

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

**NicheImage: hệ thống sinh ảnh phi tập trung dựa
trên mạng Bittensor**

Trần Thành Luân

luan.tt204665@sis.hust.edu.vn

Ngành: Khoa học máy tính

Giảng viên hướng dẫn: TS. Trần Nguyên Ngọc

Chữ kí GVHD

Khoa:

Kỹ thuật máy tính

Trường:

Công nghệ thông tin và Truyền thông

HÀ NỘI, 06/2024

LỜI CẢM ƠN

12h00, ngày 1/7/2024, đồ án tốt nghiệp chuẩn bị được đem đi in, in xong tôi sẽ vội vàng chạy ngay lên B1-405 để xếp hàng và nộp nó. Sau đó, tôi có thể về nhà ngủ một giấc sau nhiều ngày thiếu ngủ, đêm nay tôi có thể xem Bò Đào Nha đá Euro một cách thoải mái nhất, đó là những gì tôi đã nghĩ. Tuy nhiên sự thật nó rất khác, bỗng dưng tôi cảm thấy tâm trạng có phần trũng lại, có vẻ cánh cửa Bách Khoa sắp khép. Nhìn lại 4 năm qua, tôi đã kịp tạch 01 môn thể dục, trải qua đợt dịch Covid đáng nhớ, tham gia hoạt động ngoại khoá cũng rất nhiều (Đội tình nguyện CTES, CLB Hỗ trợ học tập), nhận vài cái học bổng,... đều là những kỉ niệm đáng nhớ. Những gì mà Bách Khoa đã cho tôi trong suốt khoảng thời gian qua đều rất quý giá, nhiều lúc tôi cũng tự cảm thấy mình đúng là một chút gì đó thuộc về nơi này.

Trong suốt quãng thời gian ấy, bố mẹ và gia đình luôn là điểm tựa tinh thần vững chãi, luôn là động lực để tôi đi lên trong cuộc sống. Tôi luôn cảm thấy may mắn rằng mình luôn gặp được những người bạn tốt, cùng nhau vượt qua những cuộc vui và tận hưởng những giây phút buồn bã nhất. Thầy cô luôn dẫn dắt sinh viên tới những nội dung kiến thức hay, May mắn rằng, ở cuối những năm đại học, tôi đã tìm được tình yêu đích thực của đời mình, người luôn bên cạnh tôi, yêu tôi, nấu cho tôi ăn những bữa cơm ngon, luôn động viên, an ủi tôi khi vấp ngã, người cho tôi thấy được tương lai sẽ rất tươi đẹp miễn là luôn ở bên nhau, đùm bọc và cùng nhau lớn lên.

Kết bài, tôi đã dành suốt 10 phút qua để kịp ghi lại những kỉ niệm, lời cảm ơn tới những người thân thương lên đồ án này. Giây phút nghẹn ngào hãy để cho những khoảng khắc đẹp nhất, hi vọng đồ án tốt nghiệp này, là tâm huyết suốt kì học qua của tôi sẽ đạt được những sự đánh giá tốt từ thầy cô, tôi thực sự nghĩ về điều đó. Sau đây là một đoạn thơ mà tôi đã mong muốn mang nó lên đồ án tốt nghiệp từ nhiều năm trước, mọi cảm xúc, tôi xin dành lại đây

*Nếu em về qua phố nhỏ Bách Khoa
Nhớ mang cho tôi chùm bằng lăng cuối hạ,
Nơi bè bạn đêm ngày hội hã
Mùa thi cuối cùng, mai hết tuổi sinh viên
Tác giả: không rõ*

