

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM

KHOA ĐÀO TẠO CHẤT LƯỢNG CAO

----------------------



CẤU TRÚC DỮ LIỆU VÀ GIẢI THUẬT

ĐỀ TÀI:

TÌM HIỂU VỀ BLOCKCHAIN

GVHD: Nguyễn Thiên Bảo

SVTH: MSSV:

Nguyễn Văn Lành 15110069

Nguyễn Bá Lê An 15110001

Võ Đức Huy 15110057

Trần Thanh Thông 15110135

Hoàng Phước Đại 15110028

Tp. Hồ Chí Minh, 14 tháng 12 năm 2019

**LỜI CẢM ƠN**

Trước hết, chúng em xin chân thành cảm ơn đến Thầy Nguyễn Thiên Bảo đã tận tình hướng dẫn, giúp đỡ chúng em rất nhiều trong suốt quá trình thực hiện đồ án của môn học này.

Với vốn kiến thức được tiếp thu trong quá trình học tập không chỉ là nền tảng cho quá trình nghiên cứu môn học mà còn là hành trang để chúng em bước vào đời một cách vững chắc.

Với vốn kiến thức hạn hẹp và thời gian thực hiện có hạn, bản thân còn thiếu nhiều kinh nghiệm nên chúng em không tránh khỏi những thiếu sót về nội dung báo cáo. Rất mong nhận được những ý kiến đóng góp của thầy để chúng em có thể tiếp tục phát triển đồ án này.

Xin chân thành cảm ơn!

**Nhóm sinh viên thực hiện**

Nguyễn Văn Lành

Nguyễn Bá Lê An

Võ Đức Huy

Trần Thanh Thông

Hoàng Phước Đại

**LỜI MỞ ĐẦU**

Dư luận dường như đang chia thành hai phe: Những người coi tiền điện tử là một bong bóng chỉ chực vỡ và những người coi nó là tương lai của hệ thống tài chính toàn cầu.

Trên thực tế, cuộc cách mạng mà tiền điện tử mang đến không nằm ở giá trị giao dịch hay cơ hội kiếm tiền ngắn hạn cho các tay chơi cryptocurrency mà ở chính công nghệ nền tảng đứng sau nó: Blockchain.

Blockchain khai sinh ra tiền điện tử, nhưng tiền điện tử không phải là tất cả những gì mà blockchain có thể tạo ra. Được coi là một trong những phát minh tuyệt vời nhất trong nhiều thập kỷ trở lại đây.

Blockchain là chủ đề đang vô cùng nóng trên toàn cầu hiện nay. Nó cùng với [Bitcoin](https://quantrimang.com/s/?q=bitcoin) và tiền kỹ thuật số 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.

MỤC LỤC

[CHƯƠNG I: TỔNG QUAN 1](#_Toc27209063)

[1.1. Khái niệm về Blockchain 1](#_Toc27209064)

[1.2. Lịch sử ra đời Blockchain 1](#_Toc27209065)

[1.3. Cách hoạt động của Blockchain 1](#_Toc27209066)

[1.4. Bitcoin 2](#_Toc27209067)

[1.5. Ethereum 5](#_Toc27209068)

[Chương II: ĐẶC ĐIỂM CỦA BLOCKCHAIN 6](#_Toc27209069)

[2.1. Các đặc điểm chính của Blockchain 6](#_Toc27209070)

[2.2. Các phiên bản của Blockchain 8](#_Toc27209071)

[2.3. Phân loại Blockchain 9](#_Toc27209072)

[2.4. Blockchain có thể được dùng ở đâu? 10](#_Toc27209073)

[2.5. Những bất lợi khi sử dụng Blockchain 11](#_Toc27209074)

[CHƯƠNG III: ỨNG DỤNG CỦA BLOCKCHAIN 13](#_Toc27209075)

[3.1. Trong thương mại điện tử 13](#_Toc27209076)

[3.2. Trong dịch vụ tài chính, ngân hàng 13](#_Toc27209077)

[3.3. Trong nông nghiệp 14](#_Toc27209078)

[3.4. Trong giáo dục, y tế 14](#_Toc27209079)

[CHƯƠNG IV: KẾT LUẬN 15](#_Toc27209080)

[TÀI LIỆU THAM KHẢO 16](#_Toc27209081)

**CHƯƠNG I: TỔNG QUAN**

* 1. **Khái niệm về Blockchain**

**Blockchain** (chuỗi khối) tên khai sinh: **block chain** là một cuốn sổ cái kỹ thuật số phân cấp, lưu trữ các thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa vô cùng phức tạp. Sổ cái được chia sẻ cho những người tham gia vào mạng lưới. Điều này cho thấy rằng trong toàn bộ hệ thống không phải chỉ có một vị trí duy nhất, một tài liệu có thể làm căn cứ đáng tin (authority) duy nhất, vì những lần sao chép cùng một phiên bản sổ cái được đặt ở nhiều nơi.

Blockchain được thiết kế để chống lại việc thay đổi của dữ liệu: Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó. Blockchain được đảm bảo nhờ cách thiết kế sử dụng hệ thống tính toán phân cấp với khả năng chịu lỗi byzantine cao.

