



THE DARIU FOUNDATION

BLOCKCHAIN-NFT FROM ZERO...



TS. Lê Trọng Nhân - Th.S Băng Ngọc Bảo Tâm

LỜI MỞ ĐẦU

Nhóm tác giả:

Nguyễn Văn Hạnh, Lê Trọng Nhân, Nguyễn Trần Hữu Nguyên, Võ Tấn Phương
Nguyễn Thanh Hải, Phạm Văn Vinh, Lê Phương Nam, Băng Ngọc Bảo Tâm

Mục lục

Chương 1. Giới thiệu về Blockchain	7
1 Blockchain là gì?	8
2 Ý tưởng ra đời công nghệ Blockchain	8
2.1 Hạn chế trong giao dịch	8
2.2 Hạn chế trong giao dịch qua hệ thống ngân hàng	9
3 Các đặc điểm nổi bật của Blockchain	11
4 Blockchain hoạt động như thế nào?	13
4.1 Cấu trúc của mỗi Block (Khối)	13
4.2 Quá trình cập nhật dữ liệu lên Blockchain	14
4.3 Thuật toán Blockchain	15
5 Các ứng dụng thực tiễn của Blockchain.	16
5.1 Ứng dụng trong sản xuất	16
5.2 Ứng dụng Blockchain trong thương mại điện tử	16
5.3 Ứng dụng của Blockchain trong y tế	17
5.4 Ứng dụng của Blockchain trong giáo dục	18
5.5 Ứng dụng Blockchain trong nông nghiệp	18
Chương 2. Giới thiệu về tiền mã hóa	21
1 Tiền mã hóa (Cryptocurrency) là gì	22
2 Phân biệt tiền điện tử & tiền mã hóa	22
2.1 Tiền điện tử	22
2.2 Tiền mã hóa	23
3 Các loại tiền mã hóa phổ biến hiện nay	23
3.1 Coin và Token trong Cryptocurrency	23
3.1.1 Coin là gì	23
3.1.2 Token là gì	23
3.1.3 Sự khác nhau giữa coin và token	24
3.2 Bitcoin và Altcoin trong Cryptocurrency	25
4 Ưu nhược điểm của tiền mã hóa	25
4.1 Ưu điểm của tiền mã hóa	25
4.2 Nhược điểm của tiền mã hóa	26
5 Tiền mã hóa hoạt động như thế nào?	26
6 Tính hợp pháp của tiền mã hóa ở Việt Nam	26
Chương 3. Giới thiệu về Bitcoin và Ethereum	29
1 Bitcoin là gì?	30
2 Lịch sử hình thành Bitcoin	30

3	Sự khác biệt giữa Bitcoin với các loại tiền khác	31
3.1	Tính phi tập trung	31
3.2	Tính bảo mật và tính không thể làm giả	31
3.3	Phí giao dịch thấp	31
3.4	Không thể lấy lại tiền khi giao dịch đã xảy ra	31
4	Cách thức hoạt động của Bitcoin	32
4.1	Công nghệ Blockchain	32
4.2	Công nghệ Sổ cái phân tán (DLT)	33
4.3	Ví dụ	33
5	Giá trị thực của Bitcoin nằm ở đâu?	33
6	Ethereum là gì?	34
7	Cách thức hoạt động của Ethereum	34
8	Ethereum có thể được sử dụng để làm gì?	35
9	So sánh Bitcoin và Ethereum	36
Chương 4. Giới thiệu về hợp đồng thông minh		39
1	Hợp đồng thông minh là gì?	40
2	Khác biệt giữa hợp đồng truyền thống và hợp đồng thông minh	41
3	Cách thức hoạt động của hợp đồng thông minh	41
4	Các tính năng chính của Hợp đồng thông minh	43
5	Ưu điểm và nhược điểm của hợp đồng thông minh	45
5.1	Ưu điểm	45
5.2	Nhược điểm	45
6	Quy trình tạo một hợp đồng thông minh	46
7	Các ứng dụng dựa trên hợp đồng thông minh	46
7.1	Ứng dụng cho các hoạt động quản lý	46
7.2	Ứng dụng vào công tác bầu cử	47
7.3	Ứng dụng trong chuỗi cung ứng Logistics	47
7.4	Ứng dụng vào lĩnh vực y tế	47
Chương 5. Xây dựng ứng dụng giao dịch ảo bằng Blockchain		49
1	Giới thiệu về ứng dụng	50
2	Xây dựng cấu trúc dữ liệu cho ứng dụng	50
2.1	Khái quát lập trình JSON trong Python	50
2.1.1	Đọc dữ liệu JSON	50
2.1.2	Chuyển đổi định các định dạng khác trong Python sang định dạng JSON	51
2.2	Thiết lập thông số để tương tác với server Adafruit	51
2.3	Cấu trúc của một Block	52
2.4	Cấu trúc của một Transaction	53
3	Hiện thực quy trình giao dịch cho ứng dụng	54
3.1	Hàm chuyển tiền	54
3.2	Hàm kiểm tra thông tin tài khoản	54
3.3	Hàm xác thực giao dịch	55
3.4	Hàm gửi dữ liệu	55
3.5	Xử lý transaction	55
3.6	Subscribe vào feed để nhận dữ liệu mỗi khi có dữ liệu mới	56
4	Chạy thử nghiệm ứng dụng	57

Chương 6. Quy trình xây dựng một NFT	59
1 NFT là gì?	60
2 Quy trình vận hành của NFT	60
3 NFT được phát minh từ bao giờ?	61
4 Làm thế nào để tạo và giao dịch NFT?	62
4.1 Tạo ra NFT có mất phí?	63
4.2 Làm thế nào để bán NFT?	64
5 Tại sao người ta lại mua NFT?	65
6 NFT trong thị trường nghệ thuật	65
7 Giao dịch NFT	66
Chương 7. Tạo tác phẩm nghệ thuật bằng ngôn ngữ lập trình Python	69
1 Giới thiệu về thư viện Python Turtle	69
2 Các hàm thường được sử dụng để vẽ hình	69
3 Hướng dẫn sử dụng thư viện Python turtle để vẽ một số hình cơ bản	70
3.1 Vẽ hình vuông xoắc ốc	70
3.2 Vẽ xoắn ốc tròn nhiều nét màu và thay đổi màu nền	71
3.3 Vẽ tam giác và tô màu tại vị trí người dùng click chuột vào .	72
3.4 Chương trình vẽ Doraemon	74
3.5 Một số tác phẩm nghệ thuật khác được vẽ bằng Python turtle	75
4 Pixel Art	75
4.1 Pixel là gì	75
4.2 Pixel Art là gì?	76
5 Vẽ các tác phẩm Pixel Art bằng Python	78
5.1 Tô màu cho tác phẩm Pixel Art	81
Chương 8. Quy trình tham gia giao dịch các NFT	85
1 Ví điện tử là gì?	85
1.1 Private Key và Public Key là gì?	85
2 Ví điện tử Metamask	86
2.1 Metamask là gì	86
2.2 Các chức năng của ví Metamask Wallet?	86
2.3 Hướng dẫn cài đặt Metamask trên trình duyệt Chrome	86
3 Thị trường lớn nhất thế giới về NFT - OpenSea	91
3.1 OpenSea là gì?	91
3.2 Cơ chế mua bán trên OpenSea như thế nào?	91
3.3 Có thể mua bán những gì trên OpenSea?	91
3.4 Cần gì để có thể giao dịch mua và bán trên OpenSea?	92
4 Hướng dẫn kết nối ví MetaMask với OpenSea để bắt đầu giao dịch .	92
5 Hướng dẫn tạo Collections và thêm vật phẩm số NFT để bán trên OpenSea	93
6 Niêm yết và bán các tác phẩm NFT trên sàn OpenSea	95
6.1 Set Price (giá cố định)	96
6.2 Highest Bid (đầu giá)	96
6.3 Bundle (nhóm sản phẩm)	97
7 Một số lưu ý khi đăng bán NFT	97



CHƯƠNG 1

Giới thiệu về Blockchain



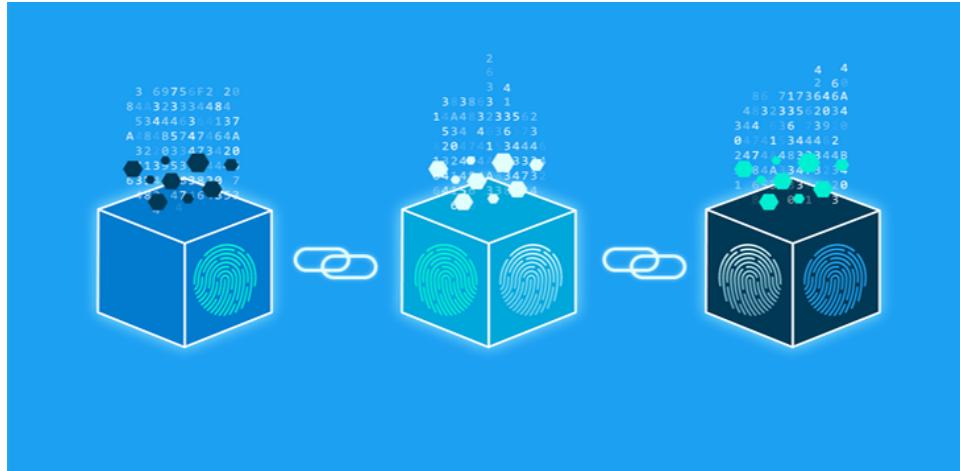
Blockchain là chủ đề đang vô cùng nóng trên toàn cầu hiện nay. Nó cùng với Bitcoin và tiền kỹ thuật số đã trở thành đề tài bàn luận trên rất nhiều mặt báo và trong những cuộc trò chuyện của mọi người. Tuy nhiên, khi nói về blockchain vẫn còn nhiều tranh cãi. Có người lo lắng rằng Bitcoin có thể chỉ là bong bóng, nhiều người cho rằng công nghệ phía sau nó là một sự đột phá, và công nghệ ấy sẽ tiếp tục con đường của mình cho đến khi được chấp nhận và tích hợp với Internet.

Vậy thì Blockchain thực chất là gì? Blockchain có thể ứng dụng vào những lĩnh vực nào trong cuộc sống và tại sao Blockchain lại được quan tâm như vậy?

1 Blockchain là gì?

Blockchain là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối (block) được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối (block) sẽ chứa thông tin về thời gian khởi tạo khối đó và được liên kết với khối trước đó, kèm một mã thời gian và dữ liệu giao dịch.

Hiểu đơn giản, Blockchain là một cuốn sổ cái điện tử được phân phối trên nhiều máy tính khác nhau, lưu trữ mọi thông tin giao dịch, và đảm bảo các thông tin đó không thể bị thay đổi dưới bất kỳ hình thức nào. Mọi thông tin được lưu trên cuốn sổ cái đó sẽ được xác nhận bởi hàng loạt máy tính được kết nối trong một mạng lưới chung. Sẽ không một cỗ máy nào có khả năng thay đổi, viết đè lên hay xóa dữ liệu trong cuốn sổ cái đó.



Hình 1.1: Các block được liên kết với nhau trên Blockchain

2 Ý tưởng ra đời công nghệ Blockchain

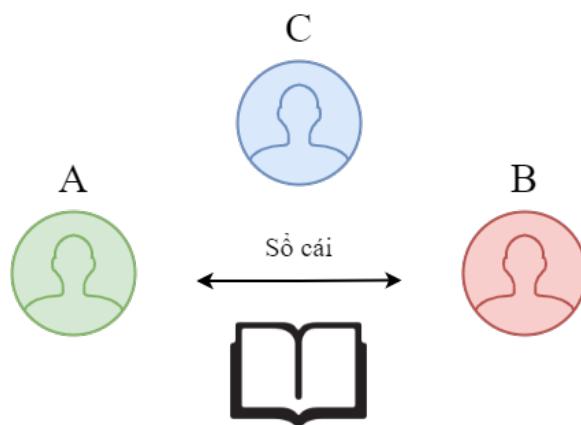
2.1 Hạn chế trong giao dịch

Ngày xưa, khi giao dịch tiền tệ, vay tiền, trả nợ, người ta sẽ thỏa thuận với nhau (giữa A và B) và ghi lại các thông tin giao dịch đó vào 1 cuốn sổ để lưu trữ nó - gọi là sổ cái. Sau đó đưa sổ này cho 1 người trung gian C uy tín nắm giữ. Và tất nhiên

người C này phải đều được A và B tin tưởng.

Ở đây chúng ta sẽ thấy các thành phần tham gia như sau:

- A & B là 2 người tham gia giao dịch với nhau.
- C là người uy tín đứng ra làm trung gian.
- Sổ cái (bằng giấy).



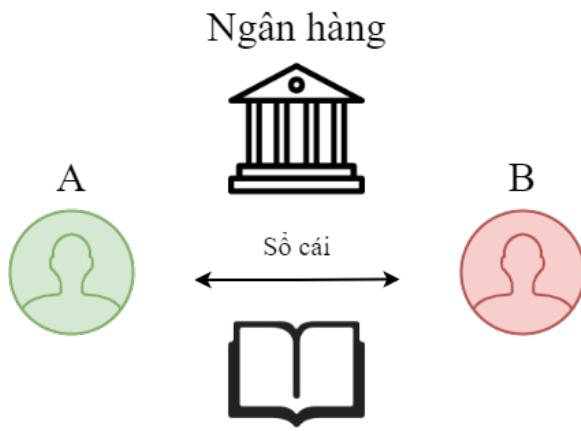
Hình 1.2: Cách giao dịch thông thường thời xưa.

Trong trường hợp này, chúng ta sẽ đối mặt với một số hạn chế:

- Cuốn sổ thường được làm bằng giấy và nó dễ bị moi mọt, bị hỏng theo thời gian. **Tức là thông tin lưu trữ trên đó không tồn tại mãi mãi.** Ví dụ: A vay tiền của B trong thời hạn 12 năm. Nhưng 10 năm sau cuốn sổ mục nát và không còn xem được thông tin trên đó. Lúc đó A chối cãi là không vay tiền của B, và B cũng không còn cuốn sổ để mang ra làm bằng chứng xác thực là A đã vay tiền của mình.
- **Thông tin có thể bị thay đổi hoặc phá huỷ:** 1 ai đó lấy trộm được cuốn sổ và họ có thể xoá 1 dòng thông tin, hoặc xé đi 1 trang sổ, lúc đó thông tin không còn toàn vẹn như lúc ban đầu của nó nữa. Tức là thông tin có thể bị thay đổi.
- **Tồn tại trung gian thứ 3:** cuốn sổ đó lại do 1 người trung gian thứ 3 đủ uy tín nắm giữ. Và không phải ai cũng có thể dễ dàng tìm được 1 người thứ 3 để đứng ra xác nhận. Và đồng thời lúc này 2 người giao dịch kia phải hoàn toàn đặt niềm tin vào người trung gian này.

2.2 Hạn chế trong giao dịch qua hệ thống ngân hàng

Tới khi xã hội phát triển, chúng ta có hệ thống ngân hàng thay thế cho người C thứ 3 trung gian kể trên. Và cuốn sổ cái làm bằng giấy được thay thế bằng hệ thống máy tính của ngân hàng.



Hình 1.3: Cách giao dịch thông qua ngân hàng.

Ưu điểm của hệ thống ngân hàng:

- Thường được chính phủ, nhà nước đứng ra đảm bảo quyền lợi của người giao dịch.
- Thông tin lưu trong hệ thống máy tính bền vững theo thời gian, không sợ bị "mục nát" theo thời gian.

Tuy nhiên, việc giao dịch qua hệ thống ngân hàng vẫn có một số vấn đề như:

- **Nguy cơ dữ liệu bị đe dọa:** Do máy chủ ngân hàng chứa rất nhiều thông tin quan trọng nên luôn là mục tiêu tấn công của nhiều kẻ xấu. Dữ liệu vẫn có thể bị đánh cắp hoặc thay đổi.

Một ngân hàng Ấn Độ mất 13,5 triệu USD vì bị tấn công mạng



Tội phạm mạng vừa tấn công vào nhiều hệ thống của ngân hàng Ấn Độ Cosmos Bank, rút hết gần 944 triệu rupee, tương đương 13,5 triệu USD, bằng việc rút tiền đồng thời trên 28 nước.

Hình 1.4: Ngân hàng ở Ấn Độ bị kẻ xấu tấn công

- **Phí giao dịch:** khoản phí khi người dùng thực hiện việc chuyển khoản cho nhau cũng là 1 vấn đề đối với các giao dịch.
- **Vấn tồn tại bên thứ 3 trung gian, đó chính là ngân hàng:** các thông tin giao dịch của người dùng do ngân hàng nắm giữ. Và họ có thể khai thác, hoặc bán thông tin này cho bên thứ 3. Ngoài ra, các **hệ thống quản lý tập trung**, ngân hàng hay nhà nước có thể yêu cầu đóng băng tài khoản của người dùng. Và đây là trường hợp mà không khách hàng nào mong muốn.

⇒ Do đó, Blockchain đã ra đời để giải quyết các vấn đề kể trên.

3 Các đặc điểm nổi bật của Blockchain

Sự ra đời của Blockchain dùng để giải quyết các hạn chế trong hệ thống giao dịch thông thường, do đó, Blockchain sẽ có các tính chất nổi bật sau:



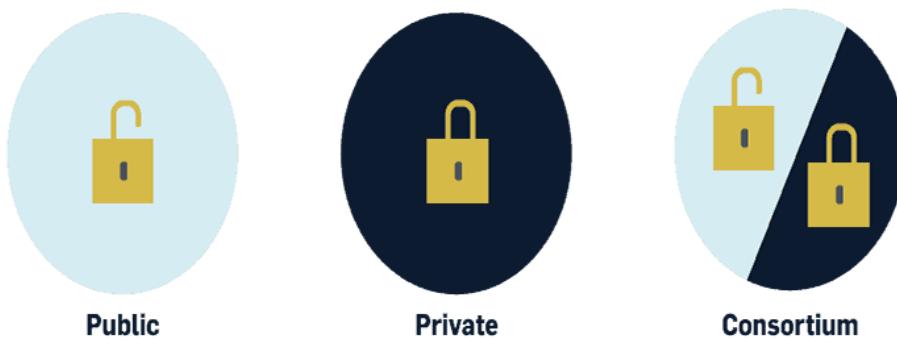
Hình 1.5: Các tính chất của công nghệ Blockchain

Cụ thể:

- **Tính phi tập trung (Decentralized):** Blockchain hoạt động độc lập theo các thuật toán máy tính, hoàn toàn không bị bất kỳ một tổ chức nào nắm quyền kiểm soát. Chính vì vậy blockchain tránh được rủi ro từ bên thứ 3.
- **Tính phân tán (Distributed):** các khối chứa dữ liệu giống nhau nhưng được phân tán ở nhiều nơi khác nhau. Nên chảng may 1 nơi bị mất hoặc hỏng thì dữ liệu vẫn còn trên Blockchain.
- **Không thể thay đổi:** một khi dữ liệu đã được ghi vào trong block của blockchain thì nó không thể bị thay đổi hoặc sửa chữa, bởi đặc tính của thuật toán đồng thuận và mã hash (mình sẽ trình bày chi tiết ở phần dưới).
- **Tính bảo mật:** chỉ có người nắm giữ Private Key (khóa riêng tư) mới có thể truy cập các dữ liệu bên trong Blockchain.
- **Tính minh bạch:** các giao dịch trong blockchain được lưu lại và mọi người có thể check các giao dịch này. Dựa vào đó, ta có thể kiểm tra và truy xuất lịch sử giao dịch. Thậm chí người ta có thể phân quyền để cho phép người khác truy cập một phần thông tin trên Blockchain.
- **Tích hợp Smart contract (hợp đồng thông minh):** dựa vào đó các điều khoản được ghi trong hợp đồng thông minh sẽ được thực thi khi các điều kiện trước đó được thỏa mãn, không ai có thể ngăn cản hoặc hủy nó.

Bên cạnh đó, hệ thống Blockchain cũng được chia thành 3 loại chính:

- **Public:** bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có rất nhiều nút tham gia. Vì vậy, muốn tấn công được vào hệ thống Blockchain này cần chi phí rất lớn và thực sự không khả thi. Ví dụ: Bitcoin, Ethereum,...
- **Private:** người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.
- **Permissioned (hay còn gọi là Consortium):** một dạng của Private nhưng bổ sung thêm 1 số tính năng khác, đây là sự kết hợp giữa Public và Private. Ví dụ: các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain của riêng mình.



Hình 1.6: 3 loại Blockchain chính

Hiện tại, công nghệ Blockchain trải qua 4 giai đoạn như sau:

- **Công nghệ Blockchain 1.0 – Tiền tệ và Thanh toán:** đây là phiên bản đầu tiên của công nghệ blockchain. Nhờ áp dụng công nghệ sổ cái phân tán phi tập trung (Distributed Ledger Technology) mà các giao dịch được diễn ra trên Blockchain được xử lý nhanh chóng và minh bạch. Ví dụ tiêu biểu cho phiên bản Blockchain 1.0 là Bitcoin, đồng tiền điện tử đầu tiên trên thế giới và đặt nền móng cho sự phát triển của thị trường Crypto.
- **Công nghệ Blockchain 2.0 – Hợp đồng thông minh:** đây là phiên bản thứ 2 của công nghệ blockchain. Với hợp đồng thông minh (hay Smart Contract), giao dịch trên Blockchain sẽ được giảm mạnh các chi phí xác thực, chống gian lận, vận hành, đồng thời tăng tính minh bạch. Phiên bản này loại bỏ hoàn toàn các yếu tố cảm tính hay đạo đức thường gặp khi làm việc với con người, ví dụ điển hình là Ethereum.
- **Công nghệ Blockchain 3.0 – Ứng dụng phi tập trung:** ứng dụng phi tập trung (DApp - Decentralized Application) là các phần mềm được triển khai độc lập, không nằm trên một máy chủ duy nhất mà lưu trữ một cách phân tán trên các kho lưu trữ phi tập trung và có thể được viết bằng bất kỳ ngôn ngữ nào.

Hầu hết mã nguồn của Dapp đều chạy trên các mạng lưới ngang hàng (Peer-to-Peer), điều này ngược lại so với các ứng dụng truyền thống và chỉ chạy trên một hệ thống tập trung duy nhất.

- **Công nghệ Blockchain 4.0 - Ứng dụng vào thực tiễn:** công nghệ Blockchain 4.0 là phiên bản Blockchain mới nhất hiện nay. Phiên bản này sẽ áp dụng tất cả những ứng dụng từ phiên 1 đến 3, đưa Blockchain vượt khỏi biên giới tài chính, và đi vào các lĩnh vực như giáo dục, chính phủ, y tế và nghệ thuật

4 Blockchain hoạt động như thế nào?

Để một block (khối thông tin) được thêm vào Blockchain, phải có 4 yếu tố:

- **Phải có giao dịch:** nghĩa là phải có hoạt động mua bán, trao đổi diễn ra. Ví dụ: bạn thực hiện mua hàng trên Amazon
- **Giao dịch đó phải được xác minh:** mọi thông tin liên quan đến giao dịch như thời gian, địa điểm, số tiền giao dịch, người tham gia... đều phải được ghi lại. Ví dụ: khi xem tình trạng đơn hàng, bạn sẽ biết được mình đã order những gì, tổng tiền là bao nhiêu, khi nào thì nhận được hàng...
- **Giao dịch đó phải được lưu trữ trong block:** bất cứ lúc nào bạn cũng xem lại được thông tin đơn hàng mà mình đã thực hiện. Chúng được lưu trữ trong mục “Quản lý đơn hàng”.
- **Block đó phải nhận được hash** (hàm chuyển đổi một giá trị sang giá trị khác): chỉ khi nhận được hash thì một block mới có thể được thêm vào blockchain.

Công nghệ Blockchain cho phép trao đổi tài sản/thực hiện giao dịch mà không cần có sự chứng kiến của người thứ ba hoặc không cần dựa trên sự tin tưởng. Hay nói cách khác, Blockchain là nền tảng cho sự ra đời của các hợp đồng thông minh.

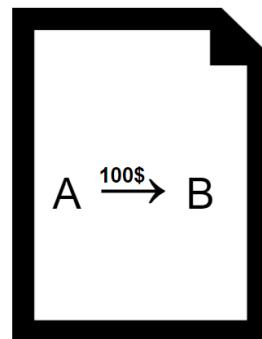
4.1 Cấu trúc của mỗi Block (Khối)

Mỗi block bao gồm 3 thành phần: Dữ liệu (Data), mã hàm băm (Hash) và mã Hash của khối trước nó.

- **Data:** các bản ghi dữ liệu đã được xác thực của anh em đã được bảo vệ bằng thuật toán mã hóa tùy thuộc vào từng blockchain.
- **Hash:** mã hàm băm của của Block. Đây là chuỗi các ký tự và số được tạo một cách ngẫu nhiên và không giống nhau. Nó đại diện riêng cho block đó và được mã hoá bằng thuật toán mã hoá. Mã hash dùng để phát hiện sự thay đổi trong các khối.
- **Previous Hash:** mã hàm băm của block trước đó. Nó dùng để các khối liền kề nhận biết khối nào trước, khối nào sau và nối với nhau.

4.2 Quá trình cập nhật dữ liệu lên Blockchain

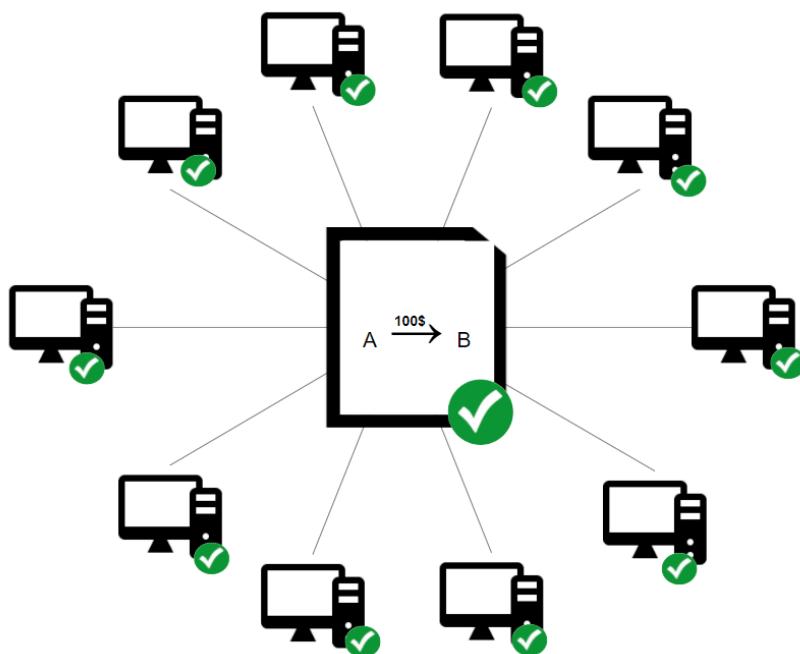
Đầu tiên, thông tin giao dịch sẽ được ghi lại trên hệ thống tạo thành bản ghi (record).



