

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
PHÂN HIỆU TẠI TP. HỒ CHÍ MINH
BỘ MÔN CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN TỐT NGHIỆP

ĐỀ TÀI:

**SÀN GIAO DỊCH PHI TẬP TRUNG
CHO TRANH ẢNH KỸ THUẬT SỐ
ÁP DỤNG CÔNG NGHỆ BLOCKCHAIN**

Giảng viên hướng dẫn: **TRẦN THỊ DUNG**
Sinh viên thực hiện: **HỒ NGUYỄN THANH PHONG**
Lớp: **CQ.59.CNTT**
Khoá: **K59**

Tp. Hồ Chí Minh, năm 2022

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
PHÂN HIỆU TẠI TP. HỒ CHÍ MINH
BỘ MÔN CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN TỐT NGHIỆP

ĐỀ TÀI:

**SÀN GIAO DỊCH PHI TẬP TRUNG
CHO TRANH ẢNH KỸ THUẬT SỐ
ÁP DỤNG CÔNG NGHỆ BLOCKCHAIN**

Giảng viên hướng dẫn: **TRẦN THỊ DUNG**
Sinh viên thực hiện: **HỒ NGUYỄN THANH PHONG**
Lớp: **CQ.59.CNTT**
Khoá: **K59**

Tp. Hồ Chí Minh, năm 2022

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

BỘ MÔN: CÔNG NGHỆ THÔNG TIN

-----***-----

Mã sinh viên: 5951071074

Họ tên SV: Hồ Nguyễn Thanh Phong

Khóa: 59

Lớp: CQ.59.CNTT

1. Tên đề tài

SÀN GIAO DỊCH PHI TẬP TRUNG CHO TRANH ẢNH KỸ THUẬT SỐ ÁP
DỤNG CÔNG NGHỆ BLOCKCHAIN

2. Mục đích, yêu cầu

a. Mục đích

Cung cấp giải pháp hỗ trợ mua bán tranh ảnh kỹ thuật số an toàn, minh bạch và có khả năng xác thực chủ sở hữu trên môi trường Internet một cách nhanh chóng và hiệu quả.

b. Yêu cầu

● Yêu cầu công nghệ

- HTML, CSS, Javascript
- ReactJS, NodeJS, MongoDB
- Solidity, ERC721
- Binance Smart Chain Testnet
- Visual Studio Code, Remix-Ethereum IDE

- **Yêu cầu chức năng**

- Chuyển đổi tranh ảnh kỹ thuật số thành tranh ảnh **NFT(Non-Fungible Token - Tài sản không thể thay thế)**
- Cấp chứng chỉ quyền tác giả tranh ảnh NFT
- Lưu trữ phi tập trung tranh ảnh kỹ thuật số
- Xây dựng sàn giao dịch phi tập trung
- Tra cứu thông tin tranh ảnh NFT thông qua mã QR
- Đăng bán hoặc tạo phiên đấu giá tranh ảnh NFT
- Mua hoặc tham gia đấu giá tranh ảnh NFT
- Cập nhật thông tin quyền sở hữu tranh ảnh NFT

- **Yêu cầu phi chức năng**

- Tốc độ: Truy cập, truy xuất dữ liệu nhanh
- Dữ liệu: Bảo toàn, minh bạch
- Giao diện: Thân thiện

3. Nội dung và phạm vi đề tài

a. Nội dung

- Mô tả vấn đề
- Hướng tiếp cận
- Kiến thức nền tảng
- Các giải pháp tương tự trên thế giới
- Giải pháp đề xuất
- Đánh giá giải pháp
- Tổng kết và hướng phát triển trong tương lai

b. Phạm vi vấn đề

- Nghiên cứu về tranh ảnh kỹ thuật số và sàn giao dịch phi tập trung
- Nghiên cứu về Blockchain, Hợp đồng thông minh, NFT(Non-fungible Token)
- Nghiên cứu về Javascript và các thư viện của Javascript

4. Công nghệ, công cụ và ngôn ngữ lập trình

- Ngôn ngữ lập trình: HTML, CSS, Javascript, Solidity
- Công nghệ: ReactJS, MongoDB
- Môi trường: NodeJS
- Mạng Blockchain: Binance Smart Chain Testnet
- Tiêu chuẩn hợp đồng thông minh: ERC721
- Công cụ: Visual Studio Code, Remix-Ethereum IDE

5. Các kết quả chính dự kiến sẽ đạt được và ứng dụng

- Áp dụng thành công công nghệ Blockchain
- Chuyển đổi tranh ảnh kỹ thuật số thành tranh ảnh NFT
- Cấp chứng chỉ xác thực quyền tác giả tranh ảnh NFT
- Xác thực tranh ảnh kỹ thuật số
- Xác thực quyền sở hữu tranh ảnh NFT
- Xây dựng sàn giao dịch phi tập trung
- Tra cứu thông tin tranh ảnh NFT thông qua mã QR
- Đăng bán hoặc tạo phiên đấu giá tranh ảnh NFT
- Mua hoặc tham gia đấu giá tranh ảnh NFT

6. Giáo viên và cán bộ hướng dẫn

Họ tên: TRẦN THỊ DUNG

Đơn vị công tác:

Điện thoại: 0388389579

Email: Ttdung@utc2.edu.vn

Ngày tháng năm 2022 Trưởng BM Công nghệ Thông tin	Đã giao nhiệm vụ TKTN Giáo viên hướng dẫn
ThS. Trần Phong Nhã	ThS Trần Thị Dung

Đã nhận nhiệm vụ TKTN

Sinh viên: Hồ Nguyễn Thanh Phong

Điện thoại: 0364015141

Ký tên:

Email: 5951071074@st.utc2.edu.vn

LỜI CẢM ƠN

Lời đầu tiên chúng em xin gửi lời cảm ơn chân thành đến quý thầy, cô giáo trong **Bộ môn Công nghệ thông tin – Phân hiệu Trường Đại học Giao thông vận tải**. Những người đã truyền dạy, đã trang bị cho em kho tàng kiến thức về bầu trời công nghệ thông tin rộng lớn. Ở đây, chúng em không chỉ học được kiến thức về sách vở mà còn học được các bài học, kỹ năng sống. Đặc biệt, em xin gửi lời cảm ơn chân thành và sâu sắc đến cô **Trần Thị Dung**, đã giúp đỡ em trong quá trình hoàn thành Đồ án tốt nghiệp, người đã bỏ thời gian quý báu, thậm chí là thời gian nghỉ ngơi để hướng dẫn, để giúp em có thêm kinh nghiệm để phân tích vấn đề một cách tốt nhất và tối ưu nhất.

Trong quá trình học tập và tìm hiểu chúng em đã nỗ lực rất nhiều với mong muốn hoàn thành Đồ án một cách tốt nhất, nhưng đời người sẽ có những thiếu sót không thể tránh khỏi, và với những người chưa chững chạc và trưởng thành như chúng em thì sai lầm là không thể không mắc phải. Chúng em mong thầy, cô bộ môn có thể thông cảm và cho chúng em những ý kiến, đóng góp để chúng em có thể hoàn thành Đồ án của mình một cách trọn vẹn nhất trước khi rời xa ngôi trường này.

Sau cùng, chúng em xin kính chúc Quý Thầy Cô trong **Bộ môn Công nghệ thông tin** lời chúc sức khỏe, luôn hạnh phúc và thành công hơn nữa trong công việc cũng như trong cuộc sống.

Em xin chân thành cảm ơn!

This image shows a full page of a document template designed for handwritten notes or essays. It features approximately 28 evenly spaced, thin grey horizontal lines across the entire width of the page. The margins are consistent on all sides, providing ample space for writing. There are no pre-printed questions, headings, or other markings on the page.

Giảng viên hướng dẫn

MỤC LỤC

CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI	1
1.1 Lý do chọn đề tài	1
1.2 Mục tiêu đề tài	2
1.3 Phương pháp nghiên cứu	2
1.4 Đối tượng nghiên cứu	3
1.5 Những điểm mới của đề tài	4
1.6 Yêu cầu chức năng và phi chức năng	4
1.7 Cấu trúc báo cáo đồ án tốt nghiệp	5
1.7.1 Chương 1: Tổng quan đề tài	5
1.7.2 Chương 2: Hướng tiếp cận	5
1.7.3 Chương 3: Giới thiệu công nghệ	6
1.7.4 Chương 4: Giải pháp đề xuất - DIGIPOS	6
1.7.5 Chương 5: Đánh giá giải pháp	7
1.7.6 Chương 6: Tổng kết và khả năng phát triển trong tương lai	7
1.7.7 Tài liệu tham khảo	7
CHƯƠNG 2: HƯỚNG TIẾP CẬN	8
2.1 Tranh ảnh kỹ thuật số	8
2.1.1 Tranh truyền thống	8
2.1.2 Tranh kỹ thuật số và hình ảnh kỹ thuật số	8
2.2.2.1 Tranh kỹ thuật số	8
2.2.2.2 Hình ảnh kỹ thuật số	8
2.1.3 Tại sao chọn tranh ảnh kỹ thuật số?	9
2.2 Sàn giao dịch phi tập trung	9
2.2.1 Sàn giao dịch tập trung	9

2.2.2 Sàn giao dịch phi tập trung	10
2.2.3 Tại sao chọn sàn giao dịch phi tập trung?	10
2.3 Blockchain	11
2.3.1 Định nghĩa	11
2.3.2 Thành phần của Blockchain.	11
2.3.3 Đặc tính của Blockchain	14
2.3.4 Các ứng dụng của Blockchain	14
2.3.5 Hợp đồng thông minh(Smart Contract)	16
2.4 Non-Fungible Token	18
2.4.1 Định nghĩa	18
2.4.2 Ứng dụng của NFT	18
2.4.3 ERC721	19
CHƯƠNG 3: CƠ SỞ LÝ THUYẾT	20
3.1 HTML	20
3.2 CSS	20
3.3 Javascript	20
3.4 ReactJS	21
3.5 NodeJS	21
3.6 IPFS	21
3.7 Solidity	22
3.8 Ví điện tử Metamask	22
3.9 Thuật toán sinh chữ ký số ECDSA	22
CHƯƠNG 4: PHÂN TÍCH THIẾT KẾ HỆ THỐNG	23
4.1 Chức năng hệ thống	23
4.2 Quy trình chuyển tranh ảnh kỹ thuật số thành tranh ảnh NFT và cấp chứng chỉ quyền tác giả	24

4.3 Quy trình xác thực bằng tranh ảnh gốc hoặc chứng chỉ	25
4.4 Xác thực tranh ảnh thông qua mã QR	26
4.5 Giải pháp về sàn giao dịch	27
4.5.1 Giải pháp trao đổi mua bán	27
4.5.2 Giải pháp đấu giá	28
4.6 Quy trình đăng bán hoặc tạo phiên đấu giá	29
4.7 Quy trình mua hoặc nhận NFT khi thắng phiên đấu giá	30
4.8 Quy trình đặt giá thầu	31
CHƯƠNG 5: ĐÁNH GIÁ GIẢI PHÁP	32
5.1 Ứng dụng	32
5.2 Kiến trúc hệ thống	37
5.3 Kiến trúc công nghệ	37
5.4 Ưu điểm và nhược điểm	38
5.4.1 Ưu điểm	38
5.4.1 Ưu điểm	38
5.5 Khả năng triển khai giải pháp	38
TỔNG KẾT VÀ KIẾN NGHỊ	39
6.1 Tổng kết	39
6.2 Kiến nghị	39
TÀI LIỆU THAM KHẢO	40

DANH MỤC CHỮ VIẾT TẮT

STT	Từ khóa	Ý nghĩa
1	NFT	Non-Fungible Token(Tài sản không bị thay thế)
2	CEX	Centralized Exchange(Sàn giao dịch tập trung)
3	DEX	Decentralized Exchange(Sàn giao phi dịch tập trung)
4	P2P	Peer-to-peer
5	HTML	Hypertext Markup Language
6	CSS	Cascading Style Sheets
7	IPFS	InterPlanetary File System
8	HTTP	Hypertext Transfer Protocol
9	ECDSA	Elliptic Curve Digital Algorithm
10	DIGIPOS	Digital Possession

BẢNG BIỂU, SƠ ĐỒ, HÌNH VẼ

Hình 4.1	Chức năng hệ thống	23
Hình 4.2	Quy trình chuyển tranh ảnh kỹ thuật số thành NFT và chấp chứng chỉ	24
Hình 4.3	Quy trình xác thực bằng tranh ảnh gốc hoặc chứng chỉ	25
Hình 4.4	Xác thực tranh ảnh thông qua mã QR	26
Hình 4.5	Giải pháp trao đổi mua bán	27
Hình 4.6	Giải pháp đấu giá	28
Hình 4.7	Quy trình đăng bán hoặc tạo phiên đấu giá	29
Hình 4.8	Quy trình mua hoặc nhận NFT	30
Hình 4.9	Quy trình đặt giá thầu	31
Hình 5.1	Quá trình chuyển đổi tranh ảnh kỹ thuật số thành NFT	32
Hình 5.2	Chứng chỉ quyền tác giả	33
Hình 5.3	Xác thực tranh ảnh NFT	34
Hình 5.4	Bộ sưu tập tranh ảnh	34
Hình 5.5	Thông tin chi tiết và thông tin đăng bán	35
Hình 5.6	Thông tin nguồn gốc tranh ảnh NFT	36
Hình 5.7	Thông tin đăng bán hoặc tạo phiên đấu giá	36
Hình 5.8	Kiến trúc hệ thống	37
Hình 5.9	Kiến trúc công nghệ	37
Hình 5.10	Khả năng triển khai giải pháp	38

LỜI NÓI ĐẦU

Ngày nay khoa học kỹ thuật đang phát triển với tốc độ rất nhanh. Công nghệ thông tin là một ngành khoa học cũng đang phát triển mạnh mẽ, ứng dụng rộng rãi trên nhiều lĩnh vực và sản sinh ra nhiều công nghệ khoa học mới. Và các năm gần đây, một công nghệ mới đang dần phổ biến với độ phủ sóng ngày càng tăng, đó là Blockchain. Với điểm mạnh của công nghệ Blockchain về Tốc độ xử lý - Khả năng lưu trữ - Độ bảo mật - Tính minh bạch. Nhiều tập đoàn, công ty về công nghệ thông tin đã cung cấp các dịch vụ và giải pháp phần mềm Blockchain trong nhiều lĩnh vực như Sản xuất, Hậu cần, Chuỗi cung ứng, Thương mại điện tử, Kinh tế chia sẻ, Nông nghiệp, Công nghệ tài chính, Dịch vụ công, Đô thị thông minh,...

