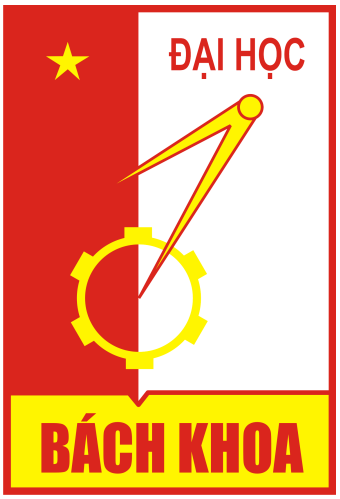
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

———————— * ————————



BLOCKCHAIN

Tìm hiểu về Bitcoin

Sinh viên thực hiện : **Nguyễn Quang Huy**

MSSV : 20151690

Lớp : KSTN-CNTT-K60

BÁCH KHOA
Ngày 15 tháng 6 năm 2018

Mục lục

1 Giới thiệu chung

Bitcoin là một loại tiền mã hóa ứng dụng công nghệ Blockchain, được phát minh bởi Satoshi Nakamoto dưới dạng phần mềm mã nguồn mở 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 trung gian nào.

Bitcoin có cách hoạt động khác hẳn so với các loại tiền tệ điển hình: Không có một ngân hàng trung ương nào quản lý nó và hệ thống hoạt động dựa trên một giao thức mạng ngang hàng trên Internet.

Bitcoin lần đầu được nhắc đến vào ngày 31 tháng 10 năm 2008 trong một bài báo về giao thức thanh toán ngang hàng của nhân vật ẩn danh Satoshi Nakamoto. Nó bắt đầu được đưa vào sử dụng từ ngày 3 tháng 1 năm 2009 với khối Bitcoin khởi thủy được ra đời(genesis block). Giao dịch Bitcoin đầu tiên được thực hiện giữa Satoshi Nakamoto và nhà mật mã học Hal Finney vào ngày 12 tháng 1 năm 2009.

Ngày 5 tháng 10 năm 2009, lần đầu tiên giá trị Bitcoin được ấn định trên sàn giao dịch, khởi điểm ở mức 1 đô la Mỹ tương đương 1.309,03 bitcoin (hoặc 1 bitcoin = 0.00076 USD).

Ngày 22 tháng 10 năm 2010, lần đầu tiên Bitcoin được sử dụng để mua hàng hóa - là một chiếc Pizza với giá 10.000 bitcoin, tương đương 25 đô la Mỹ tại thời điểm đó.

Trong năm 2011, giá trị của động Bitcoin tăng từ 0.30 đô la Mỹ lên 32 đô la Mỹ, trước khi giảm xuống còn 2 đô la Mỹ.

Bitcoin bắt đầu thu hút dư luận từ năm 2012, khi có rất nhiều bài báo nhắc đến nó. Năm 2013, một số dịch vụ lớn như OKCupid, Baidu, Reddit, Humble Bundle, Foodler và Gyft bắt đầu sử dụng nó. Tại Canada đã có máy ATM mua bán Bitcoin đầu tiên trên thế giới.

Ngày 28 tháng 2 năm 2014, sàn giao dịch Bitcoin Mt.Gox đã nộp đơn phá sản tại Nhật Bản do để mất 750.000 bitcoin của khách hàng và 100.000 Bitcoin của chính Mt.Gox tương đương 473 triệu đô la Mỹ. Vụ việc đã làm giảm uy tín của loại động tiền ảo này, khiến giá Bitcoin giảm từ đỉnh điểm 1.242 đô la Mỹ xuống còn mức thấp nhất là 152 đô la Mỹ.

Tháng 3 năm 2014, tại Việt Nam, đại lỹ mua bán Bitcoin đầu tiên ra đời với tên gọi là Bitcoin Việt Nam, cho phép mua hoặc bán bitcoin dễ dàng sau khi thực hiện thủ tục xác minh danh tính.

Tháng 7 năm 2014, tại Việt Nam, sàn giao dịch Bitcoin trực tuyến đầu tiên ra đời với tên gọi là VBTC.

Ngày 5 tháng 6 năm 2016, chiếc máy Bitcoin ATM đầu tiên tại Việt Nam bắt đầu được đưa vào thử nghiệm tại cửa hàng pizza Le Crespo tại địa chỉ 290 Lý Tự Trọng, Quận 1, thành phố Hồ Chí Minh - đối diện Starbucks vòng xoay Phù Đổng. Chiến máy này được sản xuất bởi Bit Access, điều hành bởi Bitcoin Vietnam và Bspend và được kết nối trực tiếp tới sàn giao dịch VBTC để mua và bán Bitcoin ra tiền Đồng. Hiện tại, vào tháng 5 năm 2018, giá Bitcoin đang ở mức 8.181,42 đô la Mỹ cho mỗi bitcoin.

