất định, nó ảnh hưởng đến quyền lợi của công dân và tính nhân quyền của họ. Ví dụ điển hình cho tình trạng này là xảy ra năm 2014 khi các IPS ở Thổ Nhĩ Kỳ được yêu cầu không giải quyết cho twitter.com.

Vì thế một DNS Blockchain sẽ được dựa trên hệ thống phi tập trung do đó hoàn toàn không chịu tác động của bên thứ 3 vào quá trình chuyển hướng của hệ thống DNS như hiện tại. Hơn nữa, DNS dựa trên Blockchain có thể chống lại sự kiểm duyệt và cũng tránh được vấn đề nhiễm mã độc DNS Cache hoặc giả mạo DNS.

DNS dựa trên công nghệ blockchain là một đề tài rất thu hút các nhà phát triển, họ mong muốn có được một hệ thống Internet công bằng hơn. Ví dụ Blockstack, Ethereum Name Service và Namecoin… Các dự án khác nhau trong lĩnh vực này với mong muốn đưa ra một hệ thống DNS dựa trên Blockchain.

Điểm mấu chốt của vấn đề là công nghệ Blockchain là một lực lượng không thể ngăn cản. Công nghệ này nắm giữ một tương lai hứa hẹn khi nói đến sự phát triển hệ thống DNS dựa trên công nghệ Blockchain. Các hệ thống này sẽ được bảo mật, linh hoạt và đặc biệt hơn ở đó dữ liệu sẽ không còn tập trung vào một đơn vị thứ ba nữa, nó hoàn thuộc về chủ sở hữu của nó người sáng tạo nội dung. Người dùng sẽ hưởng được nhiều quyền lợi hơn từ dữ liệu cá nhân, khác hẳn những gì mà hệ thống cũ đang hoạt động, nơi mà các công ty như Google, Facebook… sử dụng chính dữ liệu đó để kiếm tiền.

# CHƯƠNG I : TỔNG QUAN

* 1. **LÝ DO CHỌN ĐỀ TÀI**

Blockchain là một công nghệ trong đó toàn bộ dữ liệu được mã hóa thành các khối và nối với nhau tạo thành chuỗi dài. Mỗi khi có một thông tin hay một giao dịch mới phát sinh, thông tin cũ sẽ không bị mất đi mà thay vào đó là thông tin mới sẽ được lưu vào một khối (block) mới và gắn nối tiếp vào khối cũ tạo thành một chuỗi (chain).

Hơn thế nữa, thông tin của blockchain không chỉ nằm trên một máy chủ duy nhất mà nó sẽ được tự động phân tán và sao lưu trên nhiều máy chủ khác nhau có kết nối với hệ thống blockchain, từ đó tất cả mọi người đều có thể nhìn thấy và kiểm tra được giao dịch của mình. Điều này ngăn cản việc chỉnh sửa hay gian lận, thông tin được đảm bảo an toàn và minh bạch.

Công nghệ phân tán dữ liệu phi tập trung này cũng khiến giảm tải áp lực từ phía các tổ chức tài chính. Không chỉ thế, blockchain còn có tính bảo mật cao. Những vụ tấn công vào hệ thống dữ liệu tập trung (như của các ngân hàng) sẽ rất khó có thể thực hiện được đối với mạng lưới blockchain. Chẳng hạn, để hack thông tin trong một block cụ thể nào đó, hacker sẽ phải hack không chỉ block đó mà cả tất tật những block nằm trước nó, trên hàng triệu sổ cái trong mạng lưới cùng lúc.

Bên cạnh đó, ứng dụng DNS truyền thống đã và đang có nguy cơ bị đe dọa bởi các cuộc tấn công tập trung. Những cái tên lớn như Amazon, Twitter, Etsy, Github và Spotify cũng bị ảnh hưởng khi trang web của họ nằm trong hệ thống máy chủ DNS mà hacker đang nhắm vào. Giải pháp cho vấn đề này là một hệ thống DNS được xây dựng theo công nghệ Blockchain.

Blockchain đã và đang là một công nghệ được cộng đồng tin dùng với ứng dụng tiền điện tử nổi tiếng của nó. Không chỉ mang giá trị cao mà còn mang cho người dùng cảm giác an toàn trước những mối đe dọa trên mạng này. DNS truyền thống có nhiều vấn đề tồn đọng mà Blockchain có thể giải quyết được nên sự cải tiến công nghệ này chỉ còn vấn đề về thời gian.

Không phủ nhận một số ứng dụng của blockchain hiện còn nhiều yếu điểm chưa thể giải quyết tức thời. Nhìn một cách tích cực về công nghệ này, những khó khăn, thất bại hiện thời rất có thể sẽ mở đường cho những sản phẩm khả thi hơn trong tương lai, đưa blockchain tiến gần hơn tới kỳ vọng trở thành “the new internet” của những thập kỷ sắp tới.

* 1. **MỤC TIÊU XÂY DỰNG ĐỀ TÀI**

### CÁC CHỨC NĂNG CHÍNH

* Nhận dữ liệu đầu vào thông qua input form của ứng dụng.
* Đăng nhập và đăng ký để trở thành hoster ( người đăng kí tên miền ).
* Hoster có thể đăng kí tên miền và có thể sửa đổi nếu đó là tên miền mà hoster đã tạo.
* Client có thể xem được thông tin của tên miền ngay trên ứng dụng.
* Admin có thể quản lí, giám sát những dữ liệu liên quan đến hoster và client.
* Ứng dụng có thể phân giải tên miền thành địa chỉ IP đã được định nghĩa bởi hoster.
* Xuất thống kê về lượng dữ liệu đã đạt được.
* Quản lí chuỗi các server dưới dạng diagram.
* Có thể phát triển về sau.

### HOẠT ĐỘNG

* Người đăng kí miền – hoster sẽ đăng kí tên miền cho hệ thống DNS.
* Người dùng – client gửi yêu cầu phân giải cho DNS.
* Chương trình sẽ tương tác với người dùng, tiền hành nhận yêu cầu.
* Blockchain server sẽ tiến hành xác thực yêu cầu và mining các block để tìm kiếm dữ liệu phù hợp với yêu cầu và gửi lại cho chương trình.
* Chương trình sẽ gửi kết quả ra màn hình của người dùng.
* Admin sẽ tiến hành thống kê những dữ liệu liên quan theo một mốc thời gian nhất định.
  1. **HƯỚNG TIẾP CẬN ĐỀ TÀI**

Từ các mục tiêu và các hoạt động đặt ra cho đề tài, tiến hành phân tích và đưa ra các phương hướng giải quyết sau:

* Sử dụng ngôn ngữ lập trình Python và các thư viện cần thiết để xây dựng chương trình.
* Nhập các thông tin đăng kí:
  + Nhập trực tiếp vào giao diện form.
  + Lưu các dữ liệu đầu vào cơ sở dữ liệu.
* Sử dụng công nghệ Blockchain để lưu trữ những dữ liệu liên quan đến tên miền.
* Chạy song song các node để hỗ trợ đưa các block vào chain để lưu trữ.
* Các node sẽ phân giải tên miền theo giao thức đồng thuận PoC.
* Sử dụng công cụ dig để kiểm tra tên miền và trả về kết quả cho người dùng.
  1. **TÓM TẮT KẾT QUẢ ĐẠT ĐƯỢC**
* Sử dụng ngôn ngữ Python và các thư viện cần thiết để xây dựng chương trình.
* Xây dựng được một hệ thống Blockchain.
* Xây dựng được cơ sở dữ liệu và hệ thống tương tác với người dùng.
* Chương trình có thể dễ dàng mở rộng và phát triển về sau.

# CHƯƠNG II : CƠ SỞ LÝ THUYẾT

## ĐỊNH NGHĨA NGÔN NGỮ LẬP TRÌNH PYTHON

### 2.1.1. NGÔN NGỮ PYTHON

Python là một ngôn ngữ lập trình bậc cao được tạo ra bởi Guido van Rossum nhằm phục vụ cho mục đích lập trình đa tính năng. Python được thiết kế với ưu điểm là dễ đọc, dễ học và dễ nhớ. Cú pháp của Python chính là điểm cộng lớn vì sự rõ ràng, dễ hiểu và cách gõ linh động làm cho nó nhanh chóng trở thành một ngôn ngữ lý tưởng để viết mã và phát triển ứng dụng trong nhiều lĩnh vực, ở hầu hết các nền tảng.

Python hoàn toàn tạo kiểu động và sử dụng cơ chế cấp phát bộ nhớ tự động. Ngôn ngữ này có cấu trúc dữ liệu cấp cao, mạnh mẽ và cách tiếp cận đơn giản nhưng hiệu quả đối với lập trình hướng đối tượng.

Python là ngôn ngữ có hình thức đơn giản, cấu trúc rõ ràng, thuận tiện cho người mới học lập trình. Cấu trúc của nó cho phép người sử dụng viết các mã lệnh với số lần gõ phím tối thiểu.

Python hiện tại có hai phiên bản phổ biến là Python2 và Python3. Mỗi phiên bản đều có những ưu điểm so với phiên bản còn lại. Tùy vào mục đích sử dụng và môi trường sử dụng, các lập trình viên có thể lựa chọn phiên bản cho phù hợp. Tuy nhiên, Python2 sẽ không còn được hỗ trợ kể từ năm 2020 và trang chủ của ngôn ngữ này cũng khuyến khích người dùng nên chuyển sang sử dụng Python3 để có thể tận dụng tối đa sức mạnh và các ưu điểm của ngôn ngữ này.

### 2.1.2. LỊCH SỬ

Vào cuối những năm 1980, Guido Van Rossum làm việc trong Amoeba, phân phối một nhóm hệ điều hành. Ông muốn sử dụng một ngôn ngữ thông dịch như ABC (ABC có cú pháp rất dễ hiểu) để truy cập vào những cuộc gọi hệ thống Amoeba. Vì vậy, ông quyết định tạo ra một ngôn ngữ mở rộng. Điều này đã dẫn đến một thiết kế của ngôn ngữ mới, chính là Python, lần đầu được phát hành lần đầu tiên vào tháng 2 năm 1991.

### 2.1.3. CÁC TÍNH NĂNG RIÊNG CỦA PYTHON

* **Ngôn ngữ lập trình đơn giản, dễ học:**

Python có cú pháp rất đơn giản, rõ ràng. Nó dễ đọc và viết hơn rất nhiều khi so sánh với những ngôn ngữ lập trình khác như C++, Java, C#. Python làm cho việc lập trình trở nên thú vị, cho phép tập trung vào những giải pháp chứ không phải cú pháp.

* **Miễn phí, mã nguồn mở:**

Có thể tự do sử dụng và phân phối Python, thậm chí là dùng nó cho mục đích thương mại. Vì là mã nguồn mở, không những có thể sử dụng các phần mềm, chương trình được viết trong Python mà còn có thể thay đổi mã nguồn của nó. Python có một cộng đồng rộng lớn, không ngừng cải thiện nó mỗi lần cập nhật.

* **Khả năng di chuyển:**

Các chương trình Python có thể di chuyển từ nền tảng này sang nền tảng khác và chạy nó mà không có bất kỳ thay đổi nào. Nó chạy liền mạch trên hầu hết tất cả các nền tảng như Windows, macOS, Linux.

* **Khả năng mở rộng và có thể nhúng:**

Giả sử một ứng dụng đòi hỏi sự phức tạp rất lớn, có thể dễ dàng kết hợp các phần code bằng C, C++ và những ngôn ngữ khác (có thể gọi được từ C) vào code Python. Điều này sẽ cung cấp cho ứng dụng những tính năng tốt hơn cũng như khả năng scripting mà những ngôn ngữ lập trình khác khó có thể làm được.

* **Ngôn ngữ thông dịch cấp cao:**

Không giống như C/C++, với Python, không phải lo lắng những nhiệm vụ khó khăn như quản lý bộ nhớ, dọn dẹp những dữ liệu vô nghĩa,... Khi chạy code Python, nó sẽ tự động chuyển đổi code sang ngôn ngữ máy tính có thể hiểu. Không cần lo lắng về bất kỳ hoạt động ở cấp thấp nào.