Vì vậy sự đồng thuận phân cấp có thể đạt được nhờ Blockchain. Nên Blockchain phù hợp để ghi lại những sự kiện, hồ sơ y tế, xử lý giao dịch, công chứng, danh tính và chứng minh nguồn gốc. Việc này có tiềm năng giúp xóa bỏ các hậu quả lớn khi dữ liệu bị thay đổi trong bối cảnh thương mại toàn cầu.

* 1. **Lịch sử ra đời Blockchain**

Người phát minh và thiết kế ra Blockchain đầu tiên chính là **Satoshi Nakamoto**, ông tạo ra nó năm 2008 và được hiện thực hóa vào năm sau đó như là một nền tảng cốt lõi của Bitcoin, công nghệ Blockchain đống vai trò giống như một cuốn sổ cái ghi lại tất cả các giao dịch. Qua việc sử dụng mạng lưới ngang hàng (peer-to-peer) và một hệ thống dữ liệu phân cấp, Bitcoin blockchain được quản lý tự động.

Việc Blockchain ra đời đã làm cho Bitcoin trở thành loại tiền mã hóa đầu tiên giải quyết được vấn đề chi tiêu gian lận khi 1 lượng tiền được chi tiêu 2 lần (double spending). Công nghệ này của Bitcoin đã trở thành nguồn cảm hứng cho một loạt các ứng dụng khác cũng như các đồng coin sau này.

* 1. **Cách hoạt động của Blockchain**

**Công nghệ Blockchain** chính là phát minh ưu việt nhất từ chính Internet cho tới thời điểm này. Nó cho phép trao đổi giá trị mà không cần tới sự tin tưởng hoặc chứng cứ làm tin.

Ví dụ: “*tôi và bạn cá cược 50 USD cho thời tiết ngày mai ở San Francisco. Tôi đoán trời sẽ nắng, còn bạn lại cược là trời mưa*”. Vậy hôm nay chúng ta có ba tùy chọn để quản lý giao dịch này:

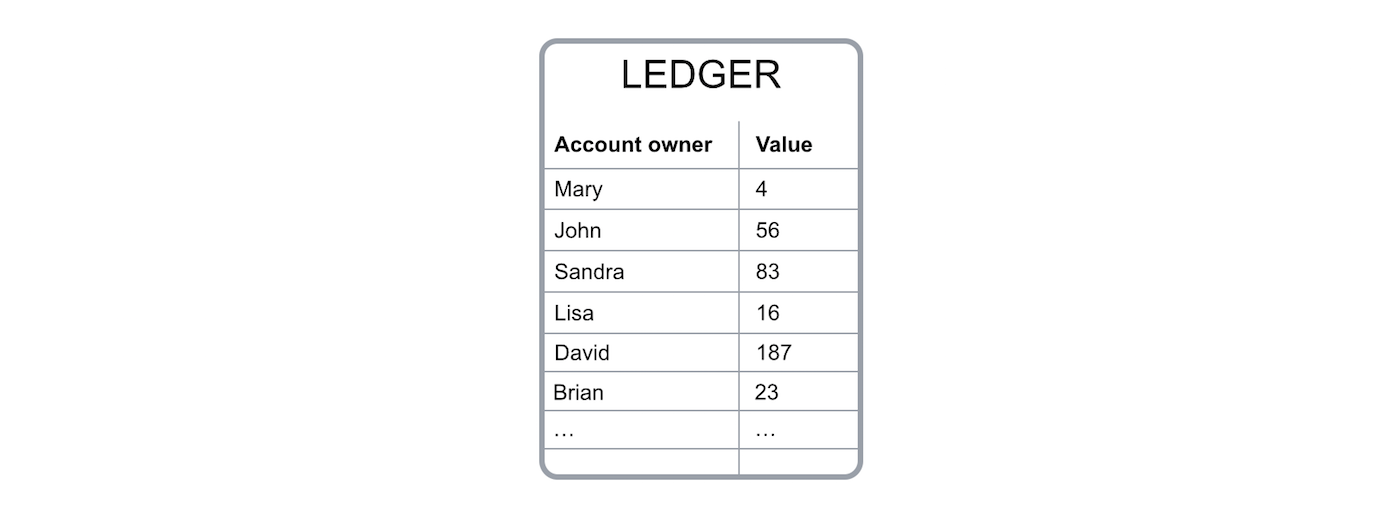
* **Chúng ta có thể tin tưởng lẫn nhau**. Mưa hoặc nắng, người thua sẽ trả 50 đô la cho người chiến thắng. Nếu chúng ta là bạn, đây có thể là một cách hay để đặt cược. Tuy nhiên, dù là bạn bè hay người lạ thì vẫn không thể dễ dàng trả tiền cho người kia.
* **Chúng ta có thể biến tiền cược thành một hợp đồng**. Với một hợp đồng tại chỗ, cả hai bên sẽ dễ phải trả tiền hơn, tuy nhiên, nếu một trong hai người quyết định không trả, người chiến thắng sẽ phải trả thêm tiền để trang trải chi phí pháp lý và bản án có thể mất một thời gian dài. Đặc biệt với một lượng tiền mặt nhỏ, điều này dường như không phải là cách tối ưu để quản lý giao dịch.
* **Chúng ta có thể nhờ đến một bên thứ ba trung lập**. Mỗi người trong chúng ta đưa 50 đô la cho một người thứ ba, cô ấy sẽ đưa tổng số tiền cho người chiến thắng. Nhưng, cô ấy cũng có thể bỏ trốn với tất cả số tiền. Vì vậy, chúng ta sẽ chọn một trong hai lựa chọn đầu tiên: tin tưởng hoặc hợp đồng.
* Blockchain cho phép viết một vài dòng code, chương trình chạy trên blockchain, mà cả hai chúng ta gửi 50 đô la vào đó. Chương trình này sẽ giữ 100 đô la an toàn và kiểm tra thời tiết ngày mai một cách tự động trên nhiều nguồn dữ liệu. Nắng hoặc mưa, nó sẽ tự động chuyển toàn bộ số tiền cho người chiến thắng. Mỗi bên có thể kiểm tra hợp đồng logic, và vì nó đang chạy trên blockchain nên nó không thể thay đổi hoặc ngừng lại. Nỗ lực này có thể là quá cao đối với một giao dịch 50 đô la, nhưng hãy tưởng tượng khi bán nhà hoặc công ty..

