JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

NFT for Collectibles.

Authors: Dr. Asha[1@], Kishore Karthikeyan[2#], Nikhil Gowda S M[3#], Prasad B Jakkali[4#], Rakesh S[5#.]

1@ - Associate Professor, Dept. of CSE, Dr. Ambedkar Institute of Technology, Bangalore-560056.
2#, 3#, 4#, 5# - Under Graduates, Dept. of CSE, Dr. Ambedkar Institute of Technology, Bangalore-560056.

ABSTRACT

Limited edition collectibles such as shoes, watches, vehicles, and so on are high-value goods whose value only grows with time, but there is no means to validate the item's originality or track the chain of ownership. This is usually done with a tangible certificate of authenticity, which can get lost or damaged over time. In this paper, we solve this problem by creating an NFT (Non-Fungible Token) for the object that will be permanently recorded on the blockchain network and will trace the chain of ownership as well as the cost at each transaction.

NFTs can be issued to rare collectibles to aid in the authentication of the item's authenticity. Blockchain tokens are classified as either fungible or non-fungible assets.

Fungible tokens are interchangeable; they are identical and can be replaced by another identical token. They may be used to represent everything from Bitcoin and video game cash to tokenized

representations of actual commodities like crude oil or gold.

NFTs (non-fungible tokens) are one-of-a-kind and cannot be traded. Non-fungible assets are unique and cannot be swapped directly, such as a piece of digital art you made, a car ownership certificate, or a gaming character.

The NFT which is created is secured by the consensus mechanism of blockchain and prevents

fraudulent transactions. The NFT can be transferred from one ETH wallet to another ETH wallet when the collectible is sold to another person and this transaction is stored in the blockchain. The NFT's whole transaction history is permanently preserved on the blockchain and can be confirmed by anybody using the token ID.

Keywords: Blockchain, NFT, token ID, smart contracts, hash function, consensus algorithm, immutable, chain of ownership, Decentralized.

1. Introduction

BLOCKCHAIN AND SMART CONTRACTS

Blockchain technology constructs a decentralized ledger by utilizing hash functions to store blocks of transactions immutably. A hash function performs a one-way cryptographic mapping of data of an indeterminate size to a fixed-size hash value, where swapping one bit in the input completely changes the hash value [1], [3]. Transactions in a blockchain are grouped into blocks, and each transaction represents an interaction between two entities. The blocks are hashed, and the resulting value from each block is incorporated inside the following block's metadata to form a chain of immutable data [1], [2]. The transactions and blocks are validated and published by mining nodes that run a consensus algorithm. The most common consensus algorithm is Proof-of-Work (PoW), which requires solving a computationally difficult puzzle [1], [4].

NFTs AND DECENTRALIZED STORAGE

Since the inception of blockchain technology in 2008, the technology has grown significantly. Most of the advancements have come with the introduction of smart contracts, which in turn have enabled the utilization of tokens. Non-Fungible Tokens have recently gained huge traction in their application to solve a challenge faced across many different digital domains, which is proving ownership [1], [5]. Proving ownership in different applications and enforcing it throughout the system has been an issue. NFTs leveraging the blockchain surged to overcome such a challenge. By giving a unique tamper-resistant token to each digital asset, we can guarantee fair payment, enforce granular access control, and preserve the buyer and seller's rights [1], [2]. NFTs achieve this through transferability, immutability, transparency, availability, and fraud prevention [1].

The storage of the NFT is usually done on a decentralized storage network. The asset is uploaded along with the corresponding metadata, and both are persistently saved on the blockchain. This approach is necessary to avoid bloating the blockchain since the assets vary in size, and the data has to be saved across the network [1].

Existing System Under the existing system, when a collectible is bought by an individual the seller gives the individual the "Certificate of Authenticity" which was issued by the manufacturer of the collectible. When another person wants to buy the collectible from the individual he can verify the authenticity of the collectible by verifying the certificate of authenticity. There is however a problem in this system that the certificate of authenticity can be lost or damaged and thus the individual will have no means of proving the authenticity of the collectible he possesses.

