***Blockchain là nền tảng cho sự ra đời của các hợp đồng thông minh.***

**https://vi.wikipedia.org/wiki/Blockchain**

**https://viblo.asia/p/tim-hieu-ve-cong-nghe-blockchain-cac-ung-dung-cua-cong-nghe-chuoi-khoi-blockchain-RQqKLkoO57z**

[**https://coin98.net/blockchain-101**](https://coin98.net/blockchain-101)

**CÁC THUẬT TOÁN BLOCKCHAIN PHỔ BIẾN.**

**1. Proof of Work (PoW):**

* [**Proof of Work**](https://coin98.net/proof-of-work-pow)là bằng chứng công việc. Trong cơ chế đồng thuận này, các thợ đào (miner) sẽ dùng sức mạnh máy tính để giải các bài toán tạo ra mã hash. Sau khi giải xong, họ sẽ giành được quyền xác thực giao dịch và tạo khối mới trong blockchain.
* Đây là cơ chế đồng thuận đầu tiên và gắn liền với Bitcoin (BTC), Ethereum (ETH),...

Dồn các con số vào Một HASH để làm cho nó trở nên khó giải hơn

**2. Proof of Stake (PoS):**

* [**Proof of Stake**](https://coin98.net/proof-of-stake-la-gi) là bằng chứng cổ phần. Cơ chế đồng thuận này sẽ không có các miner thợ đào như PoW, thay vào đó những người tham gia xác thực giao dịch sẽ phải đặt cược (stake) lượng coin lớn để giành quyền xác thực giao dịch và tạo khối. Do đó, PoS không yêu cầu phải đầu tư nhiều máy đào đắt tiền.
* Một số dự án sử dụng cơ chế này: Cosmos (ATOM), Binance Coin (BNB), Ontology (ONT),...

**3. Delegated Proof of Stake (DPoS):**

* Delegated Proof of Stake là bằng chứng ủy quyền cổ phần. Thay vì phải đặt cược để xác thực giao dịch như PoS, những người nắm giữ token sẽ tiến hàng bỏ phiếu cho một nhóm được chọn để thực hiện vai trò xác nhận các giao dịch.
* DPoS giúp đảm bảo sự trung thực và công bằng bằng việc thực hiện các hoạt động bỏ phiếu liên tục và cũng liên tục xáo trộn trong hệ thống, để đảm bảo những người được chọn là trung thực và có trách nhiệm.
* Một số dự án sử dụng cơ chế này là: Bitshares (BTS), EOS (EOS), LISK (LSK), ICON (ICX), Cybermiles (CMT),...

**4. Byzantine Fault Tolerance (BFT):**

* [**Byzantine Fault Tolerance**](https://coin98.net/byzantine-la-gi) là thuật toán đồng thuận chống gian lận trên Blockchain. Thuật toán này cho phép những người thực hiện xác minh quản lý mỗi trạng thái của một chuỗi, đồng thời chia sẻ các thông điệp với một chuỗi khác, để có được những bản ghi giao dịch chính xác và đảm bảo sự trung thực.
* Một số dự án sử dụng thuật toán BFT là: NEO (NEO), Ripple (XPR), Stellar (XLM),...

**5. Proof of Authority (PoA):**

* [**Proof of Authority**](https://coin98.net/proof-of-authority-poa-la-gi) là thuật toán đồng thuận dựa trên danh tiếng. Những người xác thực khối sẽ không được dựa trên số lượng coin họ nắm giữ, mà sẽ dựa trên chính danh tiếng của mình. Chính vì vậy, các blockchain PoA được bảo mật bởi các node xác thực được lựa chọn tùy ý như là các thực thể đáng tin cậy.
* Một số dự án tiêu biểu sử dụng thuật toán BFT là: MakerDAO (xDAI), ZINC (ZINC),...

**6. Proof of Weight (PoWeight):**

* Proof of Weight là thuật toán đồng thuận base theo thuật toán đồng thuận [**Algorand**](https://coin98.net/algorand-algo).
* Ý tưởng của nó cũng giống PoS đó là cũng dựa vào số lượng token nắm dữ trong mạng sẽ tương đương với phần trăm xác suất tạo đc ra block tiếp theo cơ chế tính của hệ thống PoWeight kèm với một vài giá trị khác được sử dụng.
* Một số dự án tiêu biểu sử dụng thuật toán PoWeightlà: Algorand (ALGO), Filecoin (FIL),...