Hình 1.7: Một bản ghi trên hệ thống.

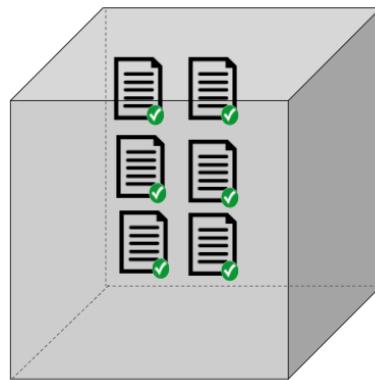
Sau đó, bản ghi sẽ được xác thực là có giá trị bởi các máy tính có trong hệ thống (được gọi là nút hay node) theo thuật toán đồng thuận trên Blockchain. Ví dụ:

- Bản ghi cho thấy một người A bán 3 Bitcoin → Hệ thống xác thực người A có 3 bitcoin trong ví → Khi ấy bản ghi có hiệu lực.
- Nếu người A chỉ có 1 Bitcoin → Hệ thống xác định tài khoản của người A không đủ Bitcoin để thực hiện giao dịch → Khi ấy bản ghi vô hiệu lực.



Hình 1.8: Các máy tính trong hệ thống sẽ xác thực giá trị của bản ghi.

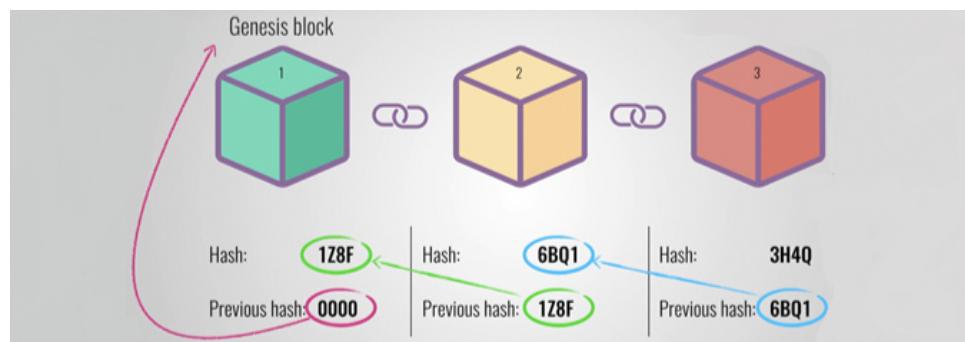
Tiếp theo, bản ghi đã xác thực có giá trị cùng với hàng loạt bản ghi đã xác thực từ những người giao dịch khác sẽ được xếp vào thành một khối thông tin (block).



Hình 1.9: Một Block gồm nhiều bản ghi đã được xác thực là có giá trị.

Cuối cùng, khối (Block) vừa mới được tạo sẽ được thêm vào chuỗi (Chain) bằng cách kết nối Previous Hash của khối cần thêm vào với mã hash của khối trước đó và tạo thành một Chuỗi khối (Blockchain).

Khối đầu tiên do không có khối nào trước nó nên mã Hash của nó là chuỗi số 0 hoặc chuỗi tự định nghĩa. Và nó được gọi là khối nguyên thuỷ hay Genesis Block.



Hình 1.10: Các khối (Block) được thêm vào chuỗi (Chain).

4.3 Thuật toán Blockchain

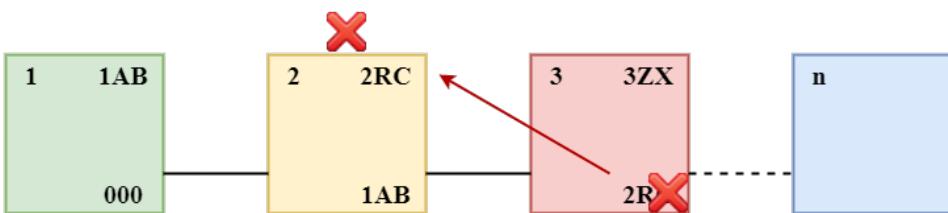
Thuật toán đồng thuận Blockchain là sự đồng ý xác thực thông tin trong bản ghi là chính xác của đa số các nút ở trong mạng lưới và cho phép ghi lại thông tin giao dịch vào trong Blockchain.

Nếu có sự thay đổi của một block trong mạng lưới. Dữ liệu này được so sánh với các dữ liệu của các khối khác. Nếu có sự khác biệt thì nó sẽ không cho phép dữ liệu ấy được ghi vào bên trong Blockchain. Đó là cách Blockchain được thiết kế để chống lại sự thay đổi dữ liệu.

Ví dụ: Trường hợp nếu có thay đổi trên 1 khối. Ở đây mình giả sử kẻ tấn công (hacker) tấn công và thay đổi thông tin trên khối A. Tại thời điểm đó:

- Mã hash của khối A bị thay đổi.

- Hệ thống sẽ so sánh mã hash đó với mã hash khối trước đó & phát hiện ra sai lệch.
- Như vậy hacker phải thay đổi hash của khối trước A. Hệ thống lại phát hiện ra sai lệch ở khối A-1. Hacker phải tiếp tục thay đổi hash của khối A-2.
- Như vậy để thay đổi được giao dịch thì hacker phải thay đổi tất cả các khối vì cơ chế đồng thuận.



Hình 1.11: Hacker phải thay đổi tất cả các khối nếu muốn tấn công hệ thống Blockchain.

5 Các ứng dụng thực tiễn của Blockchain.

Với các đặc tính kể trên, hiện nay chúng ta có thể ứng dụng Blockchain vào nhiều lĩnh vực khác nhau như:

5.1 Ứng dụng trong sản xuất

Khi ứng dụng Blockchain vào sản xuất, Blockchain sẽ thay thế các thiết bị thông minh để cấp quyền quản lý hiệu quả, bao gồm: dõi quá trình tạo ra sản phẩm, quản lý thông tin giao dịch, chất lượng sản phẩm, vận chuyển và phân phối nó tới tay người dùng cuối,... nhằm gia tăng đáng kể năng suất cho các quy trình quản lý chuỗi công ứng.

Đối với người tiêu dùng, họ có thể truy xuất ngược trở lại về lịch sử hình thành, vận chuyển của sản phẩm, để kiểm tra thông tin sản phẩm đó có phải hàng chính hãng hay không, từ đó tránh được những sản phẩm nhái, hàng giả trên thị trường.

5.2 Ứng dụng Blockchain trong thương mại điện tử

Các vấn đề lớn nhất trong lĩnh vực thương mại điện tử là tính bảo mật, quản lý chuỗi cung ứng và quá trình vận chuyển hàng hoá đến người tiêu dùng, tạo nên nhiều rào cản giữa người tiêu dùng và nhà sản xuất.

Tuy nhiên, Blockchain đã giúp giải quyết vấn đề đó bằng các hợp đồng thông minh (smart contract), tạo điều kiện cho các bên ký kết dễ dàng, tiết kiệm được chi phí nhờ lược bỏ được trung gian khi liên kết với các doanh nghiệp đa quốc gia.



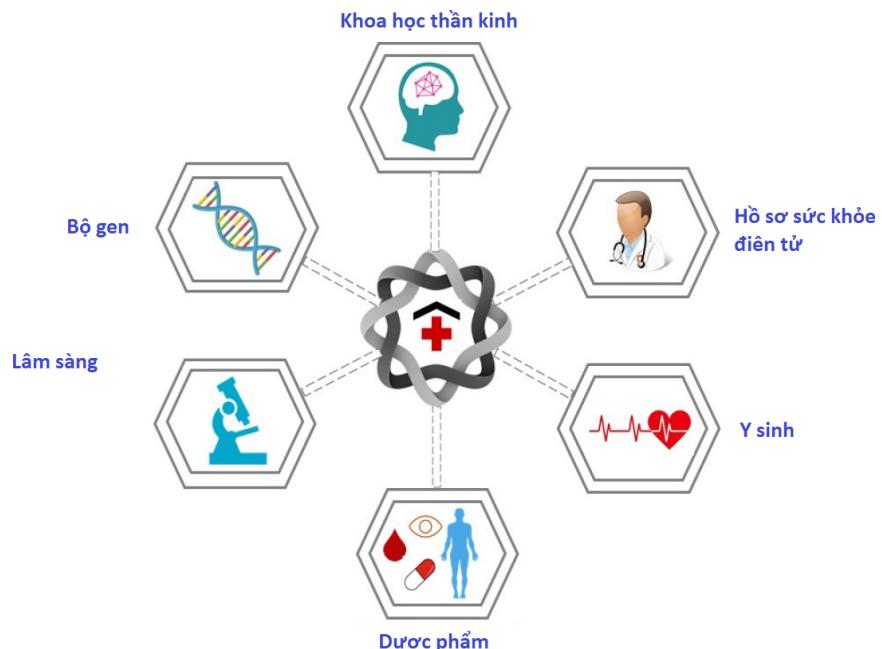
Hình 1.12: Ứng dụng Blockchain vào ngành thương mại điện tử

5.3 Ứng dụng của Blockchain trong y tế

Y tế là một lĩnh vực khá nhạy cảm với các số liệu, khi mà số liệu luôn có khoảng dao động được kiểm soát một cách chặt chẽ.

Khi ứng dụng Blockchain trong y tế, tất cả các bên được ủy quyền đều có thể truy cập cùng một thông tin chính xác và được xác minh trong vài giây.

Bệnh nhân có quyền kiểm soát dữ liệu của họ mọi lúc và có thể cấp cho người khác quyền truy cập theo yêu cầu, giảm nguy cơ bị lạm dụng và trộm cắp.



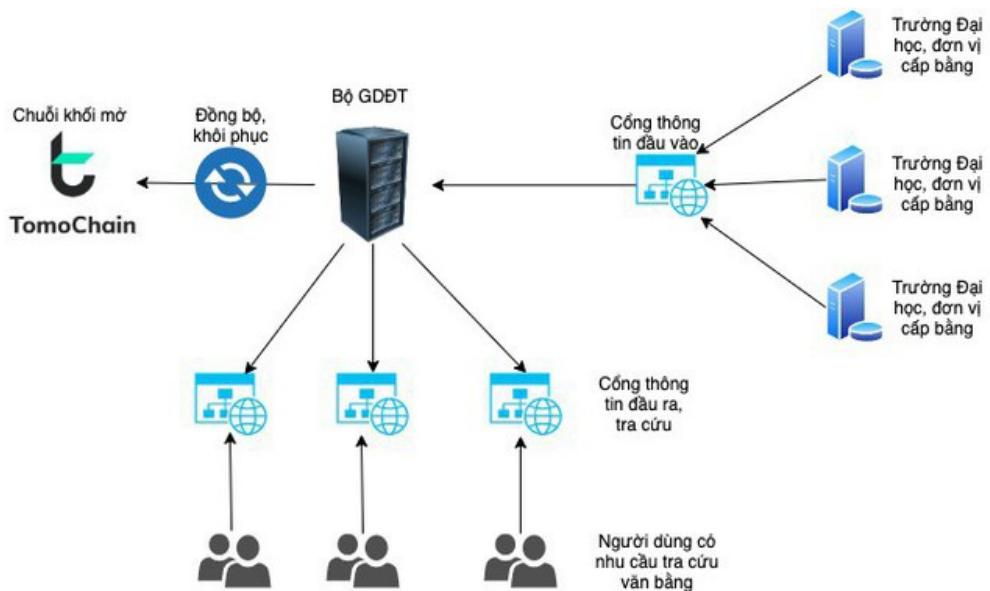
Hình 1.13: Ứng dụng Blockchain vào ngành y tế

5.4 Ứng dụng của Blockchain trong giáo dục

Ứng dụng Blockchain trong giáo dục giúp lưu trữ các dữ liệu về bảng điểm, quá trình đào tạo, kinh nghiệm giảng dạy & lịch sử của từng cá nhân, từ đó sẽ tránh được việc gian lận khi xin cấp học bổng, thăng chức, hoặc khai gian về trình độ học vấn hay kinh nghiệm làm việc.

Ngoài ra, với tính chất của hợp đồng thông minh, Blockchain còn cho phép tự động thực thi các điều khoản trong quy chế đào tạo và xử lý các trường hợp vi phạm,...

Từ 30/06/2021, Bộ Giáo dục và Đào tạo đã chính thức vận hành Hệ thống Tra cứu thông tin văn bằng chứng chỉ trên Blockchain. Đây được xem là cột mốc đánh dấu cho sự công nhận của nhà nước đối với công nghệ Blockchain nói riêng và tiền điện tử nói chung.



Hình 1.14: Ứng dụng Blockchain vào ngành giáo dục

5.5 Ứng dụng Blockchain trong nông nghiệp

Hiện nay, vấn đề về nguồn gốc xuất xứ và chất lượng được đặt lên hàng đầu trong lĩnh vực nông nghiệp. Việc ứng dụng Blockchain trong nông nghiệp với hệ thống sổ cái phân tán sẽ giúp các nhà bán lẻ và người tiêu dùng lưu trữ các thông tin giao dịch, quá trình lưu chuyển của sản phẩm từ nơi sản xuất đến các nhà bán lẻ và người dùng cuối.

Bên cạnh đó, các dữ liệu trong suốt quá trình sản xuất và bán hàng cũng được lưu trữ và cập nhật liên tục trong Blockchain như quản lý chất lượng, quản lý tài

chính, quản lý giá cả,... Điều này giúp tăng tính minh bạch của sản phẩm và tạo được lòng tin của người tiêu dùng



Hình 1.15: *Ứng dụng Blockchain vào ngành nông nghiệp*



CHƯƠNG 2

Giới thiệu về tiền mã hóa



1 Tiền mã hóa (Cryptocurrency) là gì

Tiền mã hóa (hay tiền ảo), là dạng tiền điện tử do các dự án trên Blockchain ban hành, được sử dụng như một phương tiện giao dịch trên các Blockchain như: thưởng cho các thợ đào (miner - người xác thực các giao dịch), mua vốn đầu tư dự án,... Tiền mã hóa sử dụng thuật toán mã hóa để đảm bảo mật thông tin giao dịch dưới dạng kỹ thuật số và kiểm soát việc tạo ra các đơn vị mới thông qua công nghệ Blockchain.

Bởi vì tiền mã chỉ có ở dạng mã hóa chứ không tồn tại ở hình dạng vật lý. Do đó, tiền mã hóa chỉ có thể sử dụng trên Internet trong một cộng đồng ảo cụ thể. Những người tham gia cộng đồng ảo đó có thể sử dụng tiền điện tử để giao dịch, trao đổi, thanh toán hoặc lưu trữ.



Hình 2.1: Ảnh minh họa tiền mã hóa

2 Phân biệt tiền điện tử & tiền mã hóa

2.1 Tiền điện tử

Theo định nghĩa chính xác thì tiền điện tử là tiền kỹ thuật số, tức là tiền ban hành dưới dạng số hóa và sử dụng thông qua Internet, có thể là đại diện cho tiền pháp định dưới sự bảo đảm của chính phủ như tiền nằm trong Internet Banking, hay các ví điện tử như Momo, Moca,...

Tiền điện tử được hình thành khi chúng ta đưa một lượng tiền mặt vào ngân hàng, sau đó ngân hàng sẽ nhập số tiền này vào tài khoản người dùng, từ đó chúng ta có thể giao dịch chỉ bằng việc nhập số.

Có thể nói, tiền điện tử khác tiền mặt ở chỗ, nó là những con số chỉ tài sản của mình, được những nơi uy tín đảm bảo rằng chuyển nó đi nơi khác, sẽ được đối phương chấp nhận giao dịch.

2.2 Tiền mã hóa

Tiền mã hóa thực chất cũng là một dạng tiền điện tử, tuy nhiên thay vì được phát hành hay bảo đảm bởi bất kỳ Chính phủ hay cơ quan quản lý tiền tệ ở bất kỳ quốc gia nào, tiền mã hóa được ban hành bởi những người tạo ra dự án trên Blockchain.

Đôi khi, những người này có thể ẩn danh, viết vài dòng code là tạo ra được rất nhiều tiền mã hóa. Nhưng giá trị của tiền mã hóa chỉ được cộng đồng chấp nhận khi được dùng rộng rãi, chứ không được ngân hàng hay bất cứ tổ chức uy tín nào đảm bảo rằng việc chúng ta giữ những đồng này có thể đổi lại được tiền pháp định.

Vấn đề này tạo ra những Memecoin, hay những scam coin, làm nhiều người mất tiền vì không thể bán lại cho ai. Từ đó tạo ra rất nhiều tiếng xấu cho tiền mã hóa.

→ Vậy tóm lại, tiền mã hóa có thể xem như một phần nhỏ của tiền điện tử.

3 Các loại tiền mã hóa phổ biến hiện nay

Để có cái nhìn tổng quan nhất cũng như nắm rõ tài sản mình dự định đầu tư hay đang nắm giữ thuộc loại nào, sau đây chúng ta sẽ tìm hiểu từng loại tiền mã hóa đang lưu hành trên thị trường cryptocurrency, để hiểu những tiềm năng của như rủi ro của nó.

Hiện trên thị trường có 2 cách để phân loại cryptocurrency:

- Coin và Token.
- Bitcoin và Altcoin.

3.1 Coin và Token trong Cryptocurrency

3.1.1 Coin là gì

Coin là loại tiền được ban hành, phát triển trên một Blockchain riêng biệt và hoạt động độc lập. Coin ra đời với mục đích giải quyết các vấn đề thanh toán, tài chính, bảo mật, phát triển ứng dụng,... của chính Blockchain đó. Mỗi Blockchain chỉ có 1 coin duy nhất. Ví dụ:

- Bitcoin Network có đồng coin là BTC.
- Ethereum có đồng coin là Ether.

3.1.2 Token là gì

Tương tự Coin, Token cũng là một đồng tiền được phát hành trên Blockchain, nhưng nó không có Blockchain riêng, mà phải “sống” trên Blockchain khác. Ví dụ:

- KONO (token của Konomi) là token vì được lưu trữ, giao dịch trên Blockchain Ethereum;

- MER (token của Mercurial) là token vì được lưu trữ, giao dịch trên Blockchain Solana.
- Cả hai đều không có Blockchain Konomi hay Mercurial.

Một số token khi dự án phát triển đủ mạnh sẽ hướng đến phát triển một nền tảng Blockchain riêng cho chính token đó, và khi ấy Token này sẽ được xem như là Coin.

3.1.3 Sự khác nhau giữa coin và token

Về mặt tính năng

- Coin được xem như một phương tiện trao đổi và lưu trữ giá trị cho các mục đích thanh toán, đầu tư và phát triển của một dự án Blockchain cụ thể, chính vì vậy mỗi Blockchain chỉ có một loại coin nền tảng duy nhất.
- Token sở hữu đủ các tính năng của một đồng coin thường được các dự án xây dựng trên Blockchain nền tảng ban hành, đồng thời có thêm nhiều tiện ích tùy thuộc vào từng dự án.

Về mặt kỹ thuật:

- Coin yêu cầu một nền tảng ví (Wallet) riêng và khi giao dịch gửi/nhận, phí giao dịch sẽ trừ trực tiếp vào ví của coin đó.
- Token thì không có ví riêng mà nó sử dụng ví của đồng coin nền tảng, và phí giao dịch sẽ trừ vào coin nền tảng (ví dụ như Ethereum).



Hình 2.2: Phân loại Coin & Token trong tiền mã hóa

3.2 Bitcoin và Altcoin trong Cryptocurrency

Theo cách phân loại này, chúng ta sẽ chia cryptocurrency thành 2 loại là: Bitcoin và phần còn lại.

- Bitcoin là đồng tiền điện tử đầu tiên trên thế giới và đặt nền móng cho phát triển của thị trường Crypto.
- Altcoin là từ ghép của Alternative (thay thế) và Coin để tạo thành "Altcoin", dùng để chỉ tất cả các loại coin/token khác ngoài Bitcoin, được xây dựng nhằm mục đích thay thế cho Bitcoin.

Với cách phân loại này, bất kể Coin hay Token nào trừ Bitcoin ra, đều quy về Altcoin.



Hình 2.3: Bitcoin và Altcoin trong tiền mã hóa

4 Ưu nhược điểm của tiền mã hóa

4.1 Ưu điểm của tiền mã hóa

- Đảm bảo tính minh bạch và công bằng: tiền mã hóa cho phép các Trader trao đổi với nhau một cách trực tiếp mà không cần phải có sự tham gia của bên thứ 3.
- Tiện lợi: các nhà giao dịch tiền mã hóa có thể trao đổi và giao dịch ở mọi lúc mọi nơi, chỉ cần sở hữu một thiết bị di động có kết nối ổn định với Internet là được.
- Tiền mã hóa không thể làm giả: vì không tồn tại dưới dạng vật chất và mỗi đồng tiền điện tử tồn tại dưới 1 dãy bit mã hóa duy nhất trên Internet
- Độ bảo mật an toàn cao
- Chi phí giao dịch thấp hơn nhiều lần so với tổng giá trị giao dịch
- Có tiềm năng phát triển thương mại điện tử

4.2 Nhược điểm của tiền mã hóa

- Sử dụng không quá dễ dàng: với những người đã quen sử dụng công nghệ thì vấn đề này không quá khó khăn. Nhưng đối với những ai ít có cơ hội tiếp xúc với công nghệ thì việc tạo ví Bitcoin và quản lý lại khá khó khăn. Không chừng còn bị lừa đảo 1 cách dễ dàng hơn nữa.
- Giá tiền thường biến động lên xuống mà chúng ta rất khó để đoán trước được. Điều này gần giống với sự lên xuống của thị trường chứng khoán.
- Là nơi cho tội phạm hoạt động rửa tiền: có lẽ đây là nhược điểm lớn nhất. Và cũng vì lý do này mà có những quốc gia chưa chấp nhận đồng coin là một loại tiền tệ hợp pháp.
- Tiền mã hóa vẫn chưa được hợp pháp hóa tại một số quốc gia.

5 Tiền mã hóa hoạt động như thế nào?

Tiền mã hóa được hỗ trợ bởi toán học chứ không phải là từ những văn bản của chính phủ hay tổ chức tài chính.

Trong khi, cũng giống như tất cả các loại tiền tệ, chúng vẫn phụ thuộc vào giá trị được mà chúng được công nhận rồi, sự khan hiếm của chúng dựa trên nền tảng toán học và không thể điều chỉnh bởi bất kỳ một tổ chức hay cá nhân nào.

Chúng không bị trói buộc với sự sẵn có của hàng hoá vật chất, chẳng hạn như vàng, cũng không thể được tạo ra một cách nhân tạo bởi các chính phủ hoặc các tổ chức tài chính như đồng đô la.

Tiền điện tử sử dụng một mạng lưới phân phối để cho phép hệ thống giao dịch p2p (peer-to-peer), giao dịch ngang hàng mà không cần đến các bên thứ ba. Để đảm bảo sự an toàn, mật mã sử dụng các thuật toán toán học và một số cái công khai.

Để đảm bảo mọi giao dịch đều hợp pháp, phương trình toán học phức tạp được sử dụng để liên kết mỗi tài khoản với số tiền thực mà chủ tài khoản muốn chi tiêu.

Người sử dụng, thường được gọi là những thợ mỏ, dành các tài nguyên tính toán của họ để giải quyết các phương trình và thường nhận phần thưởng với một lượng nhỏ tiền điện tử.

6 Tính hợp pháp của tiền mã hóa ở Việt Nam

Tại Việt Nam, Bitcoin và các đồng coin khác không bị cấm nhưng cũng không ủng hộ các vấn đề liên quan đến Bitcoin và chính phủ cũng nhiều lần cảnh báo người dân nên cẩn trọng khi giao dịch, đầu tư Bitcoin.

Ngày 27/2/2014, Ngân hàng Nhà nước Việt Nam lần đầu tiên ra thông cáo báo chí về tiền ảo[1]. Nội dung của Thông cáo tập trung vào một số vấn đề cơ bản như sau:

- Thứ nhất, khẳng định Bitcoin là một dạng tiền kỹ thuật số (tiền ảo), không được phát hành bởi Chính phủ hay một tổ chức tài chính, mà được tạo ra và vận hành dựa trên hệ thống các máy tính kết nối mạng internet ngang hàng.
- Thứ hai, khẳng định sự xuất hiện của Bitcoin đã gây ra nhiều tác hại, rủi ro cho người sử dụng như: Có thể trở thành công cụ cho tội phạm như rửa tiền, buôn bán ma túy, trốn thuế, giao dịch, thanh toán tài sản phi pháp; nguy cơ bị tấn công, đánh cắp, thay đổi dữ liệu hoặc bị ngừng giao dịch là rất lớn; hoạt động đầu tư vào Bitcoin ẩn chứa nhiều nguy cơ về bong bóng tài chính, gây thiệt hại cho người đầu tư; giao dịch Bitcoin không bị chi phối và kiểm soát bởi cơ quan quản lý nhà nước nào, do đó, người sở hữu Bitcoin sẽ chịu toàn bộ rủi ro vì không có cơ chế bảo vệ quyền lợi.
- Thứ ba, việc sử dụng Bitcoin (và các loại tiền ảo tương tự khác) làm phương tiện thanh toán không được pháp luật thừa nhận và bảo vệ. Các tổ chức tín dụng không được phép sử dụng Bitcoin (và các loại tiền ảo tương tự khác) như một loại tiền tệ hoặc phương tiện thanh toán khi cung ứng dịch vụ cho khách hàng.
- Thứ tư, việc sở hữu, mua bán, sử dụng bitcoin (và các loại tiền ảo tương tự khác) như một loại tài sản tiềm ẩn rất nhiều rủi ro cho người dân và không được pháp luật bảo vệ.



CHƯƠNG 3

Giới thiệu về Bitcoin và Ethereum



1 Bitcoin là gì?

Bitcoin (BTC) là một loại tiền tệ kỹ thuật số được phát hành dưới dạng phần mềm mã nguồn mở và phát minh bởi Satoshi Nakamoto, đây cũng chính là đồng tiền điện tử đầu tiên trên thế giới, đặt nền móng cho sự phát triển của thị trường Crypto.

Bitcoin sử dụng giao thức ngang hàng (peer-to-peer) cho tất cả các giao dịch, điều này giúp cho Bitcoin loại bỏ bước trung gian trong quá trình thực hiện giao dịch. Nói một cách dễ hiểu, giao dịch Bitcoin 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.



Hình 3.1: Bitcoin là gì?

2 Lịch sử hình thành Bitcoin

Vào năm 2008 cuộc khủng hoảng tài chính thế giới diễn ra do bong bóng bất động sản Mỹ. Kéo theo là Lehman Brothers – ngân hàng đầu tư lớn thứ 4 của Hoa Kỳ tuyên bố phá sản với khoản nợ 619 tỷ USD.

Nền kinh tế Hoa Kỳ và thế giới chao đảo. Hàng loạt các hệ lụy như thất nghiệp, doanh nghiệp phá sản,...

Sự hoài nghi về hệ thống ngân hàng truyền thống dấy lên từ đây. Vào thời điểm ấy, tên miền bitcoin.org được đăng ký vào 18/08/2008.

