**Ứng dụng của blockchain trong thương mại điện tử - ví điện tử (Nhóm C.A.T)**

**Lời mở đầu**

Blockchain là xu hướng công nghệ đang được ưu chuộng nhất hiện nay. Với các ưu điểm về bảo mật và sự tiện dụng, blockchain ngày càng được chọn là công nghệ cốt lõi trong thương mại điện tử và ví điện tử. Thông qua đề tài Ứng dụng blockchain trong thương mại điện tử - ví điện tử, nhóm CAT chúng em mong muốn cung cấp thêm các kiến thức cơ bản về blockchain, về cách blockchain hoạt động. Phần demo cuối bài sẽ trình bày cách ứng dụng blockchain trong việc xây dựng một ví điện tử với các chức năng cơ bản của một ví điện tử.

**Mục lục**

[**Mục lục** 1](#_Toc70242336)

[**Phân công công việc:** 1](#_Toc70242337)

[**1. Blockchain là gì?** 2](#_Toc70242338)

[**- Định nghĩa:** 2](#_Toc70242339)

[**- Lịch sử:** 2](#_Toc70242340)

[**Công nghệ Blockchain hoạt động như thế nào?** 3](#_Toc70242341)

[**2. Ví điện tử áp dụng blockchain – Ví Blockchain?** 6](#_Toc70242342)

[**- Ví blockchain là gì?** 6](#_Toc70242343)

[**- Ví dụ: Blockchain.com – Ví blockchain phổ biến nhất hiện nay:** 7](#_Toc70242344)

[**4. Demo sản phẩm ví điện tử do nhóm thực hiện:** 8](#_Toc70242345)

**Phân công công việc:**

|  |  |  |
| --- | --- | --- |
| Tên thành viên | Nội dung công việc | Phần trăm thực hiện (%) |
| Nguyễn Tuấn Anh |  |  |
| Tăng Chí Chung |  |  |
| Nguyễn Văn Thành |  |  |
|  | Tổng: | 100 |

**1. Blockchain là gì?**

**- Định nghĩa:**

Blockchain(chuỗi khối), tên ban đầu block chain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới khối trước đó, kèm một mã thời gian và dữ liệu giao dịch. Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó.

**- Lịch sử:**

Ý tưởng đằng sau công nghệ blockchain được mô tả từ năm 1991, khi các nhà nghiên cứu Stuart Haber và W. Scott Stornetta giới thiệu một giải pháp thực tế về mặt tính toán để đánh dấu thời gian các văn bản số, để chúng không bị đề lùi ngày về trước hoặc can thiệp vào. Hệ thống đã sử dụng một chuỗi gồm các khối được bảo mật bằng mật mã để lưu trữ các văn bản được đánh dấu thời gian.

Và năm 1992, các cây Merkle đã được tích hợp vào thiết kế, khiến nó trở nên hiệu quả hơn bằng cách cho phép một khối có thể tập hợp một vài văn bản. Tuy nhiên, công nghệ này đã không được sử dụng và bằng sáng chế đã hết hạn vào năm 2004, bốn năm trước khi Bitcoin ra đời.

Năm 2004, nhà khoa học máy tính và người theo chủ nghĩa mật mã Hal Finney (Harold Thomas Finney II) đưa ra một hệ thống gọi là RPoW, Proof Of Work Tái sử dụng. Hệ thống hoạt động bằng cách nhận một Hashcash không thể thay đổi hoặc không thể thay thế dựa trên token proof of work, và đổi lại đã tạo ra một token đã được ký RSA mà sau đó có thể được trao đổi trực tiếp từ người này sang người khác.