**7. Proof of History (PoH):**

* Proof of Historylà thuật toán đồng thuận xác minh thứ tự và thời gian giữa các giao dịch. Cơ chế này được xây dựng để giải quyết vấn đề về thời gian trong các mạng phi tập trung ở nơi không có cùng mốc thời gian.
* Dự án tiêu biểu sử dụng thuật toán PoH là: Solana (SOL),...

**8. Proof of Reputation (PoR):**

* Proof of Reputation là cơ chế đồng thuận dựa vào uy tín của các bên tham gia để giữ cho mạng an toàn. Một bên tham gia xác thực block phải đủ uy tín, để nếu họ cố tình gian lận thì uy tín của họ sẽ bị ảnh hưởng.
* Đây là khái niệm tương đối trừu tượng vì hầu hết các công ty tham gia vào hệ thống nếu gian lận sẽ bị ảnh hưởng đến danh tiếng, những công ty lớn sẽ thiệt hại nhiều hơn.
* Một số dự án tiêu biểu sử dụng thuật toán PoR là: GoChain Coin (GO),...

**XU HƯỚNG CÔNG NGHỆ BLOCKCHAIN.**

* Công nghệ Blockchain được tin tưởng hơn: Vì có sự can thiệp của nhà nước nên Blockchain hứa hẹn sẽ giảm bớt các vụ lừa đảo, dối trá.
* Bitcoin và các loại tiền ảo khác vẫn tiếp tục phát triển: Dù có nhiều tin đồn không hay nhưng vẫn có nhiều nhà đầu tư tin vào sự phát triển của các loại tiền ảo, nhất là Bitcoin.
* Mở rộng tính ứng dụng: Bên cạnh lĩnh vực tài chính thì công nghệ Blockchain còn có tiềm năng được ứng dụng vào hoạt động quản lý nhà nước, bầu cử và các ngành khác.
* Sự bùng nổ của game blockchain: Sự thú vị của các trò chơi được xây dựng trên nền tảng Blockchain ngày càng thu hút nhiều nhà đầu tư.

**BLOCKCHAIN LÀ CÔNG NGHỆ CHUỖI – KHỐI, CHO PHÉP TRUYỀN TẢI DỮ LIỆU MỘT CÁCH AN TOÀN DỰA TRÊN HỆ THỐNG MÃ HÓA VÔ CÙNG PHỨC TẠP.**

Nếu bạn vẫn chưa hiểu thì có thể hình dung blockchain nó giống như cái history mình thường thấy trong Git. Mỗi một commit chính là một block. Ta có thể dễ dàng xem được các commit cũ, cũng như track xem ai đã làm gì trên source code của mình, blockchain cũng y xì vậy thôi.

Điểm khác biệt và cũng là tinh hoa của blockchain đó là nó ko nằm 1 nơi như Git (các git server), mà được phân tán thành nhìu nơi (nhiều node), và tất cả là ngang hàng. Chính vì vậy mỗi một thay đổi trên 1 node phải được sự đồng thuận của cả mạng (tất cả các node). Ngoài ra còn có mấy khái niệm như Proof of Work, Stack of Work nhưng mình xin được bỏ ra vì tính chất nặng về kỹ thuật nên không hợp trong bài note này.

**CÁCH ĐỂ HOẠT ĐỘNG.**

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.

**MỖI BLOCK BAO GỒM.**

Depend on types of Blockchain.

DATA: sender, receiver, amount of coin

HASH = fingerprint = token: changing something inside the block will cause the hash to change

PREVIOUS HASH

FIRST BLOCK CALLED GENESIS BLOCK.

**NGUYÊN LÝ MÃ HÓA.**

Hệ thống blockchain được thiết kế theo cách không yêu cầu sự tin cậy và bảo đảm bởi độ tin cậy có được thông qua các hàm mã hóa toán học đặc biệt.​Để có thể thực hiện các giao dịch trên blockchain, bạn cần một phần mềm sẽ cho phép bạn lưu trữ và trao đổi các đồng Bitcoin của bạn gọi là ví tiền điện tử. Ví tiền điện tử này sẽ được bảo vệ bằng một phương pháp mã hóa đặc biệt đó là sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key).

Nếu một thông điệp được mã hóa bằng một khóa công khai cụ thể thì chỉ chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp.

Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư, có nghĩa là bạn đang tạo ra một chữ ký điện tử được các máy tính trong mạng lưới blockchain sử dụng để kiểm tra chủ thể gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và là sự kết hợp của yêu cầu giao dịch và khóa riêng tư của bạn.

* Chuỗi khối (blockchain)
* Thuật toán đồng thuận hay cơ chế phân tán đồng đẳng (Distributed)
* Tính toán tin cậy (trusted computing)
* Hợp đồng thông minh (smart contracts)
* Bằng chứng công việc (proof of work).