* **Thư viện tiêu chuẩn lớn để giải quyết những tác vụ phổ biến:**

Python có một số lượng lớn thư viện tiêu chuẩn giúp cho công việc lập trình trở nên dễ dàng hơn rất nhiều, đơn giản vì không phải tự viết tất cả code. Ví dụ: Cần kết nối cơ sở dữ liệu MySQL trên Web server? Có thể nhập thư viện MySQLdb và sử dụng nó. Những thư viện này được kiểm tra kỹ lưỡng và được sử dụng bởi hàng trăm người. Vì vậy, có thể chắc chắn rằng nó sẽ không làm hư hại code hay ứng dụng.

* **Hướng đối tượng:**

Mọi thứ trong Python đều là hướng đối tượng. Lập trình hướng đối tượng (OOP) giúp giải quyết những vấn đề phức tạp một cách trực quan. Với OOP, có thể phân chia những vấn đề phức tạp thành những tập nhỏ hơn bằng cách tạo ra các đối tượng.

### 2.1.4. CÁC LĨNH VỰC CẦN PYTHON

* **Lập trình ứng dụng web:**

Có thể tạo web app có khả năng mở rộng (scalable) được bằng cách sử dụng framework và CMS (Hệ thống quản trị nội dung) được tích hợp trong Python. Vài nền tảng phổ biến để tạo web app là: Django, Flask, Pyramid, Plone, Django CMS. Các trang như Mozilla, Reddit, Instagram và PBS đều được viết bằng Python.

* **Khoa học và tính toán:**

Có nhiều thư viện trong Python cho khoa học và tính toán số liệu, như SciPy và NumPy, được sử dụng cho những mục đích chung chung trong tính toán. Và, có những thư viện cụ thể như: EarthPy cho khoa học trái đất, AstroPy cho Thiên văn học,... Ngoài ra, Python còn được sử dụng nhiều trong machine learning, khai thác dữ liệu và deep learning.

* **Tạo nguyên mẫu phần mềm:**

Python chậm hơn khi so sánh với các ngôn ngữ được biên dịch như C++ và Java. Nó có thể không phải là lựa chọn tốt nếu nguồn lực bị giới hạn và yêu cầu về hiệu quả là bắt buộc. Tuy nhiên, Python là ngôn ngữ tuyệt vời để tạo những nguyên mẫu (bản chạy thử - prototype). Ví dụ, có thể sử dụng Pygame (thư viện viết game) để tạo nguyên mẫu game trước. Nếu thích nguyên mẫu đó có thể dùng C++ để viết game thực sự.

* **Ngôn ngữ tốt để dạy lập trình:**

Python được nhiều công ty, trường học sử dụng để dạy lập trình cho trẻ em và những người mới lần đầu học lập trình. Bên cạnh những tính năng và khả năng tuyệt vời thì cú pháp đơn giản và dễ sử dụng của nó là lý do chính cho việc này.

## ĐỊNH NGHĨA CỦA DOMAIN NAME SYSTEM

### 2.2.1. KHÁI NIỆM

Domain Name System hay còn được viết tắt là DNS. Cụm từ này mang ý nghĩa đầy đủ là hệ thống phân giải tên miền. Hiểu một cách đơn giản nhất, DNS sẽ làm công việc chuyển đổi các tên miền thành một địa chỉ IP dạng số tương ứng với tên miền đó và ngược lại từ địa chỉ IP thành tên miền.



Hình 1. Quy tắc phân giải tên miền

### 2.2.2. LỊCH SỬ RA ĐỜI

Vào những năm 1970 mạng ARPanet của bộ quốc phòng Mỹ rất nhỏ và dễ dàng quản lý các liên kết vài trăm máy tính với nhau. Do đó mạng chỉ cần một file HOSTS.TXT chứa tất cả thông tin cần thiết về máy tính trong mạng và giúp các máy tính chuyển đổi được thông tin địa chỉ và tên mạng cho tất cả máy tính trong mạng ARPanet một cách dễ dàng. Và đó chính là bước khởi đầu của hệ thống tên miền gọi tắt là DNS ( Domain name system).

### 2.2.3. CHỨC NĂNG

Domain Name System được ví như một “người phiên dịch” và “truyền đạt thông tin”. DNS có nhiệm vụ dịch tên miền thành một địa chỉ IP gồm 4 nhóm số khác nhau. Ví dụ: DNS dịch tên miền www.tenmien.com thành 421.64.874.899 hoặc ngược lại dịch một địa chỉ IP thành tên miền.

Việc “dịch” của DNS sẽ giúp người dùng đăng nhập vào một website dễ dàng hơn. Thay vì phải nhớ và nhập một dãy số địa chỉ IP của hosting, thì chỉ cần nhập tên website là trình duyệt tự động hiểu và đăng nhập vào được.

### 2.2.4. CÁCH HOẠT ĐỘNG

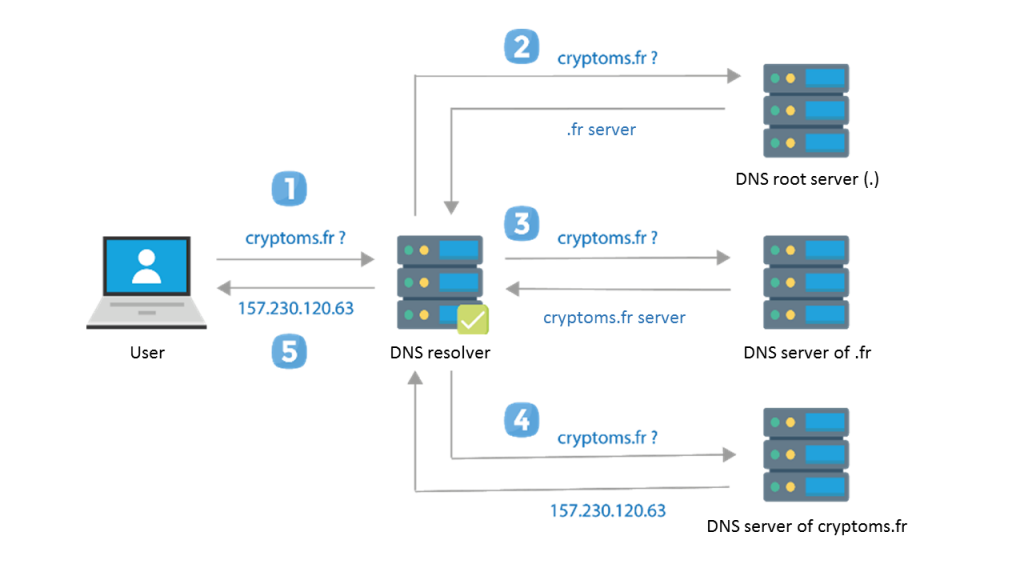
Khi người dùng muốn truy cập vào trang web có địa chỉ là cryptoms.fr

1. Người dùng gửi yêu cầu tìm kiếm địa chỉ IP ứng với tên miền cryptoms.fr tới Name Server cục bộ.
2. Máy chủ domain cục bộ sẽ tìm kiếm trong kho dữ liệu xem có cơ sở dữ liệu chuyển đổi từ tên miền sang địa chỉ IP của tên miền mà người dùng yêu cầu hay không.
3. Nếu “có” thì nó sẽ gửi trả lại địa chỉ IP của máy có tên miền đó,

Nếu “không có” nó sẽ hỏi lên các máy chủ tên miền ở mức cao nhất (ROOT). Máy chủ tên miền mức ROOT này sẽ chỉ cho máy chủ tên miền cục bộ địa chỉ mà nó quản lý có đuôi “.fr”.

1. Máy chủ tên miền cục bộ gửi yêu cầu đến máy chủ quản lý tên miền Pháp“.fr” tìm tên miền cryptoms.fr.
2. Máy chủ tên miền cục bộ sẽ hỏi máy chủ quản lý tên miền “.fr” địa chỉ IP của tên miền “cryptoms.fr” và gửi trả lại cho máy chủ tên miền cục bộ. Máy chủ tên miền cục bộ chuyển thông tin đến máy của người dùng. Người dùng sử dụng địa chỉ IP này kết nối đến server chứa website có địa chỉ “cryptoms.fr”.

Ví dụ cách hoạt động của DNS với cryptoms.fr



Hình 2. Cách hoạt động của DNS

### 2.2.5. ƯU ĐIỂM

Có 5 ưu điểm là :

* **Sự quan trọng với Internet:** DNS là một hệ thống toàn cầu giúp người dùng sử dụng Internet hiệu quả. Với tầm quan trọng của Internet đối với xã hội, điều này càng khiến DNS có vai trò không thể thiếu giúp Internet phát triển bền vững. Có thể nói nếu thiếu DNS, Internet không thể tồn tại lâu dài.
* **Không cần lưu trữ một dãy IP dài và khó nhớ:** DNS đưa ra một phương pháp tiện lợi hơn, chuyển đổi những tên domain, tên sub-domain thành IP. Việc tự nhớ một dãy số không có ý nghĩa gây cản trở giữa người dùng và trang web mà họ thường xuyên xem. DNS giúp được điều đó và mang tính hữu dụng cho các công cụ tìm kiếm.
* **Dễ truy cập hơn không có nghĩa là dễ bị tấn công hơn:** Với sự phong phú của ngôn từ, phân biệt giữa môi trường riêng tư và môi trường làm việc, giữa môi trường cộng đồng. DNS Server được thiết kế cho mục đích bảo mật thường đảm bảo rằng sẽ cản trở những mục đích tấn công vào hệ thống. Tuy nhiên một điều quan trọng là cần phải được áp dụng những biện pháp bảo mật khác với tốc độ phát triển công nghệ hiện nay.
* **DNS có tốc độ truy cập Internet cao nhất:** Doanh nghiệp hoặc cá nhân sử dụng DNS Server có thể tận dụng từ tốc độ truy cập đó để đảm bảo công việc của mình
* **Cập nhật danh sách IP dễ dàng:** Việc cập nhật IP xảy ra thường xuyên và về phía người dùng cũng vậy. Thông thường thì rất mất thời gian và công sức. Nhưng với cấu trúc của DNS thì có thể làm được việc này một cách dễ dàng.

### 2.2.6. KHUYẾT ĐIỂM

Có 5 khuyết điểm là :

* **DNS phụ thuộc vào sự kiểm soát của Hoa Kỳ:** DNS Server được kiểm soát tập trung bởi một tổ chức phi lợi nhuận là ICANN có trụ sở tại Hoa Kỳ. Điều này gây khó khăn cho các nước không phụ thuộc vào Hoa Kỳ có thể sử dụng dịch vụ này.
* **DNS queries thường không mang bất kì thông tin về client khởi tạo nó:** Điều này lý giải cho việc hacker rất hay nhắm vào DNS. Bởi vì phía Server chỉ thấy địa chỉ IP từ nơi query tới và có thể bị điều khiển bởi các hacker. ( DNS request = DNS query )
* **DNS dựa vào quan hệ chủ-tớ:** Điều này có nghĩa rằng nếu server ở máy chủ bị hỏng hoặc bị điều khiển bằng cách nào đó, sẽ khiến cho người dùng truy cập vào trang web hoặc database nằm trong server. Hacker có thể phát huy điểm mạnh của mình bằng cách nhắm vào các máy chủ và dẫn người dùng tới trang web khác, họ có thể tìm cách để lừa đảo thông tin.
* **Khi DNS Server down, World Wide Web cũng vậy:** Mặc dù đã có back up của server và server gốc. Tại vì khi một server bị crash thì sẽ dẫn tới các local network lân cận sẽ không thể kết nối với client được
* **DNS là nguyên nhân chính dẫn đến cuộc tấn công DNS:** Địa chỉ của DNS được thay đổi với địa chỉ giả mạo do đó người dùng sẽ bị dẫn đến các website khác. Từ đó hacker có thể thu thập thông tin cá nhân của người dùng đó.

### 2.2.7. DANH SÁCH CÁC BẢN GHI DNS ĐƯỢC DÙNG NHIỀU NHẤT

Bản ghi là một dạng lưu trữ một hoặc nhiều giá trị có format sẵn tùy theo tên gọi của record đó nhờ đó Server có thể hiểu và phân giải để hoạt động.

