TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
Viện Công nghệ thông tin & Truyền thông

BÁO CÁO BÀI TẬP LỚN
NHẬP MÔN AN TOÀN THÔNG TIN

ĐỀ TÀI: CÁC MÔ HÌNH TIỀN ĐIỆN TỬ TRONG GIAO DỊCH TIỀN ĐIỆN TỬ

GIẢNG VIÊN HƯỚNG DẪN: PSG.TS. NGUYỄN LINH GIANG

NHÓM SINH VIÊN THỰC HIỆN
Nguyễn Duy Dũng……..20173056
Bùi Thanh Tùng……..20173452
Nguyễn Đình Hoàng……...20173143
Đàm Việt Dũng……...20173047

MỤC LỤC

I. Giới thiệu về tiền điện tử

Tiền điện tử, hay còn được gọi là tiền kỹ thuật số, là một đơn vị tiền tệ hoạt động dựa trên các thuật toán điện tử và được lưu trữ trên Internet, hệ thống máy tính, điện thoại thông minh và các thẻ thanh toán điện tử. Tiền điện tử cho phép các giao dịch tức thời có thể được thực hiện liền mạch để thanh toán qua biên giới. Thông thường, nếu tiền điện tử không được sự cho phép ban hành của Chính phủ thì chúng không phải tiền hợp pháp và chúng cho phép chuyển quyền sở hữu xuyên biên giới.

Tiền điện tử được thiết kế cho mục đích bảo mật và mang tính ẩn danh cao cho giao dịch. Chúng được tạo ra từ hệ thống máy tính và chạy trên nền tảng công nghệ blockchain - sổ cái ghi lại tất cả các giao dịch tiền điện tử trong hệ thống. Người dùng không cần sử dụng tên của họ, và cũng không cần thông qua bất kỳ ngân hàng nào mà vẫn có thể mua tiền điện tử từ các công ty môi giới, sau đó lưu trữ và chi tiêu chúng thông qua ví điện tử.

Tiền điện tử hiện có 2 hình thức chính là tiền ảo (Virtual Currency) và tiền mã hóa (Cryptocurrency).

1. Tiền ảo

Tiền ảo là một loại tiền điện tử không được kiểm soát, được phát hành bởi Chính phủ và thường có thể được phát hành, quản lý và kiểm soát bởi các nhà phát hành tư nhân, nhà phát triển hoặc tổ chức sáng lập. Loại tiền này được sử dụng và chấp nhận giữa các thành viên của một cộng đồng ảo cụ thể. Vào năm 2014, Ngân hàng trung ương Châu Âu đã định nghĩa tiền ảo là "đại diện kỹ thuật số của giá trị không phải do Ngân hàng trung ương hoặc cơ quan công quyền phát hành, cũng không nhất thiết phải gắn với tiền định danh (tiền tệ fiat), nhưng được các thể nhân hoặc pháp nhân chấp nhận như một phương tiện thanh toán và có thể được chuyển nhượng, lưu trữ hoặc giao dịch điện tử ". Tiền ảo chỉ có sẵn ở dạng điện tử. Nó chỉ được lưu trữ và giao dịch thông qua phần mềm được chỉ định, ứng dụng di động hoặc máy tính hoặc thông qua ví điện tử chuyên dụng và các giao dịch xảy ra qua internet thông qua các mạng chuyên dụng, an toàn.

2. Tiền mã hóa

Tiền mã hóa là một tài sản kỹ thuật số được thiết kế để làm việc như là một trung gian trao đổi, sử dụng mật mã để đảm bảo các giao dịch, để kiểm soát việc tạo ra các đơn vị bổ sung và để xác minh việc chuyển giao tài sản. Tính năng đặc biệt và được cho là sức hấp dẫn chính của của tiền mã hoá là bản chất hệ thống. Tiền mã hoá không được ban hành bởi bất kỳ Ngân hàng trung ương nào, điều này khiến về mặt lý thuyết nó miễn nhiễm với sự can thiệp hoặc thao túng của Chính phủ.

Bitcoin - ra đời năm 2008 là loại tiền mã hóa đầu tiên. Cho đến nay, Bitcoin cũng chính là loại tiền mã hóa phổ biến và có giá trị nhất. Ngày nay, có hàng ngàn loại tiền mã hóa thay thế với các chức năng hoặc thông số kỹ thuật khác nhau.

3. Cách thức hoạt động

Tiền điện tử dựa trên nền tảng công nghệ dữ liệu chuỗi khối (blockchain) - một sổ cái công cộng khổng lồ liệt kê tất cả các giao dịch được xác thực bởi một hệ thống máy tính kết nối toàn cầu.

Tiền điện tử được xây dựng dựa trên những thuật toán phức tạp, trong đó cho phép các giao dịch được thực hiện trực tiếp giữa người gửi và người nhận mà không cần có sự kiểm soát của Chính phủ, ngân hàng hay các tổ chức tài chính mà vẫn đảm bảo tính an toàn và chính xác của giao dịch.

Có thể nói, sự ra đời của tiền điện tử đã đánh dấu bước ngoặc lịch sử về hình thức thanh toán điện tử.

II. Một số đồng tiền điện tử phổ biến hiện nay

Bitcoin (BTC)

Bitcoin là đồng tiền điện tử đầu tiên trên thế giới và đặt nền móng cho phát triển của thị trường Cryptocurrency (tiền mã hóa). Bitcoin sử dụng giao thức ngang hàng (peer-to-peer) cho tất cả các giao dịch và chính điều đó đã làm cho Bitcoin loại bỏ bước trung gian trong quá trình thực hiện giao dịch, giao dịch sẽ được thực hiện trực tiếp từ người gửi đến người nhận với phí giao dịch cực kỳ thấp (gần như bằng 0) mà không phải qua bất cứ tổ chức hay cá nhân trung gian nào.

Ethereum (ETH)

Đứng sau Bitcoin, Ethereum là loại tiền điện tử lớn thứ 2 thế giới theo tổng vốn hóa thị trường. Ethereum được giới thiệu vào cuối năm 2013 bởi một người chuyên nghiên cứu về lập trình tiền ảo có tên Vitalik Buterin và hệ thống được khởi động vào năm 2015. Với ý tưởng phát triển ETH để khắc phục những điểm chưa tốt mà Bitcoin gặp phải như thời gian xác nhận chậm đồng thời khuyến khích người dùng không nên khai thác riêng lẻ mà tập trung khai thác qua các mining-pool. Ethereum cung cấp cho người dùng của mình một loạt các tính năng tuyệt vời như: Quản trị phi tập trung liền mạch, sử dụng hợp đồng thông minh

RIPPLE (XRP)

RIPPLE (XRP) là một loại tiền kỹ thuật số và hệ thống thanh toán mở, RIPPLE trở nên cực kỳ phổ biến kể từ khi phát hành vào năm 2012. Đây là một hệ thống phân tán mã nguồn mở vẫn còn nằm trong phân đoạn Beta.

Mục đích của hệ thống này là giúp người dùng có thể sử dụng thẻ tín dụng, Paypal, ngân hàng hay các tổ chức tài chính khác với mức phí thấp nhất cùng với quá trình xử lí nhanh chóng.

DigiByte (DGB)

DigiByte (DGB) là một mã nguồn mở phát triển dựa trên nền tảng mã nguồn của Bitcoin và Litecoin, tốc độ của DigiByte đủ nhanh để mua một mặt hàng chỉ trong vài giây với một nút bấm trên điện thoại thông minh.

DGB là một mật mã được phân cấp chuyên nghiệp và minh bạch đã được thiết kế để giải quyết một số điểm yếu của Bitcoin và Litecoin, và nó là một cryptocoin (tập hợp tin tức tiền mã hóa) phân cấp trên toàn cầu chủ yếu dành cho hàng hoá và dịch vụ.

Litecoin (LTC)

Litecoin được thành lập bởi sinh viên tốt nghiệp đại học MIT và cựu kỹ sư Google Charlie Lee**,** Litecoin là một loại tiền mã hóa được xem là một sự thay thế cho Bitcoin. Ra mắt sau Bitcoin vài năm, Litecoin ban đầu được dự định là một phiên bản ít tốn tài nguyên hơn của Bitcoin.

Cấu trúc mã hóa cốt lõi của LTC khá giống với Bitcoin, nhưng khác với người tiền nhiệm của mình, đồng tiền mã hóa ảo theo mô hình ngang hàng này chạy trên một thuật toán Scrypt với tốc

độ tạo Block nhanh hơn Bitcoin gần 4 lần. Ngoài ra, tổng nguồn cung của token LTC lớn gấp 4 lần so với BTC.

Maker (MKR)

Maker (hay còn gọi là MKR) là đồng tiền kỹ thuật số được xây dựng dựa trên nền tảng hợp đồng thông minh được triển khai trên Blockchain Ethereum. Nó được tạo ra nhằm mục đích làm ổn định giá của một đồng tiền điện tử khác tên là DAI thông qua các hợp đồng thông minh có tên là Collateralized Debt Positions (CDPs), cũng như việc nó có thể đóng vai trò là một nền tảng hợp đồng thông minh hỗ trợ và ổn định giá trị của stablecoin DAI bằng các khái niệm thích hợp như: vị trí nợ được thế chấp (CDP), cơ chế phản hồi tự động, các nhân tố ưu đãi bên ngoài.

Binance Coin (BNB)

Binance Coin (BNB) là đồng tiền điện tử chính thức của Binance Chain. Được phát hành lần đầu tiên ra thị trường thông qua ICO vào tháng 7 năm 2017. Ban đầu, đồng BNB được xây dựng trên nền tảng Blockchain của Ethereum theo tiêu chuẩn ERC-20. Vào ngày 24 tháng 4 năm 2019, Binance chính thức hoàn thành Binance Chain Mainnet và bắt đầu hỗ trợ chuyển đổi BNB chạy trên Ethereum sang BNB chạy trên nền tảng của chính họ với tỷ lệ 1:1.

Cardano (ADA)

Cardano là đứa con tinh thần của người đồng sáng lập Ethereum - Charles Hoskinson. Trên giấy tờ, nó dường như chia sẻ rất nhiều điểm tương đồng với Ethereum như: Cho phép người dùng xây dựng các ứng dụng mới và hợp đồng thông minh.

Tuy nhiên, người ta có thể thấy rằng Cardano và token ADA được thiết kế để giúp giải quyết nhiều vấn đề liên quan đến khả năng tương tác và khả năng mở rộng đang gây khó chịu cho thế giới tiền điện tử ngày nay. Cụ thể hơn, nhóm phát triển Cardano đặc biệt tập trung vào việc tối đa hóa hiệu quả của thị trường thanh toán quốc tế bằng cách cắt giảm nhiều vấn đề liên quan đến thời gian và lệ phí hiện đang có mặt trong lĩnh vực đang phát triển này.

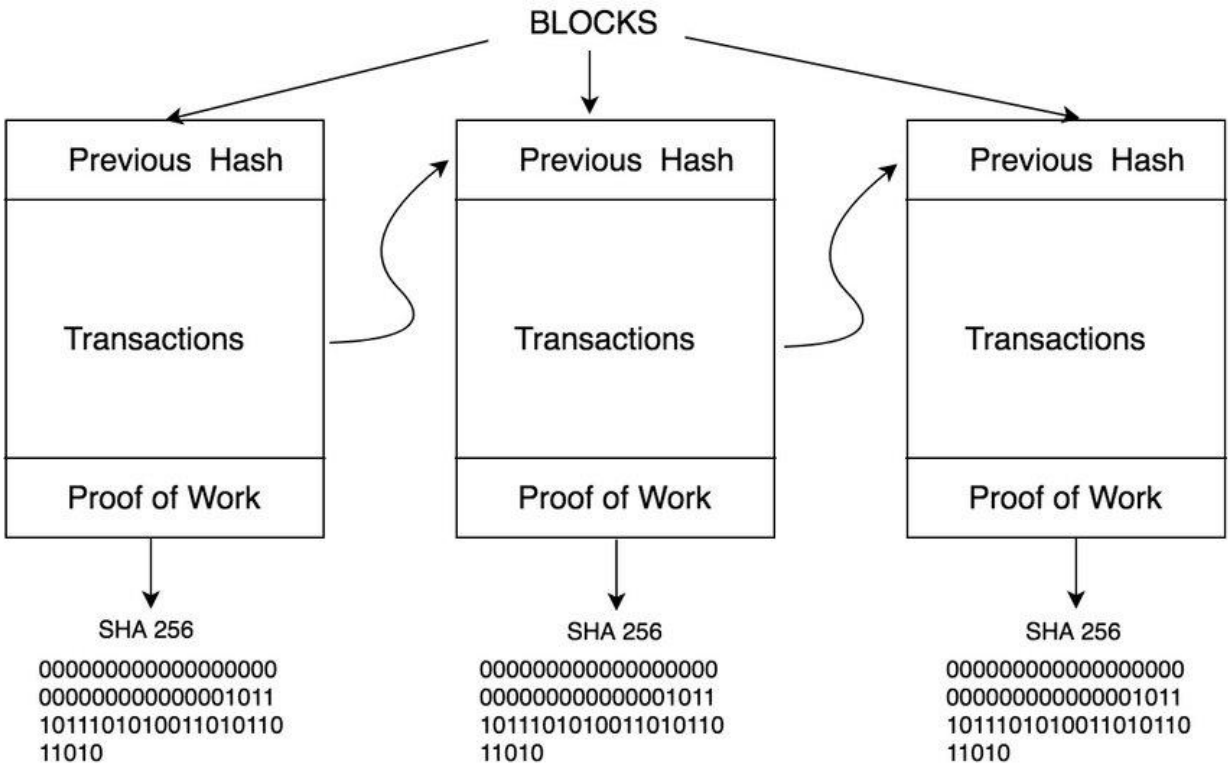
III. Công nghệ Blockchain

1. Blockchain là gì?

Blockchain như một cuốn sổ cái kế toán công cộng. Trong đó, mọi thông tin được lưu trữ và truyền tải một cách minh bạch, toàn vẹn, không thể nào thay đổi hay gian lận được. Đây là một công nghệ mới, giúp cải thiện được rất nhiều những mặt hạn chế của cách lưu trữ và trao đổi thông tin truyền thống. Bởi lý do này, mà blockchain ngày càng được ứng dụng rộng rãi trong nhiều lĩnh vực: kinh tế tài chính, giáo dục, nông nghiệp, công nghiệp, lĩnh vực giải trí, y tế hay giáo dục…

2. Cấu trúc của Blockchain

Blockchain là một database phân tán (phi tập trung) mà trong đó các dữ liệu được lưu trữ dưới dạng các block. Body của một block mang theo các transactions trên dữ liệu (như state machine). Block được kết nối với nhau theo dạng danh sách liên kết (linked list) dưới dạng mã hóa SHA256. Mã hóa của một block bao gồm cả địa chỉ của block trước và body của chính nó nên khi một block được add vào, nó không thể thay đổi cũng như tái sắp xếp.



