***Giới thiệu về Blockchain***

Slide 1:

Về bản chất thì blockchain là công nghệ lưu trữ dữ liệu tuy nhiên không giống như các công nghệ lưu trữ khác blockchain mang trong mình những đặc điểm vô cùng kỳ diệu mà không có công nghệ nào có thể làm được.

Blockchain giúp mọi người dù không hề quen biết nhưng vẫn có thể thực hiện những giao dịch quan trọng. Công nghệ này đảm bảo những giao dịch này sẽ được thực hiện đúng như quy ước mà không cần phải có bên thứ 3 làm trung gian.

Blockchain là sự kết hợp hoàn hảo của sự minh bạch và tính bảo mật, nó cho phép tất cả mọi người đều có quyền biết các thông tin giao dịch của nhau, tuy nhiên dữ liệu riêng tư của mỗi cá nhân thì vẫn đảm bảo bí mật tuyệt đối.

Một khi các thông tin đã được lưu trữ trong blockchain thì chúng ta hoàn toàn yên tâm là không có bất kỳ ai hay tổ chức nào có thể sửa đổi được nó nữa, cũng không cách nào phá hủy được nó, nó sẽ tồn tại mãi mãi theo đúng nghĩa đen đây được coi là yếu tố vô cùng quan trọng để cả thế giới đặt niềm tin vào Blockchain.

Hiện nay có nhiều người lầm tưởng Blockchain và Bitcoin là một nhưng thực chất Bitcoin cũng như hàng trăm như cái đồng đồng tiền điện tử khác đều được xây dựng dựa trên nền tảng công nghệ Blockchain có thể nói Blockchain như một cái nền móng hạ tầng kiên cố và Bitcoin là một tòa nhà chọc trời được xây trên nền móng đó.

Slide 2:

Đơn vị lưu trữ cơ bản của Blockchain là một khối dữ liệu hay còn gọi là Block. Dữ liệu của chúng ta sẽ được đóng gói trong một khối sau đó khối này sẽ được khóa lại bằng thuật toán mã hóa. Một khi đã khóa xong thì dữ liệu này sẽ không bao giờ thay đổi được nữa. Nó sẽ trở thành một bằng chứng bất di bất dịch và tồn tại mãi mãi

Slide 3:

Các khối sau khi được tạo ra sẽ được liên kết lại với nhau thành một chuỗi như sợi dây xích. Đó chính là tên gọi của công nghệ blockchain.

Slide 4:

Khối đầu tiên của chuỗi này gọi là Genesis Block(khối khởi nguồn)

Slide 5:

Sự phát triển Blockchain trải qua 3 phiên bản, ở mỗi phiên bản Blockchain cho phép xây dựng lên những ứng dụng cụ thể.

Phiên bản đầu tiên chính là các loại tiền điện tử trong đó đồng Bitcoin đang hot tại thị trường tài chính thế giới bây giờ cũng chỉ là một lĩnh vực được xây dựng trên nền tảng công nghệ blockchain và hiện nay thì đang có khoảng 700 loại tiền điện tử tương tự như Bitcoin đang hoạt động

Ở phiên bản 2.0 Blockchain sẽ cho phép xây dựng lên những ứng dụng liên quan đến tài chính và hợp đồng thông minh giúp tự động hóa các hoạt động, minh bạch hóa các giao dịch và tiết kiệm thời gian giảm thiểu chi phí cho các công tác quản trị hệ thống tài chính.

Tới phiên bản 3.0 thì Blockchain tham gia với gần như tất cả các lĩnh vực của xã hội như quân đội, giáo dục, y tế và pháp luật.

Tiếp đến là trình bày chi tiết về cấu tạo và các thành phần liên quan của blockchain sẽ do bạn Lâm trình bày

**2. Các mô hình và cách thức hoạt động của Blockchain**

Blockchain bao gồm ba khái niệm quan trọng: blocks (khối), nodes (nút) and miners (thợ đào).

**Blocks**

Đơn vị lưu trữ dữ liệu của Blockchain được gọi là block. Mọi chain đều bao gồm nhiều blocks và mỗi block có ba phần tử cơ bản:

* Dữ liệu trong một block.
* Một số nguyên 32 bit được gọi là Nonce (Number only used once). Nonce được sinh ra ngẫu nhiên khi một block được tạo. Sau đó, số nonce được thêm vào hàm hash của block.
* Một hàm băm (hash) có chức năng tóm tắt dữ liệu từ một chuỗi dữ liệu có độ dài bất kỳ thành một giá trị chuỗi ký tự hoặc số duy nhất có độ dài cố định (256 bit).

