

NFT-BASED AUTHENTIC PRODUCT VERIFICATION AND TRADING PLATFORM



Mr. Natchapol Thongruang

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Computer Science
Department of Computer Engineering
FACULTY OF ENGINEERING
Chulalongkorn University
Academic Year 2022
Copyright of Chulalongkorn University

แพลตฟอร์มการตรวจสอบผลิตภัณฑ์จริงและการทำการค้าโดยใช้เอ็นเอฟที



นายณัฏพล ทองร่วง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565
ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

ณัชพล ทองรุ่ง : แพลตฟอร์มการตรวจสอบผลิตภัณฑ์จริงและการทำการค้าโดยใช้เอ็นเอฟที. (NFT-BASED AUTHENTIC PRODUCT VERIFICATION AND TRADING PLATFORM) อ.ที่ปรึกษาหลัก : ศ. ดร.ประภาส จงสถิตย์วัฒนา

สินค้าลอกเลียนนับเป็นปัญหาที่มีมาอย่างช้านาน ถึงแม้จะมีการออกแบบวิธีแก้ปัญหาต่าง ๆ มากมายก็ยังไม่สามารถป้องกันปัญหาและความเสียหายที่อาจเกิดขึ้นได้ โดยเฉพาะกับประเภทสินค้าที่มีมูลค่าสูงอย่างสินค้าของแบรนด์ที่มีชื่อเสียงนั้น หากผู้ซื้อไม่ทราบว่าสินค้าที่ซื้อเป็นของลอกเลียนแบบหรือไม่และต้องซื้อขายในราคาที่สูง อาจทำให้เกิดความเสียหายต่อผู้ซื้อได้อย่างใหญ่หลวง

จากความพยายามนับไม่ถ้วนที่จะหาวิธีแก้ไขปัญหาสินค้าลอกเลียนแบบนั้น หนึ่งในวิธีการที่ได้รับความนิยมในยุคปัจจุบันได้แก่ การประยุกต์ใช้เทคโนโลยีบล็อกเชนเข้ามาช่วยพัฒนาระบบการตรวจสอบสินค้าที่มีประสิทธิภาพมากยิ่งขึ้น โดยวิธีการที่พบเห็นได้มากในเรื่องการป้องกันสินค้าลอกเลียนแบบนั้น คือการสร้างเหรียญเอ็นเอฟทีให้กับสินค้าแต่ละชิ้น เพื่อที่จะสามารถติดตามและตรวจสอบการซื้อขายถ่ายโอนสินค้าได้อย่างเปิดเผย เพียงแต่ระบบดังกล่าวที่ถูกรู้นำเสนอนั้นไม่สามารถป้องกันความเสียหายที่อาจเกิดขึ้นได้อย่างครอบคลุมทั่วถึง ดังนั้นงานวิจัยนี้จึงนำเสนอระบบที่จะไม่เพียงสามารถออกเหรียญเอ็นเอฟทีให้สินค้าต่างๆได้ แต่ยังสามารถครอบคลุมไปถึงการที่สามารถซื้อขายสินค้าได้อย่างมั่นใจและผู้ซื้อขายเข้ากับภาระการรับประกันสินค้า เพื่อสร้างความเสี่ยงให้กับมิจฉฉิพมากยิ่งขึ้น โดยระบบดังกล่าวนี้ได้ถูกนำไปทดสอบกับกรณีศึกษาหลัก 2 กรณี ซึ่งทำให้ได้ผลสรุปว่าตัวระบบสามารถรองรับการซื้อขายสินค้าได้ทั้งจากผู้ผลิตสู่ผู้บริโภค และจากผู้บริโภคสู่ผู้บริโภคก็ได้เช่นกัน อีกทั้งยังได้มีการวิเคราะห์ถึงค่าใช้จ่ายที่อาจจะเพิ่มมากขึ้นจากการใช้งานเทคโนโลยีบล็อกเชนในการซื้อขายสินค้าและการโอนถ่ายเหรียญเอ็นเอฟทีรวมทั้งนำเสนอสกุลเงินดิจิทัลอื่นที่อาจจะช่วยลดต้นทุนดังกล่าวได้อีกด้วย

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์

ลายมือชื่อนิสิต

ปีการศึกษา 2565

ลายมือชื่อ อ.ที่ปรึกษาหลัก

6270074321 : MAJOR COMPUTER SCIENCE

KEYWORD: non-fungible token, smart contract, blockchain, authentication,
platform

Natchapol Thongruang : NFT-BASED AUTHENTIC PRODUCT VERIFICATION
AND TRADING PLATFORM . Advisor: Prof. PRABHAS CHONGSTITVATANA,
Ph.D.

Counterfeit product has been a major problem to the economy for a while. The effect seems to be larger when it comes to the luxury product segment. When the consumers were unsure if the product that they are buying is genuine or not and its cost is very high, then the severity will become even greater.

Among the countless number of attempts to fix this solution, utilizing blockchain technology is one of the most popular approaches for present days. In anti-counterfeit domain, associating an NFT token to a physical product is the most common approach. It allows us to unlock the ability to track and trace the trades and the transfers of the product to the public. However, current systems could not fully prevent the problem from happening. To address this problem further, this research proposes a system that is not only able to mint an NFT token for a product, but also fully support the product trade process. This system also adds a warranty agreement burden to the seller, so that it will create risk factor for criminals. The proposed system was experimented with 2 main use cases which leads to the conclusion that, this system is capable of supporting both business-to-customer and customer-to-customer trades. Lastly, this research conducted a cost analysis, to understand the additional cost that the system caused and discussed some alternative blockchain networks that could minimize the cost.

Field of Study: Computer Science

Student's Signature

Academic Year: 2022

Advisor's Signature

ACKNOWLEDGEMENTS

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยความช่วยเหลืออย่างดียิ่งจากบุคคลหลายท่าน ขอขอบพระคุณบุคคลดังต่อไปนี้เป็นอย่างสูง

ขอกราบขอบพระคุณศาสตราจารย์ ดร.ประภาส จงสถิตย์วัฒนา อาจารย์ที่ปรึกษาที่เสียสละเวลา ให้คำแนะนำปรึกษา ชี้แนะแนวทางการทำวิจัยด้วยความเอาใจใส่อย่างยิ่ง ตลอดจนคอยตรวจทานปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ ที่เกิดขึ้น เพื่อให้วิทยานิพนธ์ฉบับนี้มีความสมบูรณ์ยิ่งขึ้น

ขอกราบขอบพระคุณรองศาสตราจารย์ ดร. ดวงดาว วิชาตากุล และรองศาสตราจารย์ ดร. วร เศรษฐ สุวรรณิก ที่กรุณาเสียสละเวลามาเป็นกรรมการสอบวิทยานิพนธ์และให้คำแนะนำในจุดที่ต้องแก้ไขเพื่อให้วิทยานิพนธ์ฉบับนี้มีความสมบูรณ์มากยิ่งขึ้น อีกทั้งยังขอกราบขอบพระคุณรองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ ที่กรุณาสละเวลามาร่วมเป็นกรรมการสอบโครงร่างวิทยานิพนธ์เป็นการพิเศษอีกด้วย

ขอขอบพระคุณคณาจารย์ทุกท่านในภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ได้มอบความรู้ทางด้านวิชาการที่ล้วนเป็นประโยชน์อย่างยิ่ง อีกทั้งบุคลากรทุกท่านในภาควิชาฯ ที่ช่วยประสานงานให้ข้อมูลและคำแนะนำที่ดีตลอดมา

ขอขอบคุณเพื่อน ๆ พี่ ๆ น้อง ๆ ในภาควิชาฯ และเพื่อนร่วมงานจากบริษัทต่าง ๆ ที่คอยให้คำแนะนำ และเป็นกำลังใจที่ดีเสมอมา

ขอขอบพระคุณครอบครัว ทั้งบิดา มารดา น้องชาย รวมไปถึงเครือญาติท่านอื่น ๆ ที่ให้การสนับสนุน ให้กำลังใจแก่ผู้วิจัยเสมอ และท้ายที่สุดนี้ อยากจะขอขอบคุณบุคคลที่อยู่เคียงข้าง ผู้ซึ่งเป็นแรงผลักดันแก่ผู้วิจัย จนมีกำลังใจและสามารถทำให้งานวิจัยฉบับนี้สำเร็จลุล่วงไปได้

Natchapol Thongruang

TABLE OF CONTENTS

	Page
.....	iii
ABSTRACT (THAI).....	iii
.....	iv
ABSTRACT (ENGLISH).....	iv
ACKNOWLEDGEMENTS.....	v
TABLE OF CONTENTS.....	vi
CHAPTER 1 INTRODUCTION.....	1
1.1 Motivation.....	1
1.2 Objective.....	2
1.3 Scope of work.....	3
1.4 Expected result.....	3
1.5 Research plan.....	3
CHAPTER 2 BACKGROUND KNOWLEDGE.....	4
2.1 Cryptocurrency.....	4
2.1.1 Blockchain.....	4
2.1.2 Smart Contract.....	6
2.2 Ethereum Improvement Proposals (EIP).....	8
2.2.1 ERC-20 Token Standard.....	9
2.2.2 ERC-721 Non-Fungible Token.....	9
2.2.3 ERC-1155 Multi Token Standard.....	9
2.3 InterPlanetary File System (IPFS).....	9

CHAPTER 3 LITERATURE REVIEW	11
3.1 Product Anti-Counterfeits.....	11
3.2 Non-Fungible Token Studies.....	12
3.3 Blockchain System for Anti-Counterfeiting	13
3.4 Other Blockchain Applications	13
CHAPTER 4 PROPOSED METHOD	15
4.1 Overall Architecture Design	15
4.2 Existing Work Analysis	18
4.3 Use Cases Design	19
4.3.1 Product Registration.....	19
4.3.2 Succeeded Product Trade	20
4.3.3 Failed Product Trade	21
4.3.4 Product Verification.....	22
4.3.5 Product Warranty Inspection.....	23
CHAPTER 5 SYSTEM DESIGN AND IMPLEMENTATION	24
5.1 Proposed System Design.....	24
5.1.1 Software Design	24
5.1.2 Smart Contract Design.....	25
5.1.2.1 NFT Metadata Schema	25
5.1.2.2 Product NFT.....	26
5.1.2.3 Warranty NFT.....	26
5.1.2.4 Mint Function	27
5.1.2.5 Transfer With Warranty Function.....	28
5.2 System Development	28

5.2.1	Development Environment.....	28
5.2.1.1	Hardware Specification	29
5.2.1.2	Software Specification	29
5.2.2	Web Application Development	29
5.2.3	Web Backend Development	30
5.2.4	Smart Contract Development.....	30
5.3	System User Interfaces	31
5.3.1	Marketplace Page	32
5.3.2	Product Pages.....	33
5.3.2.1	Product Registration Page	33
5.3.2.2	Product Detail Page.....	33
5.3.3	Product Trade Pages	34
5.3.3.1	Product Trade Offer Page	34
5.3.3.2	Seller Warranty Agreement Page	35
5.3.3.3	Product Trade Payment Page	36
5.3.3.4	Product Trade Completion Page.....	37
CHAPTER 6 SYSTEM TESTING AND RESULTS.....		38
6.1	System Testing on Use Cases.....	38
6.1.1	Test Case 1: Buying from official store.....	38
6.1.2	Test Case 2: Buying secondhand product.....	45
6.2	System Cost Analysis.....	46
6.2.1	Token Minting Cost.....	46
6.2.2	Total AutheNFT Trade Cost	47
6.2.3	Other Network Cost Comparison	47

CHAPTER 7 SUMMARY AND FUTURE WORK 49

REFERENCES 50

VITA..... 53



CHAPTER 1

INTRODUCTION

1.1 Motivation

Economy is the core foundation of the modern capitalist world. Countless amounts of people are implicitly involved in it every day, by purchasing something. There are various products to be chosen, from us customers who make purchases, whether to meet our basic needs or our personal desire. But products come in all sizes and shapes, and sometimes you might have bought something you did not expect it to be. Especially in the case of luxury product where the price is higher than the market average.

The problem of product authenticity in luxury product market is still an existing issue no matter how many years have passed. Building up a luxury brand and gain popularity is hard, but it is so much easier to just replicate a branded product and try to compete with them instead. Counterfeit products are more willing to sacrifice some degree of quality over lower price to be able to make profit from stealing the market share of the original product. The given scenario could harm the original product which is unfair to them having to spend time and resources to be able to come up with a successful formula. It is also bad for consumers who might accidentally purchase products with quality below standards, or in the worst case, customers being fraud from counterfeit products and ended up having to pay more for less value.

To prove product authenticity, there are various methods attempt to create a unique characteristic of the product or issuing certificate. Even with those attempts, people could still manage to make fraud possible. While the need to verify product authenticity remains, the recent technology introduces a unique digital identifier of ownership under the foundation of Blockchain.

Blockchain technology is famous for its decentralization and its ability to prove ownership. Blockchain serves as the core technology of the modern digital currency, Cryptocurrencies. Ethereum is one of the most famous cryptocurrencies with a powerful concept of Smart Contract. Instead of doing basic arithmetic for

currency transactions like other cryptocurrencies, Ethereum introduces Smart Contract, a programmable piece of code which performs automated operation when a certain condition is met. Smart Contract has open doors for the cryptocurrency and blockchain world to new possibilities. So much that the Ethereum community had to create a standardized specification called Ethereum Request for Comment (ERC).

Non-Fungible Token (NFT) is one of the ERC specifications which promises that each unit (coin/token) of the currencies that implement NFT's ERC will be unique and non-fungible. This characteristic of NFT is very interesting and creates a tremendous amount of use cases. In this research, we further discussed about previous studies in applying the NFT technology to tackle an anti-counterfeiting problem. Most of the studies focusing on generating a unique identifier of any kind and store them information into the NFT token. This approach uses the advantage of blockchain decentralization and proof of ownership allowing users to bind the physical object to a digital token. However, even if the seller has an ownership token, there is a scenario where the product could still be replicated and sold to the buyer. The buyer will still receive the NFT token but the physical product shipped to them could be the replicated one.