* **A record:** Là bản ghi được sử dụng trỏ tên website tới một địa chỉ IP cụ thể. Có thể thêm tên mới, TTL (Time to Live, thời gian tự động tải lại bản ghi), Points to (trỏ tới IP nào).
* **CNAME record:** Đóng vai trò như đặt một hoặc nhiều tên khác cho tên miền chính. Có thể tạo một tên mới, trỏ tới tên gốc là gì, đặt TTL với bản ghi này.
* **MX record:** Là một bản ghi chỉ định server nào quản lý các dịch vụ email của tên miền đó. Có thể trỏ tên miền tới mail server, đặt mức độ ưu tiên (priority), đặt TTL.
* **TXT record:** Dùng để chứa các thông tin dạng text (văn bản) của tên miền. Có thể thêm Host mới, Giá trị TXT, TTL (Time to Live), Points to.
* **AAAA record:** Dùng để trỏ domain tới một địa chỉ IPV6 address. Có thể thêm host mới, IPv6, TTL.
* **NS record:** Dùng để chỉ định nameserver cho từng tên miền phụ. Có thể tạo host mới, tên name server (NS), TTL (Time to Live).
* **SRV record:** Dùng để xác định chính xác dịch vụ nào chạy port nào. Có thể thêm Priority, Name, Weight, Port, Points to, TTL.

Ví dụ về SRV record và các thuộc tính sẽ phân giải :

|  |
| --- |
| \_xmpp-server.\_tcp.gmail.com. IN SRV 5 0 5269 xmpp-server.l.google.com. |

Trở thành các thuộc tính bên dưới :

|  |  |
| --- | --- |
| **Service:** \_xmpp-server | Tên dịch vụ |
| **Protocol:** \_tcp | Tên giao thức |
| **Host:** chat | Tên **subdomain** (nếu muốn) hoặc @ cho root |
| **TTL:** 14400 | Time to live |
| **Type:** SRV | Loại |
| **Priority:** 5 | Ưu tiên |
| **Weight:** 0 | Dòng nào sẽ được làm trước |
| **Port:** 5269 | Port |
| **Points To:** xmpp-server.l.google.com | Trỏ tới |

Bảng 1. Bảng phân giải SRV record

## ĐỊNH NGHĨA CỦA BLOCKCHAIN

### 2.3.1. KHÁI NIỆM

Blockchain là công nghệ chuỗi – khối, cho phép truyền tải dữ liệu một cách an toàn dựa trên hệ thống mã hóa vô cùng phức tạp, tương tự như cuốn sổ cái kế toán của một công ty, nơi mà tiền được giám sát chặt chẽ và ghi nhận mọi giao dịch trên mạng ngang hàng.

Mỗi khối (block) đều chứa thông tin về thời gian khởi tạo và được liên kết với khối trước đó, kèm theo đó là một mã thời gian và dữ liệu giao dịch. Dữ liệu khi đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được. Blockchain được thiết kế để chống lại việc gian lận, thay đổi của dữ liệu.

Công nghệ Blockchain là sự kết hợp giữa 3 loại công nghệ :

* **Mật mã học:** để đảm bảo tính minh bạch, toàn vẹn và riêng tư thì công nghệ Blockchain đã sử dụng public key và hàm hash function.
* **Mạng ngang hàng:** Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ bản sao ứng dụng.
* **Lý thuyết trò chơi:** Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (giao thức PoW, PoS,…) và được thúc đẩy bởi động lực kinh tế.

### 2.3.2. LỊCH SỬ RA ĐỜI

Năm 1991, Blockchain đã được mô tả vào bởi W. Scott Stornetta và Stuart Haber. Mục đích là đánh dấu thời gian vào các tài liệu để nó trở nên bất biến. Điều này có nghĩa là không thể sửa đổi ngày với bất cứ hình thức nào.

Năm 2008, nền tài chính thế giới sụp đổ. Thời điểm vàng cho một nhân vật hay một nhóm ẩn danh có tên là Satoshi Nakamoto tạo ra một giao thức mã nguồn mở có tên là Bitcoin.

Cái thú vị nhất không nằm ở giá cả lên hay xuống mà nó chính là công nghệ Blockchain. Lần đầu tiên thế giới được biết đến Blockchain!

### 2.3.3. MỤC ĐÍCH

Ở hiện tại, blockchain có rất nhiều mục đích sử dụng nhưng mục đích chính là giải quyết vấn đề trung gian giữa các giao dịch.

Có ví dụ sau :

A và B chơi trò đoán giờ check-out của C. Mỗi người cược 100.000 VNĐ. Nếu như thời điểm C check dấu vân tay, kim phút rơi vào số chẵn thì A thắng. Ngược lại, kim phút rơi vào số lẻ thì B thắng.

Để quản lý giao dịch, A và B có một số phương án như sau:

1. **Nhờ người thứ ba là D giữ tổng số tiền cược của 2 người**: 200.000 VNĐ. Người thắng sẽ được D trao lại số tiền => Nếu D trở mặt, không muốn trả lại số tiền thì cả A và B đều bị thiệt hại
2. **Chọn cách tin tưởng lẫn nhau** => Dù là đồng nghiệp thân thiết thì vẫn có khả năng người kia không chịu đưa tiền

Rõ ràng là 2 cách trên vẫn gặp phải những rủi ro nhất định. Blockchain ra đời nhằm giải quyết những vấn đề nói trên.

Thông qua một vài dòng lệnh, tiền của cả 2 sẽ được chuyển vào chương trình của Blockchain. Thu thập dữ liệu từ phần mềm chấm công, chương trình này sẽ chuyển tiền cho người chiến thắng.

### 2.3.4. CẤU TRÚC

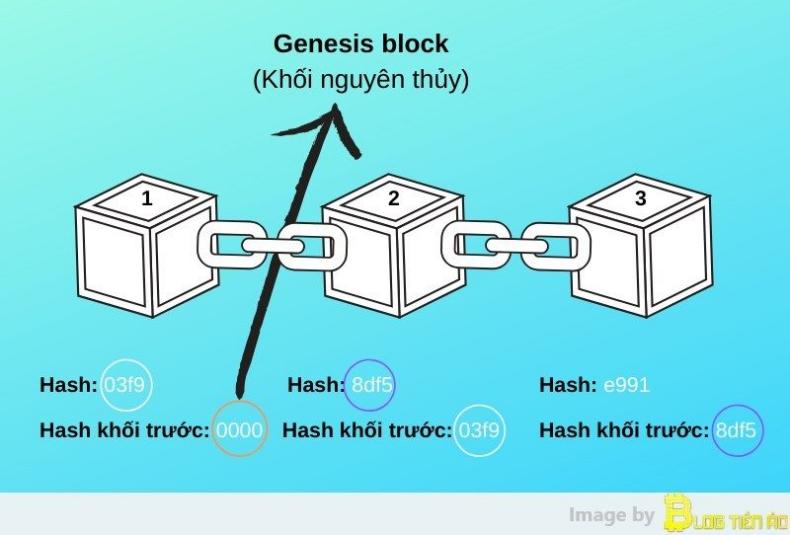
****

Hình 3. Cấu trúc của khối Block

Mỗi khối (block) sẽ được lưu trữ gồm 3 phần:

1. **Dữ liệu:** dữ liệu thông thường
2. **Hash của khối hiện tại:** Hash của khối hiện tại như một đặc điểm để nhận dạng. Nó là duy nhất và không trùng nhau.
3. **Hash khối trước:** Nhờ hash này mà các khối (block) liên kết tạo ra một chuỗi (chain). Tuy nhiên khối đầu tiên sẽ không được liên kết với bất cứ khối nào. Vì nó được tạo ra đầu tiên.

Một blockchain sẽ bao gồm nhiều block kết nối với nhau qua hash khối trước

****

Hình 4. Cấu trúc của Blockchain

### 2.3.5. ĐẶC ĐIỂM

Không thể làm giả, không thể phá hủy các chuỗi Blockchain: theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu. Ngoài ra còn 4 đặc điểm sau :

* **Bất biến:** dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.
* **Bảo mật:** Các thông tin, dữ liệu trong Blockchain được phân tán và an toàn tuyệt đối.
* **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.

### 2.3.6. PHÂN LOẠI

Hệ thống Blockchain chia thành 3 loại chính:



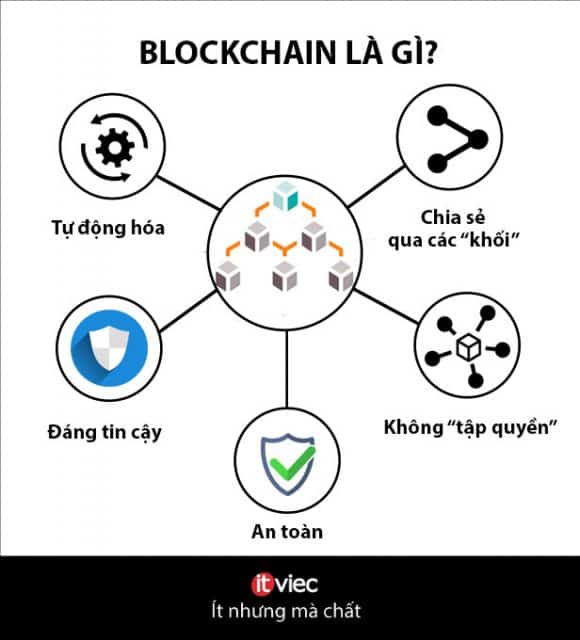
Hình 5. Phân loại blockchain

* **Public:** Bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có rất nhiều nút tham gia. Vì vậy, muốn tấn công được vào hệ thống Blockchain này cần chi phí rất lớn và thực sự không khả thi. Ví dụ: Bitcoin, Ethereum,…
* **Private:** Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.
* **Permissioned (hay còn gọi là Consortium):** một dạng của Private nhưng bổ sung thêm 1 số tính năng khác, đây là sự kết hợp giữa Public và Private. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

### 2.3.7. ƯU ĐIỂM

Ưu điểm của công nghệ Blockchain là đảm bảo tính bảo mật cao, loại bỏ tình trạng đánh cắp hoặc sửa đổi thông tin.

Các ưu điểm khác có thể liệt kê như hình:



Hình 6. Các lợi ích khi sử dụng công nghệ Blockchain

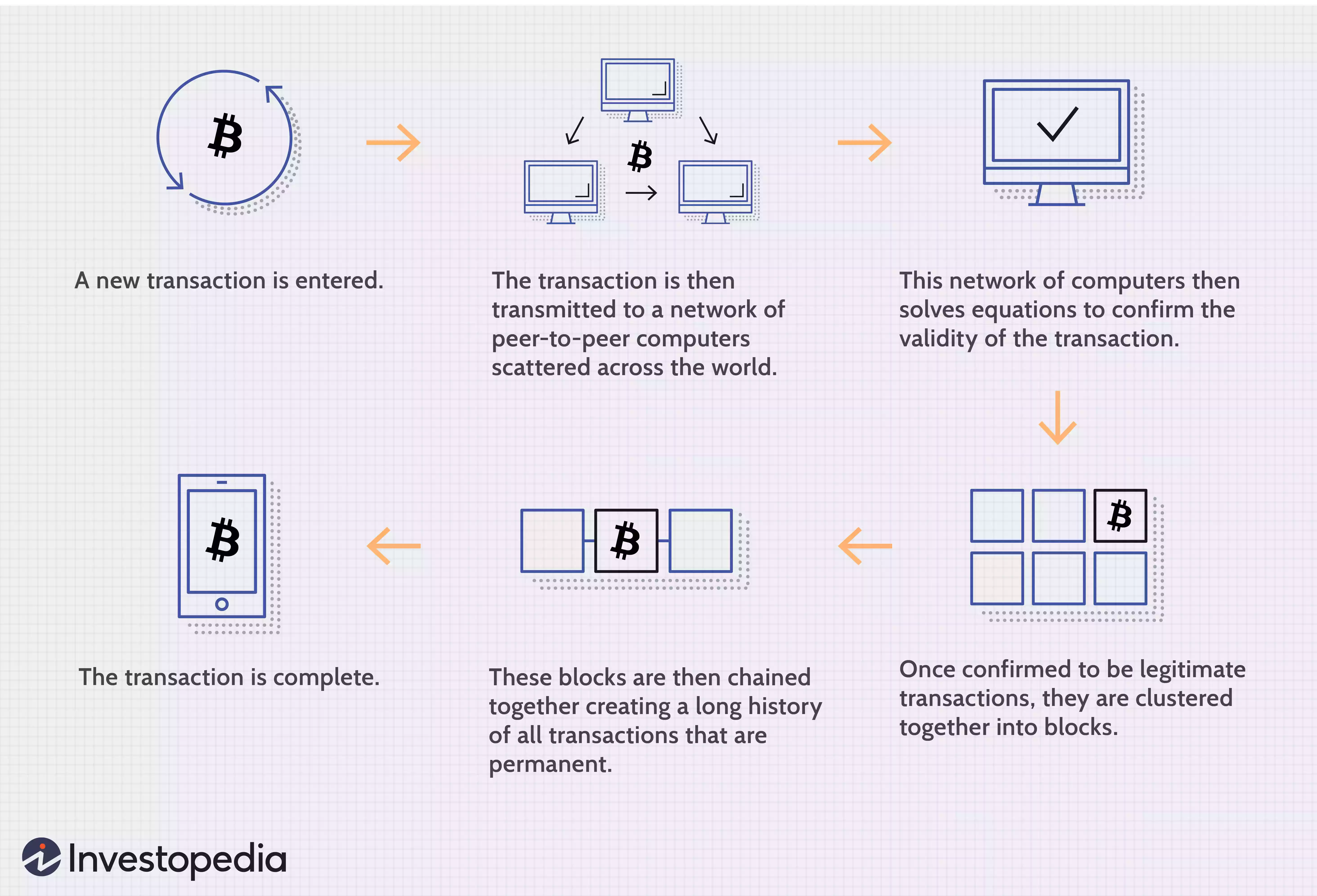
### 2.3.8. NHƯỢC ĐIỂM

Dù các ưu điểm đều mang tính đột phá và giải quyết nhiều vấn đề hiện tại, nhưng Blockchain vẫn chứa những nhược điểm đáng lưu ý :