Ví dụ: với thuật toán hash SHA256, chuỗi “Hello World” sẽ trở thành:

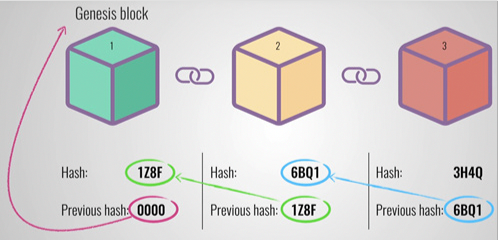
SHA256(“Hello World”) = a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Bất cứ sự thay đổi nhỏ nào trong dữ liệu gốc đều dẫn tới sự thay đổi hoàn toàn của giá trị băm:

SHA256 (“Hello Worl”) = 12fec4c65dd4455c48aff8977a7cd8ccb97539ad4cd7c37f13cf71ba8bee9a98

**Miners**

Miners tạo ra các block mới trên một chain thông qua quá trình mining.



Trong blockchain, mỗi block đều có hàm hash và số nonce riêng biệt, nhưng cũng tham chiếu đến hàm hash của block trước đó trong cùng một chain. Vì vậy, việc khai thác (mining) một block không dễ dàng, đặc biệt là trên các chain lớn.

Các thợ đào (miners) sử dụng phần mềm đặc biệt nhằm giải quyết các bài toán phức tạp để tìm ra được số nonce mà tạo ra một hàm hash được chấp nhận. Bởi vì số nonce có chiều dài 32 bits còn kết quả của hash có chiều dài 256 bits nên có khoảng bốn tỷ tổ hợp nonce-hash có thể phải được khai thác (mine) trước khi tìm được kết quả đúng. Khi điều đó xảy ra, những thợ đào (miners) được cho là đã tìm thấy "golden nonce" và block của họ được thêm vào chuỗi.

Khi thực hiện thay đổi đối với block đã có trước đó trong một chain, ta bắt buộc phải khai thác (mine) lại không chỉ block đó mà còn tất cả các block sau nó. Đây là lý do tại sao việc thao túng công nghệ blockchain cực kỳ khó khăn vì việc tìm ra các “golden nonce” đòi hỏi một lượng lớn thời gian và khả năng tính toán.

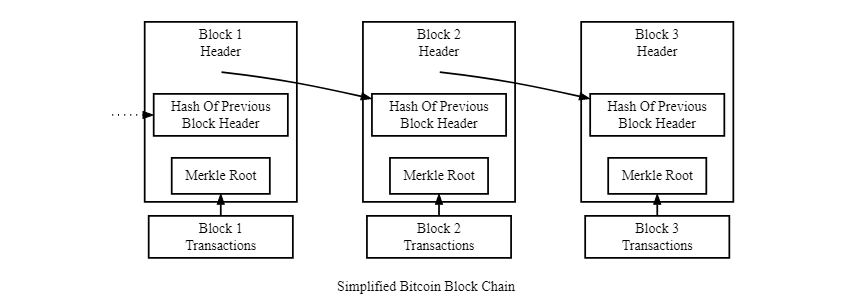
Khi một block được khai thác (mine) thành công, những thay đổi được tất cả các nodes trên mạng chấp nhận và người khai thác (miner) được thưởng crypto currency.

**Nodes**

Node đóng vai trò là cơ sở hạ tầng của Blockchain. Nó là các nút giúp lưu trữ, truyền tải và bảo quản dữ liệu blockchain, vì vậy về mặt lý thuyết, một blockchain tồn tại trên các node.

Cốt lõi của nó dựa trên các nguyên tắc của mạng P2P (Peer to Peer). Trong hầu hết các mạng, không có máy chủ trung tâm, mà là sự đồng thuận giữa những node.

Khi một thợ đào (miner) hay người xác thực (validator) thêm một block giao dịch mới vào blockchain, họ sẽ truyền block tới tất cả (hoặc một phần, tùy vào thuật toán đồng thuận của blockchain sử dụng) các node trên mạng.



Cách hoạt động node như sau:

* Các node kiểm tra xem một block giao dịch có hợp lệ không và chấp nhận hoặc từ chối nó.
* Nếu chấp nhận, các node sẽ lưu trữ các block giao dịch (lưu trữ lịch sử giao dịch blockchain).
* Các node phát và lan truyền lịch sử giao dịch này đến các node khác để đồng bộ hóa với blockchain (cập nhật về lịch sử giao dịch).

Một vấn đề lớn mà người dùng trong cộng đồng an ninh mạng phải đối mặt là họ không thể biết đầy đủ nhà cung cấp bảo mật nào mà họ có thể hoặc không thể tin tưởng. Nhưng đó lại là điều nơi mà blockchain có thể giúp ích. Với công nghệ blockchain, khách hàng sử dụng các dịch vụ an ninh mạng có thể xác minh rằng các cuộc tấn công web bị phát hiện và bị chặn trên thực tế là hợp pháp.

