# **I. PROOF OF WORK**

## ****1. Proof of work là gì?****

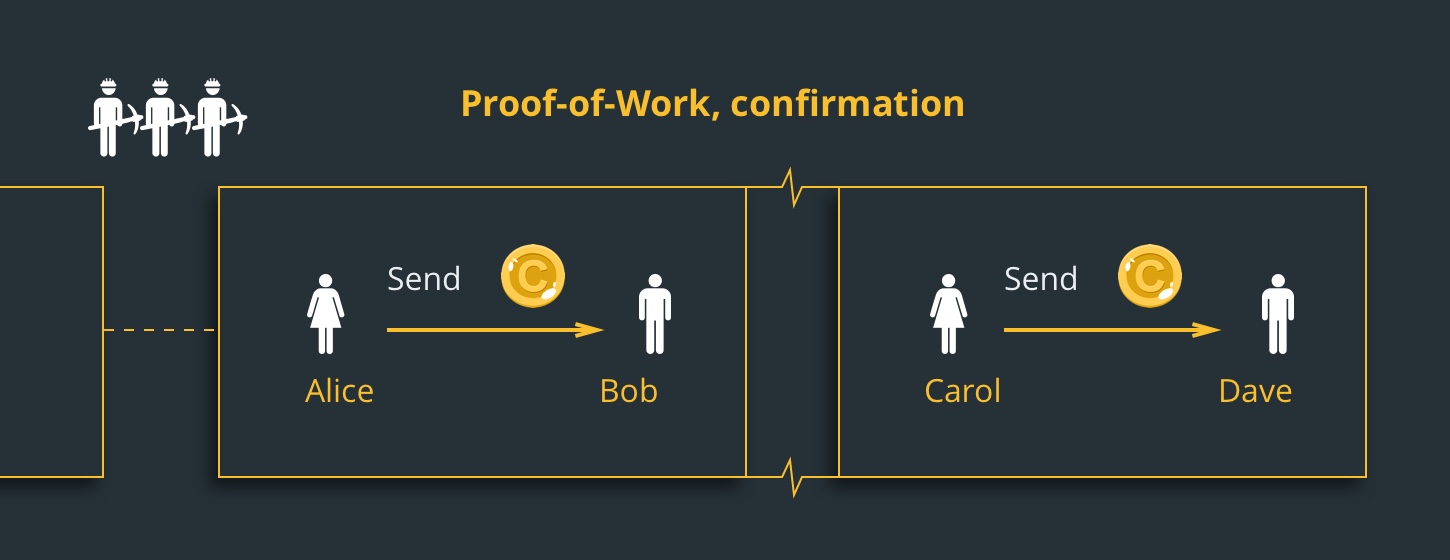
**Proof of work – PoW, là thuật toán đồng thuận ban đầu của mạng lưới**[***Blockchain***](https://pinkblockchain.com/cong-nghe-blockchain-la-gi-ung-dung-cong-nghe-blockchain/)**.**

Với Blockchain, thuật toán này được dùng để xác nhận giao dịch và tạo ra các khối (block) mới. Với PoW, các thợ đào coin cạnh tranh với nhau để hoàn tất giao dịch trên mạng lưới và nhận phần thưởng.

Như các bạn đã biết người dùng tiền tệ mã hóa chắc chắn sẽ muốn gửi token cho nhau. Hệ thống sẽ sử dụng một sổ cái phân quyền để chuyển một lượng giao dịch nhất định vào 1 khối. Tuy nhiên, phải cần đến bàn tay con người tham gia vào công đoạn xác nhận các giao dịch và sắp xếp khối.

Nhiệm vụ đặc biệt trên thường được chúng ta biết đến với tên gọi mining (đào khối/block), còn những người đảm nhiệm công việc ấy chính là các miner (thợ đào coin).

Nguyên lí chính của quá trình là một phương trình toán học phức tạp và nhiệm vụ là tìm ra phương thức để giải quyết nó càng nhanh gọn càng tốt.



**2. “Mathematical puzzle” hay “phương trình toán học phức tạp” là gì?**

***Một câu đố cần rất nhiều năng lực tính toán của máy tính mới có thể giải được.***

Một số bài toán điển hình là:

* [**Hash function**](https://pinkblockchain.com/thuat-toan-bam-hashing-algorithm-hoat-dong-nhu-nao/) (hàm băm): tìm ẩn số đầu vào khi đã biết kết quả đầu ra.
* **Integer factorization** (thừa số nguyên): tìm một số biết nó là tích của hai số khác.
* **Guided tour puzzle protocol** (giao thức hướng dẫn giải quyết bài toán): nếu server cảm thấy mình đang bị tấn công DoS, nó sẽ cần phải tính toán lại hàm băm của một số node theo thứ tự nhất định – trong trường hợp này, bài toán của chúng ta sẽ là để “tìm một chuỗi các giá trị băm”.

Câu trả lời dành cho phương trình toán học PoW được gọi là “[hash](https://pinkblockchain.com/ham-bam-khoi-block-hash-duoc-tao-ra-nhu-nao/)”.

Hàm Hash sẽ giải quyết bài toán như dưới đây để có thể tìm ra số nonce

with

Khi mạng lưới ngày càng lớn mạnh thì nó sẽ phải đối mặt với nhiều bài toán với cấp độ khó hơn. Do vậy, thuật toán để đủ sức tìm ra đáp số và đào khối thì sẽ càng cần nhiều và nhiều hash power – năng lực băm hơn nữa. Vì thế, độ khó thuật toán đào coin là một trong những vấn đề nhạy cảm nhất trên Blockchain hiện nay.

**3. Vì sao?**

***Sự chính xác trong xử lí và tốc độ của Blockchain phụ thuộc rất nhiều vào Proof of work.***

Tuy nhiên, độ khó bài toán không nên quá phức tạp vì nếu thế thì thời gian tạo khối mới thì sẽ rất lâu. Các giao dịch sẽ bị nghẽn cho đến khi nào được xác nhận chuyển vào khối và dòng chảy công việc sẽ bị ngưng trệ. Nếu bài toán không thể được giải quyết trong khoản thời gian vô hạn định, mạng lưới xem như là sụp đổ.

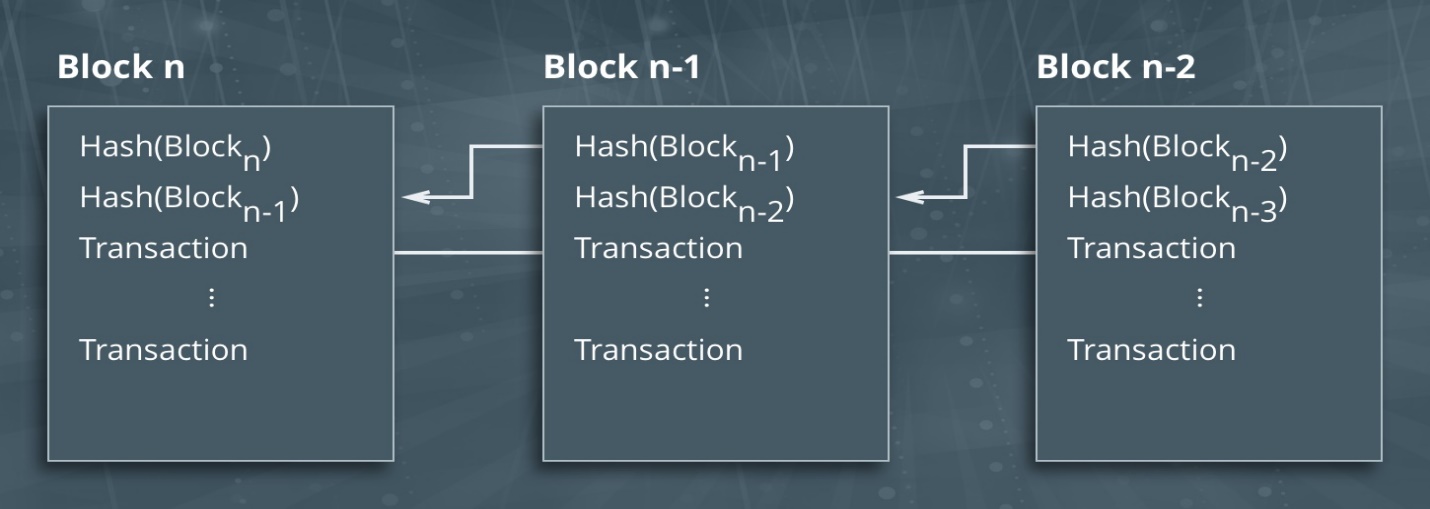
Nhưng nếu bài toán quá dễ thì mạng lưới lại tự đặt mình vào vị trí thuận lợi để bị spam, tấn công DoS và những trục trặc khác.