* **Dễ bị hacker nhắm đến:** dù được bảo vệ bởi thuật toán đồng thuận Proof of Work nhưng các ứng dụng phát triển trên nền tảng Blockchain vẫn là “con mồi” của hơn 50% các cuộc tấn công mạng.
* **Việc sửa đổi dữ liệu cực kỳ khó khăn:** một khi dữ liệu được đưa vào Blockchain thì rất khó để thay đổi. Tính ổn định vừa là lợi thế nhưng cũng đồng thời là nhược điểm của Blockchain.
* **Sự bất tiện của private key – khóa riêng:** mỗi tài khoản Blockchain sẽ được cấp khóa chung (có thể chia sẻ) và khóa riêng (cần giữ bí mật). Người dùng sử dụng khóa riêng để truy cập vào quỹ tiền của mình. Nếu mất khóa riêng, tiền của họ sẽ bị mất mà họ không thể làm gì được.

## CÁCH BLOCKCHAIN HOẠT ĐỘNG VÀ CÁC GIAO THỨC

### KHÁI QUÁT CÁCH BLOCKCHAIN HOẠT ĐỘNG



Hình 7. Qthêm một giao dịch vào blockchain

Ứng dụng thông dụng nhất về công nghệ Blockchain chính là được ứng dụng trong sổ cái kế toán để tính toán số lượng Bitcoin được lữu trữ trong từng tài khoản

- Được phân phối trên toàn thế giới thông qua một mạng lưới các máy tính ngang hàng với vai trò lưu trữ dữ liệu và thực thi các tính toán.

- Mỗi máy tính này đại diện cho một “nút” của mạng lưới Blockchain và mỗi nút đều có một bản sao của tệp sổ cái này.

- Mỗi giao dịch sẽ được lưu trữ trong một block và được thêm vào blockchain sao cho tạo được blockchain dài nhất.

### 2.4.2. CÁC QUY TẮC HOẠT ĐỘNG TRONG BLOCKCHAIN

**Quy tắc để thêm một khối block vào blockchain :**

* **Phải có giao dịch:** nghĩa là phải có hoạt động mua bán, trao đổi diễn ra. Ví dụ: thực hiện mua hàng trên Amazon
* **Giao dịch đó phải được xác minh:** mọi thông tin liên quan đến giao dịch như thời gian, địa điểm, số tiền giao dịch, người tham gia… đều phải được ghi lại. Ví dụ: khi xem tình trạng đơn hàng, sẽ biết được mình đã order những gì, tổng tiền là bao nhiêu, khi nào thì nhận được hàng…
* **Giao dịch đó phải được lưu trữ trong block:** bất cứ lúc nào cũng xem lại được thông tin đơn hàng mà mình đã thực hiện. Chúng được lưu trữ trong mục “Quản lý đơn hàng”.
* **Block đó phải nhận được hash** **(hàm chuyển đổi một giá trị sang giá trị khác):** chỉ khi nhận được hash thì một block mới có thể được thêm vào blockchain.

**Quy tắc sử dụng Public key và Private key trong blockchain:**

Để có thể thực hiện các giao dịch trên Blockchain, cần một phần mềm sẽ cho phép lưu trữ và trao đổi các đồng Bitcoin gọi là ví tiền điện tử. Ví tiền điện tử này sẽ được bảo vệ bằng một phương pháp mã hóa đặc biệt đó là sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key).

Nếu một thông điệp được mã hóa bằng một khóa công khai cụ thể thì chỉ chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp.

Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư, có nghĩa là đang tạo ra một chữ ký điện tử được các máy tính trong mạng lưới Blockchain sử dụng để kiểm tra chủ thể gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và là sự kết hợp của yêu cầu giao dịch và khóa riêng tư.

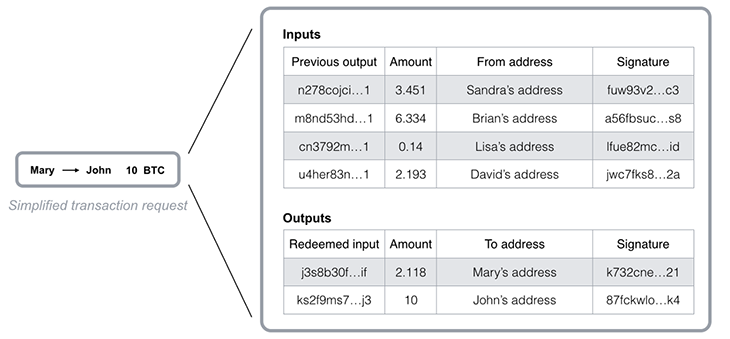
Nếu một ký tự đơn trong thông điệp yêu cầu giao dịch này bị thay đổi thì chữ ký điện tử sẽ thay đổi theo. Vì thế, hacker khó có thể thay đổi yêu cầu giao dịch hoặc thay đổi số lượng Bitcoin mà người dùng đang gửi.

Để gửi dữ liệu nói chung, người dùng cần chứng minh rằng họ sở hữu khóa riêng tư của một chiếc ví điện tử cụ thể để mã hóa thông điệp yêu cầu giao dịch. Sau khi tin nhắn của người dùng đã được gửi đi và được mã hóa thì họ không cần phải tiết lộ khóa riêng tư của họ nữa.

**Quy tắc của sổ cái :**

Mỗi nút trong Blockchain đều đang lưu giữ một bản sao của sổ kế toán. Do vậy, mỗi nút đều biết số dư tài khoản của người dùng đang là bao nhiêu. Với mỗi giao dịch, Hệ thống Blockchain chỉ ghi lại thông tin được giao dịch chứ không hề theo dõi số dư tài khoản.

Để biết số dư trên ví điện tử của mình thì cần xác thực và xác nhận tất cả các giao dịch đã diễn ra trên mạng lưới mà có liên quan tới ví điện tử của người dùng đó.



Hình 8. Cách xác định số dư của tài khoản

Việc xác minh “số dư” này được thực hiện nhờ các tính toán dựa vào liên kết đến các giao dịch trước đó. Ví dụ để gửi 10 BTC cho John, Mary cần tạo yêu cầu giao dịch bao gồm các liên kết đến các giao dịch đã diễn ra trước đó với tổng số dư bằng hoặc vượt quá 10 BTC.

Các liên kết này được xem như là giá trị đầu vào, các nút trong mạng lưới sẽ xác minh xem tổng số tiền của các giao dịch này bằng hoặc vượt quá 10 BTC không. Tất cả điều này được thực hiện tự động trong ví điện tử của Mary và được kiểm tra bởi các nút trên mạng lưới Bitcoin, Mary chỉ gửi một giao dịch 10 bitcoin tới ví của John bằng khóa công khai của John.

Thực tế là các nút sẽ kiểm tra tất cả các giao dịch có liên quan đến ví tiền điện tử người dùng sử dụng trước đó để gửi Bitcoin (BTC) thông qua việc tham chiếu các lịch sử giao dịch. Có một bản ghi sẽ lưu trữ số BTC chưa được dùng và được các nút mạng lưu giữ giúp đơn giản hóa và tăng tốc quá trình xác minh. Vì thế, các ví tiền điện tử tránh được tình trạng chi tiêu đúp giao dịch.

Mã nguồn trên mạng lưới Bitcoin là nguồn mở, có nghĩa là bất kỳ ai có máy tính kết nối được internet đều có thể tham gia vào mạng lưới và thực hiện giao dịch.

Tuy nhiên, nếu có bất kỳ một lỗi nào trong mã nguồn được sử dụng để phát thông báo yêu cầu giao dịch thì các Bitcoin liên quan sẽ bị mất vĩnh viễn.

Điểm trừ duy nhất là không thể khôi phục được 1 giao dịch đã bị mất hoặc quên mật khẩu ví tiền điện tử. Vì đây là mạng phân tán, nên phải lưu trữ mật khẩu hoặc khóa riêng tư của ví cực kì cẩn thận và an toàn.

**Quy tắc của tạo khối:**

Các giao dịch sau khi được gửi lên trên mạng lưới Blockchain sẽ được nhóm vào các khối và các giao dịch trong cùng 1 khối (block) được coi là đã xảy ra cùng thời điểm. Các giao dịch chưa được thực hiện trong 1 khối được coi là chưa được xác nhận.

Để được thêm vào Blockchain, mỗi khối phải chứa một đoạn mã đóng vai trò như một đáp án cho một vấn đề toán học phức tạp được tạo ra bằng hàm mã hóa băm không thể đảo ngược.

Cách duy nhất để giải quyết vấn đề toán học như vậy là đoán các số ngẫu nhiên, những số khi mà kết hợp với nội dung khối trước tạo ra một kết quả đã được hệ thống định nghĩa. Điều này nhiều khi có thể mất khoảng một năm cho một máy tính điển hình với một cấu hình cơ bản có thể đoán đúng các con số đáp án của vấn đề toán học này.

Mạng lưới quy định mỗi khối được tạo ra sau một quãng thời gian là 10 phút một lần, bởi vì trong mạng lưới luôn có một số lượng lớn các máy tính đều tập trung vào việc đoán ra dãy số này. Nút nào giải quyết được vấn đề toán học như vậy sẽ được quyền gắn khối tiếp theo lên trên chuỗi và gửi nó tới toàn bộ mạng lưới.

Trong trường hợp này, cả hai khối được gửi lên mạng lưới và mỗi nút sẽ xây dựng các khối kế tiếp trên khối mà nó nhận được trước tiên. Do xác suất việc xây dựng các block đồng thời là rất thấp nên hầu như không có trường hợp nhiều khối được giải quyết cùng một lúc và nhiều lần tạo ra các khối nối đuôi khác nhau. Do đó, toàn bộ chuỗi-khối sẽ nhanh chóng ổn định và hợp nhất lại khi mà mọi nút đều đồng thuận.

### 2.4.3. THUẬT TOÁN ĐỒNG THUẬN

Các blockchain công cộng (phi tập trung) được xây dựng như là các hệ thống phân tán. Vì không lệ thuộc vào một cơ quan trung ương nên các nút phân tán cần phải đồng thuận về tính hợp lệ của các giao dịch và đây là lúc để các thuật toán đồng thuận thể hiện vai trò. Chúng đảm bảo rằng các quy tắc giao thức đang được tuân theo và đảm bảo rằng tất cả các giao dịch diễn ra một cách đáng tin cậy, nhờ vậy các tài sản mã hoá lưu trữ trên blockchain chỉ có thể được chi tiêu một lần trong một giao dịch.

