Câu hỏi

Bản ghi A là viết tắt của Address ( địa chỉ )

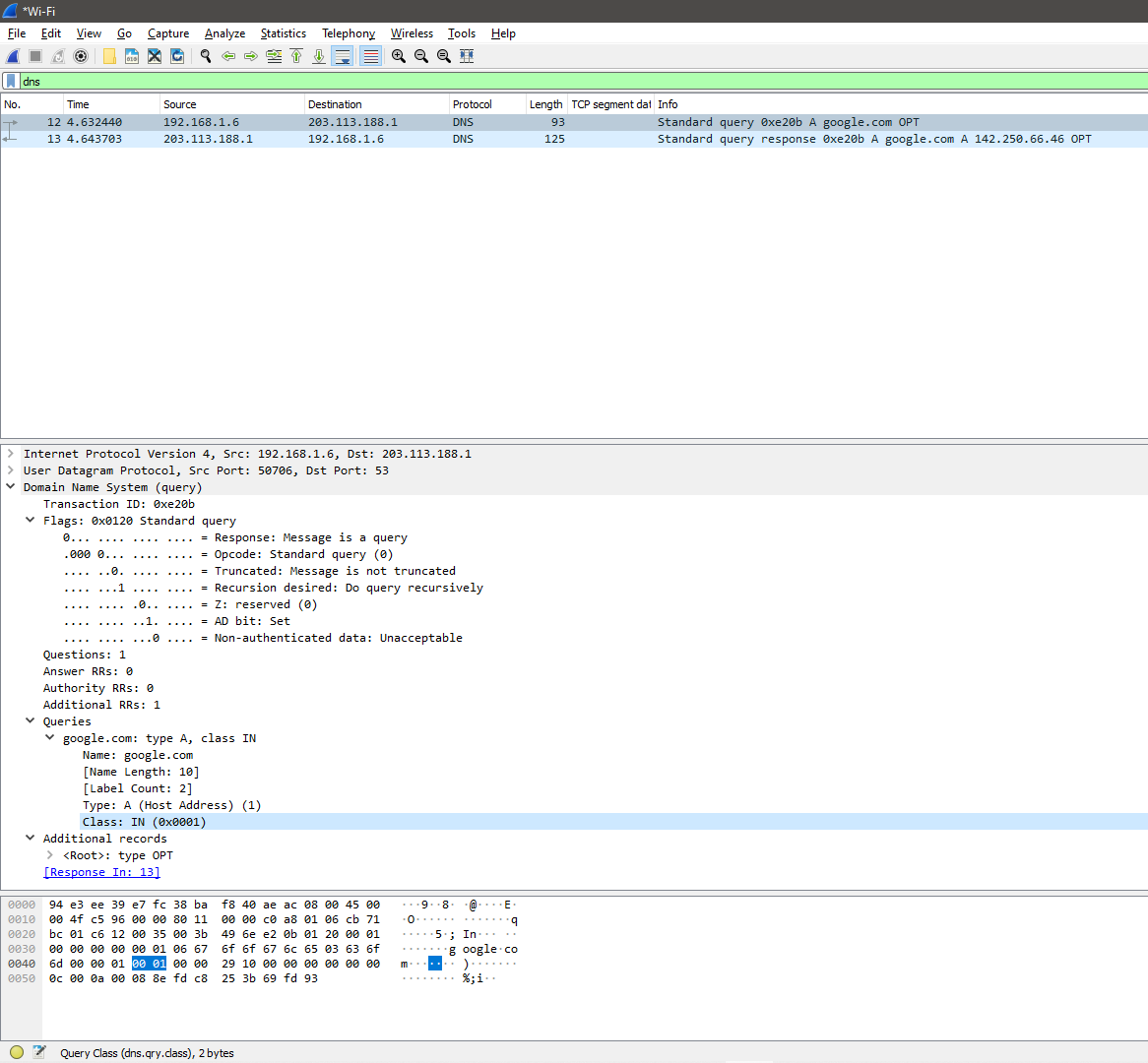
Bản ghi A là loại bản ghi DNS đơn giản nhất và là một trong những bản ghi chính được sử dụng trong máy chủ DNS, khác với record AAAA dành cho IPv6, A hoàn toàn dành cho IPv4 và có thể phối hợp tốt với các record khác như NS, SOA.

Vì phần lớn vẫn được cấu hình ở dạng IPv4 nên A record có vai trò quan trọng trong hệ thống DNS này.

