A black background with a black square

AI-generated content may be incorrect.**ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC SÀI GÒN**

**KHOA CÔNG NGHỆ THÔNG TIN**

A blue button with white text

AI-generated content may be incorrect.

**AN TOÀN BẢO MẬT TRONG HỆ THỐNG THÔNG TIN**

**BÁO CÁO**

**Ứng dụng Blockchain trong Bầu Cử**

Sinh viên thực hiện:

**Hồ Đắc Khả - 3123410143**

Giảng viên: **Trương Tấn Khoa**

Thành phố Hồ Chí Minh, tháng 10 năm 2025

**MỤC LỤC**

[LỜI CẢM ƠN 2](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark0)

[PHẦN 1: MỤC ĐÍCH ĐỀ TÀI 5](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark2)

[PHẦN 2: TÌM HIỂU CÔNG NGHỆ BLOCKCHAIN 6](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark3)

[CHƯƠNG 1: TỔNG QUAN BLOCKCHAIN 6](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark4)

* 1. [Khái niệm 6](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark5)
  2. [Các đặc tính của blockchain 7](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark6)
  3. [Nguyên lý hoạt động 12](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark7)
  4. [Ứng dụng của blockchain trong đời sống 12](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark8)

[CHƯƠNG 2: PHIÊN BẢN BLOCKCHAIN 13](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark9)

* 1. [Blockchain 1.0 (Tiền tệ) 13](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark10)
  2. [Blockchain 2.0 (Smart contract) 15](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark11)
  3. [Blockchain 3.0 (Ứng dụng phi tập trung Dapp) 15](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark12)
  4. [Blockchain 4.0 (Ứng dụng thực tiễn) 17](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark13)

[CHƯƠNG 3: CÁC LOẠI BLOCKCHAIN 18](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark14)

[CHƯƠNG 4: THUẬT NGỮ QUAN TRỌNG TRONG BLOCKCHAIN 19](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark15)

* 1. [51% Attack 19](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark16)
  2. [Public Key 19](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark17)
  3. [Private Key 20](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark18)
  4. [Mining pool 20](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark19)

[PHẦN 3: MÔ TẢ QUY TRÌNH TRIỂN KHAI ỨNG DỤNG 2](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark61)1

[*Các bước để xây dựng một project* 22](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark62)

[TÀI LIỆU THAM KHẢO 3](file:///C:\Users\KHA\Downloads\801836544-Đồ-An-Blockchain.docx#_bookmark64)3

|  |  |  |  |
| --- | --- | --- | --- |
| **MSSV** | **Họ tên** | **Phân công công việc** | **Mức độ hoàn thành** |
| 3123410143 | Hồ Đắc Khả | Code full đồ án |  |
|  |  |  |  |
|  |  |  |  |

**LỜI CẢM ƠN**

Sau quá trình học tập và rèn luyện tại trường Đại Học Sài Gòn chúng em đã được trang bị các kiến thức cơ bản, các kỹ năng thực tế để có thể hoàn thành đồ án môn học của mình.

Trong quá trình thực hiện chúng em chắc chăn không tránh khỏi được những sai sót, chính vì vậy, chúng em rất mong nhận được sự góp ý của thầy cô và các bạn nhằm hoàn thiện những kiến thức mà nhóm chúng em đã học tập và là hành trang để thực hiện tiếp các đề tài khác trong tương lai.

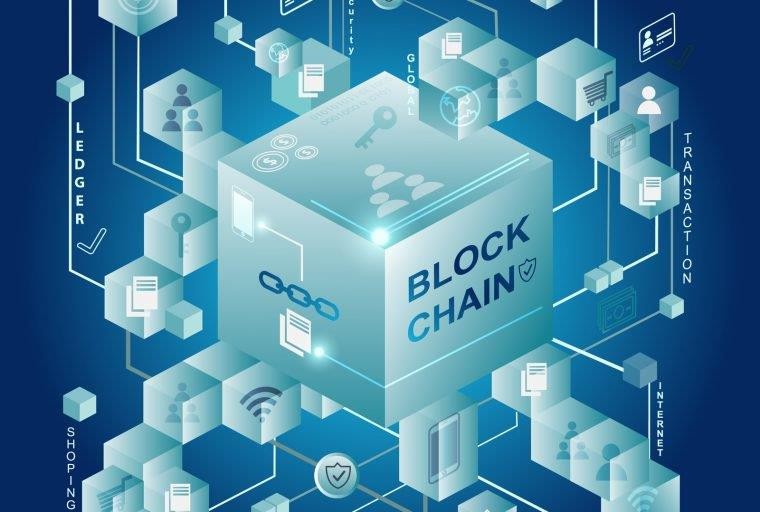
Em xin chân thành cảm ơn quý Thầy Cô!