This research aims to propose a way to address the anti-counterfeits problem in luxury product trade using NFT and Blockchain technology. We introduce an NFT collection of our own and an ERC-721 Smart Contracts to provide NFT services as a unique digital certificate and being traceable to the origin. We extended the novel design of previous anti-counterfeits system with a e-signature signing process asking the seller of product to be consent to the post-sale warranty agreement for the legal support purpose. We also designed a proof-of-concept trading platform which integrated with the payment system to aid in the authentic product trade.

1.2 Objective

There are three main objectives of this research:

1. Propose a solution to provides the prove of ownership and assists in trading and verification of luxury product for anti-counterfeiting using Blockchain technology.

2. To demonstrate the use of the proposed solution in getting the seller's consent to be responsible for the goods in trade.
3. Experiment the use of the proposed method to reflect the result of this study.

1.3 Scope of work

1. Experiment within local or testnet of blockchain network
2. Product data will be simulated from mocking company or brand
3. Digital certificate of the product is stored on IPFS
4. No actual payment functionality implemented
5. Support only NFT minted within the proposed platform

1.4 Expected result

1. Introduce new Smart Contracts for NFT application building on top of the existing ERC standards.
2. Propose an effective and seamless solution to enhance luxury product trading with NFT as proof of ownership to the product.
3. Propose a process where sellers consent in the product warranty after the trade to achieve transparency and trust in product trade.

1.5 Research plan

1. Explore topics and study background knowledge
2. Study the related works and literature review
3. Design and implement the prototype of the proposed solution
4. Summarize preliminary result
5. Thesis topic proposal examination
6. Further development as in the proposal
7. Academic paper publication
8. Conclude results and write up the thesis
9. Thesis examination

CHAPTER 2

BACKGROUND KNOWLEDGE

The background knowledge related to this research is separated into three main topics. Depression detection in deep learning, Deep Neural Network and Modern deep learning techniques.

2.1 Cryptocurrency

Cryptocurrency achieves an important milestone to the real-world application of decentralization and marks the beginning of Cryptocurrency era. The world's first cryptocurrency is Bitcoin introduced by the anonymous developer named Satoshi Nakamoto who publishes the original whitepaper [1]. The Bitcoin cryptocurrency was implemented based on the concept of Blockchain and attained decentralization through its consensus mechanism called Proof-of-Work. Since then, variations of cryptocurrency have emerged with various techniques and implementations. One currency that stood out with exceptional functionality is Ethereum currency. Ethereum was developed based on a similar foundation of Bitcoin, blockchain and consensus mechanism. However, this currency also introduces a new concept called Smart Contract which allows its transactions to be programmatically handled based on the smart contract implementation. In this section we will discuss blockchain technology and the anatomy of smart contract technology.

2.1.1 Blockchain

At the bottom most, as a foundation of cryptocurrencies, the blockchain technology is the heart of it. In cryptocurrency, the transaction of transferring assets will be recorded on a ledger or record of transactions. Blockchain system handles this ledger by encrypting the information into a piece of data, called a "block". As new transactions are committed to the network, a new version of the ledger will be encrypted to become a new block. This new block will then be linked to the previous block forming a "chain" of blocks; hence the name blockchain. In order to come up with a new block, the whole blockchain will be encrypted using a

cryptography algorithm which ensures the integrity of information, since the previous block within the chain must remain the same in order to produce the latest block.

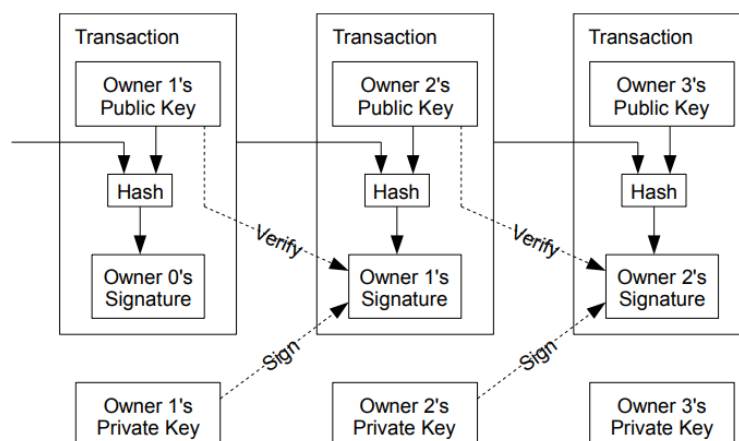


Figure 1: Bitcoin's illustration of digital asset as a chain of transactions.

As presented on the Bitcoin whitepaper, an electronic coin was introduced as a chain of digital signature. Figure 1 shows that a coin transfer is a hashing from the new owner publickey and the previous transaction which then form a hash string as the evidence of ownership. The hash string will also be signed with the previous owner privatekey to create a verifiable signature for ownership verification. It is also stated in the whitepaper that, the main problem of the idea is that the new owner can not verify that the previous owner did not double-spend the coin. In order to solve this, the proof-of-work and a combination of timestamp server was introduced.

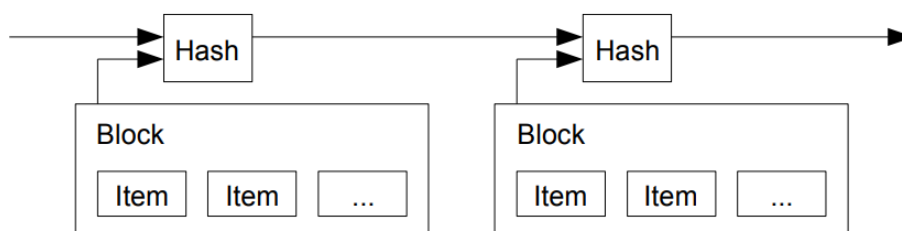


Figure 2: Timestamp server

In proof-of-work consensus mechanism, the target is to find a specific value that when hashed, such as by SHA-256 algorithm, the hash string begins with a desired amount of zero bits. The timestamp server from Figure 2 shows how the timestamp and a block together will be hashed to record the time the block existed. The following block linked from the previous one uses the additional timestamp from the previous timestamp along with itself to form a chain of hash. In combination with the timestamp server, the proof-of-work of Bitcoin was implemented by hashing a block containing a mutable number called Nonce. The miner's assignment is to change this nonce to any number until the whole block can be hashed and that the hash contains a desired amount of leading zero bits. Figure 3 illustrates how the block with nonce are linked with its following block(s). Doing this would provide integrity to the transactions because if any of the block was manipulated, the rest of the blocks after it must be re-calculated to make the whole chain compatible with the proof-of-work verification.

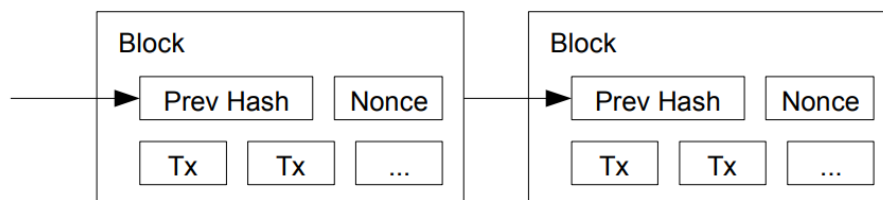


Figure 3: Bitcoin's chain of blocks

2.1.2 Smart Contract

In traditional cryptocurrency, all transactions are just a simple transfer of cryptocurrency from one wallet to another. But in 2015, since the Ethereum introduction, the term Smart Contract has been introduced. Smart contract is a computation program which deploys to the network and will be executed on the transaction of the network. It unlocks the capability of just transferring assets between wallets, into an asset calculation logic based on programmable condition. Any form of calculations within programmed conditions are possible with smart

contracts and makes Ethereum the first general purpose cryptocurrency in the blockchain world.

Bitcoin mechanism was stated in the Ethereum whitepaper [2] as capable of scripting in a weaker way of what was introduced as Smart Contract. By viewing Bitcoin mechanism as a State Transition System, we can see that transferring bitcoins through transaction is just a change of its ledger state from initial state to a new state as shown in Figure 4. From that point, Ethereum generalized Bitcoin's concept to an abstract model for broader uses. Starting with state object of Bitcoin, it contains the information about all the coins in the system and which owner address they belong to. In Ethereum state, it contains an account instead of owner address. There are two types of account, which are externally owned account and contract account. Any Ethereum account consists of four fields:

- Nonce – The same nonce as in Bitcoin to support the proof-of-work mechanism.
- Ether Balance – The account's Ether balance.
- Contract Code – An optional field for contract account to store scripting code which made Smart Contract possible.
- Storage – Empty by default and serves as an internal data storage for contract account.

Bitcoin As A State Transition System



Figure 4: Ethereum view of Bitcoin as State Transition System

Given the different types of account, they serve a different purpose and also behave differently. An externally owned account operates by sending message to another account using keys to create and sign a transaction. On the other hand, a contract account can receive a message from another account and its contract code will be activated to read or write from internal storage and send other messages or create another contract account. Comparing to the concept of transaction in Bitcoin, the concept of message is similar yet way more powerful by offering not only transactional operation but can also contain many types of data including metadata and functions. In contrast to the Figure 4 of Bitcoin, an Ethereum view of State Transition System is illustrated in Figure 5 as shown below.

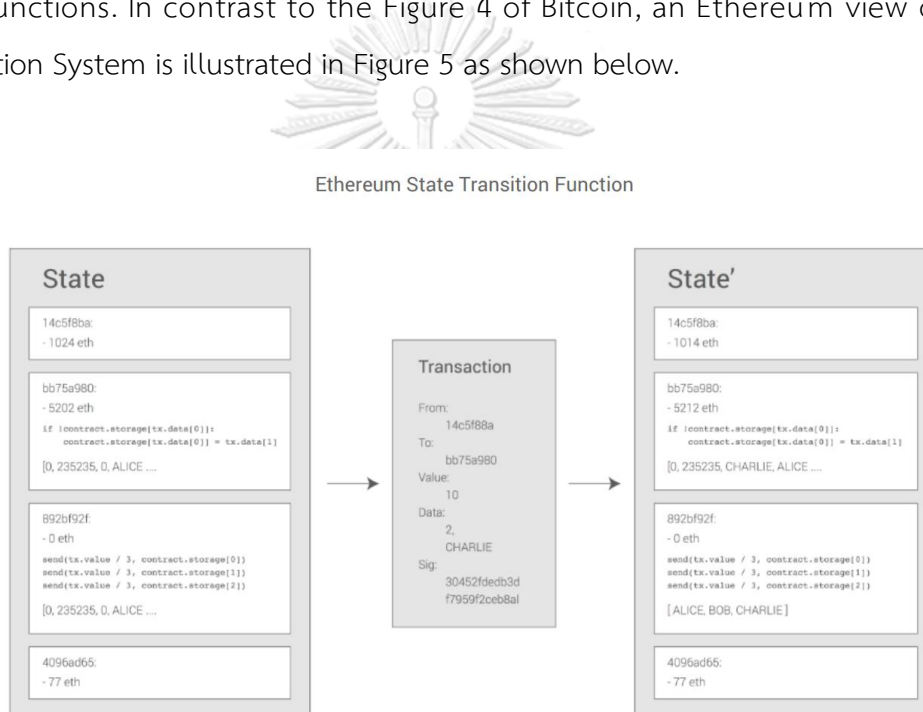


Figure 5: Ethereum State Transition Function

2.2 Ethereum Improvement Proposals (EIP)

As stated in the Ethereum's official EIP webpage, "An EIP is a design document providing information to the Ethereum community, or describing a new feature for Ethereum or its processes or environment" [3]. In this section, we will discuss 3 EIPs related to the NFT implementation.

2.2.1 ERC-20 Token Standard

Since Ethereum's smart contract is just a programmable contract, it could be implemented in any ways imaginable. This EIP-20 standard [4], under ERC category, was introduced to set guidelines on the execution of smart contracts and made their transaction support the concept of token. A (fungible) token is an asset which is possible to create another identical token with exactly the same value. It is basically the core idea of traditional cryptocurrency like Bitcoin, or currency concept in our economic world.

2.2.2 ERC-721 Non-Fungible Token

This standard introduced a completely different idea from EIP-20 but their interfaces are quite similar. EIP-721 [5] was introduced to make a token non-fungible which means each token is unique and don't share the same value.

2.2.3 ERC-1155 Multi Token Standard

With the world having 2 types of tokens to manage, there is a need to have one contract able to manage both types of tokens. This concept was introduced in EIP-1155 [6] as the standard for multi token or semi-fungible token.

2.3 InterPlanetary File System (IPFS)

The InterPlanetary File System (IPFS) was introduced in 2014 by Juan Benet [7]. This protocol and peer-to-peer network stores and shares hypermedia and files in a distributed file system. It has become popular within the blockchain developer community due to its distributed nature that aligns with the decentralization nature of blockchain.

IPFS serves content based on a content addressing method which is not centralized like location addressing such as the one from traditional web technology. In content addressing, any form of content uploaded to the network will be hashed. This hashed content is called Content Identifier (CID) and will be the access point to retrieve this content from the Merkle DAG across the IPFS network. Figure 6 shows

the example of content addressing object path in IPFS. The protocol for block exchange is BitSwap Protocol, a successor to the famous BitTorrent Protocol.

```
# format
/ipfs/<hash-of-object>/<name-path-to-object>

# example
/ipfs/XLYkgq61DYaQ8NhkcqyU7rLcnSa7dSHQ16x/foo.txt
```

Figure 6: IPFS content addressing paths

There are many implementations based on the IPFS protocol, but the one that is worth mentioning is Filecoin [8] which could be considered as the official File Storage Decentralized Application implementation from the IPFS creators.



CHAPTER 3

LITERATURE REVIEW

3.1 Product Anti-Counterfeits

Counterfeit problem is a simple yet widely spread across the globe and damaging the economy worldwide. The consumer usually prefers the product with cheaper price given the product has an acceptable quality. Using this insight, scammer or even the factory with the knowledge of producing the same type of product will try to produce a counterfeit product trying to achieve a lower price than the market to gain sales.