Do tính chất phi tập trung của chuỗi khối Bitcoin, tất cả các giao dịch có thể được xem một cách minh bạch bằng cách có một nút cá nhân hoặc sử dụng các trình khám phá chuỗi khối cho phép bất kỳ ai cũng có thể xem các giao dịch đang diễn ra trực tiếp. Mỗi nút có bản sao của chuỗi riêng của nó được cập nhật khi các khối mới được xác nhận và thêm vào. Điều này có nghĩa là nếu bạn muốn, bạn có thể theo dõi Bitcoin ở bất cứ đâu.

Các bản ghi trên blockchain là vĩnh viễn và khó thay đổi. Thay vì lấy lời của nhà cung cấp bảo mật, khách hàng có thể tham khảo chuỗi khối để xác minh dữ liệu về mối đe dọa, bao gồm cả xác thực giả. Tất nhiên, các bản ghi được lưu trữ trong chuỗi khối Bitcoin (cũng như hầu hết các chuỗi khác) đều được mã hóa. Điều này có nghĩa là chỉ chủ sở hữu của một bản ghi mới có thể giải mã nó để tiết lộ danh tính của họ (sử dụng cặp khóa công khai-riêng tư). Do đó, người dùng blockchain có thể ẩn danh trong khi vẫn giữ được tính minh bạch.

**\* An toàn và bảo mật**

Blockchain làm cho dữ liệu mở / minh bạch theo cách chưa tồn tại trong các hệ thống tài chính, đó là lý do tại sao nhiều người cho rằng blockchain có thể được sử dụng làm tiêu chuẩn mới cho tính minh bạch. Chính xác thì dữ liệu được thực hiện minh bạch trên blockchain như thế nào?

Những người tham gia mạng có khả năng truy cập các khoản nắm giữ và giao dịch của các địa chỉ công cộng bằng cách sử dụng trình khám phá khối, được sử dụng để tìm kiếm các khối của chuỗi khối, nội dung của chúng và các chi tiết liên quan của chúng.

Trong an ninh mạng, điều này có nghĩa là các dữ liệu mối đe dọa phi tập trung có thể được truy cập. Mặc dù một số người có thể tranh luận rằng các phân tích và báo cáo chuyên sâu cung cấp đủ tin cậy rằng các giải pháp bảo mật đang hoạt động đúng như mong muốn của chúng, nhưng sự thiên vị có thể phát huy tác dụng vì các công ty này đang trả tiền cho các báo cáo phân tích, chứng nhận và các xác nhận khác trong lần đầu địa điểm. Với blockchain, bất kỳ sự thiên vị nào cũng có thể bị loại bỏ nhờ tính minh bạch này.

Với blockchain, các nhà cung cấp bảo mật có thể có bằng chứng cụ thể để sao lưu các tuyên bố về hiệu suất hoặc hiệu quả của họ và các cá nhân sẽ có thể tham khảo thông tin này khi lựa chọn giải pháp an ninh mạng.

**Examples of Transparency:**

Ví dụ, các sàn giao dịch đã từng bị tấn công trong quá khứ, nơi những người giữ Bitcoin trên sàn giao dịch đã mất tất cả. Mặc dù tin tặc có thể hoàn toàn ẩn danh, nhưng Bitcoin mà họ trích xuất có thể dễ dàng theo dõi. Nếu Bitcoin bị đánh cắp trong một số vụ hack này được chuyển đi hoặc sử dụng ở một nơi nào đó, thì điều đó sẽ được biết.

**\* TIỆN ÍCH:**

1. Hợp lý hóa chuỗi cung ứng

Công nghệ chuỗi khối có thể giảm đáng kể các khâu trung gian chuỗi cung ứng tốn kém trong sản xuất. Trong cơ sở hạ tầng blockchain, dữ liệu được đồng bộ hóa trên mạng và theo cách có thể xác minh được. Các cuộc đàm phán hợp đồng phức tạp có thể được thực hiện theo cách ngang hàng, do đó, anh ta loại bỏ bất kỳ nhu cầu trung gian đắt tiền nào để tạo điều kiện thuận lợi cho việc thực hiện này và làm cho các quy trình kinh doanh nói chung hợp tác và hiệu quả hơn nhiều.

2. Theo dõi và truy tìm sản phẩm từ đầu đến cuối

Người tiêu dùng có nhiều thông tin hơn về các sản phẩm họ mua ngày nay hơn bao giờ hết. Thứ gì đó được làm ở đâu, ai làm ra nó, loại vật liệu nào được sử dụng - tất cả những chi tiết này ngày càng trở nên quan trọng đối với người tiêu dùng hiện đại, những người có vô số lựa chọn khi chọn nơi chi tiêu tiền mặt khó kiếm được của mình. Tính minh bạch là chìa khóa.