Hồ Chí Minh , tháng 10 năm 2025.

**PHẦN 1: MỤC ĐÍCH ĐỀ TÀI**

* Tìm hiểu blockchain
* Minh họa chi tiết, cụ thể Block Chain 1.0, 2.0. Các ứng dụng của nó.
* Tìm hiểu smart contract và solidity
* Tìm hiểu hệ sinh thái Etherium?
* Mô tả quy trình triển khai smart contract lên mạng lưới ethereum test
* Tìm hiểu GRT
* Ứng dụng các kiến thức đã học để triển khai ứng dụng blockchain vào thực tế.
* Triển khai ứng dụng ở mức demo.

**PHẦN 2: TÌM HIỂU VỀ CÔNG NGHỆ BLOCKCHAIN**



**CHƯƠNG 1: TỔNG QUAN VỀ BLOCKCHAIN**

* 1. **Lịch sử phát triển.**

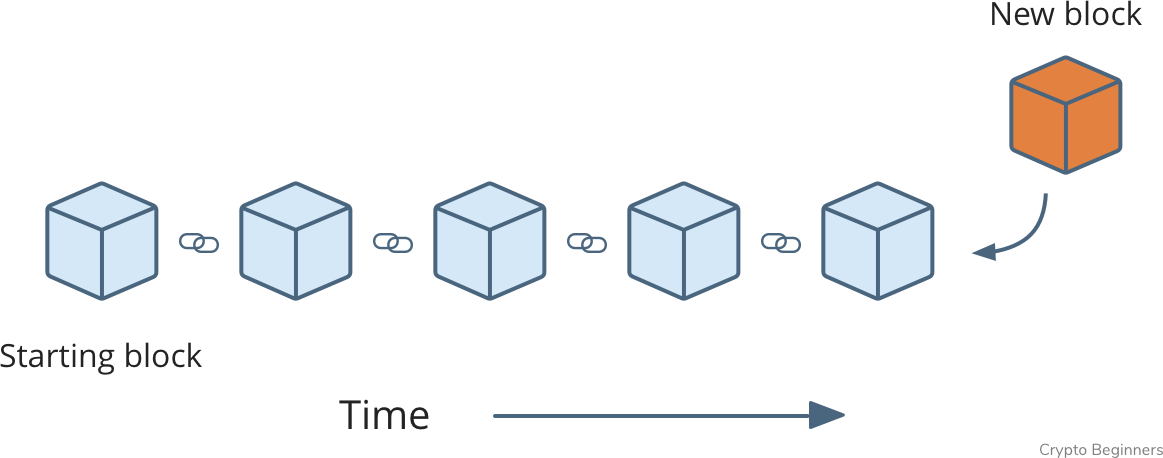
Khái niệm về một chuỗi khối được bảo mật bằng mật mã đã được đề xuất từ những năm 1990. Tuy nhiên, blockchain đầu tiên được hiện thực hóa vào năm 2008 bởi một người hoặc một nhóm người ẩn danh dưới tên Satoshi Nakamoto, với vai trò là sổ cái công khai cho các giao dịch của Bitcoin.

Ban đầu, blockchain và Bitcoin thường được xem là một. Tuy nhiên, các nhà phát triển sau đó đã nhận ra tiềm năng của blockchain vượt ra ngoài lĩnh vực tiền mã hóa. Vào khoảng năm 2014, các nỗ lực tái sử dụng công nghệ blockchain cho các ứng dụng trong chăm sóc sức khỏe, bảo hiểm, chuỗi cung ứng và nhiều lĩnh vực khác đã bắt đầu một cách nghiêm túc.

**1.2 Khái niệm.**

Blockchain , hay còn gọi là chuỗi khối , là một công nghệ sổ cái kỹ thuật số phi tập trung ,phân tán và bất biến. Nổi tiếng là công nghệ nền tảng của các loại tiền ảo hay tiền mã hóa như Bitcoin , ETH … , blockchain đang ngày càng được ứng dụng rộng rãi trong nhiều lĩnh vực khác nhau nhờ vào khả năng đảm bảo tính minh bạch , an toàn và hiệu quả.