Ngày 31 tháng 10 năm 2008, Whitepaper của Bitcoin được phát hành bởi Satoshi Nakamoto.

Ngày 3 tháng 1 năm 2009 Genesis Block – khối đầu tiên trên Blockchain của Bitcoin được tạo ra. Lần đầu tiên đồng tiền không chịu sự kiểm soát của chính phủ hay ngân hàng trung ương ra đời.

3 Sự khác biệt giữa Bitcoin với các loại tiền khác

Bitcoin (BTC) là một đồng tiền kỹ thuật số nên nó không có hình dạng. Nó cũng giống tất cả các loại tiền chính thống như USD, Euro, VND... nhưng được mã hóa bằng điện tử. Điều tạo nên sự khác biệt của Bitcoin sẽ nằm ở 4 yếu tố sau:

3.1 Tính phi tập trung

Trong thị trường tài chính tập trung truyền thống (CeFi - Centralized Finance), các loại tiền pháp định như USD, VND, EUR,... sẽ bị kiểm soát bởi các tổ chức như Ngân hàng Trung ương hay chính phủ.

Tuy nhiên Bitcoin thì không như vậy, với tính chất phi tập trung (DeFi) của mình, Bitcoin có thể được truy cập và sử dụng ở bất kỳ đâu, bất kỳ khi nào mà không chịu sự chi phối bởi cá nhân, tổ chức tập trung quyền lực nào cả. Điều này có nghĩa là không một ai có thể kiểm soát được Bitcoin.

3.2 Tính bảo mật và tính không thể làm giả

Bitcoin có độ bảo mật rất cao, xuất hiện và được phân chia hoàn toàn tự động dựa trên các thuật toán. Hack vào hệ thống mạng của Bitcoin dường như là bất khả thi. Nếu muốn làm điều đó, đồng nghĩa với việc cần phải hack vào tất cả các node ở trong mạng lưới của Bitcoin trong cùng 1 thời điểm. Và để làm điều này gần như là không thể!

Đồng thời, Bitcoin không thể được tạo ra thêm mà chỉ có thể được khai thác (hay còn được gọi là đào Bitcoin). Nghe thì khá giống với việc đào vàng, tuy nhiên, điểm khác biệt ở đây là chúng ta sẽ đào Bitcoin thông qua việc giải mã các phương trình toán học cực kỳ phức tạp. Cùng vì vậy mà Bitcoin cũng không thể bị làm giả.

3.3 Phí giao dịch thấp

Nhờ có giao thức ngang hàng (peer-to-peer) loại bỏ bước trung gian như trong quá trình thực hiện giao dịch thông thường mà phí giao dịch với Bitcoin (BTC) cực kỳ thấp, gần như bằng 0.

3.4 Không thể lấy lại tiền khi giao dịch đã xảy ra

Một khi đã thực hiện giao dịch BTC, chúng ta sẽ không thể hoàn tác hay lấy lại tiền vì thông tin lúc này đã được ghi vào Blockchain, sẽ không ai có thể thay đổi hay chỉnh sửa thông tin đó được. Do đó, chúng ta cần phải cân nhắc kỹ khi đầu tư Bitcoin.

4 Cách thức hoạt động của Bitcoin

Tất cả các tính chất ưu việt của Bitcoin được xây dựng nhờ vào hai loại công nghệ mới:

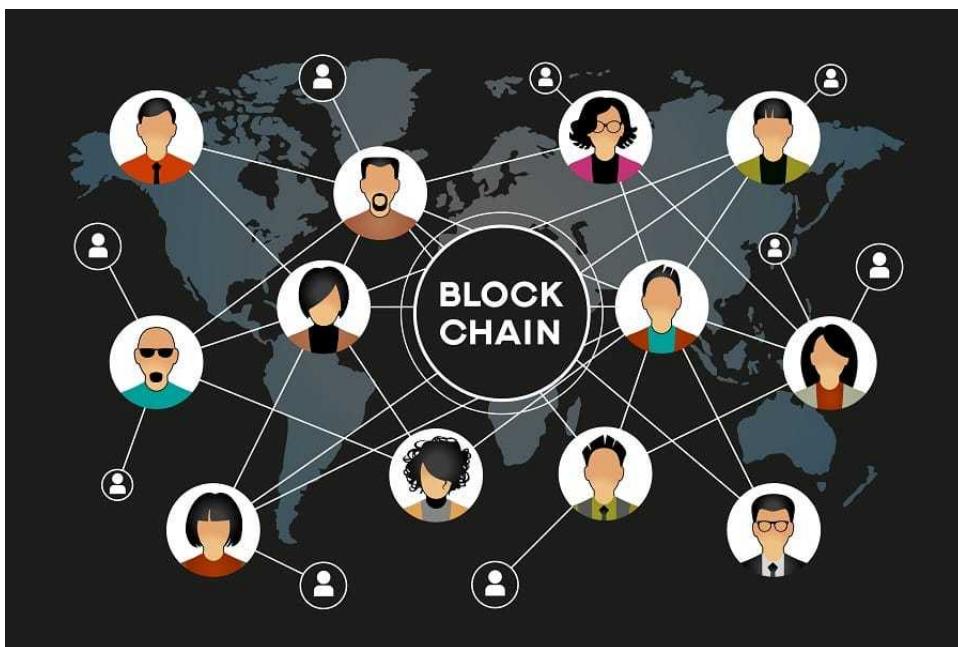
- Công nghệ Blockchain.
- Công nghệ sổ cái phân tán.

4.1 Công nghệ Blockchain

Công nghệ Blockchain được xem là bước đột phá tài chính của tương lai.

Chúng ta có thể hiểu Blockchain là một cuốn sổ cái điện tử được phân phối trên nhiều máy tính khác nhau (tính phi tập trung), lưu trữ mọi thông tin giao dịch và đảm bảo các thông tin đó không thể bị thay đổi dưới bất kỳ hình thức nào (tính minh bạch). Mọi thông tin được lưu trên cuốn sổ cái đó sẽ được xác nhận bởi hàng loạt máy tính được kết nối trong một mạng lưới chung. Sẽ không một cỗ máy nào có khả năng thay đổi, viết đè lên hay xóa dữ liệu trong cuốn sổ cái đó.

Có thể thấy, Blockchain được thiết kế để chống lại sự thay đổi dữ liệu.



Hình 3.2: Người dùng kết nối với nhau trong mạng lưới Blockchain

Chúng ta đã biết rằng, thông tin trong Blockchain không thể bị thay đổi mà chỉ được bổ sung thêm khi có sự đồng thuận của tất cả các nút trong hệ thống. Hệ thống này được bảo toàn ngay cả khi một phần trong hệ thống gặp vấn đề.

Chưa hết, Blockchain có khả năng truyền tải dữ liệu mà không đòi hỏi trung gian để xác nhận thông tin. Thật tiện ích khi một người nhập có thể chia sẻ thông tin cho nhiều đơn vị trong cùng một mạng lưới được xây dựng.

4.2 Công nghệ Sổ cái phân tán (DLT)

Công nghệ sổ cái phân tán (Distributed Ledger Technology - DLT) là một tập hợp các cơ sở dữ liệu mà không được lưu trữ hay xác nhận bởi bất kỳ một bộ máy trung ương nào hết.

Đối với DLT, người tích hợp nó sẽ có quyền kiểm soát lớn hơn đối với cách thức nó được tích hợp. Về nguyên tắc, họ vẫn có thể độc quyết cơ cấu, mục đích và quá trình vận hành mạng lưới sử dụng dịch vụ của họ. Sổ cái phân tán có được xem như là bước đầu tiên để tiến lên Blockchain.

Tuy nhiên, nó không được tạo nên bởi một chuỗi các block mà chiếc sổ cái sẽ được lưu trữ trên nhiều server khác nhau. Tiếp đó sẽ liên lạc lẫn nhau để đảm bảo duy trì dữ liệu giao dịch mới nhất và cập nhật chính xác nhất.

4.3 Ví dụ

Chúng ta có người thân bên Anh. Nếu họ muốn gửi tiền cho chúng ta thì họ sẽ phải ra ngân hàng hoặc chuyển qua thẻ VISA hay thông qua một cổng thanh toán online nào đó.

Nói chung đều phải qua một bên trung gian và mất phí. Phải mất vài giờ thậm chí vài ngày số tiền mới được chuyển đến đích.

Lúc tiền đã qua thì chúng ta phải ra ngân hàng ngồi chờ các thủ tục rút hoặc ra cây ATM rút. Quá trình này tốn nhiều thời gian, công sức và tiền phí.

Hơn nữa, chúng ta và người thân đang chọn hình thức tin tưởng vào ngân hàng.

Điều gì sẽ xảy ra nếu ngân hàng bị tấn công bởi tin tặc? Hoặc có một cá nhân nào đó trong ngân hàng sửa đổi giao dịch của chúng ta?

Nhưng nếu người thân của chúng ta sử dụng Bitcoin thì lại khác. Họ vẫn có thể gửi tiền cho chúng ta mà không phải thông qua một bên trung gian nào cả.

Chỉ cần có kết nối internet, chỉ mất 5 – 10 phút. Họ có thể gửi BTC cho chúng ta từ bất kỳ nơi nào đó trên thế giới.

Và đương nhiên ở Việt Nam chúng ta cũng sẽ nhận được Bitcoin. Phí chuyển tiền gần như = 0 Việc bán nó dễ dàng như vàng hay dollar với tỉ giá hiện tại trên các sàn giao dịch.

5 Giá trị thực của Bitcoin nằm ở đâu?

Những năm gần đây Bitcoin tăng giá trị một cách chóng mặt, BTC đã từng đạt mức giá kỷ lục là \$66.974,77/BTC vào ngày 20/10/2021 vừa qua. Nhưng đây không phải giá trị thực của nó mà chỉ là phản ánh quy luật cung cầu của thị trường mà thôi.

Vậy giá trị thực của Bitcoin nằm ở đâu? Câu trả lời thích hợp nhất chính là ở công nghệ của nó! Chính vì Bitcoin sử dụng giao thức ngang hàng (peer-to-peer) cho tất cả các giao dịch và loại bỏ bước trung gian trong quá trình thực hiện giao dịch. Đây là lý do để Bitcoin tồn tại.

6 Ethereum là gì?

Ethereum là nền tảng điện toán phân tán, mã nguồn mở dựa trên công nghệ Blockchain có khả năng thực thi hợp đồng thông minh (Smart Contract) - tức là điều khoản được ghi trong hợp đồng sẽ được thực thi một cách tự động khi các điều kiện trước đó được thỏa mãn, không ai có thể can thiệp vào. Đồng thời, Ethereum cũng cho phép các nhà phát triển xây dựng các ứng dụng phi tập trung (DApps - Decentralized Application) và các tổ chức tự trị phi tập trung (DAOs - Decentralized Autonomous Organizations). Trong đó:

- Các ứng dụng phi tập trung là các phần mềm được triển khai độc lập, không nằm trên một máy chủ duy nhất mà được lưu trữ một cách phân tán trên các kho lưu trữ phi tập trung và có thể được viết bằng bất kỳ ngôn ngữ nào.
- Các tổ chức tự trị phi tập trung là một tổ chức được vận hành bởi các thành viên dựa trên một bộ quy tắc được mã hóa bằng code. Tất cả các thành viên đều có quyền biểu quyết các quyết định quan trọng của DAOs. Đổi lại, các thành viên tham gia DAOs phải có phần thưởng khi tham gia vận hành DAOs.

7 Cách thức hoạt động của Ethereum

Về cơ bản, Blockchain của Ethereum cũng tương tự như các Blockchain khác, nó được cấu thành bởi mạng lưới các máy tính hay còn gọi là Node.

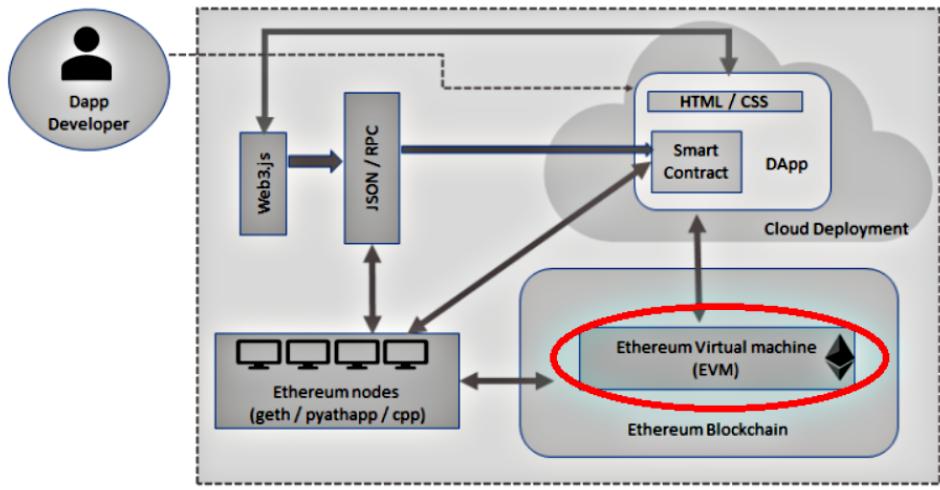
Để tham gia vào mạng lưới, các nodes cần cài đặt phần mềm Ethereum Client như Geth, Parity,....

Khi cài đặt Ethereum Client, đồng nghĩa với việc các nodes sẽ phải chạy một chương trình máy ảo là Ethereum Virtual Machine (EVM). EVM sẽ chịu trách nhiệm thực thi các hợp đồng thông minh.

Khi các nhà phát triển muốn xây dựng ứng dụng phi tập trung trên Ethereum, họ cần phải triển khai các hợp đồng thông minh thông qua ngôn ngữ lập trình Solidity.

Và để kích hoạt việc thực thi các hoạt động như hợp đồng thông minh, lệnh giao dịch... mạng lưới cần đến một lượng phí gọi là "Gas". Phí Gas trong mạng Ethereum sẽ được thanh toán bằng đồng tiền kỹ thuật số gọi là Ether(hay ETH).

Khi giao dịch được thực thi, đây là lúc cần đến việc xác nhận giao dịch đó có hợp lệ hay không. Trong mạng của Ethereum, thành phần đảm nhiệm việc xác nhận giao dịch này có tên - Miner Node.



Hình 3.3: Quy trình vận hành của Ethereum

Để mạng lưới vận hành độc lập, nhất quán các miner nodes phải tuân theo luật đồng thuận là Consensus (hay còn gọi là cơ chế đồng thuận). Ethereum sử dụng cơ chế đồng thuận tên là Proof of Work (PoW - bằng chứng công việc), tức là các miner nodes phải chứng minh được công việc họ đã hoàn thành và thông báo đến toàn mạng lưới. Sau đó, các miner nodes khác trong mạng lưới sẽ xác nhận xem bằng chứng này là có hợp lệ hay không. Công việc ở đây có thể là:

- Tạo ra block mới bằng cách tìm ra lời giải thông qua thuật toán - Ethash.
- Xác nhận giao dịch trên mạng lưới.

8 Ethereum có thể được sử dụng để làm gì?

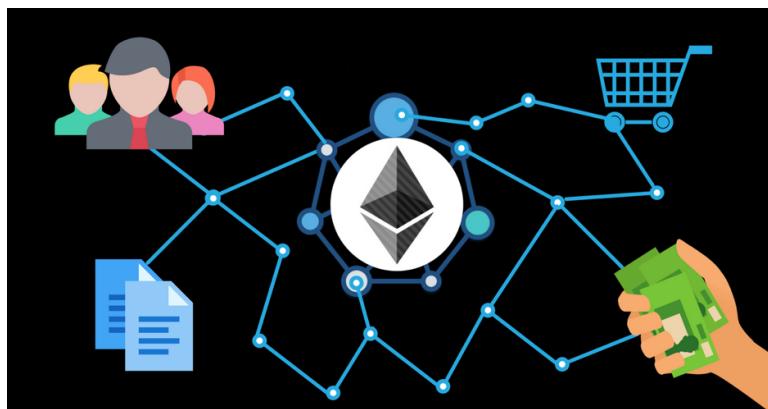
Ethereum cho phép các nhà phát triển xây dựng và triển khai các ứng dụng phi tập trung. Một ứng dụng phi tập trung hoặc Dapp phục vụ một số mục đích cụ thể cho người dùng của nó. Ví dụ, Bitcoin là một Dapp cung cấp cho người dùng một hệ thống tiền mặt điện tử ngang hàng để cho phép thanh toán qua Bitcoin trực tuyến. Bởi vì các ứng dụng phi tập trung được tạo thành từ mã chạy trên một mạng Blockchain, chúng không được kiểm soát bởi bất kỳ cá nhân hoặc thực thể trung tâm nào.

Bất kỳ dịch vụ tập trung nào đều có thể được phân cấp bằng Ethereum. Hãy suy nghĩ về tất cả các dịch vụ trung gian tồn tại trên hàng trăm ngành công nghiệp khác nhau. Từ các dịch vụ hiển nhiên như các khoản vay do ngân hàng cung cấp cho các dịch vụ trung gian hiếm khi được hầu hết mọi người nghĩ như đăng ký bằng sáng chép, hệ thống bỏ phiếu, tuân thủ quy định và nhiều hơn nữa.

Ethereum cũng có thể được sử dụng để xây dựng DAOs. DAOs được điều hành bởi mã lập trình, trên một tập hợp các hợp đồng thông minh được viết trên Blockchain Ethereum. Mã này được thiết kế để thay thế các quy tắc và cấu trúc của một tổ chức truyền thống, loại bỏ sự cần thiết cho mọi người và kiểm soát tập trung.

Ethereum cũng đang được sử dụng như một nền tảng để khởi động các tiền điện tử khác. Do tiêu chuẩn mã hóa ERC20 được định nghĩa bởi Quỹ Ethereum, các nhà phát triển khác có thể phát hành phiên bản riêng của mã thông báo này và gây quỹ với một đồng coin ban đầu (ICO). Trong chiến lược gây quỹ này, những người sáng lập đã thiết lập một số tiền họ muốn, cung cấp nó cho những người tham gia, và nhận được Ether để đổi lấy. Hàng tỷ đô la đã được tăng lên bởi ICO trên nền tảng Ethereum trong hai năm qua, và một trong những tiền điện tử có giá trị nhất trên thế giới, EOS.

Ethereum gần đây đã tạo ra một tiêu chuẩn mới gọi là mã hóa ERC721 để theo dõi các tài sản số độc nhất. Một cơ chế cho phép mọi người chứng minh quyền sở hữu hàng hóa kỹ thuật số. Nhiều trò chơi hiện đang được xây dựng bằng cách sử dụng công nghệ này, chẳng hạn như CryptoKitties , một trò chơi mà chúng ta có thể thu thập và sinh sản mèo kỹ thuật số.



Hình 3.4: Ethereum được sử dụng để phục vụ cho nhiều mục đích khác nhau

9 So sánh Bitcoin và Ethereum



Hình 3.5: Sự khác nhau giữa Bitcoin và Ethereum

Về nguồn gốc, Bitcoin được tạo ra như một loại tiền tệ và để lưu trữ giá trị. Còn Ethereum được tạo ra như một nền tảng giao dịch hợp đồng thông minh phân tán.

Lưu ý rằng Bitcoin cũng có thể xử lý được hợp đồng thông minh, và Ethereum cũng có thể được sử dụng như một loại tiền tệ. Ngoài ra, giữa Bitcoin và Ethereum còn có những điểm khác biệt cơ bản sau:

- Bitcoin có thể sử dụng để thanh toán hàng hóa và dịch vụ tại bất cứ nơi nào đồng tiền này được chấp nhận, còn đồng tiền Ether của mạng lưới Ethereum không được thiết kế như một giải pháp thanh toán thay thế, mà là để thúc đẩy các lập trình viên và các tổ chức sáng tạo và vận hành các ứng dụng phi tập trung trong mạng Ethereum.
- Thời gian tạo khối Ethereum mới là 14 tới 15 giây thay vì 10 phút trong Bitcoin. Và Việc sử dụng giao thức GHOST giúp giao dịch Ether nhanh hơn Bitcoin.
- Số lượng Bitcoin bị giới hạn ở mức 21 triệu với phần thưởng giảm còn một nửa sau mỗi 4 năm. Còn Ethereum thì không giới hạn số lượng ether. Lượng lạm phát ether hàng năm không được xác định rõ. Các ngân hàng trung ương thường thích Ethereum hơn vì cách phát hành tiền này.
- Phí giao dịch của Ethereum được trả bằng Gas (quy đổi được ra ether), được tính dựa trên khối lượng tính toán, băng thông, lưu trữ. Còn phí giao dịch Bitcoin bị cạnh tranh trực tiếp với nhau để vào được khối của Bitcoin mà bị giới hạn.
- Ethereum cho phép chạy mã Turing-complete, cho phép mọi tính toán được thực thi nếu có đủ khả năng tính toán và thời gian. Tuy nhiên điều này cũng mang lại nhiều rủi ro bị tấn công hơn cho Ethereum so với cấu trúc đơn giản hơn của Bitcoin.
- Có 13% số ether được bán cho lượng người đã tài trợ dự án ban đầu. Còn những người đầu tiên đào Bitcoin nắm giữ số lượng lớn lượng Bitcoin đang phát hành.
- Bitcoin đã có một lịch sử chưa bao giờ can thiệp vào dữ liệu trên sổ cái. Còn Ethereum đã phải chia nhánh sau khi DAO bị tấn công.



CHƯƠNG 4

Giới thiệu về hợp đồng thông minh



1 Hợp đồng thông minh là gì?

Bitcoin (Một loại tiền mã hóa dưới dạng phần mềm mã nguồn mở, giúp trao đổi trực tiếp bằng Internet) đã đặt ra nền tảng cơ bản để thiết lập hợp đồng thông minh. Thế nhưng hợp đồng thông minh chỉ thực sự được thỏa mãn mọi yêu cầu và được nhiều người sử dụng khi Ethereum (nền tảng điện toán có tính chất phân tán, công cộng, mã nguồn mở) ra đời.

Hợp đồng thông minh là các chương trình chạy trên Blockchain. Hợp đồng thông minh cũng giống như một hợp đồng kỹ thuật số bị bắt buộc thực hiện bởi một bộ quy tắc cụ thể. Các quy tắc này do bộ mã máy tính xác định trước mà tất cả các nút (node) trong mạng đều phải sao chép và thực thi các quy tắc đó.



Hình 4.1: Hợp đồng thông minh là gì?

Về bản chất, hợp đồng thông minh chỉ là một đoạn mã chạy trên một hệ thống phân tán (Blockchain), cho phép tạo ra các giao thức Permissionless (tức là không cần trao quyền). Điều đó có nghĩa là:

- Hai bên trong hợp đồng có thể đưa ra các cam kết thông qua Blockchain mà không cần phải biết về danh tính hay tin tưởng lẫn nhau.
- Họ có thể đảm bảo rằng nếu các điều kiện của hợp đồng không được thỏa mãn, hợp đồng sẽ không được thực thi.

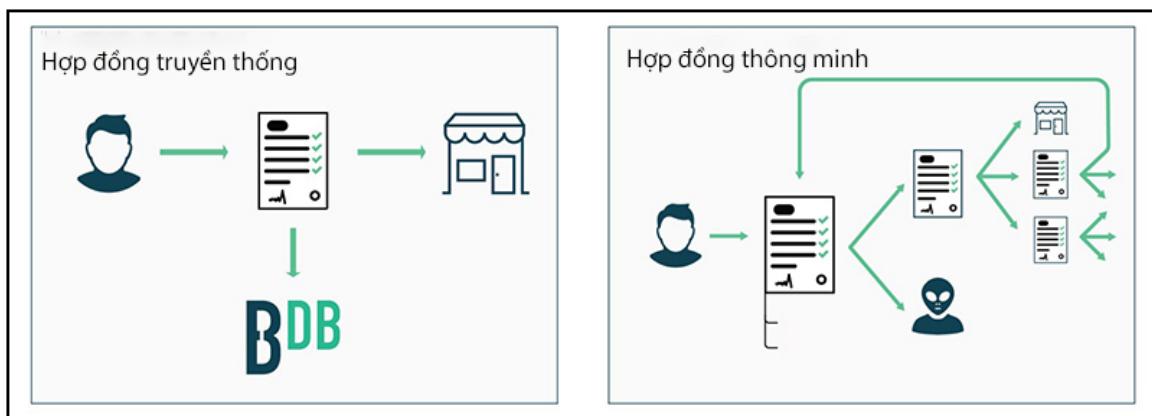
Ngoài ra, việc sử dụng hợp đồng thông minh loại bỏ nhu cầu đối với các bên trung gian, giúp giảm đáng kể chi phí hoạt động. Như vậy, hợp đồng thông minh cũng tương đương như một hợp đồng pháp lý truyền thống nhưng được ghi lại dưới ngôn ngữ máy tính. Hợp đồng thông minh mô tả khả năng tự đưa ra các điều khoản và thực thi thỏa thuận trên cơ sở hệ thống máy tính bằng công nghệ Blockchain.

Mỗi Blockchain có một phương pháp triển khai hợp đồng thông minh khác nhau, ví dụ trên Cosmos có WASM, Polkadot có ink,... Trong đó nổi bật nhất vẫn là hợp đồng thông minh chạy trên máy ảo của Ethereum (Ethereum Virtual Machine - EVM).

2 Khác biệt giữa hợp đồng truyền thống và hợp đồng thông minh

Hợp đồng truyền thống được tạo ra bởi các chuyên gia pháp lý để biên soạn một lượng lớn tài liệu và cần bên thứ ba giúp thực thi. Điều này rất mất thời gian và không minh bạch. Nếu hợp đồng xảy ra sự cố thì phải dựa vào hệ thống tư pháp để giải quyết và điều này rất tốn kém chi phí liên quan.

Đối với hợp đồng thông minh, được tạo ra bởi hệ thống máy tính bằng ngôn ngữ lập trình như C++, Go, Python, Java,... Trong đó nêu rõ các điều khoản và hình phạt tương đương với một hợp đồng truyền thống đưa ra. Chỉ có điều là hợp đồng thông minh không cần sự can thiệp của con người, do đó đảm bảo việc thực thi được chính xác và công minh nhất. Toàn bộ đoạn mã của hợp đồng thông minh này sẽ được thực hiện bởi hệ thống sổ cái phân tán Blockchain.



