**1. Cấu trúc của khối Blockchain**

- Chuỗi khối là một công nghệ mới nổi đang được các ngành khác nhau áp dụng theo cách thức sáng tạo. Một số trường hợp sử dụng trong các ngành khác nhau:

**\* Năng lượng**

- Sử dụng công nghệ chuỗi khối để tạo ra các nền tảng giao dịch năng lượng ngang hàng và hợp lý hóa việc tiếp cận năng lượng tái tạo như những trường hợp sử dụng sau:

+ Các công ty năng lượng dựa trên chuỗi khối đã tạo ra một nền tảng giao dịch để các cá nhân mua bán điện. Quá trình được tự động hóa như đồng hồ đo thông minh tạo ra các giao dịch và chuỗi khối ghi lại những giao dịch này.

+ Với các sáng kiến huy động vốn cộng đồng dựa trên chuỗi khối, người dùng có thể tài trợ và sở hữu các tấm pin mặt trời trong những cộng đồng không có khả năng tiếp cận nguồn năng lượng.

**\*Tài chính**

+ Các hệ thống tài chính truyền thống, như ngân hàng và sàn giao dịch chứng khoán, sử dụng các dịch vụ chuỗi khối để quản lý các khoản thanh toán trực tuyến, tài khoản và giao dịch thị trường.

+ Bằng cách áp dụng chuỗi khối, họ đã giải quyết được nhiều thách thức, bao gồm xử lý hàng loạt và đối soát thủ công hàng nghìn giao dịch tài chính.

**\*Truyền thông và giải trí**

+ Các công ty trong lĩnh vực truyền thông và giải trí sử dụng hệ thống chuỗi khối để quản lý dữ liệu bản quyền. Xác minh bản quyền là rất quan trọng để các nghệ sĩ nhận được thù lao công bằng.

+ [Sony Music Entertainment Japan](https://www.forbes.com/sites/amazonwebservices/2019/11/19/how-sony-is-protecting-rights-of-digital-creators-using-blockchain-on-aws/) sử dụng các dịch vụ chuỗi khối để quản lý quyền kỹ thuật số hiệu quả hơn.

**\*Bán lẻ**

+ Các công ty bán lẻ sử dụng chuỗi khối để theo dõi sự lưu động của hàng hóa giữa nhà cung cấp và người mua.

+ Ví dụ: công ty bán lẻ Amazon đã nộp bằng sáng chế cho một hệ thống công nghệ sổ cái phân tán sẽ sử dụng công nghệ chuỗi khối để xác minh rằng tất cả hàng hóa được bán trên nền tảng đều đáng tin cậy.

**2. Các cơ chế trong Blockchain**

**2.1. Cơ chế đồng thuật**  
- Là định các tập luật để các nút tham gia vào mạng ngang hàng có thể hoạt động một cách đồng bộ với nhau và thống nhất về các giao dịch nào là hợp pháp và nên được thêm vào Blockchain thông qua tương tác với hợp đồng thông.

- **Đặc điểm nổi bật**:

* Có khả năng chịu lỗi để đạt được thỏa thuận mong muốn về một giá trị dữ liệu hoặc một trạng thái mạng duy nhất.
* Tạo ra cách thức để tất cả người tham gia có thể duy trì tính an toàn, bảo mật của mạng Blockchain.
* Ngăn chặn vấn đề chi tiêu 2 lần trên Blockchain (double spending) đối với giao dịch tiền điện tử trên Blockchain.

**-** Cơ chế đồng thuận được chia ra 2 loại :

* *Proof-of-work (Bằng chứng công việc)*: Thuật toán PoW vận hành bởi các thợ đào (nút – node) cùng tham gia giải quyết một bài toán mật mã để tạo ra khối tiếp theo.
* *Proof-of-stake ( Bằng chứng cổ phẩn)*: Nguyên tắc PoS cần thợ đào chứng minh quyền sở hữu % cổ phần của họ để thực hiện % hoạt động đào thưởng tương ứng. Điều này giúp tiết kiệm nhiều năng lượng hơn (điện tử) và chi phí vận hành.