* A truy xuất nhanh, gọn, nhẹ và dễ kết hợp với các bản ghi khác để tạo DNS record hoàn chỉnh.

Ngoài ra, nhiều tên có thể trỏ đến cùng một địa chỉ, trong trường hợp đó, mỗi tên sẽ có bản ghi A riêng trỏ đến cùng một địa chỉ IP đó.

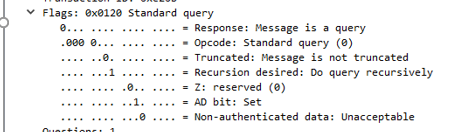
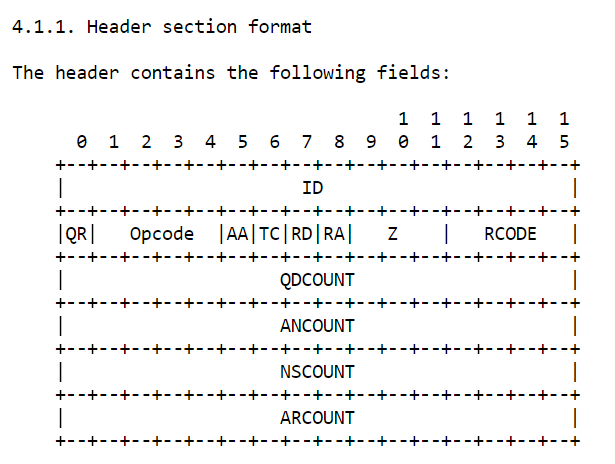
# Tại sao dns phải lập trình record như vậy ?



Hình trên là một standard format cho DNS queries có thể thấy khi dùng lệnh dig google.com trong command line

Hình dưới là format cho Header của DNS khi request tới hệ thống DNS resolver.

Các số hiển thị ở cột ngang đầu tiên thể hiện số bit.



Gồm 6 field:

ID : 16 bit, dùng để chứng minh kết quả trả về sau này sẽ được hệ thống DNS lúc nhận trả kết quả về.

Flags :

QR: 1bit , 0 là query, 1 là response

Opcode: 4 bit thể hiện loại của query ( 0 là standard query – đề tài dùng )

AA ( Authoritative Answer ): 1 bit thể hiện sự xác thực của DNS server, khẳng định đó là DNS server chứ không phải một bên thứ ba nào khác.

TC ( TrunCation ) : 1 bit bật sẽ cắt bớt độ dài khi nó trở nên quá dài hơn mức độ dài quy định là 512 bit.

RD và RA đều 1 bit , mặc định là 0

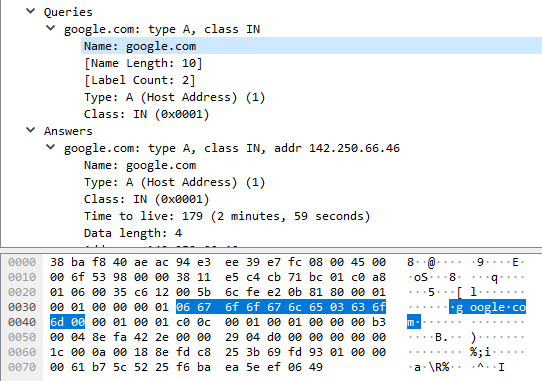
Phần còn lại sẽ null

QDCOUNT ( Question Count ) : 16 bit, dùng để đếm số câu hỏi trong DNS query và luôn có giá trị là 1.

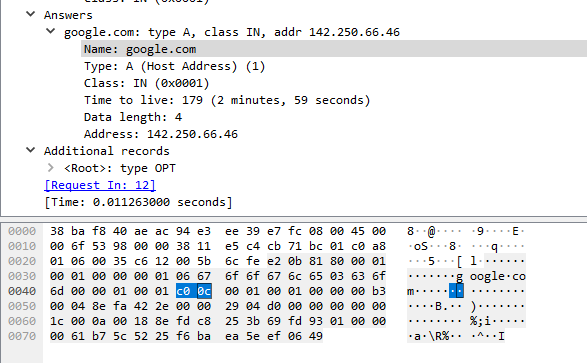
ANCOUNT ( Answer Count ) : 16 bit, đếm số lượng câu trả lời cho DNS query, tùy thuộc theo hệ thống phân giải mà sẽ có số lượng khác nhau.

