# How to bitcoin work

BITCOIN ĐƯỢC Miêu tả là tự do trong tự nhiên, nhưng không phải tất cả các nhà tự do và những người ủng hộ đồng tiền được hỗ trợ bằng vàng đánh giá cao nó tuy nhiên, và một số, trên thực tế, chủ động xem thường nó. Theo kinh nghiệm của chúng tôi, một số khái niệm cơ bản liên quan đến Bitcoin không được hiểu rõ bởi những điều này. Để hiểu đầy đủ về Bitcoin, hiểu biết và, cũng như quan trọng, triết lý tại sao nó hoạt động là điều thiết yếu. Một hệ thống phân phối bao gồm nhiều nhóm khác nhau và được quản lý bởi một vài cá nhân đồng thời duy trì tính toàn vẹn của nó và tránh tình trạng "Garry Hardtin" bi kịch của Garena? Trong điều kiện kinh tế này, các cá nhân, hành động một cách độc lập và hợp lý theo sở thích, hành xử trái ngược với lợi ích tốt nhất của cả nhóm bằng cách cạn kiệt nguồn lực chung. Một ví dụ điển hình là nơi một nhóm nông dân chia sẻ một đồng cỏ chung để chăn thả gia súc của họ. Việc lạm dụng và cạn kiệt nguồn tài nguyên thông thường, đồng cỏ, có thể xảy ra vì nó không phải là lợi ích cá nhân của một nông dân để bảo tồn nó bằng cách hạn chế tiêu thụ gia súc của gia súc.  
  
Hãy bắt đầu bằng một cuộc thảo luận về cách Bitcoin hoạt động. Để đánh giá và hiểu hầu hết cuốn sách này, một số hiểu biết cơ bản về các khái niệm chính của Bitcoin là cần thiết. Chương này sẽ cung cấp và sẽ kết luận với một quan điểm về lý do tại sao Bitcoin, như một hệ thống thanh toán, đã được chứng minh cho đến nay là một giải pháp khả thi. Để hoàn thành cuộc thảo luận của chúng tôi, chúng tôi sẽ giải thích các ý nghĩa kinh tế của Bitcoin.  
  
Ở cốt lõi của nó, Bitcoin kết hợp các khái niệm sau:  
  
• Sổ cái công cộng (gọi là chuỗi khối của Bitcoin). Hãy xem xét điều này như một quyển sách khổng lồ được công bố rộng rãi và có sổ sách kế toán của tất cả các giao dịch đã từng được thực hiện trong hệ thống Bitcoin, với các trang mới liên tục được thêm vào.  
  
• Một thuật toán mật mã được gọi là mã hóa bất đối xứng được sử dụng để ủy quyền cho các giao dịch.  
  
• Mạng lưới phân phối các nút máy tính (thường được gọi là thợ mỏ) xác minh và xác nhận các giao dịch Bitcoin và cập nhật sổ cái công cộng.  
  
Hãy khám phá những khái niệm này một cách chi tiết hơn.

## Chuỗi khối của Bitcoin: sổ sách kế toán công cộng

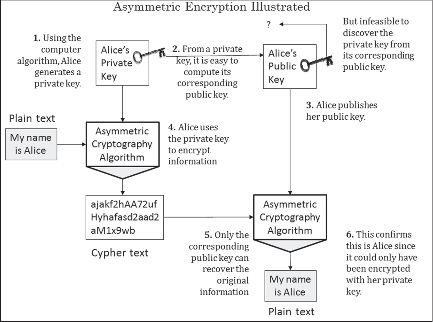
Tất cả các thành viên của mạng Bitcoin chia sẻ sổ cái công cộng, chuỗi khối. Hãy tưởng tượng một cuốn sách kế toán khổng lồ với mỗi trang liệt kê một loạt các giao dịch. Một trang mới có chứa các giao dịch Bitcoin mới nhất được gửi bởi người trả tiền trên toàn thế giới được thêm vào khoảng xấp xỉ 10 phút. Cuốn sách khổng lồ này thường xuyên có trên Internet cho bất cứ ai điều hành phần mềm Bitcoin. Lưu ý rằng các chương trình phần mềm được gọi là Ví điện tử Bitcoin có thể chạy trên điện thoại thông minh hoặc máy tính cá nhân và cho phép người dùng thanh toán qua mạng Bitcoin.  
  
Trong ngữ cảnh của Bitcoin, các trang tạo thành sổ cái được gọi là khối vì chúng đại diện cho "khối" của dữ liệu. Chuỗi khối, bao gồm nhiều khối riêng biệt, phát triển liên tục về chiều dài và chứa tất cả các giao dịch được thực hiện trong Bitcoin kể từ khi nó ra mắt vào tháng 1 năm 2009.  
  
Yêu cầu giao dịch Bitcoin bao gồm:  
  
   
  
1. Địa chỉ Bitcoin của người trả tiền, trong đó có chứa nguồn tiền để thanh toán,  
  
2. Địa chỉ Bitcoin của người nhận (người nhận thanh toán), và  
  
3. Số bitcoins đang được chuyển.  
  
   
  
Vì chuỗi cửa hàng chứa lịch sử thanh toán đi và đến liên quan đến địa chỉ Bitcoin của người trả tiền, những người khai thác mỏ cũng quản lý mạng Bitcoin có thể xác minh rằng người trả tiền có đủ tiền để trang trải thanh toán. Bất cứ lúc nào, bất cứ ai cũng có thể xem số lượng bitcoins liên quan đến (hoặc, một cách trừu tượng, giữ trong) bất kỳ địa chỉ cụ thể Bitcoin nào. Xem cho chính mình. Truy cập vào blockchain.info và nhập địa chỉ sau.

**1GaMmGRxKCNuyymancjmAcu3mvUnVjTVmh**

Trong "Search", số bitcoins liên quan đến địa chỉ này sẽ được trả lại.  
  
Mặc dù danh tính của chủ sở hữu không thể biết được từ địa chỉ Bitcoin mà không cung cấp thông tin này, bất kỳ chuyển khoản nào trong và ngoài tài khoản của anh ta, cũng như số dư hiện tại của anh ta, đều được công bố công khai để xem.

## Mã hóa bất đối xứng: Ai sẽ chi tiêu những bitcoins

Khóa mã hoá được kết hợp với một giao dịch như được mô tả ở trên. Bitcoin sử dụng một hệ thống mã hóa bất đối xứng (còn được gọi là mật mã khoá công khai), được gọi là vì thuật toán mã hóa yêu cầu một cặp khóa, mỗi mã bao gồm một loạt các chữ số dài. Một là công khai và kiểm soát hoạt động giải mã, trong khi đó, khoá cá nhân, điều khiển hoạt động mã hóa hoặc ngược lại.  
  