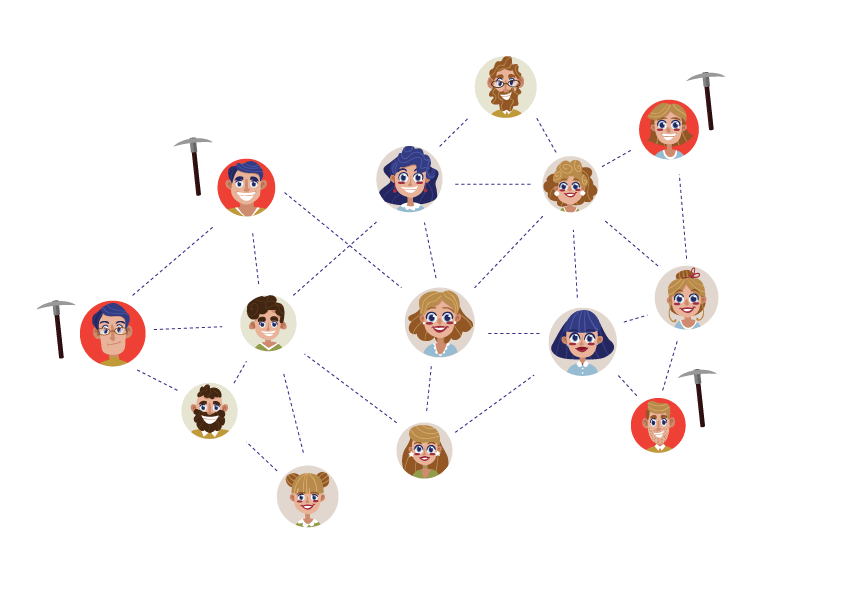
Thông thường đồng thuận (consensus) và giao thức (protocol) là sự bổ trợ cho nhau. Thế nhưng, nghĩa của chúng lại không hoàn toàn giống nhau. Về cơ bản, giao thức (protocol) có thể hiểu là các luật lệ cơ bản của mạng Blockchain. Còn về thuật toán đồng thuận lại được định nghĩa là cơ chế mà các luật lệ giao thức sẽ được tuân theo.

Bên cạnh đó, thuật toán đồng thuận sẽ giúp cho hệ thống được thực hiện theo những bước để đảm bảo làm đúng những luật lệ. Từ đó sẽ đạt được những kết quả mà người tạo lập mong đợi.

*Một ví dụ về Bitcoin và Ethereum xác định sự hợp lệ của các giao dịch và khối:*

* Bitcoin, Ethereum là những giao thức.
* Bằng chứng công việc (PoW) và bằng chứng cổ phần (PoS) là những thuật toán đồng thuận của hai giao thức trên.

**Proof of Work (PoW)** là thuận toán đồng thuận đầu tiên được tạo ra, nó được sử dụng trên Bitcoin và áp dụng nhiều đồng tiền điện tử khác. PoW là một phần thiết yếu không thể thiếu đối với quá trình đào coin.



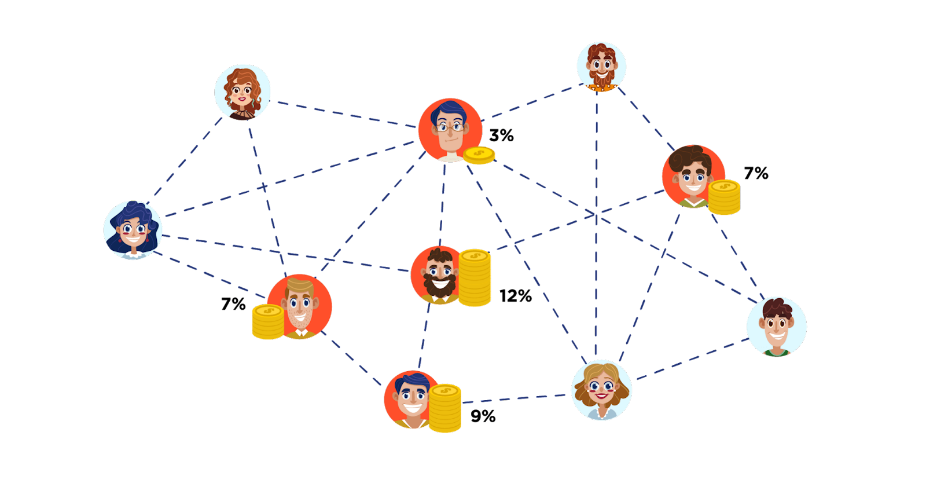
Hình 9. Thuật toán đồng thuận Proof of Work

Proof of Work đòi hỏi những người tham gia thực hiện các công việc chuyên sâu về tính toán nhưng lại có thể được xác minh một cách dễ dàng bởi những người khác trong mạng. Ví dụ như với Bitcoin, “thợ mỏ” cạnh tranh để thêm một bộ giao dịch, được gọi là một block, vào chuỗi blockchain toàn cầu trong mạng lưới. Để làm được điều này, người khai thác mỏ phải là người đầu tiên tìm ra “nonce” một cách chính xác, một chữ số sẽ được nối vào cuối chuỗi để tạo một hash bắt đầu với bằng một số chữ số “0”.

Ưu điểm lớn nhất của Proof of Work đã được chứng minh là khả năng hoạt động được trong một thời gian dài cỡ vào năm – đây là ưu điểm vượt trội hơn hẳn của Proof of Work so với các thuật toán đồng thuận khác.

Về khuyết điểm, Proof of Work tiêu thụ rất nhiều điện năng cho quá trình khai thác mỏ và thông lượng giao dịch thấp.

**Proof of Stake (PoS)** được phát triển vào năm 2011 như là một giải pháp thay thế cho PoW. Mặc dù PoS và PoW có các mục tiêu giống nhau, chúng có một số khác biệt và đặc thù cơ bản, đặc biệt là trong quá trình xác nhận khối mới.



Hình 10. Thuật toán đồng thuận Proof of Stake

Trong thuật toán đồng thuận PoS, các khối được xác nhận theo tỷ lệ cổ phần của những người tham gia. Proof of Stake yêu cầu người tham gia “đặt cọc” một phần những đồng cryptocurrency mà họ nắm giữ trong mạng lưới để xác minh các giao dịch. Thay vì “đào” bằng cách giải quyết những vấn đề khó khăn và phức tạp đòi hỏi chuyên sâu về tính toán để xác minh các giao dịch, người thợ mỏ sẽ đặt cọc tiền vào các giao dịch bằng cách khóa khoản cryptocurrency đó lại. Thợ mỏ thường được lựa chọn dựa trên các tiêu chí như giá trị mà họ đặt vào mạng lưới so với tổng giá trị của mạng lưới hoặc thời gian mà khoản cryptocurrency sẽ bị khóa hoặc tiêu chí khác để đảm bảo rằng người thợ đào phù hợp với lợi ích lâu dài của cả mạng lưới.

Ưu điểm của Proof of Stake là hiệu quả sử dụng năng lượng và khả năng ngăn chặn các cuộc tấn công tốt hơn Proof of Work, tuy nhiên ưu điểm này chưa được chứng minh là thực sự hiệu quả khi sử dụng để thực hiện các dự án lớn.

### 2.4.4. CÁC LÝ DO CHÍNH ẢNH HƯỞNG ĐẾN SỰ SỬA DỮ LIỆU TRÁI PHÉP CỦA BLOCKCHAIN LÀ BẤT KHẢ THI

Những thuật toán trên là một trong những lý do khiến cho việc sửa dữ liệu trái phép trên Blockchain là bất khả thi. Tổng cộng có 3 nguyên nhân chính :

|  |  |  |
| --- | --- | --- |
| **Cơ chế Hash** | **Cơ chế đồng thuận** | **Mạng ngang hàng (P2P Network)** |
| Để sửa được dữ liệu của một khối thì Hash của khối đó sẽ bị thay đổi. Các khối phía sau khối bị sửa trở nên không hợp lệ. Bởi vì lúc này Hash của khối trước không giống với khối bị sửa.  Vậy cách duy nhất để sửa đổi dữ liệu của một khối là phải làm cho tất cả các khối phía sau nó trở nên hợp lệ. | Để làm cho block hợp lệ thì phải can thiệp vào các khối và thay đổi Hash một lúc. Nhưng vì máy tính ngày có thể tính toán rất nhanh.  Mỗi giây, chúng có thể tính toán hàng trăm ngàn Hash. Điều này ảnh hưởng đến độ bảo mật.  Lúc này, nhờ vào cơ chế đồng thuận sẽ quyết định ai là người sẽ thêm block mới. Mục dích để chuỗi không bị ghi đè. Từ đó đảm bảo tính toàn vẹn và bảo mật. | Các blockchain sử dụng kiến trúc mạng ngang hàng thay vì một trung tâm quản lí. Điều này có nghĩa là ai cũng có thể tham gia vào mạng lưới.  Mỗi cá thể trong mạng lưới đóng vai tro như một nút (node). Họ sẽ nhận một bản copy đầy đủ của blockchain. Họ sử dụng bản copy này để xác nhận mọi thứ vẫn theo trình tự.  Tất cả các nút tạo sự đồng thuận. Nếu sự đồng thuận này lớn hơn 50% tức là khối đã hợp lệ và đươc thêm vào chuỗi khối.  Mạng ngang hàng kết hợp cùng sự đồng thuận tạo thành một lớp bảo vê tránh các hoạt động gây hại. |
|
|
|
|
|
|
|
|

Bảng 2. Bảng liệt kê các cơ chế ngăn việc sửa trái phép trên Blockchain

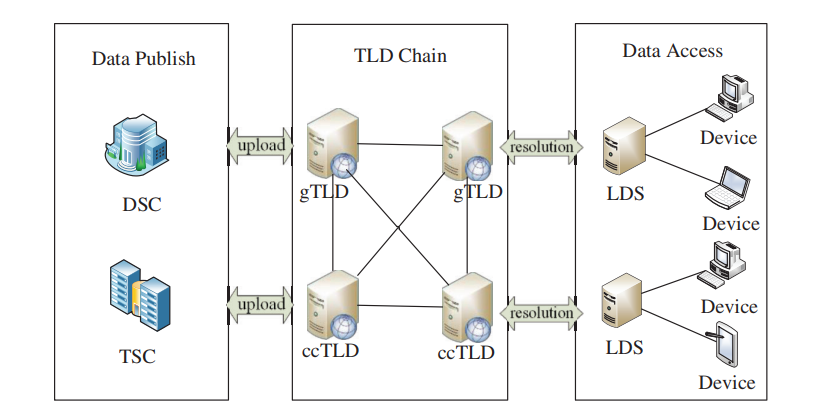
## DANH SÁCH CÁC PHẦN MỀM DNS DỰA TRÊN BLOCKCHAIN HIỆN CÓ

Sắp xếp theo độ thông dụng, có 13 phần mềm trên thị trường:

* **Namecoin**
* Sử dụng tên miền cấp cao nhất .bit.
* Người dùng có thể đăng ký, gia hạn và chuyển miền như DNS truyền thống. Đăng ký thông qua một công ty đăng ký hoặc với một số tên của đồng tiền.
* Người dùng phải cài đặt phần mềm riêng biệt để phân giải tên miền .bit vì .bit chưa được đăng ký chính thức trong hệ thống DNS hiện tại. Có thể giải quyết trường hợp này bằng dùng tiện ích mở rộng trên trình duyệt.
* **Blockstack**
* Loại bỏ các bên thứ ba quản lý hệ thống ID, cơ sở dữ liệu và máy chủ web, kết hợp DNS với Cơ sở hạ tầng khóa công khai (PKI).
* Đăng ký tên và kiểm soát chỉ với tư cách là chủ sở hữu.
* Không có các cuộc tấn công, từ chối dịch vụ DNS, hack hoặc kiểm duyệt các trang web riêng lẻ.
* **Ethereum Name Service**
* Cho phép chủ sở hữu các miền truyền thống có thể chứng minh điều đó bằng đăng ký DNSSEC, chuyển miền đó sang dịch vụ DNS chuỗi khối.
* Đăng ký miền bằng phần mở rộng .eth thông qua quy trình đấu giá.
* Nó kết hợp những ưu điểm của DNS dựa trên blockchain và truyền thống.
* Các phần mở rộng .kred, .xyz và .luxe, .pid.
* Tên miền hàng đầu được bán với giá 3,5 triệu đô la, 300.000 lượt đăng ký, 28 triệu đô la tiền đặt cọc sau 18 tháng
* **Handshake**
* Khi tên được đăng ký, khóa dưới sự kiểm soát của chủ sở hữu có thể ghi các bản ghi theo thứ tự.
* Handshake sử dụng blockchain của riêng nó để phân quyền và sắp xếp các sự kiện.
* **Nebulis**
* Tên miền được lưu trữ, cập nhật và phân giải trên chuỗi khối Ethereum, gây khó khăn cho việc hack các trang web và khởi động các cuộc tấn công man-in-the-middle và tấn công denial of service.
* **Dot BIT**
* Người dùng có thể đăng ký và kiểm soát tên miền của mình theo ý muốn.
* Bitcoin Blockchain đảm bảo rằng tất cả những người tham gia mạng đều có các bản sao dữ liệu DNS giống nhau trên máy của họ, có nghĩa là khó có thể thay đổi dữ liệu DNS một cách bất hợp pháp.
* **Emercoin DNS**
* Hỗ trợ 4 vùng miền với khả năng hỗ trợ bất kỳ vùng nào.
* DNS không dễ bị kiểm duyệt và chặn.
* Hoàn toàn phi tập trung - thông tin không thể bị thay thế hoặc bị chặn.
* Người dùng có thể chỉ định thời gian thuê tên miền lúc đăng ký.
* Người dùng có thể chấm dứt miền bằng cách xóa miền đó khỏi chuỗi khối mà không cần phải đợi hết thời gian thuê.
* **PeerName**
* Cho phép đăng ký tên miền .emc .bazar .lib .coin với chi phí $ 7 cho mỗi tên miền.
* **Blockchain DNS for Firefox**
* Hiện hỗ trợ .emc, .coin, .bazar, .lib và .bi TLD.
* Có thể dễ dàng truy cập các tên miền từ OpenNIC - cơ quan quản lý tên miền do cộng đồng định hướng với bố cục truyền thống hơn, ngoài các mạng Namecoin và Emercoin.
* **FrigGate for Chrome and other browsers**
* Hỗ trợ các trang TOR (.onion) và EmerDNS.
* Mã hóa lưu lượng và định tuyến nó qua các máy chủ VPN.
* Phần mở rộng là một tương tự nâng cao của ZenMate, Hola, Stealthy và Browsec.
* **NEM Blockchain DNS extension**
* Dễ dàng cài đặt trên trình duyệt mà không cần phải tải phần mềm.
* Được xây dựng trên blockchain.
* Mã nguồn mở
* Hồ sơ có thể được cập nhật dễ dàng bởi chủ sở hữu miền.
* Không có khả năng kiểm duyệt.
* **Unstoppable Domains**
* Hoạt động như một tiện ích mở rộng của Chrome. Đăng ký tên miền được quản lý bởi người dùng.
* Có thể chuyển nhượng, có thể tìm kiếm trên Google và các công cụ tìm kiếm khác.
* **Aloaha Blockchain DNS**
* Tên miền không thể được kiểm duyệt.
* Phần mềm là mã nguồn mở.

## CƠ CHẾ HOẠT ĐỘNG CỦA DNS DỰA TRÊN BLOCKCHAIN

Trong DNS phi tập trung, chủ sở hữu của một miền chẳng hạn như “youtube.com” lưu trữ các chữ ký mã hóa của họ trên một blockchain công khai. Điều này cho phép bất kỳ trình duyệt Web, Ứng dụng điện thoại thông minh hoặc thiết bị IoT nào kiểm tra mục nhập blockchain tương ứng và tìm ra chữ ký chính xác. Lược đồ này cho phép chủ sở hữu miền tự quản lý miền của mình và loại bỏ nhu cầu liên hệ với tổ chức trung tâm để nhận chứng chỉ. Hơn nữa, nó không chỉ liên kết mà còn hoàn toàn phân quyền việc cung cấp các yêu cầu DNS, bởi vì mỗi máy chủ blockchain hiện có thể phục vụ dữ liệu DNS.



Hình 11. Sơ đồ cơ chế Blockchain DNS

Một hệ thống Blockchain DNS hoàn chỉnh có 3 phần chính là :

1. Data Publish : Chịu trách nhiệm cho việc upload dữ liệu tên miền và thực thi những yêu cầu với dữ liệu upload.
2. Top Level Domain Chain : Blockchain lưu trữ những dữ liệu tên miền đã được đồng bộ hóa.
3. Data Access : Chịu trách nhiệm nhận yêu cầu và trả kết quả phân giải cho người yêu cầu.

Cơ chế chuẩn bị sẽ như sau:

* Trước khi những cơ quan, chức năng sẽ gửi một bộ dữ liệu tên miền vào hệ thống TLD Chain, toàn bộ dữ liệu đều phải thông qua Data Publish.
* Trong giai đoạn Data Publish, DSC ( Domain Name Service Center ) tiến hành cấp phép cho những TLD chỉ định quyền được thêm bộ dữ liệu này tránh việc lặp lại các tên có sẵn. Dù vậy nhưng DSC không trực tiếp thay đổi bộ dữ liệu.
* Sau đó gửi thông tin cho bộ phận TSC ( TLD Service Centers ), TSC sẽ đợi cho Blockchain được khởi tạo hoàn toàn và các node khởi tạo cho mình một node TLD tương ứng ( như node .com, node .net, node .vn ). Lúc đó TSC sẽ có nhiệm vụ chỉ dẫn những tên miền đã được xác định vào những node trùng khớp. Cuối cùng nếu có chỉ định cần phải sửa hoặc hủy bỏ, TSC sẽ tiến hành thực thi tùy theo trường hợp phát sinh.

Cơ chế tương tác sẽ như sau :

* Sau khi được khởi tạo và đồng bộ dữ liệu, đến với giai đoạn giữa, TLDChain hoặc có thể gọi là Blockchain sẽ chia làm 2 chuyên mục : thông thường và chỉ định theo một lựa chọn nào đó ( ở ví dụ sẽ là quốc gia ) nhờ đó có thể áp dụng phân quyền tạo nên một Permissioned Blockchain ( kết hợp giữa Public và Private )
* Giai đoạn cuối cùng là Data Access, là nơi tiếp nhận thông tin của các người dùng và trực tiếp trả về kết quả thông qua việc xử lý thông tin ở TLDChain.

## ỨNG DỤNG THỰC TIỄN CỦA CÔNG NGHỆ BLOCKCHAIN TRONG CUỘC SỐNG

Một số ngành công nghiệp mà công nghệ Blockchain có thể tác động đến như:

* Công nghệ ô tô Automotive (Automotive)
* Chế tạo (Manufacturing)
* Công nghệ, truyền thông và viễn thông (Tech, media & Telecommunications)
* Dịch vụ tài chính (Financial Services)
* Nghệ thuật & Giải trí (Art & Recreation)
* Chăm sóc sức khỏe (Healthcare)
* Bảo hiểm (Insurance)
* Bán lẻ (Retail)
* Khu vực công (Public Sector)
* Bất động sản (Property)
* Nông nghiệp (Agricultural)
* Khai thác (Mining)
* Vận tải và Logistics (Transport & Logistics)
* Công trình hạ tầng kỹ thuật (Utility)

# CHƯƠNG III : PHÂN TÍCH VÀ XÂY DỰNG

## 3.1. PHÂN TÍCH CÁC YÊU CẦU CỦA ĐỀ TÀI

### 3.1.1. Ý TƯỞNG ĐỀ TÀI

Ý tưởng đề tài xuất phát từ việc các ứng dụng từ hệ thống Blockchain ngày càng nhiều và ngày càng phổ biến trên thị trường số. Bên cạnh đó, ứng dụng quản lý tiền ảo Bitcoin được gọi là ví điện tử với ưu điểm khó thay đổi dữ liệu và có tính bảo mật cao đã được khai thác, nghiên cứu bởi các chuyên gia đầu ngành. Điều này giúp việc tìm kiếm kiến thức về Blockchain dễ tiếp cận hơn với các người tham gia vào Internet.

Liên quan đến Internet, DNS là công nghệ không thể thiếu, giúp người dùng khắp thế giới có thể tiếp cận Internet mà không cần hiểu biết sâu về kĩ thuật hay yêu cầu một kĩ năng thuộc chuyên ngành. Nhưng cơ sở hạ tầng của DNS vẫn chưa bắt kịp được sự phát triển của công nghệ hiện đại vì chưa phù hợp và tốn quá nhiều chi phí, công sức để thay thế. Với sự giúp sức từ Blockchain, mạng phi tập trung, những vấn đề đó đã tương đối được giải quyết. Vì là mạng phi tập trung nên mỗi người dùng tham gia mạng sẽ là người quản lý và người kiểm duyệt khiến cho từng quyết định với các tên miền trên DNS sẽ khách quan hơn. Đó là ưu điểm đáng có nhất với DNS mang công nghệ Blockchain.

Mục đích của đề tài là tạo ra một hệ thống mạng lưới Blockchain DNS có thể tái sử dụng và phát triển theo từng quy mô vừa và lớn. Qua đó có sự so sánh giữa hệ thống mới và cũ, giúp nhà phát triển và quản trị xem xét được tính khả thi khi thay thế hệ thống hiện tại bằng giải pháp Blockchain DNS.

### 3.1.2. ĐỐI TƯỢNG SỬ DỤNG

Đề tài hướng đến các quản trị viên, các nhà phát triển dùng để phục phục cho công việc thay đổi, bảo trì, quản lý và phát triển hệ thống DNS một cách hiệu quả và bảo mật hơn . Từ đó có thể giảm thiểu chi phí, công sức thời gian với hệ thống DNS cũ khi đầu tư vào vấn đề bảo mật.

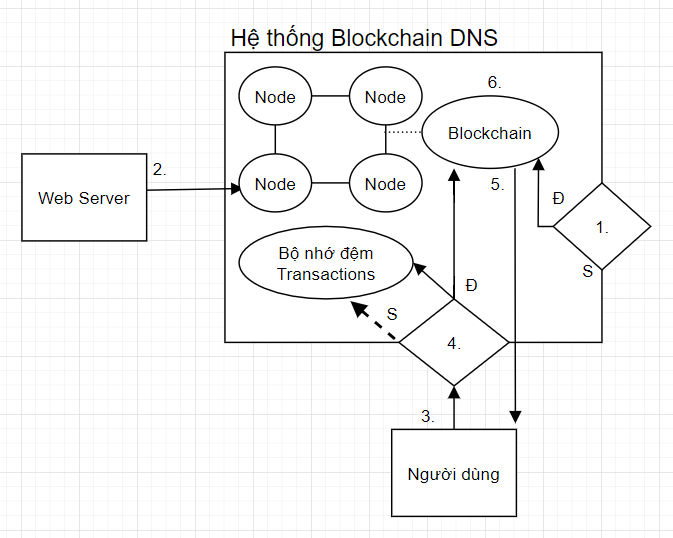
Bên cạnh đó, đề tài còn hướng đến những “thợ mỏ” (Miner) tham gia vào các quá trình xác thực lần giao dịch mới, các block mới. Họ có thể sử dụng chương trình chạy trên chính máy tính của họ để thu thập các phần thưởng từ các lần kiểm duyệt thành công. Trở thành nút mạng và trực tiếp giảm tải cho hệ thống. Từ đó, hệ thống sẽ ngày càng lan rộng và mang tới nhiều cơ hội đạt được phần thưởng từ các giao dịch mới .

### 3.1.3. CÁC CHỨC NĂNG CHÍNH CẦN THIẾT

Với một hệ thống DNS tiêu chuẩn, chức năng quan trọng nhất chính là phân giải tên miền được gửi lên hệ thống thông qua yêu cầu của người dùng. Ngoài ra các còn có các chức năng khác như :

* Đăng kí trở thành một node ( nút mạng ) tham gia vào việc vận hành Blockchain
* Đăng kí các tên miền khác vào bộ dữ liệu của hệ thống
* Quản lý được trạng thái các nút mạng.
* Liệt kê thông tin của các nút mạng.
* Quản lý được sổ cái, bảng dữ liệu chính của chương trình.
* Bảo mật bằng cơ chế xác thực bằng hash của Blockchain, không cho phép chỉnh sửa dữ liệu trái phép.
* Đọc tệp text chứa các bản ghi tên miền có định dạng phù hợp để tải lên hệ thống

### 3.1.4. NGUYÊN LÝ HOẠT ĐỘNG



Hình 12. Sơ đồ nguyên lý hoạt động của Blockchain DNS

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 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.