Hình 1: Cấu trúc của Blockchain

3. Nguyên lý hoạt động của Blockchain

3.1. Nguyên lý mã hoá

Blockchain sử dụng mô hình peer-to-peer (ngang hàng), nghĩa là các máy tính tham gia vào mạng Blockchain vừa đóng vai trò là Client vừa là Server. Vì thế, nó sẽ có một số điểm khác biệt: Trong hệ thống ngân hàng, chúng ta chỉ biết các giao dịch và số dư tài khoản của riêng mình thì trên blockchain của bitcoin người dùng có thể xem các giao dịch của tất cả mọi người. Mạng lưới Bitcoin là mạng lưới phân tán không cần bên thứ ba đóng vai trò trung gian xử lý giao dịch. Để có thể thực hiện các giao dịch trên blockchain, cần một phần mềm lưu trữ và trao đổi các đồng Bitcoin gọi là ví tiền điện tử. Ví tiền điện tử này sẽ được bảo vệ bằng một phương pháp mã hóa đặc biệt đó là sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key).

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

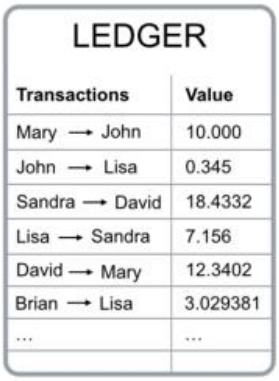
Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư, có nghĩa là người sử dụng đang tạo ra một chữ ký điện tử được các máy tính trong mạng lưới blockchain sử dụng để kiểm tra chủ thể gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và là sự kết hợp của yêu cầu giao dịch và khóa riêng tư của người dùng. Chính vì vậy nếu một ký tự đơn trong thông điệp yêu cầu giao dịch bị thay đổi thì chữ ký điện tử sẽ thay đổi theo. Vì thế, hacker khó có thể thay đổi yêu cầu giao dịch hoặc thay đổi số lượng Bitcoin đang gửi.

Để gửi Bitcoin (BTC), người dùng cần chứng minh rằng mình sở hữu khóa riêng tư của một chiếc ví điện tử cụ thể, bởi người dùng cần sử dụng nó để mã hóa thông điệp yêu cầu giao dịch. Sau khi tin nhắn đã được gửi đi và được mã hóa thì người dùng không cần phải tiết lộ khóa riêng tư của mình nữa.

3.2. Quy tắc của sổ cái

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

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



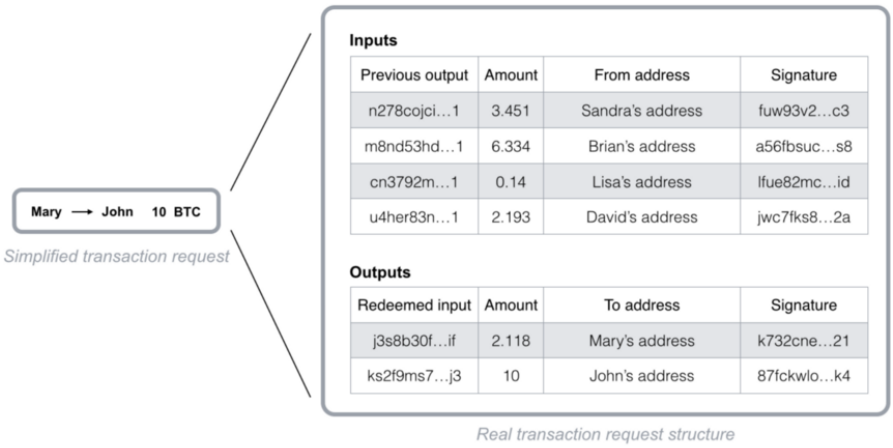
LEDGER

Transactions	Value
Mary → John	10.000
John → Lisa	0.345
Sandra → David	18.4332
Lisa → Sandra	7.156
David → Mary	12.3402
Brian → Lisa	3.029381
...	...

Hình 2: Sổ cái

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

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



Mary → John 10 BTC

Simplified transaction request

Inputs

Previous output	Amount	From address	Signature
n278cojci…1	3.451	Sandra's address	fuw93v2…c3
m8nd53hd…1	6.334	Brian's address	a56fbsuc…s8
cn3792m…1	0.14	Lisa's address	lfue82mc…id
u4her83n…1	2.193	David's address	jwc7fks8…2a

Outputs

Redeemed input	Amount	To address	Signature
j3s8b30f…if	2.118	Mary's address	k732cne…21
ks2f9ms7…j3	10	John's address	87fckwlo…k4

Real transaction request structure

Hình 3: Đầu vào và đầu ra của một giao dịch

Vậy, làm thế nào hệ thống có thể tin tưởng các giao dịch đầu vào này và xác thực tính hợp lệ của chúng?

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

Như vậy sở hữu Bitcoin có nghĩa là có các giao dịch được lưu trong sổ kế toán liên hệ đến địa chỉ ví của bạn mà chưa được sử dụng làm giao dịch đầu vào.

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

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

3.3. Nguyên lý tạo khối.

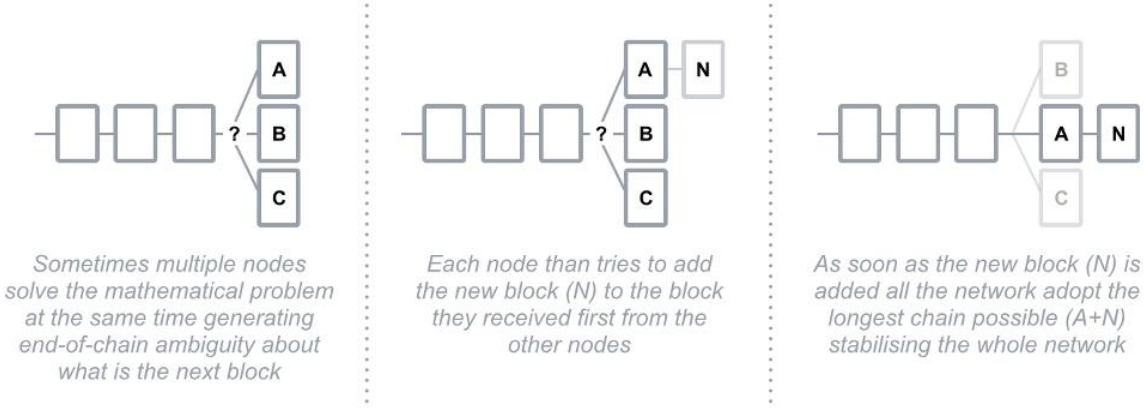
Các giao dịch sau khi được gửi lên trên mạng lưới blockchain sẽ được nhóm vào các khối và các giao dịch trong cùng 1 khối (block) được coi là đã xảy ra cùng thời điểm. Các giao dịch chưa được thực hiện trong 1 khối được coi là chưa được xác nhận. Bất kỳ nút nào cũng có thể tạo ra một khối mới. Vậy, câu hỏi đặt ra là: hệ thống sẽ đồng thuận với khối nào? khối nào sẽ là khối tiếp theo?

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

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

Vậy điều gì sẽ xảy ra nếu hai nút giải quyết cùng một vấn đề cùng một lúc và truyền các khối kết quả của chúng đồng thời lên mạng lưới? Trong trường hợp này, cả hai khối được gửi lên mạng lưới và mỗi nút sẽ xây dựng các khối kế tiếp trên khối mà nó nhận được trước tiên.

Tuy nhiên, hệ thống blockchain luôn yêu cầu mỗi nút phải xây dựng trên chuỗi khối dài nhất mà nó nhận được. Vì vậy, nếu có sự mơ hồ về việc block nào là khối cuối cùng thì ngay sau khi khối tiếp theo được giải quyết thì mỗi nút sẽ áp dụng vào chuỗi dài nhất.



Do xác suất việc xây dựng các block đồng thời là rất thấp nên hầu như không có trường hợp nhiều khối được giải quyết cùng một lúc và nhiều lần tạo ra các khối nối đuôi khác nhau. Do đó, toàn bộ chuỗi-khối sẽ nhanh chóng ổn định và hợp nhất lại khi mà mọi nút đều đồng thuận.

3.4. Thuật toán bảo mật Blockchain

Nếu có bất kỳ sự bất đồng về khối đại diện sau cùng của chuỗi thì điều này sẽ dẫn đến khả năng gian lận. Nếu một giao dịch xảy ra trong 1 khối thuộc về đuôi ngắn hơn khi khối tiếp theo được giải quyết, giao dịch đó sẽ trở lại thành giao dịch chưa được xác nhận vì tất cả các giao dịch khác được nhóm vào trong khối kia.

Mỗi block chứa một tham chiếu đến khối trước đó, và tham chiếu đó là một phần của vấn đề toán học cần được giải quyết để truyền khối sau tới mạng lưới. Vì vậy, rất khó để tính toán trước một loạt các block bởi nó cần tính ra một số lượng lớn các số ngẫu nhiên cần thiết để giải quyết một khối và đặt nó trên blockchain.

Các giao dịch trong mạng lưới blockchain của bitcoin được bảo vệ bởi một cuộc chạy đua tính toán toán học: với bất kỳ kẻ tấn công nào muốn cạnh tranh với toàn bộ mạng lưới.

Do đó, giao dịch ngày càng an toàn hơn theo thời gian. Và những khối đã được thêm vào chuỗi trong quá khứ bao giờ cũng an toàn hơn so với những khối mới được thêm vào. Bởi một block được thêm vào chuỗi trung bình cứ 10p một lần cho nên trong khoảng 1h kể từ khi giao dịch được nhóm vào trong khối đầu tiên của nó sẽ tạo ra một xác suất khá cao rằng giao dịch đã được xử lý và không thể đảo ngược.

4. Cơ chế đồng thuận trong Blockchain

Cơ chế đồng thuận trong Blockchain có thể hiểu như cách thức mà mọi người quản lý trong hệ thống blockchain có thể đồng ý cho một giao dịch xảy ra trong hệ thống. Dưới đây là các loại cơ chế đồng thuận phổ biến trong blockchain:

+ Proof of Work (Bằng chứng Công việc): Đây là cơ chế đồng thuận phổ biến nhất, được dùng trong Bitcoin, Ethereum, Litecoin, Dogecoin và hầu hết các loại tiền mã hoá. Đây là cơ chế đồng thuận tiêu tốn khá nhiều điện năng.

+ Proof of Stake (Bằng chứng Cổ phần): Đây là cơ chế đồng thuận phổ biến trong Decred, Peercoin và trong tương lai là Ethereum và nhiều loại tiền mã hoá khác. Cơ chế đồng thuận này phân cấp hơn, tiêu hao ít năng lượng và không dễ gì bị đe doạ.

+ Delegated Proof-of-Stake (Uỷ quyền Cổ phần): Đây là cơ chế đồng thuận phổ biến trong Steemit, EOS, BitShares. Cơ chế đồng thuận này có chi phí giao dịch rẻ; có khả năng mở rộng; hiệu suất năng lượng cao. Tuy nhiên vẫn một phần hơi hướng tập trung vì thuật toán này lựa chọn người đáng tin cậy để uỷ quyền.