2 Tổng quan về cách thức hoạt động của Bitcoin

Trong hệ thống thanh toán truyền thống, khi có một giao dịch thì cả 2 bên liên quan đến giao dịch đó sẽ đặt niềm tin vào một bên trung gian thứ 3, thường là ngân hàng. Bên thứ 3 này sẽ thực hiện các công việc kiểm tra, giám sát để đảm bảo giao dịch này là hợp lệ. Mọi giao dịch được thực hiện đều phải dựa vào ngân hàng. Cả hệ thống hoạt động dựa trên một niềm tin tập trung.

Với bitcoin, khác với các hệ thống giao dịch truyền thống, hoạt động dựa trên một niềm tin phi tập trung. Ở đó không hề có một cá nhân hay tổ chức nào đóng vai trò tạo kiểm chứng giống như ngân hàng. Một giao dịch giữa hai cá thể trong mạng lưới sẽ được quảng bá trong toàn mạng. Niềm tin ở đây đạt được dựa vào sự đồng thuận của tất cả các thành viên trong hệ thống.

Để thực hiện được giao dịch bitcoin, người dùng có thể dùng một ứng dụng được gọi là Ví điện tử. Ví điện tử sẽ quản lý các địa chỉ của người dùng, gọi là các bitcoin address. Một người dùng có thể có một hoặc nhiều địa chỉ bitcoin. Bất cứ ai muốn chuyển tiền cho chúng ta thì có thể chuyển tiền đến các địa chỉ này. Một địa chỉ bitcoin có dạng như sau *1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK* đi kèm với nó là mã QR tương ứng. Chúng ta có thể quét mã QR này để có thể lấy được địa chỉ một cách nhanh chóng.

2.1 Giao dịch Bitcoin

Một giao dịch bitcoin sẽ thông báo cho toàn bộ mạng biết rằng người chủ của số lượng bitcoin này đã cho phép chuyển số bitcoin đó cho người chủ mới và người chủ đó có toàn quyền sử dụng số tiền đó để thực hiện các giao dịch khác.

Mỗi giao dịch sẽ có một hay nhiều đầu vào(transaction inputs) là số tiền của một hay nhiều người gửi và một hay nhiều đầu ra(transaction outputs) là số tiền muốn chuyển cho một hay nhiều người nhận. Tổng số đầu vào bắt buộc phải lớn hơn hoặc bằng tổng số đầu ra. Phần dư của đầu vào và đầu ra được gọi là phí giao dịch(transaction fee). Phí này sẽ được chuyển cho người đã bỏ công sức ra để xác thực giao dịch đó.

Bên trong mỗi giao dịch còn chứa chữ kí điện tử(digital signature) của người gửi, đảm bảo rằng số tiền được chuyển thuộc về người gửi và chỉ có người gửi mới có khả năng kí để chuyển số tiền đó. Đồng thời, đầu ra cũng được liên kết với một khóa, mà chỉ có người nhận mới có khả năng mở khóa đó và sử dụng số tiền trong đó.

Khi muốn thực hiện một giao dịch mới, người dùng sẽ mở khóa các transaction outputs trước đó, lấy số tiền đó ra và tạo thành transaction input cho giao dịch. Ta có thể hiểu đầu ra của các giao dịch trước sẽ là đầu vào của các giao dịch hiện tại. Tuy nhiên chỉ các đầu ra chưa được mở khóa, tức là chưa được sử dụng mới có thể trở thành đầu vào của giao dịch mới. Đầu vào của giao dịch này sẽ trỏ về đầu ra của các giao dịch trước. Cứ như vậy nó tạo thành một chuỗi các giao dịch.

2.2 Đầu vào cho các giao dịch

Khi muốn thực hiện một giao dịch, người dùng phải tìm các đầu ra chưa được sử dụng trong các giao dịch trước của mình. Mỗi một ví điện tử sẽ lưu một cơ sở dữ liệu chứa các đầu ra chưa được sử dụng(unspent transaction outputs - UTXO). Khi một giao dịch được chuyển đến, người dùng sẽ dựa vào danh sách này để kiểm tra giao dịch đó có hợp lệ hay không bằng việc kiểm tra đầu vào đã được tiêu hay chưa.