Scope of Project: The scope of this project is to implement a Non-Fungible Token (NFT) system which

- Issues an NFT when the collectible is sold for the first time
- Tracks the chain of ownership of the collectible
- Makes it easy to verify the authenticity of the collectible

2. Literature review

The authors in [2] present a research paper on tokenization and blockchain. In their comprehensive study, they focus on the different categories of tokens, such as fungible, non-fungible, and semi-fungible tokens. In addition to discussing the opportunities of NFTs, they also present the risks and security concerns.

The study conducted in [5] concentrates on the market dynamics and security issues of the NFT ecosystem, particularly on the 8 NFTMs. Their research discovered bugs in several marketplaces, as well as malicious trading between users and discrepancies among some of the most expensive sales in the NFT trade.

The authors of [6] discuss the NFT state of the art, properties, and security issues as well as challenges. Their report also includes NFT opportunities such as their importance in the gaming industry, e-commerce, as well as virtual events and the protection of digital assets and collectibles.

A conceptual NFT-based patent framework design is proposed by the authors in [7]. The paper describes the solution's various layers, which include storage, authentication, verification, blockchain, and the application layer. The authors focused on utilizing NFTs to protect intellectual properties. Their framework is theoretical and can be improved upon by adding a programmable logic implementation using smart contracts.

The authors in [11] provide a perspective of the problems and solutions for smart contracts within blockchain applications. A trend of increasing publications about this subject was presented within this study. In addition, they found that the most discussed problems and solutions regarded security, privacy and scalability of blockchains along with the ability to program smart contracts themselves.

The authors in [12] discussed the Software Development Life Cycle and testing smart contracts built for blockchain applications. In addition, they found that there was not a clear methodology for validating and evaluating the methods used to test smart contracts as well as the development process. They showed that software developers would continue to create smart contracts that will have bugs or errors, proving to be a costly security vulnerability for the smart contract's customers.

The authors in [13] explored studies from 2008-2020 that related to the design patterns, design tools, testing methods, and privacy concerns associated with smart contract blockchain applications. They found that there were multiple challenges such as vulnerabilities, inefficient analysis tools, limited complexity, lack of testing, and lack of privacy. These challenges were argued to be the reason for the slow adoption of smart contracts into more applications.

The authors in [14] discussed the shortcomings that blockchain systems suffer from in terms of performance and security. They argued that these issues must be resolved for widespread adoption of blockchain applications built by incorporating smart contracts. Their goal was to provide an analysis of all blockchain systems and their functions to gain a greater understanding of the domain.

Blockchain technology can be applied to numerous different applications, such as payment or money transfer, supply chain monitoring, insurance claims, copyright infringements, healthcare, and personal identification [1].

MetaMask is an internet-browser-extension-based Ethereum wallet. MetaMask enables users to hold EOAs and sign transactions. Wallet generation algorithms enable MetaMask to generate multiple EOAs off-chain. Each EOA has a private key and a public address [3]. MetaMask also provides a seed phrase to recover EOAs in case of loss of password. The seed phrase and private keys should be kept secret. DApps connect to MetaMask automatically, following the user's approval. It allows users to see their assets, such as ETH and Tokens, and transaction history. Users can import and export private keys for EOAs [3], [4].

Hardhat is an ''Ethereum development environment for professionals'' to compile, deploy, debug, and test Solidity [15] smart contracts on Ethereum-based local networks, public testnets, and mainnets. With Hardhat, developers can also automate the repetitive tasks entailed in the

development of smart contracts and DApps. A local Ethereum network built specifically for developers is part of Hardhat [8], [10].