+ Proof of Authority (Bằng chứng Uỷ nhiệm): Đây là cơ chế đồng thuận phổ biến thường thấy trong POA.Network, Ethereum Kovan testnet. Cơ chế đồng thuận này có hiệu suất cao, có khả năng mở rộng tốt.

+ Proof-of-Weight (Bằng chứng Khối lượng /Càng lớn càng tốt): Đây là cơ chế đồng thuận phổ biến trong Algorand, Filecoin. Cơ chế đồng thuận này có thể tuỳ chỉnh và khả năng mở rộng tốt. Tuy nhiên quá trình thúc đẩy việc phát triển sẽ là một thử thách lớn.

+ Byzantine Fault Tolerance (Đồng thuận chống gian lận /Tướng Byzantine bao vây Blockchain): Đây là cơ chế đồng thuận phổ biến trong Hyperledger, Stellar, Dispatch, và Ripple. Cơ chế đồng thuận này có năng suất cao; chi phí thấp; có khả năng mở rộng. Tuy nhiên vẫn chưa thể tin tưởng hoàn toàn.

4.1 Proof of Work (PoW)

Trong Blockchain, thuật toán Proof of Work được sử dụng để xác nhận các giao dịch, tạo ra các khối mới và giúp hình thành nên chuỗi khối lớn trong hệ thống. PoW là cơ sở để các thợ mỏ cạnh tranh để hoàn thành các giao dịch trên mạng sau khi trả lời được một câu đố mật mã phực tạp và sau đó thì thợ mỏ sẽ được thưởng một khoản coin theo yêu cầu.

Trong một mạng người dùng gửi cho nhau đồng tiền điện tử, một sổ cái phi tập trung được sử dụng để tập hợp tất cả các giao dịch thành các khối liên kết (chuỗi khối). Tuy nhiên, cần cẩn thận để xác nhận các giao dịch và sắp xếp các khối. Trách nhiệm này được đảm nhiệm bởi các nút đặc biệt (Node) được gọi là thợ mỏ và một quy trình như vậy thì được gọi là khai thác khối.

PoW dùng thuật toán đồng thuận của mình để phân tích các khối dữ liệu và nhu cầu trong các khối này yêu cầu. Sau khi xử lí đưa ra câu trả lời cho một khối. Hệ thống sẽ xem xét xem câu trả lời đó có đúng không. Nếu đúng thì nó sẽ thưởng coin cho các thợ mỏ, và nếu các khối mới được tạo thì các khối sẽ tự động liên kết với nhau tạo thành một chuỗi khối.

Một số bài toán đào block điển hình là:

+ *hash function* (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 ấy, 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".

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 block thì sẽ càng cần nhiều và nhiều năng lực băm (hash power) hơn nữa. Vì thế, độ khó thuật toán đào tiền là một trong những vấn đề nhạy cảm nhất trên Blockchain hiện nay.

Ưu điểm của PoW

+ PoW có thể đảm bảo sự an toàn của toàn mạng. Đây là mục đích chính của lý do tại sao nhiều loại tiền điện tử sử dụng PoW. Nếu nhiều node đang cạnh tranh để xác định độ phân giải của vấn đề, thì năng lượng tính toán cần thiết sẽ trở nên cao đến mức chuỗi sẽ trở nên không thể đạt được đối với một hoặc thậm chí một nhóm hacker không quá lớn.

+ Phát hiện những kẻ gửi thư rác (spammers).

Nhược điểm của PoW

+ Tốn thời gian: Người khai thác phải kiểm tra nhiều giá trị nonce để tìm ra giải pháp phù hợp cho bài toán phải giải để khai thác block, đây là một quá trình tốn thời gian.

+ Tiêu thụ tài nguyên: Cần tiêu thụ lượng năng lượng tính toán cao để tìm ra lời giải cho bài toán khó và phức tạp. Nó dẫn đến sự lãng phí tài nguyên quý giá (tiền bạc, năng lượng, không gian, phần cứng).

+ Nó không phải là một giao dịch tức thời. Bởi vì phải mất một thời gian để khai thác, giao dịch và thêm nó vào blockchain để thực hiện giao dịch.

Tấn công 51%

Có thể gọi là tấn công số lượng lớn. Đây là trường hợp người dùng hoặc một nhóm người dùng kiểm soát phần lớn sức mạnh khai thác. Những kẻ tấn công có đủ sức mạnh để kiểm soát hầu hết các sự kiện trong mạng.

Họ có thể độc quyền tạo các block mới và nhận phần thưởng vì họ có thể ngăn các thợ mỏ khác hoàn thành các block. Và còn có cơ hội đảo ngược tất cả các giao dịch. Một ví dụ điển hình cho loại hình tấn công này như mạng Bitcoin Gold bị hack 18 triệu USD vào năm 2018. Và còn nhiều vụ khác mang tên "Tấn công 51%".

4.2 Proof of Stake (PoS)

Như đã biết đồng cryptocurrency đầu tiên là Bitcoin sử dụng thuật toán đồng thuận Proof-of-Work (PoW). PoW cho phép thợ đào (miner) xác thực giao dịch và tạo block mới bằng cách thực hiện tính toán dựa trên sức mạnh máy tính. Từ đó sinh ra máy đào chuyên dụng với cấu hình khủng và hiệu năng cao, giúp thợ đào cạnh tranh đào coin.

Tuy nhiên, cộng đồng tiền mã hóa nhanh chóng nhận ra những yếu điểm và bất lợi của thuật toán PoW. Năm 2011, diễn đàn Bitcointalk là nơi đầu tiên nảy sinh ra ý tưởng một thuật toán mới với tên gọi Proof-of-Stake (PoS), giải quyết một số vấn đề mà thuật toán PoW gặp phải.

Đến năm 2012, đồng coin đầu tiên sử dụng PoS ra đời. Đó chính là Peercoin (PPC). Từ đó đến nay, đã có hàng trăm đồng coin sử dụng thuật toán PoS.

Các thuật ngữ liên quan đến Proof-of-Stake (POS)

- Node (Masternode)

Là những người, hay tổ chức tham gia xác nhận giao dịch, đóng block của một đồng coin. Bằng cách chạy các phần mềm chuyên dụng của đồng coin đó, node đóng vai trò giữ ổn định trong blockchain, xác nhận giao dịch cho người dùng coin.

- Validator

Theo thuật toán PoS, không phải tất cả các node đều tham gia đóng block mới. Blockchain sẽ chọn ngẫu nhiên một node để kiểm định và đóng block. Node này được gọi là validator (người kiểm định).

- Forge hoặc Mint

Là cụm từ chỉ hoạt động kiểm định và đóng block của validator. Để phân biệt với mine (đào) trong PoW.

- Stake

Trong PoS, node muốn trở thành validator phải stake (đặt cọc) một lượng coin nhất định để làm điều kiện tham gia. Ý nghĩa của việc này là để chứng minh bạn có sở hữu coin.

Lock và Unlock

Số coin được node stake sẽ được mạng lưới lock. Trong thời gian trở thành validator, số coin stake này không được di chuyển, hay giao dịch được. Nếu không làm validator nữa thì coin mới được unlock.

Các thức hoạt động

Phương thức hoạt động của thuật toán đồng thuận PoS có thể tóm tắt như sau:
- Trong tất cả các node tham gia, blockchain sẽ lựa chọn ngẫu nhiên một node (hay masternode) để trở thành validator. Validator này có vai trò kiểm định và đóng block.
- Để trở thành validator, cần phải đặt cọc một khoản tiền vào mạng lưới để làm điều kiện tham gia.
- Blockchain sẽ lock khoản đặt cọc này này, và sẽ unlock sau khi node không tham gia validator một thời gian chứ không unlock ngay lập tức.
- Nếu block hợp lệ và ghi vào chain, thì validator sẽ nhận được một phần thưởng từ phí giao dịch.
Tuy nhiên, để blockchain minh bạch và hoạt động hiệu quả, cần có cơ chế lựa chọn validator phù hợp.

Cơ chế lựa chọn node có thể nói đến:
- Lựa chọn node ngẫu nhiên: Thuật toán Proof-of-Stake sẽ lựa chọn validator kiểm định block tiếp theo một cách ngẫu nhiên. Bằng cách sử dụng công thức tìm kiếm Hashrate thấp nhất, kết hợp với khoản đặt cược cao nhất (stake). Khi tài sản được công khai, mỗi node sẽ "tự động" lựa chọn tài khoản được quyền xử lý block tiếp theo.
- Lựa chọn node dựa trên thời gian nắm giữ tài sản: Thuật toán POS còn kết hợp phương pháp lựa chọn ngẫu nhiên với việc dựa vào tuổi đời của tài sản *(coin age)* để xem xét (tính từ lúc tài sản được hold). Node phải hold coin ít nhất 30 ngày trước khi tham gia "tranh cử" làm validator cho block tiếp theo. Như vậy thì node nào nắm giữ nhiều coin với thời gian lâu hơn sẽ có tính cạnh tranh hơn. Sau mỗi lần, tuổi đời của tài sản sẽ được "reset" trở về số 0 và phải chờ ít nhất 30 ngày nữa trước khi được quyền "tranh cử" xử lý một block khác. Ngoài ra, số ngày tối đa tham gia tranh cử là 90 ngày. Điều này giúp tránh tình trạng thao túng của những node sở hữu quá nhiều tài sản.

Ưu điểm của PoS

Tăng được lượng coin của holder. Nên dù giá có giảm thì bạn vẫn có thể lời một chút từ coin của mình.

Đào coin POS không cần máy có cấu hình khủng, chỉ cần máy tính có internet và online 24/24 thì bạn đã có thể đào được rồi.

Chi phí đào coin POS rẻ hơn POW rất nhiều. Bạn không phải tốn nhiều năng lượng như đào coin POW. Nếu không thích đào nữa thì bạn có thể chuyển coin lên sàn và bán đi là xong.

Nhược điểm của POS

Staking không phải lúc nào cũng lãi nếu lãi suất stake thấp hơn mức giảm giá coin thì holder sẽ bị lỗ.

Lãi staking không phải lúc nào cũng đồng đều.

Rủi ro bị scam, lừa đảo,… nếu bạn lựa chọn nền tảng staking không uy tín, hoặc lựa chọn coin "rác".

Vấn đề độc quyền

Độc quyền mạng lưới: Nếu một bên nắm quyền kiểm soát phần lớn tài nguyên xác thực giao dịch, thực thể này có thể sử dụng tài nguyên để áp đặt các điều kiện cho phần còn lại của mạng lưới. Từ đó, nhà độc quyền có thể chọn thực hiện những cách độc hại như double-spending (lặp chi) hoặc từ chối dịch vụ. Nếu nhà độc quyền chọn một chiến lược độc hại và duy trì sự kiểm soát của mình trong thời gian dài, niềm tin vào mạng lưới blockchain sẽ bị hủy hoại.

Các giải quyết của PoS: Những đồng coin sử dụng thuật toán Proof-of-Stake vẫn có thể gặp vấn đề độc quyền. Tuy nhiên, mạng lưới POS sẽ an toàn hơn trước các cuộc tấn công độc hại. Vì hai lý do như sau. Thứ nhất, rất khó để độc quyền trên mạng lưới POS. Như đã đề cập ở trên, các Masternode phải hold và stake coin mới có thể tham gia xác minh giao dịch. Nếu muốn độc quyền, holder phải mua trữ rất nhiều đồng coin (ít nhất 51% tổng cung). Chi phí bỏ ra là vô cùng lớn. Thứ hai, và quan trọng hơn, nhà độc quyền không có lợi ích gì khi tự tổn hại mạng lưới mà mình đang đầu tư rất nhiều tiền. Tấn công bất lợi đối với mạng lưới sẽ làm cho nhà đầu tư mất niềm tin vào đồng coin, từ đó cầu giảm, sẽ dẫn đến giá giảm. Như vậy, quỹ coin đang stake của bên độc quyền cũng bị tổn hại.

4.3 So sánh PoW và PoS

PoS là sự cải tiến của PoW nên có nhiều ưu điểm hơn:

- Do không cần tính toán giải các hàm hash phức tạp, mạng lưới PoS tốn ít thời gian và năng lượng hơn nhiều so với PoW.
- Mạng lưới sử dụng thuật toán PoS an toàn và phân quyền hơn PoW.
- Với PoW, việc đào coin hiện nay chỉ hiệu quả với những hệ thống máy đào lớn, năng lượng cao. Điều này dẫn tới sức mạnh của toàn hệ thống chủ yếu tập trung ở các mining pool lớn. Làm cho mạng lưới PoW trở nên tập trung hơn.

IV. Khóa, địa chỉ

Quyền sở hữu của bitcoin được thiết lập thông qua các khóa số, địa chỉ bitcoin và chữ kí số. Các khóa số này không được lưu trữ trên mạng lưới mà do người dùng tạo ra và lưu trữ trong một file, hay một cơ sở dữ liệu đơn giản, gọi là ví. Các khóa số trong ví của người dùng hoàn toàn độc lập với giao thức bitcoin và phầm mềm ví của người dùng có thể tạo và quản lí chúng mà không cần tham chiếu đến blockchain hay phải kết nối Internet. Khóa là nhân tố kích hoạt nhiều thuộc tính thú vị của bitcoin, bao gồm kiểm soát và tín nhiệm phi tập trung, xác thực quyền sở hữu và mô hình an ninh sử dụng bằng chứng mật mã.