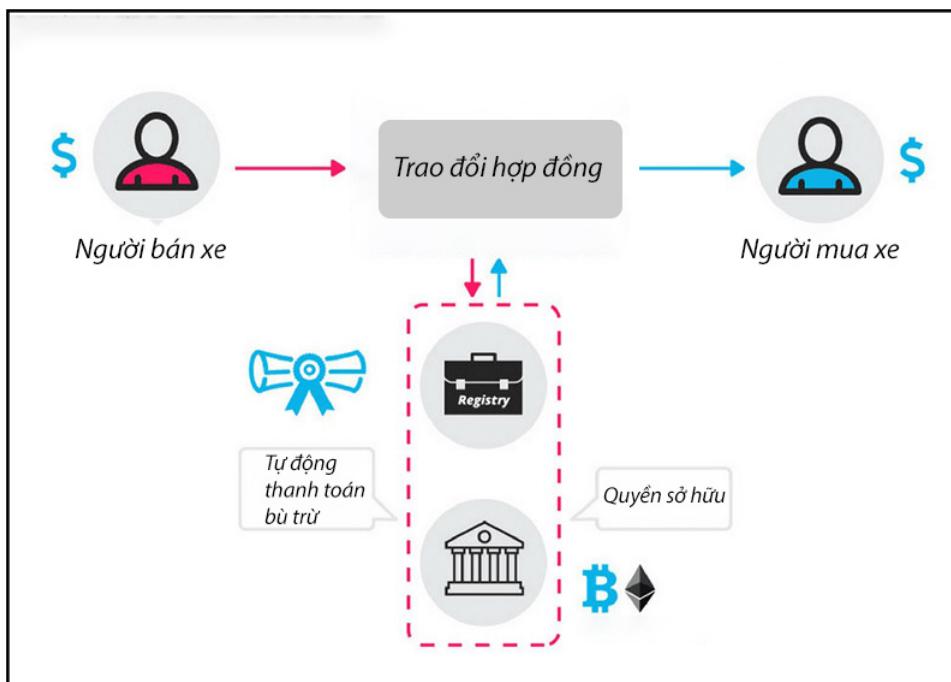
Hình 4.2: Sự khác nhau giữa hợp đồng truyền thống và hợp đồng thông minh

3 Cách thức hoạt động của hợp đồng thông minh

Hợp đồng thông minh là một giao thức đặc biệt nhằm xử lý, xác minh hoặc thực thi các hợp đồng kỹ thuật số. Hợp đồng thông minh có khả năng tự động thực hiện các điều khoản, các thoả thuận giữa các bên trong hợp đồng một cách đáng tin cậy mà không cần bên thứ ba nhờ sự hỗ trợ của công nghệ mật mã học. Các giao dịch này có thể được theo dõi chặt chẽ và không thể đảo ngược được.

Mọi điều khoản trong hợp đồng đều được minh bạch và có thể kiểm tra được, đồng thời đòi hỏi sự đồng thuận của cả hai phía. Một khi đã đồng thuận với hợp đồng, các điều khoản trong nó sẽ được thực thi hoàn toàn tự động hoặc tự động một phần mà không có sự can thiệp từ bên ngoài, hay thông qua một bên thứ ba trung

gian. Và ngay cả hai bên tham gia hợp đồng cũng không thể can thiệp hay sửa đổi lên nó. Các điều khoản trong hợp đồng thông minh tương đương với một hợp đồng có tính pháp lý và được ghi lại dưới dạng các ngôn ngữ lập trình.



Hình 4.3: Cách thức hoạt động của hợp đồng thông minh

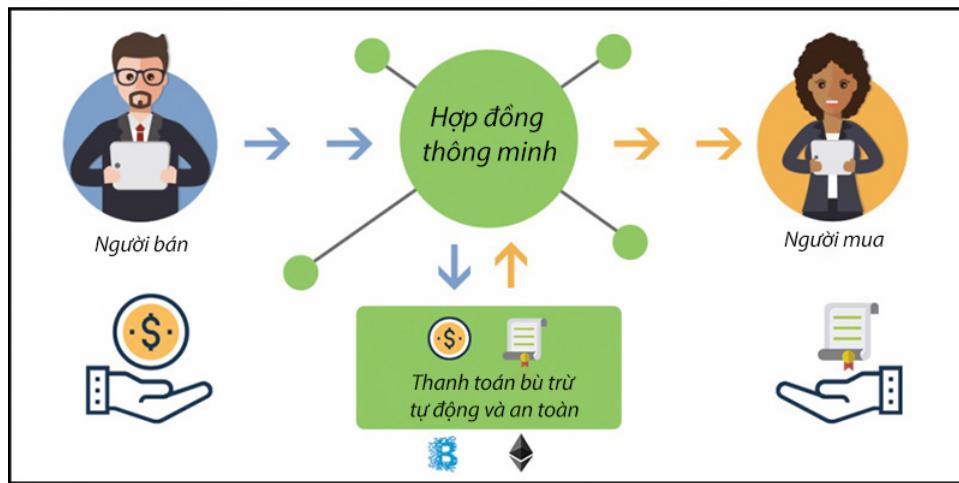
Khái niệm về hợp đồng thông minh được đưa ra đầu tiên bởi nhà mật mã học Nick Szabo vào 1994. Szabo nhận ra rằng có thể giám sát sự thực thi của các hợp đồng thông minh bằng sổ cái phi tập trung, và ông gọi đây là các hợp đồng thông minh hay hợp đồng tự thực hiện, hợp đồng Blockchain hoặc hợp đồng kỹ thuật số. Các hợp đồng có thể được chuyển đổi thành mã máy tính, được lưu trữ và nhân bản trên hệ thống và được giám sát bởi mạng lưới các máy tính ngang hàng mà ngày nay được gọi dưới tên Blockchain. Trong khi các hợp đồng tiêu chuẩn đảm bảo việc thực hiện các điều khoản dựa trên các mối quan hệ luật pháp hoặc sự tin tưởng thì hợp đồng thông minh đảm bảo việc thực thi hợp đồng dựa trên các quan hệ mật mã học và tính tin cậy của mạng lưới các nút trên Blockchain.

Nick Szabo đã nêu ra những nguyên tắc hoạt động chính và định nghĩa về một hợp đồng thông minh, tuy nhiên, tại thời điểm ấy thì các công nghệ và môi trường vẫn chưa đủ hoàn thiện để hiện thực hóa nó. Đây là một phát minh vượt qua thời đại và mãi đến sau này, với sự xuất hiện của công nghệ Blockchain thì nó mới được phát triển và hoàn thiện trong thực tế.

Dạng đơn giản nhất của các hợp đồng thông minh trên Blockchain được đặt nền móng từ Bitcoin. Tuy nhiên, nó vẫn rất đơn giản để có thể thỏa mãn được mọi yêu cầu về hợp đồng thông minh thực sự. Khái niệm hợp đồng thông minh phổ biến ngày nay được xuất phát từ Ethereum với Ethereum hợp đồng thông minh, nó cung cấp một phương thức mới để thiết lập các dạng hợp đồng trên ngôn ngữ Solidity chạy trên máy ảo Ethereum.

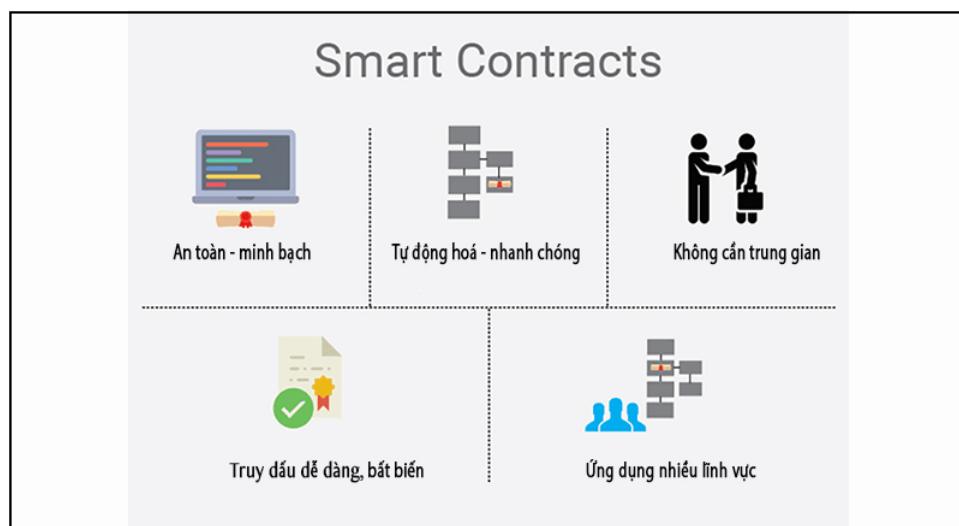
Điểm nổi bật nhất của hợp đồng thông minh là cho phép hai bên tham gia thực hiện hợp đồng từ xa một cách chính xác, an toàn và nhanh chóng; mà không cần các bên biết hoặc tin cậy lẫn nhau từ trước, cũng không cần một bên trung gian thứ ba mà chỉ cần có kết nối Internet.

Ví dụ, nếu chúng ta muốn mua một chiếc xe hơi từ một công ty nào đó và trả tiền điện tử qua Blockchain. Biên nhận sau đó sẽ được đưa vào hợp đồng thông minh của công ty đó và người bán có trách nhiệm giao mật mã và chiếc xe cho chúng ta vào một ngày nhất định đã nêu trong hợp đồng. Nếu mật mã của công ty đó không giao đúng thời hạn thì tiền sẽ được chuyển lại vào tài khoản chúng ta. Nếu đến trước thời hạn thì hệ thống sẽ giữ lại cả tiền của chúng ta và mật mã của công ty đó để chuyển vào đúng ngày.



Hình 4.4: Ví dụ minh họa giao dịch thông qua hợp đồng thông minh

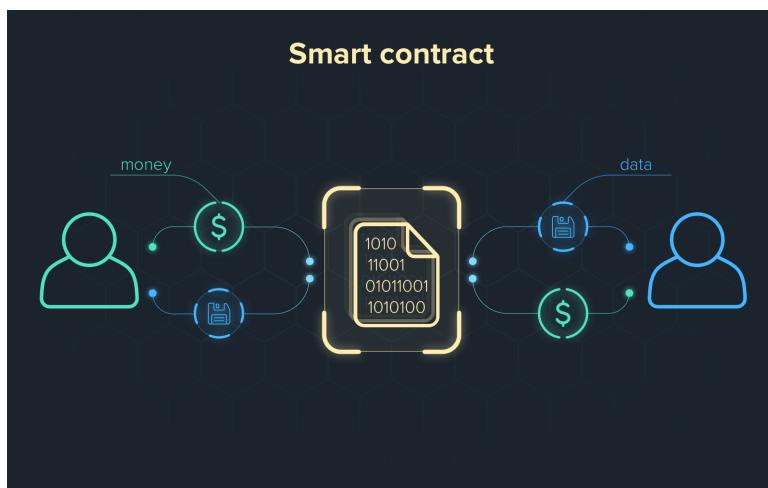
4 Các tính năng chính của Hợp đồng thông minh



Hình 4.5: Tính năng chính của hợp đồng thông minh

Hợp đồng thông minh Ethereum thường trình có các đặc điểm sau:

- **Phân tán:** hợp đồng thông minh được sao chép và phân phối trong tất cả các nút của mạng Ethereum. Đây là một điểm khác biệt so với các giải pháp khác dựa trên các máy chủ tập trung.
- **Tất định:** hợp đồng thông minh chỉ thực hiện các hành động mà chúng được thiết kế để thực hiện trong trường hợp các điều kiện được thỏa mãn. Bên cạnh đó, các kết quả của hợp đồng thông minh không đổi dù người thực hiện là ai.
- **Tự động:** hợp đồng thông minh có thể tự động hóa tất cả các loại tác vụ, nó hoạt động như một chương trình tự thực hiện. Tuy nhiên, trong hầu hết các trường hợp, nếu hợp đồng thông minh không được kích hoạt, nó sẽ duy trì trạng thái "không hoạt động" và sẽ không thực hiện bất kỳ hành động nào.



Hình 4.6: Ảnh minh họa tiền mã hóa

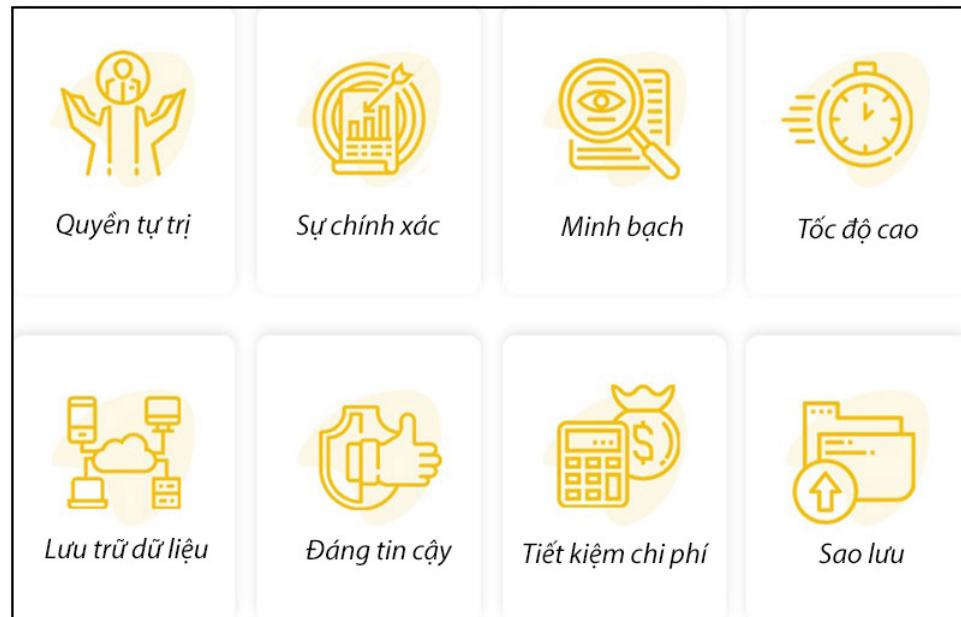
- **Không thể sửa đổi:** không thể sửa đổi hợp đồng thông minh sau khi triển khai. Chỉ có thể "xóa" chúng nếu chức năng này đã được thêm vào từ trước. Do đó, có thể nói rằng hợp đồng thông minh giống như một mã chống giả mạo.
- **Có thể tùy chỉnh:** trước khi triển khai, hợp đồng thông minh có thể được mã hóa theo nhiều cách khác nhau. Vì vậy, chúng có thể được sử dụng để tạo ra nhiều loại ứng dụng phi tập trung (Dapp). Điều này là bởi Ethereum là một Blockchain có thể được sử dụng để giải quyết bất kỳ vấn đề tính toán nào (Turing complete)
- **Không cần dựa trên sự tin cậy:** hai hoặc nhiều bên của hợp đồng có thể tương tác thông qua hợp đồng thông minh mà không cần biết hoặc tin tưởng lẫn nhau. Ngoài ra, công nghệ Blockchain đảm bảo tính chính xác của dữ liệu.
- **Minh bạch:** vì các hợp đồng thông minh dựa trên một Blockchain công khai, không ai có thể thay đổi mã nguồn của chúng, mặc dù bất kỳ ai cũng có thể xem được.

5 Ưu điểm và nhược điểm của hợp đồng thông minh

5.1 Ưu điểm

Hợp đồng thông minh là một bộ mã có thể lập trình, có khả năng tùy chỉnh cao và có thể được thiết kế theo nhiều cách khác nhau để có thể cung cấp nhiều loại dịch vụ và giải pháp.

Ngoài ra, hợp đồng thông minh là các chương trình phi tập trung và tự thực hiện (self-executing), chúng giúp tăng tính minh bạch và giảm chi phí hoạt động. Nếu được triển khai đúng cách, chúng cũng có thể tăng hiệu quả vận hành và giảm chi phí hành chính.



Hình 4.7: Ưu điểm của hợp đồng thông minh

5.2 Nhược điểm

Hợp đồng thông minh chỉ là các đoạn mã chạy trên một Blockchain do con người tạo ra, chúng không thông minh, chúng hoạt động theo cách mà nhà phát triển viết ra chúng, chứ không phải cách mà nhà phát triển nghĩ chúng sẽ hoạt động. Vì vậy Hợp đồng thông minh vẫn có rủi ro vì bộ mã có khả năng bị tấn công và có lỗi.

Ngoài ra, có một số ý kiến cho rằng các hệ thống tập trung cũng có thể cung cấp hầu hết các giải pháp và chức năng mà hợp đồng thông minh mang lại. Tuy nhiên, điều khác biệt là ở chỗ, các hợp đồng thông minh chạy trên một mạng ngang hàng (P2P) phân tán thay vì trên một máy chủ tập trung.

Đồng thời các hợp đồng thông minh dựa trên hệ thống Blockchain nên rất khó hoặc không thể sửa đổi và can thiệp. Tính chất không thể thay đổi là một ưu điểm lớn, tuy nhiên trong một số trường hợp có thể là nhược điểm. Ví dụ:

Khi một tổ chức tự trị phi tập trung (DAO) có tên là "The DAO" bị hack vào năm 2016, hàng triệu ETH đã bị đánh cắp do có sai sót trong mã hợp đồng thông minh của họ.

Vì hợp đồng thông minh của họ là không thể thay đổi, nên các nhà phát triển không thể sửa code. Điều này cuối cùng đã dẫn đến một cuộc phân tách, tạo ra Ethereum Classic và Ethereum.

6 Quy trình tạo một hợp đồng thông minh

Để tạo nên một hợp đồng thông minh, chúng ta cần phải có những yếu tố sau đây:

- **Chủ thể hợp đồng:** hợp đồng thông minh phải được cấp khả năng truy cập đến sản phẩm/dịch vụ liệt kê trong hợp đồng để có thể tự động khóa hay mở khóa chúng.
- **Chữ kí điện tử:** tất cả các bên tham gia vào hợp đồng thông minh đều phải đồng ý triển khai thỏa thuận bằng các khóa cá nhân (chữ kí điện tử) của họ.
- **Điều khoản hợp đồng:** điều khoản trong hợp đồng thông minh có dạng là một chuỗi các hoạt động. Và các bên tham gia hợp đồng đều phải ký chấp nhận nó.
- **Nền tảng phân quyền:** hợp đồng thông minh sau khi hoàn tất sẽ được tải lên Blockchain của nền tảng phân quyền tương ứng và được phân phối về cho các node của nền tảng ấy.

7 Các ứng dụng dựa trên hợp đồng thông minh

Smart Contract thích hợp để ứng dụng trong nhiều lĩnh vực của đời sống. Từ các hoạt động kinh doanh cho đến đến những lĩnh vực đặc thù như y tế, giám sát bầu cử, tham gia vào chuỗi Logistics,..

7.1 Ứng dụng cho các hoạt động quản lý

Blockchain giống như một cuốn sổ cái kỹ thuật số có khả năng lưu trữ mọi thông tin một cách tự động, minh bạch. Dữ liệu một khi đã lưu lại vào cuốn sổ cái này sẽ không thể điều chỉnh, thay đổi bởi một cá nhân hay tổ chức nào cả. Hợp đồng thông minh lưu trữ trên Blockchain đặc biệt cần thiết cho khâu quản lý.

Ngay từ năm 2015, Trust & Clearing đã bắt đầu ứng dụng Smart Contract và Blockchain vào quy trình quản lý tài sản. Theo đó, họ sử dụng công nghệ Blockchain vào việc quản lý một hệ thống thông tin chứng khoán khổng lồ với giá trị lên đến cả ngàn tỷ USD, khoảng 345 triệu giao dịch đã được lưu vào Blockchain.

7.2 Ứng dụng vào công tác bầu cử

Nếu như giám sát, thống kê kết quả bầu cử theo cách truyền thống rất khó để đảm bảo tính không bằng. Quy trình này dễ bị can thiệp, kết quả có thể bị thao túng theo ý đồ của một bên nào đó. Để khắc phục điều này, người ta đã bắt đầu ứng dụng hợp đồng thông minh vào các cuộc bầu cử.

Kết quả sẽ gần như không thể bị thao túng. Bởi mọi phiếu bầu nhiều sẽ trải qua quá trình biến hóa và lưu lại trên sổ cái Blockchain. Một vài đối tượng hay một nhóm tổ chức nào đó nếu muốn thay đổi kết quả là điều rất khó, đòi hỏi họ phải thay đổi hoàn toàn hệ thống. Và trong thực tế điều này không dễ để thực hiện.

7.3 Ứng dụng trong chuỗi cung ứng Logistics

Chuỗi Logistics giống như một hệ thống phức tạp với nhiều bên tham gia. Mỗi bên tham gia lúc này lại đảm nhiệm một công việc riêng. Quy trình vận hành một chuỗi Logistics cần phải được thực hiện tuần tự. Nhìn chung, đây là một quy trình tốn thời gian và tiền bạc. Khi phát sinh một vấn đề nào đó, rất khó để người ta có thể xử lý ngay.

Tuy nhiên, khi ứng dụng hợp đồng thông minh mọi bên tham gia đều có quyền theo dõi tiến trình theo cách đơn giản nhất. Trong quá trình thực hiện hợp đồng sẽ không xuất hiện gian lận. Việc quản lý dữ liệu luân chuyển hàng hóa được diễn ra nhanh gọn, dễ dàng tra cứu.

7.4 Ứng dụng vào lĩnh vực y tế

Hợp đồng thông minh cho phép quản lý và lưu trữ hồ sơ bệnh lý của bệnh nhân trên sổ cái Blockchain. Muốn muôn theo dõi những thông tin này đòi hỏi các bên phải có quyền truy cập.



Hình 4.8: Ảnh minh họa tiền mã hóa

Bên cạnh đó, dữ liệu sẽ tiếp tục chuyển đến bên bảo hiểm. Nếu muốn sử dụng dữ liệu này, các bên phải nhận được sự đồng ý của bệnh nhân. Trong một số trường hợp, người ta còn phải trả phí để sử dụng dữ liệu bệnh lý của bệnh nhân.



CHƯƠNG 5

Xây dựng ứng dụng giao dịch ảo bằng Blockchain



1 Giới thiệu về ứng dụng

Trong bài viết này chúng ta sẽ cùng tìm hiểu về các bước cơ bản để xây dựng một Blockchain như cách tạo, lưu trữ, đồng bộ hóa, hiển thị, và xác thực các giao dịch trước khi cập nhật các thông tin này lên Blockchain.

Ở cấp độ cao, Blockchain là cơ sở dữ liệu nơi mọi người tham gia vào Blockchain đều có thể lưu trữ, xem, xác nhận và không bao giờ xóa dữ liệu.

Ở cấp độ thấp hơn một chút, dữ liệu trong các blocks này có thể là bất kỳ thứ gì miễn là Blockchain cụ thể đó cho phép.

Ví dụ: dữ liệu trong Bitcoin Blockchain chỉ là các giao dịch Bitcoin giữa các tài khoản. Ethereum Blockchain cho phép các giao dịch tương tự của Ether, nhưng cũng có các giao dịch được sử dụng để chạy code.

Thông thường hơn một chút, trước khi một block được tạo và liên kết vào Blockchain, nó được xác nhận bởi phần lớn những người làm việc trên Blockchain, được gọi là các nodes. Blockchain thực sự là chuỗi chứa số lượng blocks lớn nhất được xác minh chính xác bởi phần lớn các nodes. Điều đó có nghĩa là nếu một node cố gắng thay đổi dữ liệu trong block trước đó, thì các block mới hơn sẽ không hợp lệ và các nodes sẽ không tin tưởng vào dữ liệu từ block không chính xác.

Lưu ý: chúng ta chỉ xây dựng một hệ thống Blockchain cơ bản, mô phỏng một phần các tác vụ ở mức khái niệm, giúp cho người đọc hiểu rõ hơn về cơ chế hoạt động của công nghệ Blockchain như: xác thực giao dịch, dữ liệu khi được add vào block và đưa lên Blockchain sẽ không thể thay thế. Chứ chúng ta không xây dựng một hệ thống Blockchain hoàn thiện như Bitcoin hay Ethereum.

2 Xây dựng cấu trúc dữ liệu cho ứng dụng

Thuật ngữ data trong Blockchain thường thay thế bằng transaction. Nên ở đây chúng ta thống nhất sử dụng thuật ngữ transaction để chỉ data trong ứng dụng này.

Ngoài ra, chúng ta sẽ sử dụng định dạng JSON để lưu lại các thông tin của các transaction, và các block. Mục đích để việc trích xuất và sử dụng các dữ liệu này được đơn giản và trực quan nhất.

2.1 Khái quát lập trình JSON trong Python

2.1.1 Đọc dữ liệu JSON

Để có thể làm việc với JSON, chúng ta cần import module json trước khi gọi các hàm để thao tác với json.

Để có thể parse một JSON string, chúng ta gọi method json.loads(). Phương thức này sẽ trả về một đối tượng dictionary chứa dữ liệu được chứa trong JSON string.

Ví dụ:

Chúng ta sẽ khai báo một string có chứa dữ liệu JSON, rồi gọi method loads() để xử lý chuỗi này. Phương thức loads() sẽ trả về một đối tượng dictionary chứa toàn bộ dữ liệu json.

Sau đó chúng ta in ra toàn bộ dữ liệu trong dictionary, rồi in ra value của key là 'sender'.

```
1 # Import json module
2 import json
3
4 # Khai bao mot JSON string
5 transaction = {"lenh": "chuyen_tien", "nguo_gui": "Tam", "nhan": "Satoshi", "so_tien": "10"}
6
7 # Doc JSON String, method nay tra ve mot Dictionary
8 mylist = json.loads(transaction)
9
10 # In ra thong tin cua Dictionary
11 print(mylist)
12
13 # In ra mot gia tri trong Dictionary
14 print(mylist['nguo_gui'])
```

Chương trình 5.1: Đọc dữ liệu JSON từ một JSON string

2.1.2 Chuyển đổi định các định dạng khác trong Python sang định dạng JSON

Trong trường hợp chúng ta cần chuyển một Python object sang định dạng JSON để có thể lưu hoặc đọc dữ liệu một cách dễ dàng hơn mà không cần nhiều thao tác xử lý, chúng ta có thể dùng hàm dumps().

Ví dụ:

```
1 transaction = {"lenh": "chuyen_tien", "nguo_gui": "Tam", "nhan": "Satoshi", "so_tien": "10"}
2
3 mylist = json.dumps(transaction)
4
5 print(mylist)
```

Chương trình 5.2: Chuyển đổi một python object sang định dạng JSON

2.2 Thiết lập thông số để tương tác với server Adafruit

Trong Blockchain, trước khi một transaction được thêm vào một Block, nó sẽ được xác thực bởi tất cả các người dùng đang tham gia vào mạng lưới này dựa trên thuật

toán đồng thuật như Proof of Work (POW) hoặc Proof of Stack (POS). Tất cả người tham gia vào mạng lưới Blockchain này đều giữ một bản sao chứa tất cả các chuỗi khối đã được thêm vào trên Blockchain.

Ngoài ra, việc một Block có thể chứa 10, 100 hay thậm chí hàng ngàn transactions là tùy vào kiến trúc mà người sáng lập ra nền tảng Blockchain đó quy định.

Tuy nhiên, chúng ta chỉ xây dựng một hệ thống Blockchain đơn giản ở mức khái niệm nên sẽ đơn giản bớt một số chi tiết so với thực tế. Cụ thể, mỗi block trong hệ thống của chúng ta sẽ chỉ cần 1 transaction và các transaction này chỉ sử dụng cho 2 mục đích là chuyển tiền mã hóa và kiểm tra thông tin tài khoản.

Bên cạnh đó, việc xác thực một transaction có hợp lệ hay không trước khi thêm vào block sẽ chỉ nhằm vào các giao dịch chuyển tiền. Nếu số tiền trong tài khoản người chuyển mà ít hơn tổng số tiền mà họ có thì transaction đó sẽ không được công nhận và vì vậy, nó không được thêm vào block để cập nhật vào Blockchain.

