KLE Society's
KLE Technological University, Hubballi.

A Minor Project Report

on

NFT-Based Decentralized Autonomous Organization for Digital Art

submitted in partial fulfillment of the requirement for the degree of

Bachelor of Engineering

in

Computer Science and Engineering

Submitted by

Priya A Jadekar	01FE20BCS078
Vivek P M	01FE20BCS084
N Soumya	01FE20BCS092
Preeti Goure	01FE20BCS114

Under the guidance of
Dr. Narayan D G

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Hubballi – 580 031

2022 -23

KLE Society's
KLE Technological University, Hubballi.

2022 - 2023

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that Minor Project titled NFT-Based Decentralized Autonomous Organization for Digital Art is a bonafide work carried out by the student team comprising of Priya A Jadekar (01fe20bcs078), Vivek P M(01fe20bcs084), N Soumya(01fe20bcs092), Preeti Goure(01fe20bs114) for partial fulfillment of completion of sixth semester B.E. in Computer Science and Engineering during the academic year 2022-23.

Guide — Head, SoCSE

Dr. Narayan D G — Dr. Meena S. M

Viva -Voce:

Name of the Examiners	Signature with date
1.	
2.	

Acknowledgement

We would like to thank our faculty and management for their professional guidance towards the completion of the project work. We take this opportunity to thank Dr. Ashok Shettar, Vice-Chancellor, Dr. B.S Anami, Registrar, and Dr. P.G Tewari, Dean Academics, KLE Technological University, Hubballi, for their vision and support.

We also take this opportunity to thank Dr. Meena S. M, Professor and Head, SoCSE for having provided us direction and facilitated for enhancement of skills and academic growth.

We thank our guide Dr. Narayan D G, Professor, SoCSE for the constant guidance during interaction and reviews.

We also thank our senior Mr. Naveen Kumar for helping us overcome the difficulties in the course of the project.

We extend our acknowledgment to the reviewers for critical suggestions and inputs. We also thank Project Co-ordinator Mr. Uday N.Kulkarni and Mr. Guruprasad Konnuramath for their support during the course of completion.

We express gratitude to our beloved parents for their constant encouragement and support.

Priya A Jadekar - 01fe20bcs078
Vivek P M - 01fe20bcs084
N Soumya - 01fe20bcs092
Preeti Goure - 01fe20bcs114

ABSTRACT

Blockchain is an emerging technology that combines several technologies to provide tamper-proof record of transactions. Recently, blockchain has found many applications in industry due to its unique characteristics such as decentralized and open ledger, traceability and immutability. Two such applications which have been extensively used are NFT marketplace and DAO (Decentralized Autonomous Organizations). Non-Fungible Tokens(NFTs) are digital assets that can come in any form like digital art, music, videos, and many more purchased by cryptocurrency. They are a secure and faster way of buying and selling assets. DAO are a legal form of organization with no central authority to make the decisions fair and transparent. In this work, we develop a NFT marketplace and integrate it with DAO. DAO decision weights are computed based on number of NFTs available with each account holder. We use Ethereum ERC-721 tokens to implement NFT and DAO. However, Ethereum 2.0 uses POS based consensus algorithm which suffers from fairness. To address this, we design Delegated Reputation based Proof of Elapsed Time (DRPoET) consensus algorithm. We evaluate the NFT integrated DAO and consensus algorithm in Ethereum based testbed. The DAO results obtained show that the weights of the individual contributor in the organization is not skewed and is fair for all in the organization compared to default algorithm. The results of DRPoET show that it performs better than POS in terms of transaction latency and fairness.

Keywords : *NFT, DAO, cryptocurrency, crypto, consensus algorithm*

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

Blockchain technology has ushered in a new era of innovation, revolutionizing various sectors and empowering individuals in unprecedented ways. Among its groundbreaking applications, two key concepts have emerged as major disruptors: NFTs (Non-Fungible Tokens), and DAOs (Decentralized Autonomous Organizations). Blockchain, as a decentralized and immutable ledger, ensures transparency, security, and trust in digital transactions. NFTs, built on blockchain, have revolutionized ownership and provenance in the digital realm, enabling the creation, trading, and authentication of unique digital assets. DAOs, on the other hand, leverage blockchain's decentralized architecture to create self-governing and community-driven organizations, eliminating traditional hierarchical structures. Together, blockchain, NFTs, and DAOs have opened up endless possibilities, transforming industries such as art, gaming, finance, and governance, and empowering individuals to take control of their digital assets and participate in decision-making processes like never before.

Non-Fungible Tokens (NFTs) are digital assets that can come in the form of digital art, music, videos, and more. They are bought online by means of cryptocurrency. They are driven by smart contracts which in turn are deployed on blockchain networks. NFTs are a secure and faster way of buying and managing assets. They can be tracked and transferred to buyers easily.

A Decentralized Autonomous Organization (DAO) is an emerging form of legal structure with no central authority. The members of the organization share a common motive and take part in all the decisions regarding the organization. The members of the DAO are the ones that hold a certain percentage of stakes in the organization.

The Consensus Algorithm is the core technology of any blockchain system. This decides the efficiency of the blockchain system. The consensus algorithm is for the selection of the miner nodes, who mine the blocks and add them to the blocks after verification. Thus, a fair and secure consensus algorithm is really important for the working of blockchain.

1.1 Motivation

A user wants to conduct an online digital art exhibition for digital artworks. However, the exhibition is online, and the user is worried that the arts will not be secured as others may easily forge or replicate them. So the concept of NFT came into the picture so that the user can buy NFT for all the digital arts as NFTs are trustworthy, easily transferable, and also maintain ownership rights on the artwork. Because there was a single point of failure in the centralized system and multiple decisions had to be taken, we introduce the concept of DAO. Blockchain eliminates the dependency on third parties hence commission over a transaction is reduced. While DAO speeds up decision-making, centralized systems facilitate organizational changes with few people controlling the key features. For a company with an NFT marketplace and DAO for the decision-making in the organization, integrating the NFT marketplace and DAO will facilitate the organization's growth as more and more NFT purchases will be facilitated. The consensus algorithm of the blockchain which holds the websites is to be fairer and more secure, as the data that is stored in the blockchain system is very confidential and useful. The present algorithms like DPoS and PoW are not fair and not secure to malicious attacks. Thus, a new algorithm is needed.

1.2 Literature Survey

The writers Balduf, Leonhard, and others examine problems with digital art storage in the article [1]. On-chain storage, decentralised storage systems, and cloud storage are the three primary methods for storing assets and metadata. There are no guarantees with cloud storage. Pixel art, ASCII art, and generative art are a few examples of digital art that can be stored as assets on-chain. In cases when on-chain storage is impractical, distributed storage systems ought to be taken into account. A hash of the referenced data must be kept on-chain for any off-chain storage solution.

Igor Barinov and others [2] introduced POSDAO, Implemented as a Decentralized autonomous organization (DAO), a Proof of Stake (POS) algorithm. It is made to offer a decentralized, equitable, and resource-conserving agreement for a public blockchain system. The algorithm functions as a collection of Solidity-written smart contracts. A general-purpose BFT consensus mechanism is used to build POSDAO, such as Authority Round (AuRa), which has a probabilistic finality, or Honey Badger BFT (HBBFT), which lacks a leader and has immediate finality. An incentive system that may be adjusted encourages validators to act in the network's best interests. In order to manage a group of validators, distribute rewards, and report and punish bad validators, the algorithm offers a Sybil control mechanism.