From the given pain point, some studies tried to address this problem even before the age of cryptocurrency. In 2005, the work from P. Lei, F. Claret-Tournier, C. Chatwin and R. Young [9] introduce a solution to prevent counterfeits from the use of track and trace system in mobile phone. The work stated that at the time of publication there are two popular technologies for anti-counterfeiting which are Authentication technologies and Track-and-trace technologies. Their work takes the track-and-trace approach by associating the physical product with a QR Code holding secret data and can be verify by a mobile phone camera. This publication has been publicly accepted and implemented for a while. But with the advancement in today's technology, replicating the QR Code and intercepting mobile phone data packet can be done easily.

The studies of anti-counterfeiting evolve as time passes. In 2007, a study from M. Lehtonen, N. Oertel and H. Vogt [10] discussed the most recent approach to anti-counterfeiting problem up until before the blockchain technology was introduced in 2008. On top of the two approaches of Authentication and Track-and-trace, another approach of cryptography was also included. The authentication approach relies on the distinctive properties or features of the physical product and building a verification system around them. The track-and-trace approach relies on the location and the chain of ownership of a certain product using technologies like RFID tag or one- or two-dimensional barcode. Lastly, the cryptographic approach applies

cryptography information to the object such as within the RFID tag. In combination with the custom interface, the cryptographic key can be use to embedded security metadata to the object.

3.2 Non-Fungible Token Studies

NFT has recently become one of the hottest topics in the blockchain field. However, even though it was not long ago since the very first NFT token was minted to the network, its use cases have evolved into various areas such as Art, Collectible, Gaming, Metaverse, etc. In 2022, A. Park, J. Kietzmann, L. Pitt and A. Dabirian conducted a study on the topic of “The Evolution of Nonfungible Tokens: Complexity and Novelty of NFT Use-Cases” [11]. In this study, they walk through the origin of the underlying technology behind NFT which is blockchain and the whitepaper from the first cryptocurrency like Bitcoin from Satoshi Nakamoto. From that point, the NFT was emerged when the public got attention of the Bitcoin and Blockchain technology and gave birth to the smart contract-based blockchain like Ethereum, which made NFT technically possible. In current use cases of NFT, they mentioned 3 main categories: art and collectibles, games and metaverses, and utilities and DeFi. Moreover, they further discussed the potential of future NFT use cases such as expanded DeFi, dematerializing real world assets, and supply chain management.

Another example that demonstrates the popularity of NFT is the work of S. Casale-Brunet, P. Ribeca, P. Doyle and M. Mattavelli in 2021 on the topic of "Networks of Ethereum Non-Fungible Tokens: A graph-based analysis of the ERC-721 ecosystem" [12]. This work systematically studies the number of interactions on the NFT ecosystem using the transaction data available on the blockchain network and visualizes them in a graph-based model. They have reached the conclusion that their studies on NFT networks are qualitatively very similar to the interactions measured from social networks.

3.3 Blockchain System for Anti-Counterfeiting

Following the trend of cryptocurrency and blockchain, these technologies are also applied to the study of anti-counterfeiting. Researchers in this area adopt the use of blockchain technology as a digital identity to hold some of the physical product information, hence associated them together. The owner of the digital asset will technically be implied to be the owner of the physical product as well. Among the same idea, the work from K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki [13] the solution was proposed around the RFID-enabled supply chain where Electronic Product Code of each product will be applied to the RFID tag. The interesting topic of solution validation was discussed in the publication. In conclusion, the NFT solution could prevent the majority of the possible counterfeit scenarios. Only when the counterfeit product was perfectly replicated to the point that the counterfeit is almost an identical item including the RFID tag, only then the proposed solution cannot prevent the buyer from possess the replicated product. Another work of J. Ma, S. -Y. Lin, X. Chen, H. -M. Sun, Y. -C. Chen and H. Wang [14] propose the use of NFT token throughout the whole supply chain from manufacturer through the seller and the end-customer but the main idea of using NFT embedded with the information of manufacturer and seller to gain trust from customer. Lastly, the recent work of P. M. Lavanya *et al.* [15] introduce a system that could verify the product authenticity via the verification of QR Code and the system backbone of blockchain to track the status of the product. The studies above are all trying to adopt the strength features of blockchain to their system, features such as Immutability, Traceability, Distributed and Decentralization.

3.4 Other Blockchain Applications

Along this NFT popularity wave, many researchers try to utilize the NFT technologies to resolve several problems and challenges. In 2021, X. Zhao and Y.-W. Si proposed "NFTCert: NFT-Based Certificates With Online Payment Gateway" [16], a solution to address the fraudulent activities caused by paper certificates. They demonstrated the possibility of implementing a smart contract to replace the traditional paper certificate with an NFT digital certificate issued by the College or

Universities and validated by the Verified Educational Institution on a Private Blockchain Network.

Another application of NFT in real world use cases is shown in the work of E. Ertürk, M. Doğan, Ü. Kadiroğlu and E. Karaarslan in 2021. Their work of "NFT based Fundraising System for Preserving Cultural Heritage: Heirloom" [17] demonstrates the use of NFT technology to help preserve the cultural heritage assets. They proposed the cultural property protection system which allows foundations to raise funds through a decentralized system without any intermediary intervention. As a result, they show the first use case on protecting the old olive tree from a new foundation organization. At the end, they further discuss the transaction fees on both Ethereum and Avalanche platforms where the first is overpriced and beyond the reasonable level, while the latter one is cheaper and more suitable.

In 2022, "NFT-based Asset Management System" from I. Abaci and E. E. Ulku [18] shows another adoption of NFT technology to the real-world problem. This work focuses on the tedious process of managing houses, businesses and lands by the government organization. They introduce the NFT-based system with 2 smart contracts, one for assets minting and another for asset subscription management.

CHAPTER 4

PROPOSED METHOD

In this proposal, we propose an NFT-based authentic product verification and trading platform called AutheNFT to assist consumers in securely trading genuine luxury products. The platform users could confidently recognize the origin of the product in trade by verifying the associated NFTs and be assured from the trade by reviewing the product warranty with seller consent.

For example, in a resale market where people resell the product they purchased from authorized seller to another person. The typical trading process would be to wire transfer the money, then delivery of product would follow. With the given process, there could be a chance of the delivered product having the quality lower than expected or didn't meet the agreement, resulting in fraudulent activity. With the use of AutheNFT, the digital certificate issued by the authorized seller or product manufacturer would ensure the authenticity of reselling product to the buyer. Changing the process of reselling from wired transfer the money via banking, to trading the money with the product and its NFT certificate. The trade between both parties is supported in multiple currency systems, whether it is a traditional payment system with fiat currency, or with the modern cryptocurrency.

4.1 Overall Architecture Design

As shown in Figure 7, the overall architecture design of the whole ecosystem consists of 2 types of users, Consumers and Producers. Producers are the representative entities of the business and products, who would be able to mint or issue a NFT via our platform using their official certificate. Consumers are end users who would purchase products from the producer directly or from another consumer through resell.

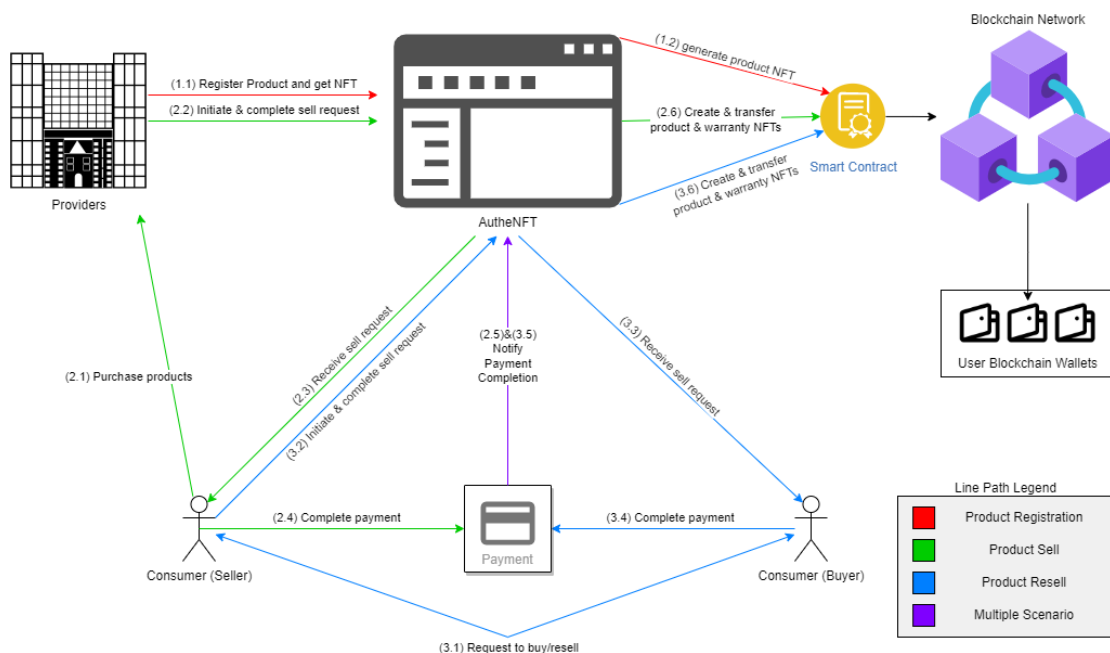


Figure 7: AuthenNFT Overall Architecture Diagram

The proposed platform is capable of supporting the following scenarios.

Direct purchase:

1. Producers register and verify their identity with the platform by signing the public agreement with signature stored on NFT token.
2. Producers register their products and mint the NFT with their self-managed certificate.
3. Product trade could be initiated from any party. The first step after trade initiation starts by the producer will be requested to sign a public product warranty with e-Signature. The signature will be temporarily stored within the system waiting to be minted into an NFT along with the warranty details.
4. Once the seller confirmed the trade with warranty signing, the consumer will receive a payment request and be redirected to the payment gateway.
5. The consumer would end up having the NFT certificate asset transferred to their digital wallet. Whether the consumer completes the payment externally and receives the NFT via manual asset transfer, or they complete the payment from the payment gateway and receive the NFT asset from the AuthenNFT platform automatically.

6. Once the product NFT has been transferred to the destination wallet. The AutheNFT platform will mint a warranty NFT using the stored signature and warranty details. The warranty NFT will then be trade to the public AutheNFT wallet for transparency and verifiability.

Resell purchase:

1. For product resell event, either the buyer or the seller can initiate an NFT trade request to AutheNFT platform by specifying the target asset and named the price.
2. The seller will be requested to sign a public product warranty with e-Signature. The signature will be temporary stored within the system waiting to be minted into an NFT along with the warranty details.
3. The buyer consumer will then receive a trade checkout notification in which they have a choice to accept the trade and proceed to the payment gateway. The buyer consumer can choose the payment method of their choice whether it is a wired-transfer or cryptocurrency transaction on the payment gateway.
4. Once the payment is completed, the NFT certificate asset would be transferred to the buyer consumer automatically.
5. Once the product NFT has been transferred to the destination wallet. The AutheNFT platform will mint a warranty NFT using the stored signature and warranty details. The warranty NFT will then be trade to the public AutheNFT wallet for transparency and verifiability.
6. The buyer consumer will officially become the rightful owner of the product. it is up to the seller to ship or deliver the product to the buyer from this point onward.

4.2 Existing Work Analysis

As discussed in chapter 3 section 3.3, all existing blockchain application for anti-counterfeiting are using ERC-721 compatible smart contract to mint the NFT token as a proof of ownership.

System	NFT Binding	Blockchain Network	First-hand Trade	Second-hand trade	Trade Interface	Seller Warranty
A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain	✓	Ethereum	✓	✓	✗ (Wallet)	✗
Blockchain-Based Application System for Product Anti-Counterfeiting	✓	Ethereum	✓	✗	✗ (Wallet)	✗
Fake Product Detection using Blockchain	✓	Ethereum	✓	✗	✗ (dApp)	✗
AuthenNFT (Proposed Method)	✓	Ethereum	✓	✓	✓	✓

Table 1: System Feature Comparison

As seen in Table 1, all systems in this analysis are addressing the problem of physical product by using NFT to bind them together. The minted NFT will be used as the core identifier to the object ownership by having metadata associated to the real-world object. They are all built on top of the Ethereum blockchain network and are all able to support the first-hand trade from product provider to the first customer. But there are some limitation to the second-hand trade as the work from J. Ma, S. -Y. Lin, X. Chen, H. -M. Sun, Y. -C. Chen and H. Wang [14] and P. M. Lavanya *et al.* [15] are only supporting the first hand trade. Moreover, all existing systems except the proposed method are all not supporting the trade interface and seller warranty. Since the proposed method AuthenNFT aims to solve the problem of anti-counterfeit in luxury product trading, the system was designed to have the

easiest trading process with least interaction between end-user and the blockchain application. This will allow user to focus on the trade, not the blockchain application usage. Lastly, even when using the blockchain technology, there are still cases where the product trade can be frauded. The AutheNFT system introduces another process to publish a legal product warranty document along with the consent from the seller by having their e-signature. This process and document aim to create the burden to the seller, make it harder to trade counterfeit items and there will be consequences to their action.