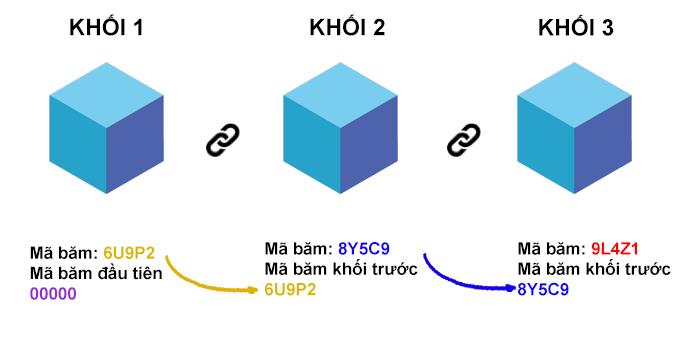
RPoW đã giải quyết vấn đề vì tiêu dùng hai lần bằng cách lưu giữ quyền sở hữu các token đã đăng ký trên một máy chủ đáng tin cậy; máy chủ này được thiết kế để cho phép người dùng trên toàn thế giới xác minh tính chính xác và liêm chính trong thời gian thực. RPoW có thể được xem là một thử nghiệm ban đầu và là những bước đầu tiên quan trọng trong lịch sử tiền điện tử.

Vào cuối năm 2008, cuốn sách trắng giới thiệu về hệ thống tiền mặt điện tử mạng ngang hàng, phi tập trung – tên là Bitcoin – đã được đăng trên danh sách nhận thư về mật mã học bởi một người hoặc tổ chức lấy biệt danh là Satoshi Nakamoto. Dựa trên thuật toán proof of work Hashcash, nhưng thay vì sử dụng một hàm tính toán dựa trên phần cứng như RPoW, tính năng chống chi tiêu hai lần trong Bitcoin được cung cấp bởi một giao thức mạng ngang hàng để theo dõi và xác thực các giao dịch. Nói ngắn gọn, các thợ đào “đào” Bitcoin để nhận phần thưởng bằng cách sử dụng cơ chế proof-of-work và sau đó xác minh bằng các node phi tập trung trong mạng. Vào ngày 3 tháng 1 năm 2009, Bitcoin ra đời khi Satoshi Nakamoto đào được khối bitcoin đầu tiên, đem lại phần thưởng 50 bitcoin. Người nhận Bitcoin đầu tiên là Hal Finney, ông ta nhận được 10 bitcoin từ Satoshi Nakamoto trong giao dịch bitcoin đầu tiên của thế giới vào ngày 12 tháng 1 năm 2009.

**- Đặc điểm:**

* Không thể làm giả, không thể phá hủy các chuỗi Blockchain: theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu.
* Bất biến: dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.
* Bảo mật: Các thông tin, dữ liệu trong Blockchain được phân tán và an toàn tuyệt đối.
* Minh bạch: Ai cũng có thể theo dõi dữ liệu Blockchain đi từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.
* Hợp đồng thông minh: là hợp đồng kỹ thuật số được nhúng vào đoạn code if-this-then-that (IFTTT), cho phép chúng tự thực thi mà không cần bên thứ ba.

**Công nghệ Blockchain hoạt động như thế nào?**



1. Nguyên lý mã hóa:

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 bạn 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.​ Hệ thống blockchain được thiết kế theo cách không yêu cầu sự tin cậy và bảo đảm bởi độ tin cậy có được thông qua các hàm mã hóa toán học đặc biệt. ​Để có thể thực hiện các giao dịch trên blockchain, bạn cần một phần mềm sẽ cho phép bạn lưu trữ và trao đổi các đồng Bitcoin của bạn 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).

2. 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.

Mỗi nút có thể nhóm các giao dịch với nhau thành một khối và gửi nó vào mạng lưới như một hàm ý cho các khối tiếp theo được gắn vào sau đó.

3. Thêm khối vào chuỗi:

Cơ chế đồng thuận phân tán đồng đẳng (hay còn gọi là cơ chế đồng thuận phân quyền) (Distributed)

Mỗi Blockchain sẽ thêm các block vào chain theo những cách khác nhau, tất cả đều sử dụng cơ chế đồng thuận phân tán đồng đẳng.

Có nhiều cơ chế đồng thuận phân tán đồng đẳng như: Proof of Work, Proof of Stake, Delegated Proof-of-Stake, Proof of Authority, Proof-of-Weight, Byzantine Fault Tolerance..