Begicheva and the co-authors [3] propose an improvised Proof of Stake Algorithm to make the fair choice of block generation. The algorithm reduces the effectiveness of Nothing at Stake and Stake Bleeding attacks by using the pseudo-random variable from an older block instead of the preceding block. Hence the probability of overtaking the main chain decreases since the attacker will be having a small amount of balance. By this, the number of forks created in blockchain and their length decreases. With the proposed algorithm, the fork will lag the main chain with its height.

Chen [4] and co-authors proposed a new algorithm based on vague set and node impact factors. They initially decide the number of agent nodes based on the predetermined threshold values and compute the ratings of all nodes using fuzzy values. After determining its need, secondary screening is conducted. The nodes' impact factors are determined based on their nearby nodes and combined with adjacency votes to further identify the nodes with identical fuzzy values. The appropriate size of the agent node-set was determined by testing and analysis of dynamic changes in the composition and scale of the agent node-set. The findings collected demonstrate that while the efficacy of the proposed method is enhanced in all types of network architectures, complex network structures exhibit the most pronounced enhancement. But because the network is getting bigger, the computational complexity is increased.

Bhujel and others [5] present the market dynamics of NFT ecosystems and analyses the challenges faced by NFTs and marketplaces in terms of security, transparency, scalability, and their consequences. If the Marketplace is compromised, attackers can find their way into users' crypto wallets from well-known marketplaces and could take large amounts of NFTs creating major issues. Transactional efficiency, storage, and gas fees are the key components of scalability issues. Off-chain storage addresses the storage problem but decreases security and decentralization. Selecting the consensus mechanism for NFT marketplace is a tedious task that includes studying about the node behavior, network latency, their failures and security.

Faqir and the co-authors [6] introduce the concept of DAO and the platforms that offer DAO creation and its management. DAO is the tool that has emerged to enable decentralized organizations to operate on the blockchain. It is a novel sociotechnical system that sets a new way for online coordination and decision-making. It also requires some research attention in the matter of security.

Decentralized Autonomous Organisations (DAO) are anticipated to have a big impact on our society's future decentralized governance. The author of [7] addresses the difficulties and constraints faced by DAOs, including concerns with governance, legislation, and security. DAOs run on a decentralized network and are controlled by transparent, irrevocable, and

enforceable smart contracts. The main characteristics of DAOs are then covered, including their autonomy, decentralized decision-making, and incentive structures. DAOs are used in a variety of fields, including banking, supply chain management, and nonprofit organizations. Increased openness, efficiency, and confidence in decision-making processes are just a few of the possible advantages of DAOs. DAOs include drawbacks and restrictions, including as the possibility for abuse and manipulation, the danger of smart contract flaws, and the infancy of blockchain regulations.

In [8] author has described the NFTs. Non-fungible tokens (NFTs) are digital assets that are unique and cannot be replicated. They have various applications, such as in digital art, gaming, licenses and certifications, fashion, and virtual worlds. NFTs are part of the Ethereum blockchain and have a digital signature of the owner incorporated in each token, which minimizes the problem of authenticity and counterfeits. NFTs can also provide ownership data for in-game objects, fuel in-game economic systems, and provide many other perks to facilitate the players. In addition, NFTs can be used to reduce the time and effort that companies have to expend on verifying critical documentation, thereby improving administrative operations.

Saito and others [9] give an introduction to DAO for the non-profit sector. It is found that DAO can enhance global cooperation between stakeholders. The paper uses SBTs, SoulBound Tokens, a type of NFT to represent commitments, credentials, and affiliations; mainly as membership NFTs. Process discussion and planning, Proposal and vote, Execution, and Peer evaluation of contributors are the processes taken in DAO.

Wang, Shuai, and their colleagues [10] provide a thorough examination of DAO (Decentralized Autonomous Organization). They define the concept of DAO, explore its characteristics, discuss the research framework surrounding it, examine common implementation approaches, identify challenges, and discuss expected future developments. Moreover, they propose a reference model comprising five layers: basic technology, governance, incentive mechanism, organization form, and manifestation layer. By utilizing smart contracts and storing management and operational guidelines on the blockchain, DAO can function autonomously, eliminating the need for centralized control or third-party interference. As a result, DAO disrupts the traditional hierarchical management model.

Li A and others [11] propose a reliable proof-of-stake consensus mechanism that effectively prevents coin age accumulation attacks and Nothing-at-Stake attacks by limiting the maximum value of the coin age and using the number of coins to choose the miners. The node with more coins has a better probability of packing and producing blocks. The most rollbacks that the RPoS system can withstand NaS assaults with effectiveness. However, it is impossible to

establish the precise number of nodes required to guarantee the RPoS system's stability and robustness.

Neal N. Xiong and others [12] design an improved DDPoS algorithm focusing on achieving high efficiency, fairness, and security. The main idea is divided into two parts. Firstly, the advantages of PoW and DPoS have been put into ad-lib the current DPoS algorithm. The nodes are selected with enough computational power rather than going for stakes. To deal with centralization and to make the algorithm fair, every node has only one vote for voting. Secondly, the downgrading mechanism is designed such that the malicious nodes are put in the candidate nodes set and their ranks are decremented by one. But the designed algorithm is not suitable for real-time application in the existing blockchain environment.

1.3 Problem Statement

To design NFT Marketplace with DAO such that the contributions of DAO are the NFTs purchased in the marketplace, furthermore to host it on a blockchain network with the designed consensus algorithm.

1.4 Objectives and Scope of the project

The NFT marketplace and DAO integration are one of a kind presently.

1.4.1 Objectives

1. To create an NFT marketplace and DAO for digital art.
2. Develop smart contracts to mint tokens.
3. To design DAO voting algorithm based on Proof of Stake.
4. To incorporate an efficient and scalable consensus algorithm.
5. To evaluate the system with the present state of art.

1.4.2 Scope of the project

The project is for the NFT marketplace for digital art only and can be further jotted down for organizations with NFTs of all kinds. The weightage of the stakeholders in the organization depends only on the value of the NFTs they purchase and that makes the richer's decision more prevalent over others. This can be reduced further by using different parameters of the NFTs like the age and number to bring in more fairness.

Chapter 2

REQUIREMENT ANALYSIS

2.1 Functional Requirements

- The user shall be able to register and log in to the marketplace.
- The user shall be able to view others' artwork.
- The user shall be able to upload artwork.
- The system shall be able to create digital tokens.
- The user shall be able to bid and sell the artwork.
- The user shall be able to view proposals in their organization.

2.2 Non Functional Requirements

- User cannot have two or more accounts
- User should be able to browse through collections without logging in.
- Each user should have an NFT account to buy or sell tokens.
- The system should be able to reach a consensus within 10 minutes.
- The DAO authorities must have a minimum of 5 tokens from the marketplace to be able to contribute their views on the proposal.

2.3 Hardware Requirements

- 16GB RAM
- Minimum 256 GB storage

2.4 Software Requirements

- OS: Ubuntu
- Programming languages: Golang, Solidity, HTML, JavaScript
- Frameworks: React.js
- Development Tool: GoLand IDE, Visual Studio Code

Chapter 3

SYSTEM DESIGN

The system comprises the website and the blockchain network. This section will give you the working and connection between the two systems.