Đầu vào của một giao dịch là đầu ra của các giao dịch trước đó

Tuy nhiên không phải người dùng nào cũng có thể lưu toàn bộ các giao dịch do yêu cầu về bộ nhớ, do đó có những node trong mạng lưu toàn bộ các đầu ra chưa được tiêu, trong khi những node khác chỉ lưu những đầu ra chưa được tiêu của chính người dùng đó. Những node này gọi là các lightweight node, khi chúng muốn kiểm tra các giao dịch được gửi đến, nó sẽ phải gửi yêu đầu để lấy về các đầu ra chưa được tiêu ứng với địa chỉ của người gửi, sau đó mới có thể kiểm tra.

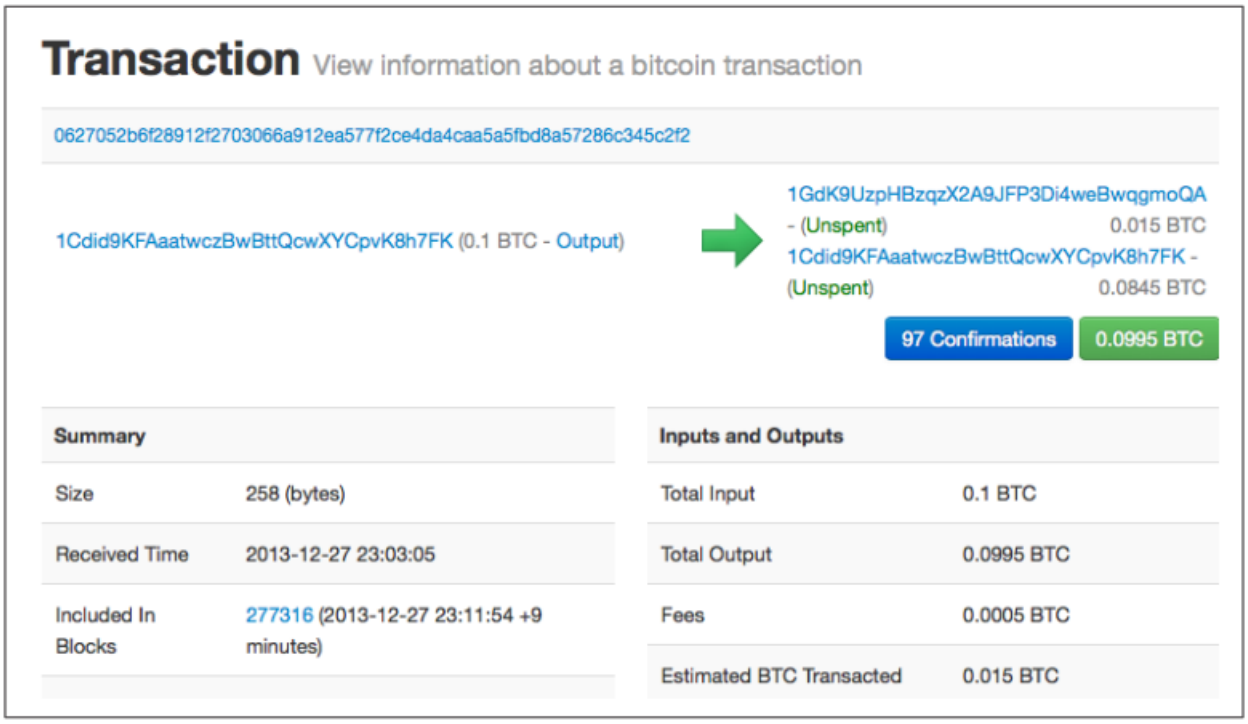
2.3 Đầu ra cho các giao dịch

Nếu số tiền của người gửi muốn gửi nhỏ hơn giá trị đầu vào của giao dịch, thì đầu ra phải gồm 2 phần, một phần có giá trị bằng giá trị số tiền muốn gửi và gửi đến người gửi, phần dư còn lại sẽ được gửi ngược lại về tài khoản người gửi. Nếu không có thành phần gửi ngược lại thì toàn bộ số dư sẽ được coi là phí giao dịch.

2.4 Lan truyền giao dịch

Sau khi giao dịch được tạo, nó sẽ được lan truyền trong mạng bitcoin là một mạng P2P. Mỗi node sẽ gửi giao dịch cho các node kết nối với nó và cứ như vậy, giao dịch được lan truyền trong toàn mạng. Để tránh hiện tượng spam, ở mỗi node sẽ có cơ chế kiểm tra giao dịch, để đảm bảo những giao dịch không hợp lệ sẽ không được lan truyền trong toàn mạng.