Để hiện thực các quy luật trên, chúng ta sẽ cần tương tác với 2 feeds trên server adafruit.

- Feed thứ nhất dùng để lưu lại các chuỗi block với các transaction đã được xác thực thành công, còn được gọi là Main net.
- Feed thứ hai dùng để xác thực các transactions mà người dùng gửi lên hệ thống trước khi thêm vào các block và cập nhật vào feed thứ nhất.

```
1 ADAFRUIT_IO_KEY = 'aio_wQbm35FrNhPIEYNXpF8LthdYS5d2'
2 ADAFRUIT_IO_USERNAME = 'bnbaotam'
3 Main_net = 'main-net'
4 Transaction_net = 'transactions-net'
5 aio = Client(ADAFRUIT_IO_USERNAME , ADAFRUIT_IO_KEY)
```

Chương trình 5.3: Thiết lập các thông tin cần thiết để tương tác với server Adafruit

2.3 Cấu trúc của một Block

Chúng ta sẽ bắt đầu bằng cách xác định các block, sẽ trông như thế nào. Trong Blockchain, mỗi khối được lưu trữ với một timestamp và một index (tùy chọn) và để giúp đảm bảo tính toàn vẹn trong suốt quá trình Blockchain, mỗi khối sẽ tự xác định hash. Giống bitcoin, mỗi hash của khối sẽ bao gồm: block's index, timestamp, data, và khối hash trước đó và dữ liệu có thể là bất cứ thứ gì chúng ta muốn.

```
1 def new_block(chain , valid_transactions , previous_hash):
2     block = {
3         'index': len(chain) + 1,
4         'timestamp': str(datetime.datetime.now()),
5         'transactions': valid_transactions ,
6         'previous_hash': previous_hash ,
7     }
8
```

```

9     #Them mot block vao feed Main_net
10    data = Data(value=json.dumps(block))
11    aio.create_data(Main_net, data)
12
13    #Cap nhat chuoi khoi bang viec them block vua tao vao
14    chain.append(block)
15    return block

```

Chương trình 5.4: Hàm tạo và cập nhật một block lên Blockchain

Trong đó:

- **index**: vị trí của Block trong chuỗi các Block đã có (được tính từ 1)
- **timestamp**: thời gian tạo ra một block. Chúng ta sử dụng phương thức `datetime.datetime.now()` để trả về thời gian ngay tại lúc gọi phương thức đó.
- **transaction**: thông tin của một giao dịch, được trình bày cụ thể ở phần 2.4
- **previous_hash**: giá trị mã hóa theo chuẩn sha256 của block trước đó, nếu nó là block đầu tiên (genesis block) thì giá trị này có thể là bất kỳ.

Ngoài ra, chúng ta cần thêm một hàm hash để mã hóa các block và thêm dữ liệu mã hóa này vào phần `previous_hash` của các block được thêm vào sau. Giúp tránh việc thay đổi dữ liệu trên Blockchain.

```

1 def hash(block):
2     string_object = json.dumps(block, sort_keys=True)
3     block_string = string_object.encode()
4
5     raw_hash = hashlib.sha256(block_string)
6     hex_hash = raw_hash.hexdigest()
7
8     return hex_hash

```

Chương trình 5.5: Hàm mã hóa một block

2.4 Cấu trúc của một Transaction

Một transaction sẽ chứa các thông tin cần thiết để hệ thống biết và xử lý giao dịch. Do hệ thống của chúng ta chỉ xử lý 2 lệnh là chuyển tiền và kiểm tra số dư nên tùy thuộc từng lệnh mà cấu trúc của các transaction sẽ khác nhau.

```

1     transaction = {
2         'lenh': chuyen_tien,
3         'nguo_gui': nguo_gui,
4         'nguo_nhan': nguo_nhan,
5         'so_tien': so_tien,
6     }

```

Chương trình 5.6: Cấu trúc transaction của lệnh chuyển tiền

```

1     transaction = {
2         'lenh': so_du,
3         'nguo_i_gui': nguo_i_gui
4     }

```

Chương trình 5.7: Cấu trúc transaction của lệnh kiểm tra số dư

Trong đó:

- **lenh**: chứa yêu cầu thực thi của người dùng.
- **nguo_i_gui**: tên người gửi.
- **nguo_i_nhan**: tên người nhận.
- **so_tien**: số coin muốn chuyển.

3 Hiện thực quy trình giao dịch cho ứng dụng

Trong phần này, chúng ta sẽ hiện thực một số hàm bổ trợ để xử lý dữ liệu của các transaction khi người dùng gửi yêu cầu lên hệ thống thông qua server Adafruit.

Nếu giao dịch này được xác thực thì gọi hàm new_block để thêm nó vào chuỗi khối và cập nhật lên Blockchain.

3.1 Hàm chuyển tiền

```

1 def chuyen_tien(transaction):
2     if xac_thuc(transaction["nguo_i_gui"], transaction["so_tien"]):
3         new_block(chain, transaction, hash(chain[-1]))
4     else:
5         print("Transaction {0} khong hop le".format(
transaction))

```

Chương trình 5.8: Hàm chuyển tiền

3.2 Hàm kiểm tra thông tin tài khoản

Trong Blockchain, thông tin số dư của một tài khoản không được lưu sẵn mà sẽ được tính lại theo các transaction từ block đầu tiên cho đến block mới nhất vừa được thêm vào trên hệ thống.

```

1 def so_du(ten):
2     tai_khoan = 0
3     block_data = aio.data(Main_net)
4     for block in block_data:
5         block_info = json.loads(block.value)
6         trans_info = block_info["transactions"]
7         command = trans_info["lenh"]

```

```

8     if command == "chuyen_tien":
9         nguoi_gui = trans_info["nguoi_gui"]
10        nguoi_nhan = trans_info["nguoi_nhan"]
11        so_tien = trans_info["so_tien"]
12        if ten == nguoi_gui:
13            tai_khoan = tai_khoan - int(so_tien)
14        elif username == receiver:
15            tai_khoan = tai_khoan + int(so_tien)
16    return tai_khoan

```

Chương trình 5.9: Hàm kiểm tra số dư

3.3 Hàm xác thực giao dịch

Chúng ta chỉ cần xác thực cho giao dịch chuyển tiền để kiểm tra xem số tiền mà người gửi yêu cầu chuyển tiền có lớn hơn số dư họ có hay không. Do tính chất của giao dịch kiểm tra số dư không có nhiều vấn đề nên chúng ta không cần phải xác thực giao dịch này.

```

1 def xac_thuc(nguoi_gui, so_tien):
2     if so_du(nguoi_gui) >= int(so_tien):
3         return True
4     else:
5         return False

```

Chương trình 5.10: Hàm xác thực giao dịch

3.4 Hàm gửi dữ liệu

```

1 def gui_transaction(transaction):
2     # Gui transaction len he thong de xac thuc tai feed 'Transaction_net'.
3     net = aio.feeds(Transaction_net)
4     aio.send_data(net.key, transaction)

```

Chương trình 5.11: Hàm gửi dữ liệu

3.5 Xử lý transaction

Bởi vì tùy theo yêu cầu của người dùng mà chúng ta sẽ có các transaction khác nhau cho nên trước khi vào bước xử lý dữ liệu bên trong, chúng ta cần phải xác định trước xem transaction nhận được thuộc loại nào.

Bên cạnh đó, vì chúng ta không cần xác thực giao dịch kiểm tra số dư cho nên các giao dịch này luôn được thêm vào block và cập nhật lên Blockchain sau khi thực hiện.

```

1 def xu_ly_transaction(transaction):
2     if transaction["lenh"] == "chuyen_tien":
3         chuyen_tien(transaction)

```

```

4     elif transaction["lenh"] == "so_du":
5         print("Tai khoan cua {0} la: {1} dong".format(
6             transaction["nguois_gui"], so_du(transaction["nguois_gui"]))
7         )
8         new_block(chain, transaction, hash(chain[-1]))

```

Chương trình 5.12: Kiểm tra yêu cầu của người dùng trước khi xử lý dữ liệu

3.6 Subscribe vào feed để nhận dữ liệu mỗi khi có dữ liệu mới

Để hệ thống của chúng ta tương tác real-time với người dùng thì chúng ta sẽ phải subscribe vào feed mà người dùng gửi các transaction của họ vào. Mục đích là để mỗi khi có một transaction nào vừa được gửi lên hệ thống, chúng ta có thể biết và xử lý transaction đó ngay lập tức.

```

1 def Subscribe():
2     def connected(client):
3         print('Listening for {0} changes...'.format(
4             Transaction_net))
5         client.subscribe(Transaction_net)
6
7     def subscribe(client, userdata, mid, granted_qos):
8         print('Subscribed to {0} with QoS {1}'.format(
9             Transaction_net, granted_qos[0]))
10
11    def disconnected(client):
12        print('Disconnected from Adafruit IO!')
13        sys.exit(1)
14
15    def message(client, Transaction_net, payload):
16        print('Feed {0} vua nhan du lieu moi: {1}'.format(
17            Transaction_net, payload))
18        transaction = json.loads(payload)
19        xu_ly_transaction(transaction)
20
21    client = MQTTClient(ADAFRUIT_IO_USERNAME,
22                         ADAFRUIT_IO_KEY)
23
24    client.on_connect = connected
25    client.on_disconnect = disconnected
26    client.on_message = message
27    client.on_subscribe = subscribe
28
29    client.connect()
30
31    client.loop_blocking()

```

Chương trình 5.13: Subscribe vào feed Transaction_net để nhận dữ liệu realtime và xử lý

4 Chạy thử nghiệm ứng dụng

Do các giao dịch chuyển tiền cần phải được xác thực bằng cách tính toán số dư từ dữ liệu của tất cả các block chứ không phải gán cho nó một giá trị. Cho nên chúng ta cần phải khởi tạo một số transaction đầu tiên để cung cấp tiền cho một số tài khoản để hiện thực các giao dịch sau này (các giao dịch này sẽ không qua khâu xác thực)

```
1 #Khai tao chuoi khoi de luu lai cac khoi duoc them vao
2     Blockchain
3 chain = []
4
5 #Kiem tra neu Blockchain da co du lieu roi thi khong can
6     phai khai tao nua
7 if len(aio.data(Main_net)) == 0:
8     #create the first transaction
9     transaction_1 = {"lenh": "chuyen_tien", "nguo_gui": "Tam",
10         "nguo_nhan": "Satoshi", "so_tien": "10"}
11     new_block(chain, transaction_1, previous_hash="Day la
12         giao dich dau tien duoc tao")
13
14     # second transaction
15     transaction_1 = {"lenh": "chuyen_tien", "nguo_gui": "Tam",
16         "nguo_nhan": "Mike", "so_tien": "10"}
17     new_block(chain, transaction_2, hash(chain[0]))
18 #Neu Blockchain da co du lieu thi cap nhat lai chain
19 else:
20     for blocks in aio.data(Main_net):
21         chain.append(blocks.value)
22
23 #goi lenh Subscribe() de bat dau tuong tac voi nguoi dung
24 Subscribe()
```

Chương trình 5.14: Thiết lập các giá trị đầu tiên cho Blockchain

Chương trình hoàn chỉnh cho ứng dụng giao dịch bằng Blockchain tại:

<https://github.com/Bnbaotam/Xay-dung-mang-Blockchain-tu-dau-bang-Python>



CHƯƠNG 6

Quy trình xây dựng một NFT



1 NFT là gì?

"Non-fungible token" là một tài sản kinh tế mã hóa (crypto economy) kỹ thuật số đại diện cho các sản phẩm và dịch vụ vật lý hay kỹ thuật số. Khái niệm "có thể thay thế" (fungible) có nghĩa tài sản này có thể được tráo đổi để có được một tài sản y hệt hay có giá trị tương đương. Một tờ tiền 10 dollar có thể được thay thế bởi một tờ y hệt hoặc 2 tờ 5 dollar. Không thể thay thế về mặt pháp lý (non-fungible) có nghĩa là một thứ không thể thay thế hay chia nhỏ thành nhiều phần - bởi vì đó là một tài sản được chứng thực là duy nhất.



Hình 6.1: NFT là gì?

Nói theo cách khác, NFT là một loại tài sản kỹ thuật số có chứa thông tin về quyền sở hữu được lưu giữ trên Blockchain. NFT được dùng để xác thực kỹ thuật số các món hàng như tác phẩm nghệ thuật, vật phẩm game,... Phần lớn NFT được lưu giữ trên mạng Blockchain Ethereum hay các mạng Blockchain khác như Flow, Solana, Polygon cũng hỗ trợ loại chứng thực số này.

Nói ngắn gọn, Blockchain là một hệ thống cho phép theo dõi giao dịch gửi và nhận thông tin trên mạng Internet. Nó có chức năng như một sổ cái lưu trữ thông tin dưới dạng các khối dữ liệu (data block) được ghép lại thành một chuỗi (chain). Tài sản số duy nhất đã được lưu trên Blockchain sẽ không thể bị thay đổi, mãi mãi độc nhất và đó là lý do tại sao chúng có thể đắt đến vậy.

2 Quy trình vận hành của NFT

NFT là một dạng chữ ký số được lưu giữ trên Blockchain, công nghệ tương tự cách mà tiền mã hóa (cryptocurrency) hoạt động. Các bằng chứng số (token) đại diện cho tài sản liên kết như tác phẩm nghệ thuật số đóng vai trò xác thực tài sản là duy nhất và là phiên bản gốc. Đó có thể là một file ảnh tĩnh, ảnh động, nhạc hay bất cứ loại tệp tin kỹ thuật số nào.

NFTs ra đời như một phương pháp đăng ký quyền sở hữu đối với một tài sản đặc biệt, bao gồm tranh ảnh nghệ thuật, vật phẩm game... Tài sản số này trở thành một NFT khi nó được đánh dấu trên Blockchain, nhờ đó nó được gán thêm một đoạn hash mã hóa đặc biệt. Khi đó tài sản được coi là đã được tokenized (xác thực số). Nhờ đó, bất kỳ ai cũng có thể xác minh được độ tin cậy của tài sản cũng như quyền sở hữu đối với tài sản đó, khiến cho việc làm giả tài sản đó trở nên bất khả thi.



Hình 6.2: Quy trình vận hành NFT

Một tài sản càng ít phổ biến thì tài sản đó càng có giá trị. Hãy nghĩ tới bức họa "Mona Lisa": chúng ta có thể sao chép ra một poster và dán nó lên tường, nhưng poster này tối đa chỉ có giá trị về cảm xúc đối với chúng ta, trong khi bức tranh gốc vẫn là duy nhất và có giá trị kinh tế vì độ hiếm của nó. NFT cho phép chúng ta xác thực quyền sở hữu bản gốc với một tài sản số ngay cả khi có hàng triệu bản sao khắp nơi trên mạng Internet.

Khi mua NFT, chúng ta đang mua lại chứng thực về quyền sở hữu của một tài sản. NFT thường được ứng dụng trong ngành công nghiệp hàng hóa sưu tầm.

Một ví dụ đặt biệt đó là NBA Top Shot, một nền tảng cho phép trao đổi các hình ảnh, video trong game và điểm nhấn của các trận đấu NBA. Khi mua các tệp dữ liệu này, người mua trở thành chủ sở hữu của các 'khoảnh khắc' ấn tượng nói trên.

Nghe có vẻ điên rồ, nhưng việc sở hữu các khoảnh khắc trong game, hay bản gốc của các ảnh động meme lại có giá trị cảm xúc lớn đối với những người sưu tầm, và chính giá trị này cùng cảm giác 'là người duy nhất' sở hữu một món đồ hiếm là mấu chốt.

3 NFT được phát minh từ bao giờ?

NFT đã có mặt từ những năm 2012 với các loại tiền mã hóa khác dựa trên Bitcoin, nhưng chúng mới chỉ bắt đầu được chú ý tới từ năm 2017 với sự xuất hiện của

CryptoPunk bởi studio game Larva Labs. Đây là một trò chơi sưu tầm với 10.000 ảnh avatar được tạo ra bằng thuật toán. Các ảnh đại diện này có hình dạng người, người ngoài hành tinh, tinh tinh và zombie. Mỗi hình đều đặc biệt và không giống bất kỳ hình nào khác. Nhờ công nghệ NFT, CryptoPunk số 7804 đã được bán với giá 7,5 triệu USD.



Hình 6.3: Các ảnh đại diện trong CryptoPunk

Cùng năm đó, Dapper Labs đã phát hành game CryptoKitties, một trò chơi trong đó người chơi có thể sưu tầm, lai tạo và trao đổi những chú mèo ảo. Hơn 10 nghìn NFT ảnh đại diện khác đã được tạo ra và một trong số đó, một con mèo ảo có tên Dragon đã được bán với giá 1 triệu USD.

Hay gần đây nhất, một cậu bé chỉ mới 12 tuổi tên là Benyamin Ahmed đã phát triển bộ sưu tập NFT và bán được 5 triệu USD.

4 Làm thế nào để tạo và giao dịch NFT?

Tạo ra NFT là một tác vụ khá đơn giản không yêu cầu hiểu biết nâng cao về kinh tế tiền mã hóa hay Blockchain. NFT có thể được tạo ra cho một file ảnh hay bất cứ loại file nào, hay được sử dụng để tạo ra các hàng hóa sưu tầm như thẻ bài...

Trước khi bắt đầu, chúng ta cần lựa chọn xem mạng Blockchain nào chúng ta muốn sử dụng để phát hành NFT. Ethereum là mạng lưới được sử dụng bởi phần lớn các nghệ sĩ khi tạo ra NFT. Tuy nhiên ngày càng có nhiều Blockchains khác trở nên phổ biến cũng có khả năng tạo ra NFT như: Binance Smart Chain, Flow bởi Dapper Labs, Tron, EOS, Polkadot, Tezos, Cosmos, WAX...

Mỗi Blockchain này đều có chuẩn NFT token, ví cũng như các sàn giao dịch riêng. Ví dụ nếu chúng ta tạo ra NFT trên Binance Smart Chain, chúng ta chỉ có thể trao đổi chúng trên các chợ NFT hỗ trợ mạng tài sản Binance Smart Chain (BSC) và



Hình 6.4: Ảnh các chú cá voi trong bộ NFT 5 triệu USD của cậu bé Ahmed.

đồng BNB. Có nghĩa là chúng ta sẽ không thể bán chúng trên các chợ như VIV3 - một nền tảng giao dịch dành cho mạng Flow của Dapper Labs, hay OpenSea vốn dành cho mạng Etherum và Polygon.

Do Etherum là mạng lưới dẫn đầu về nền kinh tế NFT, một số thứ chúng ta cần nếu chúng ta có ý định sử dụng mạng Etherum đó là:

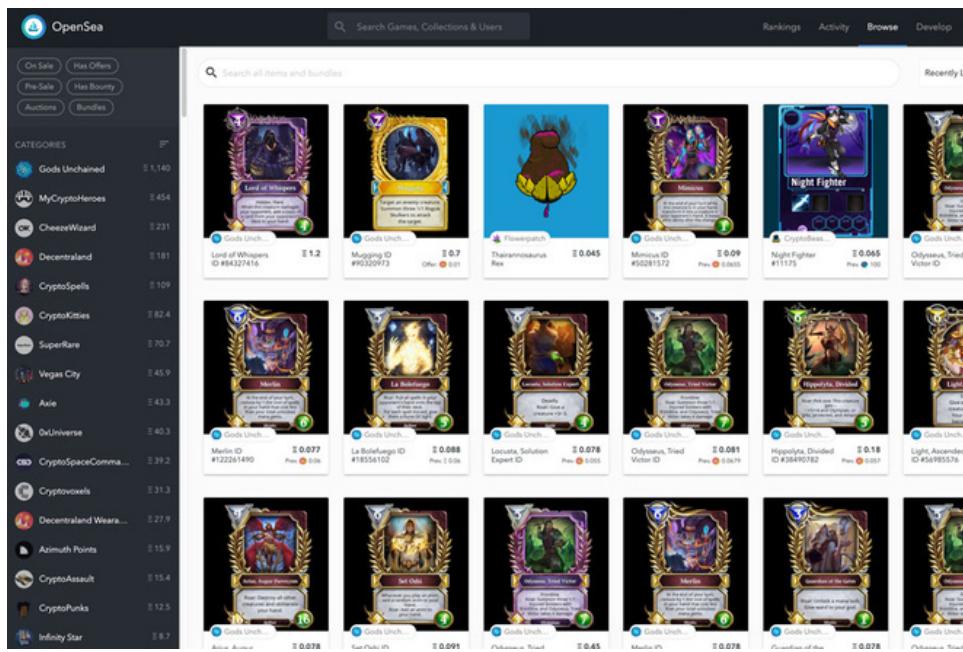
- Ví kỹ thuật số hỗ trợ ERC-721 (chuẩn token NFT Etherum) như MetaMask, Trust Wallet hay Coinbase Wallet. Khoảng 50–100 dưới dạng ETH, đồng tiền của mạng Etherum. chúng ta có thể mua ETH tại các sàn giao dịch tiền mã hóa.
- Sau khi đã sở hữu một chút ETH để giao dịch, có một số các chợ NFT cho phép chúng ta kết nối ví và đăng tải hình ảnh hoặc file chúng ta muốn biến thành NFT.
- Các chợ NFT chính trên mạng Etherum bao gồm: OpenSea, Rarible, Mintable.

Trên OpenSea và các chợ khác, chúng ta có thể đính kèm các thông tin về tính năng đặc biệt vào NFT để tăng độ hiếm và đặc biệt cho NFT của chúng ta. Các nghệ sĩ có thể đính kèm các nội dung đặc biệt chỉ chủ sở hữu có thể xem. Nội dung đính kèm này có thể là bất kì thứ gì, ví dụ mật khẩu để truy cập vào các dịch vụ hay mã coupon, thông tin liên lạc.

4.1 Tạo ra NFT có mất phí?

Mặc dù tạo ra NFT trên OpenSea gần như không mất phí, một số nền tảng khác thì thu phí. Phí này có thể chỉ là một khoản ETH nhỏ để làm phí giao dịch trên mạng Blockchain, trong trường hợp này giao dịch là tạo ra NFT mới.

Phí này thay đổi dựa trên tình trạng của mạng lưới. Càng nhiều người giao dịch thì phí càng cao và ngược lại.

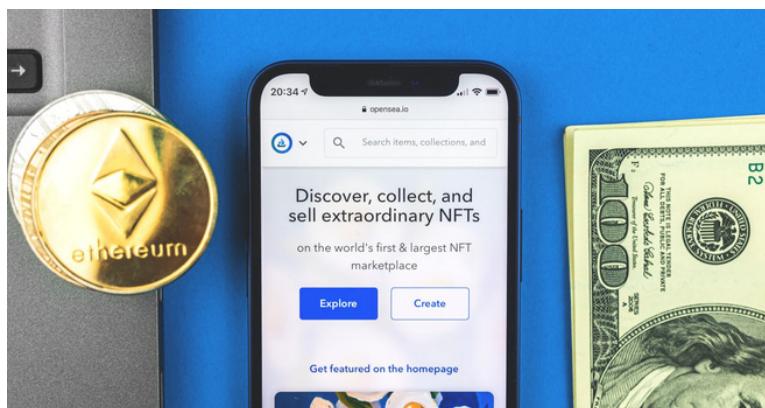


Hình 6.5: Các tác phẩm NFT trên OpenSea

4.2 Làm thế nào để bán NFT?

Để bán NFT trên chợ, chúng ta cần truy cập bộ sưu tập của chúng ta và cài đặt giá bán cho NFT. chúng ta có thể bán theo dạng đấu giá hay giá cố định

Ether và các token ERC-20 là các loại tiền mã hóa phổ biến để sử dụng buôn bán NFT, tuy nhiên, một số nền tảng chỉ hỗ trợ sử dụng token của mạng lưới nội bộ. Ví dụ VIV3 chỉ chấp nhận sử dụng token FLOW của mạng Blockchain Flow.



Hình 6.6: Có thể dùng tiền thật hoặc tiền mã hóa để mua các NFT

Một số chợ NFT khác cho phép chúng ta cài đặt tỉ lệ hoa hồng chúng ta nhận được mỗi khi NFT được bán. Các hợp đồng thông minh cho phép các nghệ sĩ có được hoa hồng mỗi khi tác phẩm được bán lại, tạo ra tiềm năng thu nhập thụ động cho các nghệ sĩ và tác giả.

Một lưu ý là để đăng NFT lên chợ đôi khi sẽ mất phí.

5 Tại sao người ta lại mua NFT?

Câu trả lời còn tùy thuộc vào việc chúng ta có trân trọng độ hiếm của một sản phẩm không. Sở hữu bản gốc bức họa Mona Lisa đối với chúng ta có giá trị hơn có một bản sao treo trên tường hay không? Với một số người thì có.

Giá trị thật sự của NFT nằm ở niềm tin vào khả năng xác thực. Cuốn sổ cái chung dễ dàng truy cập Blockchain khiến cho việc lừa đảo gian lận trong mua bán trở nên bất khả thi. Mọi thay đổi đều được ghi lại trong cơ sở dữ liệu được duy trì bởi hàng ngàn máy tính khắp thế giới và hoàn toàn có thể được truy cập bởi bất kì ai.

Điểm chính ở đây là các sản phẩm kỹ thuật số vẫn luôn dễ sao chép, làm nhái hay bị ăn cắp bản quyền. Phần lớn nhà sáng tạo ít khi kiểm ra tiền từ những thứ họ tạo ra. NFT là một cuộc cách mạng đối với vấn đề này. Tuy việc sao chép một tệp hình ảnh hay video trên máy tính vẫn rất dễ dàng, đoạn mã NFT được gán vào tệp gốc là duy nhất.

Ngày nay những mặt hàng NFT bán chạy nhất được lưu thông trên mạng lưới Ethereum, một trong những hệ thống tiền mã hóa phổ biến nhất trên thế giới.

6 NFT trong thị trường nghệ thuật



Hình 6.7: NFT trong thị trường nghệ thuật

NFT được dùng để bảo vệ quyền sở hữu trí tuệ với các tác phẩm nghệ thuật số. Thông qua NFT và hợp đồng thông minh của Blockchain, các tác giả giờ có thể nhúng thông tin nhân dạng của mình vào các tác phẩm.

Ngoài công dụng tạo ra bằng chứng xác thực và quyền sở hữu với tác phẩm nghệ thuật, NFT cũng có thể cho phép người mua truy cập các thông tin và dịch vụ liên

quan tới sản phẩm một cách dễ dàng.

NFT cũng cho phép trao đổi và lưu hành các tác phẩm số, những sản phẩm trước đây vốn không có giá trị bỗng dưng có giá hàng triệu đô nhờ NFT. Nghệ sĩ có thể dễ dàng bán các tác phẩm của mình dưới dạng một bản duy nhất hay số lượng giới hạn để thu hút nhà sưu tầm hay nhà đầu tư hợp lý.