3.1 Architecture Design

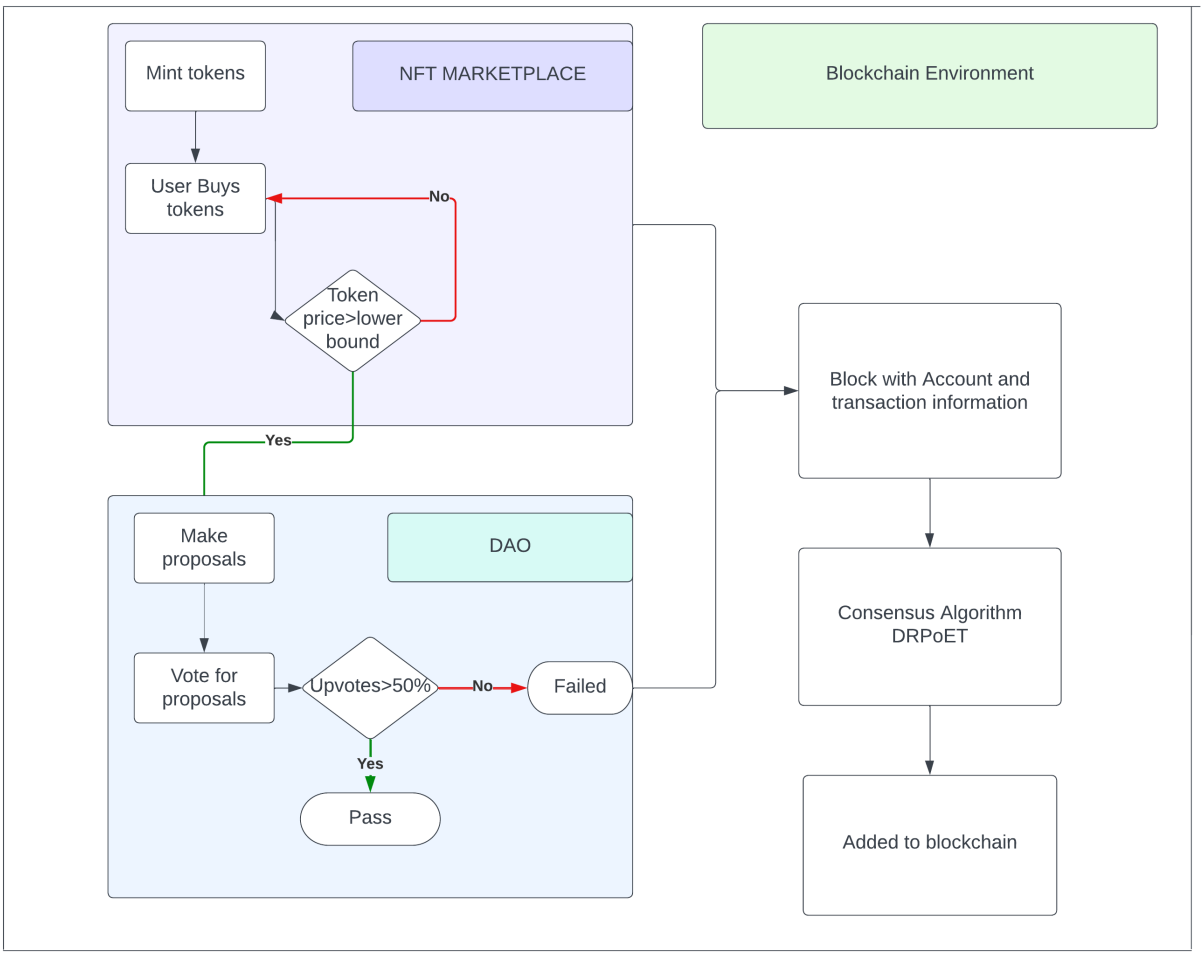

Figure 3.1: System design

Figure 3.1 gives the system diagram. A member of the organization mints the NFT tokens and lists them for purchase. Anyone with access to the marketplace and with sufficient cryptocurrency in their blockchain account can buy the NFTs. The tokens are transferred to the buyer. The data regarding the accounts and the transactions for the minting and buying the NFTs are stored in the blockchain system. Once a user's investment is higher than the lower bound, he/she can take part in the DAO decisions. The three components of the system are:

1. NFT
2. DAO
3. Consensus Algorithm

The details regarding each of the modules is given below.

3.1.1 NFT

The NFT marketplace is the page where all the NFT tokens for digital art are minted/created and are up for sale. The member of the organization can mint NFT tokens of artwork and list it for purchase. All website visitors can see the available NFTs and the information regarding their owner and the time of minting. The user of the NFT marketplace can buy the NFT tokens of his choice and enter the organization as a contributor.

3.1.2 DAO

DAO is the organizational decision-making page of the website. All the proposals for the organization are made by the stakeholders and voted on by others, thus enabling decentralized decision-making. The contributor with more than a minimum number of contributions becomes a stakeholder in the organization and can take part in making a proposal and voting for a proposal For any particular proposal, if the number of upvotes is greater than the downvotes, the proposal is passed. The proposal is rejected if the number of downvotes is greater than the number of upvotes or equal.

The below Figure 3.2 shows the working of DAO. When the NFT tokens are minted, the sum of the total price of these tokens which are up for sale, is calculated. If a user wants to buy NFT tokens, their existing contribution x must be less than 30% of p where p is calculated as 75% of the total cost of NFTs minted. This is the assumed daoBalance for a month. In the organization, a user can create a proposal or vote for the proposal only if they satisfy the conditions to become a stakeholder. That is, their contribution must be greater than the lower bound value which is set by the organization. The proposal gets accepted if the upvotes are

greater than 50% of the total votes. Otherwise, they are rejected. The organization must have at least 3 stakeholders to come to a decision. For the decisions to be fair, 30% of daoBalance is the maximum any person can contribute. The weightage for each vote depends on their contribution per total cost of the NFTs minted.