Mục tiêu của phần này là để giải thích cách blockchain hoạt động mà không thảo luận về các chi tiết kỹ thuật sâu, nhưng  đủ để có một ý tưởng chung về logic và cơ chế cơ bản.

* 1. **Bitcoin**

Bitcoin là một đơn vị tiền tệ kỹ thuật số của Bitcoin, giống như đô la, bản thân nó không có giá trị. Nó có giá trị vì chúng ta đồng ý trao đổi hàng hóa, dịch vụ để đổi lấy một lượng tiền lớn hơn dưới dự kiểm soát của chúng ta và chúng ta tin rằng người khác cũng sẽ làm như vậy.

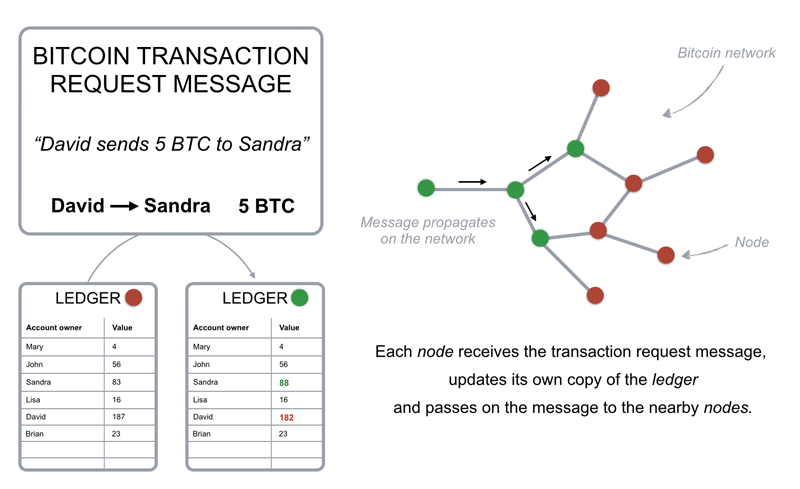
Để theo dõi lượng Bitcoin mỗi người trong chúng ta sở hữu, blockchain sử dụng một sổ cái - file kỹ thuật số - theo dõi tất cả các giao dịch của Bitcoin.



Hình 1: *Tập tin kỹ thuật số của Bitcoin đã được đơn giản hoá*

File này không được lưu trữ trên máy chủ tập trung, giống như ngân hàng hay trung tâm dữ liệu. Nó được phân tán trên toàn thế giới thông qua mạng máy tính, vừa lưu trữ dữ liệu, vừa thực hiện tính toán. Mỗi máy tính đại diện cho một nút của mạng blockchain và có một bản sao của file sổ cái.

Nếu David muốn gửi Bitcoin cho Sandra, anh ta sẽ phát một tin nhắn tới mạng nói rằng số lượng Bitcoin trong tài khoản của anh ta sẽ giảm xuống 5 BTC, và số tiền của tài khoản Sandra sẽ tăng lên theo cùng số lượng. Mỗi nút trong mạng sẽ nhận được thông báo và áp dụng giao dịch yêu cầu vào bản sao của sổ cái, do đó cập nhật số dư tài khoản.



Hình 2: Mô tả một giao dịch Bitcoin

Để có thể thực hiện các giao dịch trên blockchain, cần có một ví, một chương trình cho phép lưu trữ và trao đổi Bitcoin. Vì chỉ có mình mới có thể chi tiêu được Bitcoin của mình, mỗi chiếc ví được bảo vệ bởi một phương pháp mật mã đặc biệt, sử dụng một cặp khóa riêng biệt khác nhau nhưng có kết nối: một khoá riêng tư (*private*) và công khai (*public*).

