International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

Challenges of Implementing an NFT Marketplace

Yash Mhatre[1], Devansh Dixit[2], Ritesh Salunkhe[3], Dr. Sanjay Sharma[4]

[1],[2],[3] Student, [4] Professor Department of Computer Engineering, New Horizon Institute of Technology and Management, Mumbai

---

Abstract - *Blockchain is a revolutionary technology and will have great positive effects in our business environment in the near future. NFT stands for Non-Fungible Token. An NFT can be considered just a digital form of real-world objects like art, music, in-game items and videos. They are traded online, generally with different types of cryptocurrency. Non-fungible tokens traded on an NFT marketplace are different from fungible tokens that are bought or sold on multiple centralized or decentralized exchanges. NFTs are different. Each NFT has a digital signature that makes it impossible for them to be exchanged for another NFT. Each has its own value determined by various factors like metadata, creator, features, etc. The majority of NFTs in the present times are digital, and creators could improvise here in the future and make way for more creative things for the users.. It is very clear that blockchain technology and NFTs can offer the perfect opportunity for artists and content creators to obtain financial remuneration for their works. In this way, artists don't have to depend on galleries to sell their artwork. Instead, an artist could just sell their work to a buyer in the form of an NFT. This also results in better profit for the artists. Interestingly, Non Fungible Tokens also have the feature of royalties where a certain amount is credited to the original creator of a particular NFT every time the said NFT is sold. Since Blockchain is a relatively newer technology, resources are less and quite difficult to find the perfect one which makes it even more difficult to build a complex NFT Marketplace. NFTs have various use-cases and the NFT marketplace is supposed to be at the core of all those great use cases by providing the users a platform to mint and trade the Non-Fungible tokens.*

Key Words: Blockchain, Non-Fungible Token, Smart Contract, ERC Standards.

1. INTRODUCTION

Non-Fungible Tokens are a non-interchangeable data unit stored on the blockchain with the help of smart contracts. Although, this wasn't the first use-case for the blockchain technology. Initially, blockchain was only used for financial and trading transactions, but now several studies have shown that blockchain technology can have far bigger applications. This is due to the fact that blockchain technology has a high level of transparency. For example,the total amount of currencies and the volume of transactions in the world can be tracked swiftly and clearly. Because it is a peer-to-peer system, no central authority is required to approve or execute operations. NFT tokens have such characteristics and hold values that they cannot be modified. It does not have the same properties as fungible tokens. NFT could be anything online, such as art, gaming, or music. Each bears a digital signature that prohibits NFTs from being substituted for or compared to one another (hence, non-fungible). Non-fungible tokens are virtual tokens that reflect possession of something inherently unique and rare, such as artwork, a music, a collection, an in-game item, or real estate property, whether it is a digital or physical asset. NFT marketplaces are platforms for storing, presenting, trading, and issuing NFTs . Artists can sell their NFT artworks via dedicated marketplaces. Potential buyers can look up through the NFT Marketplace for the NFTs they desire and can easily place a bid on them or buy them.

2 TECHNICAL TERMS

2.1 Non Fungible Token (NFT)

A non-fungible token is a non-interchangeable unit of data stored on a blockchain, a form of database, that can be sold and traded with the help of smart contracts. Different types of NFT data units can be used to connect digital media such as pictures, videos, and music. Non-fungible tokens can be used to digitally represent any item, such as online-only assets like digital artwork as well as real-world assets like real estate.

2.2 Smart Contracts

Smart contracts are programs stored on a blockchain that run when their functions are called through some middleware libraries. They're typically used to automate the execution of a contract so that all parties can know the outcome straight quickly, without any need for intermediaries or wastage of time. They can also regulate a workflow, initiating the next action when certain circumstances are satisfied. They are used to interact with the blockchain for creating, storing, buying or selling tokens and much more. A token contract's basic functionality includes maintaining track of token holdings, transferring ownership of tokens based on changes in the book of token holdings in the particular token contract, and emitting events to record ownership transfers in the logs. Safe transfer is a technique that allows tokens to be removed (withdrawn) from an address after approval,

rather than being pushed (transferred) to an address where they might be lost if the address isn't ready to receive tokens. [1]

2.3 Token Standards

To be compliant with the common standards, a smart contract must adhere to a token standard, which is an interface and a set of rules. Token standards typically outline how tokens can be exchanged and how to maintain track of those transfers in a uniform manner. Token interfaces are used by programmes like wallets to recognise and engage with tokens.