Smart contracts in production are deployed on public networks called mainnets. However, deployment on mainnets is costly. For cost-effective validation, verification, and testing of smart contracts, local networks, and public testnets can be used. Similar to mainnets, testnets have their own collection of nodes running the same protocol as the respective mainnet. The popular Ethereum public testnets are Rinkeby and Ropsten [8]. Testnets generally have a lower transaction fee than mainnets. Each testnet has several faucets, which can transfer native currency, tokens, and NFTs to users as a freebie [8], [9].

A token is minted (created) by calling the appropriate method of the token contract, which generally complies with the ERC-721 or ERC-1155 standard. A single token contract can manage the ownership of a number of NFTs. Every NFT is assigned an integer called tokenId. Therefore, an NFT is uniquely identified by the ⟨token_contract_address, tokenId⟩ pair on the blockchain. A "family" of NFTs, which are either similar, or based on a common theme, called a collection. And the further function that are carried out on the token that is minted are token listing and token trading [5].

3. Design and Methodology

The NFT for Collectibles system has four main building blocks. The user interface is built using ReactJS. React JS is an open-source JavaScript library used for building UI components. A distributed ledger system is used to store the metadata. Metadata consists of the description, name and price of the NFT. The important and vital component is the blockchain. The blockchain stores the creation and transfer details of the NFT. A smart contract is used to record the data on the blockchain.

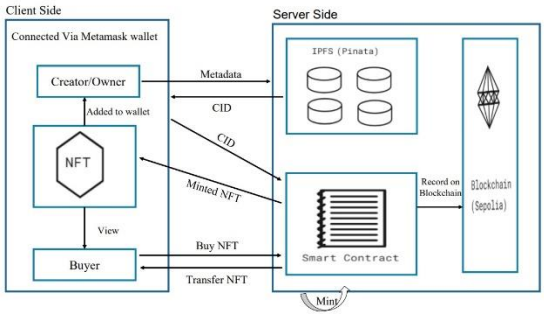

Fig. 1 System Architecture

The system uses a Etherium wallet to store NFT of the users. The Etherium wallets used are provided by Metamask. Metamask is a browser extension to handle crypto-currencies and facilitate transactions. Metamask interacts with the blockchain and writes transactions into the blockchain. Smart Contract is a set of predetermined rules established to interact with the blockchain to conduct the transactions automatically. The IPFS used is an external system. Using an external system reduces the load on the blockchain facilitating faster transactions. Thus, further enhancing the efficiency and response time of the system.

A. Connecting Wallet

The Wallet Connect feature is a critical component of the NFT Application as it enables users to securely connect their cryptocurrency wallets to the Application without exposing their private keys. This is achieved through the use of Metamask, a popular browser extension that acts as a bridge between the user's browser and their cryptocurrency wallet. When a user accesses the NFT Application, they are prompted to connect their wallet through Metamask. Once connected, the user can interact with the dApp's features, such as minting NFTs, without having to manually input their private keys. This eliminates the risk of key theft or unauthorized access to the user's digital assets. To enable secure and user-friendly interaction with the NFT dApp, we utilized React.js with Ether.js, a popular library for interacting with Ethereum-based networks. This library allowed us to connect the dApp with users' cryptocurrency wallets through the Metamask browser extension.

B. NFT Minting

NFT minting feature enables users to create and sell unique digital assets on the blockchain. To implement this feature, we utilized a combination of the IPFS, and the Ethereum blockchain. To mint an NFT, the user selects an image. Once the image is selected, the user clicks the" List NFT" button, which initiates the minting process. A JSON object is created containing the NFT's name, description, price, and the image URL generated when an image is chosen. This JSON file is then pinned to IPFS using the Pinata API's, which returns an IPFS hash in the form of CID that serves as the metadata URI for the NFT.