Để được đưa vào blockchain, hầu hết các giao dịch bitcoin đều phải có chữ kí số hợp lệ, vốn chỉ có thể tạo ra bằng khóa bí mật; do đó bất cứ ai có bản sao của khóa này đều có thể kiểm soát lượng bitcoin đó. Chữ kí số dùng để chi tiêu bitcoin còn gọi là nhân chứng (witness), một thuật ngữ dùng trong mật mã học. Dữ liệu các nhân chứng trong giao dịch bitcoin chứng thực cho quyền sở hữu thực sự đối với lượng tiền đang được chi tiêu.

Các khóa đi theo một cặp, bao gồm một khóa bí mật (cá nhân) và một khóa công khai. Người dùng bitcoin ít khi nhìn thấy các số khóa này vì chúng hầu hết được lưu trong file ví và được phần mềm ví bitcoin quản lí.

Trong phần thanh toán của một giao dịch bitcoin, khóa công khai của một người nhận được đại diện bằng vân tay số của nó, gọi là địa chỉ bitcoin, có vai trò như tên người thụ hưởng trong giao dịch ngân hàng. Thông thường, địa chỉ bitcoin được tạo ra từ khóa công khai và tương ứng với khóa đó. Địa chỉ của ví là đại diện duy nhất của khóa mà người dùng sẽ thường xuyên nhìn thấy, bởi vì đây là phần mã mà họ sẽ chia sẻ công khai.

1. Mật mã khóa công khai và tiền mã khóa

Mật mã khóa công khai sử dụng các hàm toàn học bất khả nghịch (tính toán dễ dàng theo chiều thuận, nhưng không thể tính toán theo chiều nghịch). Dựa trên các hàm toán học này, mật mã học cho phép tạo ra các bí mật số và các chữ kí số không thể làm giả. Bitcoin sử dụng phép nhân đường cong elliptic làm nền tảng cho mật mã học của nó.

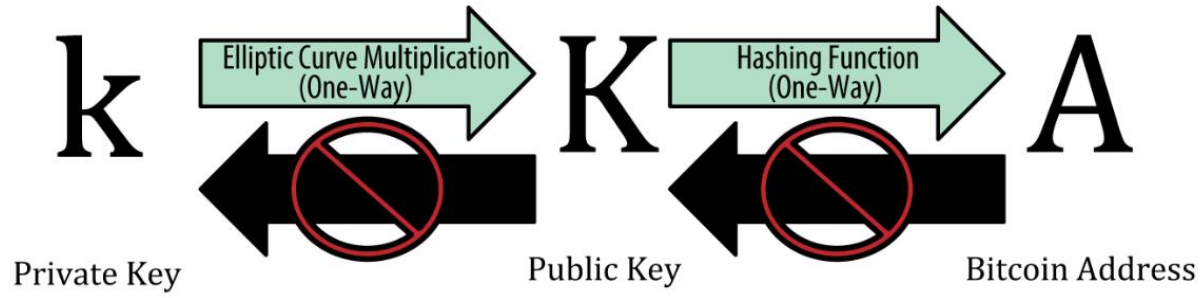
Trong bitcoin, chúng ta dùng mật mã học khóa công khai để tạo ra một cặp khóa kiểm soát quyền tiếp cận bitcoin. Cặp khóa này bao gồm 1 khóa bí mật và 1 khóa công khai sinh ra duy nhất từ nó. Khóa công khai dùng để nhận tiền còn khóa bí mật dùng để ký các giao dịch chi tiêu lượng tiền đấy.

Giữa khóa bí mật và khóa công khai có một mối quan hệ toán học cho phép dùng khóa bí mật để tạo các chữ kí trên gói tin, từ đó có thẻ xác thực chữ kí này có khớp với khóa công khai hay không mà không làm lộ khóa bí mật.

Khi chi tiêu bitcoin, chủ sỡ hữu sẽ sử dụng khóa công khai và chữ kí của mình (mỗi giao dịch sẽ có các chữ kí khác nhau nhưng đều được tạo ra từ cùng một khóa bí mật). Thông qua việc trình diện khóa công khai và chữ kí, tất cả các thành viên trong mạng bitcoin đều có thể xác minh và chấp nhận giao dịch này là hợp lệ, xác nhận người đang chuyển số bitcoin này là chủ sở hữu của chúng tại thời điểm giao dịch.

2. Khóa bí mật và khóa công khai

Một ví bitcoin chứa nhiều cặp khóa, mỗi cặp gồm 1 khóa bí mật và 1 khóa công khai. Khóa bí mật (k) là một số, thường được chọn ngẫu nhiên. Từ khóa bí mật, ta sử dụng phép nhân đường cong elliptic (một hàm mật mã một chiều) để tạo ra khóa công khai (K). Từ khóa công khai K, ta dùng một hàm băm mật mã một chiều để tạo ra một địa chỉ bitcoin (A).



Hình 4: Mối quan hệ giữa khóa bí mật, khóa công khai và địa chỉ bitcoin.

2.1 Khóa bí mật

Một khóa bí mật chỉ đơn thuần là một con số được chọn ra ngẫu nhiên. Quyền sở hữu và kiểm soát đối với khóa bí mật là nguồn gốc tạo nên quyền kiểm soát của người dùng đối với toàn bộ lượng tiền gắn với địa chỉ bitcoin tương ứng. Khóa bí mật dùng để tạo ra các chữ ký, một yêu cầu bắt buộc để chứng minh quyền sở hữu đối với một lượng tiền trong giao dịch. Khóa bí mật luôn phải được giữ bí mật, việc tiết lộ nó với bên thứ ba đồng nghĩa với việc trao quyền kiểm soát lượng bitcoin đang được khóa đó bảo vệ. Cũng cần dự phòng và bảo vệ khóa bí mật khỏi bị mất, bởi khóa bị mật sẽ không thế khôi phục và lượng tiền mà nó đang bảo vệ cũng sẽ biến mất theo.

2.2 Tạo khóa bí mật từ một số ngẫu nhiên

Bước đầu tiên, quan trọng nhất là tìm được nguồn Entropy an toàn. Về bản chất, việc tạo ra khóa bitcoin giống như việc chọn số từ 1 đến 2^{256}. Việc sử dụng phương pháp nào để chọn số không quan trọng, miễn là nó không thể dự đoán được hay không thể lặp lại được. Phần mềm bitcoin dùng trình tạo số ngẫu hiên của hệ điều hành bên dưới để tạo ra 256 bit entropy.

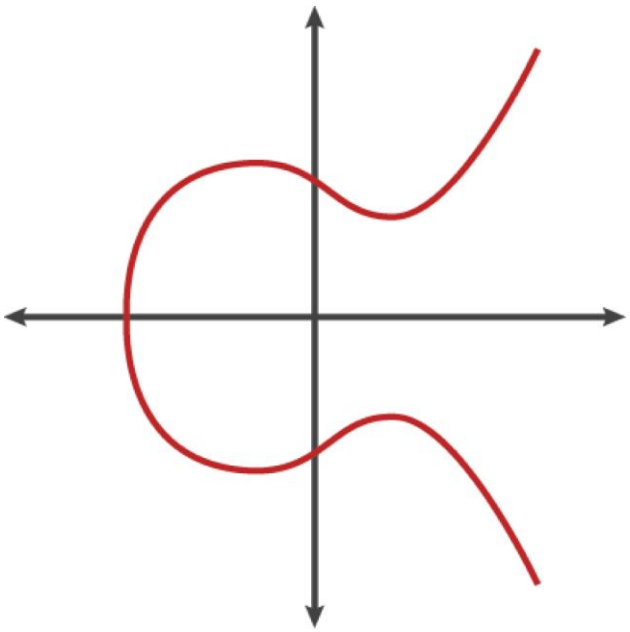
Chính xác hơn, khóa bí mật có thể là bất kì nguồn nào giữa 1 và n-1, trong đó n là một hằng số (n = $1{,}158.10^{77}$, nhỏ hơn một chút so với 2^{256}) được định nghĩa là bậc của đường cong elliptic dùng trong bitcoin. Để tạo ra một khóa như vậy, ta chọn ngẫu nhiên 1 số 256 bit và kiểm tra lại để đảm bảo rằng số này nhỏ hơn n-1. Theo cách nói khác, có thể đạt được điều này bằng cách đưa ra một chuỗi các bit ngẫu nhiên dài hơn (được thu nhập từ các nguồn ngẫu nhiên an toàn về mặt mật mã) vào một thuật toán băm SHA256, từ đây sẽ dễ dàng tạo ra một số 256 bit. Nếu số này nhỏ hơn n-1, ta được một khóa ngẫu nhiên phù hợp, nếu không ta chọn lại một số ngẫu nhiên khác.

2.3 Khóa công khai

Khóa công khai được tính ra từ khóa bí mật bằng phép nhân đường cong elliptic bất khả nghịch: K=k*G, trong đó k là khóa bí mật, G là một điểm bất biến gọi là phần tử sinh (generator point), và K là khóa công khai thu về. Phép tính ngược lại (được gọi là tìm logarit rời rạc) – tính k khi biết K là phép tính khó tương đương với việc thử vét cạn tất cả các giá trị có thể của k.

2.4 Mật mã đường cong elliptic

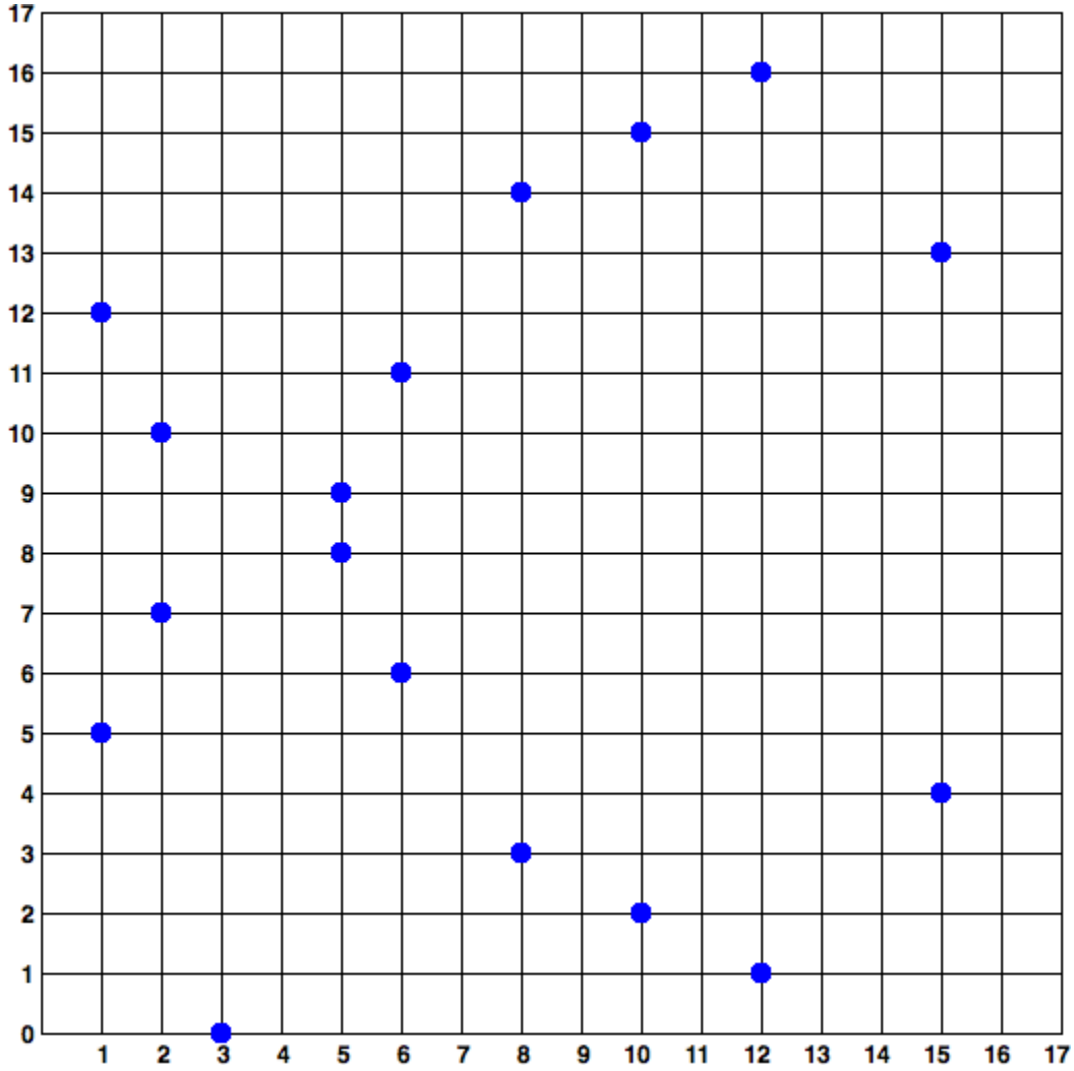
Mật mã đường cong elliptic là một dạng mật mã bất đối xứng hay mật mã khóa công khai dựa trên bài toán logarit rời rạc được biểu diễn bằng phép cộng và phép nhân trên các điểm của một đường cong elliptic.