NFT là giải pháp giúp các nghệ sĩ có được khả năng tài chính linh hoạt đối với các sản phẩm của mình. Một nhóm nhạc có thể bán các tác phẩm bằng cách gán các sản phẩm vào NFT, hay nhận hoa hồng khi sản phẩm được bán mà không cần phải tốn tiền cho các hãng phát hành, công ty đại diện.

Có nhiều cơ hội kinh doanh mở ra: không chỉ giúp ngăn chặn vi phạm quyền sở hữu, cơ chế hoạt động của NFT còn có thể ứng dụng vào nhiều ngành khác.

Không chỉ dành cho thị trường xa xỉ, đối với nhiều công ty, NFT là một lối thử nghiệm mới để kết nối với cảm xúc người tiêu dùng. Hàng snack Pringles đã phát hành những NFT "hương vị ảo" CryptoCrisp giới hạn với chỉ 50 phiên bản được bán với giá 0,0013 Ether.

7 Giao dịch NFT

Giao dịch NFT gây sốt nhất đó là giao dịch bán file ảnh JPEG "Everydays - The First 5000 Days" có chứa 5 ngàn hình ảnh được thu thập hàng ngày trong 5000 ngày từ năm 2007 của nghệ sĩ Beeple (Mike Winkelmann) với giá 69,3 triệu USD.

Giao dịch này được môi giới bởi nhà đấu giá Christie's. Đối thủ cạnh tranh Sotheby's cũng đã nhanh chóng theo chân trong lĩnh vực đấu giá NFT.

Nữ ca sĩ Canada Grimes đã thu về khoảng 6 triệu USD trong một sự kiện bán những tác phẩm nghệ thuật NFT do cô tạo ra.



Hình 6.8: Mua bán các tác phẩm NFT

Nhóm nhạc Kings of Leon là nhóm nhạc đầu tiên đăng ký phát hành album dưới dạng NFT. Bài hát When You See Yourself đã được phát hành giới hạn một số phiên bản NFT đi kèm với các bức ảnh độc quyền cũng như vé vào cửa trọn đời tại các show của nhóm.

Trong một cuộc đấu giá tháng 2 năm 2021, một đôi giày ‘ảo’ được thiết kế bởi Studio RTFKT cùng nghệ sĩ Fewo đã thu về hơn 3 triệu đô chỉ trong 7 phút. 600 đôi giày đã được bán ra và những người mua cũng nhận được một phiên bản vật lý của đôi giày này như quà tặng. Phiên bản số của đôi giày này có thể sử dụng trên các nền tảng như Snapchat hay trên video game.

CEO Twitter Jack Dorsey đã bán NFT tweet đầu tiên của anh với giá 2,9 triệu USD. Số tiền này đã được quyên góp cho tổ chức Africa Response để giúp đẩy lùi đại dịch.

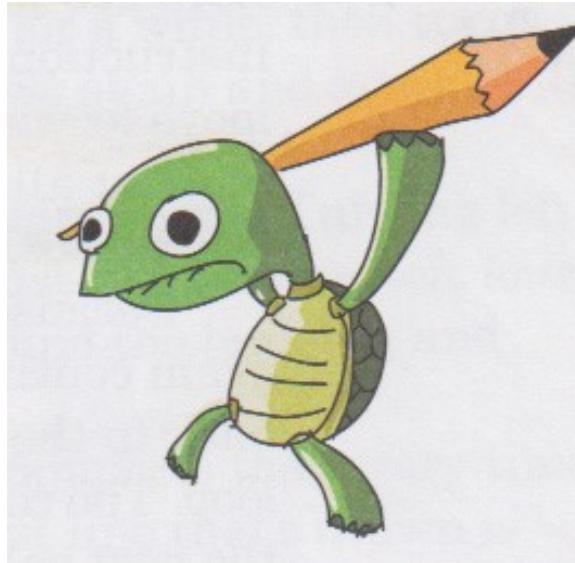
NFT của meme mèo Nyan Cat cũng được bán với giá gần 600.000 USD. Phong trào tài sản hóa meme này đã tạo ra một nền kinh tế có ‘Memecconomy’. Ngay cả các nhà báo cũng bắt sóng thị trường: tháng 3 năm 2021, Kevin Roose, một tác giả của tạp chí NY Times đã bán một bài báo (về NFT!) của anh với giá 563 nghìn USD.

CHƯƠNG 7

Tạo tác phẩm nghệ thuật bằng ngôn ngữ lập trình Python

1 Giới thiệu về thư viện Python Turtle

Thư viện Python turtle à một tính năng của Python giống như một bảng vẽ, cho phép chúng ta ra lệnh cho một con rùa vẽ tất cả trên đó! Chúng ta có thể sử dụng các hàm để có thể di chuyển rùa xung quanh. Turtle còn được gọi là ngôn ngữ Lập trình biểu trưng.



Hình 7.1: Hình ảnh con rùa tưởng tượng, thực ra chỉ là hình một mũi tên mà thôi

2 Các hàm thường được sử dụng để vẽ hình

- **screen()**: hàm này để tạo màn hình hiển thị.
- **turtle()**: hàm này được sử dụng để tạo đối tượng rùa.

- **onscreenclick(tên_hàm, 1)**: hàm này sẽ gửi tọa độ hiện tại đến hàm được sử dụng để tạo thành hình tam giác, 1 là cho nhấp chuột trái và 3 là cho nhấp chuột phải
- **listen()**: hàm này cho phép chương trình lắng nghe các kết nối đến.
- **speed(tốc độ)**: hàm này được sử dụng để tăng hoặc giảm tốc độ của con rùa. Với tốc độ nằm trong khoảng từ 1 đến 10, và giá trị 0 là nhanh nhất.
- **done()**: hàm này được sử dụng để giữ màn hình. Nếu không có hàm này, màn hình kết quả sẽ tự tắt.
- **penup()**: hàm này được tích hợp sẵn trong thư viện turtle để nhắc rùa lên không cho vẽ.
- **pendown()**: hàm này được tích hợp sẵn trong thư viện turtle để đặt rùa xuống để vẽ.
- **forward()**: hàm này được tích hợp sẵn trong thư viện turtle để di chuyển hướng về phía trước của rùa, nó lấy đơn vị pixel làm đối số
- **left()**: hàm này được tích hợp sẵn trong thư viện turtle để xoay rùa sang trái, nó lấy góc theo độ làm đối số.
- **pencolor(" ")**: hàm này để nét vẽ của con rùa có màu. Màu muôn vẽ sẽ được để trong dấu nháy đôi.
- **bgcolor(" ")**: hàm này để thiết lập màu nền. Màu nền cần thay đổi sẽ được để trong dấu nháy đôi.

3 Hướng dẫn sử dụng thư viện Python turtle để vẽ một số hình cơ bản

3.1 Vẽ hình vuông xoắn ốc

```

1 import turtle
2 pen = turtle.Pen()
3 for x in range(100) :
4     pen.forward(x)
5     pen.left(90)
6 turtle.done()

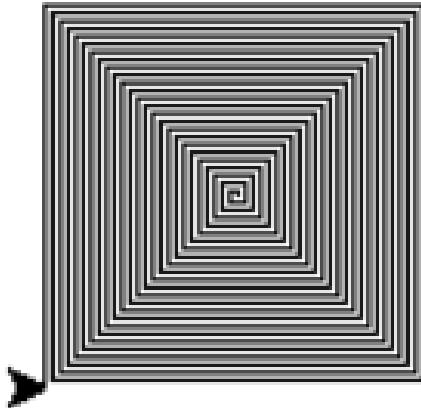
```

Chương trình 7.1: Chương trình vẽ hình vuông xoắn ốc.

Giải thích một số dòng code trong chương trình vẽ hình vuông xoắn ốc:

- `turtle.Pen()` có nghĩa là chúng ta dùng `pen` thay thế cho `turtle.Pen()` vì mỗi khi gọi hàm này của `turtle` thì cái tên ấy quá dài, không gọn. Và mặc định sau khi gọi hàm này xong con rùa đang được đặt xuống để vẽ.

- Ở vòng lặp tại dòng 3: for x in range(100), đầu tiên là lệnh t.forward(x). Lệnh này khiến cái bút của con rùa (cái mũi tên) nhích tới x dots (pixels). Với x=0 (lần đầu tiên) thì cây bút của con rùa vẫn giữ nguyên vị trí. Lệnh kế tiếp t.left(90) bắt “con rùa” quẹo trái 1 góc 90 độ và kết thúc vòng lặp đầu tiên. Các vòng lặp tiếp theo với x=1, rồi 2, 3, ... đến 99 (tức là đủ 100 vòng) thì chúng ta sẽ được kết quả như hình 7.2.



Hình 7.2: Hình vuông xoắn ốc.

3.2 Vẽ xoắn ốc tròn nhiều nét màu và thay đổi màu nền

```

1 import turtle
2 pen = turtle.Pen()
3
4 # tang toc do ve hinh
5 turtle.speed(10)
6
7 # thay doi kich thuong man hinh ve
8 # width la chieu rong, height la chieu cao
9 man_hinh = turtle.Screen()
10 man_hinh.setup(width=650, height=650)
11
12 # thay doi nen sang mau gray (mau xam)
13 turtle.bgcolor("gray")
14
15 # tao list chua cac mau
16 mau = ["red", "yellow", "blue", "green"]
17 for x in range(50,150):
18     # chia mau ra tung phan
19     pen.pencolor(mau[x%4])

```

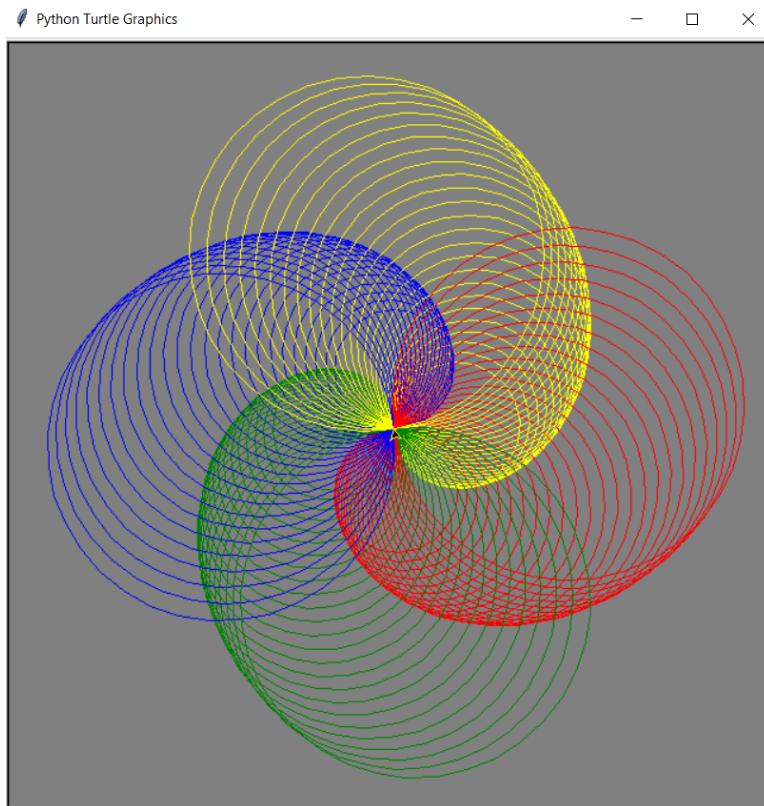
```

20
21 %ham circle() dung de ve hinh tron
22 pen.circle(x)
23 pen.left(91)
24
25 turtle.done()

```

Chương trình 7.2: Chương trình vẽ hình tròn xoắn ốc 4 màu với nền xám.

Kết quả sau khi chạy chương trình trên



Hình 7.3: Các hình tròn xoắn ốc 4 màu trên nền xám

3.3 Vẽ tam giác và tô màu tại vị trí người dùng click chuột vào

Để tô màu cho một hình vẽ, chúng ta sử dụng tổ hợp lệnh sau:

- **fillcolor(" ")**: chọn màu muôn tô. Màu muôn tô sẽ được đặt trong dấu nháy đôi.
- **begin_fill()**: bắt đầu việc tô màu. Được gọi trước khi bắt đầu vẽ.
- **end_fill()**: kết thúc việc tô màu. Được gọi sau khi đã vẽ xong hình.

```

1 import turtle
2 # tao but de ve (chinh la doi tuong rua)
3 pen = turtle.Turtle()
4 # tao ham ve tam giac

```

```

5 def ve_tam_giac(x, y):
6
7     #chon mau muon to
8     pen.fillcolor("cornflowerblue")
9
10    #bat dau to mau
11    pen.begin_fill()
12
13    # nhac but len
14    pen.penup()
15
16    # di chuyen den vi tri x va y tuong ung
17    pen.goto(x, y)
18    # dat but xuong
19    pen.pendown()
20    # dung vong lap for ve 3 canh tam giac
21    for i in range(3):
22        # ve doan thang dai 100
23        pen.forward(100)
24        # xoay trai 120 do
25        pen.left(120)
26        # ve tiep doan thang dai 100
27        pen.forward(100)
28
29    #ket thuc viec to mau
30    pen.end_fill()
31
32 # Khi nhan chuot vao man hinh se goi ham ve_tam_giac de ve
33 # tam giac
34 turtle.onscreenclick(ve_tam_giac, 1)
35
36 # lang nghe xem khi nao nguoi dung click chuot vao man hinh
37 turtle.listen()
38
39 turtle.done()

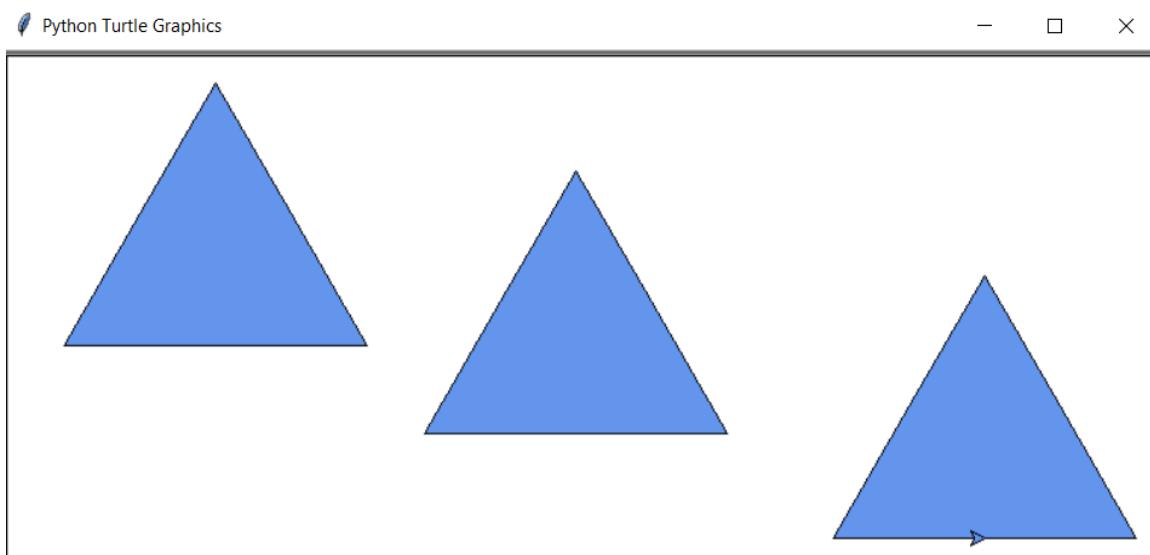
```

Chương trình 7.3: Chương trình vẽ tam giác và tô màu tại vị trí mà người dùng click chuột.

Chương trình hoàn chỉnh để vẽ và tô màu tam giác tại:

<https://github.com/Bnbaotam/Python-Turtle-NFT>

Kết quả sau khi chạy chương trình trên



Hình 7.4: Các hình tam giác sẽ được vẽ tại vị trí mà người dùng click vào.

3.4 Chương trình vẽ Doraemon



Hình 7.5: Doraemon được vẽ bằng Python turtle.

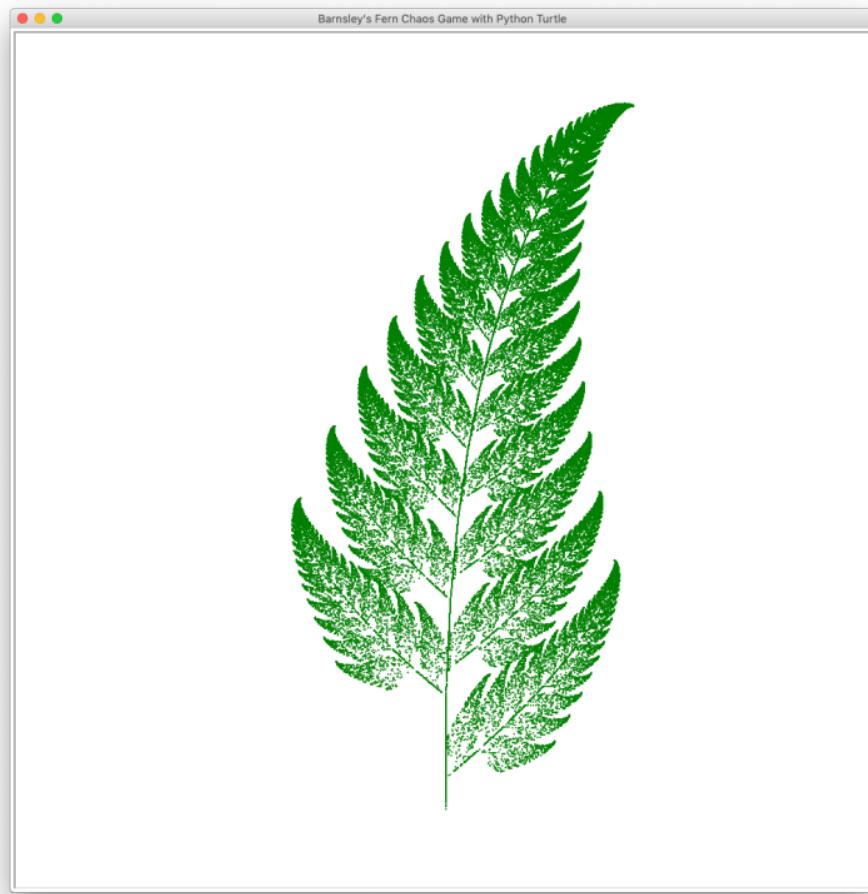
Chương trình hoàn chỉnh để vẽ, tô màu Doraemon và ký tên tại:

<https://github.com/Bnbaotam/Python-Turtle-NFT>

3.5 Một số tác phẩm nghệ thuật khác được vẽ bằng Python turtle

Chúng ta có thể tham khảo một số tác phẩm nghệ thuật được vẽ bằng Python turtle (có kèm source code cho một số tác phẩm) tương tự như hình 7.6 tại:

<https://pythonturtle.academy/>



Hình 7.6: Một chiếc lá được vẽ rất chi tiết bằng Python turtle.

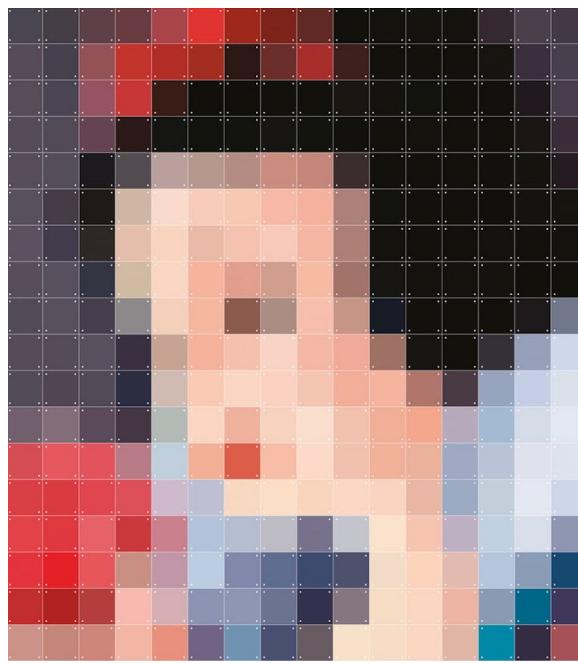
Chương trình hoàn chỉnh để vẽ chiếc lá ở hình 7.6 tại:

<https://github.com/Bnbaotam/Python-Turtle-NFT>

4 Pixel Art

4.1 Pixel là gì

Pixel là viết tắt của từ picture element tức là một điểm vật lý trên bức ảnh, có kích thước vào khoảng $0,26 \times 0,35$ mm. Pixel là đơn vị cơ bản nhất để tạo nên bức ảnh kỹ thuật số, được tạo ra từ máy ảnh, máy quay hoặc các phần mềm chuyên dụng như photoshop.



Hình 7.7: Các điểm pixel khi được phóng to lên trong một bức ảnh.

Trong photoshop, pixel được tạo ra ở dạng hình chữ nhật nhỏ có màu sắc hoặc không màu. Mỗi pixel trên màn hình hiển thị sẽ được máy tính gán cho một màu sắc trong nhóm 4 giá trị màu: red, green, blue và gray. Các pixel được sắp xếp cạnh nhau với cường độ màu giống hoặc khác nhau, tạo nên hình ảnh mà mắt người có thể nhìn thấy được. Bức ảnh càng sắc nét thì càng chứa nhiều pixel trong đó.



Hình 7.8: Sự khác nhau giữa bức ảnh 11 màu và bức ảnh lên đến hàng triệu màu.

4.2 Pixel Art là gì?

Ngày nay, với sự phát triển của công nghệ trong thời đại số, Pixel Art đã trở thành nguồn cảm hứng thiết kế của rất nhiều các người thiết kế, **tạo nên những câu chuyện, hình ảnh bằng những khối vuông**, thổi một luồng gió mới trong giới nghệ

thuật sáng tạo. Pixel Art là một hình thức nghệ thuật kỹ thuật số, được tạo ra thông qua việc sử dụng phần mềm, trong đó hình ảnh được chỉnh sửa ở cấp độ pixel, lấy cảm hứng từ đồ họa 8 bit. Trong hầu hết các sản phẩm thiết kế Pixel Art, bảng màu được sử dụng có kích thước cực kỳ hạn chế, với một số chỉ sử dụng hai màu.



Hình 7.9: Một bức tranh sơn thủy theo phong cách Pixel Art.

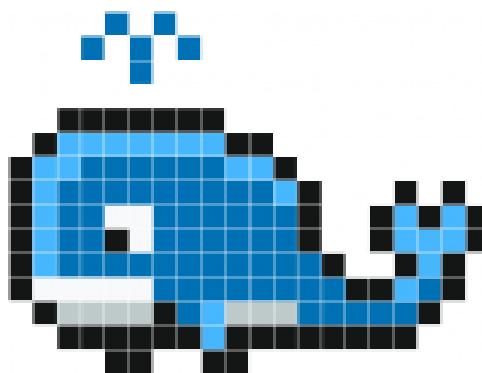
Pixel Art phần lớn bắt nguồn từ các trò chơi video cổ điển, đặc biệt là các game arcade cổ điển như Space Invaders (1978) và Pac-Man (1980) và các máy chơi game 8 bit như Nintendo Entertainment System (1983) và Sega Master System (1985). Pixel Art mang đến sự ngộ nghĩnh, hiện đại pha trộn nét hoài cổ châm phá, tạo nên sự khác biệt cho các sản phẩm thiết kế khi thế giới đang ngày càng chuyển mình chạy theo xu hướng nâng cấp đồ họa mượt mà.



Hình 7.10: Hình ảnh Pixel Art trong một trò chơi

Các ấn phẩm thiết kế Pixel Art có thể được tạo nên từ rất nhiều các phần mềm khác nhau: từ Paintms cho đến photoshop, hay thậm chí vẽ bằng Excel... cũng không rời xa được nguyên lý làm việc với các pixel - tỉ mỉ và chi tiết.

Tuy nhiên, để tạo ra một bộ sưu tập gồm nhiều các tác phẩm tương tự nha, có thể lên đến hàng trăm tác phẩm như hình 8.19. Chúng ta không thể nào vẽ từng bức hình riêng biệt được bởi vì rất tốn thời gian, và bởi vì đặc tính của Pixel Art là làm việc với các pixel một cách tỉ mỉ. Cho nên người vẽ sẽ không thể tránh khỏi việc tác phẩm này có thể khác một phần, hoặc toàn phần so với tác phẩm còn lại.



Hình 7.11: Pixel Art một chú cá voi trong bộ sưu tập NFT trị giá 5 triệu Đôla

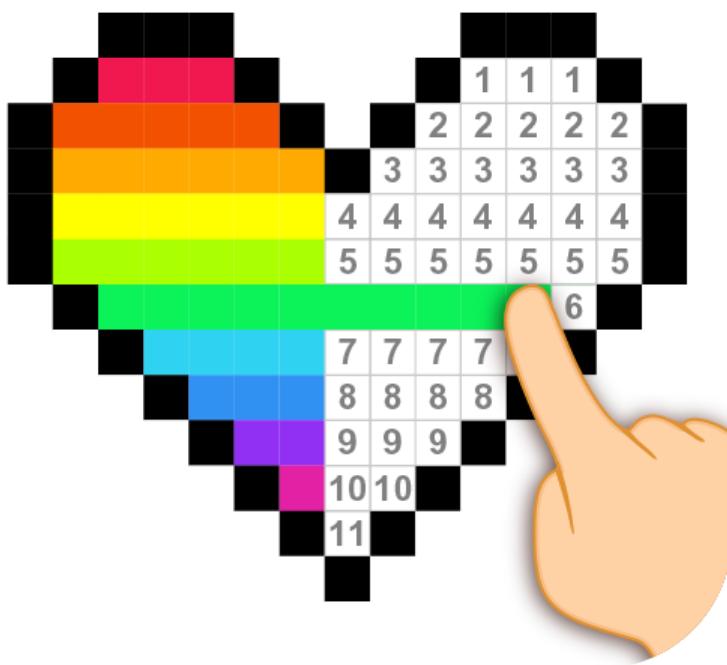
Và đó chính là lý do mà các bộ sưu tập Pixel Art NFT chúng ta thường thấy trên các sàn giao dịch đa phần đều được vẽ bằng ngôn ngữ lập trình. Chưa dừng lại ở đó, người lập trình còn có thể mã hóa thêm một số thông tin quan trọng bên trong tác phẩm của họ. Để phòng trường hợp, một người nào đó cố ý sao chép các tác phẩm này, thì người đó cũng không thể nào tạo ra được một tác phẩm giống 100% so với bản chính được. Chính điều này tạo nên sự khác biệt của các tác phẩm NFT.

5 Vẽ các tác phẩm Pixel Art bằng Python

Ý tưởng ở đây là chúng ta sẽ xây dựng một ma trận 2 chiều (như một bản vẽ) để biểu thị các giá trị pixel này. Các pixel trên ma trận này sẽ được biểu thị bằng một ô vuông và được tô màu tùy theo giá trị tại vị trí đó trong ma trận.

Ví dụ như hình 7.12, ô vuông số 4 ứng với pixel được tô màu vàng. Trong chương trình này chúng ta sẽ sử dụng thêm hàm **setheading(" ")** điều hướng mũi tên của con rùa dùng để vẽ hình, với các tham số:

- Giá trị 0: trỏ sang phải.
- Giá trị 90: trỏ lên trên.,
- Giá trị 180: trỏ sang trái.
- Giá trị 270: trỏ xuống dưới.