Các sản phẩm tiên phong như AURA, được phát triển bởi ConsenSys cùng với LVMH và Microsoft, đang đột phá. Bất kỳ chuỗi cung ứng hàng xa xỉ nào cũng phụ thuộc vào một số người chơi chuyên biệt, bắt đầu từ thiết kế, thu mua đến sản xuất và tất cả các con đường để phân phối. Dựa trên chuỗi khối Ethereum và sử dụng Microsoft Azure, nền tảng AURA cung cấp đầy đủ các dịch vụ theo dõi và truy tìm nguồn gốc hàng hóa xa xỉ. Từ nguyên liệu thô đến điểm bán cho đến chợ đồ cũ, người tiêu dùng có đầy đủ khả năng hiển thị và truy cập vào lịch sử của sản phẩm. AURA đảm bảo tính xác thực của sản phẩm, cung cấp thông tin chi tiết về nguồn gốc và thành phần sản phẩm (bao gồm thông tin về đạo đức và môi trường), hướng dẫn chăm sóc sản phẩm và các dịch vụ sau bán hàng và bảo hành.

3. Dự báo nhu cầu đáng tin cậy và lập kế hoạch hàng tồn kho:

Tính đến dữ liệu bán hàng trong quá khứ và các yếu tố thay đổi khác (ho, ho… COVID-19), dự báo nhu cầu giúp các nhà sản xuất hiểu được nhu cầu có thể xảy ra đối với sản phẩm của họ, do đó họ có thể lập kế hoạch sản xuất cho phù hợp. Dự báo nhu cầu là động lực cho hầu hết tất cả các quyết định liên quan đến chuỗi cung ứng, vì vậy độ chính xác và độ tin cậy của nó là rất quan trọng đối với sự thành công của doanh nghiệp sản xuất.

Dự báo nhu cầu không chính xác sẽ luôn dẫn đến hàng tồn kho không chính xác. Nếu bạn lập kế hoạch quá ít, bạn có nguy cơ mất cơ hội kinh doanh và sự hài lòng của khách hàng. Nếu bạn lập kế hoạch cho quá nhiều, lãng phí và chi phí phát sinh từ hàng tồn kho quá nhiều có thể gây bất lợi cho doanh nghiệp, và đây hoàn toàn là kết quả của sự không chắc chắn trong sản xuất. Theo Inbound Logistics, chi phí tồn kho dư thừa có thể dao động từ 15 đến 40% tổng chi phí tồn kho, bao gồm vốn, thuế, lưu kho, lỗi thời, hư hỏng và trộm cắp. Bạn thực hiện hàng tồn kho càng lâu, chi phí kinh doanh của bạn càng tăng.

Công nghệ chuỗi khối có thể cung cấp cho các nhà sản xuất dữ liệu dự báo chính xác và đáng tin cậy hơn nhiều cho việc lập kế hoạch nhu cầu và hàng tồn kho. Blockchains có thể theo dõi và quản lý tài nguyên một cách an toàn với độ chính xác cao. Họ lưu giữ hồ sơ tôn giáo về mọi thứ, và cả trong thời gian thực. Độ chính xác này cho phép các blockchains theo dõi tài nguyên ở cấp hệ thống, cho phép độ chính xác cao hơn, dự báo và giảm lượng hàng tồn kho, đồng thời đảm bảo cùng một mức độ dịch vụ cho khách hàng.

Script 1:

Hàm hash là một hàm số dùng để chuyển đổi dữ liệu từ một kích thước bất kì sang một kích thước nhất định.

Hàm hash là một hàm một chiều, không thể nghịch đảo và có độ dài cố định vậy nên ta không thể suy ngược đầu vào của một giao dịch từ kết quả hash cũng như suy luận lượng thông tin đầu vào dựa vào độ dài của kết quả hash.

Kết quả của hàm Hash là duy nhất đối với một đầu vào nhất định. Do vậy, người ta dùng kết quả của hàm hash để kiểm tra đầu vào giao dịch có đúng không mà không cần tiết lộ dữ liệu.

Các thuật toán hash được sử dụng rộng rãi là MD5 và SHA256. Trong đó MD5 tạo ra giá trị băm 128 bit và SHA256 tạo ra giá trị băm là 256bit và trong thực tế thì hàm SHA256 được chứng minh là an toàn và được sử dụng rộng rãi hơn.

Trong Blockchain thì các giá trị đầu ra từ hàm hash được sử dụng làm các định danh duy nhất cho các Block. Hàm hash nhận các đầu vào là dữ liệu đã mã hóa của block đó chứa thông tin về các giao dịch, thông tin về thời gian block đó được tạo ra, giá trị hash của block trước đó,…

Vì block phía sau sử dụng lại giá trị hash của block phía trước, từ đó tạo thành một chuỗi liên kết trong Blockchain.