**2.2.  Mật mã học (Cryptography)**  
- Là nhằm để đảm bảo tính bí mật, toàn vẹn và xác thực của thông tin trong sổ cái điện tử hay các thông tin truyền đi giữa các nút. Nhờ xây dựng dựa trên nền tảng toán học cùng với những kiến thức về lý thuyết trò chơi và mật mã học

**- Phân loại**  
Có hai loại phương pháp mã hóa chính:

* Mã hóa đối xứng (Symmetric Encryption): Là hình thức mã hóa để bảo mật dữ liệu, trong đó việc mã hóa và giải mã dữ liệu dùng chung một khóa. Do khóa dùng để giải mã dữ liệu nên cần được giữ bí mật, không được công khai.
* Mã hóa bất đối xứng (Asymmetric Encryption*)*: là hình thức mã hóa để bảo mật dữ liệu, trong đó việc mã hóa và giải mã dữ liệu dùng hai khóa khác nhau. Khóa dùng để mã hóa dữ liệu gọi là khóa công khai.

**2.3.Địa chỉ Blockchain (blockchain address):**

- Thể hiện dưới dạng một chuỗi dài các ký tự chữ và số, được chia sẻ công khai để những người dùng khác có thể gửi giao dịch đến. Mỗi địa chỉ Blockchain sẽ được tạo ra  từ một khóa công khai (Public-key).

- Khóa công khai này lại được tạo ra từ một khóa bí mật (Private-key) đóng vai trò như một cơ chế để chứng minh sự sở hữu khóa công khai (hay nói cách khác chính là địa chỉ Blockchain).

- Khi thực hiện một giao dịch tương tác với mạng lưới Blockchain, người dùng sẽ dùng khóa bí mật để ký chữ ký số, chứng minh người dùng đó là chủ sở hữu của hợp lệ của địa chỉ Blockchain trong giao dịch.

**2.4. Chữ ký số (Digital signature):**

- Là một chuỗi ký tự mã hóa được gửi đi cùng các dữ liệu gốc của giao dịch trên nền tảng Blockchain. Để tạo ra chữ ký số, người dùng sẽ sử dụng khóa bí mật để mã hóa (gọi là ký chữ ký số) các dữ liệu có trong giao dịch gửi đến người nhận.

- Một điểm lưu ý là khóa bí mật dùng để mã hóa này chính là khóa bí mật tạo ra địa chỉ Blockchain của người gửi. Chữ ký số sẽ thay đổi nếu dữ liệu giao dịch dùng để mã hóa thay đổi, hoặc là trong trường hợp cùng một dữ liệu đó, nhưng dùng khóa bí mật của người dùng khác.

**2.5. Hàm băm (Hash function):**

- Là quá trình chuyển đổi một lượng dữ liệu đầu vào không giới hạn và tạo ra một lượng dữ liệu đầu ra có độ dài cố định. Hàm băm thường được ứng dụng trong việc bảo vệ tính toàn vẹn của dữ liệu.

- Người dùng có thể xác minh tính hợp lệ của một giao dịch bằng cách so sánh giá trị băm của giao dịch trên ứng dụng với giá trị băm của giao dịch đó trên trình duyệt khối (Block explorer).

**3. Một số phiên bản của Blockchain**

\*Công nghệ này đã tiếp tục phát triển qua 3 thế hệ sau:

- Thế hệ đầu tiên – Bitcoin và các loại tiền ảo khác

+ Vào năm 2008, Ý tưởng của Satoshi về chuỗi khối Bitcoin đã sử dụng khối thông tin 1 MB cho các giao dịch Bitcoin. Nhiều tính năng của hệ thống chuỗi khối Bitcoin vẫn đóng vai trò then chốt trong công nghệ chuỗi khối cho đến ngày nay.

- Thế hệ thứ hai – hợp đồng thông minh

+ Một vài năm sau khi những đồng tiền thế hệ đầu tiên xuất hiện, các nhà phát triển bắt đầu xem xét về các ứng dụng chuỗi khối ngoài tiền điện tử.

+ Ví dụ: những người phát minh ra Ethereum đã quyết định sử dụng công nghệ chuỗi khối trong các giao dịch chuyển nhượng tài sản. Đóng góp đáng kể của họ là tính năng hợp đồng thông minh.

- Thế hệ thứ ba – tương lai

+ Khi các công ty khám phá và triển khai các ứng dụng mới, công nghệ chuỗi khối vẫn tiếp tục cải tiến và phát triển.

+ Các công ty đang giải quyết những hạn chế về quy mô cũng như điện toán và trong cuộc cách mạng chuỗi khối đang diễn ra này, tồn tại vô vàn cơ hội.