Làm thế nào hệ thống có thể tin tưởng giao dịch đầu vào và xem xét chúng có giá trị?

Nó kiểm tra tất cả các giao dịch trước đó có tương quan với ví bạn sử dụng để gửi Bitcoin thông qua các tham chiếu và đầu vào.

Để đơn giản hóa và đẩy nhanh quá trình xác minh, một bản ghi đặc biệt về các giao dịch không được sử dụng sẽ được giữ bởi các nút mạng. Nhờ kiểm tra bảo mật này, bạn không thể tiêu gấp đôi số Bitcoin nhận được.

Tất cả các code để thực hiện giao dịch trên mạng Bitcoin là mã nguồn mở, điều này có nghĩa là bất cứ ai có máy tính xách tay và một kết nối Internet đều có thể thực hiện giao dịch. Tuy nhiên, nếu có một lỗi trong code được sử dụng để phát thông báo yêu cầu giao dịch, Bitcoin liên quan sẽ bị mất vĩnh viễn.

Bitcoin là đồng tiền điện tử đặt nền móng cho thị trường [Cryptocurrency](https://coin98.net/cryptocurrency-la-gi/). Từ công nghệ Blockchain, hiện có rất nhiều đồng tiền điện tử được hình thành. Nhiều người đặt niềm tin vào tiềm năng mới của thị trường này.

* 1. **Ethereum**

Ethereum là một nền tảng điện toán có tính phân tán, công cộng, mã nguồn mở dựa trên công nghệ Blockchain. Ethereum được xây dựng trên cùng các nền tảng như Blockchain Bitcoin nhưng chứa nhiều tiềm năng phát triển công nghệ Blockchain cụ thể là hợp đồng thông minh trên nền tảng ethereum. Ethereum còn là một Blockchain với ngôn ngữ lập trình cho phép các ứng dụng hoạt động trên Blockchain. Điều này cũng cho phép các nhà phát triển tạo ra các chương trình hoạt động trên Blockchain đồng thời sử dụng sức mạnh tính toán của hàng ngàn máy tính được kết nối với mạng Blockchain. Gần như mọi ứng dụng chạy trên máy tính ngày nay đều có tiềm năng hoạt động trên Blockchain. Bằng cách tận dụng mạng Ethereum, các nhà phát triển có thể dễ dàng tạo các ứng dụng phi tập trung mà không cần phải tạo Blockchain và tiền kỹ thuật số của riêng họ.

**Chương II: ĐẶC ĐIỂM CỦA BLOCKCHAIN**

* 1. **Các đặc điểm chính của Blockchain**
     1. **Một cơ sở dữ liệu phân tán**

Hãy tưởng tượng một bảng tính được nhân đôi hàng ngàn lần thông qua mạng lưới máy tính, mạng lưới này được thiết kế để cập nhật thường xuyên bảng tính đó là bạn đã có thể hiểu được cơ bản về blockchain.

Thông tin được tổ chức trên một blockchain tồn tại dưới dạng cơ sở dữ liệu được chia sẻ và hòa hợp liên tục. Đây là cách để sử dụng mạng với những lợi ích rõ ràng. Cơ sở dữ liệu blockchain không được lưu trữ ở duy nhất một vị trí nào, nghĩa là các bản ghi được lưu trữ một cách công khai, dễ kiểm chứng. Không có một phiên bản tập trung nào của cơ sở dữ liệu này tồn tại, nên hacker cũng chẳng có cơ hội nào để tấn công nó. Blockchain được lưu trữ bởi hàng triệu máy tính cùng lúc, dữ liệu của nó có thể truy cập bởi bất cứ ai trên Internet.

* + 1. **Tính bền vững**

Công nghệ blockchain giống như Internet vì nó có một sức mạnh được tích hợp sẵn. Bằng cách lưu trữ những khối thông tin giống nhau trên mạng lưới của mình, blockchain không thể:

* Bị kiểm soát bởi bất kỳ một thực thể nào
* Không có điểm thiếu sót, lỗi duy nhất nào.

Bitcoin được phát hành vào năm 2008, kể từ đó, blockchain Bitcoin được vận hành, hoạt động mà không có sự gián đoạn đáng kể nào. Đến này, bất kỳ vấn đề nào liên quan đến Bitcoin là do hack hoặc quản lý kém. Nói cách khác, những vấn đề này đến từ ý định xấu và lỗi của con người, không phải là những sai sót tự thân của Bitcoin.

Internet đã chứng minh được độ bền trong gần 30 năm. Đây là bản ghi theo dõi tốt cho công nghệ blockchain khi nó tiếp tục được phát triển.