**CÁC ỨNG DỤNG THỰC TIỄN CỦA BLOCKCHAIN TRONG CUỘC SỐNG.**

Triển khai các giải pháp **Blockchain** trên nền tảng đám mây sẽ giúp các nhà cung cấp dịch vụ truyền thông tối ưu hóa các quy trình hiện có trong khi tăng cường bảo mật mạng, rà soát lại toàn bộ quy trình vận hành, các quy trình như chuyển vùng và quản lý danh tính trong mô hình kinh doanh của mình. Từ đó cải thiện và phát triển dịch vụ tốt hơn.

**Một số ứng dụng của Blockchain trong lĩnh vực truyền thông và viễn thông:**

* Phòng chống gian lận trong chuyển vùng: các thỏa thuận chuyển vùng giữa các nhà khai thác sẽ trở nên minh bạch, các nút được chỉ định có thể đóng vai trò là trình xác nhận (người khai thác) để xác minh từng giao dịch được phát trên mạng.
* Quá trình chuyển đổi [**5G**](https://vi.wikipedia.org/wiki/5G): các quy tắc và thỏa thuận giữa các mạng khác nhau sẽ có dạng hợp đồng thông minh, tự thực hiện có thể kết nối các thiết bị với nhà cung cấp dịch vụ gần nhất đồng thời đánh giá sự liên tục của kết nối và tính phí dịch vụ.
* Kết nối [**Internet vạn vậ**](https://vi.wikipedia.org/wiki/Internet_V%E1%BA%A1n_V%E1%BA%ADt)t: tạo ra một môi trường an toàn hơn để truyền dữ liệu bằng cách tạo các mạng lưới tự quản ngang hàng an toàn cao

Trong quá trình sản xuất, chúng ta cần một sổ cái để theo dõi quá trình sản xuất, tồn kho, phân phối, chất lượng, thông tin giao dịch … Blockchain sẽ thay thế các thiết bị thông minh cấp quyền quản lý, nâng cao hiệu quả và tăng đáng kể năng suất của quản lý chuỗi cung ứng quá trình.

Đối với người tiêu dùng, việc kiểm tra được tính xác thực của thông tin sản phẩm có thể ngăn chặn được hàng giả, hàng kém chất lượng trên thị trường.

**Một số ứng dụng của Blockchain trong sản xuất:**

* Theo dõi lịch trình sản xuất, số lượng hàng mua vào và bán ra.
* Quản lý hàng tồn kho, kho bãi sản xuất.
* Truy xuất nguồn gốc sản phẩm được sản xuất qua các khâu.
* Theo dõi nguồn cung cấp nguyên liệu sản xuất trong công nghiệp.

Trong thời đại công nghệ 4.0, các nước trên thế giới và Việt Nam đang đẩy mạnh triển khai số hóa thông tin trong quy trình quản lý dữ liệu trong đó có lĩnh vực y tế và chăm sóc sức khỏe. Blockchain được sử dụng trong quản lý tài sản và lưu trữ thông tin sức khỏe của bệnh nhân, quản lý hàng tồn kho, đơn đặt hàng, thanh toán thiết bị y tế và thuốc. Mặc dù có nhiều thiết bị thông minh có thể giám sát các dịch vụ này nhưng vẫn có nhiều hạn chế trong việc bảo mật thông tin cá nhân của bệnh nhân. Do đó, Blockchain là sự lựa chọn hàng đầu.

**Một số ứng dụng của Blockchain trong lĩnh vực y tế:**

* Ứng dụng phát triển bao gồm theo dõi và quản lý bệnh lý (như thuốc thông minh, thiết bị đeo có thể đo các chỉ số về sức khỏe và đưa ra phản hồi) và tăng cường quản lý chất lượng.
* Quản lý chuỗi cung ứng thuốc, thiết bị y tế: Theo dõi đầu vào, nguồn gốc, hạn sử dụng của các vật tư y tế.
* Tăng cường tính minh bạch và tự động hóa trong các giao dịch khám chữa bệnh; xuất xứ xét nghiệm lâm sàng; quyền sở hữu dữ liệu sức khỏe của bệnh nhân.

Khi Blockchain được ứng dụng vào giáo dục, thông tin lưu trữ trên Blockchain không chỉ là dữ liệu bảng điểm mà còn là quá trình đào tạo, kinh nghiệm thực tế và kinh nghiệm tuyển dụng của mỗi người. Tránh tình trạng ứng viên gian lận trong quá trình xin học bổng, thăng tiến, v.v …; trình bày sai về trình độ học vấn, kinh nghiệm làm việc, kỷ luật, v.v.