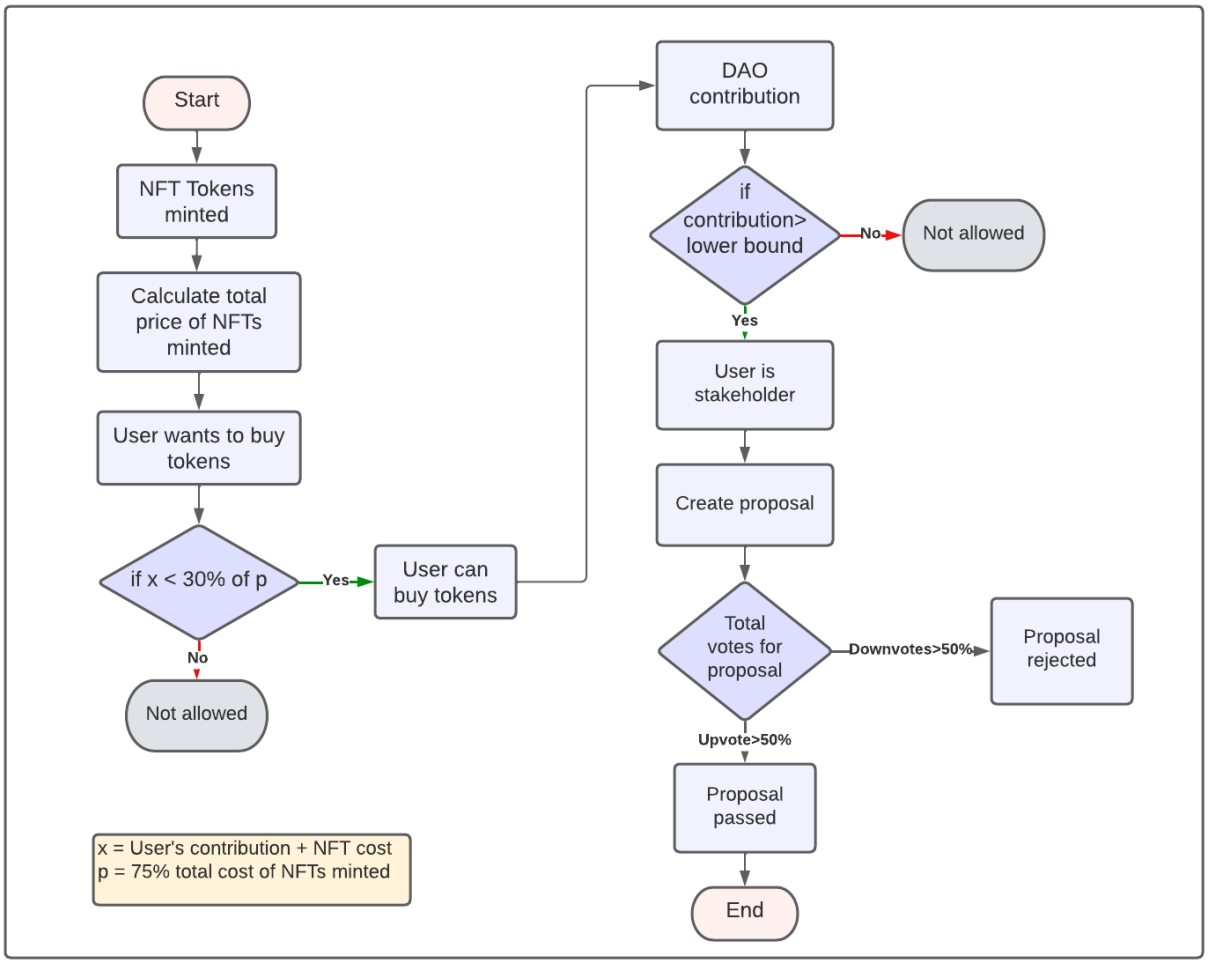

Figure 3.2: Working of DAO

3.1.3 Consensus Algorithm

The website is hosted on the Ethereum-based blockchain network. The cryptocurrency of the website is ethers. All the transactions made in the system are stored in the blockchain environment. The number of nodes and the transaction time taken for each is decided by the performance of the blockchain network. This in turn is decided by the consensus algorithm. We use the custom-made blockchain algorithm, called DRPoET, Delegated Reputation-based Proof of Elapsed Time. This consensus algorithm is fairer, more secure than the DPoS and

more efficient than PoW. The blockchain system is for permissionless systems, thus any node with access and proper computing resources can enter the system.

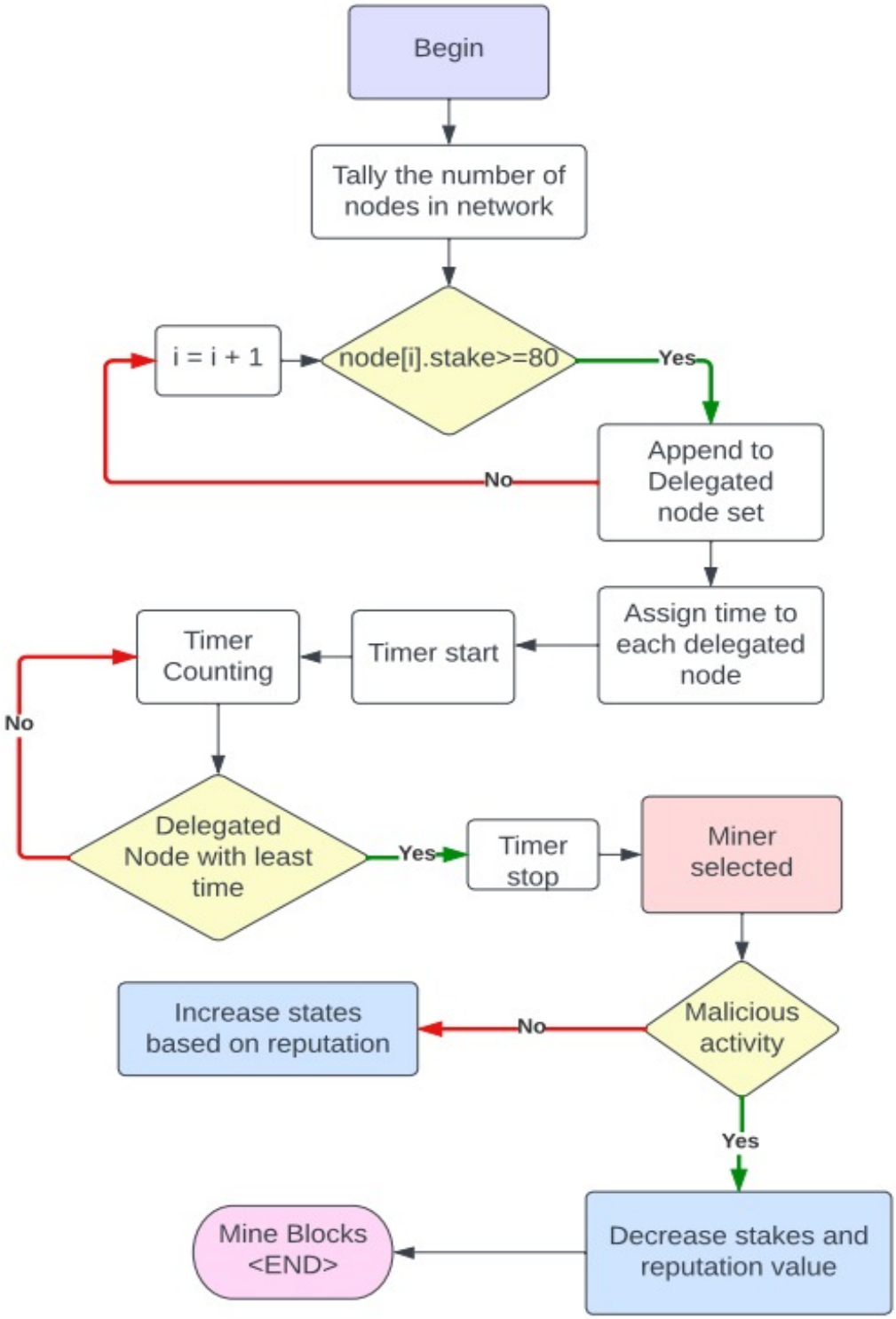

Figure 3.3: Working of Consensus algorithm

Figure 3.3 shows the flowchart of the system. Once inside the system, the nodes whose stakes are equal to or greater than the threshold are appended to the delegated node-set. In the delegated set, each node is given a random timer. Every timer is started at once, and the node whose timer is exhausted first is selected as the miner. The timer mechanism replaces the round-robin mechanism in DPoS. If the miner is good and mines valid blocks all the time, its reputation value increases concerning the block generation rate and the fairness ratio of the miner, and an incentive is provided. If the miner is malicious, the reputation value is decreased accordingly, and the stakes are withheld as a punishment.