4. Blockchain DNS kiểm tra điều kiện tạo Block theo 2 trường hợp 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.

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.

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

## 3.2. XÂY DỰNG ĐỀ TÀI

### 3.2.1. XÂY DỰNG ĐỊNH DẠNG LƯU TRỮ CHO DNS RECORD

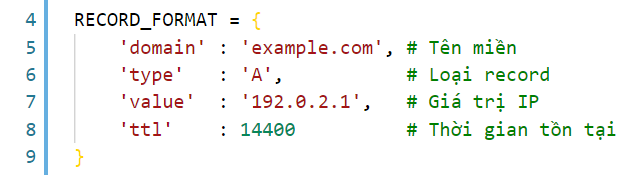
Hiện nay, các record ( bản ghi ) có rất nhiều loại như A, CNAME, MX… Phần lớn các nguồn này đều có chung mục đích là định nghĩa dạng lưu trữ tên miền theo các format ( định dạng ) sẵn có từ đó Server có thể hiểu và sử dụng được. DNS record đã có từ rất lâu và là bước đệm khiến DNS có thể phát triển phong phú và đa dạng theo nhiều nhu cầu khác nhau như hiện nay. Record đã trở thành yếu tố quan trọng cần phải có trong một hệ thống DNS Server. Với các cú pháp đã được định nghĩa sẵn, record thường được tổng hợp thông qua các file text để lưu trữ với số lượng lớn.

Mục đích của đề tài là tạo ra một định dạng chung cho record khi được sử dụng trong hệ thống Blockchain DNS nhằm để thay đổi hạ tầng của hệ thống cũ theo hướng tích cực hơn.

Hiện tại, đề tài có hai cách tạo record là tạo record thông tin mà người dùng nhập vào hoặc có thể tải file .txt chứa các record đã được format phù hợp và record sẽ được sử dụng là loại record A, record được sử dụng thông dụng nhất.

|  |  |  |  |
| --- | --- | --- | --- |
| Tên miền | Loại record | Giá trị | TTL ( Time to live ) |
| example.com | A | 192.0.2.1 | 14400 |

* Định dạng lưu trữ DNS Record : Đối với môi trường Web, kiểu JSON thông dụng nhất để lưu trữ dữ liệu nên record cũng sẽ được lưu theo kiểu JSON.



### 3.2.2. XÂY DỰNG QUY TRÌNH THÊM NODE CHO HỆ THỐNG DNS BLOCKCHAIN

Khi thêm một node vào hệ thống Blockchain, các thông tin như địa chỉ IP và Port sẽ được lưu vào một cơ sở dữ liệu để có thể sử dụng lại lúc sau. Một node sẽ đại diện là một máy tính, một phần của hệ thống giúp xử lí các tác vụ một cách nhanh chóng và minh bạch.

Nhiệm vụ của một node thông thường là tham gia vào quy trình thêm Block trong hệ thống. Đồng thời, người dùng, người quản trị viên có thể tương tác với hệ thống Blockchain thông qua giao diện chạy trên các node.

Các tham số ở các node gồm có :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Id | Nodename | Ip | Port | Is\_deleted | Is\_active |
| VARCHAR(40) | VARCHAR(64) | VARCHAR(16) | INT | BOOLEAN | BOOLEAN |

Bảng 3. Bảng liệt kê các tham số của Node

Ví dụ Node( id = ‘48e809a629154100ad1d61b0a2c30df5’, nodename = ‘This Server’,

ip = ’11.0.0.254’, port = 5000,

is\_deleted = False, is\_active = True, )

Các nodes trong chương trình sẽ được quản lý và chi phối bởi class NodeBusiness. Có những xử lý cho nodes không thể thiếu là:

* Đăng kí thông tin node :

Khi thêm thông tin, id sẽ được tạo ra ngẫu nhiên, ngoài ra các thông tin còn lại sẽ được kiểm tra định dạng trước khi đưa vào Database.

* Cập nhật thông tin :

Cập nhật lại thông tin trong node nếu đã xác thực thành công bao gồm đúng IP và các thông tin còn lại tuân theo định dạng đặt ra.

Ngoài ra, thông tin được cập nhật thường xuyên chính là is\_active.

* Xóa tạm thời thông tin Node :

Giá trị ở cột is\_deleted lúc xóa xong sẽ được cập nhật giá trị True.

Những xử lý này được chia theo nhiều trường hợp, nhất là đăng kí thông tin và cập nhật thông tin node. Thông qua giao tiếp bằng CMD, có các trường hợp cụ thể như sau :

Quy định :

\* : Mọi điều kiện ;

InIP, InPort : IP và port được nhập thông qua CMD;

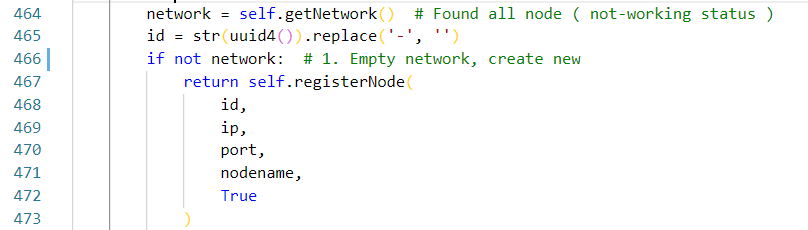
IP, Port, Is\_active : IP, port và is\_active truy xuất từ Database;

!= , == : Khác và giống nhau

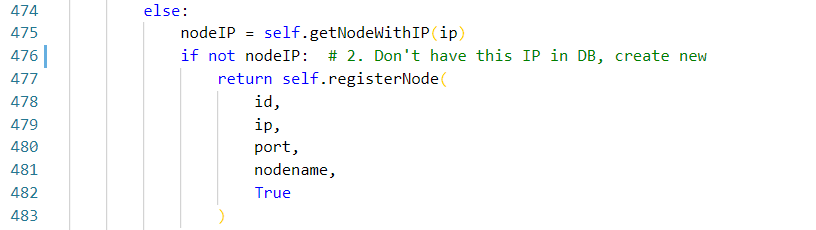
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Stt | Danh sách Node | Điều kiện IP | Điều kiện Port | Điều kiện thêm | Xử lý |
| 1 | Rỗng | \* | \* | \* | Đăng kí Node |
| 2 | Khác rỗng | IP != InIP | \* | \* | Đăng kí Node |
| 3 | Khác rỗng | IP == InIP | Port != InPort | \* | Đăng kí Node |
| 4 | Khác rỗng | IP == InIP | Port == InPort | Is\_active = True | Tìm kiếm node khác có cùng IP mà is\_active = False để cập nhật, nếu không có thì đăng kí Node |
| 5 | Khác rỗng | IP == InIP | Port == InPort | Is\_active = False | Cập nhật is\_active = True |

Bảng 4. Bảng liệt kê các trường hợp khi xử lý thông tin Node

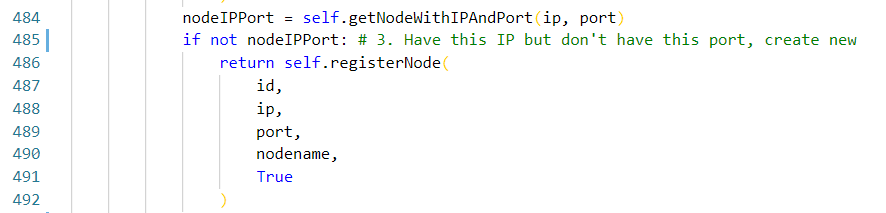
Code xử lý :



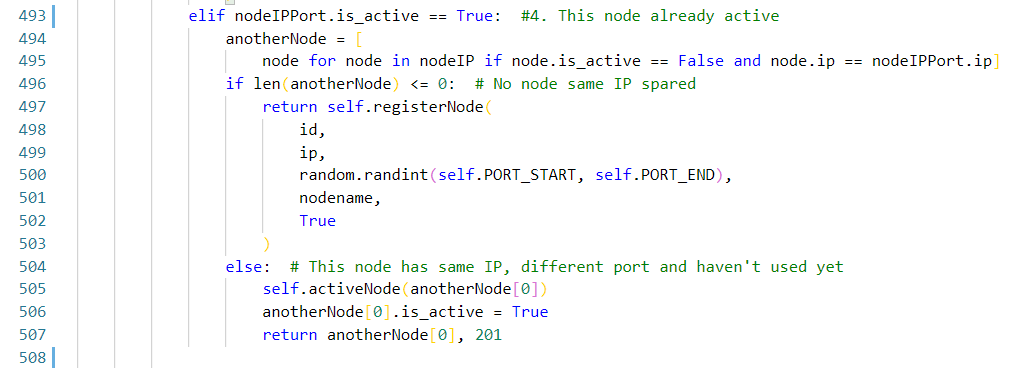
Hình 13. Trường hợp xử lý thông tin node 1



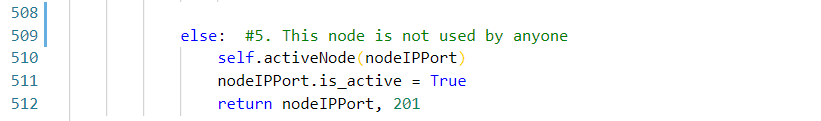
Hình 14. Trường hợp xử lý thông tin node 2



Hình 15. Trường hợp xử lý thông tin node 3



Hình 16. Trường hợp xử lý thông tin node 4



Hình 17. Trường hợp xử lý thông tin node 5

### 3.2.3. XÂY DỰNG QUY TRÌNH THÊM BLOCK CHO HỆ THỐNG DNS BLOCKCHAIN

Một block cụ thể trong hệ thống Blockchain là đại diện cơ sở dữ liệu nắm giữ những giao dịch đã được thực hiện tại một thời điểm nhất định. Số lượng giao dịch cũng là một phần quyết định đến việc tạo ra Block có khả thi hay không.

Với việc dễ sử dụng lại và quản lý các block, Block cũng sẽ lưu trữ vào Database nhưng không hủy hoại tính không thể thay đổi của Block vì khi cưỡng bức thay đổi trên Database sẽ khiến cho hash của Block này sẽ lập tức thay đổi, những Block phía sau sẽ không còn tính nhất quán trong giá trị của previous\_hash nữa.

