**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](#_Toc69657705)

[**Phân công công việc:** 1](#_Toc69657706)

[**1. Blockchain là gì?** 2](#_Toc69657707)

[**- Định nghĩa:** 2](#_Toc69657708)

[**- Tổng quan:** 2](#_Toc69657709)

[**- Đặc điểm:** 2](#_Toc69657710)

[**- Ứng dụng:** 4](#_Toc69657711)

[**2. Ví điện tử là gì?** 4](#_Toc69657712)

[**- Tổng quan:** 4](#_Toc69657713)

[**- Bảo mật:** 4](#_Toc69657714)

[**3. Ứng dụng của blockchain trong thương mại điện tử - ví điện tử?** 5](#_Toc69657715)

[**- Ưu điểm:** 5](#_Toc69657716)

[**- Ví dụ ứng dụng Blockchain trong ví điện tử:** 5](#_Toc69657717)

[**4. Demo sản phẩm ví điện tử do nhóm thực hiện:** 5](#_Toc69657718)

**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.

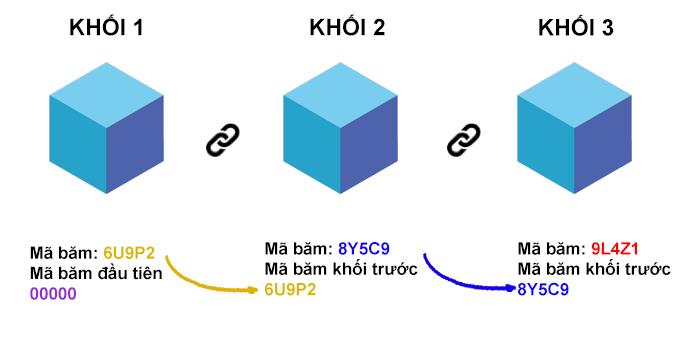
**- Tổng quan:**

Blockchain lần đầu tiên được phát minh và thiết kế bới Satoshi Nakamoto vào năm 2008 và được hiện thực hóa vào năm sau đó như là một phần cốt lõi của Bitcoin, khi công nghệ blockchain đóng vai trò như là một cuốn sổ cái cho tất cả các giao dịch. Qua việc sử dụng mạng lưới ngang hàng và một hệ thống dữ liệu phân cấp, Bitcoin blockchain được quản lý tự động. Việc phát minh ra blockchain cho Bitcoin đã làm cho nó trở thành loại tiền tệ kỹ thuật số đầu tiên giải quyết được vấn đề double spending (chi tiêu gian lận khi 1 lượng tiền được dùng 2 lần). Công nghệ này của Bitcoin đã trở thành nguồn cảm hứng cho một loạt các ứng dụng khác.

**- 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?**



**Blockchain** bao gồm ba khái niệm quan trọng: **khối, nút và công cụ khai thác**.

**● Khối (Block)**

Mỗi chuỗi bao gồm nhiều khối và mỗi khối có ba yếu tố cơ bản:

**-Các dữ liệu trong khối**

Một trường (dài 32 bit) được gọi là số nonce. Số nonce được tạo ngẫu nhiên khi một khối được hình thành, sau đó tạo ra một **giá trị băm** (**hash**) của **tiêu đề khối** (**block header**).  Giá trị băm là một số 256 bit được kết hợp với số nonce. Nó phải bắt đầu với một số lượng lớn các số không (nghĩa là cực kỳ nhỏ). Mỗi khối cũng bao gồm giá trị băm từ khối trước. Điều này trở thành một phần của tập dữ liệu được sử dụng để tạo giá trị băm  của khối mới hơn, đó là cách chuỗi được liên kết với nhau.

Khi khối đầu tiên của chuỗi được tạo, một số nonce sẽ tạo ra giá trị băm mật mã. Dữ liệu trong khối được coi là đã ký và mãi mãi gắn với nonce và giá trị băm – hash, trừ khi nó được khai thác.

● **Thợ mỏ (Miner)**

Thợ mỏ tạo ra các khối mới trên chuỗi thông qua một quá trình gọi là khai thác.

Trong một blockchain, mọi khối đều có số nonce và giá trị băm duy nhất, nhưng cũng tham chiếu giá trị băm của khối trước đó trong chuỗi, vì vậy việc khai thác một khối không dễ dàng, đặc biệt là trên các chuỗi lớn.