Nhờ các giải pháp công nghệ Blockchain, mà nhiều khó khăn trong nhiều lĩnh vực khác ngoài lĩnh vực khoa học kỹ thuật được giải quyết một cách nhanh chóng và rõ ràng. Kế thừa các đặc tính nổi bật và sự hiệu quả của giải pháp công nghệ Blockchain, đề tài xin phép áp dụng công nghệ Blockchain để thiết kế giải pháp giải quyết các vấn nạn sao chép tranh ảnh kỹ thuật số trên các sàn giao dịch tranh ảnh kỹ thuật số hiện nay, bao gồm xác thực quyền sở hữu, quyền tác giả một cách nhanh chóng, minh bạch và tốn ít chi phí. Bên cạnh đó, giải pháp của đề tài sẽ nghiên cứu và xây dựng một sàn giao dịch phi tập trung cho tranh ảnh kỹ thuật số, sàn giao dịch hỗ trợ giao dịch tranh ảnh kỹ thuật số trên nền tảng Blockchain sẽ bảo đảm quyền sở tác giả và quyền sở hữu của chủ sở hữu mới một cách minh bạch. Sản phẩm của giải pháp được đặt tên là DIGIPOS(Digital Possession - Sở hữu kỹ thuật số).

CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI

1.1 Lý do chọn đề tài

Hiện nay, khi khoa học kỹ thuật đang phát triển với tốc độ rất nhanh, đặc biệt là ngành công nghệ thông tin. Với sự phát triển nhanh chóng đó, một sản phẩm của công nghệ thông tin đang được áp dụng để hỗ trợ phát triển ngành tài chính và thị trường đó là các sàn giao dịch thương mại điện tử, hỗ trợ quản lý các giao dịch ở nhiều lĩnh vực khác nhau.

Và hiện nay, có nhiều sàn giao dịch về tranh ảnh đang hoạt động rất mạnh mẽ, mang lại lợi nhuận cao cho các họa sĩ, nhiếp ảnh gia, người kinh doanh tranh ảnh và các nhà sưu tầm tranh ảnh. Nhưng bên cạnh đó, vẫn có nhiều vấn đề khó khăn và các vấn nạn đang diễn ra trên các sàn giao dịch tranh ảnh hiện nay. Tranh ảnh không có nguồn gốc và chưa được xác minh quyền tác giả được đăng tải hàng loạt lên các sàn giao dịch tranh ảnh, gây ảnh hưởng đến quyền lợi của tác giả. Dẫn đến việc cần thiết của các tổ chức xác thực quyền tác giả của các tài sản. Nhưng các tổ chức xác thực quyền tác giả trung gian hiện nay vẫn đang sử dụng các phương pháp truyền thống để tiến hành quá trình xác minh quyền tác giả, quá trình phải trải qua rất nhiều giai đoạn từ tiếp nhận hồ sơ đến lưu trữ kết quả và còn sử dụng giấy mực để làm công cụ lưu trữ, dẫn đến quá trình xác minh tốn nhiều thời gian và chi phí. Đối với tranh ảnh không nguồn gốc và chưa được xác minh đang tồn tại trên các sàn giao dịch tranh ảnh, rất dễ dàng diễn ra vấn nạn sao chép vào đạo nhái tranh ảnh, dẫn đến việc chủ sở hữu có thể bị đánh cắp chất xám hay mất trắng tài sản của mình. Với các khó khăn và vấn nạn đó, khi sàn giao dịch thực hiện giao dịch chuyển đổi tranh ảnh không nguồn gốc hay bị sao chép và đạo nhái, sẽ gây ảnh hưởng đến quyền sở hữu của các chủ sở hữu mới cũng như đánh mất giá trị thật của tranh ảnh gốc. Ngoài ra, hầu hết các sàn giao dịch tranh ảnh hiện nay đang tổ chức theo mô hình tập trung, sàn giao dịch giữ lại tài sản và tiền của người dùng để thực hiện giao dịch chuyển đổi tài sản, không thể hiện sự minh bạch với người dùng và thao túng tài sản và tiền của người tham gia giao dịch, dẫn đến việc người dùng có thể mất trắng tài sản và tiền.

Nhận thấy các vấn đề khó khăn và các vấn nạn kể trên, em đã thực hiện nghiên cứu và thực hiện đề tài: **“Sàn giao dịch phi tập trung cho tranh ảnh kỹ thuật số áp dụng công nghệ Blockchain”**. Nhằm giải quyết các vấn đề khó khăn về quá trình xác minh quyền tác giả, cũng như tạo ra môi trường giao dịch tranh ảnh minh bạch, đảm bảo giá trị tranh ảnh và quyền sở hữu của người dùng một cách nhanh chóng và tiết kiệm chi phí.

1.2 Mục tiêu đề tài

Xây dựng ứng dụng Web áp dụng giải pháp Blockchain hỗ trợ chuyển tranh ảnh kỹ thuật số thành tranh ảnh **NFT(Non-Fungible Token - Tài sản không thể thay thế)**, cấp chứng chỉ xác thực quyền tác giả tranh ảnh NFT. Ngoài ra, giải pháp còn xây dựng sàn giao dịch phi tập trung đưa các tranh ảnh NFT ra thị trường về hội họa và nhiếp ảnh. Ứng dụng hỗ trợ người dùng thực hiện đăng bán hoặc tạo phiên đấu giá, và khi trao đổi tranh ảnh NFT vẫn đảm bảo quyền tác giả của tác giả và quyền sở hữu của chủ sở hữu mới, đặc biệt là giá trị của tranh ảnh không bị thay đổi và chia nhỏ.

1.3 Phương pháp nghiên cứu

Để thực hiện được những yêu cầu mà đề tài đặt ra. Em đã tham khảo các ứng dụng về xác thực tài sản bằng công nghệ Blockchain và các thị trường về NFT như:

- Ứng dụng xác thực tài sản:
 - BLOCKCERTS: <https://www.blockcerts.org/>
 - Origin Stamp: <https://originstamp.com/>
- Thị trường NFT:
 - OpenSea: <https://opensea.io/>
 - Binance Marketplace: <https://www.binance.com/en/nft/marketplace>
- Một số tài liệu liên quan khác

1.4 Đối tượng nghiên cứu

Tác giả tranh ảnh: Cần có một hệ thống xử lý nhanh và an toàn để xác thực quyền tác giả tranh ảnh, giúp tác giả khẳng định được quyền tác giả cũng như cấp chứng chỉ để làm căn cứ xác thực. Khi đảm bảo được quyền lợi của tác giả, tranh ảnh dễ dàng được đăng bán hay đặt vào phiên đấu giá trên thị trường hội họa và nhiếp ảnh.

Tranh ảnh kỹ thuật số: Sẽ được số hóa từ tài sản kỹ thuật số thành một loại tài sản số hóa là NFT bằng công nghệ Blockchain, từ đó đảm bảo được tính độc nhất của tranh ảnh và quyền tác giả cũng như quyền sở hữu tranh ảnh.

Tranh ảnh NFT: Đáp ứng trào lưu về công nghệ đang rất phổ biến trong nhiều lĩnh vực đặc biệt là: công nghệ thông tin, hội họa, nhiếp ảnh, Thị trường tranh ảnh NFT đang ngày càng phát triển bởi giá trị khổng lồ của tranh ảnh NFT mang lại.

Các nhà sưu tầm tranh ảnh và người dùng khác: Được hỗ trợ thực hiện nhu cầu sưu tầm tranh ảnh, hệ thống xây dựng một thị trường NFT cho phép nhiều đối tượng người dùng mua hay đấu giá các tranh ảnh NFT. Khi áp dụng công nghệ Blockchain, quá trình trao đổi mua bán tranh ảnh sẽ diễn ra nhanh chóng nhưng vẫn đảm bảo quyền tác giả của tác giả và quyền sở hữu của chủ sở hữu mới.

1.5 Những điểm mới của đề tài

Cung cấp giải pháp công nghệ mới là Blockchain trong lĩnh vực hội họa, nhiếp ảnh,...

Loại bỏ phương pháp xác thực tài sản truyền thống, áp dụng Blockchain để thực hiện quá trình xác thực.

Áp dụng tài sản được số hóa bằng công nghệ Blockchain lên tranh ảnh kỹ thuật số.

Cung cấp sàn giao dịch phi tập trung tranh ảnh NFT để người dùng có thể đăng bán, tạo phiên đấu giá, trao đổi mua bán và tham gia đấu giá tranh ảnh NFT.

Các hoạt động và giao dịch diễn ra trên DIGIPOS được xử lý tốc độ cao - bảo toàn - minh bạch.

1.6 Yêu cầu chức năng và phi chức năng

- Yêu cầu chức năng
 - Chuyển đổi tranh ảnh kỹ thuật số thành tranh ảnh NFT
 - Cấp chứng chỉ quyền tác giả tranh ảnh NFT
 - Lưu trữ phi tập trung tranh ảnh kỹ thuật số
 - Tra cứu thông tin tranh ảnh NFT thông qua mã QR
 - Xây dựng sàn giao dịch phi tập trung
 - Đăng bán hoặc tạo phiên đấu giá tranh ảnh NFT
 - Mua hoặc tham gia đấu giá tranh ảnh NFT
 - Cập nhật thông tin quyền sở hữu tranh ảnh NFT
- Yêu cầu phi chức năng
 - Tốc độ: Truy cập, truy xuất dữ liệu nhanh.
 - Dữ liệu: Bảo toàn, minh bạch.
 - Giao diện: Thân thiện.

- Yêu cầu tổ chức
 - Đơn giản, dễ hiểu.
 - Thể hiện rõ kết quả của bài toán.
 - Tổ chức lập trình theo ngôn ngữ Javascript, Solidity và các thư viện liên quan.
 - Thể hiện yêu cầu của vấn đề đặt ra.

1.7 Cấu trúc báo cáo đồ án tốt nghiệp

1.7.1 Chương 1: Tổng quan đề tài

- Lý do chọn đề tài
- Mục tiêu đề tài
- Phương pháp nghiên cứu
- Đối tượng nghiên cứu
- Những điểm mới của đề tài
- Yêu cầu chức năng và phi chức năng

1.7.2 Chương 2: Hướng tiếp cận

- Tranh ảnh kỹ thuật số
- Sàn giao dịch phi tập trung
- Blockchain
- Non-Fungible Token

1.7.3 Chương 3: Giới thiệu công nghệ

- HTML
- CSS
- Javascript
- ReactJS
- NodeJS
- IPFS
- Solidity
- Ví điện tử Metamask
- Thuật toán sinh chữ ký số ECDSA

1.7.4 Chương 4: Giải pháp đề xuất - DIGIPOS

- Chức năng hệ thống
- Quy trình chuyển đổi tranh ảnh kỹ thuật số thành tranh ảnh NFT và cấp chứng chỉ quyền tác giả
- Quá trình xác thực bằng tranh ảnh gốc hoặc chứng chỉ
- Xác thực tranh ảnh thông qua mã QR
- Giải pháp về sàn giao dịch
- Quy trình đăng bán hoặc tạo phiên đấu giá
- Quy trình mua hoặc nhận NFT khi thắng phiên đấu giá
- Quy trình đặt giá thầu

1.7.5 Chương 5: Đánh giá giải pháp

- Ứng dụng
- Kiến trúc hệ thống
- Kiến trúc công nghệ
- Ưu điểm và nhược điểm
- Khả năng triển khai giải pháp

1.7.6 Chương 6: Tổng kết và khả năng phát triển trong tương lai

- Tổng kết
- Khả năng phát triển trong tương lai

1.7.7 Tài liệu tham khảo

CHƯƠNG 2: HƯỚNG TIẾP CẬN

2.1 Tranh ảnh kỹ thuật số

2.1.1 *Tranh truyền thống*

Tranh vẽ là một dạng tác phẩm hội họa phản ánh hiện thực bằng đường nét và màu sắc. Tranh xuất hiện rất sớm trong lịch sử nhân loại, tồn tại dưới nhiều dạng và có nhiều ứng dụng. Các tranh vẽ truyền thống được xây dựng từ các nguyên liệu vật lý khác nhau như màu nước, màu sáp, màu chì, ... và hiện nay các tranh vẽ chất lượng cao còn được vẽ từ các nguyên liệu hiện đại hơn như vải lụa, sơn dầu, canvas, [1]

2.1.2 *Tranh kỹ thuật số và hình ảnh kỹ thuật số*

2.2.2.1 *Tranh kỹ thuật số*

Tranh kỹ thuật số được vẽ từ máy tính với phần mềm chuyên dụng được cài đặt và một công cụ vẽ. Tranh ảnh kỹ thuật số sẽ được vẽ từ các phần mềm máy tính với các mã màu rõ ràng và các đường nét được số hóa rõ ràng. Loại tranh ảnh này sẽ được lưu trữ như một tệp tin trên máy tính với các định dạng tệp: .png, .jpg, .svg, ...

2.2.2.2 *Hình ảnh kỹ thuật số*

Hình ảnh kỹ thuật số hay còn gọi là ảnh số. Đây là hình ảnh được ghi nhận bởi bộ cảm biến điện tử. Sau đó lưu lại trong dữ liệu bộ nhớ của máy ảnh như thẻ nhớ, đĩa, Trong điều kiện đủ ánh sáng, các nguồn sáng phản xạ vào chủ thể đến thấu kính của máy ảnh. Qua màng lọc 3 màu: đỏ, xanh lục, xanh lam, bộ phổ màu này một phần chiếu đến bộ cảm biến.