Nổi bật nhất hiện nay là cơ chế đồng thuận được sử dụng bởi Bitcoin – Proof of work (Bằng chứng công việc).

– 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.

Quy tắc đầu tiên của PoW là trung bình phải mất 10 phút để 1 block mới được thêm vào chain.

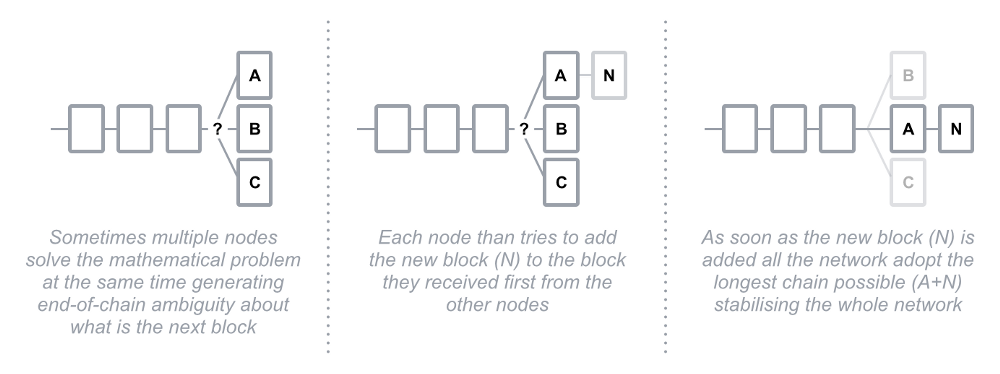
Quá trình này được gọi là “mining”, mỗi node cố gắng thêm 1 khối vào chuỗi bằng cách sử dụng sức mạnh tính toán của máy tính để giải các bài toán. Quy tắc bắt buộc 1 khối chỉ được thêm vào chuỗi chỉ khi tìm được lời giải cho các bài toán trên.

Thợ đào (miner) sẽ được thưởng 1 lượng tiền thưởng cộng với chi phí của tất cả giao dịch có trong khối khi thêm thành công một khối vào chuỗi.

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.

Cách duy nhất để giải quyết vấn đề toán học như vậy là đoán các số ngẫu nhiên, những số khi mà kết hợp với nội dung khối trước tạo ra một kết quả đã được hệ thống định nghĩa. Điều này nhiều khi có thể mất khoảng một năm cho một máy tính điển hình với một cấu hình cơ bản có thể đoán đúng các con số đáp án của vấn đề toán học này.

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.



- Những ưu điểm của Blockchain:

1. ***Tính minh bạch và không thể phá vỡ*:** có thể nói đây là một trong những đặc điểm nổi bật nhất. Tất cả mỗi thông tin được lưu trữ, truyền tải và xử lý trong hệ thống blockchain, đều được thể hiện một cách minh bạch, rõ ràng nhất và không thể thay đổi, không thể giả mạo, không thể phá vỡ. Do đó, nếu bạn muốn truy xuất những thông tin về giao dịch của mình hay của người khác ( bao gồm ngày, giờ, chi tiết về giao dịch….) thì bạn sẽ không bao giờ phải lo ngại về sự thiếu chính xác của dữ liệu.
2. ***Đặc tính ẩn danh***: trọng tâm trong việc bảo vệ sự riêng tư của blockchain chính là khả năng ẩn danh người dùng. Đặc tính này, sẽ giúp bạn có thể giao dịch một cách an toàn, bảo mật mà không cần phải lo ngại về người khác biết được danh tính của mình. Cùng với sự minh bạch, không thể phá vỡ hay thay đổi dữ liệu và đặc tính ẩn danh, giúp blockchain tạo ra một niềm tin rất lớn đối với người dùng, giúp bạn cảm thấy an tâm hơn khi tham gia vào Blockchain.
3. ***Rút ngắn được thời gian và tiết kiệm chi phí***: nếu giao dịch truyền thống, theo kiểu cần có bên thứ 3 để xác thực, tạo sự tin cậy và minh bạch, thì bạn sẽ phải chịu thêm một phần chi phí nhất định cho bên thứ 3 này. Tuy nhiên, khi bạn ứng dụng blockchain vào giao dịch của mình, với hợp đồng thông minh (smart contract) bạn và đối tác của bạn sẽ là người trực tiếp thực hiện giao dịch và hệ thống trên blockchain sẽ là người xác nhận cho bạn, mà không cần tốn thêm chi phí, thậm chí là còn tiết kiệm được cả về thời gian giao dịch.
4. ***Tính ứng dụng rộng rãi***: công nghệ blockchain có thể ứng dụng rộng rãi trong mọi mặt đời sống hiện nay. Ví dụ như ứng dụng blockchain trong nông nghiệp thực phẩm, trong quản lý giáo dục, bầu cử kỹ thuật số…. và nổi bậc nhất vẫn là công nghệ blockchain được ứng dụng trong giao dịch tài chính.