4.3 Use Cases Design

4.3.1 Product Registration

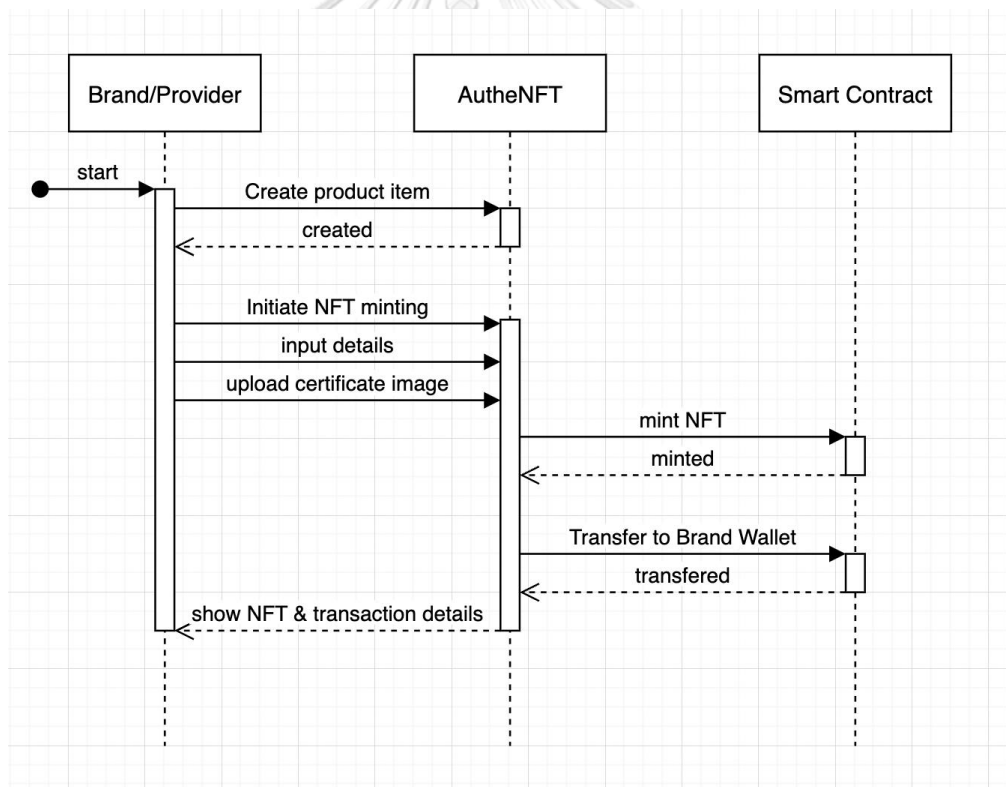


Figure 8: Asset Registration Sequence Diagram

The onboarding process for an asset is illustrated on Figure 8. There are 3 main actors involved in this process, starts with the brand or product provider registers their product with AutheNFT platform and mint NFT with product details.

The application will then contact with the smart contract on the network to issue a new NFT and transfer it to the Brand registered wallet.

4.3.2 Succeeded Product Trade

The process of product transfer including first-hand purchase and resell are almost identical as seen in Figure 9 and Figure 10. The only difference is the actors in some steps are different. A unified process helps simplify how the system operates and fraudulent proof.

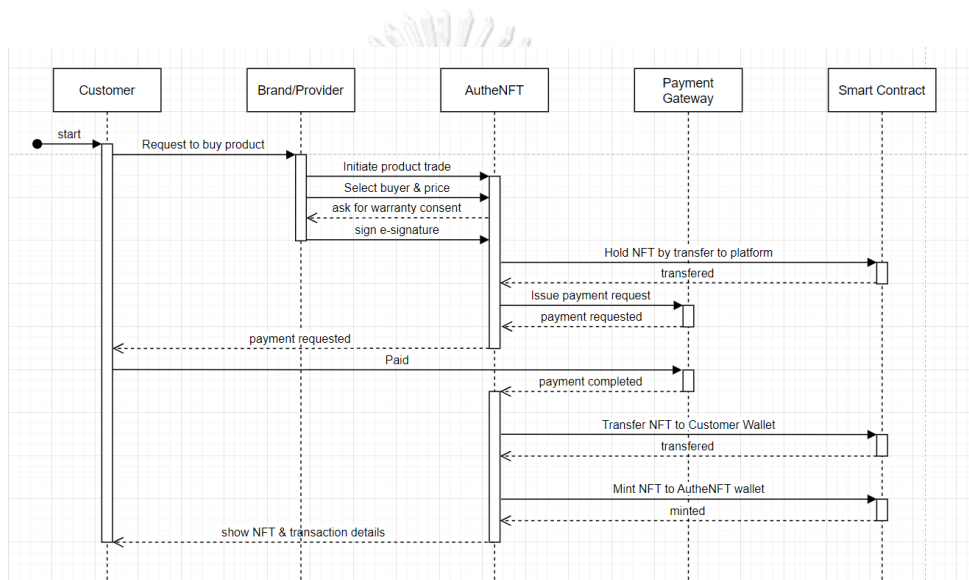


Figure 9: Asset Purchase Sequence Diagram

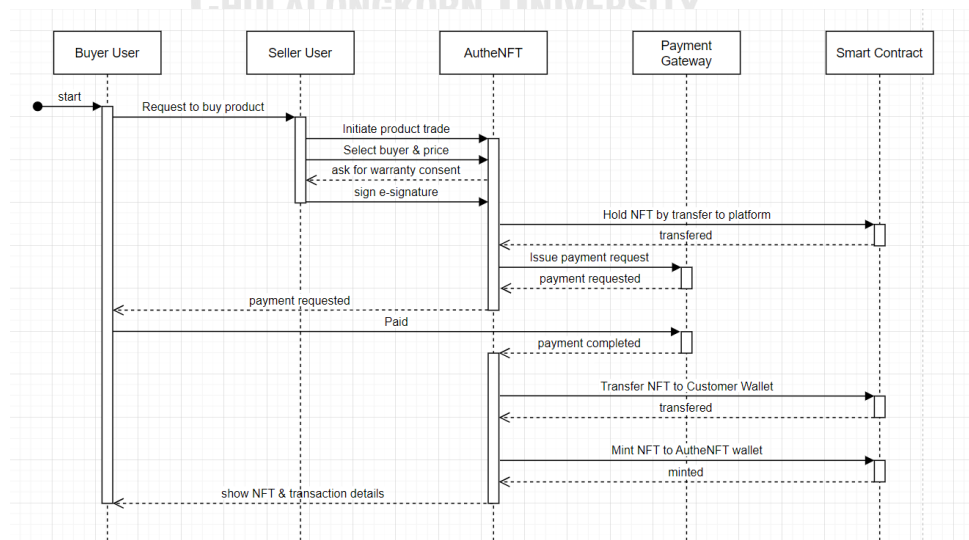


Figure 10: Asset Transfer/Resell Sequence Diagram

The process starts with a buyer notifies the owner of their desire item to purchase the product, either inside or outside of the platform. The item owner will then initiate a product trade action to the AutheNFT platform with prerequisite information of the trade. The item owner or seller will then be asked to sign a product warranty prior to the trade. After that, AutheNFT will then ask the buyer to complete the payment via supported payment method. Once the payment is done and AutheNFT has confirmed the payment, it will then proceed to contact the smart contract to complete the product certificate trade and successfully hand-over the ownership proof to the Buyer. This step includes the product warranty NFT minting and the transfer of product ownership NFT.

The warranty NFT will be created for each and every trade or change of ownership. This type of warranty is not the product warranty that will usually be issued from the manufacturer, but rather a consent from the previous owner to guaranteed that the product they are trading is authentic and that they take full-responsible if the traded product was a fraud. That is why the warranty exists for all trade operations, including user-to-user trade. It is an obligation to the previous product owner and has nothing to do with the product quality guaranteed from the manufacturer, which should not concern in this platform.

4.3.3 Failed Product Trade

In case of failure during a product trade, there will be a fallback method to resolve the situation back to the normal state. The case the product trade is unable to proceed and need to fallback is when the buyer user failed to complete the payment within the timeout period. As a subsequence to the trade failure, the product NFT transferred to the AutheNFT platform to hold the token will be transferred back to its owner when the timeout period has expired. Along with NFT returned, the payment requested on the Payment Gateway will also be cancelled. Once everything has fallback to the normal state, then the buyer will be notified of the trade cancellation and that the payment request was expired. The steps of this process are illustrated in Figure 11.

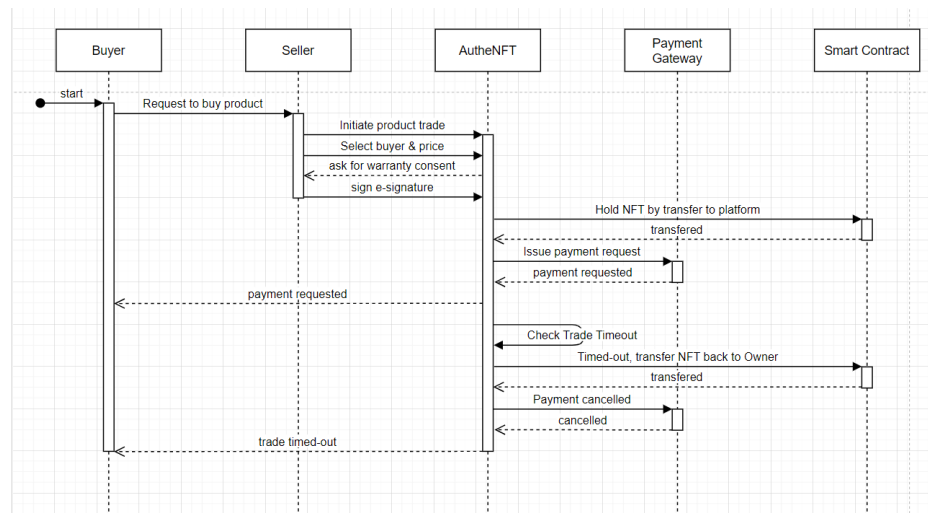


Figure 11: Failed Asset Trade Sequence Diagram

4.3.4 Product Verification

The process of item ownership verification is also provided in AutheNFT platform to assist in the trade conversation and prove of ownership. In Figure 12, any user with access to AutheNFT's ownership verification can request to check for the owner of a given NFT token id. The AutheNFT platform will retrieve the token info and response with the NFT owner information. It will also show the NFT owner's profile associated with AutheNFT platform if applicable.

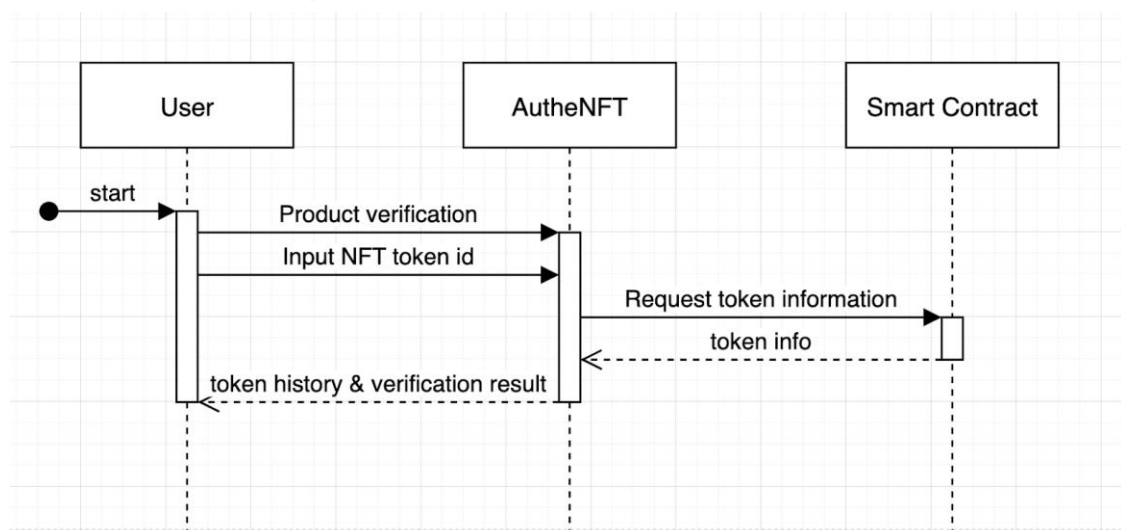


Figure 12: Asset Verification Sequence Diagram

4.3.5 Product Warranty Inspection

The process of product warranty inspection can be done after the Asset Verification page in AutheNFT platform. This feature only available for the owner of the NFT token to inspect the product warranty with consent from the previous owner. In Figure 13, after navigating to the Warranty Inspection page, the user will be able to select one of their owning NFT. The AutheNFT platform will retrieve the token info and check if the user wallet id stored within the warranty metadata matches with the current user. After the validation completed, the user will be able to see the warranty document along with the e-signature of the previous owner.

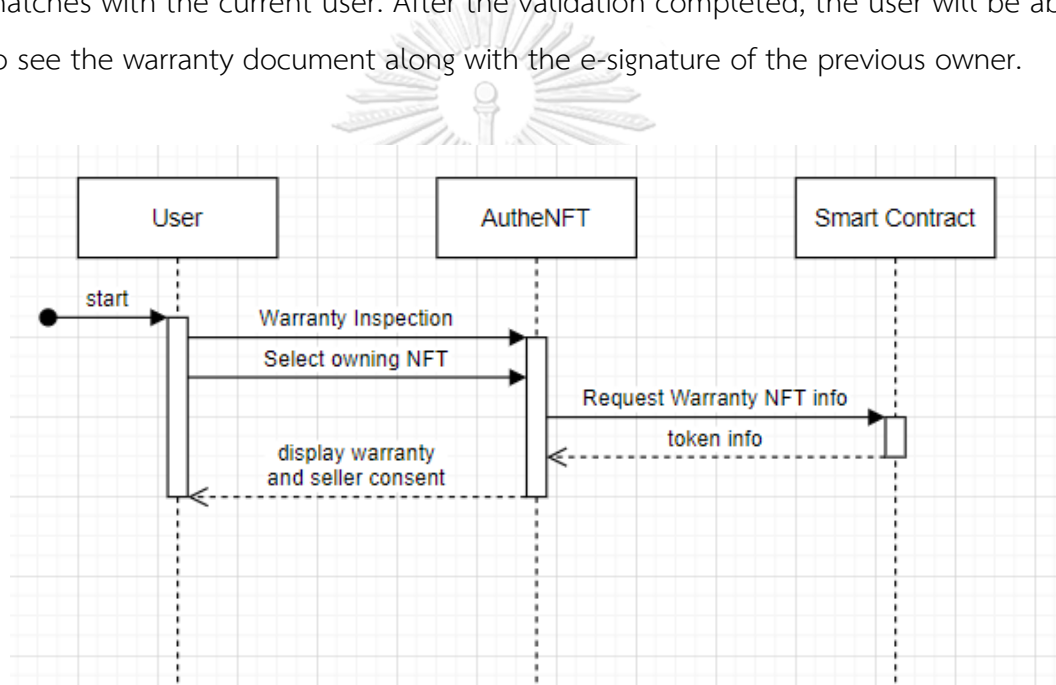


Figure 13: Product Warranty Inspection Sequence Diagram

CHAPTER 5

SYSTEM DESIGN AND IMPLEMENTATION

In this chapter, the design and implementation detail of the AutheNFT platform will be discussed in the following order, System Design, System Development and User Interfaces of the System.