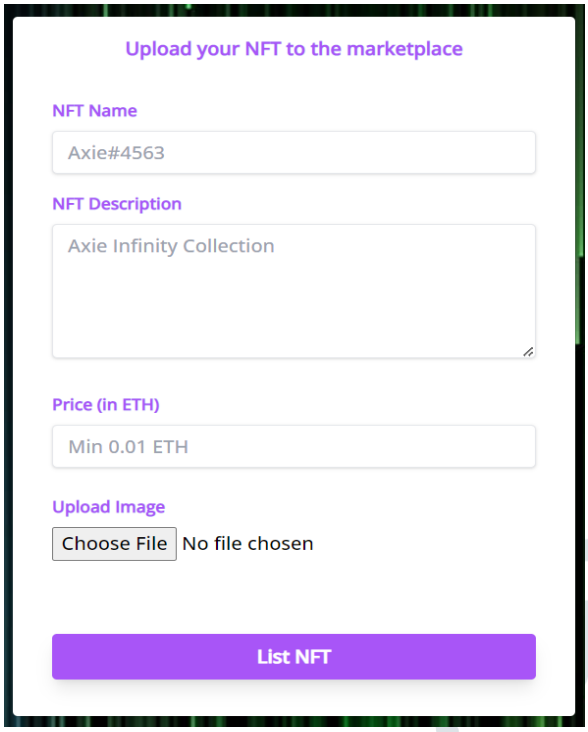

Fig. 2. NFT Description Page

The mint function in the smart contract is then called, which creates a new token on the Ethereum blockchain and sets its URI to the IPFS hash returned by the Pinata API. The smart contract also specifies the characteristics of the token, such as its tokenID, no. of transfers and the total number of tokens in existence. Once the function is executed, the NFT is minted and can be viewed in the Marketplace. The metadata stored on IPFS allows anyone to view the NFT's media such as name, description, price, and image. The token ID on the blockchain ensures that the NFT is unique and can be transferred between users. Additionally, the use of a smart contract on the Ethereum blockchain enables users to securely and transparently transfer ownership of their NFTs, as ownership information is stored on the blockchain.

C. Collection

The Collection functionality of this application enables users to browse and purchase NFTs created by other users. The feature is built on the Ethereum blockchain, utilizing the Sepolia testnet, and allows users to interact with the smart contract that handles the creation, storage, and transfer of NFTs. The marketplace displays all available NFTs stored on the contract, allowing users to browse through them and view their associated metadata such as name, description, and price. The media is stored on IPFS, ensuring decentralization and tamper-proofing. To purchase an NFT, a user clicks on the" Buy" button associated with the desired NFT, triggering a call to the smart contract's transfer function. The function transfers ownership of the NFT to the user and updates the smart contract's storage to reflect the new ownership. The transaction is then recorded on the blockchain, providing an immutable record of the transfer.

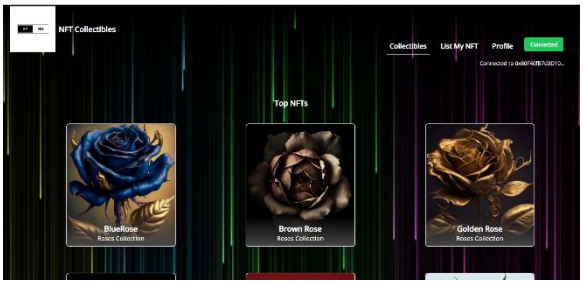

Fig. 3. NFT Collectibles Page

The Application is designed with a user-friendly interface that includes clear instructions and intuitive buttons for purchasing, changing price and selling NFTs. The use of blockchain technology and IPFS ensures the security and integrity of the NFT transactions and metadata, providing a seamless user experience.