Về cơ bản , blockchain là một cơ sở dữ liệu được chia sẻ và đồng bộ hóa giữa nhiều máy tính trong một mạng lưới . Thông tin được ghi dưới dạng các “Khối”(Block), mỗi khối chứa một tập hợp các giao dịch được mã hóa bởi “Chữ kí số” . Các khối này được liên kết với nhau theo thứ tự thời gian thành một “Chuỗi”(Chain).



*Hình 1.1. Chuỗi khối*

A white cube with black text

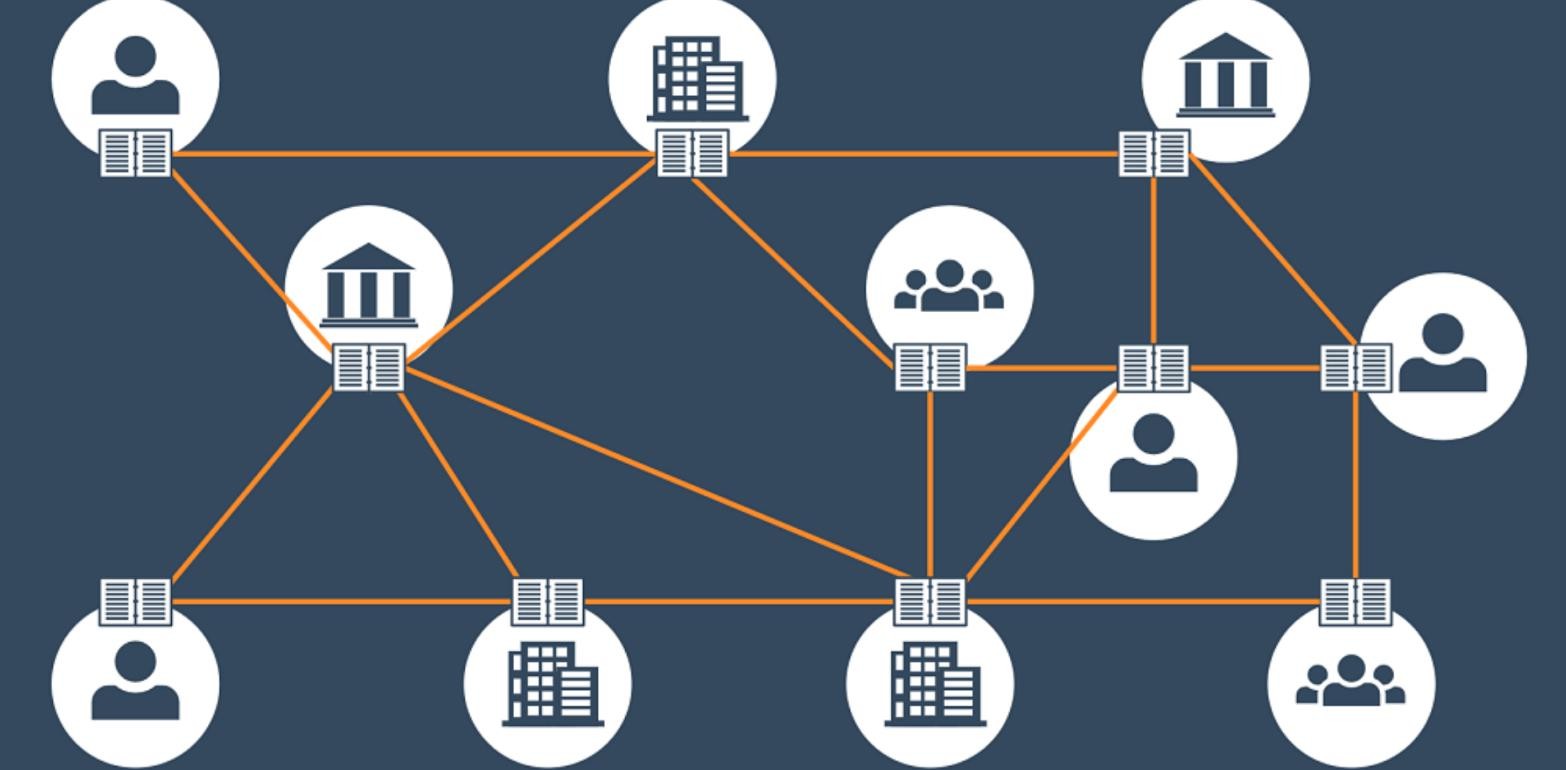
AI-generated content may be incorrect.