Cuối cùng giao dịch sẽ đến được ví của người nhận. Tuy nhiên đến lúc này, số tiền đó vẫn chưa thuộc về người nhận. Số tiền đó chỉ thuộc về người nhận khi giao dịch đó được xác nhận và được đưa vào trong một block trong blockchain.



Tổng các đầu ra và phí giao dịch sẽ bằng tổng các đầu vào

2.5 Khai thác Bitcoin

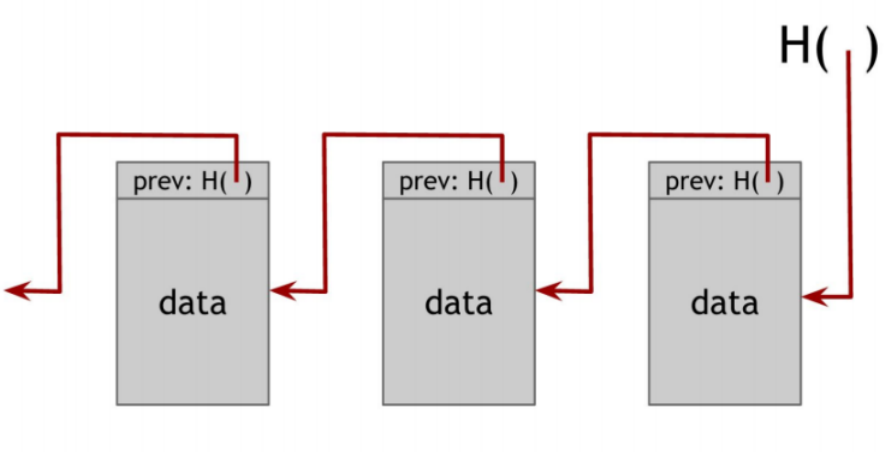
Mặc dù giao dịch đã được gửi đến toàn bộ các node trong mạng, số tiền chỉ thực sự thuộc về người nhận khi giao dịch được đưa ghi vào trong số cái, tức là được ghi vào trong một block trong blockchain và được xác nhận bởi toàn mạng.

Khi được lan truyền trong mạng, giao dịch đã được kiểm tra đầu vào để đảm bảo đầu vào là một transaction outputs chưa được tiêu. Tuy nhiên điều này vẫn chưa đủ để nói rằng giao dịch đó là hợp lệ. Một kiểu tấn công thường gặp trong hệ thống bitcoin là double-spending, tức là với cùng một số tiền, người gửi sẽ gửi cho nhiều người khác nhau.

Trong mạng có các node đặc biệt gọi là các miner có nhiện vụ xác nhận một danh sách các giao dịch để tạo thành một block và đưa block đó vào blockchain. Tuy nhiên các miner này có thể đưa các giao dịch không hợp lệ vào trong block, làm nhiễu loạn mạng. Do đó để tránh hiện tượng này, bitcoin đưa ra cơ chế khiến cho việc xác nhận một block trở nên khó khăn bằng việc giải một bài toán. Nếu một miner gian lận sau khi mất nhiều công sức để xác nhận một block không hợp lệ, các node trong mạng sẽ kiểm tra và loại bỏ node đó, dẫn đến tiêu tốn tài nguyên của miner gian lận. Từ đó giảm thiểu việc spam. Ý tưởng ở đây là không để ai cũng có thể xác nhận block bừa bãi và nếu các miner gian lận và bị phát hiện, chúng sẽ bị tiêu tốn rất nhiều tài nguyên mà không thu lại được giá trị gì.

Cứ mỗi phút, mỗi miner trong hàng nghìn miner sẽ lấy một danh sách giao dịch chưa

được xác nhận, giá trị băm SHA256 của block phía trước và một con số ngẫu nhiên gọi là số nonce tạo thành một block. Việc giải một bài toán, gọi là Proof-of-Work, bao gồm việc tìm ra số nonce bằng việc thử hàng triệu triệu phép băm block vừa tạo với hàm băm SHA256, sao cho giá trị băm thu được nhỏ hơn một ngưỡng nào đó. Ngưỡng này được gọi là target. Target càng cao thì độ khó càng thấp và ngược lại. Miner đầu tiên tìm được lời giải cho một block hợp lệ sẽ được thưởng, gồm phần thưởng cho người đầu tiên tạo ra block và phí giao dịch của các giao dịch nằm trong block đó. Miner đó sẽ gửi block cho các node khác kiểm tra tính hợp lệ và thêm block đó vào blockchain.