Cấu trúc của một Block gồm :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Id | Timestamp | Nonce | Transactions | Previous\_hash | Node\_id | Add\_by\_node\_id |
| Int | Double | Int | JSON | VARCHAR(255) | VARCHAR(40) | VARCHAR(40) |

Bảng 5. Bảng liệt kê các thuộc tính của Block

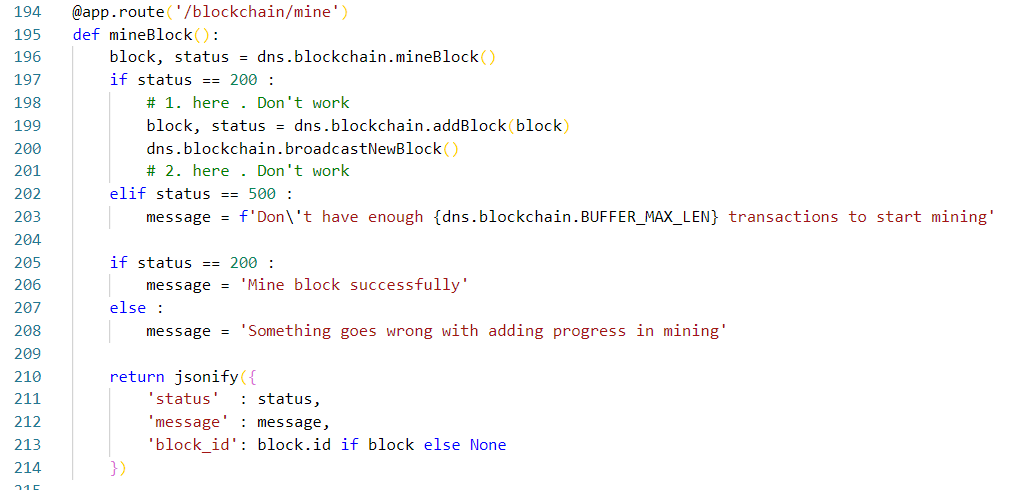
Quy trình thêm Block được chia làm các giai đoạn như sau:

1. Người dùng thêm transactions vào bộ đệm transactions của hệ thống Blockchain DNS thông qua giao diện



Hình 18. Xử lý thêm transactions trong quy trình tạo block

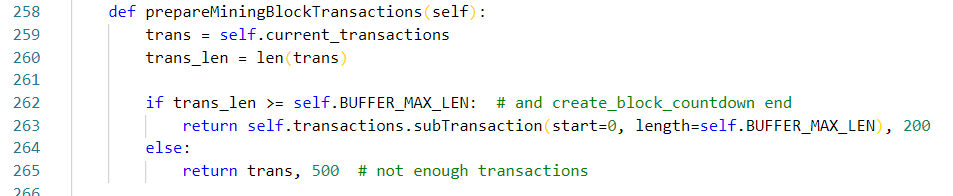
2. Sau đó khi gọi đến yêu cầu mine block,



Hình 19. Xử lý khi tiếp nhận yêu cầu mine Block

Chương trình sẽ kiểm tra điều kiện tạo block nếu có yêu cầu gọi đến và có 3 trường hợp xảy ra, tùy theo tình huống chương trình sẽ có cách xử lý nhất định:

* Trường hợp A: Không đủ số lượng transactions nhất định để tạo Block.
* Chương trình không thực hiện tạo block
* Trường hợp B: Đủ số lượng transactions cần thiết.
* Chương trình tiến hành giai đoạn tiếp theo
* Trưởng hợp C: Vượt quá số lượng transactions cần thiết.
* Chương trình sẽ trích ra số lượng transactions đủ và tiến hành giai đoạn tiếp theo, phần dư sẽ được bộ đệm transactions giữ lại.



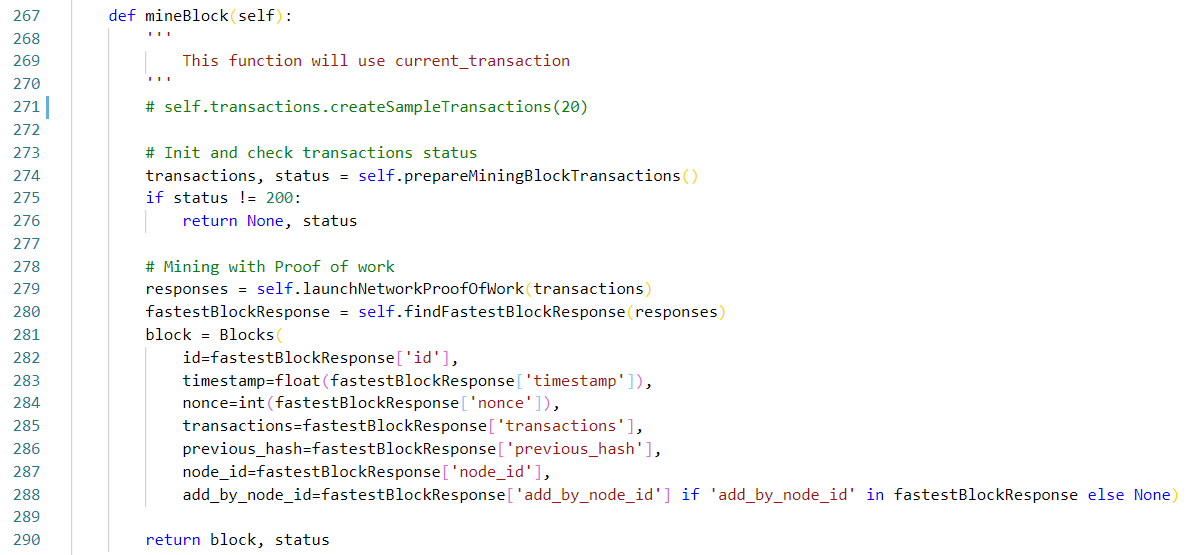
Hình 20. Điều kiện để tạo block

3. Chương trình phát động giao thức đồng thuận Proof of Work cho các node đang hoạt động trong network, tham gia vào quá trình tạo Block.

4. Sau khi các node hoàn tất hoạt động trên từng luồng khác nhau, sẽ gửi kết quả kèm theo thời gian chạy cho node phát động.

5. Chương trình sẽ kiểm tra ai có thời gian nhanh nhất Blockchain sẽ thêm block đã có add\_by\_node\_id bằng node\_id của chính node giải quyết nhanh nhất

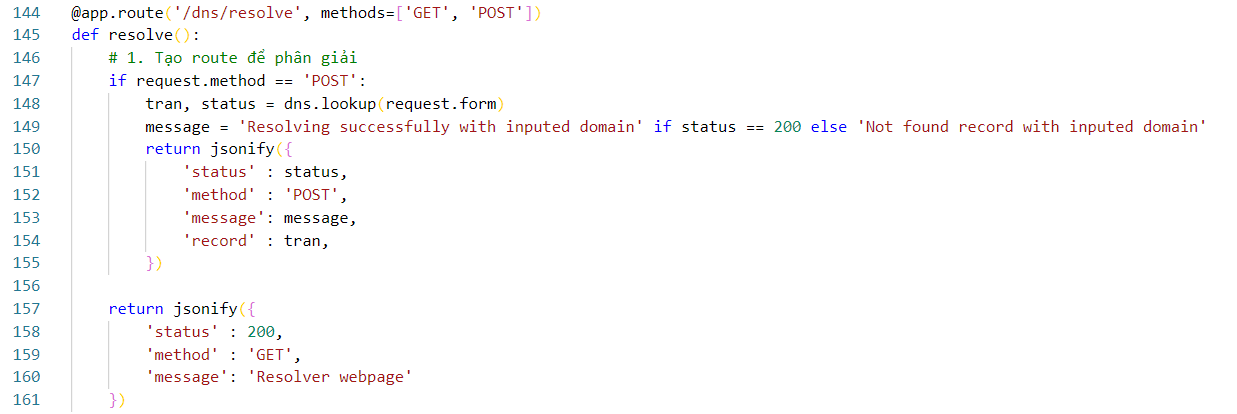
6. Chương trình phát động kết quả cho các node khác và cập nhật Blockchain đã thêm, đồng nghĩa với node dài nhất và đúng nhất.



Hình 21. Xử lý chính khi tạo block

### 3.2.4. XÂY DỰNG QUY TRÌNH PHÂN GIẢI TÊN MIỀN CHO HỆ THỐNG DNS BLOCKCHAIN

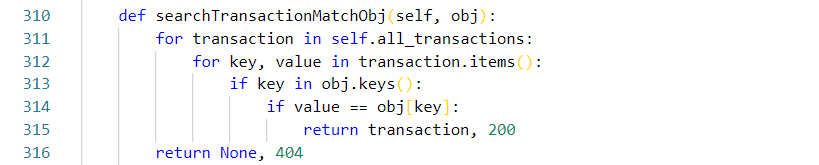
Quy trình phân giải tên miền sẽ bắt đầu khi người dùng gửi yêu cầu thông qua giao diện, chương trình sẽ nhận yêu cầu và xử lý theo các bước sau:



Hình 22. Xử lý khi tiếp nhận yêu cầu phân giải tên miền

1. Chương trình sẽ tổng hợp các transactions đã lưu trữ trong block kết hợp với bộ đệm transactions ( nếu không rỗng ).

2. Tiến hành tìm kiếm tên miền dựa trên danh sách tổng hợp đó và đưa ra kết quả hoặc None nếu không có.



Hình 23. Xử lý tìm kiếm tên miền

# CHƯƠNG IV: THỰC NGHIỆM



## GIỚI THIỆU KỊCH BẢN THỰC NGHIỆM

Kịch bản thử nghiệm bao gồm 3 website chạy song song với nhau :

* Website 1 : Là node của hệ thống Blockchain DNS, quản lý giao diện tương tác với người dùng và tham gia vào các quy trình trong Blockchain
* Website 2 : Là node của hệ thống Blockchain DNS, quản lý giao diện tương tác với người dùng và tham gia vào các quy trình trong Blockchain
* Website 3 : Được quy định bởi Web Server sử dụng Apache để thuận tiện cho việc phân giải tên miền của Blockchain DNS

Người dùng sẽ dùng giao diện của Website 1 và 2 để phân giải tên miền Website 3 và trực tiếp truy cập trong khi Blockchain DNS Server đang chạy.

Người dùng sẽ không truy cập được vào Website 3 khi Blockchain DNS tắt đi.

## XÂY DỰNG KỊCH BẢN THỰC NGHIỆM

## THỰC HÀNH

# CHƯƠNG V: KẾT LUẬN

## 5.1. CÁC KẾT QUẢ ĐẠT ĐƯỢC

## 5.2. ĐÁNH GIÁ

## 5.3. MỞ RỘNG ĐỀ TÀI

# TÀI LIỆU THAM KHẢO

## TIẾNG VIỆT

1. Blog Tiền Ảo, 28/06/2020, Công nghệ Blockchain là gì? [Tất tần tật kiến thức bạn cần biết], https://blogtienao.com/blockchain-la-gi/. Truy cập vào ngày 01/10/2021.
2. Bùi Thị Thuỳ Dung, 02/03/2021, Các ứng dụng thực tiễn của blockchain trong đời sống hiện nay, https://www.thegioididong.com/game-app/cac-ung-dung-cua-blockchain-trong-cuoc-song-hien-nay-1331843. Truy cập vào ngày 01/10/2021.
3. Đỗ Phong, 12/12/2017, Công nghệ Blockchain là gì?, https://vneconomy.vn/cong-nghe-blockchain-la-gi.htm. Truy cập vào ngày 01/10/2021.
4. Thanh Tâm, 03/03/2018, Chặng đường khai phá Blockchain, https://nhandan.vn/baothoinay-hosotulieu/chang-duong-khai-pha-blockchain-317776 . Truy cập vào ngày 01/10/2021.
5. Thu Nhung, 02/03/2021, Domain Name System là gì? Cách thức hoạt động của DNS, https://kinhtedothi.vn/domain-name-system-la-gi-cach-thuc-hoat-dong-cua-dns-402666.html. Truy cập vào ngày 01/10/2021.
6. Trần Nhựt Quang, năm 2019, Blockchain là gì? Hoạt động của Blockchain như thế nào? Ứng dụng ra sao?, https://www.dienmayxanh.com/kinh-nghiem-hay/blockchain-la-gi-hoat-dong-cua-blockchain-nhu-the-1171145. Truy cập vào ngày 01/10/2021.
7. Trang công nghệ, 12/07/2018, Liệu công nghệ Blockchain có thể thay thế DNS để mở ra kỹ nguyên mới cho Internet không?, https://vn.trangcongnghe.com/tin-tuc-cong-nghe/tien-dien-tu/135237-lieu-cong-nghe-blockchain-co-the-thay-the-dns-de-mo-ra-ky-nguyen-moi-cho-internet-khong-.html . Truy cập vào ngày 01/10/2021.

## TIẾNG ANH

1. Ameer Rosic, 04/05/2020, What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain], https://blockgeeks.com/guides/what-is-hashing/. Truy cập vào ngày 03/10/2021.
2. Aniya Erika, 17/06/2021, A Complete Guide Of Blockchain-Based DNS Platform EXIP - The Best Dns Solution With Amazing Advantages, https://www.linkedin.com/pulse/complete-guide-blockchain-based-dns-platform-exip-best-aniya-erika. Truy cập vào ngày 03/10/2021.
3. Maryanne Murray, 15/06/2018, A reuters visual guide Blockchain explained, http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html. Truy cập vào ngày 03/10/2021.
4. Paul Dughi, 04/02/2018, A simple explanation of how blockchain works, https://medium.com/the-mission/a-simple-explanation-on-how-blockchain-works-e52f75da6e9a. Truy cập vào ngày 03/10/2021.

## DANH MỤC CÁC WEBSITE THAM KHẢO

1. Github code: https://github.com/
2. Google search engine: http://www.google.com
3. Stackoverflow Community: https://stackoverflow.com/
4. Wikipedia, Open Dictionary: http://www.wikipedia.org