Bên cạnh đó, đáp án trả về cũng nên đơn giản cho công tác kiểm tra và chấp thuận. Không phải node nào cũng có thể đủ khả năng để xác định liệu tất cả công đoạn tính toán đã làm đúng theo quy trình. Lúc này thì bạn sẽ phải tin tưởng vào quyết định từ các node khác và vi phạm một trong những khía cạnh quan trọng nhất của Blockchain – tính minh bạch.

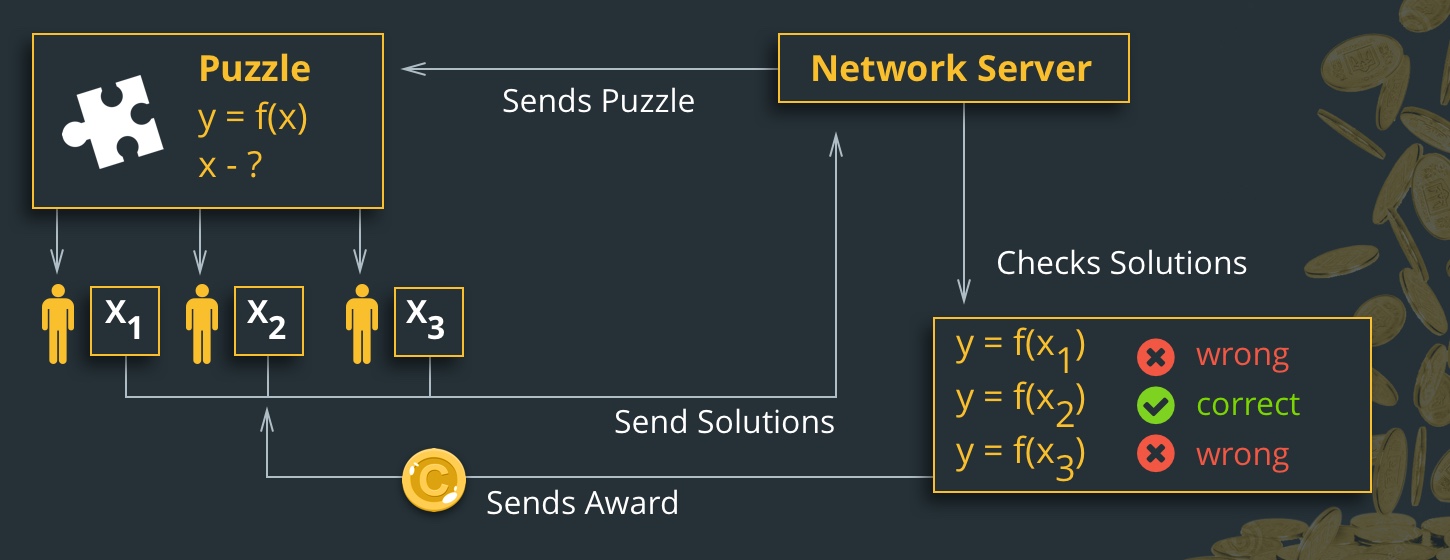
**4. PoW được thực hiện như thế nào trên Blockchain?**

***Thợ đào coin giải quyết bài toán, tạo ra khối mới rồi sau đó xác nhận giao dịch.***

Độ khó của bài toán đào khối sẽ phụ thuộc vào số lượng người dùng, năng lực khai thác hiện tại và tải trọng của mạng lưới. Hash của mỗi khối chứa trong nó hash của các khối trước đó, giúp gia tăng mức độ an ninh và tránh vi phạm.



Sau khi thợ đào coin giải quyết được bài toán thì hệ thống sẽ cho phép tạo thêm một khối mới. Các giao dịch sẽ được chuyển vào khối này và xem như là đã được xác nhận.



## ****5. Proof-of-work được áp dụng vào đâu?****

Hiện thì giao thức Proof-of-work đang được rất nhiều đồng tiền điện tử sử dụng.

Một trong những ví dụ điển hình nhất cho tích hợp PoW chính là ở Bitcoin. Chính Bitcoin đã tạo ra nền tảng giới thiệu thuật toán đồng thuận này đến với thế giới. PoW của Bitcoin có tên gọi là Hashcash. Giao thức ấy cho phép thay đổi độ khó thuật toán đào dựa trên năng lực khai thác hiện tại của mạng lưới. Thời gian trung bình tạo block mới hiện tại là 10 phút. Những đồng tiền điện tử khác trên nền tảng Bitcoin như Litecoin cũng sử dụng hệ thống tương tự.

Một mạng lưới khác sử dụng PoW là Ethereum. Vì ngay lúc này cứ 4 thì đã có đến 3 dự án chạy trên nền tảng Ethereum, cho nên có thể nói phần lớn các ứng dụng Blockchain đều đang tích hợp mô hình đồng thuận Proof-of-work.

## ****6. Tại sao phải sử dụng Proof-of-work ngay từ đầu?****

Một trong những lợi ích chính là bảo vệ chống tấn công DoS và giảm thiểu rủi ro trong hoạt động đào tiền.

Bảo vệ chống tấn công DoS (Denial of Service): PoW đặt ra giới hạn cao lên mạng lưới. Muốn thực hiện hành động gì đó thì trước hết bạn phải đáp ứng được chúng. Do đó, để tấn công vào mạng lưới thì trước hết cần phải tập hợp lượng năng lực máy tính đủ lớn và cần nhiều thời gian để tính toán. Đợt tấn công vẫn có thể triển khai được nhưng với cái giá phải trả là chi phí cực kì lớn.

Khả năng đào block: Không quan trọng là bạn có bao nhiêu tiền trong ví. Thứ tồn tại duy nhất là liệu bạn có đủ năng lực máy tính để giải toán đào block hay không mà thôi. Do đó, trên mạng lưới Blockchain, người có tiền chưa chắc đã có quyền.

## ****7. Vậy Proof-of-work có tồn tại trong mình khiếm khuyết nào không?****

Những điểm trừ chính là chi phí đắt đỏ, “sự vô dụng” của năng lực tính toán và tấn công 51%.

Chi phí đắt đỏ: Đào tiền yêu cầu trang bị những máy tính cùng phần cứng chuyên dụng đủ sức chạy những thuật toán hết sức phức tạp. Số tiền phải bỏ ra là rất lớn đối với một cá nhân riêng lẻ. Chính vì vậy, hoạt động khai thác block hiện giờ chỉ được thực hiện chủ yếu bởi các hội thợ đào (mining pool). Những nhóm người dùng nảy sử dụng các thiết bị tiêu tốn rất nhiều năng lượng, càng làm gia tăng chi phí khai thác. Chưa hết, sự xuất hiện của các hội thợ đào được lo sợ là sẽ đe doạ đến bản chất phân quyền của tiền điện tử, đặc biệt là đối với trường hợp của Bitcoin.