D. Profile

The Profile page is a key component of the NFT Marketplace dApp, providing users with an overview of their account's NFT ownership and value. The Ethereum blockchain's smart contract capabilities are integrated into the dApp's interface to implement this feature. When a user accesses their Profile page, the dApp retrieves data that relates to the user's account. This data includes the user's wallet address, the total number of NFTs owned, and the total value of the NFTs in the user's possession. The dApp displays this information in a user-friendly format on the UserProfile page. This page also displays all

Fig. 4. Profile Page

the NFTs owned by the user. The dApp queries the Ethereum blockchain's smart contract to retrieve the list of NFTs owned and fetches the NFT metadata from IPFS using the metadata URI associated with each NFT token ID. The information is displayed in a visually appealing and

easy-to-navigate format. The integration of smart contracts into the UserProfile page enables users to securely and transparently view their NFT ownership and value on the blockchain.

4. Results and analysis

The section presents in detail the results of implementing essential features. The aim of the project was to develop a NFT System with Data Integrity, Transparency, Security, Excellent Performance and Useability. Data integrity involved the study of the possibility of Data Mutation, Modification but also to the completeness, timeliness, and accuracy of the data over its entire lifetime. Data Transparency is making data easily accessible and understandable. The important functionality was to make the verifying part of the chain of ownership.

A. Transparency

Transparency is an important functional that was in focus. We successfully implemented the mechanism for the user to view an NFT on the Blockchain. A user at any point of time can view the NFT on the Blockchain. All he has to do is click on the "VIEW ON BLOCKCHAIN".

Fig. 5. NFT Page

The figure 5 shows an NFT page with the necessary NFT details. The user can verify the transfer details by clicking on the VIEW ON BLOCKCHAIN. Once the VIEW ON BLOCKCHAIN is clicked the user is redirected to the NFT details on the Blockchain. This is on the Sepolia Etherscan.

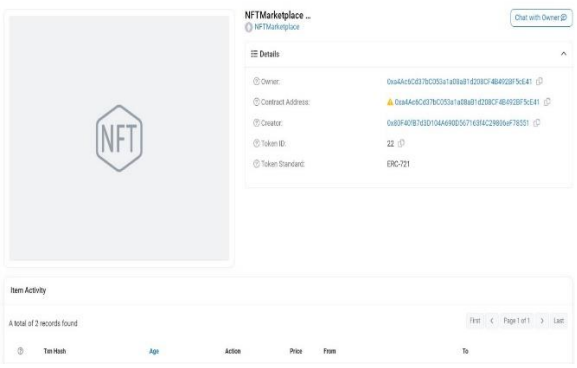

Fig. 6. NFT Description Page

The Figure 6 shows the NFT on the Blockchain. It has important details such as Owner address, Contract Address, Creator address, Token ID and the token standard. The Contract Address is the Address of the Contract through which the user minted the NFT.

B. Performance

The performance of the system in terms of UI interface, the Blockchain, minting the NFT, Transfer of NFT and Changing the price of NFT were robust and faster than average page load time. Our system has average loading time of around 900 milli seconds. The performance of the Sepolia Blockchain was monitored in Alchemy.

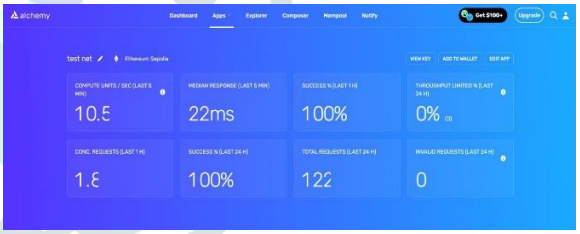

Fig. 7. Blockchain performance

The response time of the testnet averaged around 22ms which is fast for a blockchain. This was achieved by reducing the load on the Blockchain by introducing an IFPS to store the NFT media. The blockchain Successful completion of the requests was 100%. No request was ever failed. The Blockchain performed well. The overall performance of the system was effected by various components such as the pinning of the pinata file, minting of the NFT, transfer of NFT, Changing price of the NFT. Overall average time of the actions can be an average of five seconds which is individually displayed in the further graphs.