2.1.3 Tại sao chọn tranh ảnh kỹ thuật số?

Tranh ảnh kỹ thuật số	Tranh ảnh truyền thống
Thông tin rõ ràng(dung lượng, mã màu, ...)	<u>Khó xác định thành phần tranh ảnh</u>
Dễ dàng nhìn thấy	<u>Cần ánh sáng phù hợp để nhìn thấy rõ</u>
Dễ dàng chia sẻ	<u>Vận chuyển khó khăn</u>
Khó bị đánh mất	<u>Dễ dàng đánh mất</u>
<u>Dễ bị sao chép</u>	Khó sao chép
Dễ phát hiện sao chép hay đạo nhái	<u>Khó phát hiện sao chép hay đạo nhái</u>

2.2 Sàn giao dịch phi tập trung

2.2.1 Sàn giao dịch tập trung

Sàn giao dịch tập trung (Centralized Exchange - CEX) là sàn được quản lý bởi một chủ thể nhất định (tổ chức/công ty), các tài sản nạp vào sàn này đều do chủ thể đó quản lý. Với khái niệm trên, có thể nhận thấy cơ chế hoạt động của loại sàn giao dịch này dường như tương tự với ngân hàng. Người dùng cũng cần gửi tài sản của mình cho một bên thứ ba bảo vệ và lưu trữ tài sản của họ. Việc theo dõi nguồn tiền thực hiện thông qua sàn giao dịch. Thực tế, nhiều nhà đầu tư đánh giá với cách thức hoạt động như vậy, họ sẽ lựa chọn gửi tiền vào ngân hàng. Vì đây chủ thể hoạt động dưới sự điều chỉnh và quản lý của Ngân hàng Trung Ương và nhà nước. Các quy định áp dụng lên ngân hàng nghiêm ngặt và khắt khe hơn rất nhiều so với bất kỳ loại hình tổ chức công ty nào. [2]

2.2.2 Sàn giao dịch phi tập trung

Sàn giao dịch phi tập trung (Decentralized Exchange - DEX) là sàn giao dịch không cần một tổ chức/công ty trung gian để lưu trữ và quản lý tài sản của khách hàng. Thay vào đó, người dùng sẽ tự mua và bán thông qua một quy trình tự động (mạng ngang hàng). Như vậy, khi tham gia sàn giao dịch này, người dùng sẽ tự quản lý tài sản của mình. Đồng thời, khi thực hiện giao dịch, người dùng cần tự kiểm tra điểm đáng tin cậy của giao dịch mình thực hiện. Ngoài ra, khi tham gia vào sàn giao dịch phi tập trung, việc phong tỏa tài khoản và tịch thu quỹ, đánh thuế sẽ khó thực hiện. Với cơ chế hoạt động như trên, sàn giao dịch này đã loại được những yếu tố nguy hiểm từ bên ngoài như hacker, lừa đảo ở các công ty quản lý tài sản. Như vậy, yếu tố bảo mật được tăng cường khi thực hiện giao dịch trên các sàn giao dịch phi tập trung. Hiện nay, các sàn giao dịch phi tập trung đang hoạt động có thể kể đến như: Etherdelta, Kyber Network, IDEX, Ox Protocol, DDEX, CoinChangeX,... Trong đó, Vakaxa là công ty xây dựng sàn giao dịch điện tử chuyên nghiệp hàng đầu hiện nay.[2]

2.2.3 Tại sao chọn sàn giao dịch phi tập trung?

	Sàn giao dịch tập trung	Sàn giao dịch phi tập trung
<i>Độ bảo mật và an toàn</i>	<u>Sàn giữ tài sản của bạn, khi bị hack, bạn vẫn có thể mất trắng tài sản.</u>	Sàn giải quyết giao dịch trên mạng ngang hàng, việc bị hack là bất khả thi.
<i>Tính lưu ký</i>	<u>Giao dịch và tài sản do sàn kiểm soát.</u>	Bạn toàn quyền quản lý tài sản của mình.
<i>Tính xác thực</i>	<u>Sàn có khả năng thao túng và sử dụng tài sản của bạn.</u>	Minh bạch và công bằng đối với tài sản của người dùng.

2.3 Blockchain

2.3.1 Định nghĩa

Blockchain được Satoshi Nakamoto phát minh vào năm 2008 và được sử dụng trong Bitcoin, ứng dụng đầu tiên giải quyết thành công vấn đề chi tiêu kép mà không cần máy chủ tập trung. [3]

Blockchain là một cơ sở dữ liệu phân tán được sao chép và chia sẻ giữa các máy tính trong mạng lưới. Cơ sở dữ liệu này có thể được xem như một sổ cái mà mỗi máy tính tham gia sở hữu một bản sao

2.3.2 Thành phần của Blockchain.

- Sổ cái chia sẻ

Khái niệm sổ cái bắt nguồn từ ngành tài chính, là một cuốn sổ giấy hoặc tệp máy tính để lưu trữ các nghiệp vụ kinh tế phát sinh trong một thời điểm nhất định. Tương tự đối với công nghệ Blockchain, tất cả dữ liệu về các giao dịch diễn ra trong mạng sẽ được lưu trữ trong sổ cái của mạng. Dữ liệu của sổ cái được chia sẻ với tất cả những máy tính tham gia trong mạng để các máy tính này lưu trữ một bản sao. Từ đó, dữ liệu này là chỉ có thể đọc và ghi, không thể xóa hoặc sửa dữ liệu đã được lưu vào sổ cái.

Cấu trúc của sổ cái giống như một danh sách liên kết ngược, liên kết các khối với nhau. Khi các giao dịch mới được sinh ra, chúng được chứa trong một khối mới, khối này sẽ liên kết với khối trước đó và sổ cái sẽ mở rộng theo thời gian.[4]

- Mạng Peer-to-peer

P2P là một mô hình mạng thay thế cho mô hình lưu trữ client-server truyền thống. Trong mô hình máy client-server, client chỉ có thể gửi yêu cầu đến server và chờ phản hồi từ server. Không giống như client-server, mạng P2P sử dụng mô hình phi tập trung trong đó mỗi máy tính, được gọi là mạng ngang hàng, hoạt động như client và server cùng một lúc. Điều này có nghĩa là một máy tính trong mạng có thể gửi yêu cầu đến các máy tính khác, đồng thời có thể nhận và trả lời các yêu cầu từ các máy tính khác trong mạng.[5]

Nhờ kiến trúc trên, mạng P2P có nhiều ưu điểm hơn so với mô hình mạng client-server:

- *Độ hiệu quả trong xử lý*: Trong mô hình truyền thống, khi số lượng client tăng lên, hiệu suất của server sẽ giảm xuống. Nhưng đối với mạng P2P, hiệu suất của mạng tăng lên khi số lượng máy tính tham gia vào mạng tăng lên. Khi một máy tính cần tải xuống hoặc tải lên một tệp, các máy tính khác trong mạng chia sẻ băng thông với máy tính đó. Như vậy, càng có nhiều máy tính tham gia mạng, càng nhiều máy tính cùng chia sẻ băng thông thì tốc độ tải xuống sẽ càng cao. Điều này cải thiện hiệu suất của mạng. Một máy tính có thể tải xuống và tải lên cùng một lúc, đồng thời trong quá trình này, các máy tính khác có thể tham gia chia sẻ hoặc ngắt kết nối bất kỳ lúc nào.
- *Khả năng chống lỗi*: Tất cả những máy tính tham gia mạng P2P đều chia sẻ băng thông để tải xuống, vì vậy nếu một máy tính trong mạng ngắt kết nối, quá trình tải xuống sẽ được tiếp tục bằng cách gửi một yêu cầu. yêu cầu và nhận phản hồi từ các máy tính khác.

Sở cái được chia sẻ cho những máy tính tham vào mạng Blockchain thông qua mạng ngang hàng (P2P). Mỗi máy tính tham gia trong mạng giữ một bản sao của sổ cái. Điều này tạo ra sự minh bạch cho dữ liệu.

- **Mật mã học**

Cặp khóa là nền tảng của mật mã được sử dụng trong Blockchain. Mỗi cặp khóa bao gồm khóa công khai và khóa riêng tư, tương tự như tên người dùng và mật khẩu của tài khoản ngân hàng. Khóa công khai có thể được sử dụng để xem thông tin tài khoản, chi tiết giao dịch, v.v., nhưng không được sử dụng để phê duyệt các giao dịch diễn ra trên tài khoản. Giống như mật khẩu, khóa riêng tư không được chia sẻ với bất kỳ ai và được sử dụng để xác thực các giao dịch như gửi tiền.

Cách xác thực giao dịch bằng khóa riêng tư mà không cần gửi cặp khóa là sử dụng chữ ký mã hóa. Giả sử, A và B đã biết khóa công khai của nhau. A gửi cho B một tin nhắn, nhưng B muốn chứng minh rằng tin nhắn đó là do A gửi. Để làm điều này, họ sử dụng chữ ký mã hóa. A sử dụng thuật toán mã hóa tạo chữ ký trên máy tính của A, với khóa riêng tư và nội dung tin nhắn làm đầu vào. Sau đó A gửi tin nhắn và chữ ký đã tạo cho B. Khi nhận

được hai nội dung trên, B sử dụng thuật toán xác minh chữ ký, lấy thông điệp và chữ ký làm đầu vào, để xác định khóa công khai của cặp khóa mà A dùng để tạo chữ ký. Do đó, tin nhắn được xác thực là do A gửi mà không có khóa riêng tư bị lộ.

Sử dụng mật mã trong Blockchain hỗ trợ bảo mật danh tính người dùng, xác nhận tính đúng đắn của các giao dịch và góp phần tạo nên cấu trúc dữ liệu bất biến.

- ***Cơ chế đồng thuận***

Trong các hệ thống hoặc tổ chức tập trung, các quyết định được thực hiện bởi người / nhóm nắm quyền. Nhưng trong mạng lưới Blockchain (môi trường phi tập trung), điều này là không thể. Vì vậy, cần có cơ chế đồng thuận để thực hiện các quyết định đồng thuận. Hiện tại, ba cơ chế đồng thuận phổ biến nhất là[6]:

- *Proof-of-Work, PoW (bằng chứng công việc)*: Satoshi Nakamoto - người tạo ra Bitcoin là người đã phát minh ra khái niệm PoW. Các thợ mỏ giải các câu đố mật mã để khai thác một khối để thêm vào Blockchain. Sau khi giải câu đố, người thợ mỏ gửi khối lên mạng để xác minh. Khi nhiều thợ mỏ giải quyết cùng một câu đố, người giải nhanh nhất và được xác minh nhanh nhất là người chiến thắng và được giữ toàn bộ khối.
- *Proof-of-Stake, PoS (bằng chứng về tiền đặt cọc)*: PoW gây ra sự lãng phí tài nguyên để thực hiện tính toán trong mạng, vì vậy PoW ra đời để giải quyết vấn đề này. Để tìm một khối mới, thay vì toàn bộ máy tính chạy đua để giải câu đố, PoS chọn những máy tính đóng góp nhiều nhất để xác nhận khối mới này. Bạn càng gửi nhiều tiền, bạn càng có nhiều khả năng được chọn để đóng khối.
- *Proof-of-Authority, PoA (bằng chứng về danh tiếng)*: Cả hai cơ chế đồng thuận trên đều có vấn đề về khả năng mở rộng hệ thống, tức là số lượng giao dịch được thực hiện tại một đơn vị thời điểm không cao. Giao dịch càng nhiều máy tính được xác thực thì càng mất nhiều thời gian. PoS có phần nào cải thiện khả năng mở rộng so với PoW, tuy nhiên sự khác biệt không quá lớn. PoA dựa trên một số lượng hạn chế các máy tính được chọn để đóng khối, các nút này phải được phê duyệt, được làm rõ danh tính và hoạt động như người kiểm duyệt cho toàn bộ hệ thống.

2.3.3 *Đặc tính của Blockchain*

Nhờ 4 thành phần thanh của của Blockchain, công nghệ này có những đặc điểm nổi bật và riêng biệt so với các công nghệ trước đây:

- **Tính phi tập trung:** Thay thế mô hình tập trung, các thành phần trung gian trong quá trình giao dịch là ý tưởng cốt lõi của Blockchain. Việc sử dụng mạng P2P giúp Blockchain có được tính năng này. Hơn nữa, tính phi tập trung còn mang lại những ưu điểm vốn có của nó như tốc độ xử lý nhanh, tính sẵn sàng cao và tránh được các lỗi đơn lẻ. Tính phi tập trung tạo ra dân chủ cho những máy tính tham gia hệ thống.
- **Tính toàn vẹn dữ liệu:** Blockchain là một bản ghi vĩnh viễn của các giao dịch. Khi một khối được thêm vào, nó sẽ không thể thay đổi được. Điều này tạo ra sự tin tưởng trong các chi tiết giao dịch.
- **Tính minh bạch về dữ liệu:** Bởi vì Blockchain là một tệp mở, bất kỳ bên nào cũng có thể truy cập và kiểm tra giao dịch. Điều này tạo ra sự minh bạch của dữ liệu.
- **Bảo mật dữ liệu:** Với nền tảng mật mã và sử dụng sức mạnh tính toán của các máy tính tham gia để xác thực giao dịch, hệ thống Blockchain gần như không thể bị tấn công.

2.3.4 *Các ứng dụng của Blockchain*

Với những đặc tính nổi bật của mình, Blockchain trở thành công nghệ phát triển với tốc độ phi thường. Blockchain giải quyết một loạt các vấn đề khó khăn mà trước đây chưa giải quyết được. Vì vậy, nó đến được rất nhiều lĩnh vực và hứa hẹn sẽ phá bỏ nhiều rào cản. Dưới đây là một vài ứng dụng của Blockchain:

- **Tài chính:** Blockchain cung cấp một phương thức chuyển tiền an toàn, nhanh chóng và tiết kiệm chi phí hơn so với các ngân hàng truyền thống. Mỗi cá nhân có quyền tự kiểm soát tài chính của mình mà không cần phải chia sẻ với ngân hàng hay bất kỳ ai.
- **Y tế:** Nhờ Blockchain, bệnh nhân có thể quản lý đầy đủ hồ sơ bệnh án của mình. Không giống như hồ sơ giấy, hồ sơ Blockchain là duy nhất, loại bỏ sự không nhất quán và sự không cần thiết khi phải tiến hành kiểm tra sức khỏe ở các cơ sở y tế

khác nhau. Một bác sĩ có thể truy cập một cách an toàn và nhanh chóng vào hồ sơ bệnh án của bệnh nhân với sự cho phép của bệnh nhân.