1) ERC-721 Non-Fungible Token Standard concerns tokens where each token is distinct (aka non-fungible) and thus enables the tracking of distinguishable assets. Each asset's possession must be managed separately and atomically.

2) ERC-1155 Multi Token Standard allows for the management of any combination of fungible and non-fungible tokens in a single contract, including transferring multiple token types at once. Compliant tokens must implement six necessary functions and four events according to this standard.

2.4 IPFS

The InterPlanetary File System (IPFS) is a peer-to-peer network and distributed file system protocol for storing and distributing data in a decentralized way.

2.5 Layer 2 Solutions

Layer 2 refers to technologies that assist scale an application by processing transactions outside of the Ethereum Mainnet (layer 1) while preserving the same security and decentralization as the mainnet. Layer 2 solutions boost transaction throughput while lowering gas costs.

3. FEATURES

NFT Marketplace is an online platform where NFTs can be created as well as traded amongst the users. Non-Fungible Tokens cannot be auctioned off themselves. There is a need for NFT Marketplaces to cater to this demand of buying and selling NFTs alongside other features like creating or searching for them.

3.2 Auctions - Buying, Selling, Bidding

NFT Marketplaces feature a frontend called the Storefront, which is where all of the items are presented. They are divided into many categories and listed on the platform. The owner of NFTs has the ability to list them on marketplaces, while all other users can buy or bid on them.

All the transactions are saved onto the blockchain instead of a traditional database.

3.3 Creating NFTs

Creation of NFTs is the most important feature in the whole Non-Fungible token ecosystem. If an individual needs to create some NFT, they might need to code the smart contract, deploy it on the mainnet of some Blockchain network all by themselves, incurring a huge loss because of the fees. NFT Marketplaces allow everyone to create the tokens on their platform without having the need to code anything. Deployment cost for the task is negligible as well on such platforms.

3.4 Wallet Connect

Individuals need crypto wallets to perform any transaction on the marketplace. Different kinds of wallets can be connected to the marketplace giving more choice to the user.

3.5 Searching & Filters

When developing an NFT Marketplace, the feature to be able to search for any NFTs available on the platform becomes very important as it serves the primary purpose of giving the NFTs a greater reach to the audience and more choices to the individuals looking for unique and creative Non-Fungible tokens.

4. CHALLENGES

In this following section, we discuss a series of challenges we faced while trying to implement the NFT marketplace. We came across these challenges while trying to choose a proper tech stack or while actually implementing the marketplace.

4.1 ERC 721 Limitations

ERC721 is a standard for expressing possession of non-fungible tokens, or tokens that are not interchangeable. The ERC-721 establishes a standard for NFT, indicating that this type of token is distinct from others in the same Smart Contract and may have a different value., for example, due to its age, rarity, or even its aesthetic. While all NFTs have an uint256 variable named tokenId, the pair contract address, uint256 tokenId, must be globally unique for any ERC-721 Contract. It has features such as transferring tokens from one account to another, obtaining an user's current token balance, obtaining the owner of a certain token, and obtaining the entire supply of a token available on the network. And it has some additional features, such as approving the transfer of a certain quantity of token from one account to a third-party account. An ERC-721 Non-Fungible Token Contract is a Smart Contract that implements the following techniques

and events and is responsible for keeping track of the produced tokens on Blockchain once deployed. In order to create an ERC-721 token, the contract must be compliant with both the ERC-165 and ERC-721 interfaces. a) Unable to create multiple copies: When developing an NFT Marketplace, there might be a requirement to allow the user creating the token to be able to specify the number of copies for the token. Leading marketplaces currently have this feature. This is not possible when implementing a smart contract with ERC 721 standard. b) No functionality to retrieve tokenIds: TokendIds are important in a smart contract for a marketplace as they are the primary requirement for initiating any kind of transactions involving the Non-Fungible tokens. There is no functionality to get tokenIds directly from the smart contract. The only way to get the tokenId is to save a reference to it. c) Inadequate transfer functionality: ERC 721 can only send one token at a time. This results in slower transactions and very high gas fees to the end user.