Không chỉ vậy, thông qua chức năng hợp đồng thông minh, Blockchain còn có thể tự động thực hiện các điều khoản của nội quy đào tạo, xử lý các trường hợp vi phạm nội quy, cải thiện các hạn chế trong quá trình giảng dạy khi cần thiết và học viên có thể đưa ra phản hồi.

**Một số ứng dụng của Blockchain trong lĩnh vực giáo dục:**

* Hệ thống quản lý mức độ đánh giá sự uy tín trong nghiên cứu khoa học.
* Ghi lại cơ sở dữ liệu bảo mật về dữ liệu học tập và điểm số cho các hệ thống học trực tuyến, đánh giá năng lực của một cá nhân dựa trên các yêu cầu tuyển sinh đầu vào.
* Theo dõi và lưu trữ bảng điểm và bằng cấp của sinh viên và thông tin của các đơn vị đào tạo.
* Xem xét cá nhân/ứng viên có phù hợp với công việc giảng dạy hay không, từ đó đưa ra quyết định mời cá nhân đó làm việc.

Do đặc thù của ngành tài chính ngân hàng rất dễ xảy ra tình trạng tập trung quyền lực, xâm phạm bảo mật dữ liệu người dùng nên với công nghệ Blockchain hiện nay, những vấn đề này sẽ dễ dàng được giải quyết. Nhờ chức năng hợp đồng thông minh, nó có thể bỏ qua các bên trung gian, tiết kiệm chi phí, tăng tốc độ giao dịch, hạn chế rủi ro tài chính trong quá trình thanh toán và cải thiện hệ thống quản lý thông tin công nghệ cũ.

**Một số ứng dụng của Blockchain trong lĩnh vực tài chính & ngân hàng:**

* Xác thực thông tin khách hàng, khả năng tín dụng: Cho phép giao dịch ngay cả không có trung gian xác minh.
* Mạng lưới sẽ xác minh và thanh toán những giao dịch ngang hàng, công việc này được thực hiện liên tục nên sổ cái luôn được cập nhật.
* Quản lý rủi ro, hạn chế rủi ro trong thanh toán vì trục trặc kỹ thuật, vỡ nợ trước khi thanh toán giao dịch.
* Hệ thống quản lý thông minh: Blockchain cho phép liên tục đổi mới, lặp lại và cải tiến, dựa trên sự đồng thuận trong mạng lưới.

Vấn đề nan giải nhất đối với các nhà bán lẻ là quá trình phân phối hàng hoá, kho bãi cũng như quản lý thông tin sản phẩm số lượng lớn. **Blockchain** được ứng dụng như một cuốn sổ cái ghi chép thông tin chính xác với tính bảo mật cao. Nó cho phép quản lý hồ sơ về từng mặt hàng, vị trí của nó, cách xử lý, mọi thiệt hại trong quá trình phân phối, từ đó hỗ trợ hiệu quả cho các nhà bán lẻ.

**Ứng dụng của Blockchain trong lĩnh vực bán lẻ:**

* Theo dõi các mặt hàng sản xuất qua từng mã định danh lưu trên hệ thống Blockchain.
* Hợp đồng thông minh: khi có sự trao đổi hàng hóa giữa nhà sản xuất và công ty vận tải, cả hai đều đồng ý rằng mặt hàng đó đảm bảo chất lượng.
* Quản lý thông tin mặt hàng, thời gian vận chuyển, lưu kho, tồn kho.
* Hợp đồng thông minh trên Blockchain chứa đựng các thỏa thuận giữa các thực thể này để quản lý dòng tiền của các giao dịch hoặc xử lý thiệt hại khi cần thiết

Theo chuyên gia, thị trường bán lẻ hiện nay đang dần chuyển hướng sang thương mại trực tuyến đặc biệt là với sự phát triển của các sàn thương mại điện tử. Sự dịch chuyển này đặt ra vấn đề về tính bảo mật, quản lý chuỗi cung ứng, quá trình vận chuyển hàng hoá đến người tiêu dùng, chi phí từ cách làm truyền thống tạo nên nhiều rào cản giữa người tiêu dùng và nhà sản xuất.