- **Giáo dục:** Tình trạng làm giả bằng cấp cần có cơ chế hợp lý để cấp và xác nhận bằng cấp. Quá trình xác thực vật lý tốn nhiều thời gian và chi phí. Bộ chứng thư số trên Blockchain sẽ giải quyết vấn đề trên. Ngoài ra, khả năng xác thực học viên từ xa trong học tập trực tuyến cũng là một ứng dụng của Blockchain trong giáo dục.
- **Logistics:** Các quá trình trao đổi cũng như đường đi của hàng hóa trong chuỗi cung ứng được ghi lại trên sổ cái Blockchain. Điều này sẽ làm giảm gian lận và tăng khả năng truy xuất nguồn gốc trên toàn bộ chuỗi. Logistics là một ngành nghề lớn, việc áp dụng Blockchain sẽ giảm thiểu sai sót của con người và tiết kiệm rất nhiều chi phí.

2.3.5 *Hợp đồng thông minh(Smart Contract)*

Hợp đồng thông minh là một chương trình số hóa một hợp đồng thông thường. Bất kỳ hợp đồng nào được số hóa đều có thể trở thành Hợp đồng thông minh. Thuật ngữ "Thông minh" không có nghĩa là hợp đồng kỹ thuật số có thể đảm bảo sự công bằng cho các bên liên quan. Nó chỉ đảm bảo quá trình thực hiện chính xác như yêu cầu. Ví dụ như hợp đồng mua gói wifi. Nếu bên A chuyển đúng số tiền cho bên B thì bên B sẽ cho A sử dụng wifi trong thời gian tương ứng. Trên thực tế, thỏa thuận này hoàn toàn có thể do hai bên tự lập. Tình trạng này sẽ dẫn đến một số vấn đề. Có thể lập hợp đồng như thế nào để đảm bảo sự công bằng cho các bên tham gia? Hoặc làm thế nào để các bên có thể tự nguyện thực thi các điều khoản của hợp đồng? Trong ví dụ trên, cách soạn thảo hợp đồng với giá gói wifi hợp lý cho cả bên A và bên B và khi bên A chuyển tiền thì bên B sẽ cung cấp băng thông wifi như thế nào. Không những vậy, bên B còn phải đảm bảo thêm một số điều khoản như nếu băng thông wifi quá chậm thì phải tính phí thấp. Rất nhiều câu hỏi có thể phát sinh khi mọi nút tham gia vào một hợp đồng. Trên thực tế, những câu hỏi này chính là chìa khóa để chúng ta đi đến một hợp đồng công bằng, đảm bảo quyền lợi, nghĩa vụ và trách nhiệm của các bên liên quan. Việc thực hiện các điều khoản có thể được thực hiện trên hợp đồng giấy, hợp đồng miệng hoặc Hợp đồng thông minh. Điểm nổi bật của Hợp đồng thông minh là không đưa ra các điều khoản "thông minh" trong hợp đồng cho các bên liên quan, mà đảm bảo rằng hợp đồng sẽ luôn được thực hiện đúng như những gì đã được soạn thảo. Điều này phụ thuộc vào người viết Hợp đồng thông minh. Hợp đồng thông minh được xác định trước trong trường hợp nào thì nó bao hàm khả năng đó. Nhà cung cấp phải cung cấp băng thông wifi, nếu bên B không cung cấp băng thông wifi thì điều khoản khác trong hợp đồng sẽ được kích hoạt, ví dụ hai bên thỏa thuận một điều khoản khác là nếu bên B không cung cấp băng thông wifi thì bên A sẽ lấy lại tiền. Câu chuyện trên sẽ được giải quyết một cách rất đơn giản nếu cả hai bên đều tự nguyện làm theo những gì đã thỏa thuận từ trước, vì không có gì đảm bảo rằng mọi người sẽ làm điều đó. Để thực hiện những gì cả hai bên đã đồng ý, thực sự cần một bên thứ ba. Vì vậy, thay vì sử dụng một bên thứ ba, tổ chức là con người, chúng ta sử dụng Hợp đồng thông minh để kiểm soát việc thực hiện thỏa thuận.[7]

a. Một bên sẽ soạn thảo Hợp đồng thông minh là hợp đồng dưới dạng mã nguồn và đưa lên hệ thống. Nó xác định các bên liên quan, các điều kiện kích hoạt và các sự kiện

liên quan. Lưu ý: Các máy tính trong hệ thống có quyền tham gia vào bất kỳ Hợp đồng thông minh nào miễn là chúng đáp ứng các điều kiện tiên quyết trong Hợp đồng thông minh cũng như chấp nhận các điều khoản đã nêu.

b. Hợp đồng thông minh sẽ không được kích hoạt nếu không có sự kiện nào xảy ra. Sự kiện này có thể là các giao dịch được gửi đến Hợp đồng thông minh đó. Bản thân Hợp đồng thông minh không thể tự kích hoạt. Do đó, Hợp đồng thông minh chỉ mang tính bán tự trị, không hoàn toàn hoạt động.

c. Khi Hợp đồng thông minh được kích hoạt, nó coi các tương tác với nó như là các tham số đầu vào để thực thi. Hợp đồng thông minh dựa trên các tham số đó để quyết định câu lệnh nào sẽ tự động thực thi.

d. Kết quả thực thi của Hợp đồng thông minh là sự thay đổi trạng thái. Trạng thái là trạng thái hiện tại của các bên liên quan. Ví dụ: số dư tài khoản, tình trạng còn hàng, số lượng hàng hóa mà hợp đồng có thể cung cấp, . . .

Lưu ý: Một Hợp đồng thông minh sau khi được kích hoạt có thể tạo ra các tương tác làm thông số đầu vào cho các Hợp đồng thông minh khác tạo ra các giao dịch chuỗi. Nhưng suy cho cùng, để Hợp đồng thông minh đầu tiên hoạt động, nó cũng cần có sự tương tác từ bên ngoài. Sự tương tác này đến từ chính các máy tính tham gia.

2.4 Non-Fungible Token

2.4.1 Định nghĩa

NFT(Non-Fungible Token - Tài sản không thể thay thế), là một đơn vị dữ liệu trên sổ cái kỹ thuật số Blockchain. Nói một cách dễ hiểu, nó là một loại tài sản số hiện diện trên một chuỗi số (Blockchain). Blockchain này có nhiệm vụ như một sổ cái đảm bảo tính xác thực của tài sản lẫn chủ sở hữu. Hầu hết các nội dung, vật thể số trước nay đều có khả năng tái sản xuất vô hạn. Nhưng với NFT thì khác, mỗi tài sản sẽ có chữ ký số riêng biệt và vì thế nó có tính độc nhất. Mỗi NFT được đúc có một mã định danh riêng độc nhất và thuộc về một chủ sở hữu duy nhất. Vì là tài sản số, NFT cũng thường được giao dịch bằng tiền số, nhưng đôi khi cũng sử dụng đồng USD.[8]

2.4.2 Ứng dụng của NFT

NFT đã và đang được ứng dụng phổ biến nhất trong các loại nội dung số như âm nhạc, tranh ảnh hay các nội dung nghệ thuật khác. Ví dụ, khi người họa sĩ bán một bức tranh dưới dạng NFT, người mua sẽ phải trả tiền và trở thành chủ nhân của nó. Những người khác vẫn có thể xem bức tranh, nhưng chỉ người mua mới có quyền sở hữu chính thức.

NFT có tiềm năng vô hạn khi có thể tồn tại trong tất cả các kiểu vật thể số: hình ảnh, video, âm thanh, chữ viết hay thậm chí là một bài đăng Twitter. NFT còn có thể là những mảnh đất trong các môi trường thế giới ảo, là trang phục số hay quyền sử dụng ví tiền mã hóa độc quyền.

Vậy lợi ích mà NFT mang lại là gì? Việc mã hóa các tài sản có thể đem lại những lợi ích đáng kể cho cả người bán lẫn người mua. Vì tài sản NFT có thể xác thực tính thật giả, quyền sở hữu rõ ràng nên việc giao dịch mua bán cũng minh bạch, nhất là với các tác phẩm nghệ thuật mà tính thật giả rất quan trọng trong việc quyết định giá trị. Bản thân người bán cũng có thể bảo vệ quyền sở hữu trí tuệ của mình và hưởng thành quả lao động một cách công bằng hơn.

2.4.3 ERC721

ERC721 là một tiêu chuẩn dành cho hợp đồng thông minh được nhiều lập trình viên thống nhất tuân theo bởi tiêu chuẩn giúp cho việc viết hợp đồng đơn giản và có thể tái sử dụng. Việc tuân theo tiêu chuẩn là tự nguyện và được áp dụng rộng rãi. Đảm bảo token tương thích với đa dạng ứng dụng như sàn giao dịch, dapps, ví.

ERC721 là chuẩn cho Non-Fungible Token (NFT). Chữ “fungible” có nghĩa là “có thể hoán đổi, thay thế được”. Bitcoin là “fungible” và một Bitcoin này có thể thay thế cho một Bitcoin kia. Còn, NFT – Non-Fungible Token hoàn toàn khác. Một NFT này không thể thay thế cho một NFT kia.

CHƯƠNG 3: CƠ SỞ LÝ THUYẾT

3.1 HTML

HTML (viết tắt của từ Hyper Text Markup Language, hay là "Ngôn ngữ Đánh dấu Siêu văn bản") là một ngôn ngữ đánh dấu được thiết kế ra để tạo nên các trang web trên World Wide Web. Nó có thể được trợ giúp bởi các công nghệ như CSS và các ngôn ngữ kịch bản giống như JavaScript.[9]

Các trình duyệt web nhận tài liệu HTML từ một web server hoặc một kho lưu trữ cục bộ và render tài liệu đó thành các trang web đa phương tiện. HTML mô tả cấu trúc của một trang web về mặt ngữ nghĩa và các dấu hiệu ban đầu được bao gồm cho sự xuất hiện của tài liệu.

3.2 CSS

CSS là chữ viết tắt của Cascading Style Sheets, nó là một ngôn ngữ được sử dụng để tìm và định dạng lại các phần tử được tạo ra bởi các ngôn ngữ đánh dấu (HTML). Nói ngắn gọn hơn là ngôn ngữ tạo phong cách cho trang web. Bạn có thể hiểu đơn giản rằng, nếu HTML đóng vai trò định dạng các phần tử trên website như việc tạo ra các đoạn văn bản, các tiêu đề, bảng,...thì CSS sẽ giúp chúng ta có thể thêm style vào các phần tử HTML đó như đổi bố cục, màu sắc trang, đổi màu chữ, font chữ, thay đổi cấu trúc...[10]

Phương thức hoạt động của CSS là nó sẽ tìm dựa vào các vùng chọn, vùng chọn có thể là tên một thẻ HTML, tên một ID, class hay nhiều kiểu khác. Sau đó là nó sẽ áp dụng các thuộc tính cần thay đổi lên vùng chọn đó.

3.3 Javascript

JavaScript là ngôn ngữ lập trình website phổ biến hiện nay, một ngôn ngữ lập trình thông dịch với khả năng hướng đến đối tượng. Nó được tích hợp và nhúng vào HTML giúp website trở nên sống động hơn. JavaScript đóng vai trò như là một phần của trang web, thực thi cho phép tương tác người dùng cũng như phía máy chủ để tạo ra các trang web động.[11]

3.4 ReactJS

ReactJs là một thư viện viết bằng Javascript, dùng để xây dựng giao diện người dùng (UI). React được sử dụng rộng rãi và có hệ sinh thái đa dạng phong phú. Một trong những điểm hấp dẫn của React là thư viện này không chỉ hoạt động trên phía client, mà còn được render trên server và có thể kết nối với nhau. React so sánh sự thay đổi giữa các giá trị của lần render này với lần render trước và cập nhật ít thay đổi nhất trên DOM.[12]

3.5 NodeJS

NodeJS là một môi trường runtime chạy Javascript đa nền tảng và có mã nguồn mở, được sử dụng để chạy các ứng dụng web bên ngoài trình duyệt của client. Nền tảng này được phát triển bởi Ryan Dahl vào năm 2009, được xem là một giải pháp hoàn hảo cho các ứng dụng sử dụng nhiều dữ liệu nhờ vào mô hình hướng sự kiện không đồng bộ.[13]

3.6 IPFS

IPFS là viết tắt của từ Interplanetary File System, một hệ thống tập tin phân tán ngang hàng kết nối tất cả các thiết bị máy tính với nhau. Cụ thể hơn, nó sẽ phân phối dữ liệu được lưu trữ theo hình thức P2P, hay còn gọi là mạng ngang hàng (mạng đồng đẳng). Trong đó, các hoạt động của IPFS chủ yếu dựa vào khả năng tính toán bằng thông của tất cả các máy tham gia chứ không tập trung vào một phần nhỏ các máy chủ trung tâm như giao thức HTTP.[14]

Nói cách khác, IPFS là mạng lưới chuyên phát nội dung hoàn toàn phi tập trung cho phép quản lý và lưu trữ dữ liệu một cách linh hoạt. Mỗi máy tính tham gia trong mạng lưới đảm nhận nhiệm vụ download và upload dữ liệu mà không cần sự can thiệp của máy chủ trung tâm.

3.7 Solidity

Solidity được biết đến là một ngôn ngữ lập trình hướng hợp đồng, được sử dụng hầu hết trong hợp đồng thông minh (nâng cấp và tạo lập). Nói một cách đơn giản hơn thì Solidity chính là ngôn ngữ lập trình cao cấp với cú pháp và câu lệnh gần giống như các ngôn ngữ lập trình phổ biến hiện nay. Solidity là ngôn ngữ lập trình được xây dựng dưới sự thừa kế những đặc điểm phù hợp của các ngôn ngữ lập trình khác, đặc biệt là những đặc tính liên quan đến hợp đồng.[15]

3.8 Ví điện tử Metamask

Metamask là một nền tảng lưu trữ tiền điện tử, nói một cách dễ hiểu, nền tảng này là một loại ví điện tử. Ban đầu, ví điện tử được thiết lập để tương thích với chuỗi khối Ethereum. Sau này, ví Metamask được cải tiến để tích hợp với nhiều Blockchain khác nhau.[16]

Metamask được tích hợp như một tiện ích mở rộng (extensions) để hoạt động trên nhiều trình duyệt web phổ biến hiện nay như Chrome, Firefox, Brave và Edge. Hơn thế nữa, Metamask còn sở hữu ứng dụng ví trên các thiết bị di động.