*Hình 1.2. Quy trình mã hóa khối*

Các thành phần cốt lõi của BlockChain:

* Block (Khối) : Mỗi khối trong chuỗi gồm ba thành phần chính : dữ liệu giao dịch , một mã định danh duy nhất của khối đó (hash) , và mã hash của khối trước đó.
* Chain (Chuỗi ) : Việc liên kết các khối với nhau bằng mã hash của khối trước đó thành một chuỗi liên tục và không thể thay đổi . Bất kỳ thay đổi nào ở một khối nào đó sẽ làm thay đi hash của nó , dẫn đến việc phá vỡ liên kết với các khối sau đó.
  1. **Các đặc tính của Blockchain**
     1. **Cơ sở dữ liệu phân tán (Phi tập trung)**

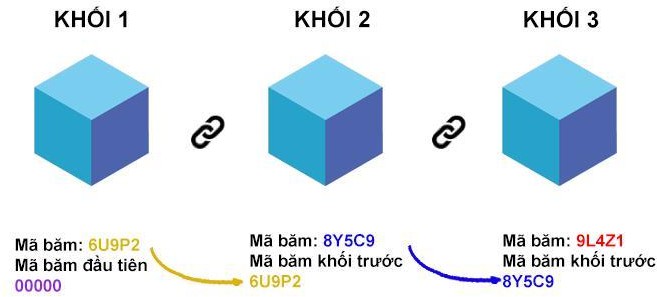
Hầu hết các Blockchain được thiết kế như một cơ sở dữ liệu phi tập trung thay vì quản lí sổ cái tập trung như ngân hàng hoặc một tổ chức nào khác. Các “tài sản” kỹ

thuật số được phân phối thay vì sao chép hoặc chuyển giao trên Blockchain. Nhờ đó, mọi người trong cùng chuỗi có thể kiểm soát thông tin, dữ liệu có trong khối

*Hình 1.3 Mô hình sổ cái phân tán*

* + 1. **Tính bền vững và tăng cường bảo mật**

Trong một Blockchain, mỗi khối đều có hàm băm riêng biệt cũng như tham chiếu đến hàm băm của khối nằm trước nó. Vì vậy, việc khai thác một chuỗi khá phức tạp, đặc biệt là trên các chuỗi lớn.



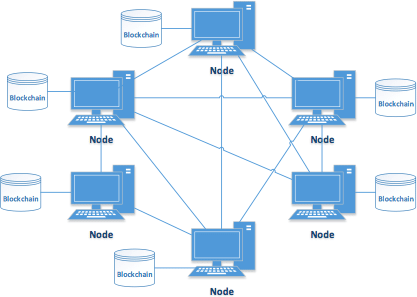
Những người khai thác chuỗi này sẽ sử dụng phần mềm chuyên dụng để giải quyết các vấn đề liên quan đến số học vô cùng phức tạp, khi muốn tìm ra một nonce tạo ra một hàm băm được chấp nhận. Bởi, mỗi nonce chỉ có 32bit trong khi mỗi hàm băm là 256bit, nên có khoảng bốn tỷ tổ hợp nonce và hàm băm cần phải được tìm kiếm trước khi tìm ra “nonce vàng” để khối của họ được thêm vào chuỗi.

Ngoài ra, nếu có bất kì sự thay đổi nào đó ở một khối thì tất cả các khối ở sau đều bị ảnh hưởng vì khối sau liên kết với khối trước bằng mã băm.

Dựa vào điều đó có thể xảy ra các cuộc tấn công hệ thống bằng cách thay đổi các khối đến khối cuối cùng tuy nhiên chỉ là có thể nhưng thực tế nó lại không thể.

***Tại sao?***

Mô hình trong blockchain là phi tập trung, mỗi máy được xem là một Node hệ thống càng nhiều Node thì càng mạnh mẽ



*Hình 1.5 Mạng lưới phi tập trung*

Mô hình này dựa trên ***Cơ chế đồng thuận phi tập trung.*** Khi một giao dịch được diễn ra và được thêm vào chuỗi thì nó cần phải được sự chấp nhận của đa số Node (máy đào) trong hệ thống này ( ở đây là các Node )

A diagram of people with a line

AI-generated content may be incorrect.