Những người khai thác sử dụng phần mềm đặc biệt để giải quyết các bài toán cực kỳ phức tạp nhằm tìm kiếm một nonce có thể tạo ra giá trị băm có thể chấp nhận được.  Bởi vì số nonce chỉ có 32 bit và giá trị băm là 256, nên có khoảng bốn tỷ kết hợp nonce-hash có thể được khai thác trước khi tìm thấy cái thích hợp. Khi làm được điều đó, các thợ mỏ được cho là đã tìm thấy "số nonce vàng" và khối của họ được thêm vào chuỗi. Khi thực hiện thay đổi đối với bất kỳ khối nào trước đó trong chuỗi yêu cầu khai thác lại thì không chỉ khối đó thay đổi, mà tất cả các khối tiếp theo cũng thay đổi theo.  Đây là lý do tại sao cực kỳ khó thao túng công nghệ blockchain. Hãy nghĩ về nó như "sự an toàn trong thuật toán" vì việc tìm ra các “số nonce vàng” đòi hỏi một lượng thời gian và sức mạnh tính toán khổng lồ. Khi một khối được khai thác thành công, sự thay đổi được chấp nhận bởi tất cả các nút trong mạng lưới và người thợ đào nhận được phần thưởng về mặt tài chính.

**● Nút (Node)**

Một trong những khái niệm quan trọng nhất trong công nghệ blockchain là phi tập trung. Không một máy tính hay tổ chức nào có thể sở hữu chuỗi. Thay vào đó, nó là một sổ cái phân tán thông qua các nút được kết nối với chuỗi. Các nút có thể là bất kỳ loại thiết bị điện tử nào giúp duy trì các bản sao của blockchain và giữ cho mạng lưới hoạt động.

Mỗi nút có bản sao blockchain của riêng nó và mạng lưới phải phê duyệt một cách có tính toán các khối mới được khai thác, để chuỗi được cập nhật, tin tưởng và xác minh.

Vì blockchains có tính minh bạch, nên mọi hành động trong sổ cái có thể dễ dàng kiểm tra và xem qua. Mỗi người tham gia được cấp một số nhận dạng kiểu vừa chữ vừa số duy nhất, hiển thị các giao dịch của họ.

Việc kết hợp thông tin công khai với hệ thống kiểm tra và cân bằng giúp blockchain duy trì tính toàn vẹn và tạo niềm tin giữa những người dùng. Về cơ bản, blockchains có thể được xem là khả năng mở rộng niềm tin thông qua công nghệ.

**Cách thêm các khối mới**

Vì các tệp blockchain được phân phối trên một mạng máy tính (nút), việc cập nhật tệp không đơn giản - các khối mới phải được đa số các máy trong mạng chấp thuận.

Các máy tính cạnh tranh với nhau để tạo ra các khối mới trong một quy trình được gọi là “khai thác”. Điều này liên quan đến việc đối chiếu dữ liệu mới vào một khối, song song với giá trị băm của khối trước đó và cố gắng tạo ra một giá trị băm mới. Cuộc cạnh tranh có thể được diễn ra theo hai cách:

Bằng chứng công việc (POW): theo hệ thống này, tất cả các máy tính trong mạng lưới cạnh tranh nhau để tạo ra giá trị băm. Khó khăn trong việc tạo giá trị băm được điều chỉnh khi hệ thống mở rộng, do đó các khối mới được tạo và phê duyệt với tốc độ không đổi khi sức mạnh tính toán trong hệ thống thay đổi. Chẳng hạn, khó khăn trong việc tạo ra giá trị băm Bitcoin, họ phải bắt đầu điều chỉnh bằng cách thay đổi số lượng số 0, đảm bảo rằng một hàm băm mới chỉ được tìm thấy một lần trong mười phút hoặc lâu hơn bởi toàn bộ hệ thống.

Bằng chứng cổ phần (POS):theo hệ thống này, các nút được chọn một cách ngẩu nhiên, có xem xét đến “khoản tiền đặt cọc – Stake” trong hệ thống tài khoản. Đây thường là số tiền điện tử mà nó sở hữu, số tiền cọc này được giữ trong hệ thống để chứng minh rằng nút có lợi ích về độ tin cậy của blockchain. Hệ thống này được tạo ra để đối phó với một số vấn đề vốn có của phương pháp bằng chứng làm việc, đặc biệt là việc sử dụng năng lượng cao.

**- 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 là gì?**

**- Tổng quan:**

Ví kỹ thuật số còn được gọi là "Ví điện tử" là một thiết bị điện tử, dịch vụ trực tuyến hoặc chương trình phần mềm cho phép một bên thực hiện các giao dịch điện tử với một bên khác để trao đổi đơn vị tiền tệ kỹ thuật số cho hàng hóa và dịch vụ.