Hình 5: Hình vẽ một đường cong elliptic

Bitcoin sử dụng một đường cong elliptic và một tập các hằng số toán học cụ thể, được định nghĩa trong một tiêu chuẩn gọi là secp256k1 do Viện Tiêu chuẩn và Kỹ thuật Quốc gia Hoa Kì (NIST) đặt ra. Đường cong secp256k1 được định nghĩa bằng hàm tạo đường cong elliptic sau đây:

$y^2 = (x^3 + 7)$ trên (F_p)
hay $y^2 \bmod p = (x^2 + 7) \bmod p$
Toán tử mod p thể hiện rằng đường con này nằm trên một trường hữu hạn có bậc nguyên tố p, còn được viết là F_p, trong đó $p = 2^{256} – 2^{32} – 2^9 – 2^8 – 2^7 – 2^6 – 2^4 – 1$ là một số nguyên tố rất lớn.



Hình 6: Hình ảnh biểu diễn một đường cong elliptic trên F(p) với p=17.

Do đường cong này được định nghĩa trên một số trường hữu hạn có bậc nguyên tố thay vì trên các số thực, nên nó trông giống như một tập hợp các chấm rải rác trong mặt phẳng 2 chiều, vì vậy nên rất khó hình dung. Tuy vậy, phần toán học này lại giống hệt với một đường cong elliptic trên các số thực. Hình ảnh trên biểu diễn cùng một đường cong elliptic như vậy trên một trường hữu hạn nhỏ hơn rất nhiều có bậc nguyên tố 17, qua đó có thể thấy một tập hợp các chấm trên một lưới tọa độ. Có thể hình dung đường cong elliptic bitcoin secp256k1 như một sơ đồ với các chấm phức tạp hơn rất nhiều, trên một lưới tọa độ vô cùng lớn.
Ví dụ về một điểm P trên đường cong secp256k1 với tọa độ (x, y):

P=(55066263022277343669578718895168534326250603453777594175500187360389116729240,32670510020758816978083085130507043184471273806592432759389043357573374824 24)

Trong toán học đường cong elliptic, có một điểm được gọi là "điểm vô cực", khá tương đồng với vai trò của số 0 trong phép cộng. Trên máy tính, đôi khi điểm này được biểu diễn bằng x = y = 0 (không thỏa mãn phương trình đường cong elliptic, nhưng đây là một trường hợp riêng biệt, có thể dễ dàng kiểm tra được).

Ngoài ra, còn có một toán tử +, được gọi là phép cộng, có các thuộc tính tương tự với phép cộng hai số thực thông thường. Cho hai điểm P_1, P_2 trên đường cong elliptic, có một điểm thứ ba $P_3 = P_1 + P_2$ cũng nằm trên đường cong đó.

Trong hình học, điểm P_3 này được tính bằng cách kẻ một đường thẳng nối P_1 và P_2. Đường thẳng này sẽ cắt đường cong elliptic tại một điểm nữa. Gọi điểm này là $P_3' = (x, y)$. Đối xứng điểm này qua trục x là điểm $P_3 = (x, -y)$.

2.5 Tạo khóa công khai

Từ một khóa bí mật dưới dạng một số được tạo ngẫu nhiên k, ta nhân nói với một điểm cho trước trên đường cong gọi là phần tử sinh G để tạo ra một điểm khác nằm ở đâu đó trên đường cong, chính là khóa công khai tương ứng K. Phần tử sinh được xác định là một phần chuẩn của secp256k1 và luôn giống nhau với mọi khóa trong bitcoin: K = k * G, trong đó k là khóa bí mật, G là phần tử sinh và K là khóa công khai tính được, cũng là một điểm trên đường cong. Do phần tử sinh là như nhau cho mọi người dùng bitcoin, nên khi nhân một khóa bí mật k với G, kết quả thu về sẽ luôn là một khóa công khai K. Mối quan hệ giữa k và K là cố định, nhưng chỉ có thể tính được một chiều từ k đến K. Đó là lý do vì sao người dùng có thể chia sẽ với bất cứ ai có địa chỉ bitcoin khóa K (công khai) mà không làm lộ khóa k (bí mật).

Thực hiện phép nhân đường cong elliptic, ta lấy khóa bí mật k được tạo ra trước đó nhân với phần tử sinh G để tìm khóa công khai K:

K=1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD * G

Khóa công khai K được định nghĩa là một điểm K = (X, y):

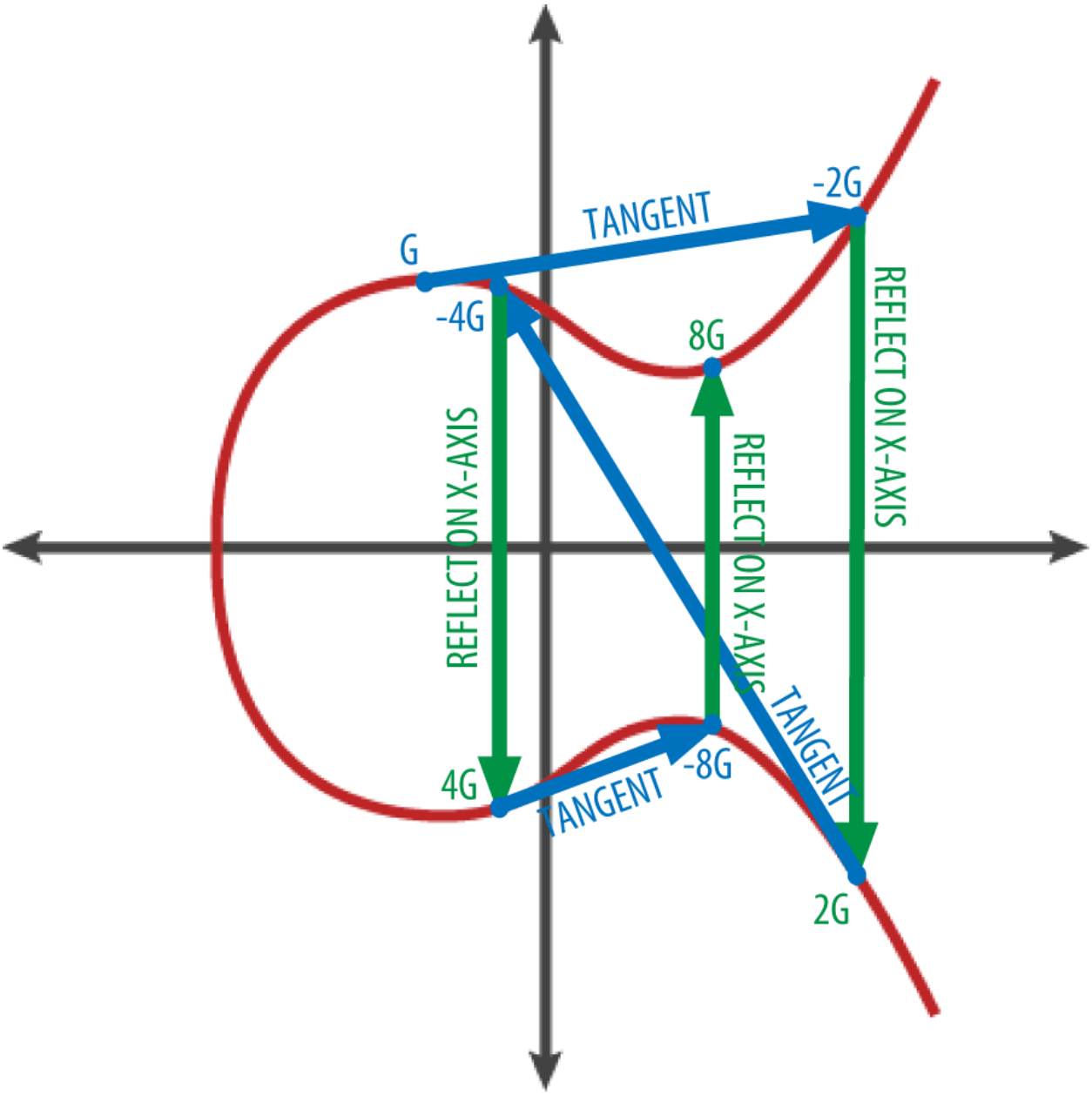
K = (x, y)

Trong đó

x=F028892BAD7ED57D2FB57BF33081D5CFCF6F9ED3D3D7F159C2E2FFF579DC341A

y=07CF33DA18BD734C600B96A72BBC4749D5141C90EC8AC328AE52DDFE2E505BDB

Để minh họa cho phép nhân một điểm với một số nguyên, ta sẽ dùng một đường cong elliptic đơn giản hơn trên các số thực. Mục tiêu của chúng ta là tìm tích số kG của phần tử sinh G, tương tự với việc nhân G với chính nó k lần liên tiếp. Tring đường cong elliptic, việc cộng thêm một điểm với chính nó tương đương với việc vẽ một tiếp tuyến tại điểm đó và xem nó cắt đường cong này một lần nữa tại đâu, sau đó đối xứng điểm này qua trục x.



Hình 7: Hình ảnh minh họa phép nhân một điểm G với một số nguyên k trên một đường cong elliptic

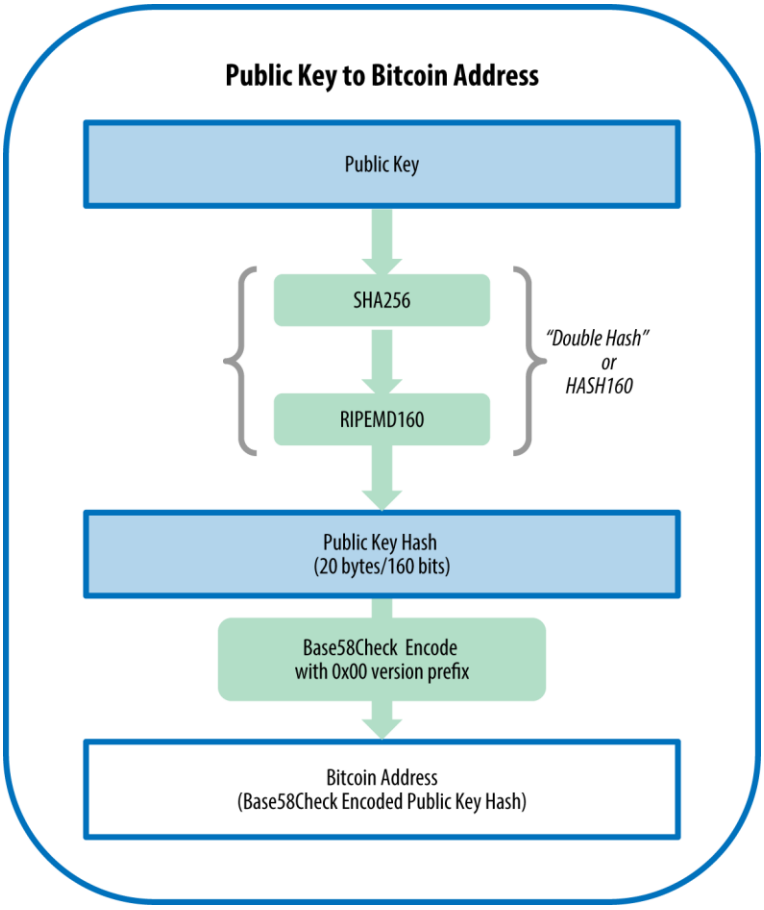
3. Địa chỉ Bitcoin

Địa chỉ bitcoin là một dãy các chữ số và ký tự có thể chia sẻ với bất kì ai muốn chuyển tiền cho bạn. Các địa chỉ tạo ra từ các khóa công khai bao gồm một dãy các số và chữ cái, bắt đầu với số "1". Đây là một ví dụ về địa chỉ bitcoin:

`1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy`

Địa chỉ bitcoin là thứ xuất hiện nhiều nhất trong các giao dịch dạng người nhận tiền. Nếu so sánh giao dịch bitcoin với giao dịch ngân phiếu giấy, địa chỉ bitcoin chính là tên người thụ hưởng. Một

địa chỉ bitcoin đại diện cho người sở hữu một cặp khóa bí mật/ công khai, hoặc nó có thể đại diện cho một thứ khác, ví dụ như một kịch bản thanh toán.
Địa chỉ bitcoin được tạo ra từ khóa công khai bằng hàm băm mật mã một chiều. Thuật toán băm là hàm một chiều tạo ra vân tay hay mã băm của một đầu vào có độ lớn bất kì. Các hàm mật mã được sử dụng rất nhiều trong bitcoin: trong các địa chỉ bitcoin, trong các địa chỉ kịch bản, … Các thuật toán được sử dụng để tạo ra địa chỉ bitcoin từ khóa công khai là thuật toán băm an toàn (Secure Hash Algorithm – SHA) và thuật toán RACE Intergrity Primitives Evaluation Message Digest (RIPEMD), cụ thể là SHA256 và RIPEMD160.
Từ một khóa công khai K, ta tính mã băm SHA256 rồi tính mã băm RIPEMD160 của kết quả thu về, từ đó tạo ra một số 160 bit (20 byte).
A = RIPEMD160(SHA256(K)), trong đó K là khóa công khai, còn A là địa chỉ bitcoin tính toán được.
Các địa chỉ bitcoin hầu như luôn được mã hóa dưới dạng Base58Check, trong đó sử dụng 58 kí tự (một hệ cơ số 58) và một dữ liệu checksum để tăng tính dễ đọc cho con người, tránh nhầm lẫn, tránh sai sót khi sao chép và nhập địa chỉ. Base58Check cũng được sử dụng theo nhiều cách khác nữa trong bitcoin cho những trường hợp người dùng phải đọc và ghi lại đúng một con số, ví dụ như địa chỉ của bitcoin, khóa bí mật, khóa mã hóa hay mã băm kịch bản.