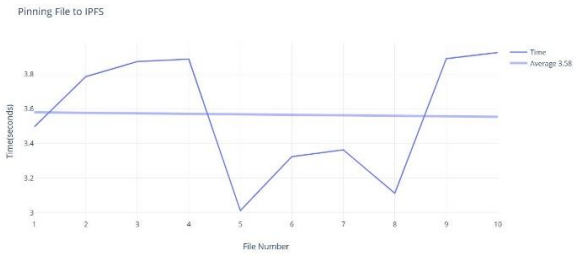

Fig. 8. Pinning performance

The figure 8 shows the time taken to pin the json and image to the IPFS. The time varied from three to four seconds. The average time taken was around 3.58 second. This speed can be increased further by upgrading to faster network.

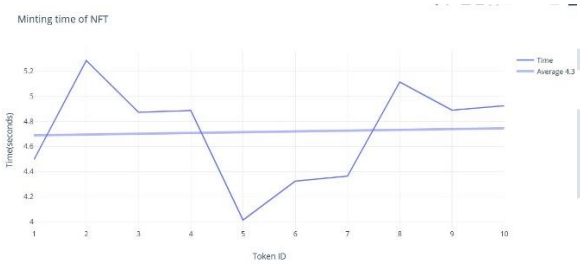

Fig. 9. Minting performance

The figure 9 shows the time taken to mint NFT. Time taken to print 10 NFT were recorded individually and graphed. The maximum time taken to mint an NFT was 5.3 seconds. The average time taken was 4.3 seconds. This time is considerably fast. The speed of minting an NFT can further be increased by deploying the Contract on the Mainnet. The Sepolia network is a testnet so slow response times are expected.

Fig. 10. Transfer performance

The figure 10 is a graph containing the time taken to transfer the NFT to the buyers account when an NFT is bought. The time taken by 10 transfers were recorded individually and graphed. The average time taken was 8.5 seconds. This is reasonably good time for a transfer on Sepolia Testnet.

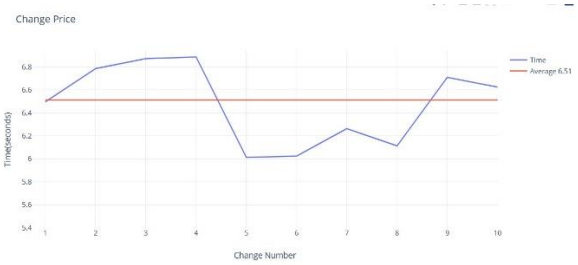

Fig. 11. Change Price Performance

The figure 11 is a graph containing the time taken to change the price of the NFT owned by the user. The time taken to change the price of the NFT were recorded individually by and graphed. The maximum time taken to change the price was 6.8 seconds. The average time was around 6.51 seconds. The change in price was recorded both on the IPFS and the Blockchain which led to increase in the time. The response of the Smart Contract was quick than the IPFS.

C. Useability

The useability study was conducted by consider the opinions of 10 users. Each of these users were asked to rate their opinion on a scale of 0 to 5 concerning minting an NFT, their Profile, Changing the price of NFT owned by them, Buying an NFT and overall experience.

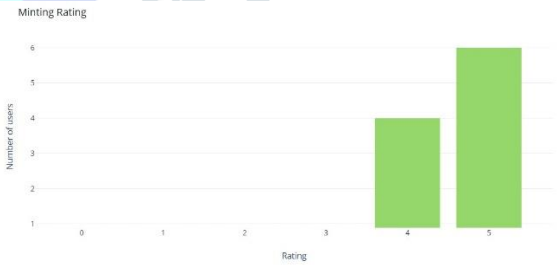

Fig. 12. Minting Experience

Out of 10 users 6 of the users rated the Minting of NFT 5 while remaining 4 users rated it 4. User who rated were satisfied with the existing method while the user who rated 4 requested for a feature to generate a image along with the capability to upload a image.