Thuật toán tạo ra một khoá riêng và dễ dàng nhận ra khoá công khai tương ứng của nó. Tuy nhiên, việc xác định khoá riêng từ khoá công khai tương ứng là không khả thi về mặt tính toán, do đó cho phép khoá công khai, như tên của nó, được công khai. Với khoá công khai, người thụ hưởng có thể lấy thông tin giao dịch, cho phép chuyển các bitcoins để tiến hành. Hình 2 dưới đây mô tả khái niệm hệ thống khóa kép của Bitcoin, cung cấp một phần cơ sở cho hoạt động của Bitcoin.



Thuật toán của phần mềm Bitcoin chỉ cho phép chủ sở hữu của khóa cá nhân sử dụng bitcoins "chi tiêu" liên quan đến địa chỉ Bitcoin đó. Người nhận, hoặc người nhận tiền, chia sẻ địa chỉ Bitcoin của mình với người trả tiền. Vì chỉ có người nhận biết khóa riêng được liên kết với địa chỉ của mình, chỉ có anh ta mới có thể truy cập, chi tiêu, hoặc chuyển các bitcoins này sau.  
  
Trong Bitcoin, người gửi ký một chữ kí số một giao dịch Bitcoin với chìa khóa riêng của mình. Các giao dịch Bitcoin thực sự chứa khóa công khai (giả sử đây là địa chỉ Bitcoin bây giờ). Sử dụng khóa công khai này, hệ thống kiểm tra xem chữ ký số có hợp lệ và do đó xác nhận rằng người gửi thực sự là chủ sở hữu khóa riêng. Hệ thống này cho phép chủ sở hữu "chi tiêu" bitcoins liên quan đến địa chỉ Bitcoin của mình trong sổ cái công cộng và sổ cái công khai (tức là chuỗi khối) sẽ được cập nhật với một trang mới (tức là block) có chứa giao dịch này. Sự bổ sung của giao dịch mới này vào chuỗi khối một cách hiệu quả nói với mạng Bitcoin để ghi nhận những bitcoins này tới địa chỉ của người nhận và ghi chúng từ địa chỉ Bitcoin của người gửi. Khóa cá nhân được làm bằng hàng loạt chữ số được lưu trữ và quản lý bởi ví bảo mật Bitcoin được bảo vệ bằng mật khẩu (ví dụ: phần mềm trên máy tính của người dùng, thiết bị di động hoặc ứng dụng web khác).

## Một mạng lưới các thợ mỏ hoạt động như minters, bookkeepers, và regulators của hệ thống

Cho đến nay, chúng ta đã nói về những giao dịch như thế nào và cách chúng được xác nhận. Nếu Bitcoin là một hệ thống điều hành trung tâm, câu chuyện sẽ kết thúc ở đây: Một thực thể duy nhất sẽ chịu trách nhiệm cho nhiệm vụ này. Tuy nhiên, Bitcoin là một hệ thống phân cấp, và, như vậy, nhiệm vụ này được chia sẻ giữa một tập hợp các nút tự nguyện tham gia (thợ mỏ) phân phối trên toàn thế giới. Hiểu được một hệ thống bao gồm sổ sách kế toán và ủy quyền chuyển khoản thanh toán có thể được thực hiện bởi các thực thể khác nhau như thế nào để hỗ trợ cho lợi ích của chính mình là cần thiết. Tính năng này của hệ thống là một trong những hiểu biết chính mà tôi đã ám chỉ trước đây như là một trong những điều mà thường xuyên bị bỏ sót bởi các nhà phê bình Bitcoin.  
  
Miners, các nút chịu trách nhiệm điều hành mạng Bitcoin, xác minh rằng các giao dịch là hợp lệ và cập nhật chuỗi khối với các khối mới bao gồm các giao dịch mới nhất trên cơ sở thường xuyên. Phần mềm Bitcoin do các thợ mỏ khai thác trên các máy tính cá nhân của họ kết hợp giao thức Bitcoin với các quy tắc và thỏa thuận.  
  
Nhìn chung, mạng Bitcoin yêu cầu chuỗi tài nguyên (sổ kế toán công cộng) được cập nhật liên tục với việc bổ sung các khối mới (các trang trong sổ sổ cái). Khoảng 10 phút một lần, một khối mới được thêm vào với danh sách các giao dịch mới nhất. Mặc dù tất cả các thợ mỏ đang làm việc trên khối tiếp theo, chỉ có một sẽ được chọn để có phiên bản cụ thể của khối được thêm vào chuỗi khối. Thật vậy, mỗi người khai thác mỏ đang hoạt động vì lợi ích riêng của mình khi ông tạo ra phiên bản riêng của khối tiếp theo và để cá nhân thu thập các khoản phí giao dịch liên quan đến khối giao dịch đó. Mặc dù các thông số cốt lõi của giao dịch Bitcoin không bị thay đổi (người trả tiền, người nhận thanh toán, số tiền), hầu hết trong số đó bao gồm phí giao dịch, do người trả tiền giải ngân và sẽ được ghi vào tài khoản của người khai thác mỏ mà khối được chọn để đưa vào chuỗi. Người khai thác mỏ này sẽ cập nhật mỗi giao dịch này và sẽ tính các khoản phí liên quan đến các giao dịch đó vào địa chỉ Bitcoin của riêng mình

Ngoài lệ phí giao dịch, các thợ mỏ có khối được thêm vào chuỗi khối cũng kiếm được khoản tín dụng bổ sung với bitcoins mới được đúc. Họ tạo ra một giao dịch bổ sung mà thêm vào tài khoản bitcoin riêng của họ. Đây được gọi là phần thưởng khôn. Hiện tại, giao thức Bitcoin cho phép các thợ mỏ tự phân bổ 25 bitcoins mới cho mỗi block được tạo ra. Đây là tổng số phí giao dịch. Ban đầu, tại thời điểm ra mắt của Bitcoin, 50 bitcoins (BTC) được phân bổ theo khối lượng mỗi block mỗi block, giảm khoảng một nửa mỗi 4 năm.  
  
Với các bitcoins mới được ghi có vào địa chỉ của ông, người khai thác mỏ mà phiên bản của khối được chọn để đưa vào chuỗi khối rõ ràng có lợi từ việc tìm ra giải pháp trước khi những người thợ mỏ của ông làm. Quá trình lựa chọn này hoạt động như thế nào sẽ sớm được giải thích. Bây giờ, tuy nhiên, xem nó như là giải quyết một vấn đề toán học bằng cách thực hiện một nhiệm vụ máy tính rất đắt tiền. Giải pháp rất khó tìm nhưng, một khi đã tìm thấy, tính chính xác của nó rất dễ kiểm chứng. Người khai quật đầu tiên tìm ra giải pháp cho khối của ông ta được phép xuất bản phiên bản này cho toàn bộ mạng lưới các thợ mỏ.  
  