Hình 7.12: Một trái tim được vẽ bằng cách tô màu các pixel trên ma trận 2 chiều.

```
1 import turtle  
2  
3 myPen = turtle.Turtle()  
# Toc do ve nhanh nhat  
4 myPen.speed(0)  
# Mau cua net ve la mau den  
5 myPen.color("#000000")  
6  
7  
8  
9  
10 # Ham ve o vuong va to mau dua vao kich thuoc  
11 def box(kich_thuoc):  
    myPen.begin_fill()  
    # 0 do.  
    myPen.forward(kich_thuoc)  
    myPen.left(90)  
    # 90 do.  
    myPen.forward(kich_thuoc)  
    myPen.left(90)  
    # 180 do.  
    myPen.forward(kich_thuoc)  
    myPen.left(90)  
    # 270 do.  
    myPen.forward(kich_thuoc)  
    myPen.end_fill()  
    myPen.setheading(0)  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26
```

```

27 # Kich thuoc o vuong dung de ve mot pixel
28 boxSize = 15
29
30 # Dich chuyen con rua den goc tren ben trai cua ban ve
31 myPen.penup()
32 myPen.forward(-100)
33 myPen.setheading(90)
34 myPen.forward(100)
35 myPen.setheading(0)
36
37
38 # Huong dan cach di chuyen con tro xung quanh truoc khi ve
39 # o vuong
40 # myPen.setheading(0)
41 # myPen.penup()
42 # myPen.forward(boxSize)
43 # myPen.pendown()
44
45
46 # Cach luu tru tac pham Pixel Art bang ma tran 2 chieu
47 pixels = [[0,0,0,0,0,1,1,1,1,1,0,0,0,0,0,0]]
48 pixels.append([0,0,0,1,1,1,1,0,0,1,1,1,1,0,0,0])
49 pixels.append([0,0,1,1,1,1,1,0,0,1,1,1,1,1,0,0])
50 pixels.append([0,1,1,0,1,1,0,0,0,0,1,1,0,1,1,0])
51 pixels.append([0,1,1,0,0,0,0,0,0,0,0,0,0,1,1,0])
52 pixels.append([1,1,1,1,0,0,1,1,1,1,0,0,1,1,1,1])
53 pixels.append([1,1,1,1,0,1,1,1,1,1,0,1,1,1,1,1])
54 pixels.append([1,1,1,1,0,1,1,1,1,1,1,0,1,1,1,1])
55 pixels.append([1,1,1,0,0,1,1,1,1,1,1,0,0,1,1,1])
56 pixels.append([1,0,0,0,0,0,1,1,1,1,0,0,0,0,0,1])
57 pixels.append([1,0,0,1,1,1,1,1,1,1,1,1,1,0,0,1])
58 pixels.append([1,1,1,1,0,0,1,0,0,1,0,0,1,1,1,1])
59 pixels.append([0,1,1,0,0,0,1,0,0,1,0,0,0,1,1,0])
60 pixels.append([0,0,1,0,0,0,0,0,0,0,0,0,0,1,0,0])
61 pixels.append([0,0,1,1,0,0,0,0,0,0,0,0,0,1,1,0])
62 pixels.append([0,0,0,1,1,1,1,1,1,1,1,1,1,0,0,0])
63
64 #Bat dau tien hanh ve cac o vuong pixel
65
66 for i in range(0, len(pixels)):
67     for j in range(0, len(pixels[i])):
68         if pixels[i][j] == 1:
69             box(boxSize)
70             myPen.penup()
71             myPen.forward(boxSize)
72             myPen.pendown()
73             myPen.setheading(270)
74             myPen.penup()

```

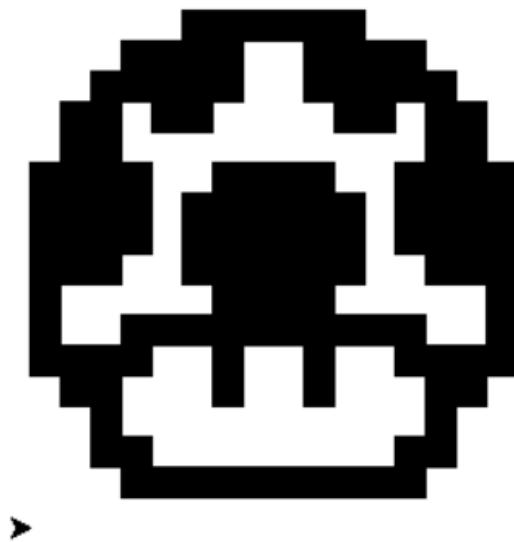
```

75     #quay ve dau hang truoc khi ve cac o vuong pixel tiep
76     #theo
77     myPen.forward(boxSize)
78     myPen.setheading(180)
79     myPen.forward(boxSize * len(pixels[i]))
80     myPen.setheading(0)
81     myPen.pendown()
82
83 turtle.done()

```

Chương trình 7.4: Chương trình vẽ Pixel Art một cây nấm.

Kết quả sau khi hiện thực chương trình trên:



Hình 7.13: Một quả nấm trong game Mario được vẽ theo dạng Pixel Art

Chương trình hoàn chỉnh để vẽ nấm trong game ở hình 7.13 tại:

<https://github.com/Bnbaotam/Python-Turtle-NFT>

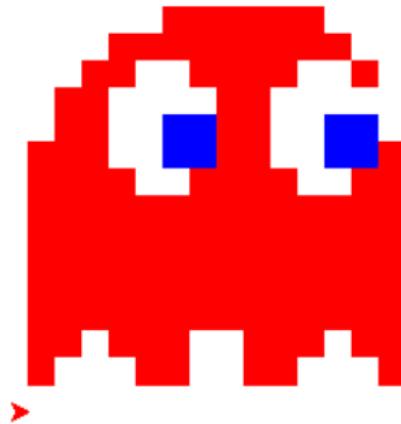
5.1 Tô màu cho tác phẩm Pixel Art

Ở chương trình vẽ nấm trong game mario, chúng ta có thể nhận thấy các giá trị 0 và 1 ở ma trận có ý nghĩa là nếu như gặp giá trị 1 thì chúng ta vẽ và tô đen ô vuông pixel tại vị trí đó, ngược lại nếu là giá trị 0 thì chúng ta bỏ qua.

Do đó, ý tưởng tô màu sẽ đơn giản như sau, chúng ta sẽ thiết lập các giá trị khác trong ma trận, ví dụ 2,3,4,... tùy chúng ta. Và chúng ta quy định rằng nếu là 2 thì chúng ta sẽ tô màu vàng, nếu là 3 thì tô màu đỏ,... Bằng cách sử dụng hàm **color()** và set màu tương ứng trước khi chúng ta bắt đầu vẽ.

Chúng ta có thể tra các mã màu mà chúng ta muốn vẽ bằng cách tìm kiếm mã màu RGB trên công cụ tìm kiếm Google sau đó chọn màu thích hợp.

Sau đây là chương trình dùng để vẽ tác phẩm ở hình 7.14:



Hình 7.14: Một nhân vật trong game Pacman

```
1 import turtle
2
3 myPen = turtle.Turtle()
4 myPen.speed(0)
5 #mau den
6 myPen.color("#000000")
7
8
9 def box(kich_thuoc):
10     myPen.begin_fill()
11     # 0 do.
12     myPen.forward(kich_thuoc)
13     myPen.left(90)
14     # 90 do.
15     myPen.forward(kich_thuoc)
16     myPen.left(90)
17     # 180 do.
18     myPen.forward(kich_thuoc)
19     myPen.left(90)
20     # 270 so.
21     myPen.forward(kich_thuoc)
22     myPen.end_fill()
23     myPen.setheading(0)
24
25
26 boxSize = 15
27
28 # Dich chuyen con rua den goc tren ben trai cua ban ve
```

```

29 myPen.penup()
30 myPen.forward(-100)
31 myPen.setheading(90)
32 myPen.forward(100)
33 myPen.setheading(0)

34

35

36 # Dung list de luu cac gia tri mau trang, do va xanh duong
37 bang_mau = ["#FFFFFF", "#FF0000", "#0000FF"]

38

39 # Thiet lap cac gia tri 0, 1, 2 ung voi cac mau o bang mau
40 pixels = [[0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0]]
41 pixels.append([0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0])
42 pixels.append([0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0])
43 pixels.append([0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0])
44 pixels.append([0, 1, 1, 0, 0, 2, 2, 1, 1, 0, 0, 2, 2, 0, 0, 0])
45 pixels.append([1, 1, 1, 0, 0, 2, 2, 1, 1, 0, 0, 2, 2, 1, 0, 0])
46 pixels.append([1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1])
47 pixels.append([1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1])
48 pixels.append([1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1])
49 pixels.append([1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1])
50 pixels.append([1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1])
51 pixels.append([1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1])
52 pixels.append([1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1])
53 pixels.append([1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1])

54

55 for i in range(0, len(pixels)):
56     for j in range(0, len(pixels[i])):
57         #doi mau net ve ung voi gia tri trong ma tran
58         myPen.color(bang_mau[pixels[i][j]])
59         box(boxSize)
60         myPen.penup()
61         myPen.forward(boxSize)
62         myPen.pendown()
63         myPen.setheading(270)
64         myPen.penup()
65         myPen.forward(boxSize)
66         myPen.setheading(180)
67         myPen.forward(boxSize * len(pixels[i]))
68         myPen.setheading(0)
69         myPen.pendown()

70

71 turtle.done()

```

Chương trình 7.5: Chương trình vẽ Pixel Art một cây nấm.

Chương trình hoàn chỉnh để vẽ nhân vật Pacman trong game ở hình 7.14 tại:

<https://github.com/Bnbaotam/Python-Turtle-NFT>

CHƯƠNG 8

Quy trình tham gia giao dịch các NFT

1 Ví điện tử là gì?

Ví tiền ảo hay ví tiền điện tử là một ứng dụng phần mềm hoặc một thiết bị phần cứng được sử dụng để lưu trữ các tài sản kỹ thuật số. Nó không giống như ví tiền trong túi của chúng ta. Thậm chí, ví tiền ảo thực sự cũng không lưu trữ tiền tệ, mà nó chỉ là nơi cất giữ chìa khóa của địa chỉ ví mà thôi.

Về cơ bản, nó sẽ thường cần một phần mềm cho phép chúng ta gửi và nhận tiền. Và số tiền này được kiểm soát bởi ai nắm trong tay khóa riêng tư (private key), và khóa công khai (public key). Tiền điện tử hay tiền ảo không được lưu trữ ở một nơi “thấy được”. Nhưng nó chỉ là các bản ghi giao dịch được lưu trữ trên blockchain.

1.1 Private Key và Public Key là gì?

Trước tiên, chúng ta cần hiểu như thế nào là các khóa bảo mật. Nó thực chất là đoạn mã hay đoạn code cho phép chúng ta truy cập vào tiền điện tử của mình. Chúng ta có hai dạng khóa chính được sử dụng Private Key và Public Key. Trong đó, người ta hay gọi Private Key là khóa riêng tư hay khóa bí mật. Còn Public Key là khóa công khai.

Khi ai đó gửi Bitcoin cho chúng ta (hay bất kỳ đồng tiền điện tử nào khác). Thì có nghĩa họ đang cấp quyền sở hữu số tiền từ ví của họ sang cho chúng ta. Lúc này, Private Key hoạt động như một mật khẩu riêng tư của chúng ta và được sử dụng để xác nhận giao dịch và chứng minh quyền sở hữu Public Key tương ứng.

Public Key như là đại diện công khai cho chủ sở hữu. Nhưng lại không tiết lộ danh tính của chủ sở hữu. Đó là lý do tại sao chúng ta gọi blockchain có tính “khuyển danh” (pseudonymous). Để một giao dịch tiền điện tử được diễn ra, thì Private Key phải khớp với Public Key của đồng tiền điện tử đó.

2 Ví điện tử Metamask

2.1 Metamask là gì

Metamask là một phần mềm ví tiền điện tử, ban đầu được sử dụng để tương tác với chuỗi khối Ethereum. Hiện nay ví Metamask có thể tích hợp rất nhiều blockchain khác nhau. Gồm phiên bản ví App dành cho Mobile và tiện ích ứng dụng trên Chrome hay còn gọi là phần mở rộng Extension.

Hiện nay ví Metamask có thể được xem là ví tiêu chuẩn, phổ biến nhất hiện nay. Được sử dụng chính để tương tác với hầu hết các blockchain, và cũng được sử dụng để thử nghiệm các mạng đang testnet.

2.2 Các chức năng của ví Metamask Wallet?

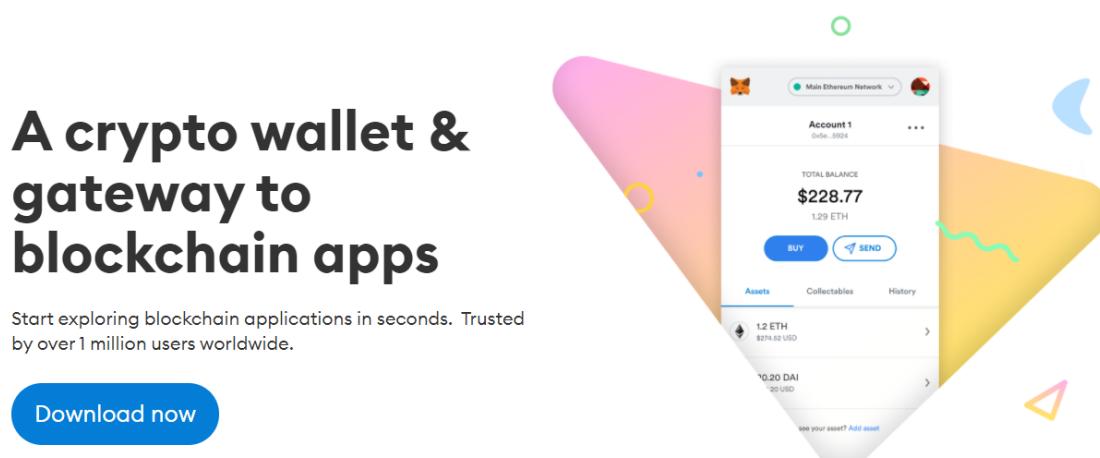
Ví Metamask cho phép người dùng lưu trữ và quản lý khóa tài khoản, theo dõi các giao dịch, trao đổi, chuyển đổi, gửi và nhận tiền điện tử, các token của mạng lưới Ethereum được cài đặt mặc định, đồng thời kết nối an toàn với các ứng dụng phi tập trung thông qua trình duyệt web tương thích hoặc trình duyệt tích hợp sẵn của ứng dụng di động.

Ví Metamask có sẵn trong phần tiện ích mở rộng của trình duyệt Chrome và dưới dạng ứng dụng dành cho thiết bị di động. MetaMask hiện là ví bảo mật an toàn, đăng nhập an toàn, ví hầu như có thể chứa và giao dịch tất cả các token hiện nay.

Ví metamask đã hỗ trợ tiếng việt nên cũng dễ dàng cho chúng ta tương tác .

2.3 Hướng dẫn cài đặt Metamask trên trình duyệt Chrome

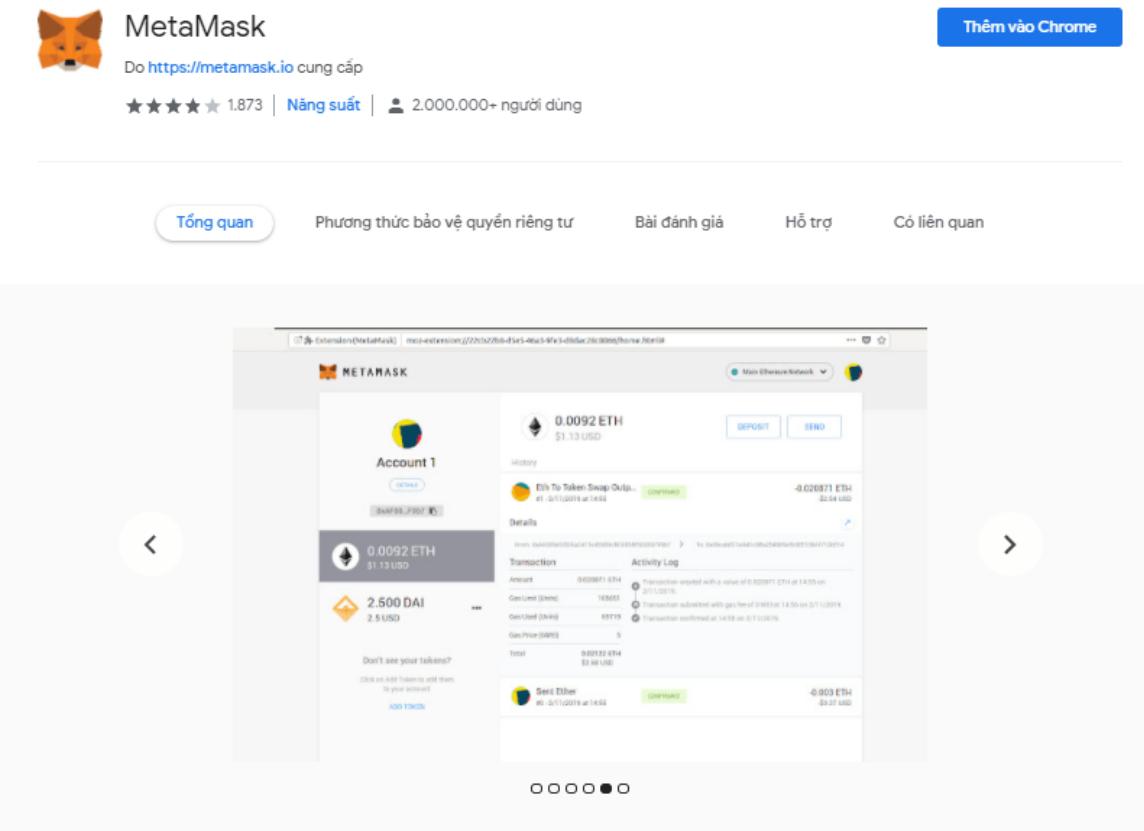
- Bước 1: Truy cập website: <https://metamask.io/>
- Bước 2: Click “Download”, chọn “Install Metamask for Chrome”



Hình 8.1: Tải và cài đặt Metamask

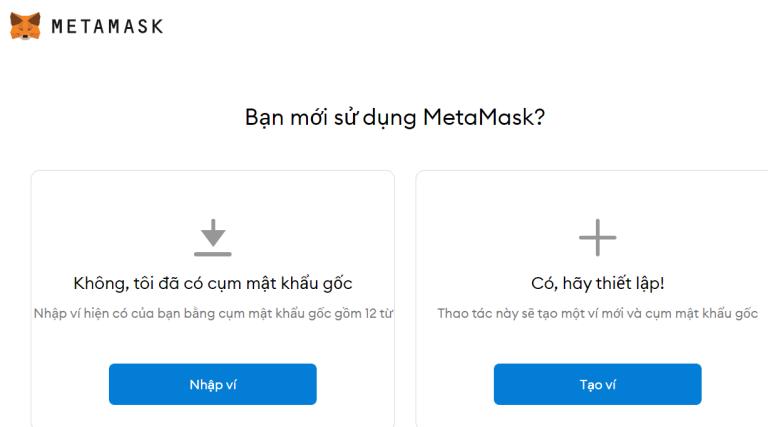
- Bước 3: Thêm tiện ích vào trình duyệt

Trang chủ > Tiện ích > MetaMask



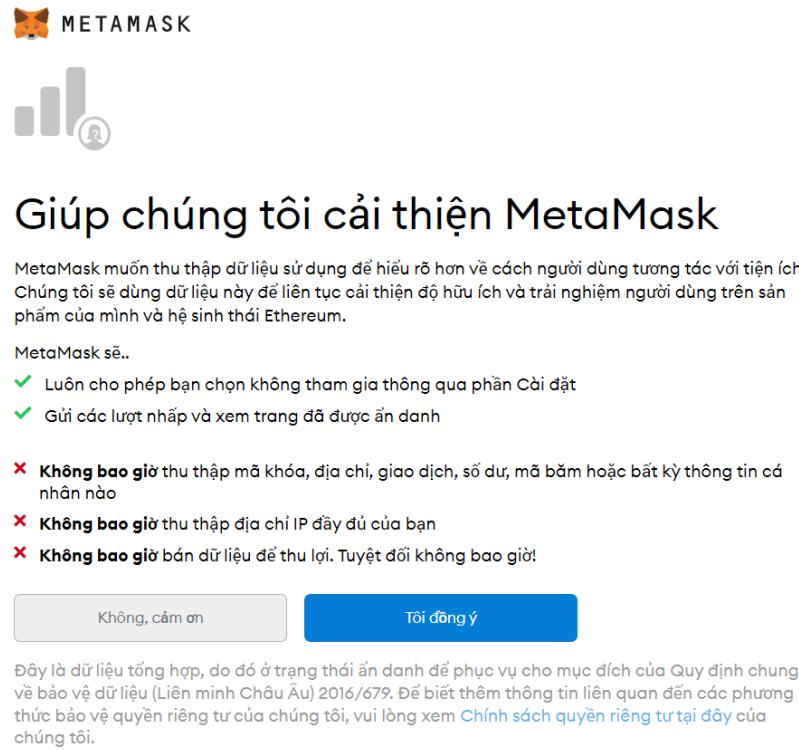
Hình 8.2: Thêm Metamask vào Chrome

- Bước 4: Nhập ví nếu chúng ta đã có “Private Key”, nếu chưa có ví hãy thiết lập chọn click “Tạo Ví”



Hình 8.3: Nhập ví hoặc tạo ví Metamask

- Bước 5: Đọc kỹ các điều khoản và Đồng ý các điều khoản



Hình 8.4: Đồng ý điều khoản Metamask

- Bước 6: Tạo mật khẩu cho ví, nhập mật khẩu 2 lần và xác nhận.

Tạo mật khẩu

Mật khẩu mới (tối thiểu 8 ký tự)

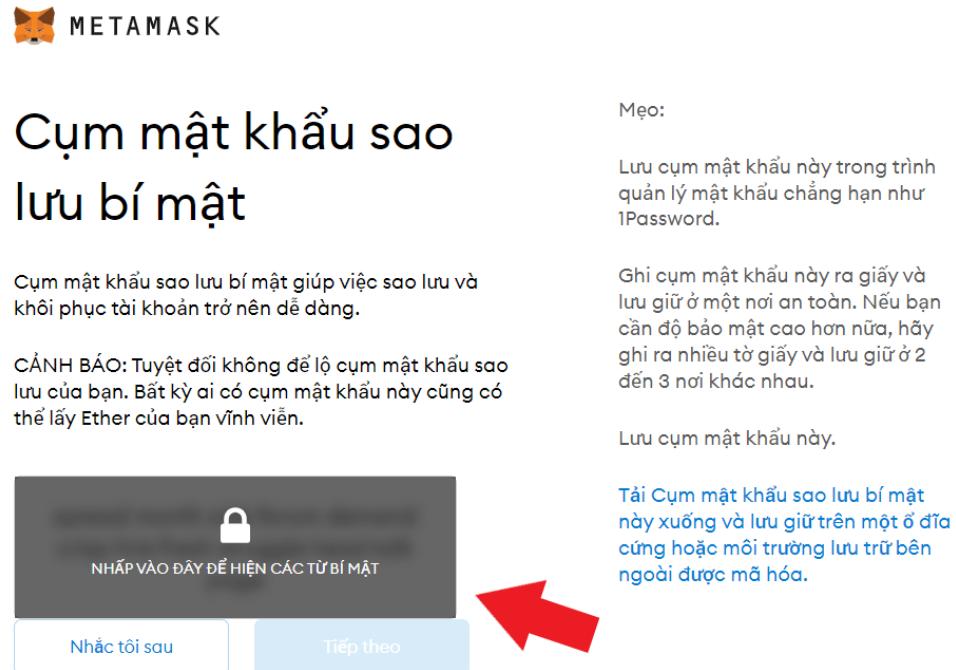
Xác nhận mật khẩu

Tôi đã đọc và đồng ý với [Điều khoản sử dụng](#)

[Tạo](#)

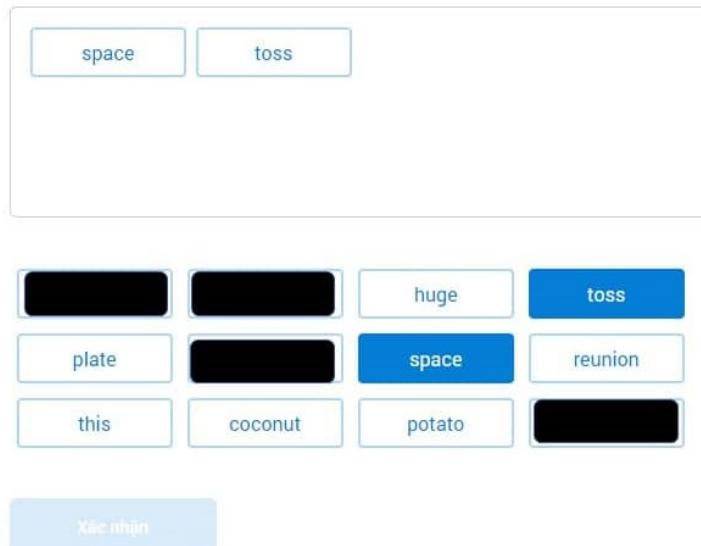
Hình 8.5: Tạo mật khẩu ví Metamask

- Bước 7: Dưới đây cụm Private Key sẽ là một chuỗi các từ và cũng chính là khóa bí mật. Nếu mất khóa này coi như mất tài khoản.