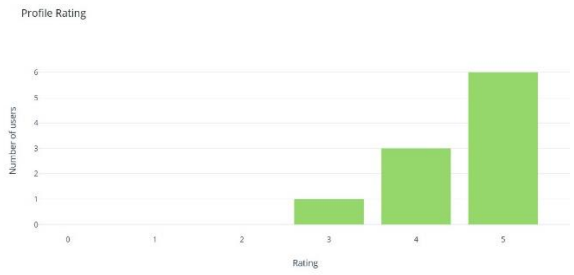

Fig. 13. Profile Experience

Out of 10 users 6 of the users rated the Profile experience 5 while 3 users rated it 4 and one user rated it 3. 6 users were satisfied with the existing system while the remaining users were Not satisfied as they needed the NFT to be sorted based on the description.

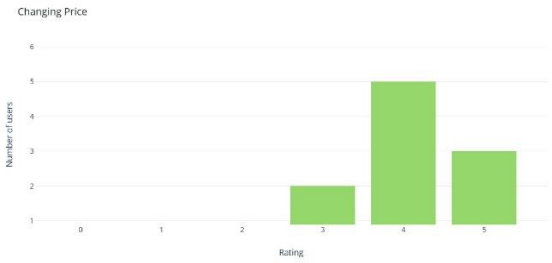

Fig. 14. Changing Price Experience

Out of 10 users 3 of the users rated the Minting of NFT 5 while 5 users rated it 4 and remaining 2 users rated it 3. User who rated were satisfied with the existing method while the user who rated 4 requested and 3 found the changing price to be slow. Some the users wanted a search mechanism to compare the prices of similar NFTs so they can decide the price of their NFT.

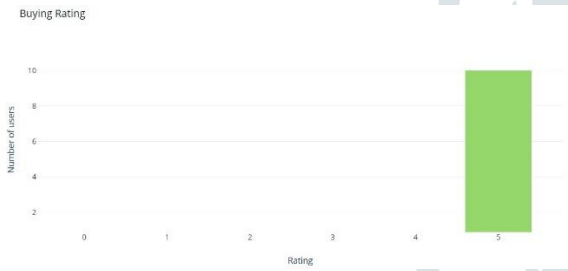

Fig. 15. Buying Experience

Out of 10 users all of the users rated the Buying of an NFT 5. They found Buying the NFT the easiest thing as it was just a button click and confirm. Most of them were surprised that buying an NFT was so easy. So all of the users were satisfied with the existing system of buying an NFT.

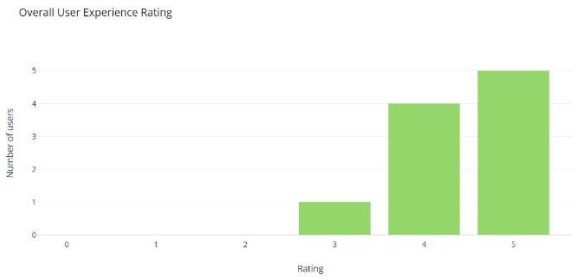

Fig. 16. Overall Experience

Among 10 users 5 user rated the overall experience as 5 stars and 4 users rated the overall experience as 4 stars. Remaining 1 user rated it as 3. Most of users were satisfied with the overall experience while some of them requested additional features while would help them browse through the marketplace and make finding an NFT to purchase easier. Some users wanted to sort their profile based on the NFT description and also a search function. Overall rating of the application is 4.4 out of 5 stars.

5. Conclusion

Our system will contribute to more transparency in the collectibles market. The collectibles industry is massive, and fraud is rampant. The advantages of generating an NFT for a physical collectible are as follows:

- The NFT is the certificate of authenticity and can be used to verify the authenticity of the collectible
- The NFT cannot be tampered with as there are several copies stored in the blockchain network thus immutable.
- Hard copies of certificates of authenticity can be lost or damaged but this cannot happen in NFT as they will always be stored in the ETH wallet.