3.2 Algorithm design

This chapter gives a brief description of the implementation details of the system by describing each component with its algorithm.

3.2.1 DAO Algorithm

Algorithm 1 shows the implementation of the DAO module. There are importantly two functions for any stakeholder. Creating a proposal and voting for a proposal. If the user wants to buy NFT tokens, their existing contribution x must be less than 30% of p where p is calculated as 75% of the total cost of NFTs minted. This is the assumed daoBalance for a month. In the organization, a user can create a proposal or vote for the proposal only if they satisfy the conditions to become a stakeholder. That is, their contribution must be greater than the lower bound value which is set by the organization. The proposal gets accepted if the upvotes are greater than 50% of the total votes.

Assumption: For a number of NFTs minted and up for sale in the NFT Market, 75% of them are purchased by the users on average.

Algorithm 1 DAO Algorithm

Input: Net profit, P
Output: Proposal voting status
T: Total number of votes
P_i: 75% of total value of NFTs minted
U_i: i^{th} User
N_i: i^{th} NFT token minted
Begin
U_i buys N_i
if $N_i.Cost + U_i.Contributions \geq 0.3 * P$ **then**
    Purchase failed
else
    NFT transfer success
end if
if $U_i.Contribution \geq lowerlimit$ **then**
    U_i is a stakeholder
    U_i can make proposal
    U_i can vote for proposal
else
    View existing proposal
end if
U_i votes for proposal
$Weightage = U_i.Contribution/P * 100$
$Vote+ = Weightage$
if $upvotes \geq 50\% \times T$ **then**
    proposal passed
else
    proposal failed
end if
End

3.2.2 Consensus Algorithm

Algorithm 2 shows the implementation details of the consensus algorithm used in the blockchain network. Every node has certain stakes, and the nodes are appended to delegated nodes set based on the threshold stakes and the threshold is taken as 80. Further, the delegated nodes are initialized with a timer. The timer mechanism is an important step taken to increase fairness and discard the round-robin mechanism, which gives importance to the stakes. A

random integer timer makes the algorithm independent of the stake.

Algorithm 2 DRPoET Algorithm

```
N_i: i^th Node
stake_i: stakes of the i^th node
D: Delegated node-set
t: Total number of delegated nodes
T: Timer of the node
M: Miner selected
Begin
while i in Nodes do
    if stake_i ≥ threshold then
        Append N_i to D
    end if
end while
Broadcast D
while i ≤ t do
    D_i[T] ← rand.Seed(196)
end while
Start Timer, T of all nodes
if D_i[T] elapses first then
    M ← D_i
end if
Broadcast M
End
```

Algorithm 3 gives the reputation mechanism incorporated into the system. This is to keep the malicious nodes in check and reduce the risks faced in the network.

Algorithm 3 Reputation algorithm

```
Input: D^t
Output: M
Begin
if M is malicious then
    R ←R−(0.6b+0.4f)
    stakes ←stakes−((stakes×R)/100)
else
    R ←R+(0.6b+0.4f)
    stakes ←stakes+((stakes×R)/100)
end if
Add block mined to B^T
End
```

Here, M: Miner node, R: reputation value of each miner, b: number of blocks mined/minute,

f: fairness index of the system, and B^T: Blockchain.

3.3 User Interface Design

The website front has mainly two parts: The NFT marketplace and the DAO site. The NFT marketplace allows users to mint and buy NFT tokens. It also allows to track all the transactions that take place in the marketplace. The DAO front allows users to view all the proposals' details and create proposals. The proposal vote is also decided on the votes of each user or stakeholder's contribution weightage. The individual page details are given in the Table 3.1

Table 3.1: User Interface Design

Content	**Details**
NFT Marketplace	Lists all the latest artworks listed for purchase and lists all the transactions made in the site.
DAO page 1	Allows stakeholder to create proposals and lists all the proposals created in the past with their status
DAO page 2	Shows the proposal details of a proposal, along with a quantitative analysis of the number of accept and reject votes.

Chapter 4

IMPLEMENTATION

4.1 Blockchain setup

The genesis.json file defines the initial state of the blockchain system. The initial states of the accounts are also defined in the Genesis file. Figure 4.1 shows the genesis.json file.

Figure 4.1: Genesis File

The nodes in the network are initialized concerning the genesis.json file. Figure 4.2 shows the command to initialize the nodes.

```
hpc@hpc-Vostro-3446:~/go/bin$ sudo ./geth --datadir ~/ethereum/node1 init genesis.json
```

Figure 4.2: Initializing the nodes

Each account is credited with a sufficient amount(stake) for transactions Figure 4.3 depicts the command to initialize the network and add the nodes.

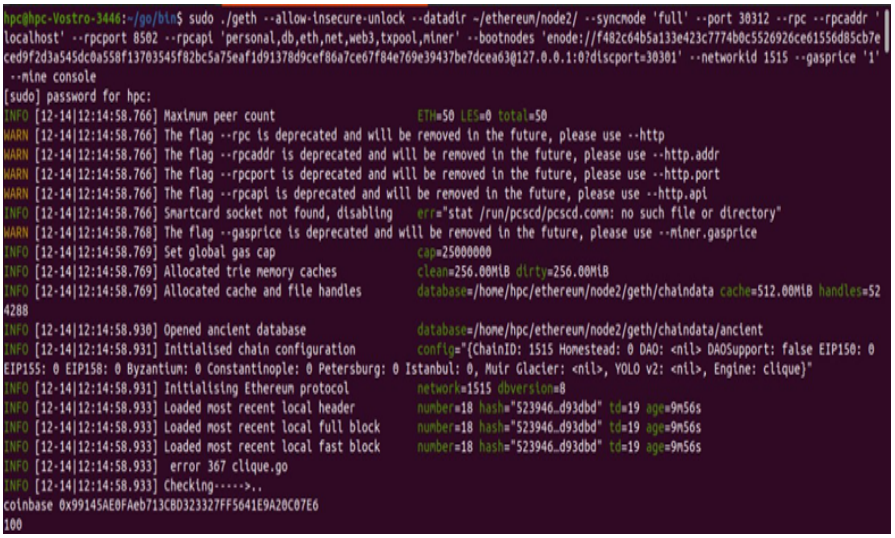

Figure 4.3: Peer-to-peer network

4.2 DAO

Figure 4.4 gives the contributing function in the smart contract interacts with the NFT marketplace to take contributions from the users.

```
function contribute() payable external returns (uint256) {
    require(msg.value > 0 ether, "Contributing zero is not allowed.");
    maxper = ((30 * mintedmax)/100);
    if((msg.value + contributor[msg.sender]) < maxper)
    {
        if (!hasRole(STAKEHOLDER_ROLE, msg.sender)) {
        uint256 totalContribution =
            contributors[msg.sender] + msg.value;

        if (totalContribution >= MIN_STAKEHOLDER_CONTRIBUTION) {
            stakeholders[msg.sender] = totalContribution;
            contributors[msg.sender] += msg.value;
            _setupRole(STAKEHOLDER_ROLE, msg.sender);
            _setupRole(CONTRIBUTOR_ROLE, msg.sender);
        } else {
            contributors[msg.sender] += msg.value;
            _setupRole(CONTRIBUTOR_ROLE, msg.sender);
        }
    } else {
        contributors[msg.sender] += msg.value;
        stakeholders[msg.sender] += msg.value;
    }

    daoBalance += msg.value;
```

