

**TRƯỜNG ĐẠI HỌC QUỐC GIA TP – HỒ CHÍ MINH**  
**ĐẠI HỌC KHOA HỌC TỰ NHIÊN**



**BÁO CÁO: PHÂN TÍCH YÊU CẦU**  
**ĐỒ ÁN: XÂY DỰNG GAMEFI TRÊN MẠNG**  
**BLOCKCHAIN**

**GIẢNG VIÊN:**

Nguyễn Đình Thúc

Nguyễn Văn Quang Huy

Ngô Đình Hy

**LỚP:**

20CNTThuc

**SINH VIÊN:**

Hoàng Hữu Minh An 20127102

Trần Hoàng Minh Quang 20127299

Ho Chi Minh, 12-03-2024

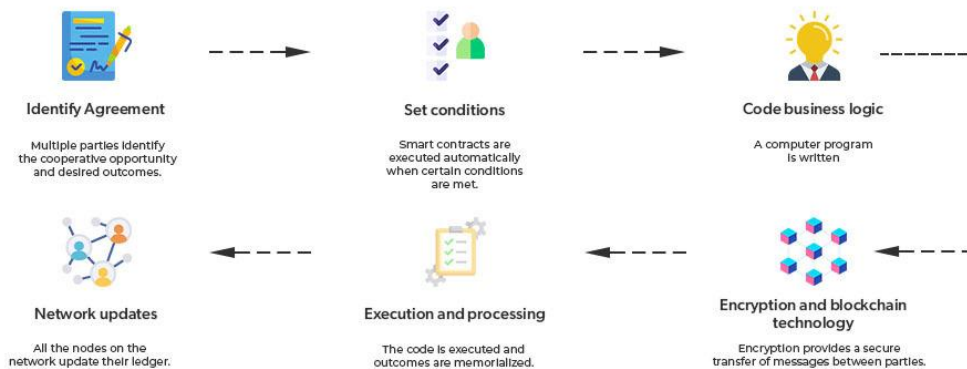
# Contents

I. Smart contract: .....	3
II. Tổng quan kiến trúc Blockchain:.....	4
III. Layer 1:.....	5
IV. Layer 2 (Polygon): .....	5
V. FLP Token: .....	7
VI. Link github:.....	7
VII. Tham khảo: .....	7

## I. Smart contract:

Smart contracts là các chương trình máy tính tự động hóa được thiết kế để thực thi và quản lý các giao dịch mà không cần sự can thiệp của bên thứ ba chạy trên blockchain thông qua EVM.

### How does a Smart Contract Work?



Đặc điểm của Smart Contract:

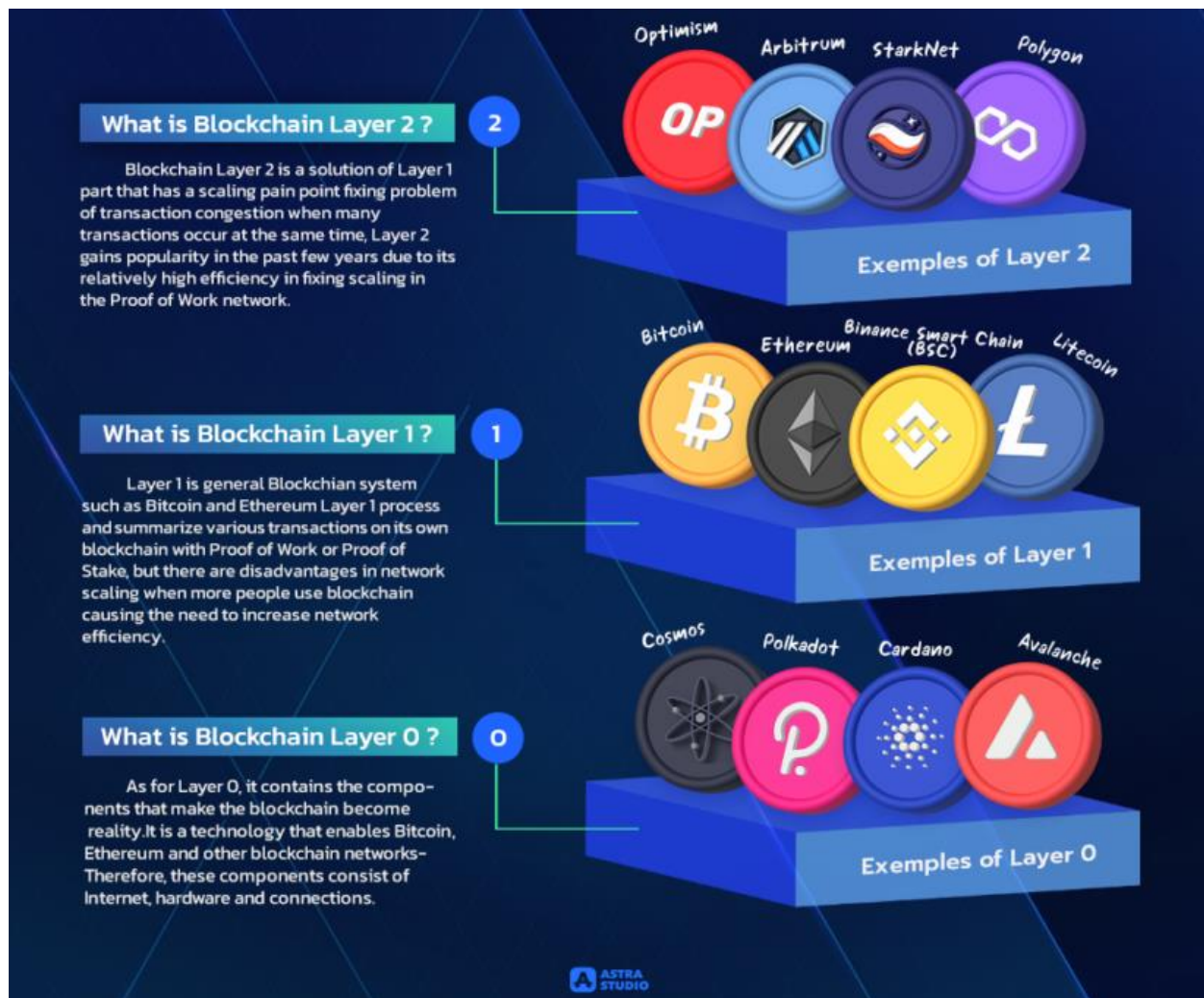
- **Điểm mạnh:**
  - Immutable - khi deploy không thể thay đổi
  - Không bị ai quản lý
  - Không cần server
  - Gửi/Nhận tiền tệ dễ dàng
- **Điểm yếu:**
  - Mắc, vì phải trả tiền gas cho các node hoặc validator
  - Chậm
  - Khả năng lưu trữ chậm
  - Không thể API bên ngoài