Hình 8: Hình ảnh minh họa sự chuyển đổi khóa công khai thành địa chỉ bitcoin

Mã hóa Base58 và Base58Check

Để biểu diễn các số dài một cách ngắn gọn và sử dụng ít biểu tượng hơn, nhiều hệ thống máy tính vận dụng các hình thức biểu diễn kết hợp giữa số và chữ cái để biểu diễn một hệ cơ số lớn hơn 10 (ví dụ hệ hexa). Gọn hơn nữa, biểu diễn Base64 (hệ cơ số 64) sử dụng 26 chữ cái viết thường, 26 chữ cái viết hoa, 10 chữ số và thêm 2 kí tự như "+" và "/" để truyền dữ liệu nhị phân qua các phương tiện truyền thông dưa trên văn bản như email. Base64 được sử dụng chủ yếu để thêm dữ liệu nhị phân đính kèm qua email. Base58 là một dạng mã hóa nhị phân dựa trên văn bản được phát triển đẻ sử dụng trong bitcoin và nhiều loại tiền mã hóa khác. Nó mang đến một sự cân bằng giữa hình thức biểu diễn ngắn ngọn, tinh dễ đọc và khả năng phát hiện và ngăn ngừa sai sót. Base58 là một tập con của Base64, sử dụng chữ hoa và chữ thường nhưng bỏ qua một số kí tự thường dễ bị nhầm lẫn với nhau.

Ví dụ bảng chữ cái đầy đủ của Base58:

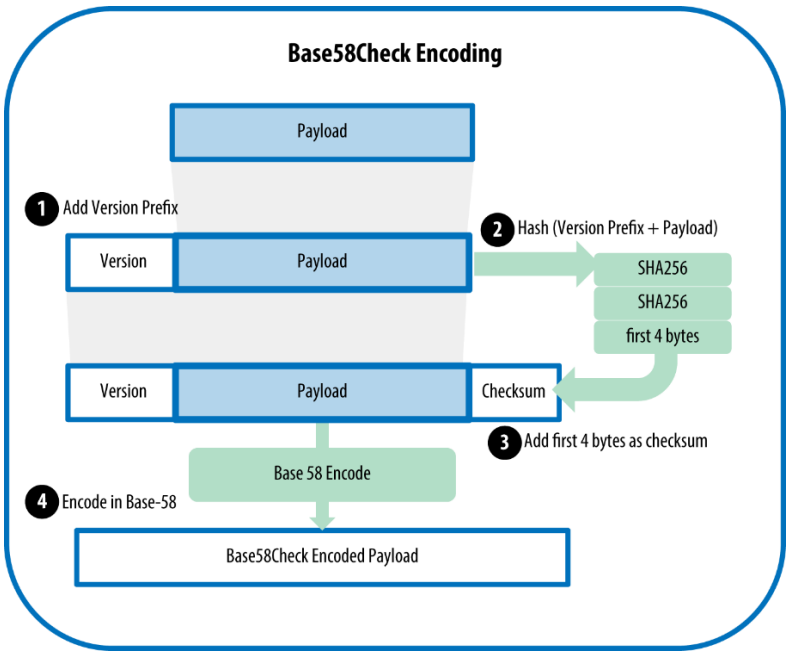
```
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz
```

Để ngăn chặn hiệu quả hơn nữa các lỗi đánh máy hay đọc nhầm, bitcoin còn sử dụng Base58Check, một dạng mã hóa Base58 được tích hợp mã kiểm tra lỗi. Mã checksum là một nhóm gồm 4 byte được thêm vào cuối dữ liệu đang được mã hóa. Giá trị checksum này được tạo ra từ giá trị mã băm của dữ liệu mã hóa, do đó có thể dùng để phát hiện hoặc ngăn chặn các lỗi đánh máy hay sao chép. Khi thấy một mã Base58Check, phần mềm giải mã sẽ tính toán checksum của dữ liệu và so sánh với checksum đi kèm theo mã. Nếu hai giá trị này không khớp với nhau, có nghĩa là đã phát sinh lỗi và dữ liệu Base58Check này được xem như không hợp lê.

Điều này giúp ngăn ngừa việc phàm mềm vì chấp nhận một địa chỉ bitcoin bị gõ nhầm là đích đến hợp lê, tránh việc mất tiền oan.

Để chuyển dổi dữ liệu (một con số) sang dạng Base58Check, đầu tiên ra thêm một tiền tố vào dữ liệu, gọi là "byte phiên bản", nhằm dễ dàng xác định dữ liệu được mã hóa. Ví dụ, trong trường hợp địa chỉ bitcoin, phần tiền tố là 0 (0x00 trong hệ hexa), còn tiền tố dùng để mã hóa khóa bí mật là 128 (0x80 trong hệ hexa). Tiếp theo, ta tính checksum SHA kép, tức là áp dụng thuật toán băm SHA256 hai lân trên kết quả vừa được tạo ra (tiền tố + dữ liệu):

```
checksum = SHA256(SHA256(prefix+data))
```



Hình 9: Hình ảnh một định dạng Base58 có đánh số phiên bản và checksum dùng để mã hóa dữ liệu bitcoin tránh nhầm lẫn

Từ kết quả của mã băm 32 byte, ta chỉ lấy 4 byte đầu tiên làm mã kiểm tra lỗi, hay checksum, checksum này được nối vào cuối dữ liệu. Kết quả cuối cùng bao hồm 3 phần: một tiền tố, dữ liệu và một checksum. Kết quả này được mã hóa bằng bảng ký tự Base58 đã đề cập.
Trong bitcoin, hầu như các dữ liệu hiển thị cho người dùng đều được mã hóa Base58Check để chúng trở nên dễ đọc, ngắn ngọn và dễ phát hiện lỗi. Tiền tố phiên bản trong mã hóa Base58Check được dùng để tạo ra các định dạng dễ phân biệt. Khi được mã hóa trong hệ Base58, các định dạng này sẽ chưa các ký tự đặc biệt ở đầu của dữ liệu được mã hóa Base58Check. Các ký tự này giúp con người dễ xác định được loại dữ liệu được mã hóa và cách sử dụng của nó. Đây là điều giúp phân biệt giữa, chẳng hạn, một địa chỉ bitcoin được mã hóa Base58Check bắt đầu bằng số 1 với 1 khóa bí mật WIF được mã hóa Base58Check bắt đầu bằng số 5. Bảng sau đây ví dụ về các tiền tố phiên bản và các ký tự kết quả trong Base58 tương ứng:

Loại	Tiền tố phiên bản (hệ hexa)	Tiền tố kết quả trong Base58
Địa chỉ bitcoin	0x00	1
Địa chủ P2H	0x05	3
Địa chỉ testnet bitcoin	0x6F	m hoặc n
Khóa bí mật WIF	0x80	5, K hoặc L
Khóa bí mật mã hóa BIP-38	0x0142	6P
Khóa công khai mở rộng BIP-32	0x0488B21E	xpub

4. Các định dạng khóa

Có thể biểu diễn khóa bí mật và khóa công khai theo một số định dạng khác nhau. Tuy trông khác nhau, song các hình thức biểu diễn này đều mã hóa cùng một số giống nhau. Các định dạng này được sử dụng chủ yêu để giúp người dùng có thể dễ dàng đọc và sao chép các khóa mà không mắc sai sót.

4.1 Các dạng khóa bí mật

Có thể biểu diễn khóa bí mật theo một số định dạng khác nhau, tất cả đều tương ứng với một số 256 bit. Các định dạng khác nhau được dùng trong những tình huống khác nhau. Các định dạng trong hệ hexa và hệ nhị phân thường được dùng nội bộ trong phần mềm và ít hiển thị với người dùng. WIF được dùng để nhập/ xuất các khóa giữa các ví và thường được dùng để biểu diễn mã QR (mã vạch) của khóa bí mật.

Loại	**Tiền tố**	**Mô tả**
Thô	Không có	32 byte
Hexa	Không có	64 chữ số hệ hexa
WIF	5	Mã hóa Base58Check: Base58 với tiền tố phiên bản là 128 và mã checksum 32 bit
WIF nén	K hoặc L	Như trên, thêm vào hậu tố 0x01 trước khi mã hóa

Ví dụ:

Định dạng	**Khóa bí mật**
Hexa	1e99423a4ed27608a15a2616a2b0e9e52ced330ac530edcc32c8ffc6a526aedd
WIF	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
WIF nén	KxFC1jmwwCoACiCAWZ3eXa96mBM6tb3TYzGmf6YwgdGWZgawvrtJ

Tất cả những dạng biểu diễn này chỉ những cách thức khác nhau để biểu diễn cùng một số, cùng một khóa bí mật. Tuy chúng trông khác nhau, nhưng có thể chuyển dổi từ một dạng bất kì này sang một dạng bất kì khác.

4.2 Các dạng khóa công khai

Các khóa công khai cũng có thể được biểu diễn theo nhiều cách khác nhau, thường là dưới dạng khóa nén hoặc không nén.

Như chúng ta đã thầy ở trên, khóa công khai là một điểm trên đường cong elliptic, bao gồm một cặp tọa độ (x, y). Nó thường được biểu diễn với một tiền tố 04 theo sau là 2 số 256 bit: một là tọa độ của điểm x, số còn lại là tọa độ của điểm y. Tiền tố 04 dùng để phân biệt khóa công khai nén với khóa công khai không nén (bắt đầu bằng 02 hoặc 03).

Sau đây là khóa công khai được tạo ra từ khóa bí mật ở trên, biểu diễn dưới dạng tọa độ x, y:

```
x=F028892BAD7ED57D2FB57BF33081D5CFCF6F9ED3D3D7F159C2E2FFF579DC34
1A
```

y=07CF33DA18BD734C600B96A72BBC4749D5141C90EC8AC328AE52DDFE2E505BDB

Đây cũng chính là kháo công khai được biểu diễn dưới dạng một số 250 bit (130 chữ số hexa) với tiền tố 94 theo sau với các tọa độ x và y, dạng 04 x y:

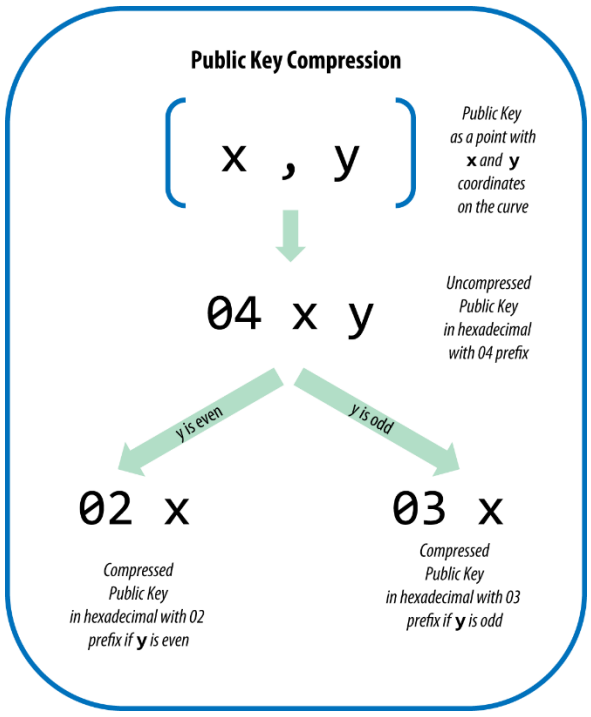
K=04F028892BAD7ED57D2FB57BF33081D5CFCF6F9ED3D3D7F159C2E2FFF579DC341A07CF33DA18BD734C600B96A72BBC4749D5141C90EC8AC328AE52DDFE2E505BDB

Khóa công khai nén

Khóa công khai nén được đưa vào bitcoin để giảm kích cỡ các giao dịch và tiết kiệm dung lượng ổ cứng trên các nút chứa cơ sở dữ liệu blockchain của bitcoin. Hầu hết các giao dịch đều chứa khóa công khai, vốn là một điều kiện bắt buộc để xác thực thẩm quyền của chủ sở hữu và để chi tiêu bitcoin. Một khóa công khai chiếm 520 bit (tiền tố + x + y), và khi nhân nó với hàm trăm giao dịch trong mỗi block, hoặc hàng vạn giao dịch mỗi ngày ta sẽ nhận được một khối dữ liệu đáng kể được thêm vào blockchain.