Figure 4.4: Contribute function

Figure 4.5 gives the function voting function, where the vote of the stakeholder is respectively increased according to their weightage of contribution.The proposal gets accepted if the upvotes are greater than 50% of the total votes. Otherwise, they are rejected. The organization must have at least 3 stakeholders to come to a decision. For the decisions to be fair, 30% of daoBalance is the maximum any person can contribute. The weightage for each vote depends on their contribution per total cost of the NFTs minted.

```
function performVote(uint256 proposalId, bool choosen)
    external
    stakeholderOnly("Unauthorized: Stakeholders only")
    returns (VotedStruct memory)
{
    ProposalStruct storage proposal = raisedProposals[proposalId];

    handleVoting(proposal);

    if(choosen)
    {
        proposal.upvotes += ((stakeholders[msg.sender]*100)/mintedmax);
    }
    else
    {
        proposal.downvotes += ((stakeholders[msg.sender]*100)/mintedmax);
    }
    stakeholderVotes[msg.sender].push(proposal.id);

    votedOn[proposal.id].push(
        VotedStruct(
            msg.sender,
            block.timestamp,
            choosen
        )
    );
```

Figure 4.5: Vote function

4.3 Consensus Algorithm

The DR-PoET consensus algorithm has two main components: The timer and the reputation. The Timer is the period of each node's random wait time, during which it must sleep and Reputation is the value assigned to each node and its value is updated based on its behavior. The Reputation value lies between 0 to 100. Figure 4.6 shows the miner reputation and timer variable added to the structure of delegated nodes.

```
type TallyStake struct {
        Owner     common.Address `json:"owner"`
        OStakes   uint64         `json:"o_stakes"`
        Timestamp time.Time      `json:"timestamp"`
        CoinAge   uint64         `json:"coin_age"`
        Reputation float32
}

type TallyDelegatedStake struct {
        Owner     common.Address `json:"owner"`
        OStakes   uint64         `json:"o_stakes"`
        numblocks uint64         `json:"numblocks"`
        sleeptime time.Duration  `json:"sleeptime"`
        miner_time int
        NumBlocks int
        Reputation float32
}
```

Figure 4.6: Parameters added to the DPoS system

Figure 4.7 shows the timer implementation wherein we take the randomly generated time and it is assigned to the node. When the node has more than 80 stakes then the node gets appended to Delegated node set with its attributes such as address, stakes,and total number of blocks, timer, and reputation.

```
n := rand.Intn(196)
if snap.TallyStakes[i].OStakes >= 80 {
        snap.TallyDelegatedStake = append(snap.TallyDelegatedStake, &TallyDelegatedStake{
                Owner:   snap.TallyStakes[i].Owner,
                OStakes: snap.TallyStakes[i].OStakes,
                miner_time: n,
                NumBlocks: 0,
                Reputation: snap.TallyStakes[i].Reputation,
        })
}
```

Figure 4.7: Implementation of timer

Figure 4.8 shows the reputation of a node. When the node is malicious, its malicious fairness is calculated by taking a number of blocks as a parameter. The Reputation of a node is subtracted from the calculated reputation. The number of stakes of a node is also reduced using the calculated reputation. The calculated stakes are assigned to the node. If the stakes are less than the threshold, then the node is downgraded from the Delegated node-set.

```
if c.malicious == true {
        rep := float32((mined_blocks * 6 / 10) + (4 * (mined_blocks / sum) / 10))
        if rep > float32(100) {
                rep = float32(100)
        }
        snap.TallyDelegatedStake[miner_index1].Reputation = snap.TallyDelegatedStake[miner_index1].Reputation - rep
        snap.TallyStakes[miner_index2].Reputation = snap.TallyDelegatedStake[miner_index1].Reputation
        fmt.Println("before", c.stake)
        c.stake = c.stake - (c.stake * uint64(rep) / 100)
        fmt.Println("Downgrading This Node")
        fmt.Println("After Downgrading Node have Reputation", snap.TallyStakes[miner_index2].Reputation)
        fmt.Println("After", c.stake)
        c.malicious = false

}
```

Figure 4.8: Reputation Calculation of Node

Chapter 5

RESULTS AND DISCUSSIONS

5.1 Experimental Setup

The system was tested on a physical machine with an Intel processor with an i5 core CPU, which runs at 1.70 GHz. This machine uses Ubuntu 22.04.5 LTS Operating system. The blockchain was set up with 4GB RAM and 512GB secondary storage.

Table 5.1: Configurations of the system used

Components	Software/Language	Version
Operating System	Ubuntu	22.04.5LTS
Blockchain	Ethereum	4.0
Blockchain Client	Geth	1.9.26
Programming Language	Go	1.19.4
Framework	React.js	18.2.0

5.2 NFT Marketplace

The NFT marketplace allows users to mint and buy NFTs. Figure 5.1 shows the NFT marketplace. Users can mint, buy and sell NFTs.

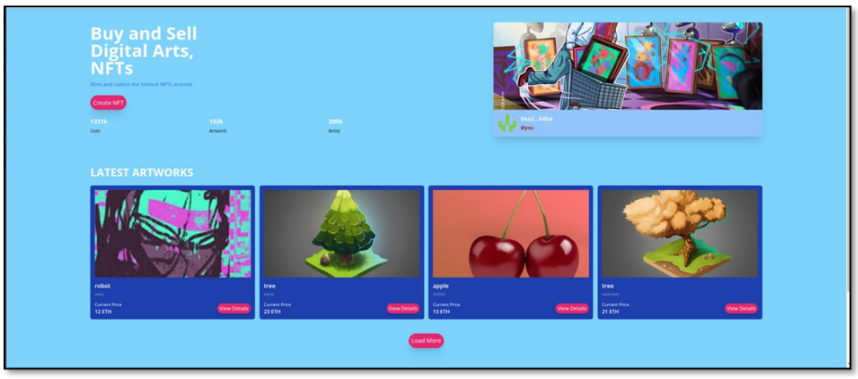

Figure 5.1: NFT Marketplace with tokens for sale

Figure 5.2 shows the purchase of tokens using a metamask wallet. To maintain fairness in the DAO organization, the users in the NFT marketplace can buy tokens only if the value of their current contribution and NFT cost is less than 30% of the total minted NFT cost price.