*Hình 1.6. Cơ chế đồng thuận phi tập trung*

Vì vậy trên lý thuyết hệ thống này có thể xảy ra cuộc ***tấn công 51%.***

Khi một hacker hoặc tổ chức cá nhân có số lượng Node trên hệ thống này chiếm đến 51% thì mọi giao dich sẽ bị thao túng dựa vào cơ chế đồng thuận đại đa số.

Giải quyết câu hỏi tại sao ở trên thì một hacker có thể sửa đổi một dãy block tuy nhiên trên hệ thống này mỗi cá nhân đều sở hữu một bản sổ cái vì vậy để hoàn toàn thay đổi các khối này thì phải thay đổi ***51%*** Node trên hệ thống lúc này thông tin sửa đổi đó mới được chấp nhận.

* Điều này chỉ diễn ra trên lý thuyết còn thực tế để tấn công hệ thống trên là một điều không thể
  + 1. **Tính minh bạch**

Các block được nối tiếp nhau tạo thành chuỗi, một khi một block đã được cập

nguyên tắc ghi chép phổ biến trong tài chính là không được phép xóa bỏ dữ liệu đã cập nhật, thay vào đó cập nhật thêm các block mới, với nội dung cần chỉnh sửa và tên tuổi của người chỉnh sửa. Điều này vừa giúp rõ ràng thông tin lẫn sự toàn vẹn của các dữ liệu đã được tạo.

Blockchain minh bạch để mỗi người có thể theo dõi dữ liệu nếu họ muốn.

* + 1. **Tính bất biến**

Một khi dữ liệu được đưa vào một khối thì sẽ được mã hóa bằng thuật toán mã hóa băm kết hợp RSA security (mã hóa bất đối xứng) đảm bảo rằng dữ liệu không thể sửa đổi

1. A group of black and red logos

   AI-generated content may be incorrect.

*Hình 1.7. Thuật toán mã hóa*

**1.3 Nguyên lí hoạt động**

A diagram of different types of computer components

AI-generated content may be incorrect.

*Hình 1.8. Nguyên lý hoạt động*

* 1. **Ứng dụng của blockchain trong đời sống.**

Blockchain hiện đang được ứng dụng vào rất nhiều lĩnh vực trong đời sống.

* + - Ứng dụng của blockchain trong thương mại điện tử
    - Ứng dụng của Blockchain trong chuỗi cung ứng
    - Ứng dụng của blockchain trong dịch vụ tài chính, ngân hàng
    - Ứng dụng của blockchain trong nông nghiệp
    - Ứng dụng của blockchain trong y tế
    - Ứng dụng của Blockchain trong Internet of Things (IoT)
    - ...

**CHƯƠNG 2: PHIÊN BẢN BLOCKCHAIN**

* 1. **Blockchain 1.0 (Tiền tệ).**

Năm 2005 , người ta đề ra ý tưởng về việc tạo ra một loại tiền điện tử . Sổ cái Blockchain ra đời như một phương tiện hỗ trợ hoạt động của loại tiền này . Nói cách khác , Bitcoin loại crypto đầu tiên cũng chính là ứng dụng đầu tiên của Blockchain.



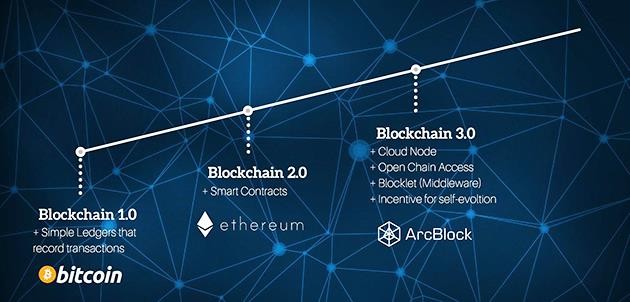
*Hình 1.9. Bitcoin*

* + 1. **Blockchain 1.0 hoạt động như thế nào?**

**Cụ thể khi khách hàng muốn sử dụng Bitcoin để thanh toán dịch vụ hay hàng hóa , người dùng sẽ ra lệnh ghi chép và xác nhận giao dịch. Giao dịch sẽ được ghi một cách công khai thành những khối block được xếp vào chuỗi, và được xác nhận bởi những người sử dụng Bitcoin khác. Trung bình cứ 10 phút, một khối block mới được tạo ra thông qua việc “đào” Bitcoin.**