5.1 Proposed System Design

5.1.1 Software Design

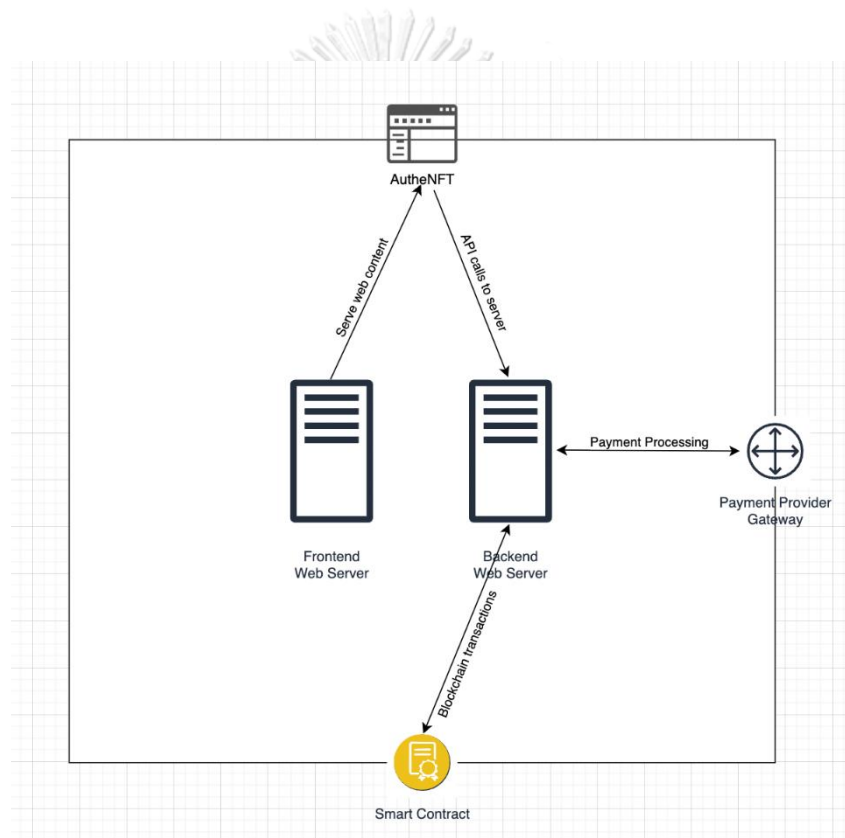


Figure 14: AutheNFT web application architecture design

The architecture for the proposed AutheNFT platform is a web application based on the Client-Server architecture, as shown on Figure 14 above. The separation between frontend and backend servers aims to improve the performance of them by splitting their workload and they can be scaled individually. The backend server is responsible for processing most of the application functionalities, including user authentication, serving frontend data, connecting with external payment

gateway and also handling most of the smart contract interaction such as token transfer, token minting, etc.

5.1.2 Smart Contract Design

The smart contract is the heart of the modern blockchain operations. It could be considered as a programmable transaction provider. The AutheNFT provides an NFT minting functionality and NFT trading with special side effects and additional Warranty Token which requires a customized smart contract to serve the platform use cases. The following bullets show requirements beyond the ERC-721 smart contract interface provided:

- Support custom metadata upon NFT minting process
- Support the non-transferrable product warranty NFT minting automatically
- Support association between product NFT and warranty NFT
- Support warranty chain metadata and traceable history

5.1.2.1 NFT Metadata Schema

```
{
  "name": "SN0012345",
  "description": "Proof of product authenticity from Brand@",
  "image": "https://<ipfs-provider>/QmWmvTJmJU3pozR9ZHFmQC2DND
wi2XJtf3QGyYiiagFSWb",
  "attributes": [
    {
      "trait_type": "model",
      "value": "Malibu"
    },
    {
      "trait_type": "Color",
      "value": "Mocha"
    },
    ...
  ]
}
```

Figure 15: Metadata of NFT from AutheNFT platform

The schema shown on Figure 15 is based on the JSON Schema and complies with the standardized ERC-721 as the metadata for the NFT token stored on the IPFS distributed file system. There are 4 main properties for each token minted on the AutheNFT platform as following:

- name - product name as the brand or provider would like to specify
- description - short description to summarize the product
- image - proof of product authenticity as an image of digital certificate
- attributes - list of product attributes as specified by the brand or provider

Non-Fungible Tokens or NFTs that was minted from AutheNFT smart contract will have this flexible metadata. From this design, it is possible to have multiple types of NFT from a single smart contract as a single NFT collection and future changes will not require a re-deployment of smart contract.

5.1.2.2 Product NFT

This type of NFT use the metadata schema from section 5.1.2.1. This is the core token of the AutheNFT platform, where the token will represent a physical product registered by the user. Since all blockchain transaction are recorded with in blocks and stored on the blockchain, it is very important that the NFT is created by a trusted party. In case of anti-counterfeit, the product owner or manufacturer should be the one who issue their products' NFT. There is no limitation to how the image metadata of the product NFT should be picked, but one good example is to store something that could verify the authenticity of the product such as certificates. The attributes metadata is very flexible and extensible as much as the product owner wanted it to be.

5.1.2.3 Warranty NFT

On the other hand, warranty NFT shares the same schema as product NFT from 5.1.2.2 but with some specification from the AutheNFT platform. The trading platform has full control and ownership of this token as the goal for its existence is

to host the product warranty somewhere in the blockchain, so the holder of this token can be anyone.

As for the warranty NFT metadata specification, the image metadata will contain an e-signature image uploaded from the previous product owner. This e-signature was signed to an e-document stored under attributes metadata. The attributes metadata is still extensible and flexible array, but there will always be 4 key-value pairs pre-filled in this metadata array. Those key-value pairs are

- `tokenId` – identifier to Product NFT that this warranty applied
- `previous-transaction` – hash string of the previous trade of this product NFT. This information allows us to identify which trade operation that this warranty applied
- `signer` – a wallet address of the previous owner, who signed the signature in image metadata
- `warranty-document` – IPFS address to the warranty text file that this warranty signature referred

5.1.2.4 Mint Function

Beyond the standard implementation of ERC-721 interfaces that we got from open-zeppelin library, our smart contract requires a special functionality when performing standard operations such as minting and transferring the tokens.

Algorithm 1 Pseudo Code for `mintNFT()`

INPUTS :(`toAddress`, `tokenMetadataUri`)

Increment `tokenId`

Mint new token using (`toAddress`, `tokenId`)

Set token metadata (`tokenId`, `tokenMetadataUri`)

Figure 16: NFT Minting Pseudo Code

The NFT minting method was overridden to allow us to properly configure the token metadata and be complied with our scheme. The pseudo code of such method is shown in Figure 16.

5.1.2.5 Transfer With Warranty Function

While the smart contract is capable of transferring tokens with a standard Transfer method, we designed our trading process to include the Warranty Token Minting as part of the Product Token trade. This functionality can be executed only by the platform which is the trade authority of the proposed trading process within the scope of this research. The pseudo code of such method is shown in Figure 17.



Algorithm 2 Pseudo Code for transferWithWarranty()

INPUTS :(*tokenId, fromAddress, toAddress, warrantyMetadataUri*)

Update associated *tokenId* to *warrantyMetadataUri*
 mintNFT() using (*AUTHENFT_ADDRESS, warrantyMetadataUri*)
if *isMinted* = true **then**
 Transfer token using (*fromAddress, toAddress, tokenId*)
end if

Figure 17: NFT Transfer with Warranty Pseudo Code

5.2 System Development

The development of the system is separated into four areas, which are development environment, web application, web backend and smart contract development.

5.2.1 Development Environment

The development environment for this project on both hardware and software are as below. It is expected for the similar system and development environment to achieve similar result from the implementation of the system.

5.2.1.1 Hardware Specification

- CPU: Intel(R) Core(TM) i7-8650U CPU @ 2.11 GHz
- RAM: 16.0 GB
- GPU: Intel(R) UHD Graphics 620

5.2.1.2 Software Specification

- OS: Windows 11, 64-bit operating system, x64-based processor
- IDE: Visual Studio Code
- Programming Languages: Typescript & Solidity
- Software Runtime: NodeJS
- Frontend Framework: NextJS with ReactJS
- Database: MongoDB NoSQL Database

5.2.2 Web Application Development

The web application was developed using NextJS, a meta-framework for web application development with rich predefined functionality such as directory routing, data fetching, rendering strategy, etc. A NextJS project will also be initialized with a predefined project structure as seen in Figure 18.

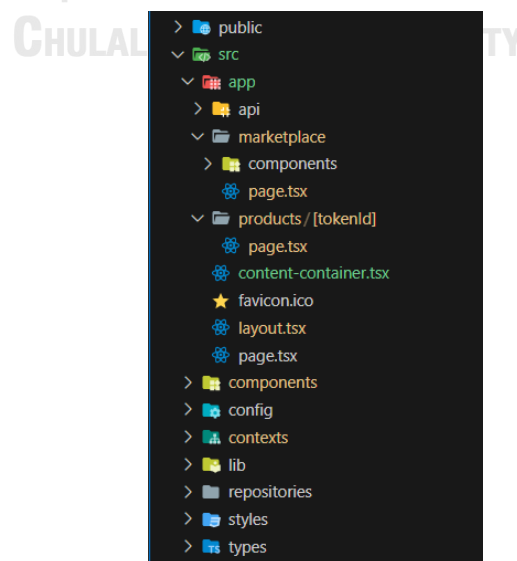


Figure 18: Project Structure

The main codebase resides under /src directory where ReactJS source code will be handled by NextJS via CLI commands. Directory Routing is a strategy in which could reduce the complexity of managing routing with code. It works by having all of the files and directory with all the same structure under /src/app. Each directory under /app will be route path. The page.tsx and layout.tsx files under each directory are the content of those route paths or subpaths.

5.2.3 Web Backend Development

The backend service was implemented separately as another server to serve requests from the web application and to communicate with the smart contract on blockchain. This design provides a separation of concern for the web application, improving both performance and security.

The backend was implemented using NodeJS with ExpressJS as our HTTP server and EtherJS as a library to communicate with the blockchain.

5.2.4 Smart Contract Development

In the beginning of the Ethereum development phase, developers were developing things from scratch using a newly developed programming language, solidity, and with minimal tools to assist their development. In today's modern age of cryptocurrency, the community and ecosystem of each cryptocurrency has grown in terms of community size and the tools supporting the developers.