NSCOUNT ( Namespace ... ) và ARCOUNT ( Additional record ... ) sẽ không sử dụng nên null.

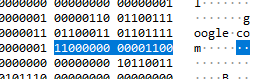
Ta đã có được Header, giờ sẽ đến với phần response, ta sẽ đến khái niệm Compresion, khi google.com được phân giải thành HEX trên bảng HEX của Wireshark sẽ có 12 byte quy định tên ‘google.com’.



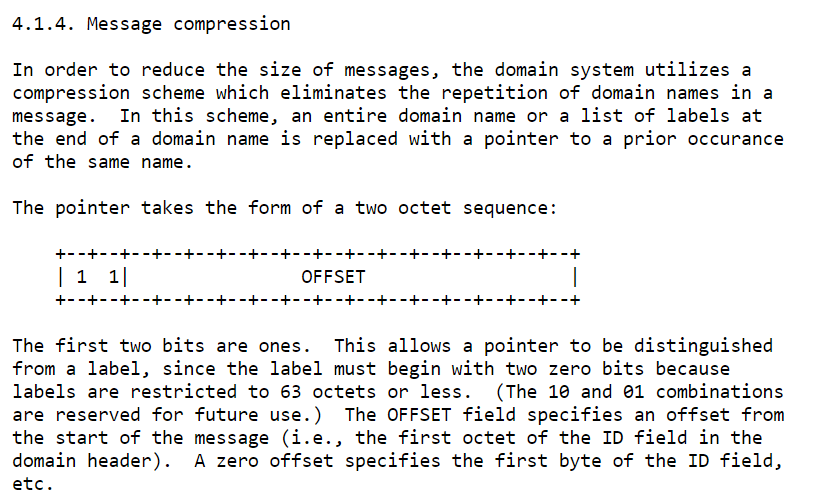
Nhưng khi xuống dưới Answers này thì còn lại 2 byte, và



Xem dưới dạng bit nó sẽ là



Theo công thức dưới hai bit 11 ở đầu là hằng số, phần vị trí phía sau dùng để quy định khoảng cách từ đầu query đến vị trí đó sẽ tìm thấy được tên ‘google.com’. Hay còn nói là khi gặp các byte này, pointer sẽ quay về đầu của query ( đoạn ID ) và nhảy 1 khoảng bằng offset để lấy giá trị tại vị trí đó.



# Các node kết nối với nhau trong mạng như thế nào ?

Có tồn tại danh sách các node trong hệ thống Blockchain mỗi khi một máy tính download chương trình và đăng kí node với hệ thống, điều này sẽ được lưu lại và phân phối cho các node khác để cập nhật và danh sách này sẽ được lưu trong bộ nhớ để tái kết nối khi node hiện tại có sự số.

<https://www.quora.com/In-a-blockchain-network-how-do-new-nodes-know-the-IP-addresses-of-other-nodes-to-connect-to>

# Nếu Internet tắt thì còn Blockchain không ?

Khi Internet tắt đi hoặc mỗi node trong mạng đều bị tắt đồng loạt thì

* Dữ liệu blockchain sẽ được lưu trữ ở mỗi máy ( node ) vì được copy từ blockchain chính.
* Nhưng những mạng đó không thể liên lạc với nhau hay thực thi được tác vụ và dịch vụ nào.
* Giao dịch nếu không may chưa được thêm vào node nhưng mà vẫn còn ở bộ đệm transaction sẽ tùy theo hệ thống đó có lưu trữ vào bộ nhớ phần cứng trước khi mất kết nối hay không ? Nếu có, giao dịch vẫn được lấy lại và gửi lên hệ thống để thực thi như bình thường.
* Mỗi máy tính nếu được bật hoặc có Internet vẫn có thể tìm thấy được nhau và tìm ra nhau, tái kết nối và thực thi giao dịch như bình thường cho dù có node tạo node phát sinh, cũng có hàm để giải quyết chênh lệch và đồng bộ blockchain

<https://bitcoin.stackexchange.com/questions/91093/can-we-shutdown-the-bitcoin-blockchain>

# Tại sao không ghép chung hệ thống DNS và hệ thống blockchain ?

Vì hệ thống Blockchain + UI phải hoạt động liên tục để tiếp nhận yêu cầu từ người dùng và việc thực thi tạo node, account, transaction hay block không được dừng lại.