Một ví điện tử bao gồm phần mềm và thiết bị thông tin. Phần mềm cung cấp chế độ bảo mật và mã hóa cho thông tin cá nhân và giao dịch thực tế. Thông thường, khách hàng tự giữ và bảo quản ví điện tử và hoàn toàn tương thích với các trang web thương mại điện tử. Ví điện tử server, cũng được gọi là ví mỏng, là loại ví mà một tổ chức tạo ra cho khách hàng được lưu trữ trên server của họ. Ví điện tử server đang được các nhà bán lẻ ưa chuộng vì tính bảo mật, hiệu quả, có thể thêm tiện ích cho người dùng, làm tăng sự thích thú khi mua bán. Thiết bị thông tin thực chất là cơ sở dữ liệu thông tin do người dùng tự thêm vào. Các thông tin này bao gồm: địa chỉ chuyển hàng, địa chỉ hóa đơn, cách thức thanh toán (bao gồm số thẻ tín dụng, ngày hết hạn, và số bảo mật), và các thông tin khác.

**- Bảo mật:**

Người tiêu dùng không bắt buộc phải điền vào biểu mẫu đặt hàng trên mỗi trang web khi họ mua một mặt hàng vì thông tin đã được lưu trữ và được tự động cập nhật và nhập vào các trường đặt hàng trên các trang web của người bán khi sử dụng ví điện tử. Người tiêu dùng cũng được hưởng lợi khi sử dụng ví kỹ thuật số vì thông tin của họ được mã hóa hoặc bảo vệ bằng mã phần mềm riêng; người bán được hưởng lợi khi nhận được sự kết hợp của biện pháp bảo vệ chống gian lận, nhận thanh toán nhanh hơn, giảm chi phí giao dịch và giảm mất mát do trộm cắp.

Với các yêu cầu về bảo mật thông tin người dùng và thông tin giao dịch, ta có thể thấy Blockchain là một công nghệ hoàn hảo để tích hợp vào ví điện tử để tăng cường độ bảo mật cũng như tăng tốc độ, hiệu suất của các giao dịch điện tử.

**3. Ứng dụng của blockchain trong thương mại điện tử - ví điện tử?**

**Ví điện tử** thường được tích hợp trong các ứng dụng điện thoại hoặc sử dụng qua website có công dụng như một chiếc ví giúp bạn đựng tiền từ các tài khoản ngân hàng, có chức năng thanh toán và giao dịch trực tuyến với các trang web điện tử hoặc các loại phí trên internet mà có liên kết và cho phép thanh toán bằng ví điện tử.

Các nhà cung cấp dịch vụ này sẽ hợp tác với ngân hàng để quản lý tiền của bạn và thông qua kết nối này, nhà quản lý sẽ giảm sự quản lý các giao dịch thanh toán từ thẻ khách hàng bởi các giao dịch này sẽ do nhà cung cấp ví điện tử quản lý.  Thanh toán bằng ví điện tử sẽ làm giảm bớt lượng tiền mặt trong lưu thông, góp phần ổn định lạm phát...

Ngoài ra một số khách hàng thường nhầm lẫn giữa ví điện tử và ngân hàng sốbởi một số điểm như giúp thanh toán hoàn toàn trực tuyến thông qua website hoặc ứng dụng điện thoại....  Tuy nhiên ngân hàng số khác ví điện tử ở chỗ là có thể thực hiện tất cả các tính năng như một ngân hàng đích thực chứ không chỉ riêng thanh toán và giao dịch như vay nợ ngân hàng, gửi tiền tiết kiệm, tham gia các dịch vụ tài chính khác như: bảo hiểm, đầu tư, mở thẻ tín dụng,….

**- Ưu điểm:**

Việc ứng dụng blockchain trong thương mại điện tử giúp khắc phục những bất cập tồn đọng bởi những thế mạnh mang lại như:

**Bảo mật tối ưu:** Không ai có thể hack, lấy cắp thông tin trên Blockchain bởi thông tin lưu trữ trên Blockchain được bảo mật an toàn.

**Hạn chế chi phí:** Nhờ tính minh bạch, rõ ràng, Blockchain tạo được niềm tin nhất định từ thị trường giúp các nhà đầu tư tiết kiệm chi phí cho các hạng mục quảng cáo.

**Tốc độ giao dịch nhanh:** Thông qua hợp đồng thông minh (Smart Contract), mọi giao dịch tại hệ thống thương mại điện tử được thực hiện nhanh chóng và rút ngắn được thời gian giao dịch cho người tiêu dùng.

**Dịch vụ thường được thục hiện khi sử dụng ví điện tử blockchain:**

- Thanh toán trực tuyến: Giúp thanh toán trong các giao dịch mua sắm trực tuyến, các dịch vụ ăn uống giải trí, hoặc thanh toán hóa đơn tiền điện nước, điện thoại, vé máy bay, cước internet, ...