**- Ứng dụng:**

Blockchain được ứng dụng vào rất nhiều lĩnh vực như: Tiền điện tử, chuỗi cung ứng, hợp đồng thông minh, các dịch vụ tài chính, video games, chăm sóc sức khỏe, tên domain... và gần đây là được ứng dụng vào thương mại điện tử.

**2. Ví điện tử áp dụng blockchain – Ví Blockchain?**

**- Ví blockchain là gì?**

Ví blockchain là một ví tiền điện tử cho phép người dùng quản lý các loại tiền điện tử khác nhau — ví dụ: Bitcoin hoặc Ethereum. Ví blockchain giúp ai đó trao đổi tiền một cách dễ dàng. Các giao dịch được bảo mật vì chúng được ký bằng mật mã. Ví có thể truy cập từ các thiết bị web, bao gồm cả thiết bị di động và quyền riêng tư và danh tính của người dùng được duy trì. Vì vậy, ví blockchain cung cấp tất cả các tính năng cần thiết cho việc chuyển và trao đổi tiền giữa các bên khác nhau một cách an toàn và bảo mật.

**- Ví blockchain hoạt động như thế nào?**

Public key (khóa công khai) và private keys (khóa bí mật)

Đối với đồng tiền kĩ thuật số, public key (khóa công khai) sẽ hoạt động như địa chỉ. Bạn có thể chia sẻ khóa công khai này với những người khác để nhận thanh toán. Private keys (khóa bí mật) được sử dụng để ký các giao dịch, để không ai có thể chi tiêu đồng tiền ngoài chủ sở hữu của chúng. Người dùng sẽ phải giữ bí mật Private keys (khóa bí mật) của họ! Chúng ta cũng gửi khóa công khai cùng với giao dịch và nó có thể sử dụng để xác minh rằng chữ ký hợp lệ và dữ liệu không bị giả mạo.

Các đặc điểm của ví blockchain:

**Dễ sử dụng**: ví blockchain cũng giống như các loại ví điện tử khác, người dùng có thể thực hiện các giao dịch chuyển - nhận tiền điện tử cũng như các dịch vụ thanh toán khác.

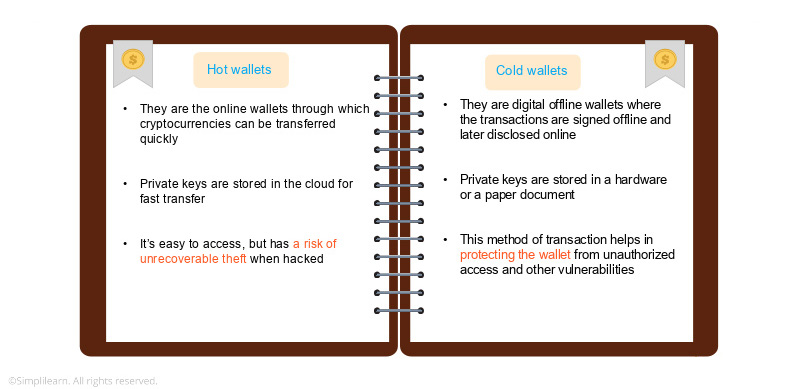
**Bảo mật cao**: mức độ bảo mật của ví blockchain tùy thuộc vào thuật toán bảo mật được áp dụng trong ví cũng như private key của bạn.