Solidity is an object-oriented, statically-typed programming from Ethereum team designed to implement Smart Contracts. It adopts the curly-bracket convention from famous programming languages such as C++, Python and Javascript. An example syntax of solidity code is shown in Figure 19.


```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.16 <0.9.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Figure 19: Solidity Sample Code

Moreover, developing things from scratch take significant time to reinvent the wheel. That is where a smart contract development environment such as Hardhat comes in. Hardhat is a JavaScript's npm package which serves as an all-in-one Ethereum development environment with many features such as project template, scripting and the most important of all, contract deployment. Hardhat abstracts all of the hard work into a single command.

5.3 System User Interfaces

In Figure 20, the overview of AutheNFT user interfaces and their navigations are shown. The main landing pages are Marketplace Page, Product Page and Trade Page. Each of the pages will be discussed in the following sections.

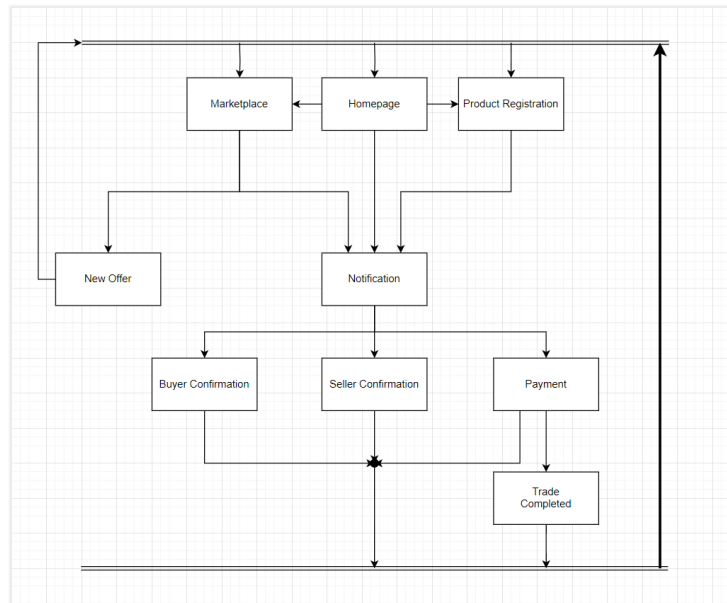


Figure 20: Window Navigation Diagram of AutheNFT

5.3.1 Marketplace Page

Marketplace is where the platform users can browse and trade genuine product as they wish. This page existence is to demonstrate the possibility of trading genuine product online with trustable platform. In Figure 21 below is the screenshot of the Marketplace Page.

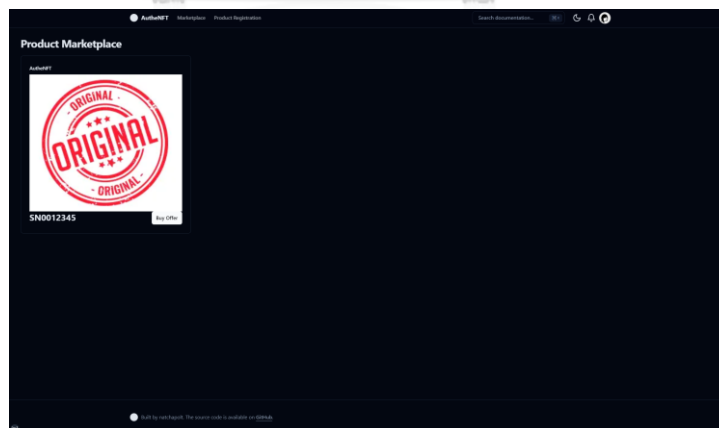


Figure 21: AutheNFT Marketplace Page Screenshot

5.3.2 Product Pages

5.3.2.1 Product Registration Page

Product Registration Page is the entry point for physical products to have digitalized entity as an NFT token. In this page, the product owner, ideally the manufacturer, will be filling information about the product and upload the image that suggested to be a certificate of product. The screenshot of this page is shown in Figure 22.

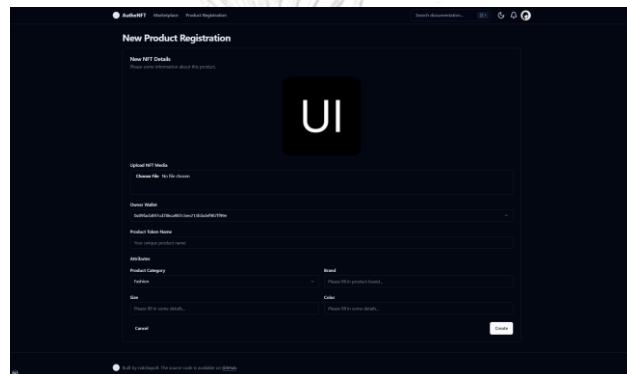


Figure 22: AutheNFT Product Registration Page Screenshot

5.3.2.2 Product Detail Page

Product Detail Page is where users can view metadata information and other useful insights about this product such as possession history, warranty, pricing trend and etc. This page also serves as a trading entry point for both parties to initiate the trade as well. The screenshot of this page is shown in Figure 23.

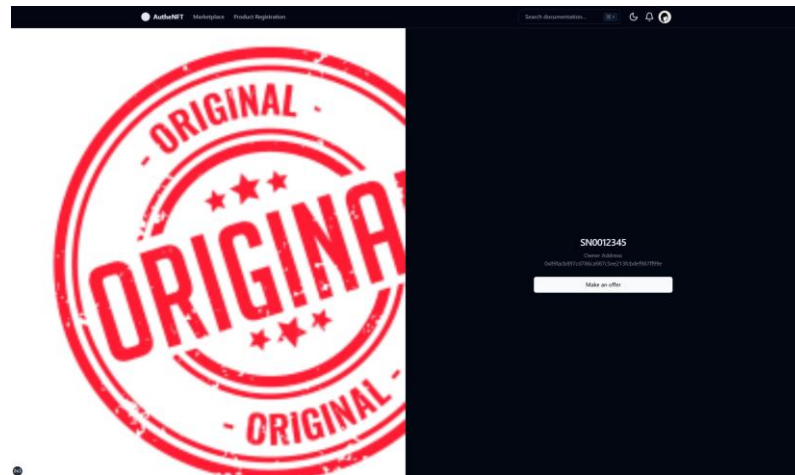


Figure 23: AutheNFT Product Page Screenshot

5.3.3 Product Trade Pages

Trading is the key functionality of this platform. In order to buy genuine product, the trading process must be solid and trustworthy. We divided the trading process into 4 steps with each step having their own page. The four pages are Trade Offer Page, Warranty Agreement Page, Trade Payment Page and Trade Completion Page.

5.3.3.1 Product Trade Offer Page

The first step in trading with AutheNFT platform is the trade offer. User from the sell or buy side could initiate the trade offer from the Product Page. After that, they will land on the Trade Offer Page which will require the user to fill in information such as offering price. Once completed, the offer will be sent to the system to notify the user that will take action in the next step. The screenshot for this page is shown in Figure 24.

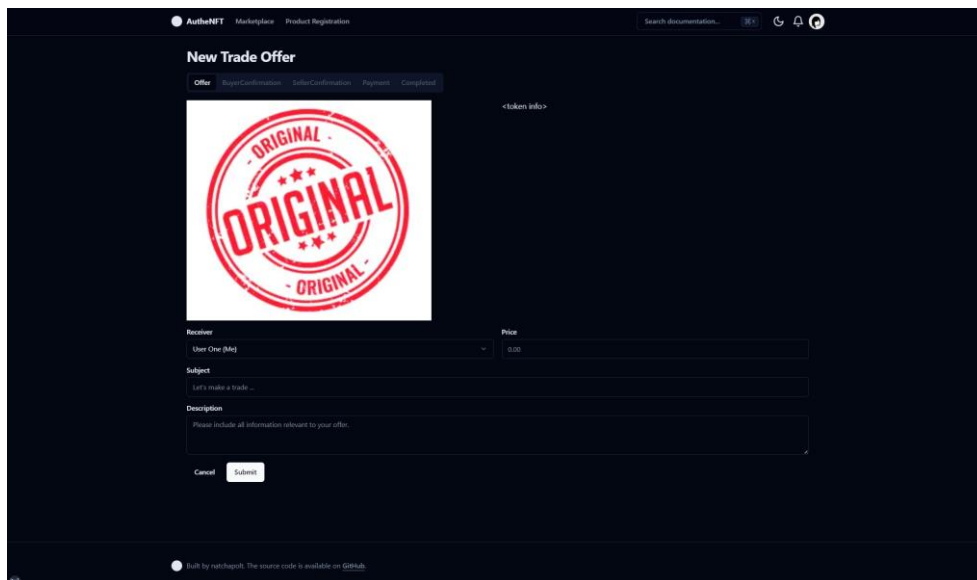


Figure 24: AutheNFT Trade Offer Page Screenshot

5.3.3.2 Seller Warranty Agreement Page

As a second step of the trade, the selling user will be notified to land on Warranty Agreement Page in which they will be informed of the Warranty that all sellers are obliged to. At the end of the page, the user will need to agree with the warranty by signing an e-signature to the AutheNFT. Once completed, they will be asked to transfer the product token in trade to AutheNFT platform. This step marks the end of trade offer from seller side. The screenshot of this page is shown in Figure 25.

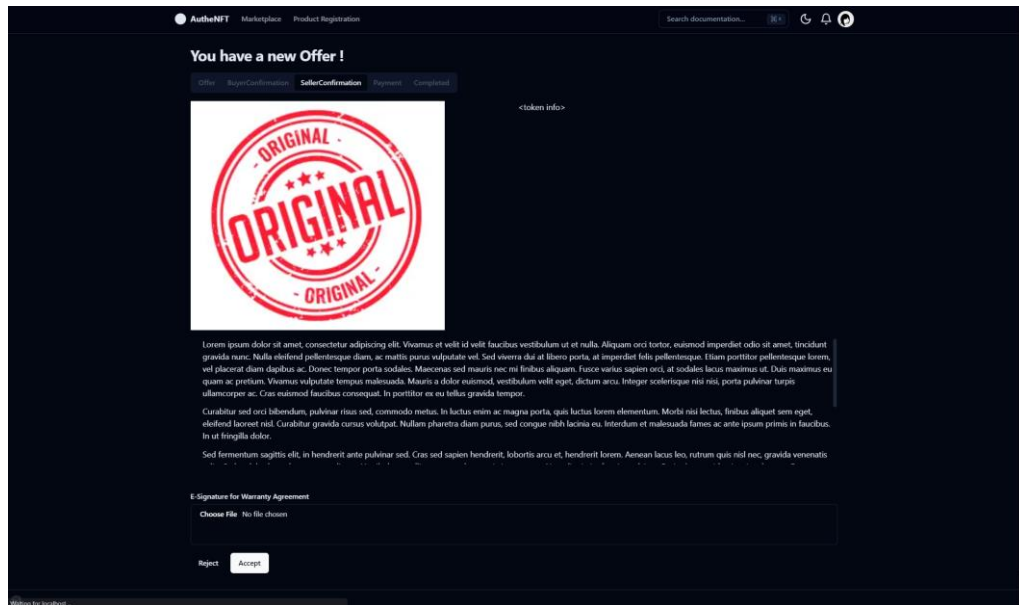


Figure 25: AutheNFT Warranty Agreement Page Screenshot

5.3.3.3 Product Trade Payment Page

Following the completion of trade offer from seller side, the buying user will be notified of payment to complete. In this page, the buyer has to complete the payment in order to proceed to receive the product token and waiting for product shipping from seller. The screenshot of this page is shown in Figure 26.

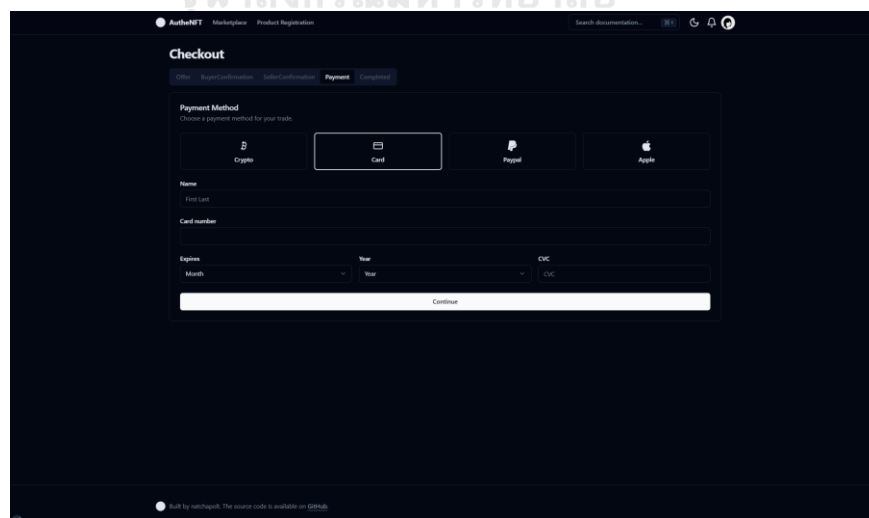


Figure 26: AutheNFT Payment Page Screenshot

5.3.3.4 Product Trade Completion Page

At the last step of product token trading, once the blockchain transaction that transfer token to buyer has been completed, then the buyer will be notified of the successful trade. The buyer will be able to land on the Trade Completion Page to see the information about the product token, warranty and transaction information. The screenshot of this page is shown in Figure 27.

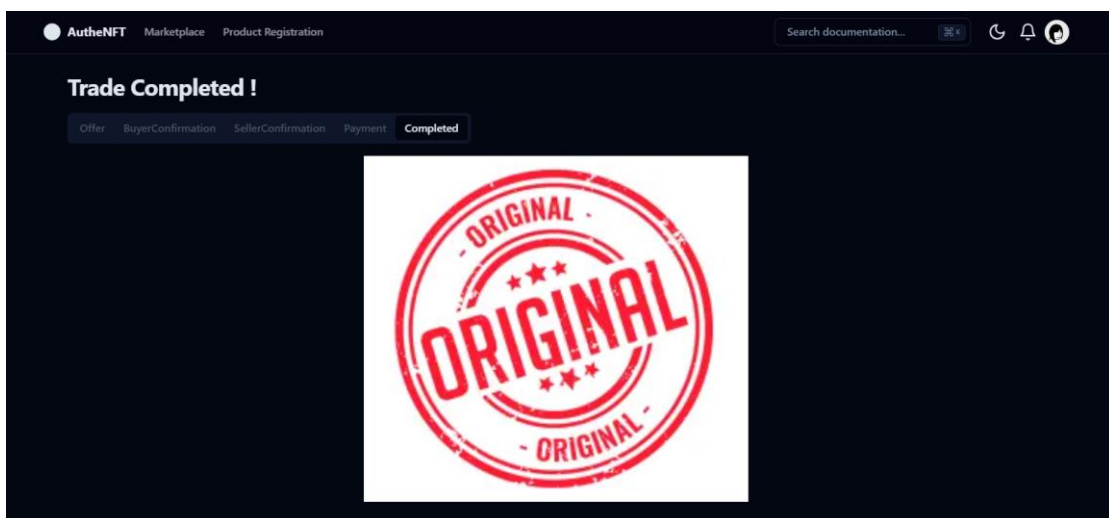


Figure 27: AutheNFT Trade Completion Page Screenshot

CHAPTER 6

SYSTEM TESTING AND RESULTS

6.1 System Testing on Use Cases

The testing of the platform will be conducted by the two main scenario which are when the product was traded first-handed and when the product was traded second-handed. These scenarios will demonstrate how the AutheNFT platform could be used in the regular trading situations.


6.1.1 Test Case 1: Buying from official store

1. Register product with AutheNFT

When an official brand wants to sell their products with NFT token, AutheNFT platform onboards their product via a Product Registration page where the manufacturer will be able to register their products and create the counterpart NFT tokens of their products. The sample of the page is shown in Figure 28.

New Product Registration

New NFT Details
Please provide information about this product.



Upload NFT Media
Choose File Portrait.jpg

Owner Wallet
0x89facb897cd786ca987c5ec213fcbdef987ff99e

Product Token Name
SN0012345

Attributes

Product Category Fashion	Brand GUCCI
Size M	Color Red

Cancel Create

Figure 28: minting a new token 'SN0012345' from Product Registration Page

Behind the scene, the certificate image and product information will be saved as files in the backend server and will be uploaded to IPFS where they are stored across the public network. In this proposal, we use Pinata, an IPFS pinning provider. In Figure 29, the two files are stored on IPFS with CID as shown below.

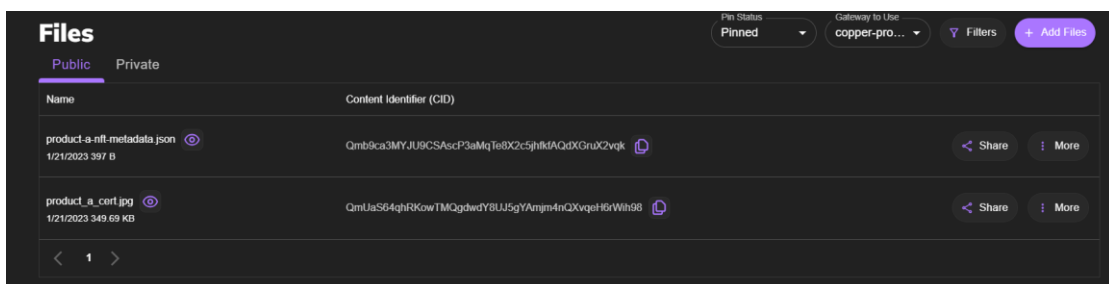


Figure 29: Pinata web portal shows NFT Token 'SN0012345' files on IPFS

2. Verify product created by official store

To make sure that the product was successfully registered and the nft token was generated for the registered product, we can check the latest transaction of the platform nft collection. As seen in Figure 30, even on public website like Etherscan, we can see that the token was generated and transfer to the correct recipient that was provided. Furthermore, if we check on the AutheNFT platform under marketplace page, there will be a new nft token shown in the marketplace listing as shown in Figure 31. Once confirmed from both places, we can conclude that the product was successfully registered.