Như chúng ta thầy trong phần "Khóa công khai", khóa công khai là một điểm (x, y) trên đường cong elliptic. Bởi vì đường cong này biểu diễn một hàm toán học và một điểm trên đường cong này đại diện cho một nghiệm của phương trình, nên nếu chỉ biết tọa độ x ta có thể tính tọa độ y bằng cách giải phương trình $y^2 \bmod p = (x^3 + 7) \bmod p$. Điều này cho phép chúng ta chỉ cần lưu tọa độ x của điểm khóa công khai, bỏ qua tọa độ y và giảm đi 256 dung lượng bit nhớ của khóa cũng như dung lượng cần để lưu trữ nó. Một mức giảm gần 50% về kích thước trong mỗi giao dịch như vật khi cộng lại sẽ tạo thành một lượng dữ liệu rất lớn được tiết kiệm theo thời gian.

Trong khi các khóa công khai không nén có tiền tố 04, các khóa công khai nén bắt đầu bằng tiền tố 02 hoặc 03, bởi vì vế trái của phương trình là y^2, nghiệm y sẽ là một căn bậc hai, có nghĩa là giá trị có thể âm hoặc dương. Hình dung trực quan, điều này có nghĩa là kết quả tọa độ của đồ thị y có thể nằm trên hoặc dưới trục x. Vì vậy, tuy có thể bỏ qua tọa độ y, nhưng ta vẫn cần lưu lại dấu của y; hay nói cách khác, ta phải nhớ xem nó ở trên hay dưới trục x vì mỗi cách chọn sẽ cho ra một điểm khác nhau và một khóa công khai khác nhau. Khi tính toán đường cong elliptic trong số học nhị phân trên một trường hữu hạn bậc nguyên tố p, tọa độ y sẽ có giá trị chẵn hoặc lẻ, tương ứng với dầu dương/ âm như vừa giải thích. Vì thế, để phân biệt 2 giá trị khả thi này của y, ta lưu một khóa công khai nén tiến tối 02 nếu y chẵn, 03 nếu y lẻ, cho phép phầm mềm tự suy ra đúng tọa độ y từ tọa độ x và giải nén khóa công khai ra tọa độ đầy đủ của điểm.



Hình 10: Hình ảnh phép nén khóa công khai

Dưới đây là khóa công khai đã tạo ở trên, được biểu diễn dưới dạng một khóa công khai nén lưu trữ trong 264 bit (66 chữ số hệ hexa) với tiền tố 03 ngụ ý tọa độ y là lẻ:

`K=03F028892BAD7ED57D2FB57BF33081D5CFCF6F9ED3D3D7F159C2E2FFF579DC341A`

Khóa công khai nén này tương ứng với cùng một khóa bí mật, nghĩa là nó được tạo ra từ cùng một khóa bí mật. Tuy nhiên, trông nó khác với khóa công khai không nén. Quan trọng hơn, nếu chuyển đổi khóa công khai nén này thanh một địa chỉ bitcoin thông qua hàm băm kép (RIPEMD(SHA256(K)), nó sẽ tạo ra một địa chỉ bitcoin khác. Điều này có thể gây nhầm lẫn, bởi vì như thế có nghĩa là một khóa bí mật có thể tạo ra một khóa công khai biểu diễn theo hai định dạng khác nhau (nén và không nén) và từ đó có thể tạo ra 2 địa chỉ bitcoin khác nhau. Tuy vậy, với cả 2 địa chỉ bitcoin này, khóa bí mật vẫn chỉ là một.

Khóa cong khai nén dần trở thành yếu tố mặc định trong các phầm mềm bitcoin, qua đó góp phần đáng kể vào việc giảm kích thước giao dịch và do đó giảm cả kích thước blockchain. Tuy nhiên, không phải tất cả phần mềm đều hỗ trợ khóa công khai nén.

Các phầm mêm mới ra đời có hỗ trợ khóa công khai nén phải tính đến các giao dịch từ các phần mềm trước đó, vốn không hỗ trợ khóa công khai nén. Điều này đặc biệt quan trọng khi một ứng dụng ví nhập khóa bí mật từ một ứng dụng bitcoin khác, bởi vì ví mới sẽ phải quét blockchain để tìm các giao dịch tương ứng với khóa được nhập này. Ví bitcoin nên quét tìm các địa chỉ nào: địa chỉ được tạo bởi khóa công khai không nén hay địa chỉ được tạo bởi khóa công khai nén? Cả hai đều là địa chỉ bitcoin hợp lệ, đều có thể ký bởi cùng môt khóa bí mật, nhưng chúng lại là 2 địa chỉ khác nhau.

Để giải quyết vấn đề này, khi khóa bí mật được xuất từ một ví, định dạng WIF biểu diễn chúng sẽ được cài đặt khác đi trong các ví bitcoin mới hơn, qua đó chỉ ra rằng các khóa bí mật này được dùng để tạo ra các khóa công khai nén và vì thế tạo ra các địa chỉ bitcoin nén. Điều này cho phép ví nhập các khóa này có thể phân biệt được các khóa bí mật có nguồn gốc từ ví cũ hay ví mới và tìm trên blockchain những giao dịch có các địa chỉ bitcoin tương ứng với các khóa công khai không nén hay nén.

Khóa bí mật nén

Thuật ngữ "khóa bí mật nén" là một cách gọi sai, bởi khóa bí mật nén khi được xuất dữ liệu dưới dạng WIF nén thực ra lại dài hơn 1 byte so với một khóa bí mật không nén. Sở dĩ như vậy là khóa bí mật có thêm 1 byte hậu tố (biểu diễn là 01 trong hệ hexa) ngụ ý rằng khóa bí mật này xuất phát từ một phần mềm ví mới hơn và chỉ nên dùng nó để tọa khóa công khai nén. Bản thân khóa bí mật không thể nén và không thể bị nén. Thuật ngữ "khóa bí mật nén" thực ra có nghĩa là "khóa bí mật chie nên dùng để tạo khóa công khai nén", trong khi "khóa bí mật không nén" thực ra có nghĩa là "khóa bí mật chỉ nên dùng để tọa khóa công khai không nén". Để tránh nhầm lẫn, chỉ nên gọi định dạng xuất ra là "WIF nén" hay "WIF" chứ không nên gọi bản thân khóa bí mật là nén.

Bảng dưới đây minh họa ví dụ cùng khóa, khác định dạng

Định dạng	Khóa bí mật
Hexa	1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD
WIF	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
Hexa nén	1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD01
WIF nén	KxFC1jmwwCoACiCAWZ3eXa96mBM6tb3TYzGmf6YwgdGWZgawvrtJ

V. Ví điện tử

"Ví điện tử" dùng để nói chỉ một số yếu tố khác nhau trong tiền điện tử.

Ở mức khái quát, ví là ứng dụng đóng vài trò giao diện người dùng chính. Ví kiểm soát quyền truy cập tiền của người dung, quản lý các khóa và địa chỉ, theo dõi số dư, tạo và ký các giao dịch. Ở góc độ hẹp hơn, từ góc nhìn của một lập trình viên, từ "ví" chỉ cấu trúc dữ liệu dùng để lưu trữ và quản lý các khóa của người dùng.

Trong chương này, chúng ta sẽ xem xét nghĩa thứ hai, trong đó ví là nơi chưa các khóa bí mật, thường được cài đặt như các file có cấu trúc hay các cơ sở dữ liệu cơ bản.

1. Tổng quan về công nghệ ví điện tử

Một sự nhầm lẫn khái niệm thường gặp là ví không chứa các loại tiền. Trên thực tế, ví chỉ chứa các khóa. Các "coin" (tiền) được ghi lại vào blockchain trên mạng bitcoin. Người dùng kiểm soát tiền của mình trên mạng lưới bằng cách dùng khóa trong ví để ký các giao dịch, Ở một góc độ nào đó, chúng ta có thể coi ví tiền điện tử là một chùm chìa khóa chứa các cặp khóa bí mật/ công khai.

Người dùng ký các giao dịch bằng các khóa, qua đó chứng minh rằng họ sở hữu đầu ra giao dịch (tức là tiền của họ). Số tiền này được lưu trên blockchain dưới dạng các đầu ra giao dịch (thường được ký hiệu là vout hay txout).

Có hai loại ví chính, được phân biệt bằng mối liên hệ giữa các khóa chứa trong ví

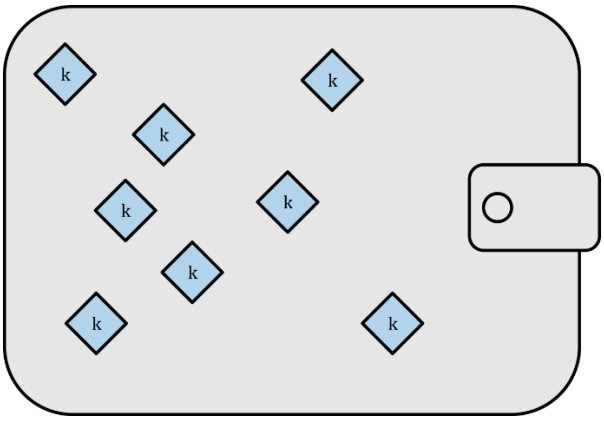
Loại đầu tiên là ví bất định, trong đó mỗi khóa được tạo ra độc lập từ một số ngẫu nhiên. Các khóa này không liên quan đến nhau. Loại ví này được gọi là ví "JBOK", viết tắt của cụm từ "Just a Bunch Of Keys" ("chỉ một đống khóa")

Loại thứ hai là ví tất định, trong đó tất cả các khóa đều được tạo ra từ một khóa duy nhất (master key), hay còn gọi đó là hạt giống (seed). Tất cả các khóa trong loại ví này đều liên quan đế nhau và có thể được tạo lại nếu có hạt giống gốc. Có một số cách tạo khóa khác nhau được dung trong các ví tất định, trong đó cách phổ biết nhất là sử dụng cấu trúc dạng cây gọi là ví tất định phân cấp (hierarchical deterministic) hay ví HD

Các ví tất định được khởi tạo từ một hạt giống. Để chúng dễ sử dụng hơn, các hạt giống được mã hóa thành từ Tiếng Anh, còn được gọi là các từ mật mã trợ nhớ. Các phần tiếp theo sẽ giới thiệu khái quát về các công nghệ này.

2. Ví bất định (Ngẫu nhiên)

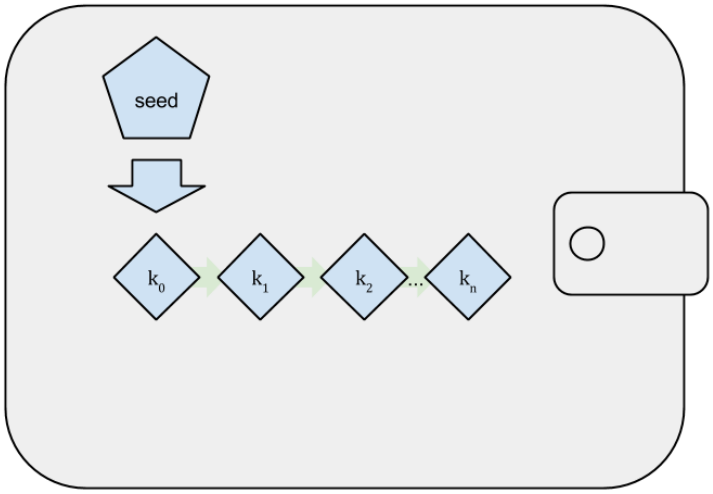
Trong ví tiền điện tử đầu tiên, ví là tập hợp các khóa bí mật được tạo ngẫu nhiên. Ví dụ, phần mềm Bitcoin Core gốc tạo sẵn 100 khóa bí mật ngẫu nhiên khi khởi động lần đầu tiên và tạo ra thêm các khóa khi cần thiết, mỗi khóa chỉ sử dụng một lần. Việc quản lý, sao lưu và nhập các ví này rất phiền phức, vì vậy chúng ta đang bị thay thế bởi các ví tất định. Điểm bất lợi của khóa ngẫu nhiên đấy là nếu tạo nhiều khóa, bạn sẽ phải giữ bản sao của tất cả các khóa đó, điều này cũng đồng nghĩa với việc phải sao lưu ví thường xuyên. Phải sao lưu từng khóa, nếu không số tiền do các khóa kiểm soát sẽ bị mất vĩnh viễn nếu không thể truy cập được ví. Điều này xung đột trực tiếp với nguyên tắc tránh dùng lại địa chỉ thông qua việc sử dụng mỗi địa chỉ cho riêng một giao dịch. Việc dùng lại địa chỉ làm giảm đi tính bảo mật do liên kết nhiều giao dịch và địa chỉ lại với nhau.



Hình 11: Ví bất định (ngẫu nhiên) - một tập hợp các khóa được tạo ngẫu nhiên

3. Ví tất định

Ví tất định là ví chứa các khóa bí mật được tạo ra từ một hạt giống chung bằng hàm băm một chiều, Hạt giống này là một số được tạo ngẫu nhiên sau đó kết hợp với dữ liệu khác, ví dụ một số chỉ số hay một "mã chuỗi" (chain code) để tạo ra các khóa bí mật. Trong ví tất định, chỉ cần hạt giống này là sẽ khôi phục lại tất cả các kháo đã được tạo ra, do đó chỉ cần một bản sao lưu vào thời điểm tạo là đủ. Hạt giống này cũng có thể xuất và nhập ví, cho phép dễ dàng di chuyển qua lại tất cả các khóa của người dung giữa các bản thực thi ví khác nhau.