**Cho phép giao dịch tức thì** trên các khu vực địa lý. Không rào cản, không qua trung gian.

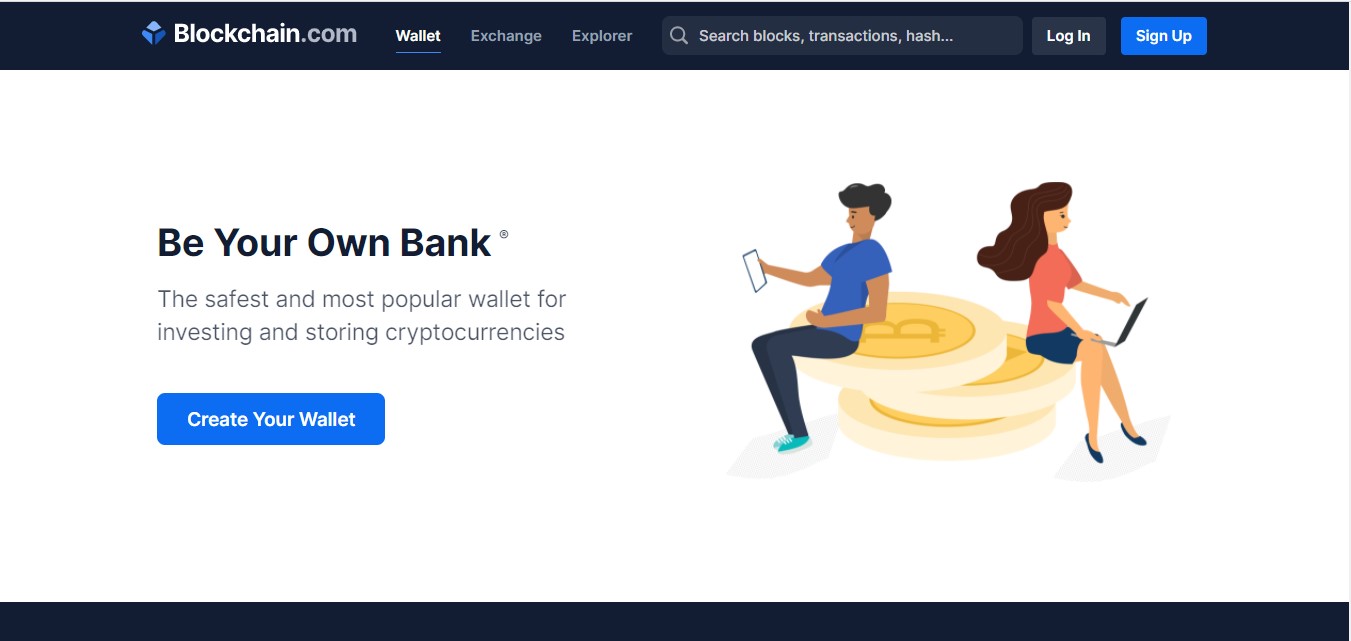
**Phí giao dịch thấp** do không qua trung gian.

**Cho phép giao dịch giữa các loại tiền điện tử khác nhau**, chuyển đổi đơn giản, thuận tiện.

**- Các loại ví blockchain:**

****

**- Ví dụ: Blockchain.com – Ví blockchain phổ biến nhất hiện nay:**



**4. Demo sản phẩm ví điện tử do nhóm thực hiện:**

**Các chức năng của ví blockchain:**

* Tạo tài khoản người dùng
* Tạo ví blockchain
* Kiểm tra thông tin ví và thông tin người dùng
* Nạp tiền vào ví, kiểm tra số dư tài khoản
* Tạo giao dịch mới, chuyển tiền giữa các tài khoản

**Tạo đối tượng block, thứ tạo ra blockchain**

- Block chứa mã hash của nó, mã hash của khối trước nó, nonce, timetamp và thông tin giao dịch.