4.2 ERC 1155 Drawbacks

ERC-1155 is a one-of-a-kind token that can be used to generate both fungible and non-fungible (NFTs) tokens. In batch token transfers, it's much faster and more gas efficient than single transfers. ERC-1155 allows various types of tokens and NFTs to be created within a single contract itself. ERC-1155 can use a single contract to make various types of NFTs. Gas fees are cut by 90%, making it an affordable way for anyone to start minting on blockchain.The only major disadvantage is that the NFT is more difficult to trace in terms of ownership—in order to save data on the blockchain, ERC-1155 requires specifications based on Ethereum logs that are less reliable. Token standards such as ERC-20 and ERC-721 necessitate the deployment of a different contract for each token type or collection. Because each token contract is separated into its own permissioned address, this creates a lot of redundant bytecode on the Ethereum blockchain and inhibits some functionalities. a) Limited Resources: ERC 1155 is a relatively newer ERC standard and does not have the kind of support that ERC 721 enjoys from the blockchain community. To develop any smart contract using ERC 1155, one might need to extensively search through the internet. b) Semi-Fungible Characteristic: Since the token standard allows to operate multiple kinds of tokens, there is a mandatory requirement to input totalSupply for each token that is to be minted. When we create a NFT and input more than 1 as the value for totalSupply, it creates a Semi-fungible token which defeats the purpose of the whole Non-Fungible token ecosystem.

4.3 High Gas Fees

Rising gas prices have become a serious issue for NFT exchanges, particularly when minting NFTs on a large scale, which necessitates uploading metadata to the blockchain system. Because smart contracts require computational resources and storage to be processed, every NFT-related operation is more expensive than a basic transfer transactionWhile implementing a marketplace to place transactions on the blockchain, gas fees play an important role taking into consideration the user experience. If gas fees are not affordable enough, the user might skip the platform altogether. Blockchain networks such as Ethereum have very high fees for each transaction. This results in a huge loss to the end user when they are making transactions on the platform. Layer 2 blockchain networks are a great solution to avoid higher gas fees.

4.4 Network Limitations

Before building an NFT Marketplace or any Decentralized Application (DApp), a blockchain network must be selected for on-chain transactions. There are numerous blockchain networks available to choose from. Each with its own unique features. There are different criterias on which selection of the blockchain network should depend upon.

1) Transaction Fee:

As discussed above, transaction fees play a major role in selecting a specific blockchain network according to the application's needs. Many popular blockchain networks like Bitcoin or Ethereum have very high fees for every transaction. Layer 2 solutions are being built on top of these Layer 1 networks to solve the problem of transaction fees.

2) Transaction Throughput (per second):

The number of transactions executed in a particular amount of time is referred to as throughput. Transaction throughput is a term used in the blockchain world to describe the rate at which a blockchain processes transactions. It is generally stated in transactions per second (TPS). Having a lower TPS would imply that the network takes longer to confirm transactions. This would result in a bad experience for the end user.

3) Transaction Speed

Transaction speed refers to how quickly a single transaction is completed. There is also another concept called Block Time, which refers to the time in which a block will get appended to the blockchain.

4) Consensus Protocol

A consensus algorithm is a computer science procedure that allows remote processes or systems to agree on a single data value. Consensus methods are used in networks to achieve reliability where faulty nodes might also be present. Following are the distributed consensus algorithms that are often used including Proof-ofStake

(PoS), Proof-of-Work (PoW), proof-of-importance, Delegate Proof-of-Stake (DPoS), proof-of-burn, proof-of activity, proof-of-deposit. [2]

i. POW Based Blockchains: Blockchain working on top of Proof of Work consensus protocols have a limit on block size and require a certain amount of time to construct a block. Furthermore, each transaction must wait for a large number of block confirmations.

ii. POW Based Blockchains:

Blockchain networks using Proof of Stake as the consensus protocol use a staking methodology to get around these limitations, which allows them to reach high throughput but reduces decentralization.

Table - 1: Comparison of Blockchain Networks and Performance Characteristics

Blockchain Networks	Transaction Fee ($)	Transaction Throughput (tps)	Transaction Time
Ethereum [7]	5-100	15-30	2-5 mins
Solana [8]	0.00025	50000-60000	2.5 sec
Cardano [9]	0.5-1	250- 1000	3-5 mins
Ripple [10]	-0.1	1500	4-6 sec
Stellar [11]	0.5-0.1	1000	2-5 sec

4.5 Smart Contract Risks

A smart contract is designed to ensure that all the parties involved in the transaction perform their necessary duty with certainty. The Blockchain concept aims to remove third-party intermediaries for transactions. It aims to make business and trading between anonymous and identified participants easier. A smart contract reduces the complexity and costs of traditional procedures while maintaining their validity and legitimacy. [3] Some advantages of smart contracts are security, transparency, accuracy, speed and efficiency. These contracts are software-based and can be accessed via the internet. They are able to conduct transactions quickly as a result of this. As a result, they are able to complete transactions fast. Many traditional corporate processes can be cut in half with this speed. Automated contracts use the highest level of data protection presently accessible, the same as modern crypto-currencies. Smart contracts are very secure if they are coded accordingly. Smart contracts have the ability to encode complex corporate, financial, and legal agreements on the blockchain network, posing the risk of one-to-one mapping of these agreements from the physical to the digital medium. Smart contract faults may also result in costly errors and the possible loss of users' assets. There have also been numerous recent incidents of hacker attacks draining customers' accounts by exploiting faults in smart contract coding. Smart contract risks can be classified into three categories: of a sentence.

a) Operational Risks: Such risks occur when some authorization features are exploited when the blockchain network's governance is flawed or insufficient. Operational risks can be of various types involving different kinds of functions.