## II. Tổng quan kiến trúc Blockchain:

Cấu trúc đa tầng của blockchain có thể hiểu một cách đơn giản như sau:

- Layer 0: Cơ sở hạ tầng mà trên đó có thể xây dựng nhiều blockchain Layer 1.
- Layer 1: Các blockchain cơ sở được các nhà phát triển sử dụng để xây dựng các ứng dụng, chẳng hạn như các ứng dụng phi tập trung (DApp).
- Layer 2: Các giải pháp mở rộng quy mô xử lý hoạt động bên ngoài các blockchain layer 1 để giảm tải giao dịch cho chúng.

Tương tự, cấu trúc blockchain cũng được chia thành nhiều lớp (Layer) với chức năng khác nhau: Layer dữ liệu (Data Layer), Layer mạng lưới (Network Layer), Layer đồng thuận (Consensus Layer), Layer kích hoạt (Incentive Layer), Layer hoạt động (contract Layer) và Layer ứng dụng (Dapp layer).



### III. Layer 1:

Các blockchain Layer 1 như Bitcoin hay Ethereum là dạng blockchain độc lập nguyên khối, tức tự bản thân nó đã tương đối hoàn chỉnh và có thể hoạt động ổn định mà không cần đến bên thứ ba nào.

Ví dụ: Khi một người dùng Bitcoin chuyển Bitcoin cho người dùng khác, giao dịch sẽ được ghi lại trên layer 1 của blockchain Bitcoin. Cụ thể, thông tin về giao dịch này sẽ được bao gồm trong một khối mới và được xác nhận thông qua thuật toán đồng thuận PoW trước khi được thêm vào blockchain. Điều này làm cho giao dịch trở nên không thể sửa đổi và được phân phối rộng rãi trên mạng lưới Bitcoin.

Ưu điểm:

- **Security:** Cung cấp mức độ bảo mật và phân cấp cao, giúp chúng có khả năng chống lại các cuộc tấn công
- **Wide adoption:** Các blockchain layer1, chẳng hạn như Bitcoin và Ethereum, đã được áp dụng rộng rãi và được công nhận là tài sản kỹ thuật số khả thi.
- **Interoperability:** Blockchain layer 1 có thể tương tác với các blockchain và tài sản kỹ thuật số khác, thúc đẩy một hệ sinh thái được kết nối nhiều hơn.

Nhược điểm:

- **Scalability:** Lượng giao dịch hạn chế có thể dẫn đến tắc nghẽn mạng và phí giao dịch cao.
- **Energy consumption:** Một số blockchain layer1, như Bitcoin, sử dụng thuật toán đồng thuận Proof of Work (PoW), tiêu thụ một lượng năng lượng đáng kể.

### IV. Layer 2 (Polygon):

Layer 2 là thuật ngữ chung cho các giải pháp mở rộng quy mô Ethereum nhằm xử lý các giao dịch ngoài Ethereum layer 1 trong khi vẫn tận dụng tính bảo mật phi tập trung mạnh mẽ của Ethereum layer 1. Layer 2 là một chuỗi khối riêng biệt mở rộng Ethereum.