- Nhận và chuyển tiền: ví điện tử có khả năng giữ tiền cũng như tham gia các giao dịch chuyển khoản giữa các tài khoản ngân hàng như một tài khoản ngân hàng bình thường một cách nhanh chóng.

- Nạp và rút tiền từ tài khoản điện tử để duy trì và sử dụng mà không cần e ngại vấn đề an toàn và bảo mật của ví**.**

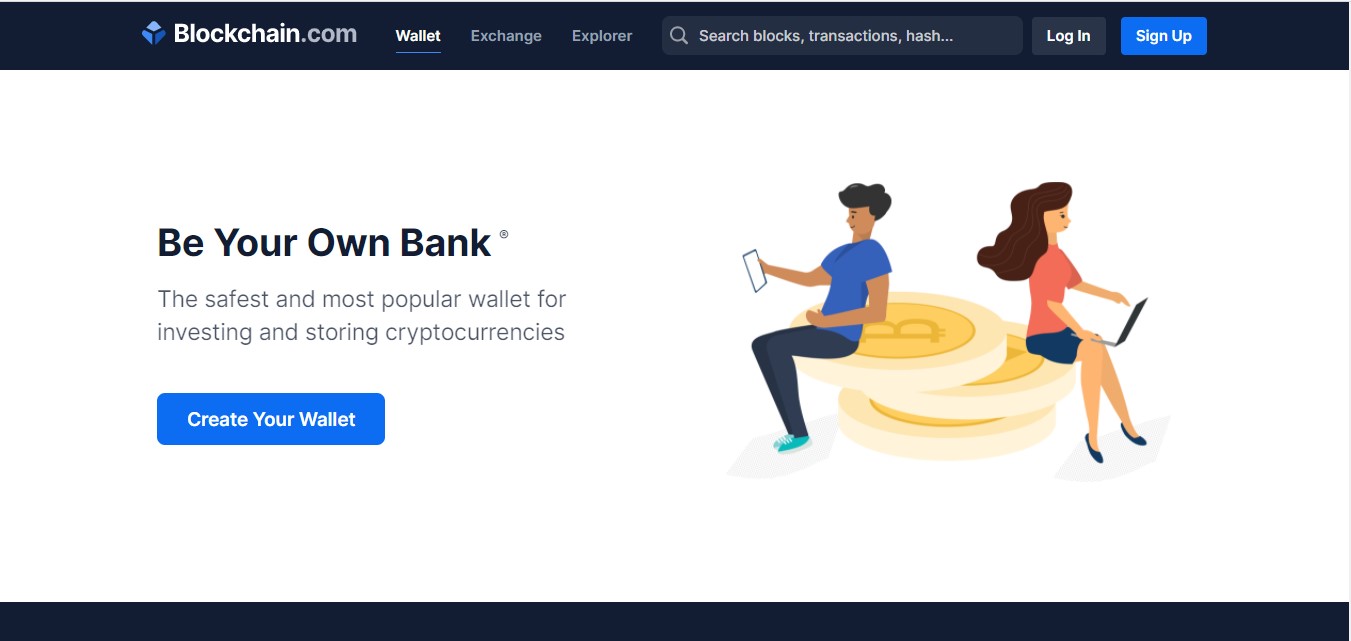
**- Ví dụ ứng dụng Blockchain trong ví điện tử:** Blockchain.com – nền tảng ví điện tử giao dịch tiền điện tử nổi tiếng nhất hiện nay.

## **Nhược điểm của ví điện tử**

* Khả năng bảo mật của ví điện tử mặc dù đã được nâng cấp nhưng vẫn khiến cho người sử dụng chưa thật sự tin tưởng.
* Phí dịch vụ còn cao so với các hình thức thanh toán khác

## **Tính năng của ví điện tử**

* Thanh toán hóa đơn, hàng hóa, dịch vụ một cách nhanh chóng, thuận tiện: bạn có thể sử dụng ví điện tử để thanh toán mua hàng trực tuyến, thanh toán trực tiếp.
* Đặt vé máy bay, vé tàu, khách sạn
* Thanh toán hóa đơn điện, nước, thanh toán cước điện thoại.
* Nhận và chuyển tiền trực tuyến



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

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

### **Tiếp theo cúng 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](https://en.wikipedia.org/wiki/SHA-1) 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**

### public key(khóa công khai) và private keys(khóa bí mật)

Đối với đồng tiền kĩ thuật số của chúng ta, 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 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 2 coin 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.

## 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).