**Một số ứng dụng của Blockchain trong lĩnh vực thương mại điện tử:**

* Quản lý thông tin dữ liệu khách hàng.
* Theo dõi thông tin, tình trạng sản phẩm thông qua [**số serial**](https://vi.wikipedia.org/wiki/S%E1%BB%91_x%C3%AAri), [**QR**](https://vi.wikipedia.org/wiki/M%C3%A3_QR).
* Xây dựng hệ thống thanh toán và chấp nhận ví điện tử, khách hàng thân thiết, thẻ quà tặng, tri ân khách hàng….
* Vận hành và quản lý chuỗi cung ứng

Chuỗi thực phẩm cần trở nên bền vững hơn để nâng cao lòng tin và sự trung thành của người tiêu dùng, và chìa khóa để nâng cao lòng tin là khả năng truy xuất nguồn gốc hiệu quả. Hệ thống sổ cái phân tán sẽ giúp nhà bán lẻ và người tiêu dùng lưu trữ thông tin giao dịch, đồng thời tăng tính minh bạch của thông tin trong suốt quá trình sản phẩm từ cơ sở sản xuất đến cơ sở chế biến. Nhà phân phối, siêu thị, cửa hàng bán lẻ và cuối cùng là người tiêu dùng.

Các dữ liệu liên quan tới quản lý chất lượng, quản lý giá cả, quản lý tài chính, quản lý bán hàng đều có thể được tiếp tục cập nhật vào trong chuỗi **Blockchain.**

**Một số ứng dụng của Blockchain trong lĩnh vực nông nghiệp:**

* Quản lý chuỗi cung ứng sản phẩm, chuỗi phân phối hàng tồn kho.
* Lưu trữ thông tin hàng hóa, quy trình chăm sóc, các tiêu chuẩn cho thực phẩm sạch.
* Truy xuất nguồn gốc, vòng đời sản xuất nông sản.

Thông tin khách hàng được chuyển đổi từ nhiều hệ thống từ khâu lựa chọn đại lý, đặt vé xe, đặt phòng khách sạn đến các địa điểm thăm quan, do đó đòi hỏi tính ổn định và bảo mật cao. Bên cạnh đó chi phí giao dịch cũng là yếu tố được cân nhắc trong quá trình khai thác ngành dịch vụ không khói này. **Blockchain** tham gia giải quyết các vấn đề trên, thay thế hệ thống quản lý truyền thống nhiều trục trặc, sai sót.

**Một số ứng dụng của Blockchain trong lĩnh vực du lịch:**

* Theo dõi hành lý, đặt phòng khách sạn, vé máy bay.
* Dịch vụ nhận dạng: Tiết kiệm thời gian cho quá trình check in tại các sân bay, khách sạn, địa điểm du lịch.
* Thanh toán đa dạng: Cho phép thanh toán đến từ nhiều ngân hàng toàn cầu, ví điện tử, tiền điện tử…
* Thông tin khách hàng thân thiết, khách VIP…

Trong vòng đời của một sản phẩm, qua mỗi bước trong chuỗi cung ứng, dữ liệu được tạo ra và được ghi lại dưới dạng các giao dịch, tạo ra lịch sử vĩnh viễn cho sản phẩm. **Blockchain** chính là công cụ để quản lý kho dữ liệu khổng lồ đó. **Blockchain** có thể giúp tăng tính hiệu quả trong việc chia sẻ thông tin về quá trình sản xuất, vận chuyển, bảo quản, sự hao mòn giá trị của sản phẩm tới các bên liên quan. Giải quyết những vấn đề thách thức trong [logistics](https://vi.wikipedia.org/wiki/H%E1%BA%ADu_c%E1%BA%A7n) như độ trễ trong giao nhận hàng, mất các giấy tờ, chứng từ, tài liệu, nguồn gốc sản phẩm không rõ ràng, cùng các lỗi khác trong quá trình chuyển giao giữa các thành viên trong chuỗi hoạt động logistics.

**Một số ứng dụng của Blockchain trong lĩnh vực vận tải và logistics :**

* Truy xuất nguồn gốc, xác thực giấy tờ minh bạch, rõ ràng.
* Đóng gói thông minh.
* Kết hợp trí tuệ nhân tạo (AI) và Internet vạn vật để giám sát hành trình vận chuyển cũng như các phương tiện vận chuyển.
* Giảm chi phí trung gian, tiết kiệm chi phí nhờ áp dụng hợp đồng thông minh.

**[Textbook]19-Architecture for blockchain applictions**

Blockchain làm gì để không thay đổi được vì nó là secure security?

Hash function:

* Unique hash (Mỗi Hash chỉ duy nhất có 1)
* Commitment (Ứng dụng của hash 🡪 Lời hứa, chắc chắn là sẽ bầu cử nhưng ẩn danh)
* Puzzle friendly (Tăng giảm độ khó của hash)