Block này chứa hàm băm của block phía trước tạo thành môt chuỗi các block

Tuy nhiên những giao dịch trong block vừa được thêm vẫn chưa thể đảm bảo 100% sẽ không bị thay đổi trong tương lai. Trong blockchain, block này chứa giá trị băm của block phía trước, nên khi một người muốn thay đổi nội dung của một block, dẫn đến thay đổi giá trị băm của nó và nội dung block kế tiếp. Để đảm bảo tính hợp lệ của block kế tiếp, người đó phải tìm ra số ngẫu nhiên mới ứng với block này. Và cứ như vậy, dẫn đến thay đổi toàn bộ nội dung của chuỗi blockchain.

Độ cao của một block trong chuỗi được định nghĩa là khoảng cách từ block đầu tiên trong chuỗi đến block đó, trong khi chiều sâu của một block được định nghĩa là khoảng cách từ block cuối trong chuỗi đến block đó. Độ sâu của block sẽ ứng với số lần xác nhận(confirmation) của các giao dịch trong block đó. Khi số confirmation càng lớn thì ta càng tự tin rằng các giao dịch sẽ không bị sửa đổi trong tương lai. Trong thực tế, 6 lần xác nhận được coi là không thể sửa, vì khi đó nó yêu cầu một lượng tính toán rất lớn để sửa lại nội dung của 6 block.

3 Khóa, địa chỉ, ví điện tử

3.1 Hàm băm mật mã

Trước hết ta sẽ xem xét khái niệm hàm băm mật mã. Một hàm băm là một hàm tính toán học có các đặc tính:

- Đầu vào có thể là một chuỗi có độ dài bất kì.
- Đầu ra có độ dài cố định.

- Dễ tính toán, tức là khi băm một chuỗi n bit mất một khoảng thời gian O(n)

Một hàm băm mật mã sẽ có thêm các đặc tính: kháng đụng độ, che dấu.

Một hàm băm được gọi là kháng đụng độ nếu không thể tìm ra 2 giá trị x≠y để $H(x) = H(y)$. Điều này không có nghĩa là đụng độ không thể xảy ra do không gian input là vô tận trong khi không gian output là hữu hạn. Xét hàm băm SHA256 cho đầu ra là chuỗi 256-bit. Khi đó nếu thử $2^{256} + 1$ đầu vào, chắc chắn sẽ tìm được 2 giá trị x≠y để $H(x) == H(y)$. Tuy nhiên số phép thử này là vô cùng lớn. Ta luôn đảm bảo đươc sự kiện tìm ra đụng độ có xác suất vô cùng bé.

Che dấu: Khi cho 1 giá trị băm y ta không thể tìm được giá trị x ban đầu. Điều này chỉ đạt được khi không gian input là đủ lớn, nếu không ta có thể thử băm toàn bộ input và so sánh giá trị băm.

3.2 Chữ kí điện tử

Tương tự như chữ ký tay, chúng ta kì vọng chữ ký điện tử có đặc tính chỉ có người chủ có thể sử dụng chữ ký của họ. Tuy nhiên chữ kỹ tay có thể bị sao chép từ văn bản này sang văn bản khác. Chữ ký điện tử có thêm đặc tính nó gắn liền với một văn bản cụ thể. Các văn bản khác nhau được kí bởi cùng 1 người sẽ có chữ kí khác nhau.

Ý tưởng ở đây ta sẽ sử dụng một cặp khóa private key và public key. Private key được giữ bởi người chủ, public key được gửi công khai cho mọi người. Dựa trên private key và tin nhắn, người chủ sẽ tạo ra một chữ ký ứng với tin nhắn đó. Mọi người có thể kiểm tra tin nhắn đó có phải do người chủ đó kí hay không bằng cách sử dụng hàm nhận đầu vào là khóa công khai, tin nhắn được gửi và chữ kí của người gửi, giá trị trả về là đúng hoặc sai. Khi có tin nhắn và các chữ ký tương ứng, ta không thể tìm ngược lại khóa riêng tư.

Trong một giao dịch bitcoin, người gửi sẽ đính kèm chữ kí của mình trong giao dịch, mọi người có thể sử dụng public key của người gửi để kiểm tra số bitcoin được gửi đi là thuộc về người gửi. Trong giao dịch còn chứa địa chỉ của người nhận là giá trị băm của public key và chỉ có private key của người nhận mới có thể mở khóa và sử dụng số tiền được gửi.