Hệ thống DNS thì giống phần lớn với hệ thống Blockchain nhưng chỉ khác là DNS sẽ lắng nghe gói tin ở cổng giao tiếp 53 và đợi cho đến khi có gói tin được gửi đến thì mới phân giải và trả kết quả về.

Khi thử kết hợp 2 hệ thống lại với nhau, hệ thống Blockchain sau khi phát động hệ thống DNS như hệ thống con sẽ khiến cho Blockchain dừng hoạt động tạm thời đến khi DNS có được gói tin từ cổng 53.

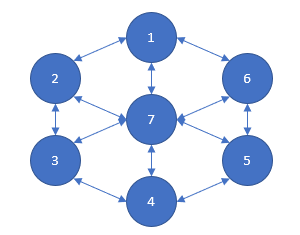
Điều này đi ngược với mô hình thiết kế và hạn chế xử lý của cả 2 hệ thống, hệ thống Blockchain dừng và hệ thống DNS sẽ không có dữ liệu tên miền được gửi qua.

# Masternode và node khác nhau gì ? Phi tập trung sao lại có masternode ?

**Node là gì?**

Một chuỗi khối tồn tại là từ các khối dữ liệu, các khối dữ liệu này được lưu trữ trên các node. Các node có thể là bất kỳ loại thiết bị nào nhưng chủ yếu là máy tính, máy tính xách tay hoặc thậm chí là máy chủ lớn hơn. Các node tạo thành cơ sở hạ tầng của một blockchain.

Tất cả các node trên một chuỗi khối được kết nối với nhau và chúng liên tục trao đổi dữ liệu chuỗi khối mới nhất với nhau, để tất cả các node luôn được cập nhật. Họ lưu trữ, truyền tải và bảo quản dữ liệu blockchain, vì vậy về mặt lý thuyết một blockchain sẽ tồn tại trên các node. Một node đầy đủ về cơ bản là một thiết bị (giống như một máy tính) có chứa một bản sao đầy đủ lịch sử giao dịch của chuỗi khối.



7 node (máy chủ/máy tính), tất cả được kết nối với nhau, chạy một chuỗi khối giống nhau.

**Sự khác biệt giữa một miner và một node**

Miner (thợ đào) luôn cần chạy một node đầy đủ để chọn các giao dịch hợp lệ và tạo thành một khối mới. Nếu không có node đầy đủ, nó không thể xác định giao dịch được đề xuất nào là hợp lệ theo lịch sử giao dịch của blockchain hiện tại, vì nó không có quyền truy cập vào lịch sử blockchain đầy đủ.

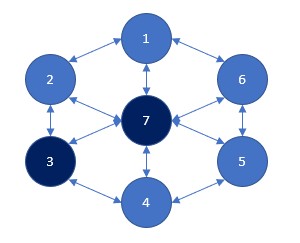
Do đó, một miner cũng luôn là một node đầy đủ. Tuy nhiên, một node không nhất thiết phải đồng thời là một miner. Một thiết bị có thể chạy một node đầy đủ bằng cách nhận, lưu trữ và truyền tất cả dữ liệu giao dịch giống như một máy chủ mà không cần tạo ra các khối giao dịch mới.

Như vậy một nodes đầy đủ trong blockchain là bản sao đầy đủ lịch sử giao dịch blockchain trên bất kỳ thiết bị nào.

**Masternodes là gì?**

Và cuối cùng, một số blockchains cũng có các masternode. Masternode thường được trang bị nặng hơn các node bình thường. Bên cạnh việc xác thực, lưu và truyền tải các giao dịch, các masternode đôi khi cũng tạo điều kiện cho các sự kiện khác trên blockchain phụ thuộc vào bản chất của chúng, chẳng hạn như điều chỉnh các sự kiện bỏ phiếu, cung cấp thực thi các hoạt động giao thức và thực thi luật của blockchain theo đó.

