**BLOCKCHAIN**

**1. Khái quát về Blockchain**

**1.1 Khái niệm Blockchain**

Blockchain là một **cơ sở dữ liệu phân tán** hoạt động như một **sổ cái kỹ thuật số** ghi lại giao dịch theo cách **bất biến và bảo mật**. Dữ liệu trong Blockchain được chia thành các **khối (blocks)** và liên kết với nhau thành một **chuỗi (chain)** thông qua thuật toán **mã hóa (hashing)**.

Nói cách đơn giản, Blockchain là một hệ thống lưu trữ thông tin mà **không thể thay đổi hoặc làm giả dữ liệu**.

**1.2 Lịch sử ra đời**

* **1991**: Nhà khoa học Stuart Haber và W. Scott Stornetta lần đầu tiên đề xuất một hệ thống chuỗi khối có thể lưu trữ tài liệu được đóng dấu thời gian.
* **2008**: Satoshi Nakamoto giới thiệu **Bitcoin** và công nghệ Blockchain chính thức ra đời.
* **2015**: Ethereum ra mắt, mở ra kỷ nguyên **Hợp đồng thông minh (Smart Contracts)**, giúp Blockchain không chỉ phục vụ tiền điện tử mà còn có nhiều ứng dụng khác.

**1.3 Cách hoạt động của Blockchain**

Blockchain hoạt động theo cơ chế sau:

1. **Tạo giao dịch** → Một giao dịch mới được tạo ra (ví dụ: gửi tiền qua Bitcoin).
2. **Xác nhận giao dịch** → Các máy tính (nodes) trong mạng kiểm tra tính hợp lệ của giao dịch.
3. **Thêm vào khối** → Khi giao dịch được xác thực, nó được nhóm vào một khối và thêm vào Blockchain.
4. **Chuỗi khối mở rộng** → Khối mới liên kết với khối trước đó bằng **hàm băm (hash function)**.
5. **Giao dịch hoàn tất** → Thông tin giao dịch được ghi lại vĩnh viễn và không thể thay đổi.

**2. Đặc điểm của Blockchain**

**2.1 Tính phi tập trung (Decentralization)**

Không có **máy chủ trung tâm** kiểm soát Blockchain. Thay vào đó, nó hoạt động trên **mạng ngang hàng (P2P)**, giúp loại bỏ sự phụ thuộc vào bên trung gian như ngân hàng hoặc chính phủ.

**2.2 Tính bảo mật (Security)**

Dữ liệu trên Blockchain được mã hóa bằng **mật mã học (Cryptography)** và rất khó bị tấn công vì hacker phải thay đổi toàn bộ chuỗi khối.

* Sử dụng thuật toán mã hóa mạnh mẽ (như SHA-256, ECDSA).
* Các giao dịch phải được xác thực trước khi thêm vào chuỗi khối

**2.3 Tính minh bạch (Transparency)**

Tất cả các giao dịch được ghi lại công khai trên sổ cái phân tán.

Bất kỳ ai cũng có thể kiểm tra lịch sử giao dịch (trên các blockchain công khai như Bitcoin, Ethereum).**2.4 Tính bất biến (Immutability)**

Một khi dữ liệu được ghi vào Blockchain, nó **không thể thay đổi hoặc xóa bỏ**, giúp đảm bảo tính toàn vẹn của dữ liệu.

**3. Phân loại Blockchain**

**3.1 Blockchain công khai (Public Blockchain)**

* Mọi người có thể tham gia và kiểm tra giao dịch.
* Ví dụ: **Bitcoin, Ethereum**.

**3.2 Blockchain riêng tư (Private Blockchain)**

* Chỉ một số tổ chức được cấp quyền truy cập.
* Ví dụ: **Hyperledger Fabric, Corda**.

**3.3 Blockchain liên kết (Consortium Blockchain)**

* Một nhóm tổ chức cùng kiểm soát Blockchain.
* Ví dụ: **Ripple (XRP), IBM Food Trust**.

**3.4 Hybrid Blockchain (Blockchain lai)**

* Kết hợp giữa **Public và Private Blockchain**.
* Ví dụ: **Dragonchain**.

**4. Ứng dụng của Blockchain**

**4.1 Tiền điện tử (Cryptocurrency)**

Blockchain là nền tảng của các loại tiền điện tử như **Bitcoin, Ethereum, Binance Coin**, giúp thực hiện giao dịch mà không cần trung gian.

**4.2 Hợp đồng thông minh (Smart Contracts)**

Hợp đồng thông minh là **chương trình tự động thực thi** khi các điều kiện được đáp ứng, giúp giảm chi phí giao dịch và loại bỏ bên trung gian.

**4.3 Quản lý chuỗi cung ứng (Supply Chain)**

Blockchain giúp theo dõi hàng hóa từ **khâu sản xuất đến tay người tiêu dùng**, đảm bảo tính minh bạch và chống gian lận.

**4.4 Ngành tài chính (Finance & Banking)**

Nhiều ngân hàng và công ty tài chính đang ứng dụng Blockchain để **giảm chi phí giao dịch và tăng bảo mật**. Ví dụ: **Ripple (XRP)** giúp chuyển tiền quốc tế nhanh hơn.

**4.5 Y tế (Healthcare)**

Blockchain có thể lưu trữ hồ sơ bệnh án **bảo mật và minh bạch**, giúp bệnh nhân và bác sĩ dễ dàng truy cập.

**4.6 NFT (Non-Fungible Token)**

NFT sử dụng Blockchain để chứng minh **quyền sở hữu tài sản kỹ thuật số** như tranh ảnh, âm nhạc, video. Ví dụ: **Bored Ape Yacht Club (BAYC)**.