Bởi vì vậy nên khi ta thay đổi nội dung của một Block thì giá trị hash của tất cả Block nằm phía sau trong chuỗi cũng phải thay đổi theo để tạo thành một chuỗi hợp lệ. Nhờ tính chất này nên người ta đã tận dụng và tạo ra cơ chế đồng thuận trong Blockchain.

Cơ chế đồng thuận blockchain có thể được định nghĩa là một cơ chế mà qua đó các nút phân tán trong hệ thống đều đạt được sự đồng thuận.

Trong cấu trúc truyền thống, sự đồng thuận hiếm khi là vấn đề nhờ vào sự tồn tại của cơ quan trung ương. Trái lại, trong một hệ thống phân tán như blockchain, mỗi giao điểm vừa là máy chủ vừa là không gian lưu trữ dữ liệu. Vì vậy, mỗi giao điểm phải trao đổi thông tin với giao điểm khác để đạt được sự đồng thuận.

Có hai cơ chế đồng thuận được sử dụng rộng rãi trong Blockchain, đó là Proof of Work và Proof of Stake

* Proof of Work

PoW là thuật toán đồng thuận đầu tiên được tạo ra. Nó được sử dụng trên Bitcoin và nhiều đồng tiền điện tử khác. Thuật toán Proof of Work là một phần thiết yếu của quá trình đào coin.

Cách thức hoạt động đó là những người tham gia blockchain (được gọi là thợ đào) phải giải bài toán cần tính toán phức tạp để có thể thêm một khối vào blockchain.

Các thợ đào cần tìm được hệ số Nonce để giá trị hash của block thỏa một điều kiện nào đó đã được blockchain đặt ra, gọi là golden nonce. Giả sử blockchain yêu cầu giá trị hash của block phải được bắt đầu bằng 000, thợ đào cần tìm số Nonce để giá trị hash thỏa điều kiện đặt ra.

Đào coin dùng PoW liên quan đến nhiều nỗ lực băm, ở đây là tìm ra giá trị “golden nonce”, vì vậy khả năng tính toán càng lớn có nghĩa là thực hiện được nhiều phép thử hơn trên mỗi giây. Nói cách khác, thợ đào có tỷ lệ băm cao có cơ hội tốt hơn để tìm một lời giải hợp lệ cho khối tiếp theo.

Thuật toán đồng thuận PoW đảm bảo rằng các thợ đào chỉ có thể xác nhận một khối giao dịch mới và thêm nó vào blockchain nếu các nút phân tán của mạng đạt được sự đồng thuận và đồng ý rằng hàm băm khối được đưa ra bởi thợ đào là một bằng chứng công việc hợp lệ.

* Proof of Stake

PoS thay thế PoW bằng một cơ chế mà trong đó các khối được xác nhận theo tỷ lệ cổ phần của những người tham gia. Trình xác nhận hợp lệ của mỗi khối (cũng được gọi là thợ đúc tiền) được xác định bằng tỉ lệ cổ phần của đồng tiền điện tử chứ không phải bằng lượng công suất tính toán được phân bổ.

Mỗi hệ thống PoS có thể thực hiện thuật toán theo nhiều cách khác nhau, nhưng nói chung, Blockchain được bảo đảm bằng một quá trình bầu chọn giả ngẫu nhiên dựa trên việc xem xét tài sản của nút và độ tuổi của coin - cùng với một hệ số ngẫu nhiên.

Cơ chế đồng thuận đóng vai trò quan trọng trong việc duy trì tính toàn vẹn và bảo mật của mạng tiền điện tử. Chúng cung cấp phương tiện để các nút phân tán đạt được sự đồng thuận về phiên bản đúng của blockchain. Việc đồng thuận với trạng thái blockchain hiện tại là điều cần thiết cho một hệ thống kinh tế kỹ thuật số hoạt động đúng.

Script 2:

Hiện nay người ta sử dụng các loại tiền tệ như tiền giấy, tiền xu, vàng bạc và tiền điện tử. Các loại tiền trên đều được sử dụng phổ biến và khá quen thuộc với chúng ta, trừ tiền điện tử mới trở nên phổ biến gần đây. Vậy tiền điện tử là gì?

Tiền điện tử được tạo thành từ những bit số hay còn được gọi là tiền đã được số hóa. Tiền điện tử chỉ hoạt động trong môi trường điện tử dùng để thanh toán chi phí. Để thực hiện được các giao dịch, người dùng phải dựa trên 3 yếu tố: Internet, mạng máy tính và các phương tiện điện tử của tổ chức phát hành.

Tiền điện tử không hiện hữu như một vật chất mà tồn tại vô hình thông qua môi trường điện tử. Chúng được lưu trữ trên: Internet, điện thoại, thông tin và các thẻ thanh toán điện tử khác. Điều này đồng nghĩa với việc người dùng không thể cầm nắm số tiền của mình được.