Future Enhancements One of the areas which we would like to explore would be smart NFTs. In smart contracts, we will be able to create an NFT for digital items which have gained value or experience. A very good field where smart NFTs can be applied is gaming. A good example would be a professional e-sports gamer who would be able to sell the skin he used in a tournament in the form of an NFT just the way footballs used in tournaments are sold for a higher amount of money.

6. References

[1] B. Ammar, M. Mohammad, I. Yaqoob, S. Khaled, H. R. Hasan, and R. Jayaraman, "Blockchain and NFTs for Trusted Ownership, Trading, and Access of AI Models," IEEE Access, vol. 10, pp. 112233-112234, Oct 2022.

[2] C. Dan, E. Joshua, and A. George, "A framework for creating deployable smart contracts for non-fungible tokens on the Ethereum blockchain," IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), pp. 100-102, July 2020.

[3] N. P. Imperius, and A. D. Alahmar, "Systematic Mapping of Testing Smart Contracts for Blockchain

Applications," IEEE Access, vol. 10, pp. 112845-112847, Nov 2022.

[4] Lennart Ante, "Non-fungible token (NFT) markets and its relationship with Bitcoin and Ethereum," BRL Working Paper Series, No.20, pp. 1-6, Jun 2021.

[5] D. Dipanjan, B. Priyanka, R. Nicola, K. Christopher, V. Giovanni, "Understanding Security Issues in the NFT Ecosystem," ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 668-670, Nov 2022.

[6] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," Tech Report on NFT (cs.CR), vol. 3, Oct 2021.

[7] S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, "Patents and intellectual property assets as non-fungible tokens; key technologies and challenges," IEEE Access, vol. 12, no. 1, pp. 1-13, Dec 2022.

[8] M. Umer, L. U. Khan, S. S. Hassan, Z. Han, and C. S. Hong, "FL-Incentivizer: FL-NFT for Federated Learning Model Trading and Training," IEEE Access, vol. 11, pp. 4383- 4384, Dec 2022.

[9] M. Madine, S. Khaled, R. Jayaraman, B. Ammar, H. Hasan, and I. Yaqoob, "Blockchain and NFTs for Time-Bound Access and Monetization of Private Data," IEEE Access, vol. 10, pp. 94188-94191, Aug 2022.

[10] K. Hyoungsung, K. Hyun-sik, and P. Yong-suk, "Perpetual Contract NFT as Collateral for DeFi Composability," IEEE Access, vol. 10, pp. 126802-126807, Nov 2022.

[11] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," Telematics Inform, vol. 35, no. 8, pp. 2337-2354, July 2018.

[12] N. Sanchez-Gomez, J. Torres-Valderrama, J. A. Garcia-Garcia, J. J. Gutierrez, and M. J. Escalona, "Model-based software design and testing in blockchain smart contracts: A systematic literature review," IEEE Access, vol. 8, pp. 164556-164569, Sept 2020.

[13] B. Hu, Z. Zhang, J. Liu, Y. Liu, J. Yin, R. Lu, and X. Lin, "A comprehensive survey on smart contract construction and execution: Paradigms, tools, and systems," *Patterns*, vol. 2, no. 2, Feb 2021.

[14] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," J. Netw. Comput. Appl., vol. 182, Art. no. 103035, May 2021.

[15] M. Jurgelaitis, L. Ceponiene, R. Butkiene, "Solidity Code Generation from UML State Machines in Model-Driven Smart Contract Development," IEEE Access, vol. 10, pp. 33465-33473, Feb 2022.

[16] C. Chen, L. Zhang, Y. Li, T. Liao, S. Zhao, Z. Zheng, H. Huang, and J. Wu, "When Digital Economy Meets Web3.0: Applications and Challenges," IEEE Open Journal of the Computer Society, vol. 3, pp. 234-242, Nov 2022.

[17] Web3: https://ethereum.org/en/web3/.

[18] https://www.alchemy.com/company.