Những thợ mỏ này nhận được khối và giải pháp của nó và sau đó làm việc để xác thực và xác nhận nó, nghĩa là, xác nhận rằng các giải pháp tìm thấy bởi người khai thác đầu tiên vào khối là chính xác. Giao thức Bitcoin thiết lập sự khó khăn của vấn đề theo cách mà trung bình khoảng 10 phút được yêu cầu để tìm ra giải pháp.

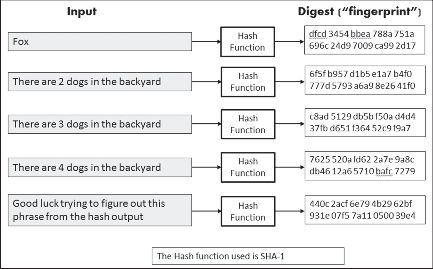
Nếu những người khai thác mỏ giải quyết được khối lượng này đã được cho phép với hơn 25 bitcoins mới được cho phép, các thợ mỏ khác sẽ từ chối khối nhà kho đó và sẽ tiếp tục tìm kiếm giải pháp cho các phiên bản của riêng họ. Mỗi khối là hơi khác nhau và do đó mỗi có một giải pháp khác nhau.  
  
Trong những gì có vẻ như phản trực giác, khi một thợ mỏ giải quyết được nhiệm vụ tính toán, tất cả các thợ mỏ khác đều chấp nhận thất bại, đồng ý bao gồm khối thợ mỏ này làm khối kế tiếp trong chuỗi khối với điều kiện nó có thể được xác nhận và bắt đầu làm việc trên khối tiếp theo. Công việc này liên quan đến việc mỗi thợ mỏ thêm vào tất cả các giao dịch gần đây nhất đã được đưa ra kể từ khi tạo khối trước đó sang một khối mới, và đến lượt nó sẽ được giải quyết và bổ sung vào chuỗi khối không bao giờ kết thúc

Cách thức hoạt động của Bitcoin giải thích tại sao người khai thác mỏ đầu tiên tìm ra giải pháp sẽ tự tín dụng mình với số lượng phần thưởng khối được cho phép bởi giao thức Bitcoin. Làm như vậy đảm bảo chấp nhận khối của ông ta bởi những người khai thác mỏ khác và nhận các phần thưởng liên quan (tức là phí giao dịch). Tương đương, các thợ mỏ khác không đạt được lợi ích bằng cách từ chối khối này mặc dù nó là hợp lệ. Hệ thống thanh toán Bitcoin sẽ chỉ giữ giá trị khi nó hoạt động bình thường. Nếu các thợ mỏ đã từ chối tất cả các khối nhưng họ là của riêng, không có sự đồng thuận nào sẽ đạt được, giá trị của toàn bộ hệ thống sẽ bị phá hủy, và không ai trong số các thợ mỏ sẽ có thể được hưởng lợi. Trong trường hợp như vậy, bất kể số lượng bitcoin mà các thợ mỏ giữ sẽ trở nên vô giá trị. Vì vậy, tất cả các thợ mỏ đều được hưởng lợi nếu tất cả đều tôn trọng các giao thức Bitcoin được thành lập trong phần mềm Bitcoin chia sẻ. Do đó, Bitcoin thể hiện sự nghịch đảo của bi kịch của các cộng đồng được mô tả trước đó.

Bây giờ chúng ta hãy nghiên cứu kỹ các chi tiết của những gì chúng ta đã mô tả trước đây như là công việc tính toán đắt tiền cần thiết để giải quyết vấn đề toán học của một khối. Đối với một người khai thác mỏ để có khối của mình được lựa chọn, ông phải có giải quyết được một vấn đề liên quan đến khối. Quá trình lựa chọn này được gọi là "bằng chứng của tác phẩm" vì nó ngụ ý rằng người thợ mỏ phải làm việc đó. Để hiểu đầy đủ cơ chế liên quan, trước tiên chúng ta cần hiểu khái niệm mật mã được biết đến như là một hàm băm. Sau đó, chúng ta có thể giải thích nó được sử dụng như thế nào trong bối cảnh chứng từ của người khai thác mỏ.

## Chức năng băm mật mã - một "dấu vân tay" kỹ thuật số

Băm mật mã là một thuật toán phức tạp thực hiện một văn bản chuyển đổi nhiệm vụ rất cơ bản với độ dài bất kỳ (một toàn bộ cuốn sách, một tài liệu, một câu, hoặc thậm chí một từ đơn) thành một chuỗi các số ngẫu nhiên có chiều dài ngẫu nhiên xuất hiện ngẫu nhiên. Hình 3 sau đây cung cấp một số ví dụ. Đầu ra của một hàm băm, hoặc đơn giản là băm, thường được gọi là tiêu đề thư và có thể được coi là "dấu vân tay" của tài liệu.



Trong hình trên, lưu ý rằng đầu vào "Có 2 con chó ở sân sau" dẫn đến tiêu hóa hoàn toàn khác với "Có 3 con chó ở sân sau". Đơn giản chỉ cần thay đổi một ký tự dẫn đến kết xuất với tất cả các chữ số hoàn toàn khác nhau. Các kết quả tiêu hóa trong con số này được thể hiện dưới dạng số thập lục phân. Không giống như hệ thống thập phân mà chúng ta thường sử dụng, hệ thập lục phân có 16 cơ sở. Nó sử dụng mười sáu biểu tượng để biểu diễn mười sáu số trong hệ thống. Các ký hiệu từ 0 đến 9 đại diện cho các số từ 0 đến 9, và các chữ cái từ A đến F đại diện cho số từ 10 đến 15. Như vậy số thập lục phân F đại diện cho số 15. Vì vậy số thập lục phân 5A36 bằng (5 x 163) + (10 x 162 ) + (3 x 161) + (6 x 160), bằng hệ số thập phân, đến 23.094. Thử nghiệm với việc chuyển từ Hex đến Dec trên máy tính của máy tính của bạn để xem nó hoạt động như thế nào.

Một người dùng Bitcoin không kiểm soát được kết quả đầu ra (tiêu hóa trong hình 3). Ngoài ra, cho một đầu ra tiêu chuẩn cụ thể, việc tìm kiếm một đầu vào mà có thể tạo ra nó là gần như không thể. Vì vậy, tạo ra một tiêu hóa rất dễ dàng, nhưng bắt nguồn văn bản gốc từ tiêu hóa là không thể. Sử dụng dấu hiệu tương tự của dấu vân tay của con người, cho một dấu vân tay duy nhất, chúng tôi sẽ nhận thấy không thể xác định người rời khỏi đó trừ khi người đó đã được lấy dấu vân tay trước.