“Sự vô dụng” của năng lực máy tính: Thợ đào đúng thật là phải làm việc cật lực mới có thể tạo ra block mới, quá trình ấy tiêu thụ rất nhiều điện năng. Tuy nhiên, công việc tính toán của họ cũng không thể mang đi áp dụng ở những nơi khác. Họ chỉ có thể bảo đảm mạng lưới vận hành trơn tru nhưng lại không thể ứng dụng kĩ năng của mình vào kinh doanh, làm khoa học hay tham gia bất cứ lĩnh vực nào nữa cả.

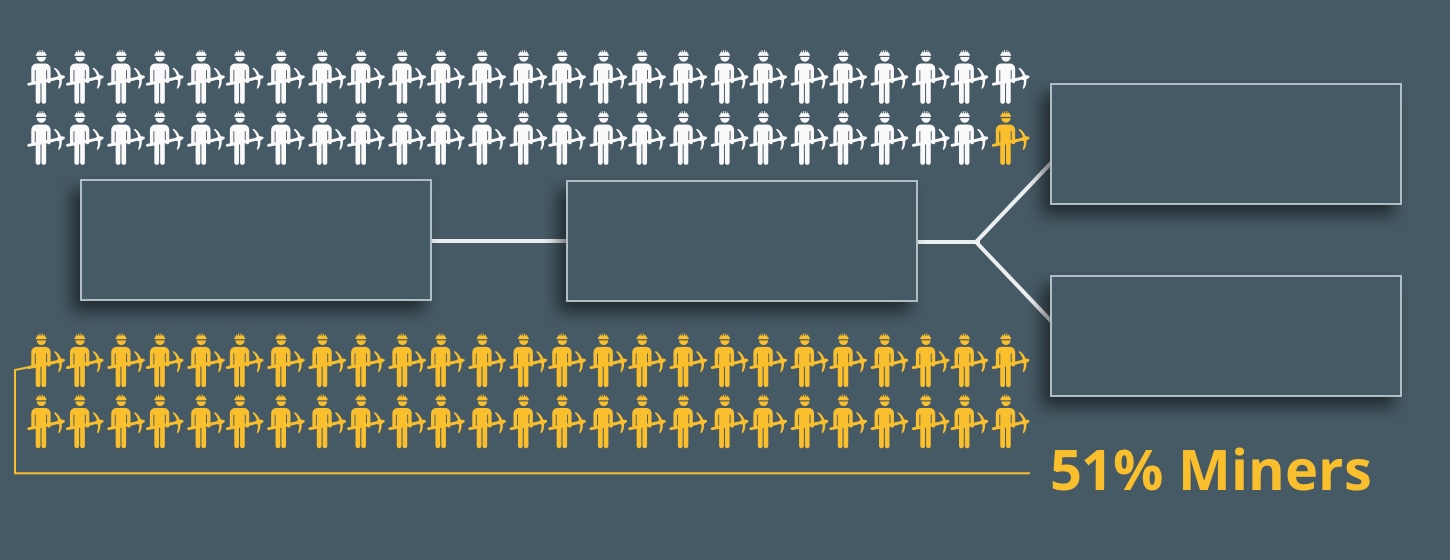
## ****8. Tấn công 51% là cái gì nữa đây?****

Một cuộc tấn công 51%, hay tấn công đa số, xảy ra khi một nhóm người dùng kiểm soát đa số năng lực khai thác.

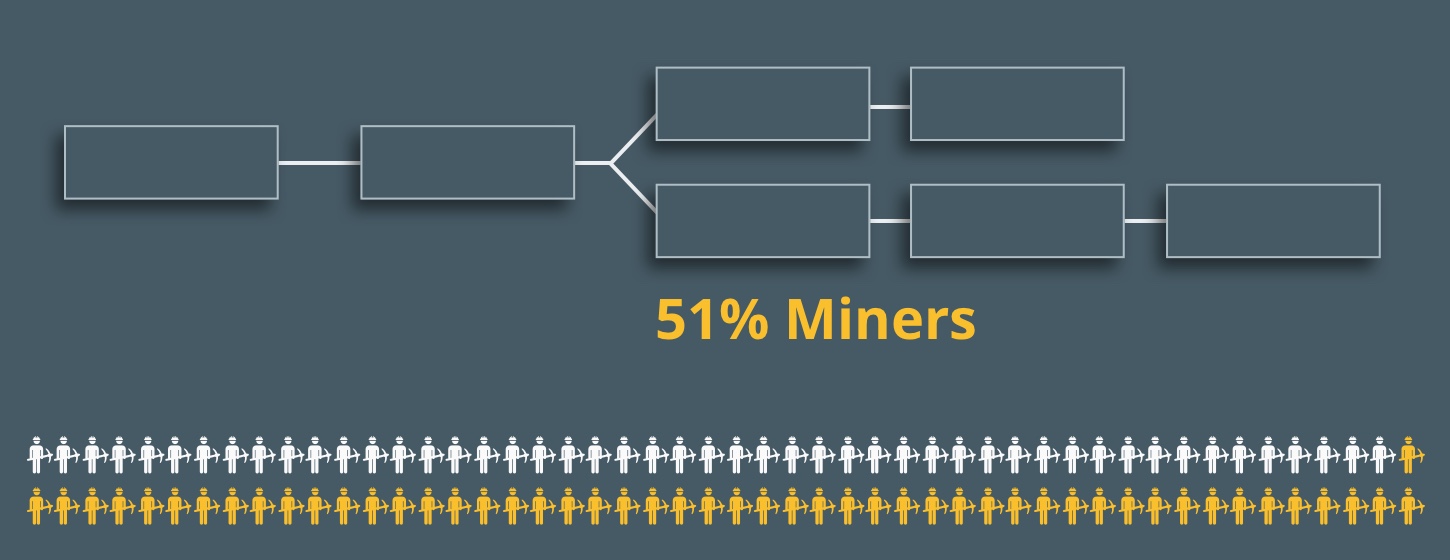
Khi ấy thì những kẻ tấn công sẽ có đủ quyền lực để kiểm soát và tác động lên đa số các sự kiện xảy ra trên mạng lưới.

Chúng có thể độc quyền quá trình tạo block mới và giành lấy toàn bộ phần thưởng vì chúng hoàn toàn dễ dàng ngăn những thợ đào khác giải xong bài toàn trước.Chúng thậm chí còn có thể đảo ngược giao dịch.