**Tức là , dựa vào giao thức của Bitcoin , cơ sở dữ liệu Blockchain được chia sẻ cho tất cả các máy tính tham gia vào hệ thống này. Mỗi máy tính sẽ có một bản sao chép của Blockchain có chứa dữ liệu ghi chép lại và là bằng chứng cho việc một giao dịch được hoàn tất.**

* **Bởi chỉ cần liên tưởng với các loại tài sản khác (thay vì tiền điện tử ) , chắc chắn sẽ nhìn thấy tiềm năng vô hạn của nó từ đó ra đời các phiên bản cao hơn blockchain 2.0,3.0 và 4.0 đáp ứng tất cả nhu cầu thực tế.**



***Hình 1.10. Giai đoạn phát triển***

* + 1. **Ứng dụng của Blockchain 1.0.**

**Hỗ trợ mọi giao dịch chuyển đổi tiền tệ , kiều hối và hệ thống thanh toán kỹ thuật số trong lãnh thổ tiền điện tử nói chung và Bitcoin nói riêng bằng các thuật toán về tiền tệ (Ví Blockchain).**

* 1. **Blockchain 2.0 (Smart Contract)**

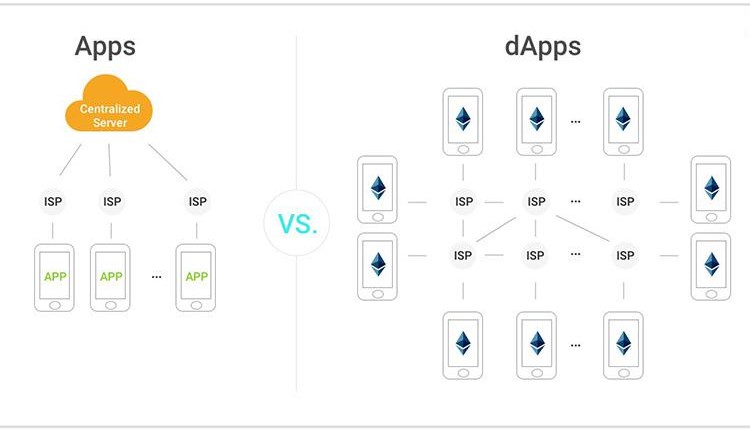
**Blockchain đã thoát ra khỏi sự hạn hẹp bằng cách vượt ra khỏi lĩnh vực crypto mà tiếp đến với Smart Contract. Công nghệ này có tác dụng bảo vệ các hợp đồng thông minh dưới sự can thiệp của những người có mục đích không tốt. Khi làm việc trên loại hợp đồng này , người sử dụng sẽ không cần tiêu tốnchi phí vào việc xác thực , vận hành và chống gian lận.**



***Hình 1.11. Smart contract***

* 1. **Blockchain 3.0 (Ứng dụng phi tập trung Dapp)**

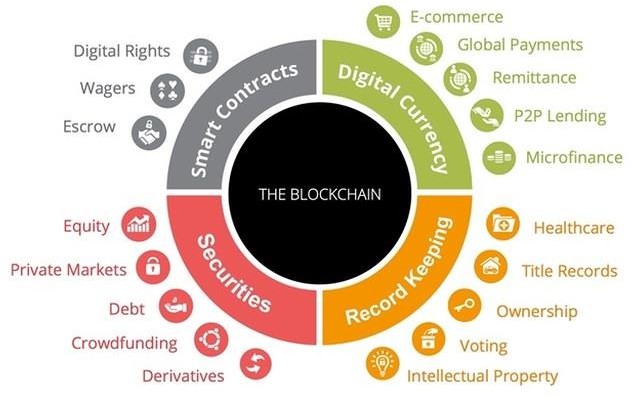
DApps là viết tắt của Decentralized application tức ứng dụng **phi tập trung.** **Có thể hiểu đơn giản thông qua việc lấy ví dụ từ các ứng dụng trên CHPlay hay App Store là các ứng dụng được tạo ra bởi một tổ chức, cá nhân nào đó và chịu sự chi phối của họ. Trái lại, các ứng dụng xuất hiện trên Blockchain không chịu sự kiểm soát của bất cứ một cá nhân thay vào đó là một tập thể những người có mặt trong chuỗi. Đó chính là sự phi tập trung của ứng dụng trên Blockchain.**