Trước đó chúng tôi đã đề cập rằng tất cả các thợ mỏ có thể dễ dàng xác minh rằng một giải pháp là chính xác một khi nó đã được tìm thấy nhưng việc tìm kiếm nó là một phần khó khăn. Đó là lý do tại sao băm mật mã là lý tưởng cho mục đích của Bitcoin. Người khai thác mỏ, trong nỗ lực giải quyết khối, phải tạo ra một mẫu cụ thể được hiển thị bởi nội dung của tiêu hóa. Vì sao chép một đầu ra cụ thể trong tiêu hóa là không thể, chúng phải tăng một chữ số trong văn bản và tính toán lại băm cho đến khi chúng vấp ngã theo mô hình cụ thể trong tiêu hóa được yêu cầu bởi giao thức Bitcoin. Quá trình này tương tự như việc thay đổi số lượng chó ("2 con chó", "3 con chó", "4 con chó") trong ví dụ trong Hình 3 để tạo ra các tiêu hóa khác nhau. Ví dụ, nói rằng các giao thức Bitcoin hiện tại quy định rằng các nội dung của tiêu hóa hiển thị một mô hình bắt đầu với "00". Bằng cách thay đổi số lượng chó trong ví dụ, số hệ thập lục phân tương ứng trong tiêu hóa cuối cùng sẽ đáp ứng yêu cầu này, chỉ ra một giải pháp cho khối.  
  
Những người khai thác mỏ tìm kiếm giải pháp thường phải tính toán băm hàng triệu lần để tìm đúng mô hình, nhưng chỉ cần một phép tính băm đơn bởi những người khai thác mỏ khác là cần thiết để xác nhận nó một khi nó được tìm thấy.

Thuật toán băm của Bitcoin, tạo ra nội dung của tiêu hóa từ văn bản đầu vào, làm cho hệ thống được mô tả ở trên. Do đó, một hàm băm mật mã lý tưởng có bốn tính chất chính1:  
  
   
  
• Tính giá trị băm tương ứng với bất kỳ thông điệp nào là đơn giản.  
  
• Tạo ra một thông điệp có một băm nhất định là không thể.  
  
• Sửa đổi một tin nhắn mà không thay đổi băm là không thể.  
  
• Tìm ra hai thông điệp khác nhau có cùng một hàm băm là không thể.

Ví dụ sau, lấy từ Wikipedia, minh họa chức năng băm sử dụng.  
  
Alice đặt ra một vấn đề khó khăn toán học cho Bob và tuyên bố cô đã giải quyết nó. Bob muốn tự mình thử, nhưng cũng muốn đảm bảo rằng Alice không lừa gạt. Do đó, Alice viết ra giải pháp của mình, tính toán băm của nó và cho Bob biết giá trị băm (trong khi giữ bí mật giải pháp). Sau đó, khi Bob tự giải quyết vấn đề này vài ngày sau đó, Alice có thể chứng minh rằng cô đã có giải pháp trước đó bằng cách tiết lộ nó và có Bob băm nó và kiểm tra xem nó có phù hợp với giá trị băm đã trao cho anh ta trước đây. (Đây là một ví dụ về một kế hoạch cam kết đơn giản, trong thực tiễn thực tế, Alice và Bob sẽ là các chương trình máy tính, và bí mật sẽ là một cái gì đó không dễ dàng giả mạo hơn là giải pháp câu đố được tuyên bố).

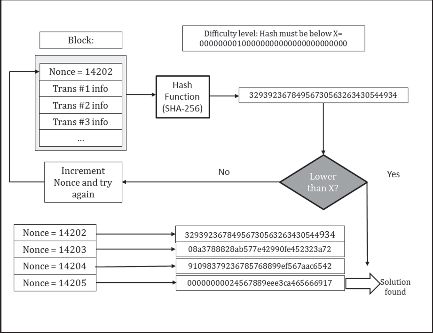
Các hàm Hash tạo thành một phần của tiến trình cho phép người dùng ký một văn bản hoặc văn bản trong Bitcoin. Trong bối cảnh công việc bằng chứng của Bitcoin, sẽ được thảo luận dưới đây, hai đặc tính hữu ích nhất của các hàm băm là:  
  
   
  
• Không thể tạo ra một thông điệp từ một hash nhất định  
  
• Tạo ra một hash hoàn toàn mới bằng cách thay đổi chỉ một ký tự trong tin nhắn  
  
   
  
Một số thuật toán hash đã được tạo ra, và Bitcoin sử dụng hai trong số chúng: SHA-256 cho chứng nhận của công việc và RIPEMD-160 cho địa chỉ Bitcoin. Hàm băm là trọng tâm của chứng minh của tác phẩm, và chúng ta sẽ thảo luận tiếp theo.

## Miner’s Proof of work

Vào bất kỳ thời điểm nào, mỗi người khai thác mỏ đều tích cực tham gia vào việc tạo ra khối tiếp theo để thêm vào chuỗi khối bằng cách giải quyết một vấn đề khó khăn, được gọi là bằng chứng của công việc. Người khai thác đầu tiên để giải quyết công việc bằng chứng được thưởng bằng những bitcoin tươi mới (25 bitcoins như trong văn bản này) và với các khoản phí giao dịch tích luỹ liên quan đến các giao dịch trong khối được tạo ra. Phí giao dịch, thường là một khoản tiền danh nghĩa, được người trả tiền thêm vào khi họ gửi các giao dịch. Đến khoảng năm 2140, tất cả các bitcoins sẽ được khai thác, và các thợ mỏ sẽ được khen thưởng hoàn toàn với phí giao dịch.

Bằng chứng của tác phẩm có thể được coi như là một cuộc chạy đua giữa các thợ mỏ mỏ để khám phá ra băm SHA-256 của khối mà họ đang cố tạo ra sẽ có một đặc tính nhất định. Như chúng ta đã thấy ở trên, sản lượng băm chỉ đơn giản là một số lượng lớn được thể hiện theo hệ thập lục phân. Mục tiêu của người khai thác, vấn đề phải được giải quyết, đó là tạo một đầu ra băm dưới một giá trị nhất định. Người khai thác đầu tiên tính toán giá trị có đặc tính này sẽ thắng, và phiên bản của khối sẽ, sau khi xác nhận bởi các thợ mỏ khác, sẽ được thêm vào chuỗi khối được thảo luận ở phần đầu của chương này.  
  