Ví điện tử còn cho phép người dùng các ứng dụng phi tập trung mà không cần phải đồng bộ toàn bộ Blockchain trên thiết bị hay máy tính. Chính vì những tiện ích đó, Metamask đang dần chiếm được lòng tin của người dùng.

3.9 Thuật toán sinh chữ ký số ECDSA

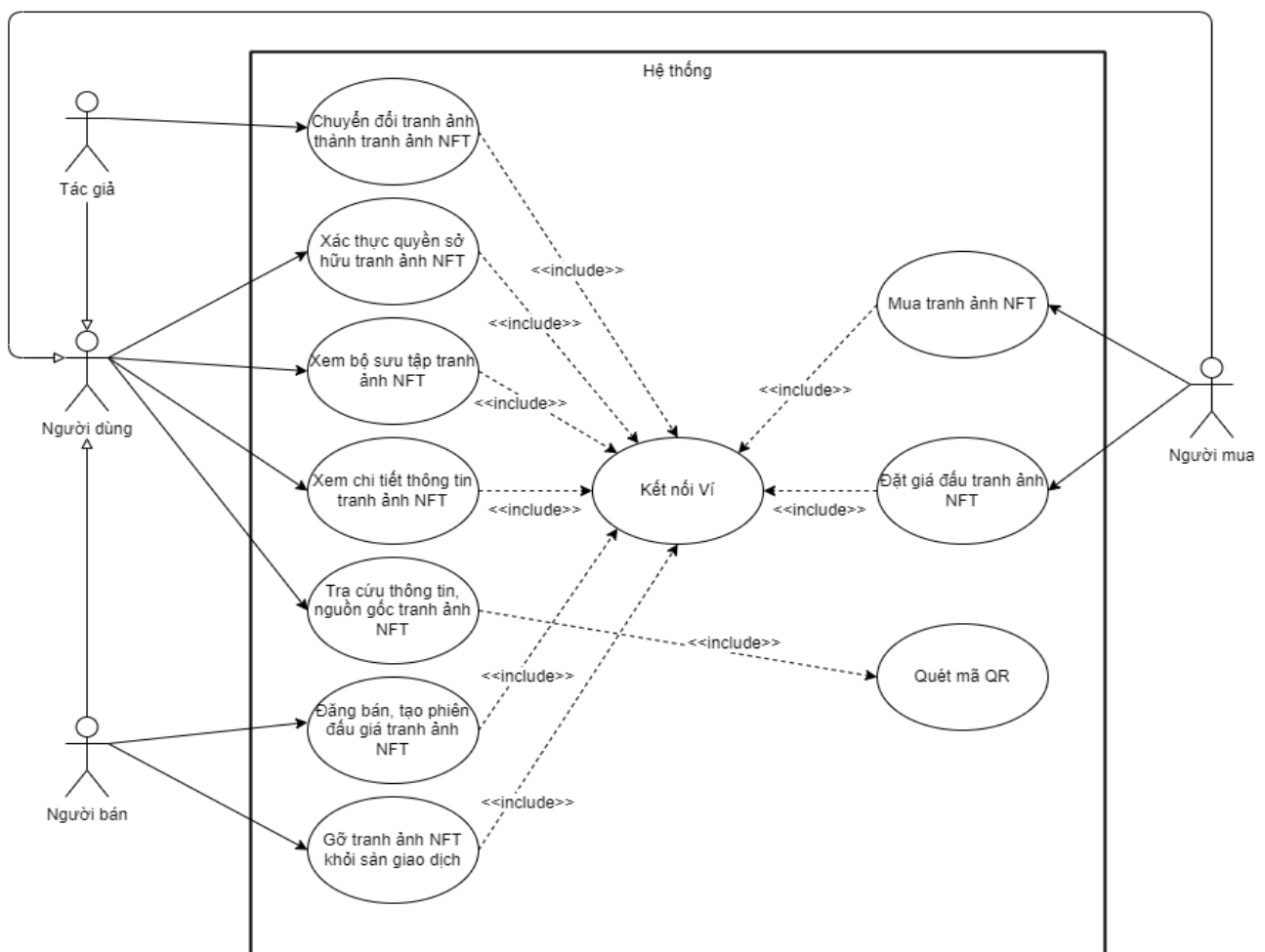
ECDSA là viết tắt của Elliptic Curve Digital Signature Algorithm – thuật toán sinh chữ ký số dựa trên đường cong Elliptic.

ECDSA có một cặp key Private key và Public key. Private key dùng để mã hóa, Public key dùng để xác nhận tính đúng đắn của chữ ký (dữ liệu đã được mã hoá) này. Public key không thể giải mã được dữ liệu đã được mã hoá, do đó dữ liệu gốc luôn luôn được an toàn.[17]

CHƯƠNG 4: PHÂN TÍCH THIẾT KẾ HỆ THỐNG

Nhận thấy các khó khăn và và vấn nạn đang diễn ra trên các sàn giao dịch tranh ảnh tập trung hiện nay, em xin thiết kế một hệ thống để đề xuất giải pháp công nghệ giải quyết và hạn chế các khó khăn và vấn nạn đó. Hệ thống được đặt tên là ***DIGIPOS***(*Digital Possession - Sở hữu kỹ thuật số*).

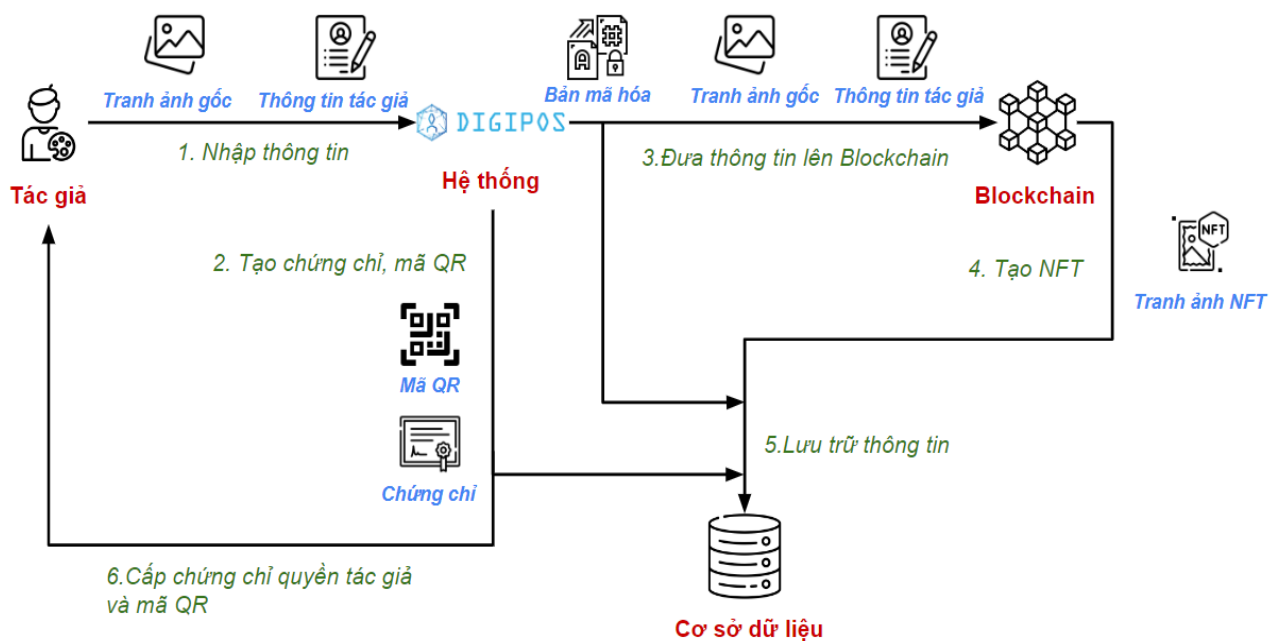
4.1 Chức năng hệ thống



Hình 4.1 Chức năng hệ thống

4.2 Quy trình chuyển tranh ảnh kỹ thuật số thành tranh ảnh NFT và cấp chứng chỉ quyền tác giả

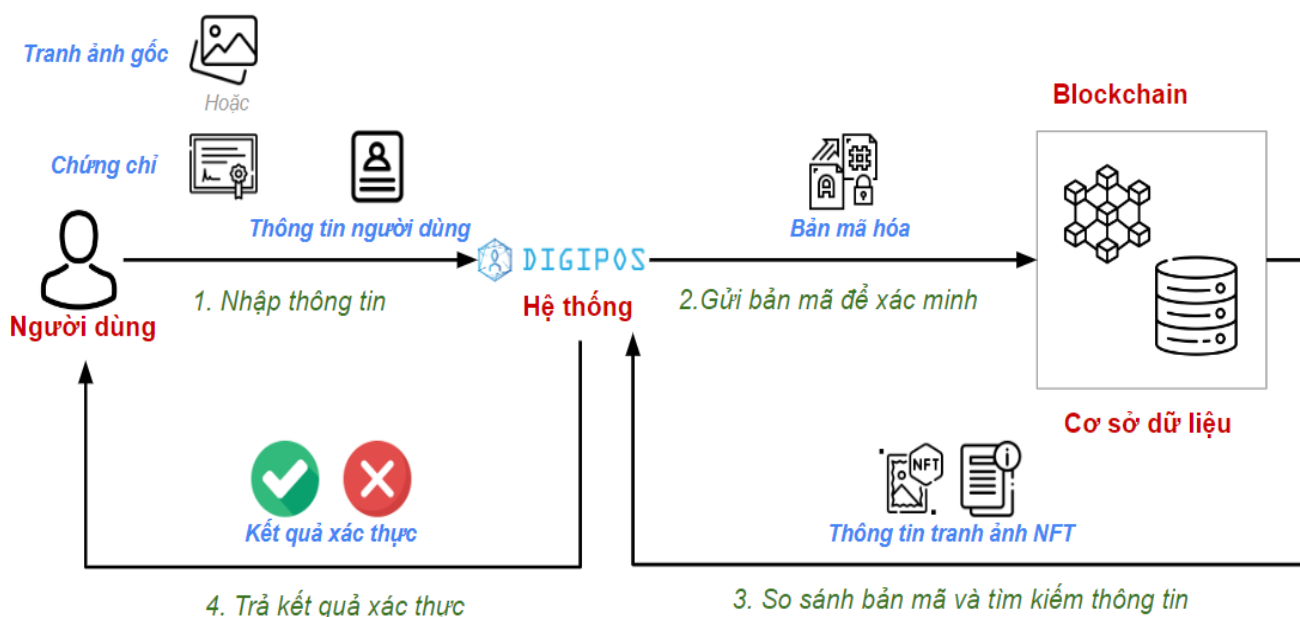
- Ở quy trình này, tác giả sẽ cung cấp tranh ảnh gốc(.png, jpg, ...) và thông tin tác giả (địa chỉ Blockchain, ...) vào hệ thống DIGIPOS.
- DIGIPOS sẽ lấy các thông tin trên để tạo chứng chỉ quyền tác giả và mã QR được đính kèm trên chứng chỉ. Bên cạnh đó, DIGIPOS sẽ băm tranh ảnh gốc để lấy bản mã hóa của tranh ảnh này và lưu trữ bản mã hóa đó để hạn chế tình trạng sao chép.
- Sau đó, các thông tin về tranh ảnh, chứng chỉ và tác giả sẽ được DIGIPOS sử dụng hợp đồng thông minh để đưa lên Blockchain và chuyển đổi thành dạng tài sản số NFT.
- Khi các quá trình diễn ra thành công, DIGIPOS sẽ gửi chứng chỉ quyền tác giả tranh ảnh về cho tác giả.



Hình 4.2 Quy trình chuyển tranh ảnh kỹ thuật số thành NFT và cấp chứng chỉ

4.3 Quy trình xác thực bằng tranh ảnh gốc hoặc chứng chỉ

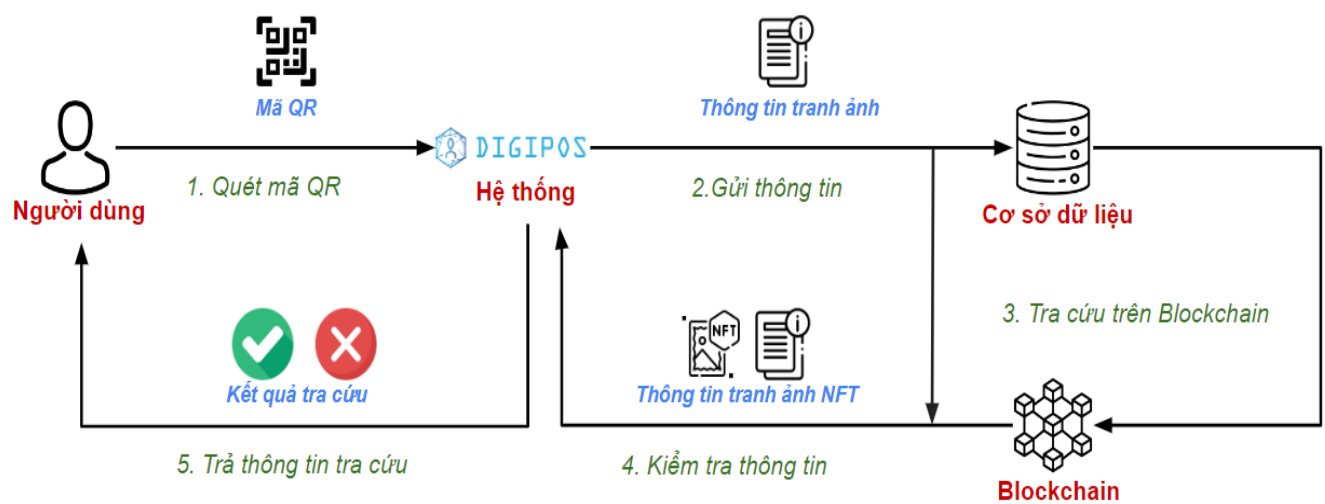
- Ở quy trình này, người dùng sẽ chọn tranh ảnh(.png, jpg, ...) gốc hoặc chứng chỉ quyền tác giả và thông tin của người dùng(địa chỉ Blockchain, ...) để gửi vào hệ thống DIGIPOS
- DIGIPOS sẽ băm tranh ảnh gốc và gửi bản mã hóa tranh ảnh gốc để tìm kiếm thông tin tương ứng, và tiến hành sử dụng thông tin tìm được tiếp tục tìm kiếm thông tin tương ứng được lưu trên Blockchain.
- Khi tìm được thông tin tranh ảnh NFT và bắt đầu xác thực quyền sở hữu tranh ảnh NFT được lưu trữ minh bạch ở Blockchain với thông tin người dùng gửi vào DIGIPOS.
- Quyền sở hữu NFT được lưu trữ minh bạch ở Blockchain sẽ quyết định người dùng có phải chủ sở hữu hoặc tác giả của tranh ảnh hay không.