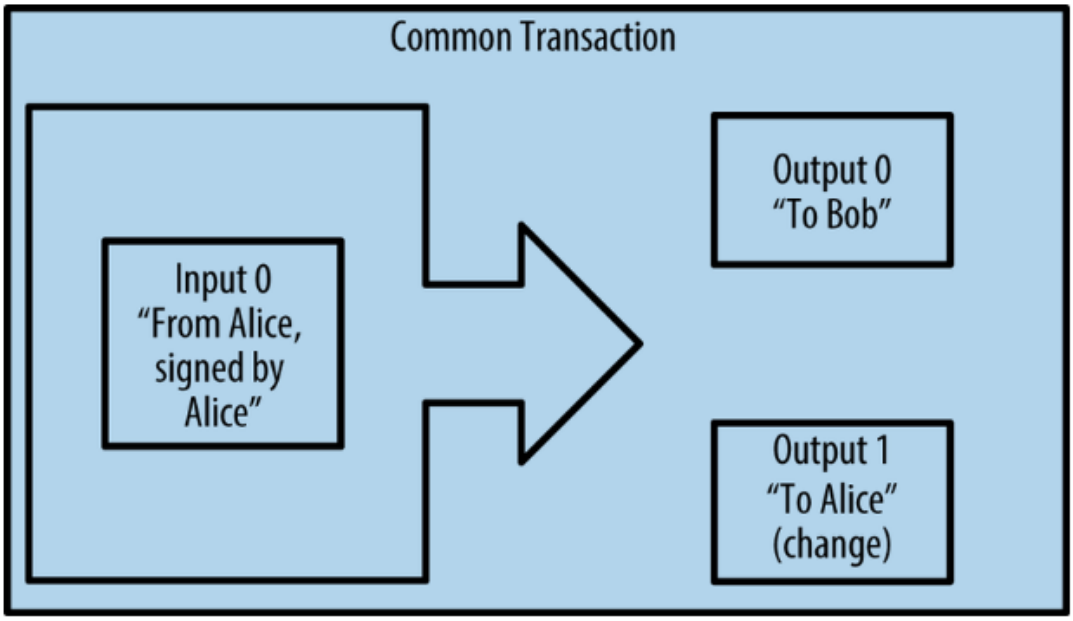


Hình 12: Ví tất định - một chuỗi khóa tất định được tạo ra từ một hạt giống

VI. Giao dịch (Transaction)

Giao dịch là sự chuyển giao giá trị giữa các ví trong hệ thống blockchain. Ví giữ một mẩu dữ liệu bí mật được gọi là khóa riêng hoặc hạt giống, được sử dụng để ký các giao dịch, cung cấp bằng chứng toán học rằng chúng đến từ chủ sở hữu của ví. Các chữ ký cũng ngăn cản việc giao dịch không bị thay thế bởi bất cứ ai một khi nó đã được phát hành. Tất cả các giao dịch được phát lên mạng và thường bắt đầu được xác nhận trong vòng 10-20 phút, thông qua một quá trình gọi là khai thác .

Thật ra, chẳng có đồng tiền điện tử nào tồn tại, chỉ có giao dịch được lưu lại mà thôi. Một sự thật thú vị là tiền điện tử không hề tồn tại, ngay cả trên ổ cứng. Thay vào đó, chỉ có thông tin giao dịch giữa các địa chỉ được lưu trữ lại, tất cả các giao dịch được lưu trữ trong sổ cái chung như đã đề cập từ trước gọi là blockchain. Thực chất lượng tiền điện tử mà một người nào đó có được tính bằng tổng tất cả giá trị của các đầu ra của các transaction trước đó mà có địa chỉ thụ hưởng trỏ đến địa chỉ của người đó. Nó tuân theo quy tắc đầu ra của transaction này sẽ là đầu vào của transaction khác. Giống như việc ta tiêu tiền giấy, số tiền ta có thực chất là tiền mà ta được người khác đưa cho và tổng đống tiền đó lại ta có số tiền ta đang có. Sẽ có nhiều dạng giao dịch có dạng 1 đầu vào 1 đầu ra, 1 đầu vào nhiều đầu ra, nhiều đầu vào và 1 đầu ra và v.v..



Hình 13: Giao dịch một đầu vào nhiều đầu ra

Ở hình trên, output 0 có thể sử dụng cho lần chi tiêu tiếp theo của Bob và tiền thừa trả về ví của Alice là output 1 kia cũng có thể sử dụng cho lần tiếp theo.

Vì vậy nên thực chất số tiền có ở trong ví chỉ là nó đi tìm những giao dịch vẫn chưa được sử dụng mà có địa chỉ thụ hưởng trỏ về địa chỉ của ví mình và tính tổng giá trị của chúng sẽ ra số tiền người giữ ví đó đang có.

Để dễ minh họa, ví dụ rằng Alice cần gửi cho Bob vài bitcoin.

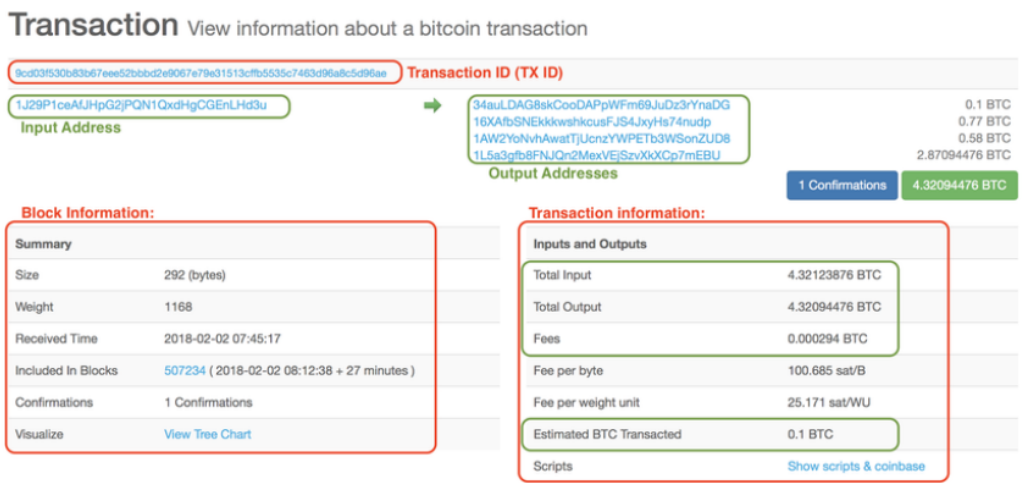
1. Thông tin của một giao dịch

Nếu Alice gửi một vài bitcoin cho Bob, giao dịch đó sẽ có ba phần thông tin:

+ Thông tin đầu vào: Những địa chỉ bitcoin được Alice sử dụng để nhận bitcoin trước đây.

+ Khoản tiền: Đây là số lượng bitcoin mà Alice gửi cho Bob.

+ Thông tin đầu ra: Địa chỉ bitcoin của Bob.



Hình 14: Thông tin đầu vào, đầu ra của một giao dịch

2. Tiền điện tử được gửi đi như thế nào

Sau khi ví lấy được các giao dịch có địa chỉ của Alice mà chưa được sử dụng và để đem vào thanh toán trong giao dịch với Bob thì giao dịch mới sẽ được tạo thành rồi đưa lên mạng bitcoin.

Như đã biết mỗi địa chỉ trong Bitcion sẽ chứa 2 khóa là khóa công khai (public key) và khóa bí mật (private key). Hai khóa này có liên quan đến nhau nhưng sẽ không có cách nào có thể từ public key có thể tìm ra private key. Điều quan trọng ở đây bây giờ là bất kỳ một transaction nào xuất phát từ địa chỉ của Alice sẽ cần ký với chữ ký được tạo ra từ private key của Alice. Vì private key là bí mật chỉ có Alice biết nên không ai có thể giảo mạo Alice để xác nhận rằng tiền đó cả. Một tính năng vô cùng tuyệt vời của bitcoin đó là nếu chữ ký được tạo bằng private key tương ứng với public key đó, chương trình sẽ xác thực giao dịch mà không cần biết khóa riêng là gì. Mạng bitcoin sau đó xác nhận xem trước đây Alice đã sử dụng bitcoin đó chưa bằng cách chạy qua lịch sử địa chỉ của Alice để kiểm tra, điều này ví sẽ tự động làm ví nó đã viết địa chỉ của Alice và public key cùng vì tất cả các giao dịch đều công khai trên sổ cái bitcoin.

3. Xác nhận giao dịch

Đầu tiên, ví sẽ tiến hành kiểm tra nhanh giao dịch trên. Nó sẽ kiểm tra xem liệu Alice có đủ bitcoin trong tài khoản của mình hay không và địa chỉ của Bob cung cấp có phải là một địa chỉ bitcoin còn sử dụng được hay không. Sau khi thông qua 2 bài kiểm tra trên, giao dịch này sẽ được đóng gói kèm với các giao dịch khác để tạo thành một khối (block). Khối này di chuyển tới các thợ đào tiền ảo. Mục tiêu của các thợ đào là xác thực khối đó và thêm nó vào blockchain (đây là quá trình cập nhật sổ cái). Khi các thợ đào nhận được một khối các giao dịch và tìm cách đưa vào blockchain, họ đang sử dụng hàm hash để giải quyết câu đố dưới dạng mật mã.

Các thợ đào tiền ảo sử dụng khối mới (bao gồm các giao dịch được đóng gói trong khối này) kết hợp với một dãy số được tạo ra ngẫu nhiên (gọi là tham số nonce), đưa nó vào hàm băm khối và sau đó nhận được một giá trị hash cụ thể. Những gì mà một thợ đào tiền ảo cố gắng thực hiện là tìm một giá trị hash bắt đầu với nhiều con số 0. Họ sẽ liên tục thử các dãy số nonce khác nhau

cho đến khi đạt được giá trị hash cần thiết. Tất cả thợ đào tiền ảo đang trong một cuộc cạnh tranh khốc liệt để tìm ra giá trị hash chính xác đó. Điều này là vì thợ đào nào tìm ra giá trị chính xác sẽ đưa giải pháp chính xác tới node nhỏ để được xác thực. Khối mới được thêm vào blockchain và thợ đào giành chiến thắng sẽ được thưởng một số bitcoin. Giao dịch bitcoin của Alice giờ đã được ghi nhận vào Blockchain. Ví tiền bitcoin của Bob cũng có thêm bitcoin và số dư của ông Alice bị trừ đi bitcoin. Sau đó, quá trình đào tiền ảo bắt đầu lại từ đầu, với một loạt các giao dịch được gói lại vào một khối mới, và tất cả thợ đào tranh nhau tìm ra giá trị hash chính xác.

Bởi vì các giao dịch cần được xác nhận bởi các thợ khai thác và công đoạn này cần một khoảng thời gian nhất định do vậy các giao dịch luôn tốn một khoảng thời gian để hoàn thành.

Các giao dịch sẽ tốn một khoản chi phí. Phí giao dịch được tính bởi nhiều yếu tố. Một số ví cho phép đặt các khoản phí này một cách thủ công. Ta có thấy tình huống tổng tất cả đầu ra của các giao dịch sẽ không bằng tổng tất cả các đầu vào, đó được ngầm hiểu chính là phí giao dịch và phí này sẽ được dành cho các thợ đào có công xác thực giao dịch.

Cuối cùng, các giao dịch bitcoin là có thể chia nhỏ. 1 satoshi là 1 phần 100 triệu bitcoin và có thể lập thành 1 giao dịch.

KẾT LUẬN

Bài báo cáo của nhóm đã trình bày và làm rõ khái niệm tiền điện tử, các đồng tiền điện tử, giao dịch và các công nghệ đứng đằng sau nó. Đây là một vấn đề không còn quá mới tuy nhiên các tài liệu bằng Tiếng Việt còn hạn chế và chưa được xác thực, vì vậy bài báo chủ yếu tham khảo và dịch lại từ các nguồn tài liệu từ nước ngoài. Do thời gian và kiến thức còn hạn chết, mong nhận được thêm nhiều ý kiến tham khảo từ thầy và các bạn

TÀI LIỆU THAM KHẢO

Mastering Bitcoin: Unlocking Digital Cryptocurrencies - Andreas M. Antonopoulos

https://topdev.vn/blog/blockchain-la-gi/

https://blockgeeks.com/guides/what-is-blockchain-technology/

https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

https://cointelegraph.com/explained/proof-of-work-explained

https://vi.wikipedia.org/wiki/Ti%E1%BB%81n_%C4%91i%E1%BB%87n_t%E1%BB%AD

https://en.wikipedia.org/wiki/Digital_currency

https://topdev.vn/blog/giao-dich-trong-bitcoin-hoat-dong-nhu-the-nao/