TÓM TẮT NỘI DUNG ĐỒ ÁN

Gần đây, các dịch vụ AI như ChatGPT, Dalle, MidJourney,... đã không còn xa lạ với người sử dụng phổ thông, chúng len lỏi và thay thế cách làm việc, tiếp cận của nhiều mảng công việc khác nhau. Tuy nhiên đây đều là các dịch vụ được cung cấp bởi các tổ chức lớn và đều là mã nguồn đóng, hay còn gọi đây là các dịch vụ AI tập trung (Centralized AI). Với lượng người dùng lớn, các yếu điểm của Centralized AI càng được thể hiện rõ: tính minh bạch, bảo mật và khả năng mở rộng rất hạn chế. Ngược lại với Centralized AI đó là Decentralized AI, nơi mà dữ liệu, tài nguyên, mô hình được tổ chức phi tập trung. Federated learning là một lĩnh vực được nghiên cứu sôi nổi trong những năm gần đây với mục tiêu phân cấp, bảo mật dữ liệu, tuy nhiên công nghệ này vẫn chưa đem lại hiệu quả lớn. Xu hướng phi tập trung đã xuất hiện từ lâu với đại diện là công nghệ Blockchain, những điểm mạnh của blockchain rõ ràng là sự bù đắp cho những gì Centralized AI còn thiếu. Nổi bật trong các mạng blockchain về AI đó là Bittensor. Với mục tiêu tạo một thị trường AI cạnh tranh, cùng với tiêu chuẩn hạ tầng xây dựng phù hợp như một cơ sở để xây dựng hệ thống AI trên đó. Đồ án này sẽ tiếp cận giải quyết vấn đề về Centralized AI dựa trên việc xây dựng một subnet trong mạng blockchain Bittensor cho bài toán cụ thể là hệ thống sinh ảnh. Bằng việc xây dựng incentive mechanism dựa trên đánh giá về khả năng serving với 2 yếu tố chính là tốc độ và generation bandwidth cùng với cơ chế incentive splitting giúp subnet có khả năng phục vụ nhiều loại mô hình và xây dựng hạ tầng cho validator & miner, subnet mang tên NicheImage đã tham gia main-net, là subnet thứ 23 của bittensor, với mục tiêu cuối cùng là tạo ra hệ thống Decentralized Image Generation. Trải qua hơn 1 triệu blocks trên main-net, với quá trình sai và sửa liên tục, NicheImage đã dần đi vào giai đoạn ổn định, API sinh ảnh đã có những organic traffic đầu tiên, minh chứng được subnet đã đạt được mục tiêu ban đầu.

Sinh viên thực hiện
(Ký và ghi rõ họ tên)

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....	1
1.1 Đặt vấn đề.....	1
1.2 Các giải pháp hiện tại và hạn chế	1
1.3 Mục tiêu và định hướng giải pháp	3
1.4 Đóng góp của đề án	5
1.5 Bố cục đề án	5
CHƯƠNG 2. NỀN TẢNG LÝ THUYẾT	7
2.1 Blockchain.....	7
2.1.1 Lịch sử	7
2.1.2 Blockchain là gì?	8
2.1.3 Mạng blockchain Ethereum.....	10
2.1.4 Mạng blockchain Polkadot và Substrate SDK	12
2.1.5 Bittensor - Mạng lưới AI phi tập trung	14
2.2 Image Generation Model	16
2.2.1 Diffusion model	17
2.2.2 Conditioned Generation.....	19
2.2.3 Latent Diffusion Model	20
2.2.4 Stable Diffusion XL	21
CHƯƠNG 3. PHƯƠNG PHÁP ĐỀ XUẤT.....	25
3.1 Tổng quan giải pháp.....	25
3.2 Mô hình sinh ảnh Text To Image	25
3.3 Incentivized Volume Mechanism	26
3.3.1 Miners	26
3.3.2 Validators.....	28

3.4 Tổng quát hoá cơ chế Incentive cho nhiều models trong một subnet.....	30
3.5 Mở rộng khả năng serving cho miner.....	32
3.6 Xây dựng cụm server tính điểm cho validator	32
3.7 Xây dựng luồng chia sẻ quyền sử dụng miner của validator	33
CHƯƠNG 4. ĐÁNH GIÁ THỰC NGHIỆM.....	35
4.1 Mục tiêu đánh giá.....	35
4.2 Hiệu quả của cơ chế incentive theo volume	35
4.3 Đánh giá hiệu năng scale up của miner	36
4.4 Multi models - Incentive Splitting thực tế với NicheImage.....	37
4.5 Proxy Client: API, Playground Demo và Collaboration	38
4.6 Subnet Emission.....	39
4.7 Thực nghiệm Mining trên Subnet NicheImage.....	39
CHƯƠNG 5. KẾT LUẬN	41
5.1 Kết luận.....	41
5.2 Định hướng phát triển	41
TÀI LIỆU THAM KHẢO.....	42