* + 1. **Minh bạch và không bị phá vỡ**

Mạng lưới blockchain tồn tại trong trạng thái của sự thỏa thuận, tự động kiểm tra 10 phút một lần. Một loại hệ sinh thái tự kiểm soát giá trị kỹ thuật số, mạng lưới sẽ điều hòa mọi giao dịch xảy ra trong khoảng 10 phút. Mỗi nhóm giao dịch này được gọi là khối. Hai đặc tính quan trong được rút ra từ đây:

* Minh bạch: Dữ liệu được nhúng trong mạng như một khối, công khai.
* Nó không bị thể bị hỏng: Khi thay đổi bất kỳ đơn vị thông tin nào trên blockchain có nghĩa là sử dụng một lượng lớn máy tính để ghi đè lên toàn bộ mạng.

Về lý thuyết, điều này có thể xảy ra. Trong thực tế, nó không xảy ra. Ví dụ, việc kiểm soát hệ thống để chiếm lấy Bitcoin sẽ khiến giá trị của nó bị hủy hoại.

* + 1. **Một mạng lưới các nút**

Một mạng lưới các nút tính toán tạo thành blockchain. Nút ở đây là máy tính được kết nối với mạng blockchain, sử dụng client để thực hiện nhiệm vụ xác nhận và chuyển tiếp các giao dịch. Nút sẽ nhận được một bản sao của blockchain, được tải tự động khi tham gia mạng lưới blockchain.

Các nút này cùng nhau tạo ra một mạng lưới cấp 2 mạnh mẽ, một góc nhìn hoàn toàn khác về cách mà Internet có thể hoạt động. Mỗi nút là một "quản trị viên" của mạng blockchain và tự động tham gia vào mạng, động lực cho việc tham gia này chính là cơ hội giành được Bitcoin.

Nút còn được gọi là [đào Bitcoin](https://quantrimang.com/huong-dan-dao-bitcoin-cho-nguoi-moi-bat-dau-136592), nhưng thuật ngữ này có chút nhầm lẫn. Trong thực tế, mỗi người đang cạnh tranh để giành Bitcoin bằng cách giải quyết những câu đố. Bitcoin là "lẽ sống" của blockchain ngay từ khi nó được hình thành. Bitcoin mới chỉ được công nhận như một phần rất nhỏ trong số những tiềm năng của công nghệ blockchain.

Có khoảng 700 loại tiền kỹ thuật số tương tự như Bitcoin, ngoài ra còn có rất nhiều những biến thể của khái niệm blockchain ban đầu hiện đang hoạt động hoặc đang được phát triển.

* + 1. **Tăng cường bảo mật**

Nhờ lưu trữ dữ liệu trên mạng của mình, blockchain loại bỏ những rủi ro đi kèm với dữ liệu được tổ chức tập trung. Mạng của nó không có những điểm dễ bị tổn thương.

Trong khi đó, vấn đề bảo mật trên Internet thì ngày càng trở nên phức tạp. Chúng ta đều dựa vào hệ thống username/password để bảo vệ danh tính và tài sản của mình trên mạng, nhưng hệ thống này vẫn có nhiều khả năng bị phá vỡ.

Phương pháp bảo mật của blockchain sử dụng công nghệ mã hóa với cặp khóa public/private. Khóa public (một chuỗi dài các số ngẫu nhiên) là địa chỉ của người dùng trên blockchain.

Bitcoin gửi qua mạng sẽ được ghi nhận thuộc về địa chỉ đó. Khóa private giống như [mật khẩu](https://quantrimang.com/s/?q=m%E1%BA%ADt+kh%E1%BA%A9u), cho phép chủ sở hữu truy cập vào Bitcoin hoặc các tài sản kỹ thuật số khác. Lưu trữ dữ liệu trên blockchain và nó sẽ không bị hư hỏng.

Điều này là sự thật, mặc dù bảo vệ tài sản kỹ thuật số của bạn sẽ yêu cầu bảo mật khóa private bằng cách in ra, tạo ví kỹ thuật số để đựng giống như ví đựng tiền giấy.

* 1. **Các phiên bản của Blockchain**

Hiện tại **Blockchain** có 3 phiên bản dưới đây:

* **Blockchain 1.0** – Tiền tệ và Thanh toán: Ứng dụng chính của phiên bản này là tiền mã hoá: bao gồm việc chuyển đổi tiền tệ, kiều hối và tạo lập hệ thống thanh toán kỹ thuật số. Đây cũng là lĩnh vực quen thuộc với chúng ta nhất mà đôi khi khá nhiều người lầm tưởng Bitcoin và Blockchain là một.
* **Blockchain 2.0** – Tài chính và Thị trường: Ứng dụng xử lý tài chính và ngân hàng: mở rộng quy mô của Blockchain, đưa vào các ứng dụng tài chính và thị trường. Các tài sản bao gồm cổ phiếu, chi phiếu, nợ, quyền sở hữu và bất kỳ điều gì có liên quan đến thỏa thuận hay hợp đồng.
* **Blockchain 3.0** – Thiết kế và Giám sát hoạt động: Đưa Blockchain vượt khỏi biên giới tài chính, và đi vào các lĩnh vực như giáo dục, chính phủ, y tế và nghệ thuật. Ở những lĩnh vực này sẽ là lại có nhiều loại như physical, digital hay human in nature.
  1. **Phân loại Blockchain**
     1. **Public Blockchain**