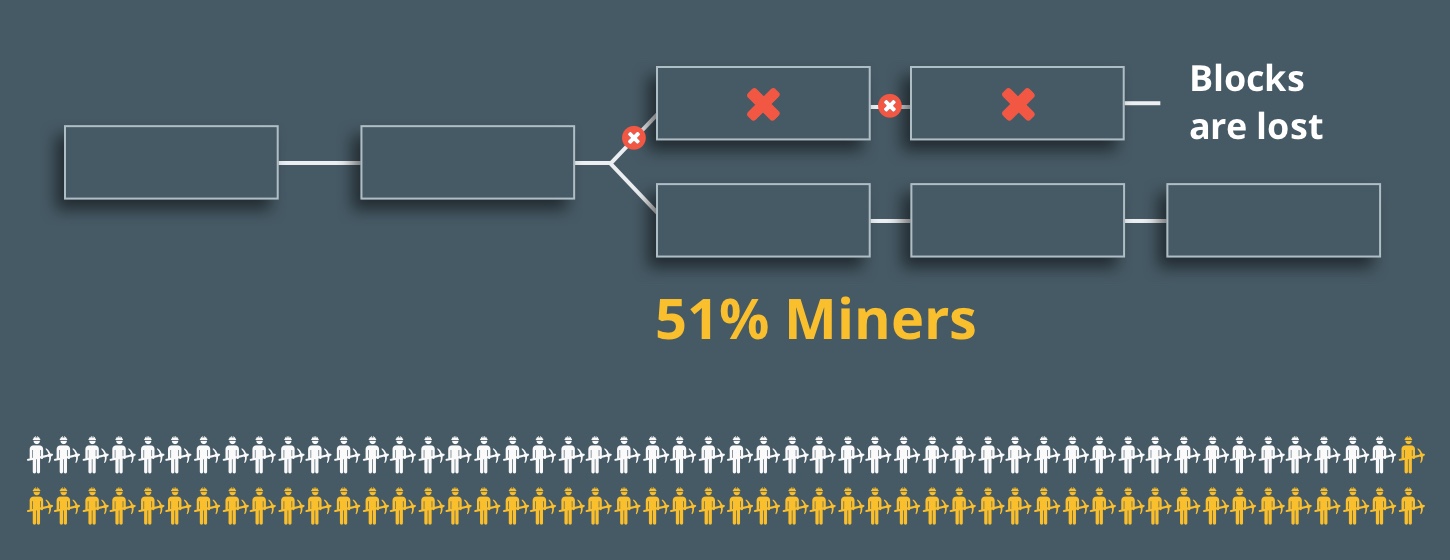
Ví dụ, hãy giả dụ Alice gửi Bob một số tiền thông qua Blockchain. Alice bị dính tấn công 51%, Bob thì không. Giao dịch tuy đã được chuyển vào trong block thế nhưng những kẻ tấn công lại chặn không cho chuyển tiền. Và thế là sẽ có một đợt fork xảy ra trên Blockchain.



Lúc đó thì thợ đào sẽ phân nhánh thành hai chain nhỏ hơn. Một bên chắc chắn sẽ có 51% số thợ đào, chính vì thế chain đó sẽ đào được nhiều block hơn.



Đến cuối cùng, chain dài hơn sẽ tồn tại, chain ngắn hơn sẽ bị đào thải. Giao dịch giữa Bob và Alice xem như chưa từng xảy ra. Bob sẽ không nhận được tiền của mình.



Từ những bước trên, kẻ tấn công có thể đảo ngược lại giao dịch.

Mặc dù vậy, tấn công 51% vẫn không phải là một lựa chọn có lợi về kinh tế. Nó yêu cầu phải tập hợp một lượng năng lực đào áp đảo. Và khi tin tức về việc này lan truyền, người dùng sẽ cân nhắc từ bỏ mạng lưới vì họ xem như nó không còn duy trì được tính phân quyền nữa. Giá của đồng tiền điện tử gắn liền với Blockchain ấy sẽ rớt thê thảm. Tất yếu, người dùng sẽ mất toàn bộ tài sản của mình.

# **II. BITCOIN**

## 1. Giới thiệu tổng quan về Bitcon

Bitcoin (ký hiệu: **BTC, XBT, [BitcoinSign.svg](https://vi.wikipedia.org/wiki/T%E1%BA%ADp_tin:BitcoinSign.svg)**) là một loại [tiền mã hóa](https://vi.wikipedia.org/wiki/Ti%E1%BB%81n_m%C3%A3_h%C3%B3a), được phát minh bởi một người ẩn danh tên [Satoshi Nakamoto](https://vi.wikipedia.org/wiki/Satoshi_Nakamoto) dưới dạng phần mềm [mã nguồn mở](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_ngu%E1%BB%93n_m%E1%BB%9F) từ năm 2009. Bitcoin có thể được trao đổi trực tiếp bằng thiết bị kết nối Internet mà không cần thông qua một [tổ chức tài chính](https://vi.wikipedia.org/wiki/T%E1%BB%95_ch%E1%BB%A9c_t%C3%A0i_ch%C3%ADnh) [trung gian](https://vi.wikipedia.org/wiki/Trung_gian_t%C3%A0i_ch%C3%ADnh) nào.

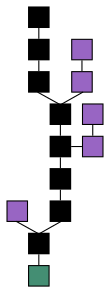
Bitcoin có cách hoạt động khác hẳn so với các loại tiền tệ điển hình: Không có một [ngân hàng trung ương](https://vi.wikipedia.org/wiki/Ng%C3%A2n_h%C3%A0ng_trung_%C6%B0%C6%A1ng) nào quản lý nó và hệ thống hoạt động dựa trên một giao thức [mạng ngang hàng](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_ngang_h%C3%A0ng) trên Internet. Sự cung ứng của Bitcoin tự động và hạn chế được phân chia theo lịch trình định sẵn dựa trên các [thuật toán](https://vi.wikipedia.org/wiki/Thu%E1%BA%ADt_to%C3%A1n). Bitcoin được cấp tới các máy tính "đào" Bitcoin để trả công cho việc xác minh giao dịch Bitcoin và ghi chúng vào cuốn sổ cái được phân tán trong mạng ngang hàng - được gọi là [blockchain](https://vi.wikipedia.org/wiki/Blockchain). Cuốn [sổ cái](https://vi.wikipedia.org/w/index.php?title=S%E1%BB%95_c%C3%A1i&action=edit&redlink=1)này sử dụng Bitcoin là đơn vị kế toán. Mỗi bitcoin có thể được chia nhỏ tới 100 triệu đơn vị nhỏ hơn gọi là satoshi.

[Phí giao dịch](https://vi.wikipedia.org/w/index.php?title=Ph%C3%AD_giao_d%E1%BB%8Bch&action=edit&redlink=1) có thể áp dụng cho giao dịch mới tùy thuộc vào nguồn tài nguyên của mạng. Ngoài phí giao dịch, các thợ đào còn được trả công cho việc tạo ra các khối (block) chứa nhật ký giao dịch. Cứ mỗi 10 phút, một khối mới được tạo ra kèm theo một lượng Bitcoin được cấp phát. Số bitcoin được cấp cho mỗi khối phụ thuộc vào thời gian hoạt động của mạng lưới. Vào tháng 7 năm 2016, 12,5 bitcoin được cấp phát cho mỗi khối mới. Tốc độ [lạm phát](https://vi.wikipedia.org/wiki/L%E1%BA%A1m_ph%C3%A1t) sẽ giảm một nửa còn 6,25 bitcoin vào tháng 7 năm 2020 và tiếp tục giảm một nửa sau mỗi chu kỳ 4 năm cho tới khi có tổng cộng 21 triệu Bitcoin được phát hành vào năm [2140](https://vi.wikipedia.org/w/index.php?title=2140&action=edit&redlink=1). Ngoài việc đào Bitcoin, người dùng có thể có Bitcoin bằng cách trao đổi lấy Bitcoin khi bán tiền tệ, hàng hoá, hoặc dịch vụ khác.

Bitcoin là loại tiền mã hoá điển hình nhất, ra đời đầu tiên, và được sử dụng rộng rãi nhất trong thương mại điện tử. Các doanh nghiệp có xu hướng muốn thanh toán bằng Bitcoin để giảm thiểu chi phí thanh toán giữa hai bên. Đến tháng 10 năm 2017, lượng [tiền cơ sở](https://vi.wikipedia.org/wiki/Ti%E1%BB%81n_c%C6%A1_s%E1%BB%9F) của Bitcoin được định giá hơn 252 tỷ đô la Mỹ - là loại tiền mã hóa có giá trị thị trường lớn nhất. Những biến động lớn trong giá trị của mỗi bitcoin đã tạo nên những lời chỉ trích về tính phù hợp kinh tế của Bitcoin như là một loại tiền tệ chính thức.

Lưu ý rằng, thuật ngữ Bitcoin được viết hoa khi nhắc tới như một giao thức, phần mềm, hoặc cộng đồng và được viết thường khi được nhắc tới như một đơn vị tiền tệ.