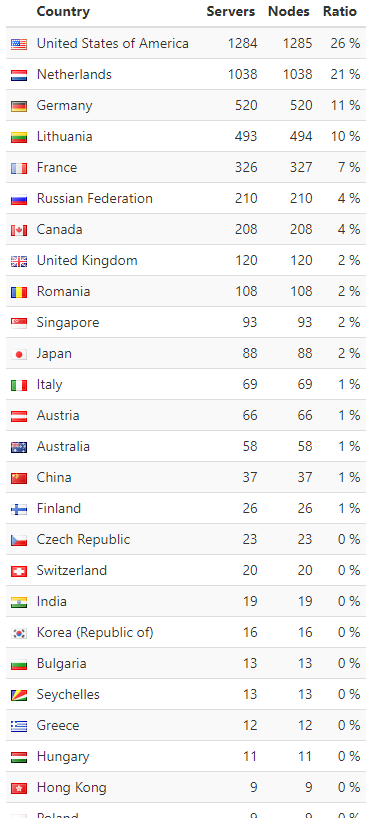
Các masternode thường luôn trực tuyến (24/7) và tạo điều kiện cho bộ nhớ nhiều hơn các node bình thường. Bạn có thể hiểu một masternode giống như lưu trữ một máy chủ rất lớn trên mạng. Bởi vì việc lưu trữ một masternode thường đòi hỏi nhiều tài nguyên hơn (điện, thời gian hoạt động, bảo trì, không gian lưu trữ, bộ nhớ), nên việc lưu trữ một masternode thường cung cấp khoản thanh toán dưới dạng lãi suất.



7 node, 5 node bình thường và 2 ‘masternode’, các masternode nặng hơn và có thể có thêm sức mạnh trên blockchain.

**Ai có thể chạy một masternode?**

Không phải ai cũng có thể chạy một masternode. Bởi vì quyền kiểm soát masternode có thể bị lạm dụng và do đó nó yêu cầu máy chủ lưu trữ phải ký quỹ một lượng tiền điện tử tối thiểu (thường là khá lớn) làm tài sản thế chấp. Tài sản thế chấp này sẽ được dùng khi máy chủ masternode vi phạm các quy tắc của blockchain. Lãi suất mà một máy chủ masternode nhận được được tính trên khoản tiền gửi thế chấp của họ.

[](data:image/svg+xml,%3csvg%20xmlns=)

# Hiểu gì về SHA 256 ? Tại sao SHA 512 không được sử dụng ?

SHA (Secure Hash Algorithm hay thuật giải băm an toàn) là năm thuật giải được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao.

Thuật giải SHA là thuật giải băm mật được phát triển bởi cục an ninh quốc gia Mỹ (National Security Agency hay NSA) và được xuất bản thành chuẩn của chính phủ Mỹ bởi viện công nghệ và chuẩn quốc gia Mỹ (National Institute of Standards and Technology hay NIST)

Năm thuật giải SHA chuẩn là SHA-1 (trả lại kết quả dài 160 bit), SHA-224 (trả lại kết quả dài 224 bit), SHA-256 (trả lại kết quả dài 256 bit), SHA-384 (trả lại kết quả dài 384 bit), và SHA-512 (trả lại kết quả dài 512 bit).

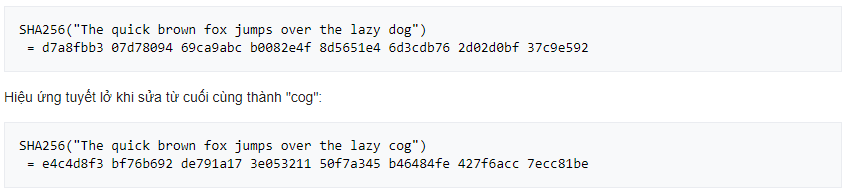
Những thuật giải này được gọi là "an toàn" vì theo chuẩn FIPS 180-2 phát hành ngày 1 tháng 8 năm 2002:

"1) Cho một giá trị băm nhất định được tạo nên bởi một trong những thuật giải SHA, việc tìm lại được đoạn dữ liệu gốc là không khả thi. Hay còn được gọi là mã một chiều,

2) Việc tìm được hai đoạn dữ liệu khác nhau có cùng kết quả băm tạo ra bởi một trong những thuật giải SHA là không khả thi.

3) Bất cứ thay đổi nào trên đoạn dữ liệu gốc, dù nhỏ, cũng sẽ tạo nên một giá trị băm hoàn toàn khác với xác suất rất cao."

Ví dụ mã SHA-256 của một thông điệp:



Vậy BruteForce 2256 khó đến thế nào?