Để đơn giản, hãy tưởng tượng rằng sản lượng băm thực sự là một số từ 0 đến 1.000.000 và rằng người khai thác đầu tiên để có được sản lượng băm dưới 10.000 thắng. 10.000 hoạt động như một ngưỡng, và mỗi khối trong Bitcoin chứa một số có mục đích duy nhất là để có được ngưỡng.

Số trong khối Bitcoin được kiểm tra so với giá trị ngưỡng được gọi là "nonce". Mỗi thợ mỏ tăng nonce của mình bằng một lượng nhất định cho đến khi sản lượng băm cho khối của nó là dưới ngưỡng. Như chúng ta đã nói ở trên, mỗi block của người khai thác mỏ có những thông tin khác nhau và do đó một kết quả đầu ra băm khác nhau cho cùng một "nonce". Quá trình này được minh họa trong Hình 4.



Giao thức Bitcoin, được vận hành bởi phần mềm chạy trên mỗi máy tính của người thợ mỏ, điều chỉnh mức độ khó khăn của vấn đề để mất khoảng 10 phút trước khi người thợ mỏ đầu tiên giải quyết nó. Mục đích là để có chuỗi khối được cập nhật thường xuyên với một khối mới có chứa các giao dịch mới nhất được gửi trong 10 phút trước. Giá trị này hơi tùy tiện và, như sẽ được thấy trong các chương sau, Satoshi đã dành một số cuộc thảo luận của mình cho chủ đề này.  
  
Thảo luận trước đây so sánh nonce với ngưỡng. Bởi vì các số của băm, được gọi là bằng chứng của tác phẩm, nằm trong hệ số thứ sáu thập lục phân, hoặc số 16, sẽ chuyển thành X số đầu tiên là số 0, trong đó X được điều chỉnh theo định kỳ để giữ mức độ khó khăn các bằng chứng của việc tương đối ổn định.

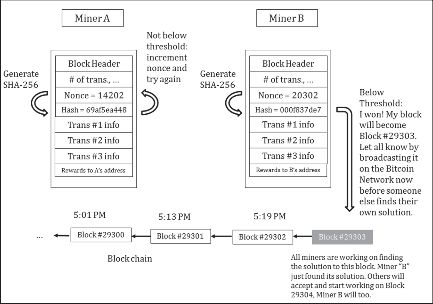
Ví dụ, giả sử rằng khối # 282,435 của chuỗi khối có đầu ra SHA-256 sau đây:

0000000000000000c6647dad26b01b28f534223450d75d3b6b2882855039b673

Nhớ lại rằng trong hệ thống số 16 cơ sở, có các ký hiệu đại diện cho mười sáu số từ 0 đến 15; các ký hiệu đại diện cho 0 đến 9 trong hệ thống này từ 0 đến 9 như trong thập phân, hoặc cơ sở 10, hệ thống, và các số 10 đến 15 của hệ thống hex được đại diện bởi A đến F. Số thập lục phân ở trên là 64 ký số. Vì các thuật ngữ bên trái trong một số thập lục phân đại diện cho số mũ cao hơn của 16 vì thế số lớn hơn, để làm cho đầu ra băm nhỏ hơn, các chữ số hàng đầu trong sản lượng băm phải là 0. Đó là lý do tại sao nói rằng sản lượng băm phải dưới một một ngưỡng nhất định được dịch là có một số các chữ số hàng đầu nhất định 0. Được xem bằng cả hai cách, bằng chứng là tìm ra một nonce sẽ tạo ra một đầu ra băm dưới ngưỡng được thiết lập bởi giao thức Bitcoin vào thời điểm đó.

Trong ví dụ trong hình 4, minh chứng của minh chứng, chỉ với mười sáu chữ số đầu tiên của đầu ra bằng 0 có thể sản lượng băm giảm xuống dưới ngưỡng thiết lập bởi giao thức của Bitcoin. Do đó, người khai thác mỏ có số này lần đầu tiên và do đó "won" khối đó đã phải tiếp tục thay đổi số "nonce" cho đến khi một số thập lục phân có ít nhất số lượng mong muốn của hàng đầu 0s được tạo ra. Như trong một cuộc xổ số, các thợ mỏ thường mua nhiều nhất "vé" (tức là tạo ra nhiều sản lượng SHA-256) có cơ hội tốt hơn để tìm một con số có đúng số 0s. Yêu cầu này của hệ thống Bitcoin đã dẫn đến một cuộc đua để tạo ra phần cứng có khả năng tạo ra nhiều băm / giây. Người khai thác may mắn lần đầu tiên phát hiện ra băm cho khối # 282,435 của chuỗi khối tăng số nonce lên 505,482,605 theo thập phân, có nghĩa là người thợ mỏ này phải tạo ra hơn 500 triệu "hash" trước khi tìm ra một con số đúng với số zeroes hàng đầu.

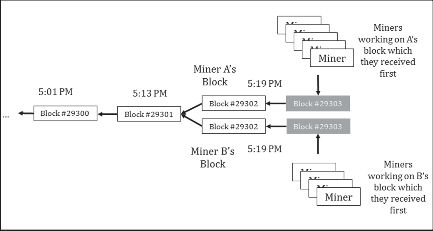
Như đã nói trước đây, mục tiêu của giao thức Bitcoin là tạo ra một khối các giao dịch tạo ra khoảng 10 phút một lần. Đối với một mức độ khó nhất định, nếu có nhiều thợ mỏ tham gia - hoặc chính xác hơn, vì nhiều khối hơn nữa được tính toán trong mỗi giây - cơ hội phát hiện ra tiêu chuẩn bắt buộc (sản lượng băm) trong ít hơn 10 phút tăng. Sau một số khối nhất định, giao thức Bitcoin đánh giá tốc độ khối được tạo ra như thế nào; nếu trung bình ít hơn 10 phút, mức độ khó khăn sẽ tăng lên (tức là, số lượng 0 hàng đầu tăng lên, giảm xác suất của bất kỳ người khai thác mỏ nào có được tiêu hóa có đặc tính đó); nếu lâu hơn, khó khăn sẽ giảm (tức là, số lượng hàng đầu giảm 0, làm tăng khả năng có được nó).  
  
Khi người khai thác phát hiện ra một nonce cung cấp sản lượng băm chính xác, khối được phát, và các thợ mỏ khác xác minh nó, chấp nhận nó, và bắt đầu làm việc trên khối tiếp theo. Như vậy, Bitcoin hoạt động như một trò chơi xổ số liên tục đang khởi động lại mỗi 10 phút. Ai sẽ là người may mắn để tìm một nonce với các đặc điểm chính xác?