***Hình 1.12. Phân biệt App và Dapp***

* **Mô hình website truyền thống: Frontend -> API -> Database**
* **Mô hình website Dapps: Fronten -> Smart Contract (ABI) -> Blockchain**
  1. **Blockchain 4.0(Ứng dụng thực tiễn)**

**Blockchain của thời đại này không chỉ tập trung vào lĩnh vực tài chính mà còn trở thành một một giải pháp cho tất cả các vấn đề cơ bản của đời sống. Blockchain có tác dụng hỗ trợ các doanh nghiệp xây dựng một quá trình làm việc xuyên nền tảng , chẳng hạn như chuỗi cung ứng , hệ thống xử lý đơn hàng tự động, thanh toán , thu thập dữ liệu Internet.**



***Hình 1.13. Ứng dụng blockchain***

**CHƯƠNG 3: CÁC LOẠI BLOCKCHAIN**

**Như đã đề cập ở những phần trước . Có 2 loại blockchian:**

* **Blockchain công khai (Public Blockchain): Dữ liệu ở chế độ công khai , bất kỳ ai cũng có thể tải xuống một giao thức để đọc , ghi hoặc tham gia mạng (Bitcoin , Ethereum,Litecoin ,….)**
* **Blockchain riêng tư (Private Blockchain): Cho phép các tổ chức sử dụng công nghệ sổ cái phân tán đó dữ liệu không công khai , những người tham gia trên mạng này sẽ bị hạn chế một số quyền như đọc và ghi dữ liệu.**

| **Tiêu chí** | **Public Blockchain (Chuỗi khối công khai)** | **Private Blockchain (Chuỗi khối riêng tư)** |
| --- | --- | --- |
| **Quyền truy cập** | **Mọi người đều có thể tham gia, đọc, ghi và xác minh giao dịch.** | **Chỉ người được cấp quyền (do tổ chức quản lý) mới có thể tham gia và xác minh.** |
| **Ví dụ tiêu biểu** | **Bitcoin, Ethereum, Solana, Litecoin** | **Hyperledger Fabric, R3 Corda, Quorum** |
| **Cơ chế đồng thuận** | **Proof of Work (PoW), Proof of Stake (PoS), v.v. – yêu cầu nhiều tài nguyên.** | **Raft, PBFT (Practical Byzantine Fault Tolerance), hoặc các cơ chế đồng thuận nhẹ hơn.** |
| **Tốc độ giao dịch** | **Chậm (vì cần nhiều nút xác minh, phân tán toàn cầu).** | **Nhanh hơn (vì ít nút và có quyền kiểm soát tập trung).** |
| **Bảo mật** | **Rất cao nhờ tính phi tập trung và minh bạch, khó bị tấn công.** | **Bảo mật phụ thuộc vào tổ chức quản lý, dễ bị tấn công nội bộ hơn.** |
| **Quyền kiểm soát dữ liệu** | **Không có tổ chức trung tâm kiểm soát — người dùng kiểm soát dữ liệu của mình.** | **Có tổ chức trung tâm kiểm soát và cấp quyền truy cập.** |
| **Minh bạch** | **Dữ liệu công khai, ai cũng có thể xem giao dịch.** | **Dữ liệu riêng tư, chỉ bên được cấp quyền mới thấy.** |
| **Khả năng mở rộng (Scalability)** | **Hạn chế (do mạng lưới lớn và phi tập trung).** | **Cao hơn (ít nút, kiểm soát tốt hơn).** |
| **Chi phí vận hành** | **Cao (do phí giao dịch, tiêu thụ năng lượng lớn).** | **Thấp hơn (vì kiểm soát được tài nguyên).** |
| **Ứng dụng phổ biến** | **Tiền điện tử, tài sản kỹ thuật số, hợp đồng thông minh công khai.** | **Doanh nghiệp, ngân hàng, quản lý chuỗi cung ứng, chính phủ.** |
| **Mức độ phi tập trung** | **Hoàn toàn phi tập trung.** | **Bán tập trung hoặc tập trung.** |
| **Tính ẩn danh** | **Cao – người dùng thường không cần tiết lộ danh tính thật.** | **Thấp – yêu cầu xác thực danh tính rõ ràng.** |

***Hình 1.14. Bảng so sánh hai loại blockchain***