Hình 4.3 Quy trình xác thực bằng tranh ảnh gốc hoặc chứng chỉ

4.4 Xác thực tranh ảnh thông qua mã QR

- Ở quy trình này, người dùng sẽ gửi mã QR vào hệ thống DIGIPOS, hệ thống sẽ dựng vào thông tin được lưu trên mã QR để tìm kiếm thông tin tranh ảnh được lưu ở cơ sở dữ liệu.
- Tiếp tục tìm kiếm tranh ảnh NFT được lưu trên Blockchain với dữ liệu tìm được.
- Với dữ liệu được lưu trữ minh bạch ở Blockchain, hệ thống sẽ dựa vào dữ liệu này để kiểm tra quyền sở hữu và quyền tác giả của tranh ảnh, sau đó gửi kết quả về cho người dùng.



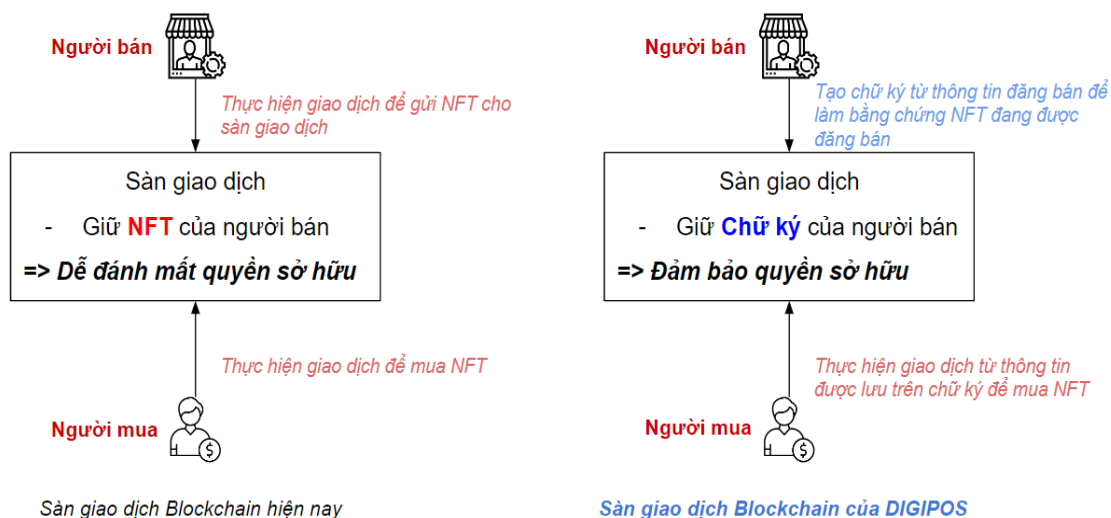
Hình 4.4 Xác thực tranh ảnh thông qua mã QR

4.5 Giải pháp về sàn giao dịch

Đỏ nhạt: mất phí; xanh nhạt: không mất phí

4.5.1 Giải pháp trao đổi mua bán

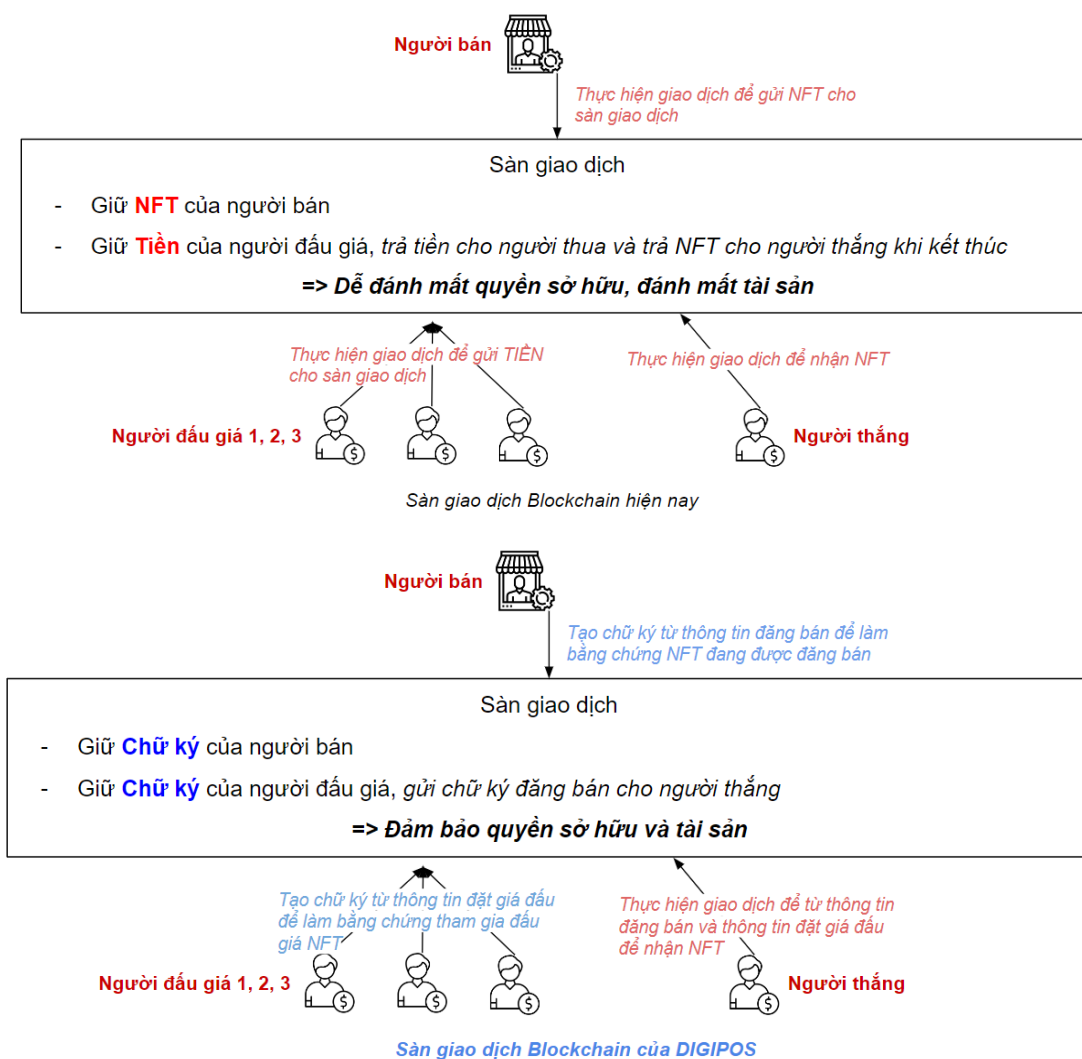
- Hiện nay, các sàn giao dịch tập trung đang tổ chức giao dịch với mô hình tập trung, các sàn giao dịch này giữ các tài sản NFT của các chủ sở hữu. Để phiên giao dịch diễn ra, chủ sở hữu phải bỏ chi phí kích hoạt hợp đồng thông minh để thực hiện thêm một giao dịch chuyển tài sản NFT cho sàn giao dịch giữ. Điều này không đảm bảo tính minh bạch của sàn giao dịch, cũng như tài sản có thể bị thao túng dẫn đến việc chủ sở hữu mất trắng tài sản và người mua được đảm bảo mua đúng tài sản toàn vẹn giá trị.
- Từ đó, DIGIPOS cung cấp giải pháp sử dụng chữ ký số, hệ thống sẽ sử dụng thuật toán sinh chữ ký số ECDSA để làm bằng chứng tài sản NFT được đăng bán nhưng không gây sai lệch thông tin đăng bán, sàn giao dịch của DIGIPOS áp dụng tính phi tập trung để thực hiện giao dịch giữa các người dùng với nhau, không thao túng tài sản của người dùng và chỉ giữ bằng chứng tài sản được đăng bán. Khi người mua thực hiện giao dịch để mua sản phẩm, người đó chỉ cần bỏ phí để kích hoạt hợp đồng thông minh và thông tin được truyền vào hợp đồng là thông tin lưu trên chữ ký số. Cuối cùng quá trình giao dịch diễn ra chỉ với một lần giao dịch duy nhất mà không ảnh hưởng đến quyền sở hữu hay giá trị tài sản.



Hình 4.5 Giải pháp trao đổi mua bán

4.5.2 Giải pháp đấu giá

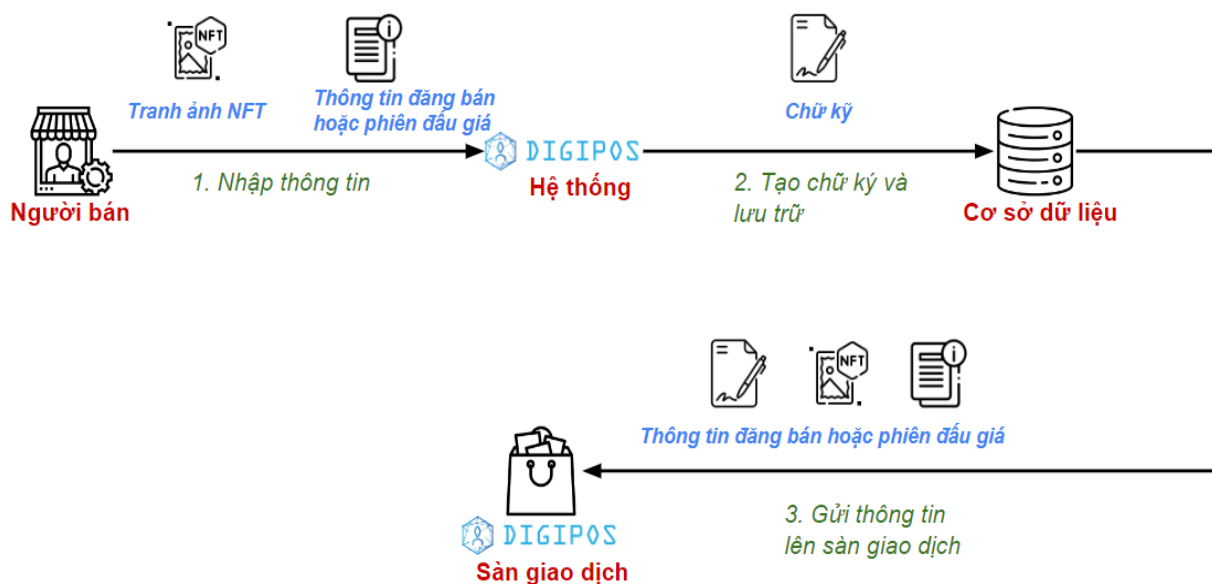
- Tương tự quá trình mua bán trao đổi tài sản NFT ở các sàn giao dịch tập trung, thì quá trình diễn ra phiên đấu giá ở các sàn này cũng diễn ra với rất nhiều giao dịch trung gian, tốn nhiều chi phí kích hoạt hợp đồng thông minh. Đặc biệt là người tham gia đấu giá phải gửi tiền vào sàn đấu giá, dẫn đến việc sàn này giữ cả tài sản và tiền các bên tham gia phiên đấu giá.
- Ngược lại, sàn giao dịch mà DIGIPOS cung cấp chỉ giữ chữ ký số của người tham gia đấu giá để làm bằng chứng, và phiên đấu giá kết thúc với một giao dịch diễn ra dành cho người thắng, và tài sản được chuyển đổi trực tiếp từ người bán sang người thắng.



Hình 4.6 Giải pháp đấu giá

4.6 Quy trình đăng bán hoặc tạo phiên đấu giá

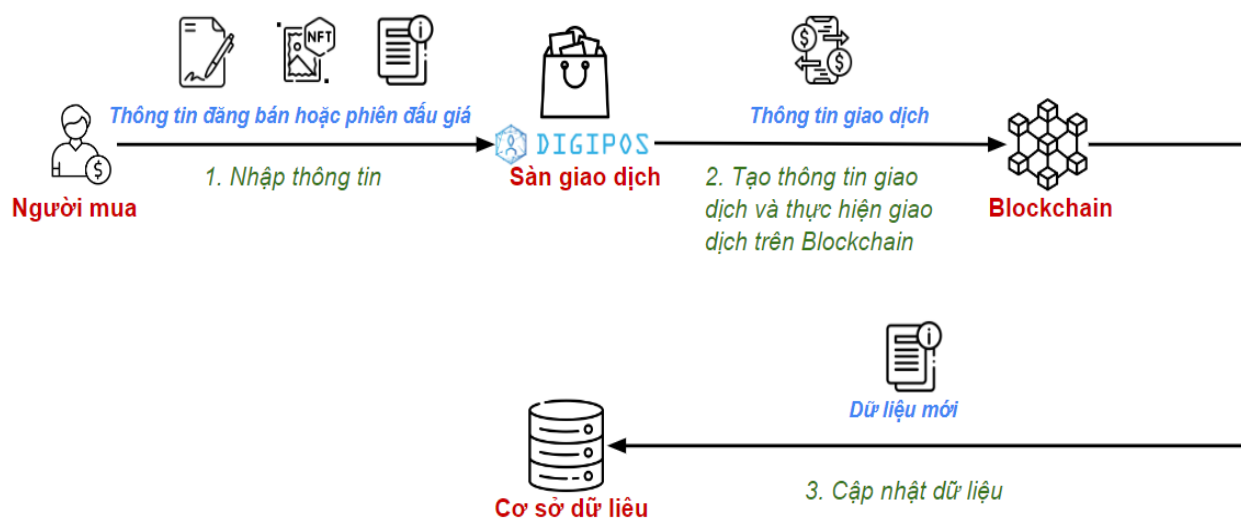
- Ở quy trình này, người bán sẽ gửi thông tin tranh ảnh NFT và thông tin đăng bán hoặc phiên đấu giá(giá, giá sàn, thời gian bán, ...) vào hệ thống DIGIPOS.
- Hệ thống sẽ sử dụng thuật toán sinh chữ ký ECDSA để tạo chữ ký làm bằng chứng tranh ảnh được đăng bán trên sàn giao dịch DIGIPOS.
- Thông tin đăng bán hoặc tạo phiên đấu giá sẽ được lưu trữ ở cơ sở dữ liệu và hiển thị trên sàn giao dịch.