Public Blockchain là mạng Blockchain mà bất kỳ ai cũng có thể đọc và thực hiện giao dịch. Tất cả các máy tính trong mạng đều tham gia vào quá trình xác nhận giao dịch. Tấn công vào loại mạng Blockchain hoặc thay đổi dữ liệu tùy ý là không thể vì cơ chế khuyến khích, sự đồng thuận phân tán của toàn bộ mạng cũng như chi phí tính toán cao. Ví dụ: Bitcoin, Ethereum là hai mạng thuộc loại Public Blockchain tiêu biểu nhất

* + 1. **Private Blockchain**

Không giống như Public Blockchain, trong Private Blockchain quyền đọc dữ liệu có thể được công khai cho mọi người hoặc giới hạn trong một nhóm người tham gia hoặc không cho phép người dùng đọc dữ liệu trong một số trường hợp, đặc biệt là không có quyền. ghi dữ liệu vì đây thuộc về một tổ chức bên thứ ba đáng tin cậy. Là một Private Blockchain, thời gian xác nhận giao dịch khá nhanh vì chỉ cần một số lượng nhỏ thiết bị để xác thực giao dịch, tùy thuộc vào cấu hình mạng Blockchain ban đầu.

* + 1. **Consortium Blockchain**

Đây là mô hình Blockchain được kết hợp giữa Public Blockchain và Private Blockchain để tận dụng tối đa lợi thế và hạn chế các điểm yếu của hai loại Blockchain. Quyền đọc dữ liệu trên Blockchain của Consortium tương đối giống với Public Blockchain. Nhưng quy trình chấp thuận sẽ được quyết định bởi nhiều tổ chức đáng tin cậy hoặc bởi một nhóm người được chỉ định. Ví dụ: Các ngân hàng hay tổ chức liên doanh sẽ sử dụng Blockchain cho riêng mình, Ripple là một trong những mạng nổi bật.

* 1. **Blockchain có thể được dùng ở đâu?**
     1. **Hợp đồng thông minh**

Ở cấp độ phát triển hiện tại của công nghệ, hợp đồng thông minh có thể được lập trình để thực hiện những chức năng đơn giản. Ví dụ, một giao dịch phát sinh có thể được thanh toán khi công cụ tài chính đáp ứng một số tiêu chuẩn, với việc sử dụng công nghệ blockchain và Bitcoin cho phép thanh toán tự động, không cần sự tham gia của con người hay bên trung gian làm chứng.

* + 1. **Quản trị**

Bằng cách tạo ra những kết quả minh bạch và có thể truy cập công khai, công nghệ cơ sở dữ liệu phân tán có thể mang lại sự minh bạch đầy đủ cho cuộc bầu cử hay bất cứ hình thức thăm dò nào khác. Những hợp đồng thông minh dựa trên Ethereum sẽ giúp tự động hóa toàn bộ quá trình.

* + 1. **Kiểm tra chuỗi cung ứng**

Người tiêu dùng ngày càng muốn biết rằng có bao nhiêu phần trăm sự thật trong những tuyên bố về tiêu chuẩn sản phẩm của các công ty. Blockchain cung cấp cách thức xác nhận dễ dàng rằng những sản phẩm chúng ta mua là chính hãng. Tính minh bạch đi kèm với dấu thời gian dựa trên blockchain của ngày tháng, vị trí - ví dụ, trên viên kim cương, sẽ tương ứng với số sản phẩm.

* + 1. **Quản lý danh tính**

Nhu cầu xác thực danh tính trên web ngày càng trở nên bức thiết, nhất là đối với những giao dịch tài chính trực tuyến. Những giải pháp hiện có để phục vụ nhu cầu này chưa thực sự hoàn hảo. Với blockchain, chúng ta sẽ có những phương pháp nâng cao để chứng minh mình là ai, cùng với khả năng số hóa tài liệu cá nhân. Như trên đã nói, trong nền kinh tế chia sẻ hay các giao dịch kinh doanh, một danh tính tốt là vô cùng quan trọng.

* + 1. **Giao dịch chứng khoán**

Khả năng của blockchain trong thị trường chứng khoán đang được kiểm tra mạnh mẽ. Khi thực hiện ngang hàng, xác nhận giao dịch trở nên gần như tức thời. Nhờ vậy, những khâu trung gian như kiểm toán viên, người lưu ký,... có thể được loại bỏ.

* 1. **Những bất lợi khi sử dụng Blockchain**

Blockchain không phải là một phép màu hay toàn là những điều quyến rũ, nó cũng có những trở ngại nhất định mà trong tương lai gần chúng ta cần phải khắc phục.

Những quảng cáo hoặc lời thổi phồng xung quanh blockchain có thể khiến nhiều người mù quáng, không nhận ra sự thật rất rõ ràng rằng, blockchain tồn tại những bất lợi khi sử dụng khiến các ngành công nghiệp phải tìm cách giảm thiểu nó trước khi có thể áp dụng trên quy mô lớn.