The screenshot shows the Etherscan interface for 'AutheNFT #1'. The main area displays a placeholder for the NFT image with a hexagonal 'NFT' logo. To the right, a 'Details' panel lists the following information:

- Owner: 0x42e6b4f2588B09f0F7C685A81A37A60bC03dc5De
- Contract Address: 0xc58272a8f9b963A06e4E1E3d2B2BBc234b40f7b
- Creator: 0x42e6b4f2588B09f0F7C685A81A37A60bC03dc5De
- Token ID: 1
- Token Standard: ERC-721

Below the details is the 'Item Activity' section, showing a table with one record:

Txn Hash	Age	Action	Price	From	To
0x9c4649d9e873f2907...	22 mins ago	Mint		0x000000...00000000	0x42e6b4...C03dc5De

A note at the bottom states: "The NFT page displays details such as properties and trading history for a specific token ID in an NFT contract. Learn more about this page in our Knowledge Base."

Figure 30: Etherscan public web with AutheNFT Token information

The screenshot shows the AutheNFT Marketplace interface. The main content area features a product card for 'AutheNFT' with a red circular stamp that says 'ORIGINAL' and 'SN0012345'. A 'Buy Offer' button is visible below the product image. The top navigation bar includes 'AutheNFT', 'Marketplace', and 'Product Registration'. A search bar is located in the top right corner.

Figure 31: AutheNFT Marketplace Page with NFT Token 'SN0012345'

3. Customer buying product from the store

In this scenario, we assumed that a customer walks into a luxury fashion store and would like to buy a new product line that comes together with an NFT Token when bought from official store.

The customer will be asked to create an account with AutheNFT platform. Once the account is ready and associated with Ethereum Wallet, then the official store will go to the product detail page and initiate trade offer to the buyer wallet as shown in Figure 32.



Figure 32: AutheNFT Product Detail Page of NFT Token 'SN0012345'

The official store will land on the Trade Offer Page and they will be able to set the offer details. When ready, the official store will submit an offer to the receiver which in this case is the buyer account. Figure 33 shows the sample view of Trade Offer Page.

 A screenshot of a dark-themed web interface titled 'New Trade Offer'. At the top, there is a progress bar with five steps: 'Offer' (selected), 'BuyerConfirmation', 'SellerConfirmation', 'Payment', and 'Completed'. Below this, there is a large white square containing a red circular stamp that says 'ORIGINAL' with three stars above and below it. To the right of the stamp, there is a '<token info>' link. Below the stamp, there are several form fields: 'Receiver' with a dropdown menu showing 'User One (Me)', 'Price' with a text input field containing '0.00', 'Subject' with a text input field containing 'Let's make a trade ...', and 'Description' with a larger text area containing the placeholder text 'Please include all information relevant to your offer.'. At the bottom left, there are two buttons: 'Cancel' and 'Submit'.

Figure 33: AutheNFT Trade Offer Page sending offer of NFT Token 'SN0012345' trade

- Customer received notification to accept trade offer

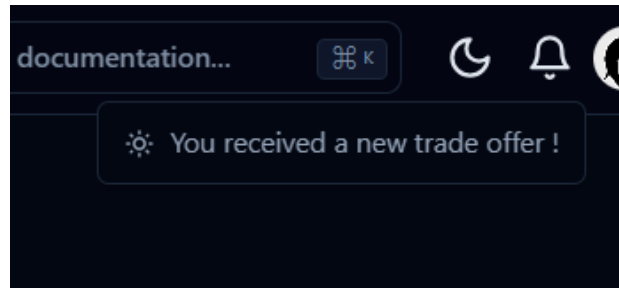


Figure 34: Sample of notification as an entry point to many pages

Once the offer was sent from the official store, the buyer will be notified on the AutheNFT platform for a new trade offer to be accepted as shown in Figure 34. When clicked on the notification, the buyer will land on a Buyer Confirmation Page where they will see the full detail of the offer that were made to them. After the buyer has reviewed the detail of the trade, then you can click Accept to proceed to the next step. Example of Buyer Confirmation Page is shown in Figure 35.

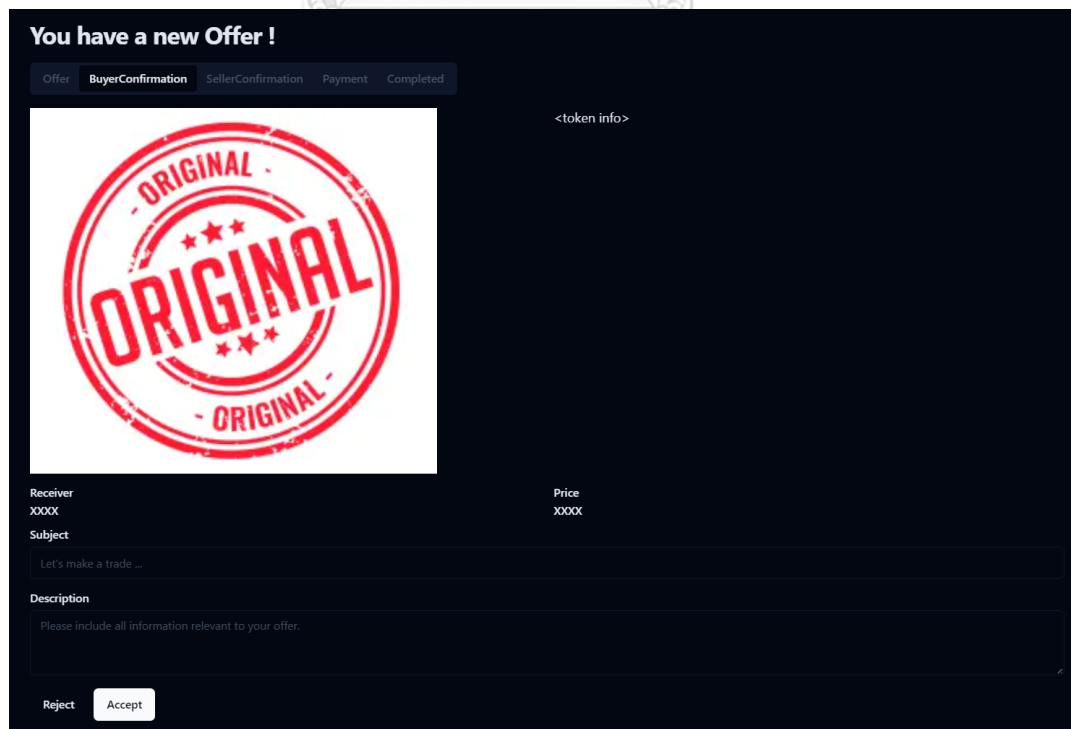


Figure 35: Buyer Confirmation Page to respond to trade offer of 'SN0012345'

5. Store confirm to proceed with the product trade

When the buyer accepted the trade, the notification on the token owner side will be notified. The official store will then see a notification similar to the buyer but will land them to the Seller Confirmation Page as shown in Figure 36.

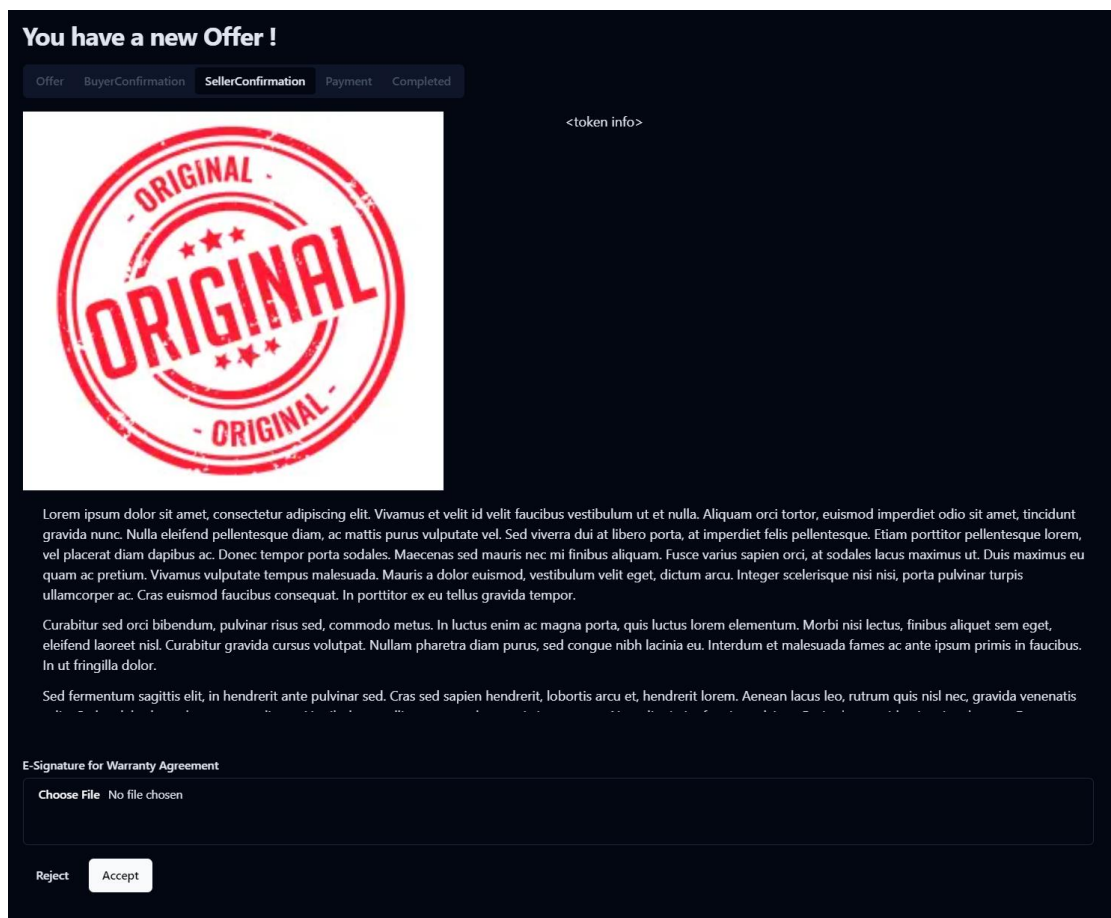


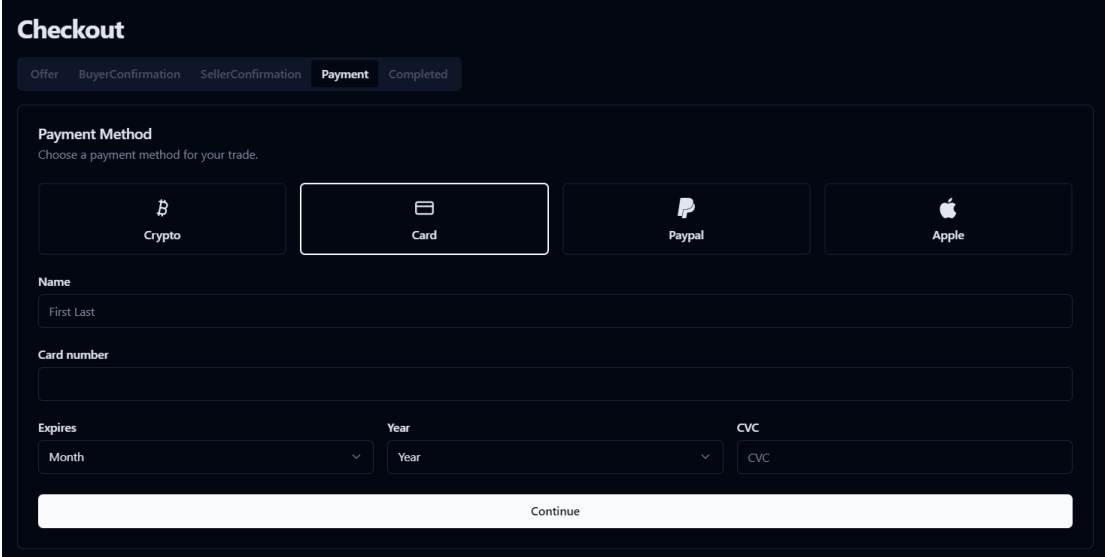
Figure 36: Seller Confirmation Page with Warranty Agreement for 'SN0012345'

In this page, the seller is required to consent to the Warranty Term and Condition as displayed in the text above. The seller will also have to sign E-Signature as a proof of acceptant to the warranty document that will be issued by AutheNFT. After all conditions are met, then the Accept button will be clickable. If the seller accepts this trade offer and warranty condition, then the e-signature information will be sent to the AutheNFT server to prepare for when the trade completed. The NFT

Token of the product that the seller owns will be asked to transfer and temporarily stored in the AutheNFT platform wallet and wait for the trade completion as well.

6. Customer proceeds to payment and completes the trade

After seller confirmation, the buyer will be notified via the notification again. In this step, the buyer will land to the payment page where they are expected to pay for the product, in which the payment options are both cryptocurrency and regular fiat currency.



Checkout

Offer BuyerConfirmation SellerConfirmation **Payment** Completed

Payment Method
Choose a payment method for your trade.

Crypto Card Paypal Apple

Name
First Last

Card number

Expires **Year** **CVC**
Month Year CVC

Continue

Figure 37: general Payment Page with multiple payment options

Once the payment in Figure 37 was completed, the AutheNFT server will process the trade request. Behind the scene, the AutheNFT server will first upload the e-signature of the seller and contact the Smart Contract to mint a new warranty nft token. This warranty token will store information about the current trade, buyer, seller and warranty condition with the media of the token being the signature of the seller stored on IPFS. Next, the AutheNFT server will initiate a token transfer with the Smart Contract from itself to the buyer wallet.

Figure 38 shows a Trade Completion Page where the buyer will be landed once the payment and AutheNFT server completed its transactions. This page marks the end of the successful trade.

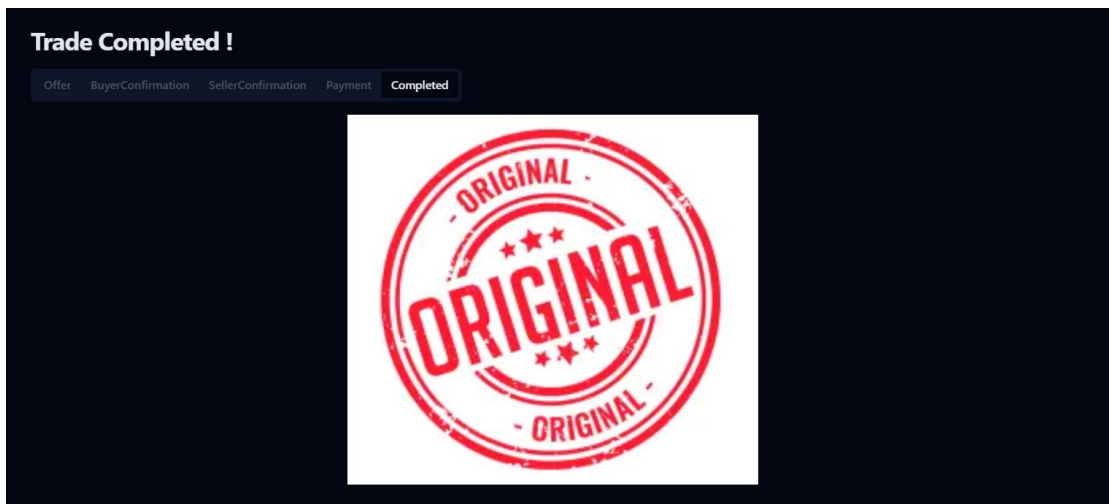


Figure 38: Trade Completed Page for Buyer User on ‘SN0012345’ trade

6.1.2 Test Case 2: Buying secondhand product

1. Buyer found product listing on marketplace page

In this scenario, the AutheNFT marketplace page is viewed by a buyer user. The buyer can browse all of the products that was registered with AutheNFT platform and send a trade offer for any listing product that the buyer interested in. Once clicked on the interested listing, the buyer will see product information on Product Detail Page as usual. Both marketplace and product detail pages will be similar to Figure 21 and Figure 23 respectively.

2. Buyer initiates trade offer

Once proceed to make an offer, the buyer will land on the Make Offer Page same as the one in Figure 24. The interface and process of making an offer is also identical to “Test Case 1 – step 3”. However, the advantage of making an offer as a buyer is that there is no need for Buyer Confirmation step anymore. The trade offer will proceed to the Seller Confirmation step right away and the seller will be notified of the offer. Figure 39 below shows the first step in Seller Confirmation page when offered from a buyer.