Hash = Digital signature (Chữ ký số)

Cách để tạo ra Chữ ký số: Có rất nhiều thuật toán để tạo ra chữ ký số, trong số đó là mã hóa SHA256 và mã hóa ECDSA.

**Tiếp theo chúng ta sẽ cần một cách để sinh ra chữ ký số (Digital signature)**

Có rất nhiều thuật toán mã hóa bạn có thể lựa chọn, tuy nhiên SHA256 phù hợp tốt cho ví dụ này. Chúng ta có thể import java.security.MessageDigest; để có được quyền truy cập vào thuật toán SHA256.

**ECDSA** là gì?

ECDSA là viết tắt của Elliptic Curve Digital Signature Algorithm, tạm gọi là thuật toán chữ kí số đường cong Elliptic. Đây là 1 thuật toán nổi tiếng trong mật mã học, thường được sử dụng trong các nền tảng blockchain, ví dụ như Bitcoin, Ethereum ...  
Thuật toán này được sử dụng để tạo chữ kí số (digital signature) cho dữ liệu (ví dụ 1 tệp tin) giúp ta có thể xác minh tính xác thực của dữ liệu mà không ảnh hưởng đến độ bảo mật của nó. Có thể so sánh chữ kí số với chữ kí ngoài đời thực về tác dụng của nó, có 1 chút khác biệt là ngoài đời ta có thể giả mạo chữ kí của người khác mà không bị phát hiện nhưng ECDSA signature thì ta không thể giả mạo.

Nguyên lí cơ bản

Nguyên lí của thuật toán rất đơn giản, ta có 1 phương trình toán học được thể hiện bằng 1 đường cong Elliptic trên đồ thị.

Giải mã thuật toán

ECDSA chỉ sử dụng toán học **số nguyên**, phạm vi của các số bị ràng buộc bởi số lượng bit được sử dụng trong chữ kí, thông thường ECDSA sẽ sử dụng tổng cộng 160 bit do đó sẽ có 1 phạm vi tương đối rộng đủ được coi là an toàn (phải tốn 1 lượng tính toán không tưởng để tấn công vét cạn và không khả thi với năng lực phần cứng hiện tại).  
ECDSA sử dụng hàm băm mật mã SHA1 để băm thông điệp và kí vào thông điệp đã được băm. Hàm băm đơn giản là 1 phương trình toán học mà với mỗi thay đổi dù là nhỏ nhất ở đầu vào, nó sẽ cho ra đầu ra hoàn toàn khác, SHA1 luôn cho ra đầu ra với kích thước cố định là 160 bit (tương đương 20 byte), điều này đặc biệt hữu ích với ECDSA để tăng tính bảo mật của giải thuật.

Mã hoá SHA là gì?

SHA (Secure Hash Algorithm) bao gồm 5 thuật toán được chấp nhận bởi FIPS – Tiêu chuẩn Xử lý Thông tin Liên bang, dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao. 5 thuật toán đó bao gồm:

SHA-1 (trả lại kết quả dài 160 bit)

SHA-224 (trả lại kết quả dài 224 bit)

SHA-256 (trả lại kết quả dài 256 bit)

SHA-384 (trả lại kết quả dài 384 bit)

SHA-512 (trả lại kết quả dài 512 bit)

**SHA-256 là gì?**

SHA-256 là Thuật toán băm bảo mật 256 bit và dùng để tạo ra các hàm băm không thể đảo ngược và duy nhất. Số lượng hàm băm có thể có càng lớn, thì xác suất để hai giá trị sẽ tạo ra cùng một giá trị băm càng nhỏ.