Hình 4.7 Quy trình đăng bán hoặc tạo phiên đấu giá

4.7 Quy trình mua hoặc nhận NFT khi thắng phiên đấu giá

- Với bằng chứng tranh ảnh NFT được chủ sở hữu đăng bán hoặc tạo phiên đấu giá từ chữ ký số, người mua hoàn toàn có thể tin tưởng thông tin đăng bán là chính xác.
- Ngoài thuật toán sinh chữ ký số ECDSA, DIGIPOS còn xây dựng hợp đồng thông minh một cách chặt chẽ, khi thông tin từ chữ ký số không hợp lệ thì giao dịch không thể diễn ra.
- Khi thông tin hợp lệ, người mua chỉ cần bỏ chi phí để kích hoạt hợp đồng thông minh để thực hiện giao dịch chuyển đổi tranh ảnh NFT trực tiếp từ người bán sang người mua, thông tin về quyền sở hữu NFT sẽ được ghi vào Blockchain và lưu trữ minh bạch



Hình 4.8 Quy trình mua hoặc nhận NFT

4.8 Quy trình đặt giá thầu

- Tương tự quá trình đăng bán hoặc tạo phiên đấu giá tranh ảnh NFT, DIGIPOS sẽ tạo chữ ký số từ thông tin đấu giá của người tham gia đấu giá để làm bằng chứng có tham gia phiên đấu giá.

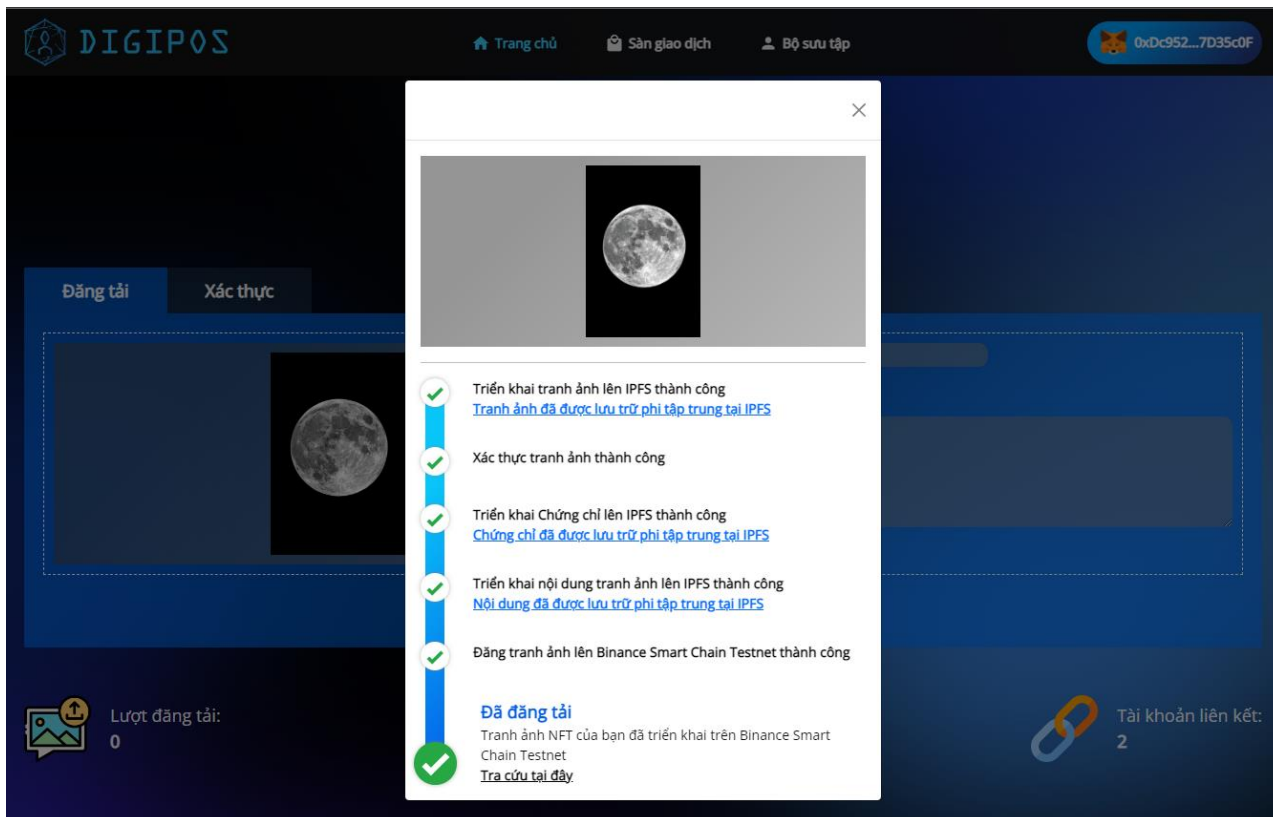


Hình 4.9 Quy trình đặt giá thầu

CHƯƠNG 5: ĐÁNH GIÁ GIẢI PHÁP

5.1 Ứng dụng

- Quá trình chuyển đổi tranh ảnh kỹ thuật số thành tranh ảnh NFT



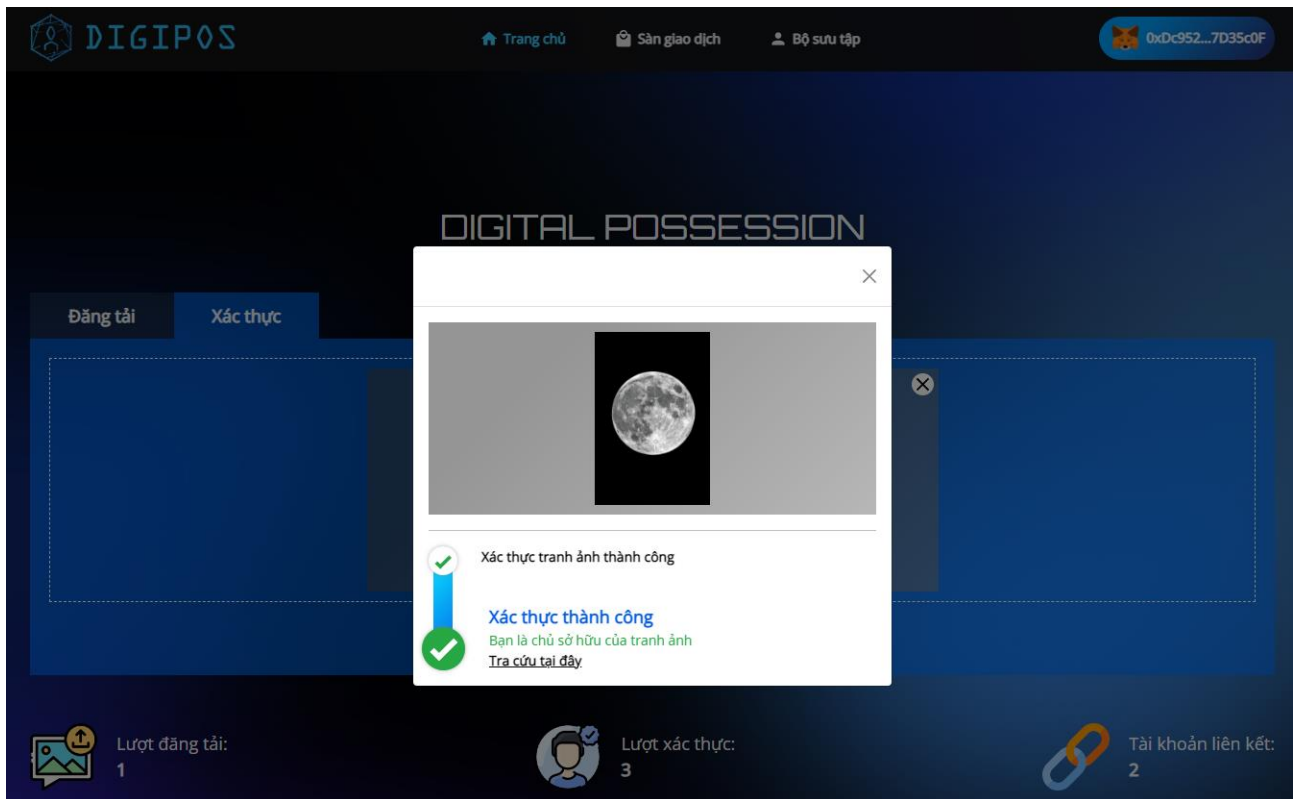
Hình 5.1 Quá trình chuyển đổi tranh ảnh kỹ thuật số thành NFT