## Miners’ consensus & orphan blocks

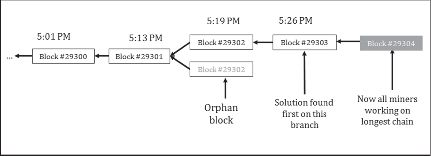
Như đã nói trước đó, Bitcoin dựa chủ yếu vào sự đồng thuận để hoạt động. Khái niệm này, sẽ được thảo luận thêm trong Chương 9, có hiệu lực khi hai thợ mỏ giải quyết các khối của họ cùng một lúc. Khi điều này xảy ra, hai thợ mỏ đều phát tán các khối của họ bao gồm các giải pháp trên hệ thống Bitcoin. Tất cả các thợ mỏ khác nhận và giữ lại cả hai nhưng công việc của họ trên khối tiếp theo của họ sẽ được dựa trên hai khối hiện tại họ nhận được đầu tiên. Nói 50% các thợ mỏ nhận được khối từ Miner A đầu tiên và những người khác nhận được Blade B của khối đầu tiên. Tình huống này được minh họa cho khối # 29302 trong Hình 6 dưới đây.

Tình huống này tương tự như một cuộc đua đi làm thêm giờ. Mà trong hai khối trở thành một phần của chuỗi khối đúng sẽ phụ thuộc vào tốc độ khối tiếp theo được giải quyết và ai, người khai thác mỏ nhận khối A hoặc người nhận khối B. Tại thời điểm này, có hai phiên bản của chuỗi khối tồn tại, với một nửa các thợ mỏ có phiên bản của một nhà khai thác A của khối # 29302 và một khác có phiên bản của thợ mỏ B. Trong hai phiên bản này sẽ tồn tại phụ thuộc vào phiên bản người khai thác giải quyết khối kế tiếp, # 29303 trong Hình 6, đã có trên máy tính của mình. Khi chặn # 29303 được giải quyết, phiên bản này của chuỗi chặn sẽ trở thành dài nhất của hai và do đó chính thức. Tất cả các thợ mỏ sau đó thả các phiên bản khác của chuỗi khối, mà trở thành những gì được biết đến như là một khối mồ côi. Quá trình này được minh họa trong Hình 7.



## Why does Bitcoin work?

Cho đến nay, chúng tôi đã đề cập đến cách Bitcoin hoạt động, nhưng không phải tại sao. Để hiểu được điều này, cần phải có kiến thức về một số khái niệm bổ sung, ví dụ như phần mềm nguồn mở. Những khái niệm này như sau và được giải thích dưới đây:



• Bitcoin là phần mềm mã nguồn mở.

• Phần mềm Bitcoin thiết lập các chỉ thị hoạt động mà các thợ mỏ và khách hàng ví tiền phải tuân theo.  
  
• Phần mềm Bitcoin cũng định nghĩa và vận hành một giao thức truyền thông.  
  
• Chia sẻ tập tin chia sẻ của chuỗi khối cho phép mở sổ sách kế toán mở.

Phần mềm nguồn mở là phần mềm máy tính có sẵn mã nguồn cho mọi người xem. Hơn nữa, nó hoạt động dưới một giấy phép đặc biệt cho phép bất cứ ai sửa đổi và sử dụng nó. Với mã nguồn, một lập trình viên có thể tái tạo lại chương trình (tệp nhị phân chạy trên máy tính) và sửa đổi nó theo ý thích. Do đó đã nảy sinh nhiều người bắt chước Bitcoin, các đồng tiền ảo khác với nó chỉ có tính thẩm mỹ, và phần lớn, không bao gồm các cải tiến đáng kể, ngoại trừ một số ít như Namecoin. Phần lớn các loại tiền tệ ảo thay thế này dựa trên việc thay đổi tỷ lệ tạo ra khối, tổng số đồng xu trong lưu thông, và thuật toán băm mật mã được sử dụng.

Mã của phần mềm là mã nguồn mở cho phép một chuyên gia phân tích nó và để xác nhận tính toàn vẹn của nó, nghĩa là xác nhận rằng nó thực hiện những gì nó muốn làm. Một ví dụ nổi bật về phần mềm nguồn mở là Linux, đã di dời Microsoft Windows trong thị phần trong ngành công nghiệp máy chủ. Bởi vì nó là mã nguồn mở, các vấn đề được tìm thấy và được sửa chữa nhanh hơn nhiều so với nếu nó độc quyền vì nhiều lập trình đang liên tục kiểm tra và cải tiến mã. Linux cho đến nay đã chứng minh rằng sự tốt đẹp và tự tin hơn có thể làm việc trong buổi hòa nhạc, ít nhất là đối với việc quản lý phần mềm nguồn mở. Sự mở cửa này đảm bảo mức độ toàn vẹn cao không thể đạt được trong phần mềm độc quyền, chỉ có danh tiếng của công ty chịu trách nhiệm về phần mềm đảm bảo rằng nó thực hiện những gì nó được cho là làm.

Bitcoin cũng hoạt động trên Internet bằng cách sử dụng một giao thức xác định các hoạt động mà các thợ mỏ và khách hàng ví tiền phải tuân theo. Wallet Client - các chương trình phần mềm là các ứng dụng trên điện thoại thông minh hoặc các chương trình trên máy tính cá nhân - là những gì được sử dụng khi ai đó gửi một giao dịch thanh toán, mà các thợ mỏ sau đó xác nhận trước khi được kết hợp trong chuỗi chặn. Một người đào mỏ đơn lẻ lệch lạc từ giao thức sẽ bị các công nhân mỏ khác từ chối hoạt động và sẽ không được phép đóng góp vào hoạt động của mạng.  
  
Một cuộc tranh luận điển hình chống lại Bitcoin liên quan đến giới hạn số lượng bitcoins tối đa sẽ được tạo ra, mà Satoshi Nakamoto đặt ở mức 21 triệu. Một khi đạt được, những gì có thể ngăn cản một ai đó tăng giới hạn này? Không có gì thực sự, nhưng anh ta cần sự hợp tác của đa số thợ mỏ để thay đổi này được chấp nhận. Thậm chí phần lớn các thợ mỏ cũng đồng ý dỡ bỏ hạn chế này, nếu không đồng ý thì sẽ có một sự chia rẽ trong chuỗi cửa khẩu. Những người ủng hộ việc nâng hạn chế sẽ sử dụng một phiên bản của chuỗi chặn trong khi những người không ủng hộ sẽ sử dụng một phiên bản khác. Có hiệu quả, chúng ta sẽ có hai loại tiền tệ ảo chứ không phải là một, "Bitcoin ban đầu" và "Bitcoin Định lượng gia tăng". Về lâu dài, một trong những sẽ giữ giá trị của nó lâu hơn và tốt hơn và do đó sẽ trở thành phiên bản ưa thích, trong khi khác sẽ giảm giá trị. Điều gì sẽ được bạn đoán là một trong những sẽ giữ giá trị của nó lâu hơn và giữ lại sự quan tâm của người sử dụng Bitcoin? Cá nhân, tôi có một ý tưởng rất tốt mà một.  
  