### a. [Blockchain](https://vi.wikipedia.org/wiki/Blockchain) - Chuỗi khối

[](https://vi.wikipedia.org/wiki/T%E1%BA%ADp_tin:Blockchain.svg)

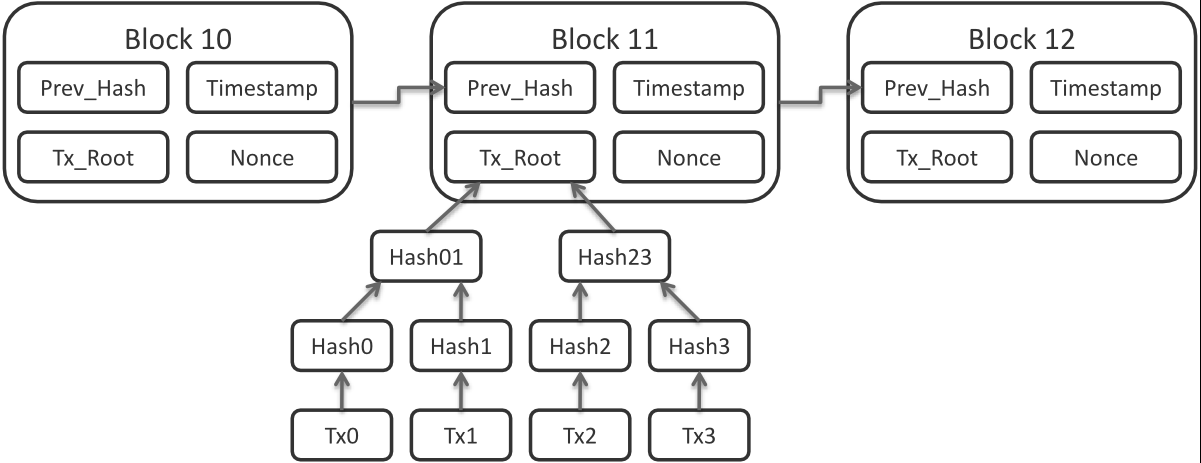
Chuỗi chính (màu đen) bao gồm chuỗi khối dài nhất tính từ khối khởi thủy (genesis) màu xanh. Khối orphan màu tím không được chấp nhận do không đạt sự đồng thuận của mạng lưới.

Mọi [dữ liệu](https://vi.wikipedia.org/wiki/D%E1%BB%AF_li%E1%BB%87u) trên mạng Internet đều rất dễ dàng bị sao chép, mỗi giao dịch Bitcoin cũng chỉ là một khối thông tin. Bình thường, khi giao dịch trực tuyến, chúng ta sẽ cần đến một bên trung gian thứ ba mà chúng ta tin tưởng (ví dụ: công ty [Paypal](https://vi.wikipedia.org/wiki/PayPal), công ty Ngân Lượng, Ngân hàng [Vietcombank](https://vi.wikipedia.org/wiki/Vietcombank),...) với một [cơ sở dữ liệu](https://vi.wikipedia.org/wiki/C%C6%A1_s%E1%BB%9F_d%E1%BB%AF_li%E1%BB%87u)tập trung để xác minh [giao dịch](https://vi.wikipedia.org/wiki/Giao_d%E1%BB%8Bch_t%C3%A0i_ch%C3%ADnh) nhằm chống gian lận khi kẻ gian sử dụng lại khối thông tin này nhiều lần. Công nghệ [blockchain](https://vi.wikipedia.org/wiki/Blockchain) đã giải quyết được bài toán này (double-spending) mà không cần tới bên trung gian thứ ba tin cậy. [Blockchain](https://vi.wikipedia.org/wiki/Blockchain) là một cuốn sổ cái ghi lại tất cả các giao dịch. Dữ liệu trong cuốn sổ cái liên tục được mạng lưới máy tính ngang hàng trên thế giới cập nhật và bảo trì. Giao dịch khi A gửi X bitcoin cho B được ghi lại trên toàn hệ thống, tất cả các máy tính trong mạng này sẽ xác minh và ghi lại giao dịch đó vào cuốn sổ cái rồi cấp phát dữ liệu này tới các máy tính khác. [Blockchain](https://vi.wikipedia.org/wiki/Blockchain) là một cơ sở dữ liệu phân tán vô chủ; các máy tính liên tục thực hiện việc kiểm toán độc lập bằng cách xác minh dữ liệu nhận tới và so sánh với chữ ký của giao dịch đó.

Về công nghệ, các giao dịch được xác minh bởi thuật toán [chữ ký số](https://vi.wikipedia.org/wiki/Ch%E1%BB%AF_k%C3%BD_s%E1%BB%91) dựa trên đường cong Elliptic và được xác nhận bởi chuỗi các quá trình xử lý lần lượt các [hàm băm](https://vi.wikipedia.org/wiki/H%C3%A0m_b%C4%83m) [SHA256](https://vi.wikipedia.org/wiki/SHA) bởi các thợ đào Bitcoin. Mỗi khối trong blockchain chứa tất cả thông tin giao dịch trong khối đó trong 1 [cây Merkle](https://vi.wikipedia.org/wiki/C%C3%A2y_Merkle) - là một [cây nhị phân](https://vi.wikipedia.org/wiki/C%C3%A2y_t%C3%ACm_ki%E1%BA%BFm_nh%E1%BB%8B_ph%C3%A2n) có thứ tự được xây dựng từ một dãy các đối tượng dữ liệu sử dụng [hàm băm](https://vi.wikipedia.org/wiki/H%C3%A0m_b%C4%83m_m%E1%BA%ADt_m%C3%A3_h%E1%BB%8Dc) - để đạt hiệu quả cao trong việc lưu trữ và xác minh với lượng [dữ liệu lớn](https://vi.wikipedia.org/wiki/D%E1%BB%AF_li%E1%BB%87u_l%E1%BB%9Bn) các giao dịch. Khi có một giao dịch không hợp lệ, hệ thống sẽ loại bỏ nó bằng cách chọn theo số đông. Cách giải quyết về sự đồng thuận này của công nghệ blockchain là lời giải cho [bài toán các vị tướng Byzantine](https://vi.wikipedia.org/wiki/B%C3%A0i_to%C3%A1n_c%C3%A1c_v%E1%BB%8B_t%C6%B0%E1%BB%9Bng_Byzantine) trong ngành [khoa học máy tính](https://vi.wikipedia.org/wiki/Khoa_h%E1%BB%8Dc_m%C3%A1y_t%C3%ADnh)[[18]](https://vi.wikipedia.org/wiki/Bitcoin#cite_note-18). Càng có nhiều máy tính tham gia vào hệ thống ngang hàng cho blockchain thì sức mạnh xử lý và độ an toàn của hệ thống blockchain đó càng cao.

Công nghệ blockchain có rất nhiều ứng dụng khác mà tiền tệ Bitcoin chỉ là một trong số đó, ví dụ: Ứng dụng cho việc đăng ký sử dụng đất đai, các loại [công chứng](https://vi.wikipedia.org/wiki/C%C3%B4ng_ch%E1%BB%A9ng), [hợp đồng](https://vi.wikipedia.org/wiki/H%E1%BB%A3p_%C4%91%E1%BB%93ng) thông minh (tự động cho phép hoặc hủy giao dịch với một số điều kiện được lập trình sẵn), đăng ký [tên miền](https://vi.wikipedia.org/wiki/T%C3%AAn_mi%E1%BB%81n), quy trình bỏ phiếu,... khi các thuật toán trở nên đáng tin cậy hơn các bên trung gian thứ ba (mà có thể không đáng tin cậy vì tệ nạn [tham nhũng](https://vi.wikipedia.org/wiki/Tham_nh%C5%A9ng)). Công nghệ blockchain cho phép những người lạ có thể giao dịch an toàn với nhau mà không cần tin tưởng nhau.