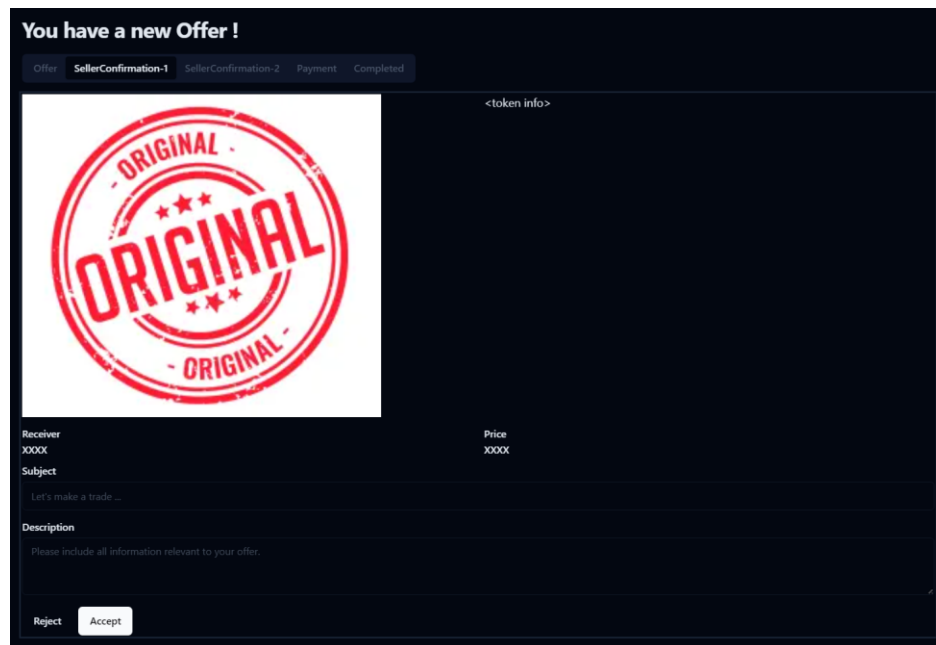


Figure 39: Alternatively, the confirmation pages change from Buyer-Seller to Seller1-Seller2 based on who initiated the trade offer

3. Repeated “Test Cast 1 – step 5 and 6”

After the trade has been accepted by the Seller, the whole trading process will be repeated as seen in Test Case 1 – step 5 and step 6, starting from getting the Seller consent to the warranty, until the end where buyer pays for the token and completed the trade.

6.2 System Cost Analysis

6.2.1 Token Minting Cost

A single operation to mint NFT token costs 1 Ethereum transaction as shown in Figure 40. The average cost of Ethereum transaction is around 24 Gwei or around \$0.79, based on Etherscan statistics which can be seen in Figure 41. That amount is the cost for each product registered to the platform.

TX Hash	Method	Age	From	To	TokenID
0x9c4649d9e873f2907...	MINT NFT	6 days 4 hrs ago	0x000000...00000000	0x42e6b4...c03dc5De	#1

Figure 40: Transaction created from NFT Token Mint operation

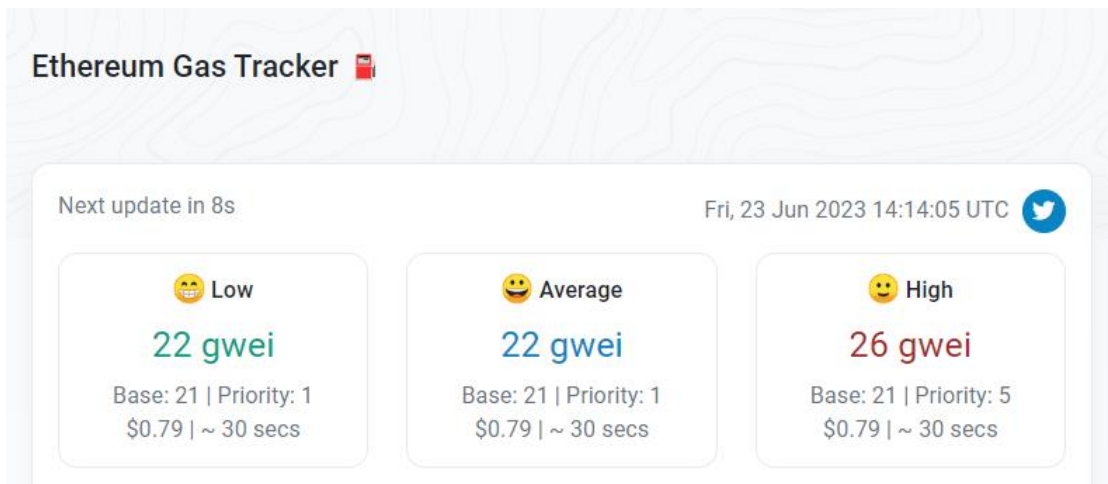


Figure 41: Ethereum Gas Price from Etherscan on 23rd June 2023

6.2.2 Total AutheNFT Trade Cost

Trading an asset in AutheNFT platform performs 3 blockchain transactions. These transactions happened when the seller stores the NFT Token with the platform and the last two transactions happened after the buyer completed the payment, then the platform will publish the warranty to the public network and transfer the NFT Token to the buyer. So, the total cost of each product trade is around \$2.37.

6.2.3 Other Network Cost Comparison

The cost or fee from using the AutheNFT can be categorized into 3 operations which are Product Registration, Rejected Trade Offer and Completed Trade Offer as seen in Table 2. It also shows the number of transactions needed for each operation category. The cost for transaction fee of Ethereum are \$0.79 and \$2.37 as discussed in previous sections. However, based on the survey of alternative blockchain networks such as Stellar and Polkadot, those newer network with less user count are way cheaper. Even a newer generation with more powerful features, like Polkadot, are still cheaper than Ethereum. This table shown that if we change the core blockchain network that operates the blockchain operations for AutheNFT to

something else, we could reduce the cost of trade even more and offer a better experience to the platform user.

Fee Category	Trx Amount	Ethereum (ETH)		Stellar (XLM)		Polkadot (DOT)	
		Fee per trx	Total Fee	Fee per trx	Total Fee	Fee per trx	Total Fee
Product Registration	1	\$0.79	\$0.79	\$0.10	\$0.10	\$0.46	\$0.46
Rejected Trade Offer	2	(0.00182 ETH)	\$1.58	(1.04 XLM)	\$0.20	(0.08 DOT)	\$0.92
Completed Trade Offer	3		\$2.37		\$0.30		\$1.38

Table 2: Transaction Fee cost comparison between ETH, XLM and DOT



CHAPTER 7

SUMMARY AND FUTURE WORK

Anti-counterfeit products can be found anywhere in the world, regardless of countless effort to prevent or destroy them. As shown in this work, many attempts to address the mentioned problem has never completely achieve the solution yet. In this research, we have proposed an improved, yet another, trading and verification platform for genuine product trade. This platform is not only verifying and showing information about the product to the user, but it also assists user in a more trustable trade by providing information about product token, product history and, most importantly, a consent from the seller to the product warranty. We discussed the design of process, design of software and implementation detail of the platform. Lastly, we demonstrate the primary use cases of online trading platform comparing AutheNFT to the trading platform in the market. And in the end, we discussed the cost of using Blockchain technology in the product trade.

This work of AutheNFT platform is a prototype to the ideal genuine product trading platform with some room to improve. In future work, we could change the core blockchain network from Ethereum to cheaper option. We can even adopt newer technology such as one that allows us to trade token across chains. On the product trade process, we could improve the warranty to be consent from both seller and buyer to be agree upon an amendable warranty contract. Finally, we could reduce the operation cost by using zero-cost network such as testnet or localnet for internal operation, but compromising the transparency of information on blockchain network.

REFERENCES

1. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.
2. Buterin, V. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. 2014.
3. Martin Becze, H.J., et al. *EIP-1: EIP Purpose and Guidelines* 2015.
4. Fabian Vogelsteller, V.B. *EIP-20: Token Standard*. 2015.
5. William Entriken, D.S., Jacob Evans, Nastassia Sachs, *EIP-721: Non-Fungible Token Standard*. 2018.
6. Witek Radomski, A.C., Philippe Castonguay, James Therien, Eric Binet, Ronan Sandford *EIP-1155: Multi Token Standard*. 2018.
7. Benet, J., *IPFS - Content Addressed, Versioned, P2P File System*. 2014, arXiv.
8. Labs, P., *Filecoin: A Decentralized Storage Network*. 2017.
9. P. Lei, F.C.-T., C. Chatwin and R. Young, *A secure mobile track and trace system for anti-counterfeiting*. 2005.
10. M. Lehtonen, N.O.a.H.V., *Features, identity, tracing, and cryptography in product authentication*, in *2007 IEEE International Technology Management Conference (ICE)*. 2007: Sophia Antipolis, France.
11. Park, A., et al., *The Evolution of Nonfungible Tokens: Complexity and Novelty of NFT Use-Cases*. IT Professional, 2022. **24**(1): p. 9-14.
12. Casale-Brunet, S., et al., *Networks of Ethereum Non-Fungible Tokens: A graph-based analysis of the ERC-721 ecosystem*, in *2021 IEEE International Conference on Blockchain (Blockchain)*. 2021. p. 188-195.
13. K. Toyoda, P.T.M., I. Sasase and T. Ohtsuki, *A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain*. IEEE Access, 2017. **5**: p. 17465-17477.
14. J. Ma, S.-Y.L., X. Chen, H. -M. Sun, Y. -C. Chen and H. Wang, *A Blockchain-Based Application System for Product Anti-Counterfeiting*. IEEE Access, 2020. **8**: p. 77642-77652.
15. Lavanya, P.M. and e. al., *Fake Product Detection using Blockchain*, in *2021 4th*

- International Conference on Computing and Communications Technologies (IC CCT)*. 2021, IEEE: Chennai, India.
16. Zhao, X. and Y.-W. Si, *NFTCert: NFT-Based Certificates With Online Payment Gateway*, in *2021 IEEE International Conference on Blockchain (Blockchain)*. 2021. p. 538-543.
 17. Erturk, E., et al., *NFT based Fundraising System for Preserving Cultural Heritage: Heirloom*, in *2021 6th International Conference on Computer Science and Engineering (UBMK)*. 2021. p. 699-702.
 18. Abaci, I. and E.E. Ulku, *NFT-based Asset Management System*, in *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. 2022. p. 697-701.





จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

VITA

NAME Natchapol Thongruang
DATE OF BIRTH 28 March 2020
PLACE OF BIRTH Thailand
INSTITUTIONS ATTENDED King Mongkut's University of Technology Thonburi