Cộng đồng phát triển Bitcoin rất thận trọng về những thay đổi, và, ít nhất cho đến nay, các phương tiện được ưa chuộng để thay đổi lớn là tạo ra các loại tiền tệ ảo mới, một số không có giới hạn về số lượng đồng xu.

Một đặc điểm cuối cùng củng cố Bitcoin là, không chỉ là phần mềm mã nguồn mở, mà còn là kế toán của nó. Một số đã được gọi là chuỗi khối "kế toán gấp ba" như nó revolutionizes kế toán. Bất cứ ai cũng có thể kiểm tra chuỗi khối và xác minh rằng kế toán không tuân theo yêu cầu hiện tại và các yêu cầu kỹ thuật của giao thức Bitcoin. Việc chia sẻ tập tin chia sẻ của chuỗi khối có nghĩa là bất cứ ai chạy phần mềm Bitcoin được kết nối với mạng Bitcoin và có quyền truy cập vào chuỗi khối.  
  
Để hiểu rõ hơn về sự sáng tạo của nền tảng khái niệm của Bitcoin, tôi khuyên bạn nên đọc sách trắng của Satoshi Nakamoto. Thông tin tôi cung cấp ở đây nên làm cho bài báo dễ tiếp cận hơn. Bản sao của bài báo này được đưa vào cuối cuốn sách này.

## Implications of Bitcoin

Tác động của Bitcoin như một hệ thống tiền tệ là rất lớn. Một lợi thế là khả năng nó cho phép mọi người "đổ tiền" tiền tệ trên khắp hành tinh như đơn giản chỉ là gửi email. Điều này đặc biệt thuận lợi cho người lao động nhập cư muốn gửi tiền cho người thân ở nước xuất xứ. Ngược lại, các công ty chuyển tiền qua biên giới đòi phí cao để làm như vậy. Có những khoản phí liên quan đến chuyển đổi từ tiền tệ quốc gia sang BTC và ngược lại, nhưng lệ phí chuyển đổi này rất nhỏ so với chi phí đấu nối dây.

Một lợi ích khác được đề cập trước đó là mua sắm trực tuyến và các khoản đóng góp trực tuyến. Tôi tin tưởng rằng hệ thống thanh toán bằng thẻ tín dụng hiện tại sẽ được thay đổi hoàn toàn trong tương lai. Thanh toán bằng thẻ tín dụng đòi hỏi phải có nhiều thông tin về người trả tiền, bao gồm địa chỉ thanh toán và mã 3 chữ số ở mặt sau của thẻ tín dụng. Về bản chất, đây là Bitcoin tương đương với việc cấp chìa khóa mã hóa cá nhân của bạn cho người bán. Số lượng gian lận cao do sự yếu kém về bảo mật này đã thể hiện ở mức phí cao và khoản bồi hoàn mà thương nhân phải đối mặt. Các công ty thẻ tín dụng dành một khoản tiền lớn mỗi năm để đối phó với các khoản phí gian lận. Những chi phí này được chuyển giao cho các thương gia, những người lần lượt chuyển cho người tiêu dùng thông qua giá cả cao hơn cho hàng hoá và dịch vụ.

Một tác động lớn khác của Bitcoin là trên mặt tiền, cụ thể là khả năng của hệ thống để được tiền và không chỉ là một loại tiền tệ. Một loại tiền tệ có các thuộc tính sau đây1:  
  
   
  
• Là một phương tiện trao đổi (được sử dụng như một trung gian trong thương mại)  
  
• Là một đơn vị tài khoản (có thể được đếm, có thể định lượng)  
  
• Độ bền (dài)  
  
• Chia hết (để có các đơn vị nhỏ hơn)  
  
• Là xách tay (để có thể vận chuyển dễ dàng)  
  
• Là có thể thay thế được (có thể hoán đổi lẫn nhau, 1 đơn vị giá trị cụ thể có thể thay thế một đơn vị khác giống nhau)

Tiền có tất cả các tài sản được liệt kê ở trên và, ngoài ra, một trong những khác:  
  
• Khả năng duy trì giá trị của nó trong dài hạn.  
  
Không giống tiền, một loại tiền tệ chịu lạm phát. Vào đầu những năm 1900, lạm phát được định nghĩa đơn giản là hành động bơm phồng lên một cái gì đó, như trong trường hợp của đồng tiền, bằng cách in thêm. Từ điển của ngày hôm nay định nghĩa nó như một sự tăng giá chung. Tuy nhiên, giá cả gia tăng là một triệu chứng của đồng tiền mất giá, nó xảy ra khi nó có nhiều hơn trước đây. Điều thú vị nhưng không đáng ngạc nhiên là sự chuyển đổi này theo định nghĩa tương ứng với thời điểm mà các đồng tiền giấy trở nên xa hơn và xa hơn nữa từ vàng và bạc, một sự phát triển dẫn tới giá cao hơn. Tổ tiên của chúng tôi đã thấy, ví dụ, giá lương thực hầu như không đổi trong suốt thời gian sống của chúng. Tuy nhiên, dân số ngày nay đã được điều kiện để xem giá cả gia tăng như một thực tế không thay đổi của cuộc sống, như lực hấp dẫn. Nó như thể, ở nơi mà trời mưa mọi lúc, không ai có mối liên hệ giữa đám mây và mưa. Nhưng ai có thể đổ lỗi cho họ vì họ chưa bao giờ nhìn thấy bầu trời xanh? Theo cách tương tự, hầu hết mọi người ngày nay không nhận thức được giá lương thực tăng cao do lạm phát tiền tệ, đôi khi còn kéo dài nhiều năm vì giá cả tăng lên tự biểu hiện. Đây là trường hợp lạm phát tiền tệ của những năm 1960 chỉ biểu hiện trong thập kỷ tiếp theo, những năm 1970.