Có một số layer 2 khác nhau, mỗi loại có mô hình bảo mật và đánh đổi riêng. Layer 2 loại bỏ gánh nặng giao dịch khỏi layer 1, cho phép nó trở nên ít tắc nghẽn hơn và mọi thứ trở nên có khả năng mở rộng hơn. Trong đề án này, ta sẽ tập trung vào Polygon:

Polygon là giải pháp Layer 2 sử dụng cơ chế đồng thuận Proof of Stake (POS) được phát triển nhằm giải quyết các vấn đề về tốc độ, phí giao dịch và khả năng mở rộng của Ethereum. Polygon đang hoạt động như một sidechain của Ethereum có khả năng tương thích với EVM và đang được gọi là Polygon POS.

Ban đầu, Polygon sử dụng plasma chain với việc xử lý giao dịch trên các sidechain riêng biệt và sau đó được tổng hợp lại trên mainnet Ethereum chính. Điều này giúp cải thiện hiệu suất và giảm phí giao dịch cho người dùng.

Hiện tại, Polygon sử dụng ZK-rollups để kết hợp một lượng lớn các giao dịch được xử lý off-chain thành 1 giao dịch duy nhất. Cơ chế này giúp tăng tính ẩn danh cho các giao dịch đồng thời đảm bảo sự riêng tư cho người dùng.

Ngoài ra, Polygon sử dụng kiến trúc Heimdall để chọn block producer (nhà sản xuất khối) nhằm tăng khả năng mở rộng và bảo mật của mạng lưới. Các block producer được chọn ngẫu nhiên trong số các validator trong Polygon PoS nhằm tăng cường tính bảo mật và khả năng mở rộng của mạng lưới.

So sánh Polygon và Ethereum:

Đặc điểm	Polygon (MATIC) 	Ethereum (ETH) 
Token	MATIC	ETH
Cơ chế đồng thuận	Proof of Stake (PoS)	Proof of Work (PoW)
Khả năng mở rộng	Polygon được thiết kế để nâng cao khả năng mở rộng của Ethereum, giúp cải thiện tốc độ và phí giao dịch	Khả năng mở rộng hạn chế dẫn đến phí giao dịch cao hơn và thời gian xử lý chậm hơn khi mạng tắc nghẽn
Hệ sinh thái	Hệ sinh thái của Polygon không đa dạng như Ethereum nhưng được hưởng lợi từ khả năng tương tác với mạng Ethereum	Ethereum có một hệ sinh thái đa dạng và được phát triển tốt
Mục đích sử dụng	Polygon phù hợp với các DApp với khả năng mở rộng tốt và chi phí thấp.	Chủ yếu được sử dụng cho các ứng dụng phi tập trung (DApps) và hợp đồng thông minh
Mô hình bảo mật	Sử dụng PoS, cung cấp mô hình bảo mật tiết kiệm năng lượng và tiết kiệm chi phí	Dựa vào PoW để bảo mật, có thể tốn nhiều tài nguyên
Tốc độ giao dịch	Tốc độ giao dịch nhanh hơn và phí thấp hơn nhờ các giải pháp mở rộng Layer 2	Thời gian xác nhận giao dịch có thể chậm hơn khi mạng tắc nghẽn
Giải pháp mở rộng Layer 2	Polygon là giải pháp mở rộng Layer 2 cho Ethereum, cung cấp nhiều công nghệ mở rộng quy mô khác nhau bao gồm cả PoS và sidechain	Ethereum đang tiếp cận giải pháp Layer 2 như Optimistic Rollups và zk-Rollups
Framework phát triển	Hỗ trợ Solidity, làm cho nó tương thích với các công cụ và ngôn ngữ phát triển hiện có của Ethereum	Solidity là ngôn ngữ lập trình chính cho hợp đồng thông minh Ethereum



## V. FLP Token:

Mục đích: sử dụng Openzeppelin, Hardhat và Polygon để viết smart contract cung cấp FLP token cho người dùng một cách minh bạch. Kết hợp với cofig.js để theo dõi các địa chỉ ví ở các mạng khác nhau.

Vai trò:

- Token có thể được sử dụng như một đơn vị thanh toán trong trò chơi, cho phép người chơi mua và bán các sản phẩm và dịch vụ trong trò chơi. Điều này có thể bao gồm mua vật phẩm trong trò chơi, nâng cấp nhân vật, mua vật liệu, và các giao dịch khác.
- Token có thể được sử dụng như một loại tiền tệ trong trò chơi, giống như ticket, vàng, xu, hoặc kim cương. Người chơi có thể kiếm hoặc được thưởng token thông qua việc hoàn thành nhiệm vụ, đạt thứ hạng cao hoặc tham gia vào các hoạt động khác trong trò chơi.

## VI. Link github:

Link github: [floppy-bird-smartcontract: 🌸 Build a Game Fi - Solidity, Smart Contracts #P2 #HCMUS #doanmahoa \(github.com\)](#)

## VII. Tham khảo:

[1]: [ERC20 - OpenZeppelin Docs](#)

[2]: [Hardhat's tutorial for beginners | Ethereum development environment for professionals by Nomic Foundation](#)

[3]: [jayden-dang/01-blockchain-basic: The Curriculums \(github.com\)](#)