2256 = 115792 089237316 195423570 985008687 907853269 984665640 564039457 584007913 129639936 > 1078

Giả định mỗi máy tính cá nhân có tốc độ 4Ghz có thể xử lý 1.4G phép tính băm mỗi giây, 1.4x109hash/s, Trái Đất có 7 tỷ người mỗi người có một máy tính như vậy, sức mạnh tính toán của toàn thể Trái Đất là: 1019hash/s

Trong giản Ngân Hà (Milkyway) có khoảng 100 tỷ ngôi sao, giả định rằng 1% trong số đó có nền văn minh như Trái Đất thì sức mạnh tính hash của Ngân Hà là: 1019hash/s x 1% x 100x109 = 1028hash/s

Vũ trụ khả kiến được cho là có 100 tỷ thiên hà, và vũ trụ toàn thể được cho là lớn gấp 10 lần như vậy, thì sức mạnh tính hash của vũ trụ toàn thể là: 1028hash/s x 100x109 x 10 = 1042hash/s

Với tốc độ tính toán này, để kiểm tra toàn bộ 1078 trường hợp, vũ trụ toàn thể cần đến 1036 giây ≈ 3.17x1028 năm, hay ≈ 2.4x1018 lần tuổi của chính vũ trụ, tức là việc này không khả thi.

Chính vì vậy SHA-256 được cho là rất an toàn.

Việc dùng đến SHA 512 là vượt quá khả năng tính toán của một máy tính thông thường mà hệ thống không chỉ làm 1 SHA không mà có rất nhiều SHA

https://vncoder.vn/online-tool/sha256-hash-5

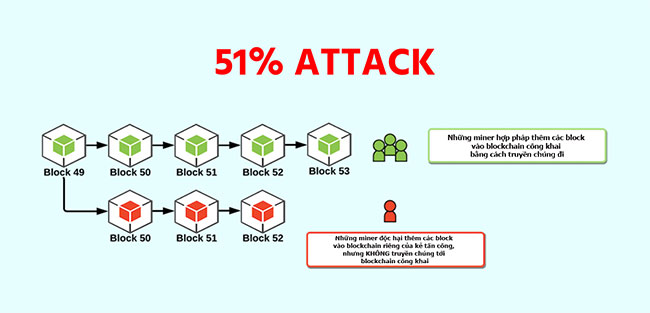
# Tấn công 51% là gì ?

Tấn công 51% (51% Attack) đề cập đến một cuộc tấn công tiềm năng vào tính toàn vẹn của hệ thống blockchain, trong đó một tác nhân hoặc tổ chức độc hại duy nhất tìm mọi cách để kiểm soát hơn một nửa tổng sức mạnh hash của mạng, có khả năng gây gián đoạn mạng.

Nếu một người dùng xấu hoặc một nhóm người dùng xấu cùng hành động, kiểm soát hơn 50% tổng tỷ lệ hash của mạng trong một blockchain, chúng có thể ghi đè cơ chế đồng thuận (consensus mechanism) của mạng và thực hiện các hành vi độc hại. Kẻ tấn công sẽ có đủ sức mạnh khai thác để cố ý sửa đổi thứ tự của các giao dịch, ngăn một số hoặc tất cả các giao dịch được xác nhận (hay còn gọi là transaction denial of service - từ chối dịch vụ giao dịch). Hắn ta cũng có thể ngăn một số hoặc tất cả các miner (những node tham gia hệ thống blockchain) khác khai thác, dẫn đến thứ gọi là độc quyền khai thác.

Ví dụ, nếu một kẻ xấu chiếm 51% sức mạnh hash của mạng Bitcoin, hắn có thể thực hiện giao dịch OTC ngoại tuyến bằng cách gửi một số Bitcoin vào ví tiền điện tử để đổi lấy USD. Do đó, ngay sau khi giao dịch được xác nhận bởi các node mạng, buyer (bot giao dịch tiền điện tử) sẽ ngây thơ giao USD cho kẻ lừa đảo.

Sau đó, tác nhân độc hại có thể quay trở lại blockchain trước khi việc chuyển BTC được xác nhận và khai thác một chuỗi thay thế, trong đó việc chuyển BTC không được bao gồm. Phần lớn sức mạnh mạng sẽ đảm bảo rằng điều này buộc phải được phần còn lại của mạng chấp nhận như một giao dịch hợp lệ.



https://quantrimang.com/51-attack-la-gi-180744#:~:text=T%E1%BA%A5n%20c%C3%B4ng%2051%25%20(51%25%20Attack)%20%C4%91%E1%BB%81%20c%E1%BA%ADp%20%C4%91%E1%BA%BFn,n%C4%83ng%20g%C3%A2y%20gi%C3%A1n%20%C4%91o%E1%BA%A1n%20m%E1%BA%A1ng.