Bên cạnh đó, tiền điện tử có thể hiểu là phương thức thanh toán thông qua chữ ký bảo mật. Cũng như tiền giấy, tiền điện tử là công cụ dùng để giao dịch, tích lũy giá trị. Tiền điện tử có thể chuyển đổi thành tiền giấy theo yêu cầu của chủ sở hữu.

Tiền điện tử được chia làm 3 loại như sau:

* Tiền số pháp định: Là tiền điện tử được Chính phủ công nhận. Chúng được lưu trữ trong thẻ ATM, tài khoản ngân hàng, ví điện tử,… Tiền pháp định có giá trị ngang hàng với tiền mặt.
* Tiền ảo: Là tiền điện tử được phát hành và kiểm soát bởi các tổ chức, doanh nghiệp. Tiền ảo không được Chính phủ công nhận. Chúng chỉ hoạt động trong một môi trường ảo phục vụ những mục đích nhất định.
* Tiền mã hóa: Đây là tập hợp con của đồng tiền. Tiền mã hóa dựa trên nền tảng kỹ thuật số không bị chi phối bởi Chính phủ. Ưu điểm của dòng tiền này là tính bảo mật cao, không qua trung gian nên đảm bảo được an toàn.

**Coin là gì?**

Coin là một dạng tiền kỹ thuật số, được tạo ra bởi kỹ thuật mã hóa, lưu trữ giá trị theo thời gian.

Về cơ bản, Coin tương đương với tiền tệ. Bitcoin là một ví dụ điển hình nhất, Bitcoin dựa trên [công nghệ Blockchain](https://cryptoviet.com/blockchain-la-gi) mang tính công khai và phân tán với một sổ cái chung, trên đó tất cả giao dịch được công khai một cách minh bạch. Blockchain đảm bảo tính minh bạch và giảm thiểu gian lận.

Coin có đặc điểm tương tự như tiền tệ : chúng có thể được phân loại, có thể phân chia, được chấp nhận, di động, bền vững và có nguồn cung hữu hạn. Hấu hết những người tham gia thị trường Crypto đều nghĩ rằng Crypto tương lai sẽ thay thế tiền tệ.

**Token là gì?**

Token là tài sản kỹ thuật số do các dự án phát hành, thực hiện các chức năng tương tự như Coin, nhưng khác biệt chính là nó cho phép những người nắm giữ các Token này tham gia vào mạng lưới hệ thống.

Token thể hiện chức năng của tài sản kỹ thuật số, đại diện cho phần vốn của công ty, cho phép truy cập vào chức năng của dự án và nhiều hơn thế nữa.

Token đại diện cho một loại tài sản hay một ứng dụng, do đó Security và Utility là 2 dạng phân biệt lẫn nhau của Token. Security Token được thiết kế chia sẻ tài sản của công ty, trong khi đó Utility Token có một số trường hợp để sử dụng bên trong dự án đó.

+ Security token hay còn gọi với tên gọi khác là token chứng khoán. Chúng được xem như là một dạng cổ phiếu điện tử.

+ Utility token là một loại token tiện ích. Chứng được sinh ra theo mục đích và tính năng riêng theo mong muốn của người phát hành.

Ta có ba cách để phân biệt Coin và Token.

### Về định nghĩa

* Coin là đồng tiền ảo có thể hoạt động một cách riêng lẻ.
* Token là đồng tiền ảo phải dựa trên nền tảng của một loại tiền ảo khác để hoạt động. Ví dụ nền tảng Ethereum có thể dùng để xây dựng các loại token.

### Về mặt tính năng:

* Coin được tạo ra với mục đích sử dụng như một loại tiền tệ, một đơn vị lưu trữ giá trị và để giao dịch.
* Token thì có mục đích sử dụng rộng hơn Coin. Token có thể là nhiên liệu cho một mạng lưới hoạt động hay là đơn vị trao đổi trong một ứng dụng.

### Về mặt kỹ thuật:

* Một loại coin cần phải được phát triển ví lưu trữ riêng. Phí giao dịch sẽ được trừ thẳng vào coin đó.
* Token thì có thể lưu trữ cùng một ví được phát triển riêng cho nền tảng gốc. Phí giao dịch phải trả theo quy định của nền tảng gốc.

**Sàn giao dịch Crypto:**

Trên sàn giao dịch, các đồng tiền điện tử được niêm yết với thông tin cụ thể về giá cả, biến động giá và biểu đồ thị trường. Đây là nơi diễn ra các cuộc giao dịch, mua/bán giữa các nhà đầu tư. Những nhà đầu tư này thường có mục tiêu chung là tạo ra lợi nhuận.

Tiền điện tử được đánh giá dựa trên 3 yếu tố chính

* Khối lượng mua – bán
* Đơn vị phát hành
* Những thông tin liên quan đến kinh tế, chính trị.