DANH MỤC HÌNH VẼ

Hình 1.1	Ảnh sinh từ mô hình Stable Diffusion XL.	2
Hình 1.2	Xây dựng ứng dụng AI dựa trên mạng Bittensor.	3
Hình 1.3	Luồng sử dụng của người dùng NicheImage API	4
Hình 2.1	Các khối (blocks) được hình thành và kết nối với nhau trong blockchain [1].	8
Hình 2.2	Xây dựng DApps tại Ethereum.	11
Hình 2.3	Kiến trúc hoạt động của bản của Subnet	16
Hình 2.4	Huấn luyện mô hình từ đầu và finetuning mô hình đã huấn luyện	17
Hình 2.5	Minh hoạ Markov chain của quá trình forward (reverse) diffusion process [13].	18
Hình 2.6	Thuật toán huấn luyện và inference mô hình denoise diffusion [13].	19
Hình 2.7	Mô hình Conditional Latent Diffusion Model [16].	21
Hình 2.8	Trái: Mô hình SDXL và SDXL sử dụng refiner cho thấy sự vượt trội khi so với Stable Diffusion 1.5 và 2.1. Phải: Kiến trúc mô hình SDXL sử dụng Latent Diffusion Model và Refiner [18].	22
Hình 2.9	Ảnh hưởng của size-conditional lên kết quả đầu ra của mô hình [18].	22
Hình 2.10	Phân bố dữ liệu huấn luyện theo kích thước [18].	23
Hình 2.11	Phiên bản finetune SDXL được cộng đồng ưa chuộng sử dụng.	23
Hình 2.12	So sánh SDXL và các mô hình (dịch vụ) sinh ảnh khác [18].	24
Hình 3.1	Sử dụng mô hình SDXL trong thư viện diffusers: Mô hình sẽ được nạp vào GPU dưới dạng pipeline. Tiếp theo, phần mô tả bức ảnh sẽ được định nghĩa là biến string. Sau đó biến này được đưa qua pipeline và nhận output là ảnh tương ứng.	26
Hình 3.2	Mã nguồn cung cấp bởi NicheImage cho phép miner scale up số lượng replicas của server sinh ảnh dựa trên nhiều GPU	27
Hình 3.3	Mã giả cho quá trình xây dựng rate limit của miner.	28
Hình 3.4	Mô tả Validator: serving queue và luồng tiêu thụ.	29
Hình 3.5	Mã giả cho bước xây dựng serving queue của Validator.	29
Hình 3.6	Incentive Splitting cho nhiều models.	31
Hình 3.7	Subnet Rewarding Server setup for validator.	32

Hình 3.8	Tổng quát kiến trúc của NicheImage khi giao tiếp với End User thông qua API - Proxy Client. Đường nét liền thể hiện sự giao tiếp trực tiếp, đường nét đứt thể hiện giao tiếp gián tiếp.	34
Hình 3.9	Validator có bandwidth khác nhau tỉ lệ thuận với lượng stake. .	34
Hình 4.1	Đánh giá hiệu quả của Incentivized Volume Mechanism. . . .	35
Hình 4.2	Biểu đồ scatter plot của miners incentive trong subnet NicheImage.	36
Hình 4.3	Biểu đồ tần xuất của miners incentive	37
Hình 4.4	Benchmark hiệu quả của mở rộng serving với nhiều GPU. . .	37
Hình 4.5	Sự phân hoá mô hình trên thực tế tỉ lệ với incentive distribution đã định ra	38
Hình 4.6	Demo ứng dụng sinh ảnh sử dụng API của NicheImage. . . .	38
Hình 4.7	NicheImage API được tích hợp vào	39
Hình 4.8	Biểu đồ điểm số được tính bởi validator "Taostats & Corcel" theo thời gian	40

DANH MỤC BẢNG BIỂU

Bảng 4.1	Thông tin các mô hình được cung cấp tại subnet NicheImage.	38
----------	--	----

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

1.1 Đặt vấn đề

Trí tuệ nhân tạo (AI) và công nghệ chuỗi khối (blockchain) là những công nghệ đã đạt được nhiều bước tiến lớn, thay đổi cách vận hành và thói quen trong cuộc sống của con người. Trong khi AI mang lại giá trị lớn trong việc cải thiện hiệu suất làm việc, sáng tạo nội dung, thực hiện những tác vụ khó yêu cầu độ phức tạp cao thì blockchain tạo nên một tiêu chuẩn cho sự bảo mật, minh bạch cho dữ liệu giao dịch. Tuy nhiên, mỗi mảng công nghệ đều có điểm yếu riêng. Đối với AI, các mô hình mạnh mẽ lại ngày càng yêu cầu tài nguyên tính toán cao hơn, dẫn tới người dùng phải tìm tới những dịch vụ tập trung (Centralized AI) như ChatGPT, Claude, tuy nhiên những dịch vụ này rất hạn chế về khả năng mở rộng... Đối với blockchain, các tính chất về bảo mật, minh bạch lại được tập trung phát triển vào những nền tảng giao dịch, mã hoá mà chưa thực sự có nhiều ảnh hưởng tới thói quen của người dùng phổ thông. Hai mảng công nghệ này thường được coi là đối lập và không có liên kết với nhau. Tuy nhiên, nếu kết hợp chúng lại với nhau, các điểm yếu nêu trên sẽ được giải quyết.