* + 1. **Rất tốn điện**

Vì mỗi blockchain đã sao chép chính mình đến mọi nút trên blockchain nên đã tạo ra một số lượng lớn những sự dư thừa. Mỗi lần giao dịch Bitcoin được thực hiện, nó được xác nhận nhiều lần vì có nhiều nút trên mạng. Quy trình này sử dụng rất nhiều điện. Các blockchain tư nhân có thể không bị ảnh hưởng nhiều vì họ có thể giới hạn các blockchain đến một số ít máy tính. Tuy nhiên, nếu là ngân hàng, phải xử lý hàng nghìn giao dịch mỗi phút trên toàn cầu, thì đây sẽ là vấn đề lớn.

* + 1. **Tốn không gian lưu trữ**

Ngay bây giờ, để vận hành một nút trên blockchain Bitcoin, bạn phải tải xuống 60GB dữ liệu.

Sẽ như thế nào nếu dữ liệu là **1 Terabyte (1 TB)?**

Nếu thị trường Bitcoin phát triển mạnh, sẽ có nhiều blockchain với dung lượng hàng Terabyte xuất hiện trong thực tế. Khi đó, chỉ có các trang trại máy chủ và những người thực sự quan tâm đến việc thương mại hóa tiền kỹ thuật số quy mô lớn, mới có thể vận hành toàn bộ các nút.

Điều này sẽ tạo ra một mạng lưới tập trung, vốn được coi là một sự phân quyền kỳ lạ.

* + 1. **Nhược điểm của tính không thể bị phá vỡ**

Giả sử bạn có một chiếc ví trên mạng, bạn bị mất chìa khóa chứng thực để mở ví đó. Không có liên kết để reset mật khẩu, không có hotline hỗ trợ.

**Bạn mất toàn bộ số tiền trong ví. Không có sự thu hồi.**

* **Bạn Mất trắng.**

Nếu đặt một thứ gì đó lên blockchain, phải thật chắc chắn là mình sẽ không hối hận. Vì giao dịch một khi được thực hiện sẽ không thể đảo ngược, hay làm lại.

Nó sẽ ở trên blockchain **mãi mãi**, theo đúng nghĩa đen luôn.

**CHƯƠNG III: ỨNG DỤNG CỦA BLOCKCHAIN**

**Blockchain** được ứng dụng lần đầu tiên vào Bitcoin và sau này nó được sử dụng rộng rãi trong lĩnh vực tiền điện tử (Cryptocurrency), nhưng hiện tại Blockchain đã được ứng dụng trong hầu hết các ngành công nghiệp khác nhau.

* 1. **Trong thương mại điện tử**
* **Warranteer**: Là một ứng dụng blockchain cho phép người tiêu dùng dễ dàng truy cập thông tin về sản phẩm họ đã mua và nhận hỗ trợ dịch vụ trong trường hợp có trục trặc sản phẩm.
* **Blockpoint**: Là một ứng dụng đơn giản hóa việc tạo ra các hệ thống thanh toán và chấp nhận ví điện tử, chương trình khách hàng thân thiết, thẻ quà tặng và các chức năng khác.
* **Loyyal**: Được hỗ trợ bởi công nghệ blockchain và hợp đồng thông minh, nền tảng dịch vụ khách hàng thân thiết và tích điểm thưởng này tạo ra nhiều chương trình tùy chỉnh hơn, cho phép khách hàng tích điểm thưởng từ nhiều thương hiệu khác nhau.
  1. **Trong dịch vụ tài chính, ngân hàng**
* **Bitcoin Atom**: Là một nhánh mới của Bitcoin cho phép trao đổi tiền mã hóa dễ dàng mà không tốn phí giao dịch và không thể bị tấn công khi giao dịch, khiến Bitcoin thực sự được phân cấp lại. Công nghệ này dựa trên các hoán đổi nguyên tử (atomic swaps) – được xem là một công cụ vô giá để trao đổi các đồng tiền mã hóa và không cần phải có một bên thứ ba đáng tin cậy. Nhưng hiện tại, việc áp dụng rộng rãi các giao dịch hoán đổi nguyên tử đã bị ngăn chặn vì chúng đòi hỏi phải có kỹ năng kỹ thuật cao; Bitcoin Atom có thể giải quyết vấn đề này một phần nào đó.
* **Aeternity**: Là một nền tảng blockchain có khả năng mở rộng cao này có thể được sử dụng cho bất kỳ ứng dụng nào yêu cầu tốc độ giao dịch cao, bao gồm các hợp đồng thông minh được tạo ra từ các thanh toán chuỗi, nano và vi mô.
* **Ripple**: Ripple nhắm đến việc trở thành một nhà cung cấp giải pháp thanh toán toàn cầu bằng cách kết nối ngân hàng, nhà cung cấp dịch vụ thanh toán, doanh nghiệp và các giao dịch tài sản kỹ thuật số, cho phép giải quyết ngay tức thì, theo nhu cầu trên toàn cầu
* **Securrency**: Đây là một nền tảng giao dịch tiền mã hóa và một vài loại tài sản, bao gồm cả những tài sản không hoán đổi thành tiền mặt, được trao đổi thông qua token của Securrency. Dự án cho phép tiền mã hóa được giao dịch bên ngoài các giao dịch chuyên dụng của chúng.
* **ABRA**: Là một ứng dụng toàn cầu và ví tiền mã hóa cho phép bạn mua, đầu tư và trữ 20 loại tiền mã hóa, bao gồm Bitcoin, ethereum, litecoin…
  1. **Trong nông nghiệp**
* **Food industry**: Là ứng dụng Blockchain có thể cải thiện tính minh bạch và hiệu quả trong việc tìm ra những loại thực phẩm có thể bị ô nhiễm và ở đâu trong suốt chuỗi cung ứng.
* **OriginTrail**: Là một nền tảng blockchain cho phép người tiêu dùng biết hàng hóa thực phẩm mà họ mua đến từ đâu và cách chúng được sản xuất.
  1. **Trong giáo dục, y tế**
* **MedRec**: Để cung cấp cho bất kỳ nhà cung cấp dịch vụ y tế truy cập an toàn vào hồ sơ của bệnh nhân, MedRec sử dụng blockchain để tiết kiệm thời gian, tiền bạc và các quy trình lặp lại trong việc tiến hành thủ tục giữa các cơ sở và nhà cung cấp khác nhau. Bệnh nhân cũng có thể truy cập vào hồ sơ y tế của họ để nghiên cứu các đơn vị cung cấp dịch vụ y tế.
* **MedicalChain**: Là công ty trong lĩnh vực chăm sóc sức khỏe đầu tiên sử dụng công nghệ blockchain để tạo thuận lợi trong việc lưu trữ và sử dụng hồ sơ y tế điện tử để cung cấp trải nghiệm y học từ xa (telemedicine) hoàn chỉnh. Họ là các bác sĩ thực tế trong hệ thống chăm sóc sức khỏe của Anh và muốn thay đổi hệ thống này từ bên trong.