Hiện tại, có hơn 400 sàn giao dịch phân rộng trên thế giới (theo thống kê của Coinmarketcap). Trong đó, sàn giao dịch tiền điện tử lớn và uy tín nhất vẫn là Binance (Trung Quốc).

**Top 10 sàn giao dịch crypto lớn nhất Việt Nam:**

Như mọi người thấy thì đây là top 10 sàn giao dịch Crypto lớn nhất Việt Nam. Trong đó 3 sàn lớn nhất là Binance, Huobi, Gate.io.

Binance: là sàn giao dịch tiền điện tử có nguồn gốc từ Trung Quốc, được sáng lập năm 2017. Hiện tại, sàn giao dịch này đã vượt mặt nhiều đối thủ để thống lĩnh vị trí đầu bảng. Tại Việt Nam và nhiều quốc gia trên thế giới, Binance đã quá nổi tiếng bởi độ uy tín, hiệu quả.

Huobi: là đối thủ nặng ký của Binance tại Việt Nam ở thời điểm hiện tại. Sàn giao dịch tiền điện tử này đã có mặt trên thị trường vào ngày 15/05/2013. Huobi phổ biến trên nhiều quốc gia như: Hàn Quốc, Nhật Bản, Hồng Kong, Việt Nam,…

Gate.io: cho ra mắt người dùng vào năm 2013 với tên gọi đầu tiên là Bter.com. Đây là một trong những sàn giao dịch tiền điện tử lâu đời nhất tại Trung Quốc. Gate.io chịu sự quản lý của tập đoàn Gate Technology Inc., trụ sở Hoa Kỳ.

**Ví tiền điện tử:**

Trước khi tìm hiểu các loại ví tiền điện tử tốt nhất, chúng ta cần hiểu ví tiền điện tử là gì? Hiểu một cách đơn giản, ví tiền điện tử là nơi lưu trữ tiền ảo. Thông thường, chúng được bảo vệ bằng mật khẩu hoặc nhiều cách khác để ngăn chặn việc truy cập trái phép. Không chỉ là nơi lưu trữ, nhiều loại ví tiền điện tử còn cho phép người dùng swap, giao dịch tiền điện tử một cách nhanh chóng.

Cộng đồng tiền điện tử hay nói với nhau rằng “Not your keys, not your Bitcoin” Có nghĩa là nếu không có ví thì số coin đó vẫn chưa thuộc về bạn. Vì nếu bạn lưu trữ trên các sàn giao dịch thì số BTC đó không thuộc sở hữu của của bạn mà nếu sàn ngưng hoạt động thì bạn vẫn mất số tài sản đó.

**Phân loại ví tiền điện tử:**

**Ví nóng:**

Là loại ví dùng để giao dịch Bitcoin của bạn bất cứ khi nào cũng cần phải kết nối với internet để kết nối với mạng Bitcoin. Thường là các loại ví trữ Bitcoin trực tuyến (online) nên bắt buộc phải có kết nối internet.

Ưu điểm: Ví nóng có ưu điểm là đăng ký tạo ví Bitcoin miễn phí, thiết lập dễ dàng, tiện sử dụng khi giao dịch, mua bán hay thanh toán.

Nhược điểm: Mức độ bảo mật không cao, không cao bằng ví lạnh thôi, chứ nhiều ví nóng vẫn bảo mật rất tốt và uy tín.

**Ví lạnh:**

Cũng là ví dùng để giao dịch Bitcoin nhưng bạn không cần phải kết nối internet mà vẫn có thể giao dịch được, vì nó được sử dụng để lưu trữ Bitcoin ngoại tuyến (Offline).

Ưu điểm: Ví cứng là loại ví bảo mật an toàn tốt nhất mà bạn có thể trữ Bitcoin, vì không có kết nối với Internet nên hacker không thể nào hack được tiền của bạn. Tất nhiên, vẫn có rủi ro, ví dụ bạn làm mất ví và quên luôn cả mã khôi phục thì coi như mất tiền.

Nhược điểm: Chi phí để mua một chiếc ví lạnh khá cao từ 2,5 triệu đến 3,5 triệu VNĐ, nếu bạn là nhà đầu tư nhỏ lẻ thì phí mua không hề ít. Ngoài ra, thiết lập ví lạnh Bitcoin hơi phức tạp nếu bạn là người mới, giao dịch gửi/nhận cũng không tiện bằng ví nóng.

----------next slide ----------------

**Ví web online** – một loại ví có thể nói là phổ biến nhất hiện nay, bạn có thể đăng ký ví Bitcoin và các Altcoin hoàn toàn miễn phí và thiết lập nhanh chóng để giao dịch coin. Với ví web thì Coinbase và Blockchain là hai loại ví bitcoin uy tín nhất hiện nay mà bạn có thể sử dụng để trữ Bitcoin và Ethereum, hai ví này cũng có luôn ứng dụng ví trên điện thoại.