Với mục tiêu đưa AI phi tập trung thay thế, khắc phục những vấn đề của AI tập trung, ta sẽ giải quyết bài toán nhỏ hơn trong lĩnh vực sinh ảnh. Hiện nay, các dịch vụ sinh ảnh nổi tiếng như MidJourney hay DALL-E đã đạt được số lượng người dùng lớn, tuy nhiên các vấn đề về của AI tập trung vẫn thường xuyên xuất hiện, đặc biệt là khả năng mở rộng còn hạn chế. Hơn nữa, các mô hình sinh ảnh mã nguồn mở đã phát triển mạnh mẽ cùng với sự phát triển mạnh của cộng đồng đã cho các kết quả tốt như mô hình Stable Diffusion (hình 1.1).

1.2 Các giải pháp hiện tại và hạn chế

Hiện tại, hầu hết các giải pháp AI đều tập trung vào mô hình tập trung, nơi mà các tổ chức lớn như OpenAI, Microsoft và Google nắm giữ quyền kiểm soát và phát triển công nghệ. Các hệ thống như ChatGPT, GPT-4 và DALL-E của OpenAI, cũng như dịch vụ sinh ảnh của MidJourney, là những ví dụ điển hình.

Tuy nhiên, các giải pháp tập trung này tồn tại nhiều hạn chế đáng kể:

1. **Bảo mật và quyền riêng tư:** Việc tập trung dữ liệu tại các tổ chức lớn dẫn đến những lo ngại về bảo mật và quyền riêng tư. Dữ liệu người dùng có thể bị lạm dụng hoặc truy cập trái phép, gây ra các rủi ro về thông tin cá nhân.
2. **Minh bạch và khả năng kiểm soát:** Người dùng thường không có quyền kiểm soát và không thể biết rõ cách thức mà dữ liệu của họ được sử dụng hoặc các



Hình 1.1: Ảnh sinh từ mô hình Stable Diffusion XL.

quyết định được đưa ra như thế nào. Điều này tạo ra sự thiếu minh bạch và tin tưởng.

3. **Khả năng tiếp cận:** Do tính tập trung, các dịch vụ AI này có thể gặp phải các vấn đề về tiếp cận, chẳng hạn như giới hạn địa lý hoặc yêu cầu chi phí cao, làm giảm khả năng tiếp cận của người dùng toàn cầu.
4. **Tính mở rộng:** Các hệ thống tập trung đôi khi gặp khó khăn trong việc mở rộng quy mô một cách hiệu quả, đặc biệt khi nhu cầu sử dụng tăng đột biến. Điều này có thể dẫn đến giảm hiệu suất và trải nghiệm người dùng.
5. **Độ tin cậy:** Phụ thuộc vào một số ít các tổ chức lớn cũng làm tăng rủi ro về độ tin cậy. Nếu các dịch vụ này gặp sự cố hoặc bị tấn công, người dùng sẽ bị ảnh hưởng nặng nề.

Những hạn chế này đã thúc đẩy sự phát triển của các giải pháp AI phi tập trung, nhằm khắc phục các vấn đề về bảo mật, quyền riêng tư, minh bạch, khả năng tiếp cận, tính mở rộng và độ tin cậy. Để bảo mật quyền riêng tư, dữ liệu của người dùng nhưng vẫn đảm bảo các mô hình liên tục được cập nhật và huấn luyện dựa trên dữ liệu mới, các nghiên cứu về học liên kết (federated learning) đã được đề xuất và đang cố gắng đưa vào thực tiễn nhưng vẫn còn nhiều hạn chế trong việc phòng chống tấn công bằng mô hình độc hại, bảo mật trong quá trình gửi cập nhật mô hình từ thiết bị tới máy chủ. Hơn nữa, các thuật toán học liên kết đến nay chưa thể hiện được sự mạnh mẽ và cần nhiều nỗ lực phát triển hơn trong tương lai. Song hành với sự phát triển của AI, blockchain là công nghệ xuất hiện đại diện cho tính