**CHƯƠNG IV: KẾT LUẬN**

Một số chuyên gia đã đưa ra danh sách dài những điểm tương đồng giữa hai thời đại và hai hiện tượng, một số chuyên gia lại cảnh báo rằng blockchain có thể sẽ có kết cục giống như bong bóng dot com vào năm 1999, sau đó mới đạt đến thời điểm chín muồi khi nó được chấp nhận rộng rãi. Điều này có nghĩa rằng, blockchain tạo điều kiện cho những tài sản bị định giá quá cao, có thể gây ra sự điều chỉnh thị trường trong tương lai, làm ảnh hưởng đến nhiều công ty và toàn bộ ngành.

Chúng ta không biết trước tương lai sẽ như thế nào, nhưng bất chấp sự thay đổi, khủng hoảng từ năm 1999, Internet đã không biến mất, nó vẫn tiếp tục con đường của mình bằng cách định hình toàn bộ ngành công nghiệp. Điều tương tự rất có thể cũng sẽ xảy ra với công nghệ blockchain.

Blockchain thực sự có thể biến đổi thị trường, vì chúng ta có thể kiểm soát được mọi giao dịch, hợp đồng hoặc bất kỳ sự di chuyển nào trong mạng. Chúng ta có thể làm cho các giao dịch và quy trình P2P trở nên minh bạch, được bảo mật với sự trợ giúp của mật mã, có dấu thời gian và dễ theo dõi. Điều này khác với Internet ngày nay, nơi các trung gian đóng vai trò quan trọng. Các công ty như Facebook, Google, chính phủ, ngân hàng, công ty công nghệ cao đều là những trung gian ảnh hưởng đến thông tin và quy trình trong mạng Internet. Blockchain loại bỏ những trung gian như vậy vì lợi ích của tất cả mọi người.

 Có thể thấy ứng dụng của Blockchain dường như là không có giới hạn. Trong năm 2018, blockchain là chủ đề nóng hổi trên các diễn đàn, hội nghị, hội thảo được tổ chức tại Việt Nam. Tại các hội nghị, diễn đàn, hội thảo, nhiều chuyên gia đã trình bày về khả năng ứng dụng của blockchain trong các lĩnh vực như truy xuất nguồn gốc nông sản (ví dụ của Hợp tác xã xoài Vĩnh Xương), vận chuyển (nghiên cứu ứng dụng của VnPost), bệnh án điện tử (nghiên cứu của Trung tâm Công nghệ lõi Viettel)   Điều này cho thấy sức hút của Blockchain đối với Chính phủ, các nhà đầu tư, doanh nghiệp, các nhà sáng lập của Việt Nam, …

**TÀI LIỆU THAM KHẢO**

[1] <https://toiyeubitcoin.com/blockchain-la-gi/#Blockchain_la_gi>

[2]<https://quantrimang.com/blockchain-la-gi-bong-bong-hay-cuoc-cach-mang-thuc-su-sau-internet-143099>

[3]<http://aita.gov.vn/tong-quan-ung-dung-cua-cong-nghe-blockchain-doi-voi-cac-nganhnghe>