The smart contract has functions that allow a privileged role to change the asset's functionality unilaterally and indiscriminately. There are many applications like staking, farming where it might be required that a user's funds be managed completely by the smart contract. And if there is even a little bug in the smart contract code, it might lead to severe complications and can also result in the user losing all of their funds.

b) Implementation Risks: Implementation risks are those where intrinsic errors result in unintended behavior from the smart contract. They can include risks like rolling one's own logic for smart contracts. These can be risky because they are not yet tested and a first. Incorrect implementation of signatures or unauthorized transfer of assets are also included in implementation risks.

c) Design Risks: Design risks occur when accepted system characteristics are exploited to change desired smart contract behavior, posing a design vulnerability. Through mempool transaction reordering, the smart contract enables for asynchronous processing transactions, which may be used for profiteering or protocol accuracy. To ensure proper security and completeness of the smart contract code, it should always be audited by a third party auditor before pushing it for production use.

5. CONCLUSION

In this work, we discussed most of the challenges faced while implementing an NFT Marketplace. Since NFT Marketplace is built upon a blockchain network, it is bound to face the challenges of that particular blockchain network. It should also be noted that even though there are some challenges, they can be overcome by proper implementation and a good system architecture for the overall application. Many of the challenges discussed above can be solved using a Layer 2 solution for the marketplace. They are very fast and gas efficient which would result in a good user experience. Choosing the right ERC standard is the first and most crucial step for implementing a marketplace and can vary application to application. With this work, it will help to choose a proper

approach for implementing an NFT Marketplace and also consider what points to keep in mind while executing it.

6. ACKNOWLEDGEMENT

We owe a sincere thanks to our New Horizon Institute of Technology and Management, especially our Head of Department and our guide, Dr. Sanjay Sharma for their kind cooperation and guidance which helped us in the completion of this project which would have seemed difficult without their motivation, constant support and valuable suggestions. Moreover, the completion of this research would have been impossible without the cooperation, suggestions and help of our family and friends.

REFERENCES

[1] M. di Angelo and G. Salzer, "Tokens, Types, and Standards: Identification and Utilization in Ethereum," 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2020, pp. 1-10, doi: 10.1109/DAPPS49028.2020.00001.

[2] H. R. Andrian, N. B. Kurniawan and Suhardi, "Blockchain Technology and Implementation : A Systematic Literature Review," 2018 International Conference on Information Technology Systems and Innovation (ICITSI), 2018, pp. 370-374, doi: 10.1109/ICITSI.2018.8695939.

[3] Thomas Kitsantas, Athanasios Vazakidis and Evangelos Chytis. "A Review of Blockchain Technology and Its Applications in the Business Environment". International Conference on Enterprise, Systems, Accounting, Logistics & ManagementAt: Chania, Crete, Greece, July 2019.

[4] Lennart Ante, "The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum". Blockchain Research Labs, BRL Working Paper Series No. 20, June 06, 2021.

[5] Ferdinand Regner, André Schweizer, Nils Urbach. "NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application" , ResearchGate, December 2019.

[6] Ethereum Introduction. Available online: http://ethdocs.org/en/latest/introduction/index.html (accessed on 31 October 2018).

[7] Neo White Paper. Available online: https://solana.com/solana-whitepaper.pdf

[8] Russell, K.A.; David, B.; Oliynykov, R. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In Proceedings of the Advances in Cryptology—CRYPTO 2017, Santa Barbara, CA, USA, 20–24 August 2017; pp. 357–388.

[9] David, S.; Noah, Y.; Arthur, B. The Ripple Protocol Consensus Algorithm, Ripple Labs Inc., 2014. Available online:https://ripple.com/files/ripple_consensus_whitepaper.pdf (accessed on 31 October 2018)

[10] Mazieres, D. The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus. 2016. https://www.stellar.org/papers/stellar-consensus-protocol.pdf