Để duy trì sức mua của mình trong thời gian dài (tức là, để không phải chịu lạm phát), nguồn cung tiền phải được giới hạn. Vàng và bạc là tiền của sự lựa chọn trong hàng ngàn năm. Nguồn cung cấp của họ trên hành tinh này là rất hạn chế và đòi hỏi bất kỳ ai có ý định mua thêm nó để trao đổi năng lượng và thời gian cho họ thông qua khai thác mỏ. Bạn có thể nói rằng nỗ lực khai thác một kim loại quý là tương tự như chứng minh của công việc trong hệ thống Bitcoin. Trái ngược với công việc thực tế này chỉ với việc in nhiều hóa đơn hơn. Tiền giấy ban đầu được thông qua để chỉ hành động như là một sự thay thế thuận tiện (phái sinh) cho kim loại quý, do đó tạo điều kiện thuận lợi cho các giao dịch. Đồng tiền giấy, dễ lặp lại, luôn bị lạm phát, vì các thợ thủ công thợ bạc - và sau đó là các ngân hàng - đã sử dụng ngân hàng dự trữ phân đoạn để cho vay nhiều hơn (nghĩa là in thêm tiền giấy) hơn là thực sự có vàng trong kho. Điều này đã dẫn tới những cuộc "khủng hoảng ngân hàng" thường xuyên xảy ra trong các cuốn sách lịch sử.

Trước khi sự ra đời của máy tính và mạng lưới, các giao dịch đã được giới hạn trong kim loại quý và tiền tệ giấy. Kể từ đó, truyền thông điện tử đã giới thiệu một cách mới để thực hiện các giao dịch mà vàng và bạc không bao giờ có thể là một phần trực tiếp. Cho đến nay, chỉ có các loại tiền tệ có thể chuyển đổi qua trung tâm và có thể chuyển đổi bằng điện đã tồn tại, cho phép các nhà kiểm soát tự do quyết định việc quyết định kích cỡ của nguồn cung tiền tệ cơ bản. Tổng thống Nixon đã chứng minh điều này một cách rõ ràng khi ông ta loại bỏ khả năng chuyển đổi của đô la sang vàng trên các thị trường ngoại hối. Cuộc chiến tranh Việt Nam và "xã hội vĩ đại" của Lyndon Johnson được tài trợ bằng cách làm suy yếu đồng đô la Mỹ thông qua báo in điện tử. Phải mất thời gian để tự biểu lộ thông qua việc tăng giá hàng hóa, nhưng một khi nó đã làm, giá vàng bằng đô la đã có hiệu quả cao hơn mức giá cố định 35 đô la một ounce vàng chiếm ưu thế trước khi đô la bị hủy liên kết khỏi tiêu chuẩn vàng. Sau đó, nó trở thành một loại tiền tệ tự do trôi, liên tục bơm hơi, giống như bất kỳ đồng tiền quốc gia nào khác hiện nay.

Như chúng ta đã thảo luận ở Chương 7, tiền tệ giấy (fiat) cho phép các chính phủ chi tiêu khoản chi tiêu thâm hụt bằng cách ăn cắp từ giá trị của đồng tiền lưu hành. Người nghèo và, ở mức độ nào đó, tầng lớp trung lưu bị ảnh hưởng nhiều nhất bởi lạm phát tiền tệ trong khi nợ sử dụng phong phú và các công cụ tài chính khác nhau để mua lại các công ty và bất động sản thương mại có lợi nhuận. Họ biết rằng khoản nợ này sẽ bị giảm giá trị cùng với đồng tiền, mang lại một khoản lợi nhuận tăng thêm. Cách thứ nhất để giải quyết "cuộc chiến chống đói nghèo" là để thoát khỏi lạm phát tiền tệ và trở lại một hình thức tiền có giá trị giữ trong dài hạn. Nhưng đừng mong đợi chính phủ đề xuất hoặc thậm chí giải trí một đề xuất liên quan đến quá trình hành động này.

Hiện nay, nhiều bài báo và tạp chí về Bitcoin cho thấy bản chất "giảm phát" là tiêu cực chính của nó. Bằng cách giảm phát, họ có nghĩa là giá đo bằng BTC sẽ giảm. Trên thực tế, đây là lợi ích chính của Bitcoin. Họ báo cáo rằng mọi người sẽ "tích trữ" bitcoins hơn là chi tiêu chúng trong nền kinh tế. Trước hết hãy tưởng tượng rằng ngày mai bitcoins sẽ trở thành đơn vị tiền tệ được lựa chọn cho đất nước của bạn. Là con người, bạn vẫn phải ăn và để cung cấp cho một nơi trú ẩn; do đó bạn sẽ phải làm cho hai chi phí. Những nhận xét trong những bài báo này chứng minh là một quan niệm sai lầm về tiền là gì. Bằng cách tiết kiệm chứ không phải chi tiêu - "tích trữ" chỉ là một điều kỳ diệu cho việc tiết kiệm - người ta đang trì hoãn việc tiêu thụ đến một thời gian sau. Chúng ta đã chứng kiến hành vi này được gọi là "triệu phú bitcoin", một số người đã cảm thấy thoải mái khi chi tiêu một số bitcoins của họ vào các mặt hàng xa xỉ. Trong một hệ thống kinh tế dựa trên tiền tệ giữ giá trị của nó trong dài hạn tiết kiệm không phải là cạnh tranh cho các nguồn lực với các nhà sản xuất, nhà xây dựng, nhà máy, và những người chiết xuất hàng hoá (tức là các mặt hàng thương mại) bằng cách trì hoãn chi tiêu. Bằng nguồn lực, chúng tôi muốn nói đến bất kỳ hình thức năng lượng, hàng hoá, thời gian và lao động, đặc biệt là lao động chuyên biệt. Hãy tưởng tượng trường hợp của một người quyết định tiết kiệm bằng cách ở nhà chứ không phải là móc nối xe kéo và đi xuyên quốc gia để đi nghỉ mát. Bằng cách không đi du lịch, ông cho phép xăng mà ông sẽ phải chi tiêu để đi du lịch để được sử dụng, ví dụ như, một nhà sản xuất để vận chuyển vật liệu để xây dựng một nhà máy mới. In đô la không tạo ra nhiều thùng dầu, thêm gigawatts điện, hoặc nhiều giờ trong một ngày. Tôi đã mô tả khái niệm này với các ví dụ khá đơn giản, nhưng tôi hy vọng bạn có thể thấy rằng một loại tiền tệ như Bitcoin, với khả năng giữ giá trị của nó có nguồn gốc từ nguồn cung hạn hẹp, có những chi tiết lớn.

Trong chương này, chúng tôi đã giới thiệu công nghệ đằng sau Bitcoin, khái niệm phần mềm nằm dưới nó và chúng tôi đã đề cập đến quan điểm khác về kinh tế mà Satoshi Nakamoto có thể sẽ tuân thủ. Bây giờ bạn đã có một sự hiểu biết tốt về những gì Bitcoin là tất cả về và làm thế nào nó hoạt động, biến trang và đáp ứng Bitcoin của người sáng tạo, Satoshi Nakamoto!