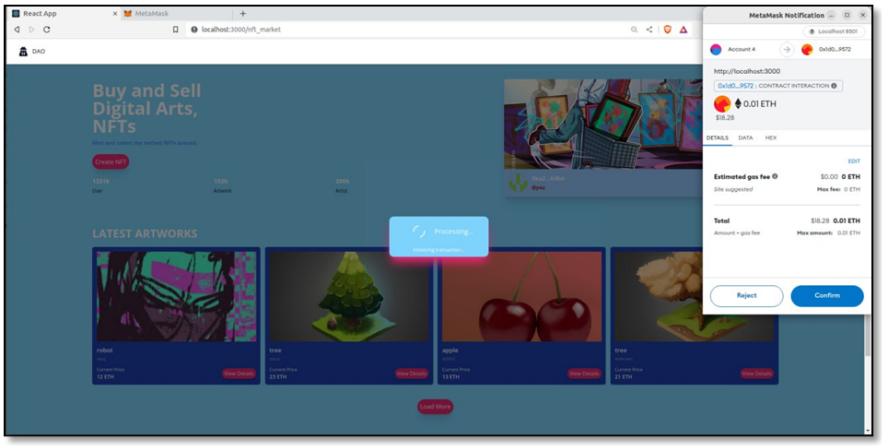

Figure 5.2: NFT purchase using metamask wallet

5.3 DAO

The DAO front page gives an overview of the proposals created and allows stakeholders to develop proposals. The users can be a part of DAO contribution if their contribution is greater than the lower bound of that organization. Only these stakeholders can create and vote to the proposals. Figure 5.3 shows the page to create proposals. Every proposal created on the site comes with a gas value to be paid from the metamask wallet.

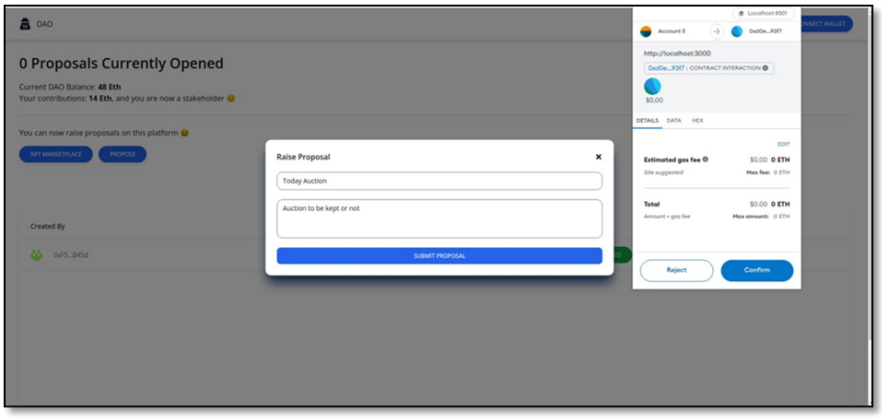

Figure 5.3: DAO creates proposals prompt

Figure 5.4 shows the DAO proposal details page shows the details of the proposal selected. The stakeholder gets an option to either accept the proposal or reject it, as shown at the bottom of this image. The algorithms mentioned above play an important role in bringing fairness to this voting. The blue bar in the image shows the accepted rate and the red one shows the rejected rate. The result not only depends on the number of votes for accept or reject but also on how much power the stakeholder holds.

Figure 5.4: DAO proposal votes

5.3.1 User weightage analysis

For 10 users, the contributions of each of them are generated randomly and the weightage of each of the user's votes is calculated. The mean weightage of each user is calculated as shown in the algorithm 1. The capping is applied while buying NFTs, each user can buy tokens only if his contribution and NFT cost are less than 30% of the prices which is calculated as 75% of the total cost of NFTs minted. Figure 5.5 shows the distribution of the weightage of each user for any existing DAO without the capping of contributions and Figure 5.6 shows the weightage of each user after applying the capping to bring fairness. The chart shows that no user has got the majority of the weightage and the decision will not be skewed.

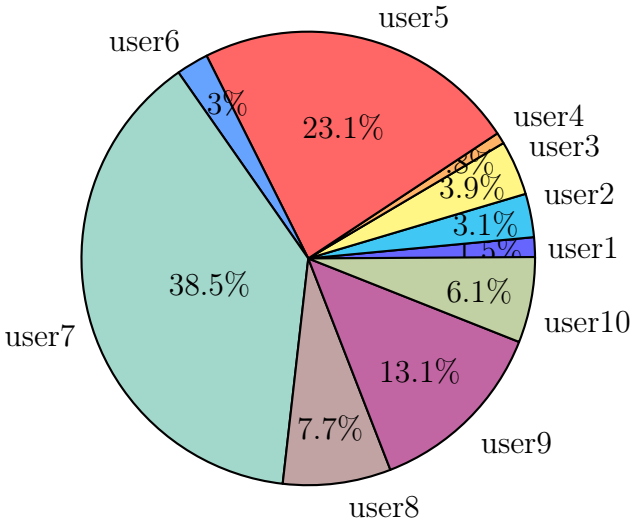

Figure 5.5: User weightage distribution before capping

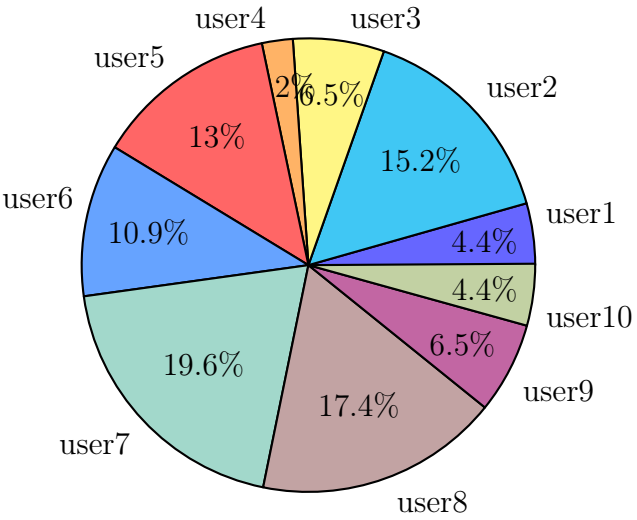

Figure 5.6: User weightage distribution after capping

5.4 Consensus Algorithm Efficiency Analysis

5.4.1 Impact of Network

The efficiency of any blockchain network is calculated with respect to the consensus algorithm. We have taken the time required for 100 transactions for varying numbers of nodes. The time taken is jotted down in the graph in Figure 5.8 against the time taken for the PoW consensus algorithm.

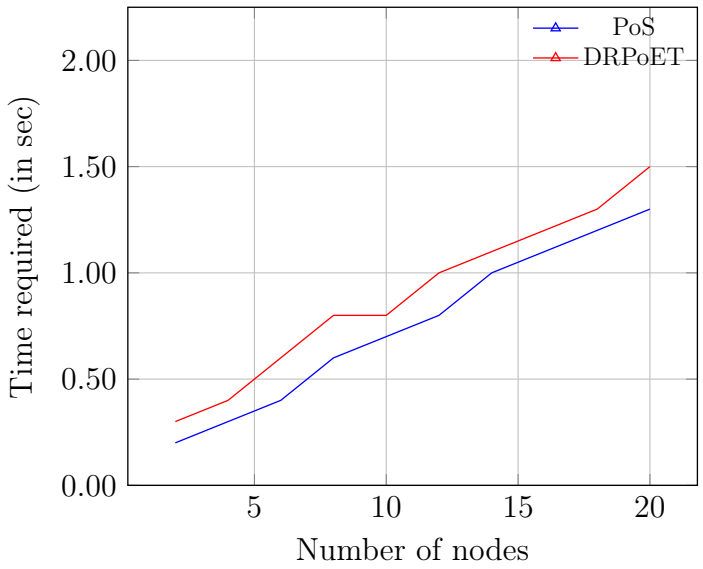

Figure 5.7: Impact of network size

5.4.2 Impact of Load

Figure 5.8 depicts the impact of load, in terms of transactions for a fixed number of nodes in the network. We have taken 20 nodes and the time required for the transactions is recorded 10 times. The average time required for each number of transactions is recorded and compared with the PoW algorithm.