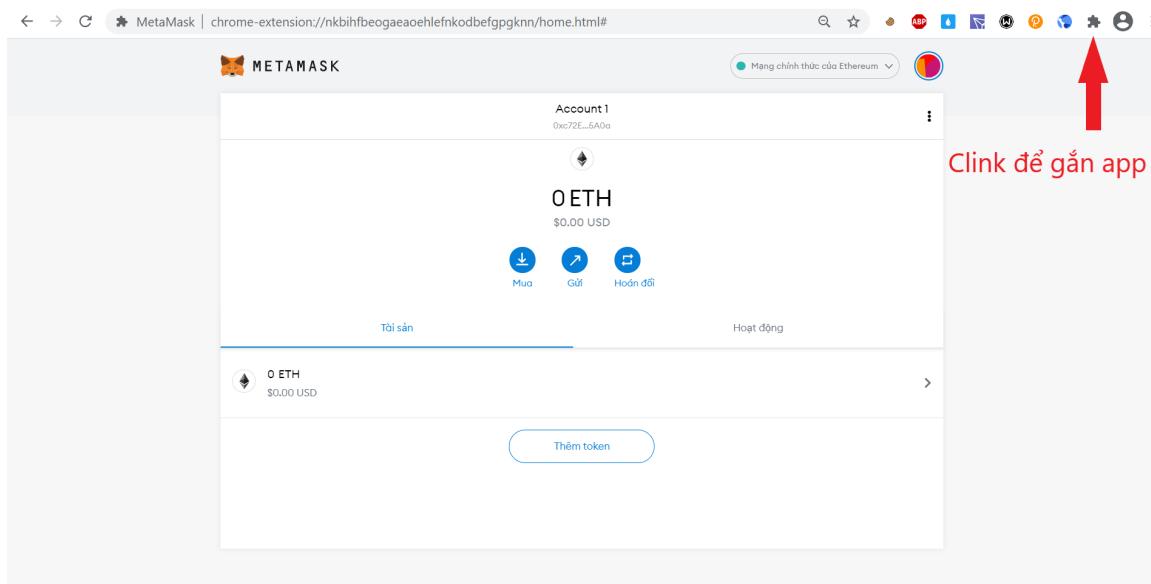
Hình 8.6: Khóa Private Key Metamask

- Bước 8: Nhập lại thứ tự Private Key đã lưu, và bấm xác nhận. Nếu quên cụm từ khóa bí mật (Seed Phrases) thì đồng nghĩa với việc ví của chúng ta sẽ mất luôn, nên chúng ta cần phải ghi rõ lại Seed Phrases lại vào giấy một cách cẩn thận.



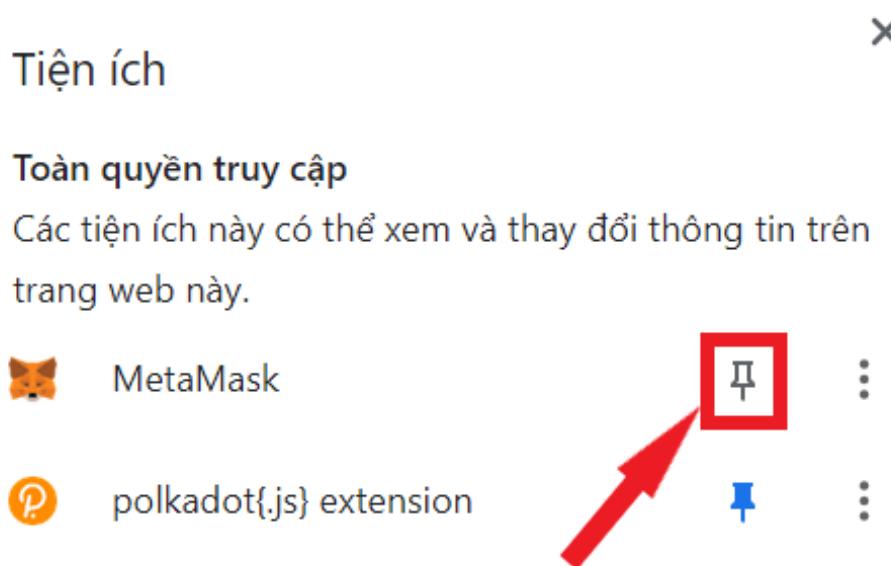
Hình 8.7: Xác nhận lại 12 cụm từ khôi phục theo đúng thứ tự

- Bước 9: Đồng ý và đi đến giao diện ví. Ở góc trình duyệt có phần gắn app lên trình duyệt. Chúng ta click vào biểu tượng để gắn.



Hình 8.8: Cài đặt ví Metamask vào thanh công cụ của Chrome

- Bước 10: Hoàn thành việc gắn ví lên trình duyệt. Sau khi chúng ta ghim, app sẽ nằm trên góc trình duyệt.



Hình 8.9: Ghim Metamask vào thanh công cụ trên Chrome

Lưu ý: lúc này tài khoản của chúng ta vẫn đang là 0. Cho nên, nếu chúng ta muốn thực hiện giao dịch, chúng ta phải chuyển coin vào ví hoặc mua coin thông qua một số sàn giao dịch tiền mã hóa như Binance, Coinbase, OpenSea, ... Bên cạnh đó, tùy sàn giao dịch mà cách tạo tài khoản cũng như cách thức giao dịch sẽ khác nhau.

Trước khi giao dịch, chúng ta nên tìm hiểu và chọn sàn giao dịch uy tín, tránh tiền mất tật mang. Có một số lưu ý quan trọng khi tham gia thị trường tiền mã hóa như sau:

- Không nên chia sẻ mật khẩu (sàn, ví...) cho bất kỳ ai để tránh mất tiền và tài khoản bị đánh cắp
- Không đầu tư nhiều hơn số tiền chúng ta có thể mất
- BẤT BUỘC phải có ví (wallet) để lưu trữ coin. Tránh trường hợp: SÀN SẬP và TÀI SẢN CỦA CHÚNG TA BỊ MẤT.
- Mọi quyết định cuối cùng đều do chúng ta chọn. Cho nên, hãy dành thời gian nghiên cứu THẬT KỸ trước khi đầu tư.

3 Thị trường lớn nhất thế giới về NFT - OpenSea

3.1 OpenSea là gì?

OpenSea là thị trường ngang hàng đầu tiên và lớn nhất dành cho hàng hóa tiền điện tử, bao gồm đồ sưu tầm (collectibles), vật phẩm trò chơi (game items) và các hàng hóa ảo khác được bảo đảm bằng Blockchain. Trên OpenSea, bất kỳ ai cũng có thể mua hoặc bán những mặt hàng này thông qua hợp đồng thông minh.

Những hàng hóa này là các mặt hàng kỹ thuật số mà chúng ta có thể thu thập. Chúng có thể có các danh mục khác nhau và chúng là hàng kỹ thuật số và mã hóa 100%, chúng ta sở hữu chúng 100% sau khi mua vì các giao dịch và bằng chứng quyền sở hữu được lưu trữ mãi mãi trên Blockchain Ethereum.

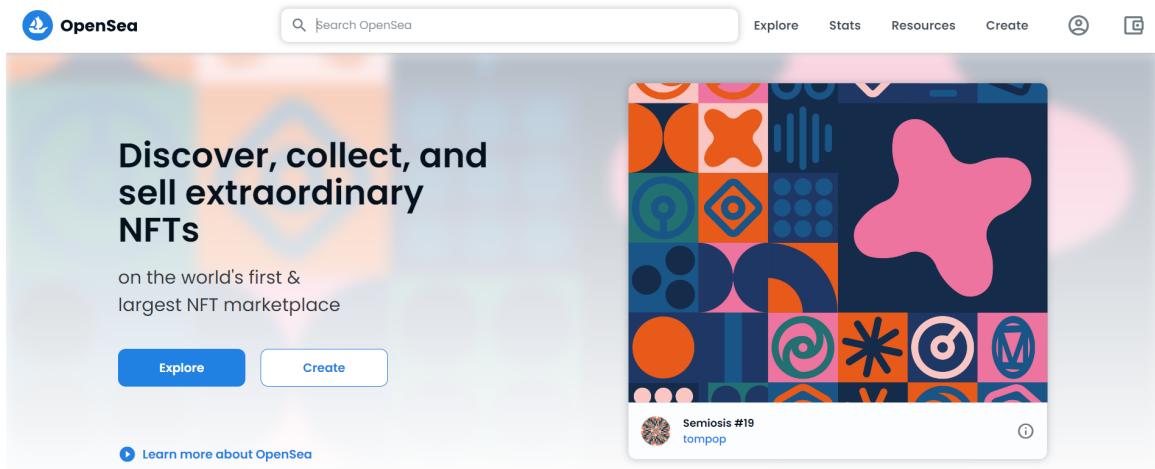
3.2 Cơ chế mua bán trên OpenSea như thế nào?

Mang triết lý của công nghệ phi tập trung. Mọi giao dịch trên OpenSea sẽ được thực hiện dưới dạng hợp đồng thông minh. Nghĩa là không có bên thứ ba nào giữ các mặt hàng của chúng ta. Thay vào đó, nó được lưu trữ trong ví được hỗ trợ, như MetaMask.

3.3 Có thể mua bán những gì trên OpenSea?

Trên lý thuyết, với OpenSea chúng ta có thể mua bán bất cứ tài sản nào được hỗ trợ bởi công nghệ blockchain. Danh mục hiện tại mà OpenSea dùng để phân loại các tài sản đang được giao dịch trên sàn, bao gồm:

- Các đồ sưu tầm
- Các vật phẩm trong game
- Tên miền
- Tác phẩm nghệ thuật kỹ thuật số (NFT)



Hình 8.10: Giao diện của OpenSea.

3.4 Cân gì để có thể giao dịch mua và bán trên OpenSea?

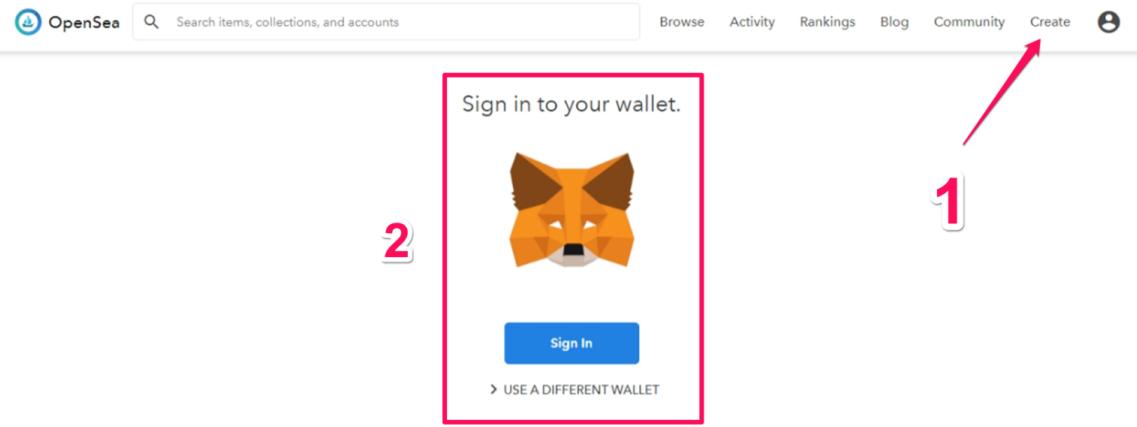
Nếu chúng ta là người mới tìm hiểu. Thì cách liệt kê sau đây là cần thiết để chúng ta gia nhập thị trường NFT. Những điều kiện phải có để chúng ta có thể mua và tự niêm yết vật phẩm mình lên sàn để bán.

- Một ví MetaMask để kết nối với tài khoản OpenSea. Thực ra, OpenSea không chỉ hỗ trợ thanh toán với MetaMask, nhưng nhiều ví khác như Bitski, Fortmatic, WalletConnect, WalletLink... MetaMask vẫn là phổ biến nhất.
- Dĩ nhiên, chúng ta cần tiền để mua ETH (hoặc một altcoin nào dùng để thanh toán).

Các phần tiếp theo sẽ trình bày chi tiết hơn các bước cũng như các lưu ý để chúng ta hiểu rõ hơn về quy trình này.

4 Hướng dẫn kết nối ví MetaMask với OpenSea để bắt đầu giao dịch

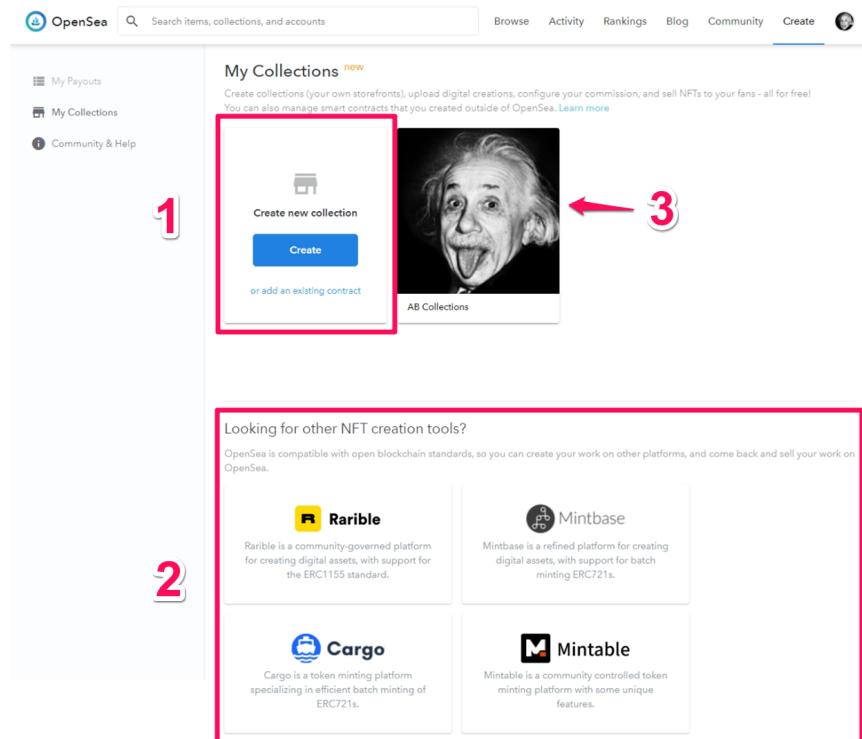
- Khi chúng ta nhấn vào "Create" để tạo bộ sưu tập vật phẩm và thêm vật phẩm thì OpenSea sẽ đòi hỏi chúng ta phải đăng nhập MetaMask và kết nối với MetaMask trước.
- Có rất nhiều ví khác được hỗ trợ trong phần "USE DIFFERENT WALLET". Nhưng mặc định vẫn là MetaMask. chúng ta bấm "Sign In". Khi đó, ví MetaMask dưới dạng extension của trình duyệt sẽ hiện ra và tự động kết nối nhanh chóng.



Hình 8.11: Kết nối ví Metamask với OpenSea.

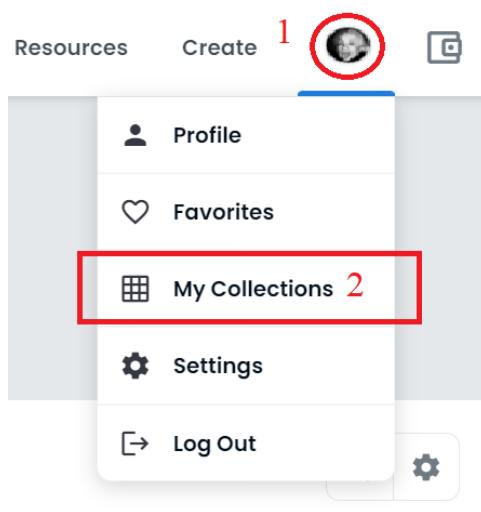
5 Hướng dẫn tạo Collections và thêm vật phẩm số NFT để bán trên OpenSea

Nhìn chung, giao diện của OpenSea khá dễ sử dụng. “Collections” có nghĩa là bộ sưu tập. Nó như một cửa hàng của riêng chúng ta trên chợ NFTs này vậy. chúng ta có thể tạo nhiều “cửa hàng” khác nhau tùy theo loạt vật phẩm số muốn bán.



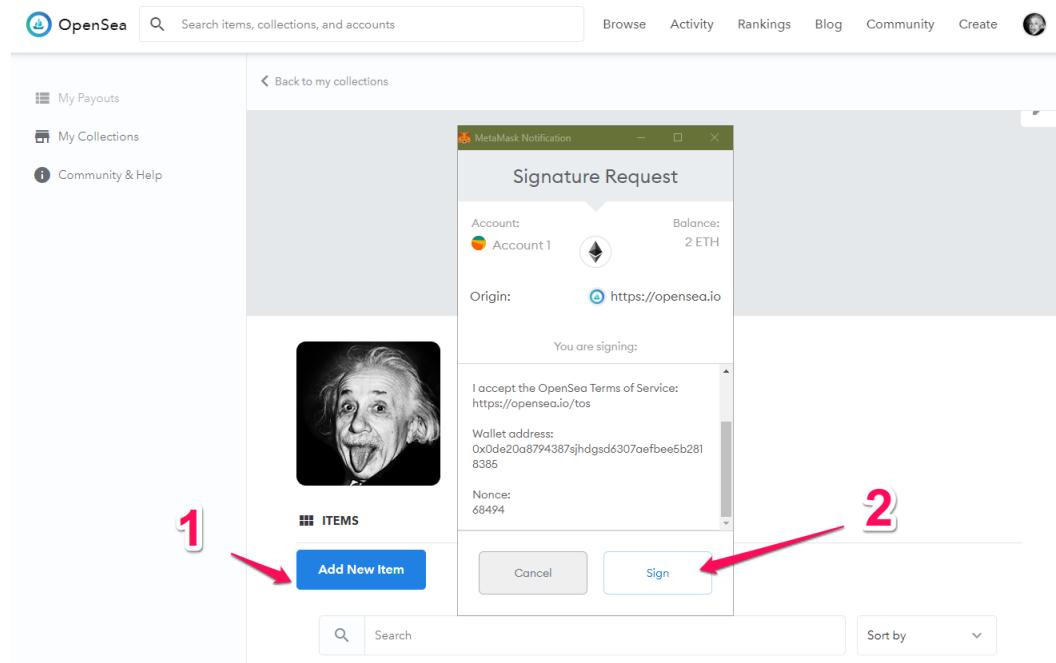
Hình 8.12: Giao diện bộ sưu tập trên OpenSea.

- Sau khi kết nối MetaMask thành công. Chung ta di chuyển chuột vào ô màu ảnh đại diện ở góc trên cùng bên phải, chọn “My Collection” và click vào đó. Giao diện điền thông tin Collections sẽ hiện ra và chúng ta có thể tùy hứng chọn avatar, đặt tên, mô tả...



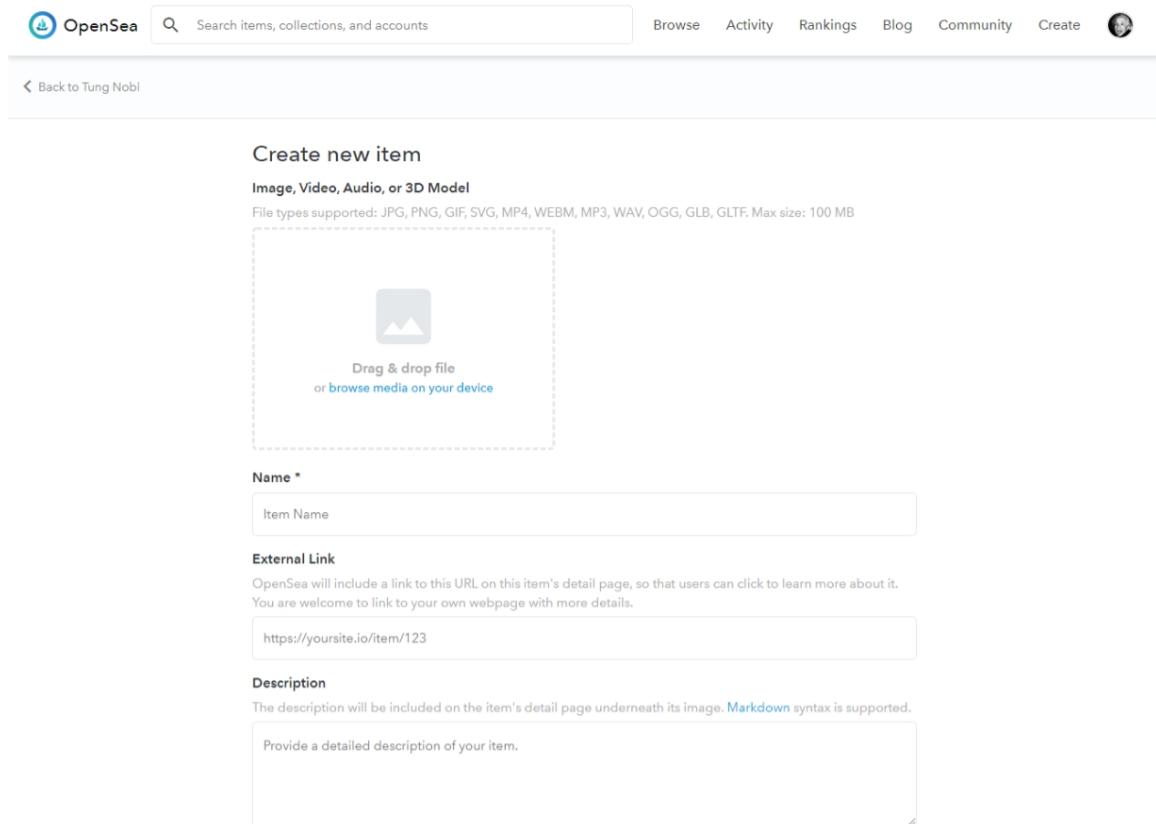
Hình 8.13: Tạo bộ sưu tập riêng.

- OpenSea còn tương thích với nhiều công cụ tạo NFT khác. OpenSea để xuất một số công cụ tạo NFT như Rarible, MintBase, Cargo... chúng ta có thể vào đây tạo NFT rồi quay lại OpenSea để list lên bán.
- Đây là một “Collections” đã tạo thành công với tên và avatar. Bấm vào Collection mới tạo này để thêm vật phẩm số muốn bán.



Hình 8.14: Giao diện thêm NFT cần bán.

- Trong giao diện Collection, chúng ta chọn “Add new item” để thêm NFT.
- Một giao diện MetaMask với NONCE (số sử dụng 1 lần) sẽ hiện ra. Thực chất, chúng ta cần hiểu, việc thêm NFT này nghĩa là chúng ta đang tạo một smart contract trên chuỗi khôi ETH. Nên bước này là cần thiết. Chọn “Sign”. Giao diện điền thông tin NFT sẽ hiện ra.



Hình 8.15: Giao diện điền thông tin NFT để bán..

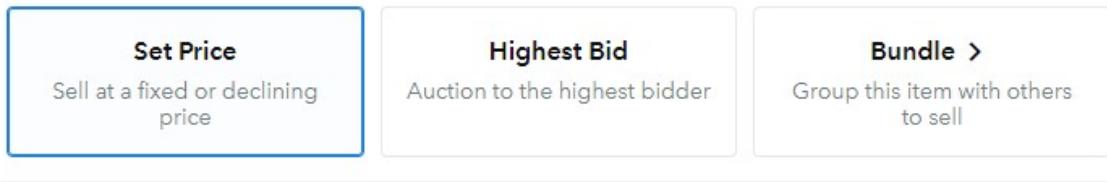
Sau đó, chúng ta sẽ được đưa đến giao diện điền thông tin NFT. Tại chúng ta hãy upload tác phẩm của mình lên. Đó có thể là bức tranh nghệ thuật, đoạn nhạc chúng ta sáng tác, một mô hình 3D... Sau khi điền xong bấm “Create” là xe như hoàn tất.

6 Niêm yết và bán các tác phẩm NFT trên sàn OpenSea

Sau khi chúng ta đã list lên OpenSea, chỉ cần vào mục “Sell” và thiết lập giá để bắt đầu bán nó.

Sẽ có 3 phương án để chúng ta lựa chọn: “Set Price” (Niêm yết một giá cố định), “Highest Bid” (đầu giá) hoặc “Bundle” (nhóm sản phẩm này với những sản phẩm khác để bán).

Select your sell method



Hình 8.16: 3 phương án bán tác phẩm NFT.

6.1 Set Price (giá cố định)

- **Starting price**: chọn mức giá muôn bán
- **Include ending price**: giá kết thúc (Mức giá này phải nhỏ hơn hoặc bằng giá khởi điểm) và giá bán sẽ giảm dần từ giá khởi điểm đến giá kết thúc trong thời gian bán.

The screenshot shows the configuration interface for setting a fixed price for an NFT listing:

- Starting Price**: Set an initial price. (Value: 1)
- Include ending price**: A toggle switch is turned on.
- Ending price**: Must be less than or equal to the starting price. The price will progress linearly to this amount until the expiration date. (Value: 0)
- Expiration date**: Your listing will automatically end at this time. No need to cancel it! (Set to "in 5 days" at 04:25 PM)

Hình 8.17: Giao diện thiết lập giá cố định.

- **Schedule for a future time**: lên lịch để bán NFT sau một khoảng thời gian nhất định
- **Privacy**: chúng ta có thể để NFT của chúng ta ở chế độ riêng tư hoặc chỉ định người mà chúng ta muốn bán.

6.2 Highest Bid (đầu giá)

- **Minimum Bid**: giá tối thiểu (khách hàng sẽ phải đặt mức giá lớn hơn hoặc bằng giá tối thiểu)
- **Reserve price**: giá khởi điểm (giá khởi điểm phải lớn hơn giá tối thiểu). Nếu chúng ta không nhận được bất kỳ giá thầu nào lớn hơn hoặc bằng giá khởi điểm. Phiên đấu giá sẽ kết thúc và NFT không được bán. (Reserve price đảm bảo chúng ta luôn bán được NFT với giá mong muốn)

- **Expiration Date:** cài đặt thời gian cho phiên đấu giá

The screenshot shows the auction settings section of the OpenSea platform. It includes three main input fields: 'Minimum Bid' set to 1, 'Reserve price' set to 2, and 'Expiration Date' set to 'in 5 days' at '04 : 25 PM'. Below these fields is a note about the auction ending automatically at the specified time.

Minimum Bid	1
Reserve price	2
Expiration Date	in 5 days at 04 : 25 PM

Your auction will automatically end at this time and the highest bidder will win. No need to cancel it!

Hình 8.18: Giao diện thiết lập đấu giá.

6.3 Bundle (nhóm sản phẩm)

Nếu chọn Bundle, chúng ta có thể nhóm nhiều NFT lại để bán thành 1 combo. Quá trình cài đặt cũng tương tự như bán 1 NFT đơn.

7 Một số lưu ý khi đăng bán NFT

chúng ta có thể trả tiền hoa hồng cho những người giới thiệu thành công khách hàng cho chúng ta (tối đa 2,5%)

OpenSea sẽ thu 2,5% tiền bán NFT của chúng ta trong trường hợp NFT được bán thành công.

Nếu đây là lần đầu chúng ta bán NFT trên OpenSea, chúng ta sẽ phải trả **phí Gas** trước khi đăng bán. Giao dịch này, về cơ bản tạo ra một hợp đồng thông minh giao dịch cá nhân cho ví của chúng ta, hiện phí đang rất cao do tắc nghẽn trên blockchain Ethereum nhưng chúng ta chỉ phải thực hiện một lần. Nếu chúng ta bán các tác phẩm của mình bằng đơn vị tiền tệ không phải là ETH, chúng ta cũng sẽ được yêu cầu chấp thuận token đó để giao dịch phát sinh một khoản phí gas khác (nhỏ hơn). Đây là phí một lần nên từ lần thứ hai chúng ta sẽ không phải trả thêm một xu nào.

Cuối cùng chúng ta chọn “Post your listing” để đăng bán NFT của mình.

Summary

Listing

Your item will be listed for ♦1.

[Post your listing >](#)

Bounties EDIT

OpenSea rewards 1% to registered affiliates who refer your buyer.

Fees

Listing is free! At the time of the sale, the following fees will be deducted. [Learn more.](#)

To OpenSea	2.5%
Total	2.5%

Hình 8.19: Giao diện tổng hợp thông tin và xác nhận.