Ví dụ:

|  |  |
| --- | --- |
| DỮ LIỆU | CHUỖI MÃ HÓA |
| Bitcoin Vietnam News | f3ad777234a24bfacbd8123d6ea0a1961e8539b74b5fa8f2f371ea2cf7b21215 |
| cryptoviet.com | cbab80bf094869581bb45557b64a8db0b8bab8c8817b5facd0c975d9a5a47805 |

SHA-256 là một nhánh của hàm băm mật mã SHA-2 được sử dụng trong nhiều phần khác nhau của mạng Bitcoin:

Khai thác sử dụng SHA-256 là thuật toán Proof of Work.

SHA-256 được sử dụng trong việc tạo ra các địa chỉ bitcoin để cải thiện an ninh và bảo mật.

Thuật toán SHA-256 tạo ra một mã băm có cố định 256-bit (32-byte) gần như duy nhất. Một chuỗi băm được tạo ra không thể được tính toán trở lại. Điều này làm cho nó phù hợp để xác nhận mật khẩu, thách thức xác thực hàm băm, chống giả mạo, chữ ký số.

SHA-256 là một trong những hàm băm kế tiếp đối sau SHA-1 và là một trong những hàm băm mạnh nhất hiện tại.

**Chuẩn bị ví:**

- Tạo public key(khóa công khai) và private keys(khóa bí mật);

- Viết các hàm xem số dư và kiểm tra quỹ (sendFunds);

- Viết các hàm xem khóa công khai và khóa riêng tư;

**Các giao dịch và chữ ký số:**

Mỗi giao dịch sẽ mang một lượng dữ liệu nhất định:

* Khóa công khai (địa chỉ) của người gửi tiền.
* Khóa công khai (địa chỉ) của người nhận tiền.
* Giá trị / số tiền cần chuyển.
* Đầu vào, là các tham chiếu đến các giao dịch trước đó chứng minh người gửi có tiền để gửi.
* Kết quả, cho thấy số lượng địa chỉ liên quan nhận được trong giao dịch. (Những đầu ra này được tham chiếu như đầu vào trong các giao dịch mới)
* Một chữ ký mã hoá, chứng minh chủ sở hữu địa chỉ là người gửi giao dịch này và dữ liệu không bị thay đổi. (ví dụ: ngăn cản một bên thứ ba thay đổi số tiền đã gửi)

Giờ hãy cùng tạo 2 class rỗng TransactionInput ,TransactionOutput và Transaction class.

Mục đích của chữ ký là gì và nó làm việc như thế nào?

Chữ ký thực hiện hai nhiệm vụ rất quan trọng trên blockchain: Thứ nhất, nó chỉ cho phép chủ sở hữu chi tiêu tiền của họ, thứ hai, nó ngăn chặn người khác can thiệp vào giao dịch trước khi một block mới được khai thác.

Ví dụ: Bob muốn gửi 2coin đến Sally, do đó ví của họ tạo ra giao dịch và gửi cho người khai thác mỏ để thêm dữ liệu vào trong block tiếp theo. Một thợ mỏ cố gắng để thay đổi người nhận của 2 đồng tiền là John. Tuy nhiên, may mắn thay, Bob đã ký kết dữ liệu giao dịch với khóa riêng của mình, cho phép bất cứ ai kiểm tra xem dữ liệu giao dịch đã được thay đổi bằng khóa công khai của Bob hay không.

**Kiểm tra tính toàn vẹn của blockchain:**

Hàm isChainValid() Boolean method, sẽ lặp qua tất cả các block trong chuỗi và so sánh tất cả các hash. Phương thức này sẽ cần thiết để kiểm tra tính toàn vẹn của blockchain.

**Cách tiền điện tử được sở hữu:**

Để bạn sở hữu 1 bitcoin, bạn phải nhận được 1 Bitcoin. Sổ cái không thực sự thêm một bitcoin cho bạn và trừ đi một bitcoin từ người gửi, người gửi phải tham chiếu rằng trước đây họ đã nhận được một bitcoin, sau đó một giao dịch được tạo ra cho thấy 1 Bitcoin được gửi đến địa chỉ của bạn. (Đầu vào của giao dịch tham chiếu đến kết quả các giao dịch trước đó).