### b. [Đào](https://vi.wikipedia.org/wiki/Khai_th%C3%A1c_m%E1%BB%8F) Bitcoin

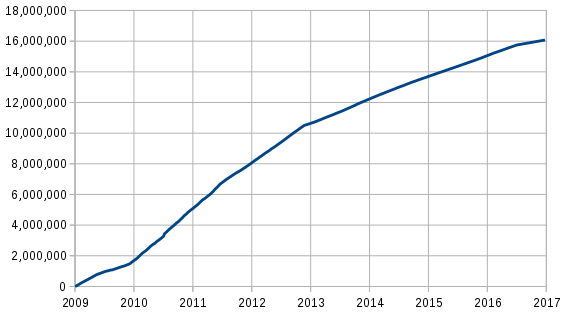


Dữ liệu trong một khối Bitcoin

Để có thể được cả mạng lưới chấp nhận, khối mới cần phải chứa bằng chứng công việc (proof-of-work). Proof-of-work yêu cầu thợ đào tìm kiếm một số nonce, mà khi nội dung của khối được hash ([hàm băm mật mã học](https://vi.wikipedia.org/wiki/H%C3%A0m_b%C4%83m_m%E1%BA%ADt_m%C3%A3_h%E1%BB%8Dc)) cùng nonce, kết quả tạo ra một số nhỏ hơn số target của mạng lưới (số target càng nhỏ thì độ khó càng cao). Nói cách khác: Proof-of-work rất dễ cho các máy tính xác nhận, nhưng cực kỳ mất nhiều thời gian để có thể tạo ra. Thợ đào phải thử rất nhiều giá trị nonce khác nhau trước khi đạt được độ khó mà mạng lưới yêu cầu.

Cứ mỗi 2016 khối được tạo ra (mất khoảng 14 ngày), độ khó lại được mạng lưới tự động tinh chỉnh dựa trên khả năng của toàn bộ mạng lưới, với mục đích là để giữ khoảng thời gian giữa các khối mới được tạo ra là 10 phút. Từ tháng 3 năm 2014 tới tháng 3 năm 2015, số lượng nonce trung bình mà máy đào phải hash thử trước khi tạo được ra khối mới đã tăng từ 16,4 tỷ tỷ lên 200,5 tỷ tỷ.

Cách hệ thống proof-of-work hoạt động, kèm theo việc xâu chuỗi lại các khối khi dữ liệu của khối mới bao gồm hash của khối cũ, giúp cho việc thay đổi blockchain cực kỳ khó, khi mà kẻ tấn công cần phải thay đổi tất cả các khối phía sau để việc thay đổi một khối được chấp nhận. Điều này đòi hỏi kẻ tấn công cần có hơn 50% sức mạnh xử lý của toàn mạng [Blockchain](https://vi.wikipedia.org/wiki/Blockchain). Các khối mới liên tục được tạo ra, và độ khó của việc thay đổi 1 khối tăng dần theo thời gian với số lượng khối cần thay đổi (còn được gọi là mức xác thực của một khối - confirmations) tăng lên.



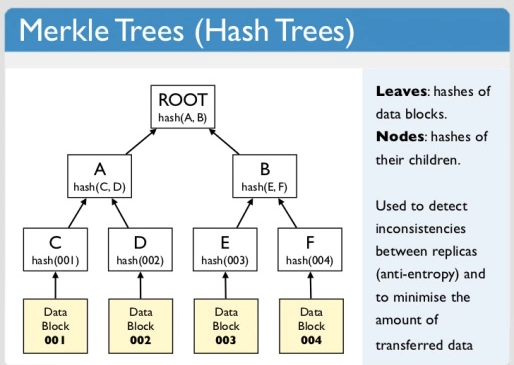
Tổng số bitcoin đang lưu hành

Thợ đào (hoặc mỏ đào) Bitcoin tìm được ra khối mới sẽ được thưởng số bitcoin thưởng trong khối đó cộng toàn bộ [phí giao dịch](https://vi.wikipedia.org/w/index.php?title=Ph%C3%AD_giao_d%E1%BB%8Bch&action=edit&redlink=1) được xử lý trong khối đó. Tại thời điểm cuối năm 2016, phần thưởng đang là 12,5 bitcoin cho mỗi khối. Để nhận được phần thưởng này, một giao dịch đặc biệt có tên là coinbase được đưa vào thanh toán. Tất cả Bitcoin tồn tại được khởi tạo từ những giao dịch nguồn (coinbase) đó. Giao thức Bitcoin quy định rằng phần thưởng sẽ giảm một nửa sau mỗi 210.000 khối (khoảng 4 năm). Cuối cùng, phần thưởng sẽ tiệm cận tới 0 khi số bitcoin trên thị trường đạt ngưỡng 21 triệu bitcoin vào năm 2140. Lúc đó, thợ đào sẽ chỉ có phần thưởng là phí giao dịch. Nói cách khác, Satoshi đã tạo ra một [chính sách tiền tệ](https://vi.wikipedia.org/wiki/Ch%C3%ADnh_s%C3%A1ch_ti%E1%BB%81n_t%E1%BB%87) dựa trên sự khan hiếm nhân tạo khi sáng tạo ra Bitcoin rằng sẽ chỉ có tổng cộng 21 triệu bitcoin được lưu hành.

Trong thực tế, các thợ đào thường sẽ tham gia vào các mỏ đào lớn để tập hợp được khả năng tính toán của máy đào thành viên trong mỏ đó nhằm tăng xác suất tạo được ra khối mới, và sau đó tiền công sẽ được chia đều theo khối lượng công việc cho thành viên trong mỏ đào. Việc đào mỏ đã tạo ra một loạt công nghệ chuyên biệt để đào Bitcoin. Hiện tại, hệ thống đào Bitcoin hiệu quả nhất sử dụng vi mạch tích hợp chuyên dụng [ASIC](https://vi.wikipedia.org/wiki/ASIC) vì chúng xử lý tính toán số học nhanh hơn bộ vi xử lý máy tính (kể cả trong [bo mạch đồ họa](https://vi.wikipedia.org/wiki/Bo_m%E1%BA%A1ch_%C4%91%E1%BB%93_h%E1%BB%8Da)) mà lại khi sử dụng ít điện năng hơn.

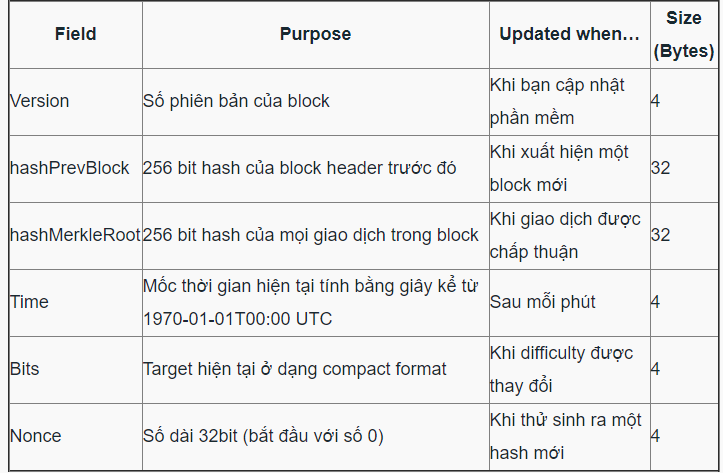
## 2. Thuật toán Hashcash SHA 256

Công việc đào bitcoin sử dụng hàm hashcash proof of work; thuật toán hashcash đòi hỏi các thông số sau: service string, nonce, và counter. Đối với bitcoin, service string được mã hóa trong cấu trúc dữ liệu của block header, và bao gồm các trường như version (phiên bản), hash của block trước đó, merkle tree root hash của tất cả các giao dịch trong block, thời gian hiện tại, và difficulty. Bitcoin lưu trữ các nonce trong trường extraNonce – một phần trong giao dịch coinbase (được lưu trữ ở nút mạng bên trái trên sơ đồ merkle tree) – giao dịch coinbase (hay còn gọi là generation transaction) là loại giao dịch đặc biệt đầu tiên chứa trong block.