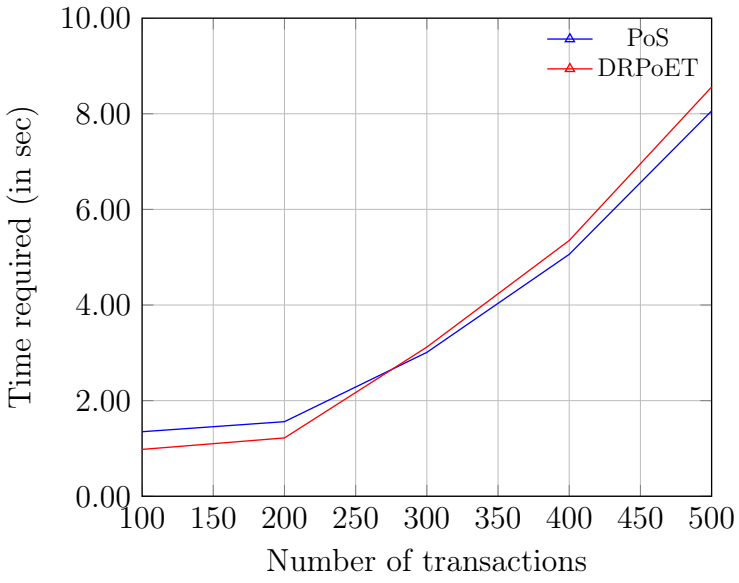

Figure 5.8: Impact of load

5.4.3 Fairness Analysis

The Fairness Index is calculated using Jains' Fairness Index formula.

$$J(x_1, x_2, \ldots, x_n) = \frac{(\sum_{i=1}^{n} x_i)^2}{n \cdot \sum_{i=1}^{n} x_i^2}$$

Here, n = percentage of blocks generated by each node is given in Figure 5.9 Number of delegated nodes in the network: 10
Node 1 blocks generated: 10%
Node 2 blocks generated: 11%
Node 3 blocks generated: 10.4%
Node 4 blocks generated: 9.2%
Node 5 blocks generated: 11%
Node 6 blocks generated: 9.55%
Node 7 blocks generated: 9.25%
Node 8 blocks generated: 10.5%
Node 9 blocks generated: 9.5%
Node 10 blocks generated: 9.6%

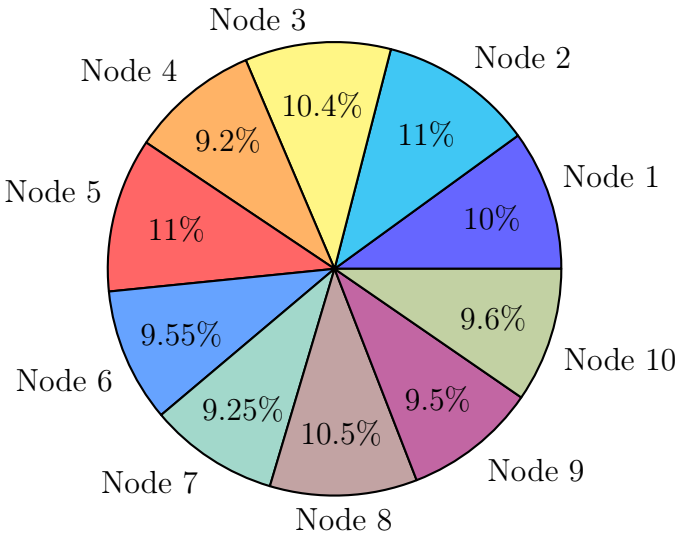

Figure 5.9: Block percentage of every node

Therefore: N = 10, x1 = 10, x2 = 11, x3 =10.4, x4 =9.2, x5=11, x6 = 9.55, x7 = 9.25, x8 = 10.5, x9 = 9.5, x10 = 9.6

(Xi)2 = 1004.225, Therefore Fairness Index, FI equals 10000/(1004.225 * 10) equals 0.995.
FI of Ethereum, PoS: 0.90
Thus, the fairness of the proposed system is higher than the PoS algorithm.

Chapter 6

CONCLUSION AND FUTURE SCOPE

This work integrates the NFT marketplace and the DAO for an organization that transacts digital art. The integration is a novel idea and the successful implementation benefits the organization with NFT marketplaces to grow and have a better-decentralized decision-making platform. The results show that the generated DAO allows users to vote for proposals more fairly. The weightage of votes for each user is distributed evenly and not skewed towards any user. This ensures fairness. The websites are hosted on a custom blockchain network that runs on the DRPoET consensus algorithm, which is a fairer and more secure algorithm than the present algorithms in use. Thus, confidential transaction information is assured to be safe from malicious attacks.

For the future scope of this work, we aim to evaluate the DAO-based decision algorithm and DRPoET in a larger test-bed and by considering multiple performance evaluators.

REFERENCES

[1] L. Balduf, M. Florian, and B. Scheuermann. Dude, where's my nft: Distributed infrastructures for digital art. In *Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good*, DICG '22, page 1–6, New York, NY, USA, 2022. Association for Computing Machinery.

[2] I. Barinov, V. Arasev, A. Fackler, V. Komendantskiy, A. Gross, A. Kolotov, and D. Isakova. Proof of stake decentralized autonomous organization. 2019.

[3] A. Begicheva and A. Kofman. Fair proof of stake. 05 2018.

[4] S. Bhujel and Y. Rahulamathavan. Improvement of delegated proof of stake consensus mechanism based on vague set and node impact factor. entropy. *Sensors*, 24(22):8833, Nov 2022.

[5] S. Bhujel and Y. Rahulamathavan. A survey: Security, transparency, and scalability issues of nft's and its marketplaces. *Sensors*, 22(22):8833, Nov 2022.

[6] Y. Faqir, J. Arroyo, and S. Hassan. An overview of decentralized autonomous organizations on the blockchain. pages 1–8, 08 2020.

[7] L. Liu, S. Zhou, H. Huang, and Z. Zheng. From technology to society: An overview of blockchain-based dao. *IEEE Open Journal of the Computer Society*, 2:204–215, 2021.

[8] W. Rehman, H. e Zainab, J. Imran, and N. Z. Bawany. Nfts: Applications and challenges. In *2021 22nd International Arab Conference on Information Technology (ACIT)*, pages 1–7. IEEE, 2021.

[9] Y. Saito and J. Rose. Reputation-based decentralized autonomous organization for the non-profit sector: Leveraging blockchain to enhance good governance. *Frontiers in Blockchain*, 5:1083647, 01 2023.

[10] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang. Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems*, 6(5):870–878, 2019.

[11] X. Wei and Z. HE. Robust proof of stake: A new consensus protocol for sustainable blockchain systems. *Sustainability*, 12:2824, 04 2020.

[12] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, 7:118541–118555, 2019.