- Cấp chứng chỉ quyền tác giả tranh ảnh NFT



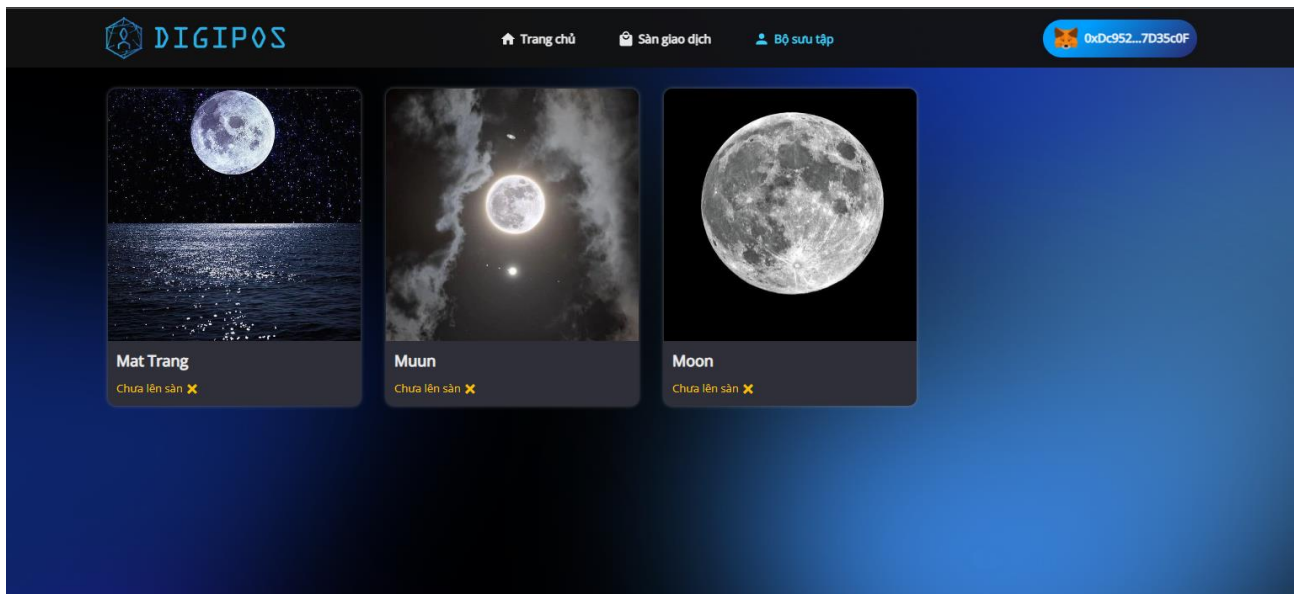
Hình 5.2 Chứng chỉ quyền tác giả

- Quá trình xác thực tranh ảnh NFT



Hình 5.3 Xác thực tranh ảnh NFT

- Bộ sưu tập tranh ảnh của người sở hữu



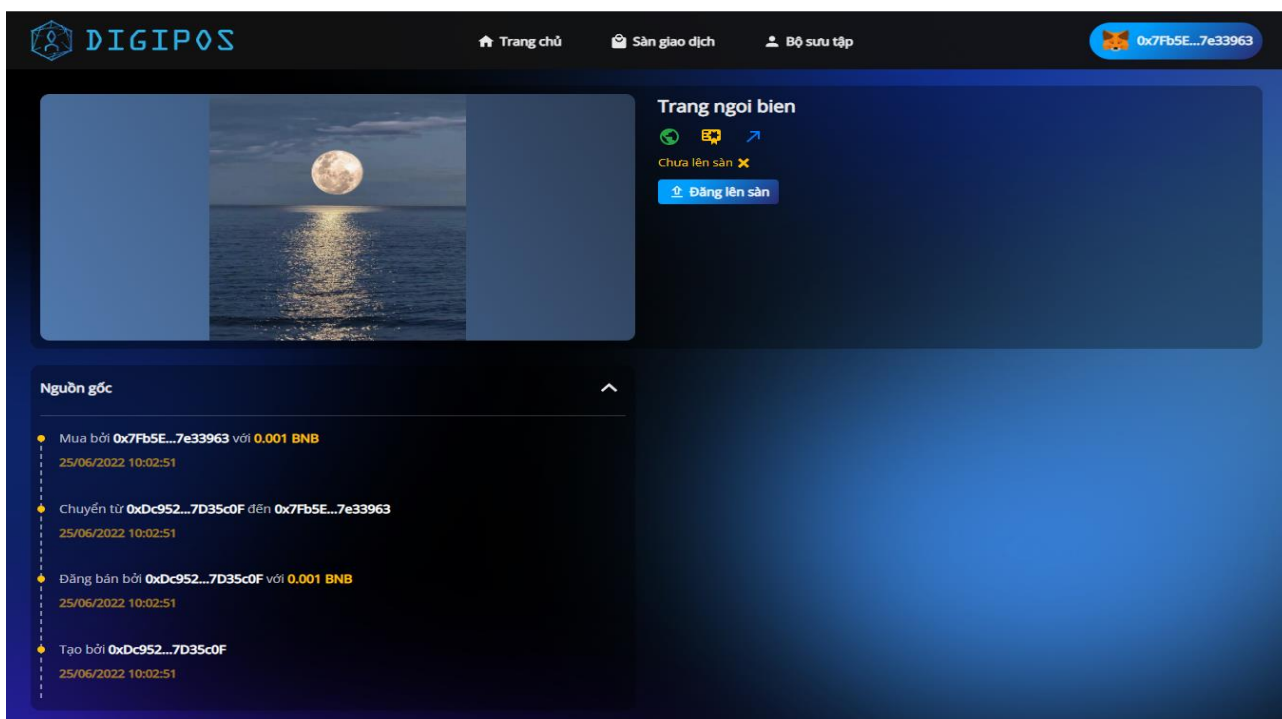
Hình 5.4 Bộ sưu tập tranh ảnh

- Thông tin chi tiết tranh ảnh NFT và thông tin đăng bán hoặc tạo phiên đấu giá

The screenshot shows the DIGIPOS NFT marketplace interface. At the top, there's a header with the DIGIPOS logo, navigation links (Trang chủ, Sản giao dịch, Bộ sưu tập), and a user profile icon with the address 0xDc952...7D35c0F. The main content area displays the 'Moon' NFT, which is a circular image of the moon. To the right of the image, there's a section titled 'Moon' with a status 'Chưa lên sàn' (Not on sale) and a 'Đăng lên sàn' (List on sale) button. Below this, there's a form for listing or bidding. The form has two columns: 'Thời gian diễn ra' (Duration) with a date range '25/06/2022 10:39 - 02/07/2022 10:39' and a checkbox 'Kích hoạt đấu giá' (Enable auction) which is checked; and 'Giá' (Price) with fields for 'Giá' (Price) and 'Giá sàn' (Floor price), both set to 'BNB'. There are 'Đăng lên sàn' (List on sale) buttons for both sections. At the bottom, there's a 'Nguồn gốc' (Origin) section showing the NFT was created by '0xDc952...7D35c0F' on '25/06/2022 10:02:51'.

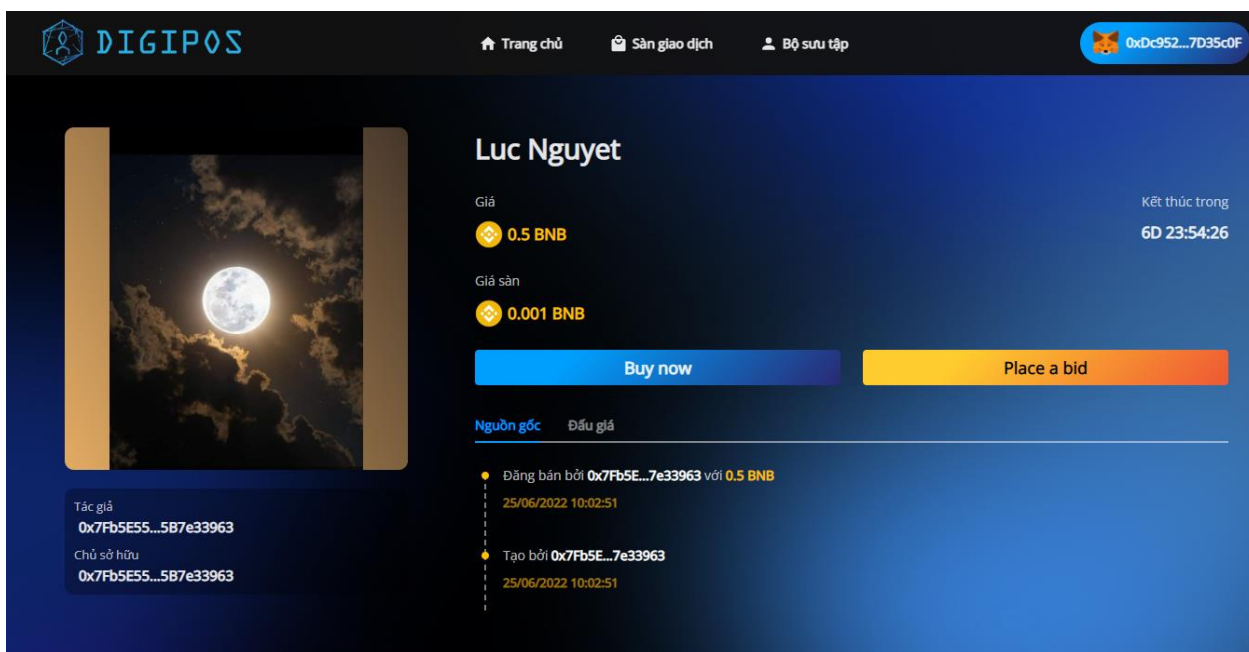
Hình 5.5 Thông tin chi tiết và thông tin đăng bán

- Thông tin nguồn gốc của tranh ảnh NFT



Hình 5.6 Thông tin nguồn gốc tranh ảnh NFT

- Thông tin đăng bán hoặc phiên đấu giá tranh ảnh NFT



Hình 5.7 Thông tin đăng bán hoặc tạo phiên đấu giá

5.2 Kiến trúc hệ thống

Lớp đối tượng

Mỗi đối tượng đều được định danh bằng địa chỉ Blockchain(Public key). Định danh được sử dụng cho các hoạt động trong hệ thống.

Lớp ứng dụng

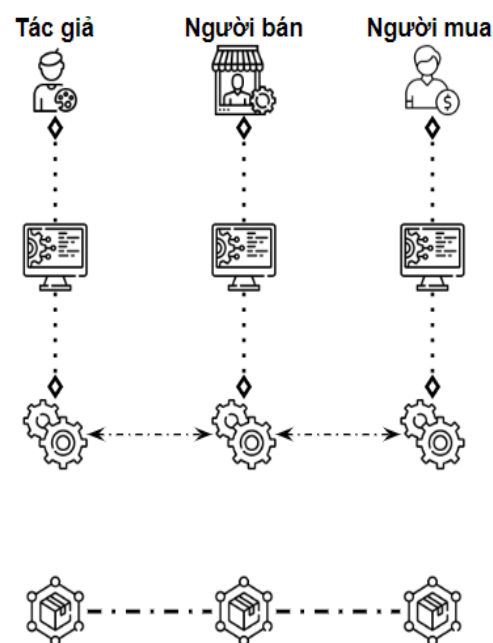
Ứng dụng cung cấp dịch vụ chuyển đổi và xác minh tranh ảnh NFT cũng như tạo ra thị trường tranh ảnh NFT. Hỗ trợ người dùng tra cứu dữ liệu tranh ảnh phi tập trung.

Lớp xử lý

Dữ liệu được thiết kế dựa trên tiêu chuẩn được sử dụng chung trên toàn cầu. Hệ thống Hợp đồng thông minh hỗ trợ chuyển đổi tranh ảnh kỹ thuật số thành tranh ảnh NFT.

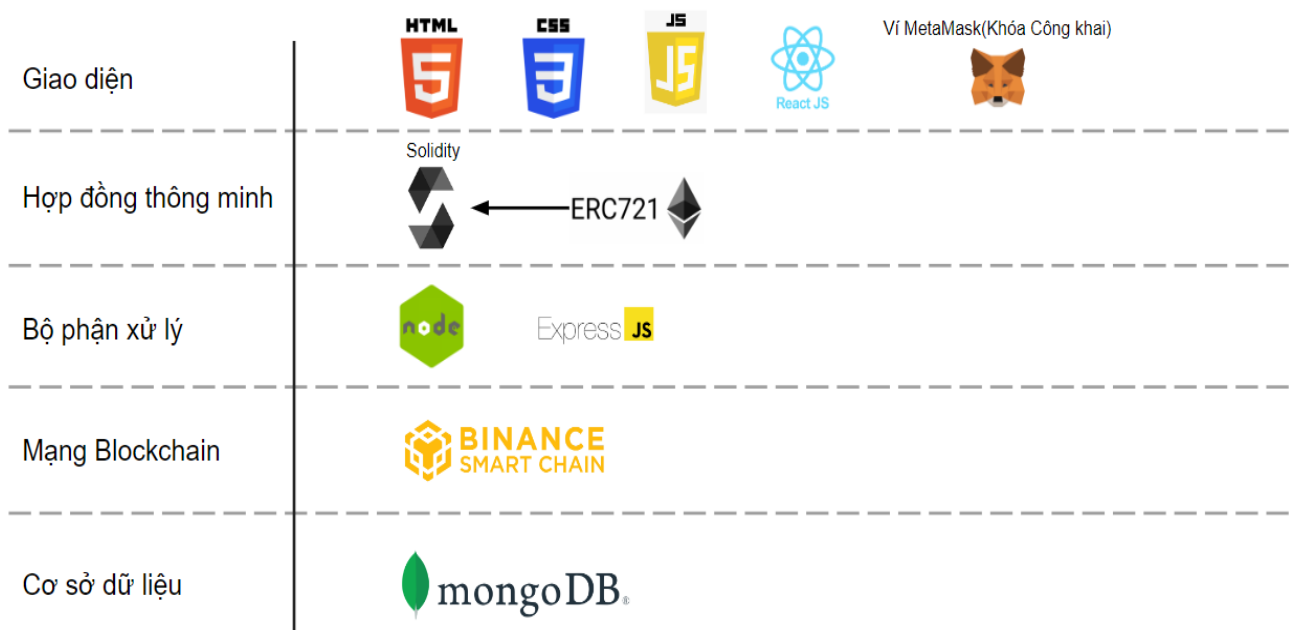
Lớp Blockchain

Dữ liệu được xác minh bằng chữ ký và các thuật toán mật mã học. Mạng Blockchain cho phép chia sẻ dữ liệu tranh ảnh và chống thay đổi dữ liệu.



Hình 5.8 Kiến trúc hệ thống

5.3 Kiến trúc công nghệ



Hình 5.9 Kiến trúc công nghệ

5.4 Ưu điểm và nhược điểm






















5.4.1 Ưu điểm

- Giải pháp mới với các tính năng đột phá, tin cậy tức thì.
- Có rất nhiều phương pháp để xác minh chứng chỉ.
- Giảm chi phí sử dụng (ít giao dịch hơn).
- Khả năng mở rộng (hợp đồng thông minh có thể nâng cấp).

5.4.1 Nhược điểm

- Phí biến đổi cho việc chuyển đổi và truy xuất NFT.
- Khó tiếp cận người dùng chưa có kiến thức về công nghệ Blockchain.

5.5 Khả năng triển khai giải pháp

	 originstamp	 BLOCKCERTS	 OpenSea	 BINANCE NFT	 DIGIPOS
Quyền tác giả					
Quyền sở hữu					
Trao đổi, mua bán					
Chi phí	Cao	Cao	Cao	Cao	Thấp
Pháp lý					

Hình 5.10 Khả năng triển khai giải pháp

TỔNG KẾT VÀ KIẾN NGHỊ

6.1 Tổng kết

- Hoàn thiện được ứng dụng mô tả giải pháp xác thực quyền tác giả và quyền sở hữu tranh ảnh kỹ thuật số
- Xây dựng thành công một sàn giao dịch tranh ảnh kỹ thuật số với mô hình phi tập trung
- Hỗ trợ quy trình xác minh quyền tác giả và cấp chứng chỉ một cách nhanh chóng, cũng như lưu trữ thông tin quyền tác giả một cách minh bạch
- Ứng dụng công nghệ Blockchain như một giải pháp công nghệ
- Hoàn thiện hợp đồng thông minh cung cấp điều khoản trong các quá trình xác minh, xác thực và giao dịch tranh ảnh
- Đặc tả về kiến trúc hệ thống và kiến trúc công nghệ
- Đánh giá ưu điểm và nhược điểm của giải pháp
- Xem xét và đánh giá khả năng triển khai giải pháp

6.2 Kiến nghị

- Phát triển thêm trên nhiều lĩnh vực ngoài hội họa và nhiếp ảnh
- Nâng cấp hợp đồng thông minh
- Hoàn thiện về mặt ứng dụng
- Giải quyết các vấn đề về pháp lý

TÀI LIỆU THAM KHẢO

- [1] TheFriendlyRobot, “Tranh”, 2021
- [2] “Sàn giao dịch tập trung và phi tập trung có điểm gì khác biệt?”, 2020
- [3] Jasmine, “Blockchain là gì và nó được ứng dụng thế nào trong cuộc sống?”, 2021
- [4] Quang Ori, “Cùng tìm hiểu sơ cái blockchain là gì?”, 2020
- [5] Nguyễn Hưng, “Peer to peer là gì?”, 2021
- [6] Thạc sĩ Đinh Thùy Dung, “Cơ chế đồng thuận là gì? Đặc điểm và nội dung về Cơ chế đồng thuận”, 2022
- [7] TH, “Hợp đồng thông minh là gì? Những điều bạn cần biết về hợp đồng thông minh”, 2021
- [8] Chi Phạm, “NFT là gì? Tìm hiểu cách kiếm tiền tỷ nhờ đầu tư NFT”, 2021
- [9] Nguyễn Trí Minh Hoàng, “HTML”, 2022
- [10] TopDev, “CSS là gì?”, 2020
- [11] Nguyễn Hưng, “JavaScript là gì? Kiến thức chi tiết về JavaScript cơ bản”, 2021
- [12] Tran Cong Trinh, “Bắt đầu với ReactJs”, 2017
- [13] Nguyễn Hưng, “NodeJS là gì? Tổng quan kiến thức về Node.JS”, 2022
- [14] Vinh Vo, “IPFS là gì? Tiềm năng của IPFS trong Blockchain”, 2022
- [15] ITNavi, “Solidity là gì? Tổng quan về ngôn ngữ lập trình Solidity”, 2022
- [16] Hoàng Chương, “Metamask là gì? Có an toàn không? Cách tạo ví Metamask”, 2020
- [17] Do Trung Kien, “ECDSA - hệ mật dựa trên đường cong Elliptic và ứng dụng trong Blockchain”, 2020