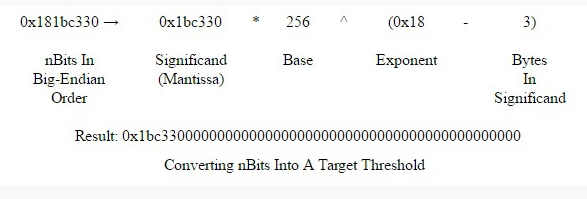
Thông số counter khá ngắn – 32bit – cho nên mỗi lần counter wrap, trường extraNonce sẽ phải được tăng lên (hoặc thay đổi khác đi) để tránh công việc bị lặp lại. Nguyên tắc cơ bản của thuật toán hashcash khá dễ hiểu. Khi thợ mỏ đào bitcoin, thuật toán hashcash sẽ liên tục hash block header trong khi gia tăng counter và trường extraNonce. Việc tăng trường extraNonce đòi hỏi phải tái cấu trúc lại merkle tree, bởi vì giao dịch coinbase là nút mạng phía bên trái.

Block header bao gồm các trường sau:



Phần thân của block chứa đựng các giao dịch. Nó chỉ có thể được hash gián tiếp thông qua Merkle root. Bởi vì các giao dịch không được hash trực tiếp, cho nên việc hash một block chứa 1 giao dịch đòi hỏi công sức tương tự với việc hash một block chứa 10,000 giao dịch.

Dạng compact format của target là một loại mã hóa floating-point (dấu phẩy động) đặc biệt sử dụng 3 bytes mantissa: byte đầu là phần mũ (chỉ có 5 bit thấp nhất được sử dụng) và số nhân là 256. Hầu hết các trường này đều giống nhau đối với tất cả người dùng. Tuy nhiên có thể có vài biến thể nhỏ trong các mốc thời gian. Nonce thường sẽ khác nhau, nhưng nó sẽ tăng theo một cách tuyến tính. “Nonce” bắt đầu = 0 và được gia tăng sau mỗi hash. Khi nào Nonce quá tải (xảy ra thường xuyên), counter sẽ wrap và phần extraNonce của giao dịch coinbase sẽ được gia tăng, và làm thay đổi Merkle root.



Hơn nữa, rất khó có chuyện hai thợ đào có cùng một Merkle root giống nhau bởi vì giao dịch đầu tiên trong block của thợ đào chính là giao dịch coinbase (được chuyển tới địa chỉ ví Bitcoin của người đó). Với việc block của người này chắc chắn khác với block của những người khác, nên hash của anh ta tạo ra chắc chắn sẽ khác. Mỗi hash anh ta tính toán sẽ có tỷ lệ cơ hội dành chiến thắng tương tự với bất kỳ hash nào khác được tính toán bởi những người khác trong mạng lưới.

Bitcoin sử dụng: SHA256(SHA256(Block\_Header)) nhưng cần phải chú ý thứ tự sắp xếp của byte.

Lấy ví dụ đoạn code python tính toán ra block hash với hash nhỏ nhất vào tháng 7 năm 2011, Block 125552. Block header được hình thành từ 6 trường đã được mô tả ở trên, kết nối với nhau tạo thành giá trị “little endian” trong hệ đếm thập lục phân.



# III. LITECOIN

## 1. Giới thiệu.

- [Litecoin](https://en.wikipedia.org/wiki/Litecoin) (LTC) là loại tiền tệ mã hóa hay tiền tệ ngang hàng của internet, cho phép thanh toán tức thời và gần như miễn phí cho bất kỳ ai trên thế giới, nó được phân cấp tương tự như Bitcoin, dựa trên nền tảng Peer To Peer.

*- Litecoin* đươc phát minh bởi một cựu nhân viên Google là Charles Lee vào 7/10/2011 trên mã nguồn Github được công bố dưới giấy phép mở MIT/X11 trong đó cho phép bạn có quyền chạy, sửa đổi và sao chép phần mềm đồng thời phân phối bản sửa đổi tùy theo ý muốn, mở ra một kỷ nguyên mới cho tiền ảo.

- Có một quá trình xuất bản minh bạch, do đó cho phép việc kiểm tra một cách độc lập các tập tin chạy và mã nguồn tương ứng. Litecoin là một mạng lưới thanh toán toàn cầu dựa trên mã nguồn mở và có tính chất phân tán thuần túy, không cần có bất cứ thực thể quản lý trung tâm nào, được bảo đảm bằng các định luật toán học và giúp từng người kiểm soát được tài chính của chính mình. Nhờ có sự hỗ trợ đáng kể trong ngành công nghiệp, khối lượng giao dịch và tính thanh khoản, **Litecoin là một phương tiện trung gian thương mại** đã qua thử thách bên cạnh Bitcoin

- Nếu như bitcoin sử dụng nền tảng mã hóa SHA256 thì Litecoin đã biết cách cải tiến hơn với Scrypt, điều này cho phép người khai thác tiền ảo có thể cùng lúc đào cả Bitcoin và Litecoin, mà không sợ xung đột hệ thống.

## 2. Đơn vị tính của Litecoin

Giống như Bitcoin thì Litecoin cũng được chia ra thành 1 triệu đơn vị:

* 0.001 mLTC (millicoin)
* 0.000001 µLTC (microcoin)
* 0.00000001 Đơn vị nhỏ nhất

## 3. Sự khác nhau giữa Bitcoin và Litecoin

|  |  |  |
| --- | --- | --- |
|  | **Bitcoin** | **Litecoin** |
| Tổng số coin | 21 Million | 84 Million |
| Thuật toán | SHA-256 | Scrypt |
| Thời gian trung bình  cho mỗi block | 10 minutes | 2.5 minutes |
| Phần thưởng cho mỗi block | Giảm một nửa sau mỗi 210,000 blocks. | Giảm một nửa sau mỗi 840,000 blocks |
| Phần thưởng ban đầu | 50 BTC | 50 BTC |
| Phần thưởng cho mỗi block hiện tại | 25 BTC | 50 BTC |
| Vốn hóa thị trường | $10,467,596,650.78 | $540,274,528.26 |

## 4. Giá trị của đồng tiền ảo Litecoin

\* Được tính từ ngày 28/8/2013 đến 21/6/2017

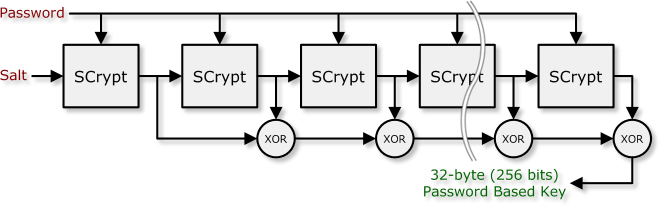
Theo như biểu đồ trên thì giá của 1 LTC = $49.39 đang tăng 3.39%, tổng vốn hóa thị trường là $2.551.138.762, tương đương với 1,021,270 BTC. Hiện tại, nó cũng đang được xếp thứ 4 trên bảng xếp hạng tiền ảo thế giới, chỉ đứng sau đồng BTC, ETH và Ripplecoin.

****

## 5. Thuật toán mã hóa phân cấp Scrypt.

- Scrypt là một hàm dẫn xuất khóa (hàm hash) trong bộ nhớ cứng. Những chức năng của bộ nhớ cứng đòi hỏi một số lượng lớn RAM để có thể tiến hành giải quyết. Điều này có nghĩa là một **chip ASIC** tiêu chuẩn được sử dụng để giải quyết [Bitcoin](https://cafebitcoin.vn/tien-dien-tu/bitcoin-la-gi/)SHA-256 Proof of Work sẽ cần phải dự trữ một khoảng không gian cho bộ nhớ truy cập ngẫu nhiên thay vì sử dụng năng lượng băm tinh khiết.