**Ví phần mềm (Software Wallet)** là một dạng ví nóng, bạn có thể tải phần mềm ví về để cài đặt trực tiếp trên máy tính của bạn để quản lý tiền. Ngoài ra, một số phần mềm ví hỗ trợ cả ứng dụng trên điện thoại rất tiện lợi và an toàn. Ví bitcoin phần mềm có ưu điểm là bạn được giữ luôn Private key, tức là tiền của bạn do chính bạn kiểm soát, dịch vụ ví họ chỉ cung cấp nền tảng để bạn quản lý mà thôi chứ không hề giữ tiền của bạn.

**Ví cứng:** có hình dạng giống như chiếc USB, nó tách dời hoàn toàn với môi trường internet, khi nào bạn muốn giao dịch thì có thể kết nối ví lạnh với máy tính thông qua cổng USB. Vì thế hacker hoàn toàn không thể lấy cắp tiền trong ví cứng Bitcoin của bạn.

**Ví giấy Bitcoin** hay **Paper Wallet** là một dạng ví trữ lạnh, đúng như tên gọi của nó thì ví giấy Bitcoin là một tờ giấy, trên đó có in Private key, thông tin địa chỉ ví BTC và mã QR-code của bạn để sử dụng khi cần. Ưu điểm của ví giấy là không cần kết nối với Internet vẫn có thể giao dịch bình thường nên tránh được các mối nguy hại từ hacker, nhưng nhược điểm là dễ rách, nát và nếu mất bạn sẽ không thể lấy lại được tiền của mình.

Một trong nhưng vấn đề của tiền mã hóa là giá trị biến động lớn trong thời gian ngắn. Điều này dẫn đến việc nó khó có thể được áp dụng vào việc thanh toán tiền cho dịch vụ và hàng hóa. Stablecoin ra đời để khắc phục nhược điểm này. Stablecoin là tài sản kỹ thuật số được thiết kế để bắt chước giá trị của các loại tiền pháp định như đồng đô-la hoặc đồng euro. Chúng cho phép người dùng chuyển giá trị trên toàn cầu với giá rẻ và nhanh chóng trong khi vẫn duy trì sự ổn định về giá chứ không biến động như các loại tiền mã hóa khác.

Về phân loại thì stablecoin được chia làm 4 loại:

Thứ nhất là Fiat-collateralized . đây là loại stablecoin Được đảm bảo, thế chấp bằng tiền pháp định như đô la Mỹ($), bảng Anh (£), …

Thứ hai là Commodity-collateralized. đây là loại stablecoin Được đảm bảo, thế chấp bằng các tài sản hàng hóa như bất động sản, kim loại quý,...

Thứ ba là Crypto-collateralized. đây là loại stablecoin Được đảm bảo, thế chấp bằng các loại tiền điện tử khác như Bitcoin(BTC), Ethereum(ETH),...

Thứ tư là Non-collateralized, đây là loại stablecoin Không được đảm bảo, thế chấp bằng tài sản có giá trị thực. Giá trị được ổn định thông qua các thuật toán.

Stablecoin được ổn định bằng các cơ chế cân bằng giá.

Cơ chế đầu tiên là Redeem & expand, thường được áp dụng cho loại stablecoin được thế chấp bằng tiền pháp định hoặc hàng hóa. Đây là một cơ chế đơn giản, sẽ có một tổ chức trung tâm hoặc ngân hàng, dự trữ một lượng tiền pháp định đứng ra đảm bảo việc quy đổi, hoạt động giống như cách mà cách chính phủ và các ngân hàng ổn định giá cả thị trường.

Ví dụ, đối với các loại Stablecoin như USDT hay USDC khi giá rời peg thì hệ thống có cơ chế cân bằng như sau:

* Nếu USDC < $1 => nên đổi USDC để lấy tài sản thế chấp cơ bản, do đó mua một đô la với giá ít hơn một đô la.
* Nếu USDC > $1 => nên thế chấp đồng đô la để minted ra USDC và bán nó trên thị trường để kiếm chênh lệch.

Cơ chế cân bằng giá thứ 2 là Leveraged Loans, thường được áp dụng cho loại stablecoin được thế chấp bằng tiền mã hóa khác. Đây là một cơ chế khá phức tạp vì cần ít nhất 3 tài sản (stablecoin, tiền mã hóa làm tài sản thế chấp , tài sản được dùng để quy đổi với stablecoin)

Cơ chế này yêu cầu giá trị của tiền mã hóa thế chấp lớn hơn nhiều so với giá trị stablecoin được tạo ra để tránh các cuộc tấn công đầu cơ.

Một ví dụ tiêu biểu của loại này là DAI một stablecoin được gắn với đô la Mỹ nhưng được thế chấp bằng tiền điện tử Ethereum.