- Scrypt chỉ điều chỉnh số lượng các biến ngẫu nhiên cần lưu trữ so với SHA-256.



- Litecoin sử dụng các thuật toán scrypt. Thuật toán này đã kết hợp các thuật toán SHA-256, nhưng nhiều tuần tự tính toán hơn so với SHA-256 trong Bitcoin.

- Scrypt sử dụng số lượng lớn RAM tốc độ cao. Scrypt tạo ra một loạt các số giả ngẫu nhiên cần được lưu trữ ở một vị trí trong bộ nhớ RAM. Sau khi thuật toán truy cập các số này một vài lần thì sẽ trả về một kết quả. Việc tạo ra các con số đòi hỏi nhiều tính toán và vì chúng được truy cập vài lần nên sử dụng bộ nhớ RAM kết hợp với sức mạnh băm hơn là tạo ra chúng bằng cách làm tắt (gộp 2 bước thành 1) - việc mà sẽ dẫn đến giảm thời gian và lãng phí bộ nhớ về tốc độ tối ưu hóa.

- Lợi ích chính của thuật toán Scrypt là nó làm giảm lợi thế của các thợ mỏ ASIC Bitcoin trong mạng. Điều này có nghĩa là cần có thêm nhiều thợ mỏ tham gia vào mạng lưới và đóng góp đủ để làm cho nó đáng giá với công sức của họ. Một ưu thế khác là nó chiếm ít năng lượng vì tổng công suất mạng ít hơn. Thuật toán Scrypt sẽ ưu tiên nhiều RAM hơn và khả năng xử lý song song, đó là lý do tại sao các loại máy đào GPU vẫn còn có thể hoạt động khi độ khó của coin tăng lên.

**\* Lợi ích chính của thuật toán mã hóa phân cấp Scrypt:**

- Làm giảm lợi thế của các thợ mỏ ASIC Bitcoin trong mạng.

→ Điều này có nghĩa là cần có thêm nhiều thợ mỏ tham gia vào mạng lưới và đóng góp đủ để làm cho nó đáng giá với công sức của họ.

- Chiếm ít năng lượng vì tổng công suất mạng ít hơn: Thuật toán Scrypt sẽ ưu tiên nhiều RAM hơn và khả năng xử lý song song, đó là lý do tại sao các loại máy đào GPU vẫn còn có thể hoạt động khi độ khó của coin tăng lên.

# **IV. THUẬT TOÁN ETHASH**

## 1. Giới thiệu.

**Ethash** là thuật toán băm được dùng cho **proof-of-work**trong các loại tiền điện tử dựa trên [Ethereum](https://cafebitcoin.vn/tien-dien-tu/ethereum-la-gi/). Nó sử dụng các phiên bản thay thế của SHA3-256 và SHA3-512 thường được gọi là “Keccak-256” và “Keccak-512”.

Từ phiên bản 1.0 Ethash đã được thiết kế để có khả năng chống lại ASIC (ASIC -vi mạch tích hợp chuyên dụng trong điện tử học. Nó là máy đào chuyên dụng tiền ảo) và dễ cho việc kiểm tra. Nó cũng sử dụng một phiên bản sửa đổi nhỏ của Hashimoto để làm giảm chi phí tính toán.

Ethash là tên của thuật toán ProofofWork được sử dụng trong Ethereum. Ban đầu, điều này đã được đề xuất như là thuật toán Dagger-Hashimoto, nhưng nhiều đã thay đổi kể từ khi thực hiện đầu tiên và thuật toán PoW bây giờ đã phát triển thành những gì được gọi là Ethash bây giờ. Tương tự như bitcoin, ý tưởng cốt lõi đằng sau khai thác mỏ là tìm ra một nonce mà một khi băm kết quả trong một mức độ khó xác định trước. Ban đầu, độ khó rất thấp khi Ethereum mới và thậm chí cả CPU và khai thác GPU đơn lẻ đều có lợi nhuận ở một mức độ nhất định, nhưng điều đó không còn là trường hợp nữa. Bây giờ khai thác gộp lại có thể mang lại lợi nhuận, hoặc các trang trại khai thác GPU lớn được sử dụng cho mục đích khai thác.

Ethash là một thuật toán cứng-bộ nhớ, điều này gây khó khăn cho việc triển khai trên phần cứng chuyên dụng. Như trong bitcoin, ASIC đã được phát triển, kết quả là tập trung khai thác trong nhiều năm, nhưng thuật toán ProofofWork cứng nhắc là một cách để ngăn chặn mối đe dọa này và Ethereum triển khai Ethash để ngăn cản sự phát triển của ASIC cho khai thác mỏ. Thuật toán này yêu cầu chọn tập hợp con của một tài nguyên cố định được gọi là DAG (Đồ thị tuần hoàn hướng) tùy thuộc vào nonce và chặn tiêu đề. DAG có kích thước khoảng 2 GB và thay đổi mỗi 30000 khối. Khai thác mỏ chỉ có thể bắt đầu khi DAG được tạo ra hoàn toàn khi lần đầu tiên một nút khai phá bắt đầu. Thời gian giữa mỗi 30000 khối là khoảng 5,2 ngày và được gọi là kỷ nguyên. DAG này được sử dụng như một hạt giống của thuật toán Proofof Work được gọi là Ethash. Theo thông số kỹ thuật hiện tại, thời gian được xác định là 30.000 khối.

Chương trình phần thưởng hiện tại là 5 Ether để tìm kiếm thành công một nonce hợp lệ. Ngoài việc nhận được 5 Ether, thợ mỏ thành công cũng nhận được chi phí của khí được tiêu thụ trong khối và một phần thưởng bổ sung cho việc bao gồm các khối cũ (khối) trong khối. Một khối tối đa được phép cho mỗi khối và được thưởng 7/8 phần thưởng khối bình thường. Để đạt được khoảng thời gian 12 giây, khối khó khăn được điều chỉnh ở mọi khối. Phần thưởng tỷ lệ thuận với tỷ lệ băm của thợ mỏ, về cơ bản có nghĩa là tốc độ của trình khai thác có thể băm nhanh đến mức nào. Khai thác có thể được thực hiện bằng cách đơn giản tham gia mạng Ethereum và chạy một máy khách thích hợp.

Yêu cầu quan trọng là nút phải được đồng bộ hóa hoàn toàn với mạng chính trước khi khai thác có thể bắt đầu.

## 3. So sánh các thuật toán khác

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Thông số** | **Bitcoin** | **Litecoin** | **Ethreum** | **Monero (XMR)** | **Dash (DASH)** |
| **Giới hạn coin** | 21 triệu | 84 triệu | Unlimited | Unlimite | Unlimite |
| **Thuật toán** | **SHA-256** | **Scrypt** | **Ethash**  **Keccak256** | **CryptoNight**  **CryptoNote** | **X11** |
| **Đơn vị tính hash** | G hash/s = triệu hash/s | K hash/s | M hash/s | Hash/s | M hash/s |
| **Thời gian tạo khối trung bình** | 10 phút | 2.5 phút | 13-15s | 60 s | 2 – 5 phút |
| **Thiết bị** | GPU, ASIC | GPU, CPU, ASIC | GPU  (ASIC resistance) | GPU, CPU | GPU |
| **Đặt lại độ khó** | 2016 khối | 2016 khối |  |  |  |
| **Tác giả** | Satoshi Nakamoto | Charles Lee | **Vitalik Buterin.** | Wladimir J. Van der Laan | Evan Dufield |
| **Ngày tạo ra** | 3/01/2009 | 7/10/2011 | 30/06/2015 | 18/04/2014 | 3/2015 |