Project Report

Title: Voting DAO & Funding Pool Web3 Decentralized Blockchain System

Student Name: Eskandar Atrakchi

Student ID No.: x23137517

Course Description: Academic internship

Date of Report Finalization: 15th/April/2025

# EXECUTIVE SUMMARY

Summary of the problem: systems are centralized and controlled by big companies and institutions for example, banks control our money as they can freeze it, decline transactions, or even lose it as the case in 2000 in dot com bubble and other financial crises, also giant companies like Google can decline you account creation if you don’t agree to their terms and conditions and we all agree their actions violates our privacy as they run their ads on us to make money.

According to the World Bank's latest report nearly 1.7 billion people are unbanked globally {Reference No. 1}, makes it not feasible to deploy global project to include all people around the world in dealing with money by depending on the banks. Getting all people globally to transact money from different countries in the world would require different bank transactions from different countries, this would be extremely expensive and slow also in assumption that all participants can get access to banks which it is not true.

Creating voting and financial transactable system depending on them would create some transparency concerns regardless of the speed of the banks in doing transactions that are way too slow, that in assumption that they will not get the participants rugged by declining account creation or freezing transactions for silly reasons.

Blockchain-based solution: all this can be solved by the proposed project where it implements P2P environment where no third parties needed for any action for example, the votes will be held by smart contract on the blockchain where nobody controls it as it is decentralized, when the owner wants to send money to anyone anywhere in the world as the money will be finalized in speed of light, this happens when the owner executes piece of code from smart contract on the blockchain.

The project solves database problem, by storing votes, members, pool funding history, transactions out and in on the blockchain with no databases managers as nodes fixes this problem, this is an amazing technology still not full used yet. Once it is fully implemented, we will be liberated from banks and giant monopoly companies, and this project is showcase what this technology can do.

Table of Contents

[EXECUTIVE SUMMARY 2](#_Toc195913450)

[INTRODUCTION 4](#_Toc195913451)

[BODY 4](#_Toc195913452)

[Background Information 4](#_Toc195913453)

[Theoretical Framework 5](#_Toc195913454)

[Review of Literature 5](#_Toc195913455)

[Methodology 7](#_Toc195913456)

[Approach 1: non token weighted voting system 7](#_Toc195913457)

[Approach 2: Non-Quadratic Voting or Delegated Voting 7](#_Toc195913458)

[Approach 3: Financial pool 8](#_Toc195913459)

[Findings 8](#_Toc195913460)

[Voter Participation 9](#_Toc195913461)

[Sybil Resistance 9](#_Toc195913462)

[Technical Complexity 10](#_Toc195913463)

[Discussion of Findings 10](#_Toc195913464)

[Non-Token based vs Quadratic voting 10](#_Toc195913465)

[Decentralization vs. Efficiency Trade-offs 11](#_Toc195913466)

[Scalability and User Adoption 11](#_Toc195913467)

[Smart Contract Risks and Audit Considerations 11](#_Toc195913468)

[P to P concept 11](#_Toc195913469)

[Conclusion 12](#_Toc195913470)

[Recommendations 12](#_Toc195913471)

[APPENDIX 13](#_Toc195913472)

[References 16](#_Toc195913473)

# INTRODUCTION

We certainly developed from web1 to web2 and now we are kind of stuck in web2 knowing that web2 has a lot of issues such as lack of transparency, trust, and it is centralized by big monopoly companies, web3 is the next step moving forward to better technology.

The purpose of a voting and financial pool system built using web3 is to achieve the things that web2 cannot achieve. Therefore, anyone in the world can deal with money or vote while no need to have a bank account where there are estimated 1.7 billion people do no have bank accounts {Reference No. 1}

In the DAO anyone anywhere can send value, receive value, and vote and all what it required is a device and internet connection.

This report will outline background information, theoretical framework, and I will make a review of literature knowing the methodology and token approach with discussion of findings.

Before we continue, we will give some definition of terms that we will be using in this report later:

1. DAO: is a Decentralized Autonomous Organization, which it is a type of organization that operate without a central authority.
2. Smart Contract: piece of code that it is self-executing agreement; in my project I have used solidity programming language, and that piece of code is stored on blockchain.
3. Ethereum: is decentralized open source blockchain platform, in my project I have used MegaETH test net and deployed the smart contract on blockchain using remix.org IDE.
4. Web3: decentralized web and user has ownership over their data.
5. Trust-less system: meaning a system that depends on verification, not trust, in contrast banks depend on trust not verification.
6. P to P system: a system does not require third parties.
7. Web3 Wallet: a decentralized wallet that only the owner can control it.
8. consensus mechanisms: protocols that agreed to ensure the state of the blockchain and the ledger database with recorded transactions health.
9. Sybil attack: when single entity uses multiple fake identities.
10. Financial pool: pool that anyone with web3 wallet can fund and then the owner can send the funds to anyone anywhere in the world in speed of light.
11. NFTs: non fungible tokens, unique images stored on the blockchain using decentralized IPFS database to retrieve images whenever blockchain users what to view them.

# BODY

## Background Information

There are a lot of problems in voting and funding in the current systems, from funding side third party will be holding the value such as a bank knowing that banks are not exempt from flaws, for example the money you hold in the bank is not actually yours it is the banks money and what you see in your App in just numbers! Banks are centralized and have lack of transparency, require trust in them as no one will have a look at their database as it is not allowed, and all this applies to DAO voting system when we use web2 also a lot of fraud is possible to happen for example a voter can vote more than once or voting manipulation possible to happen since it is centralized.

Blockchain solves this in a very smart way as it is decentralized meaning there are multiple nodes that running the network and a failure in one of the nodes won’t affect the overall blockchain, and also the most important thing about the blockchain is that it is trust-less meaning no third party required to trust as it is P to P system.

## Theoretical Framework

The project DAO is that anyone anywhere in the world can access and vote or send value by just having device and internet connection as it is trust-less and leader-less community as it depends on smart contracts, all decision and finances are determined by community members via a process that is transparent and decentralized also can be audit as smart contracts can be audit.

The membership works by MetaMask web3 wallet address or any other wallet, but MetaMask is recommended for this project, where anyone can create wallets for free all actions, transactions, and code are publicly available on the blockchain.

Smart contract involvement in this DAO project is that it is autonomous, meaning executable once it is approved by the community, the owner can create smart contracts and deploy them on Ethereum blockchain and can use DAO project to execute the smart contract, if the community want to execute the contract then the community will decide in a trust-less leader-less way, members also can finance the decision with no bank account required at all, all what members have to do is sending Ethereum, USDC, USDT, DAI, or any crypto currency to the financial pool using the DAO project.

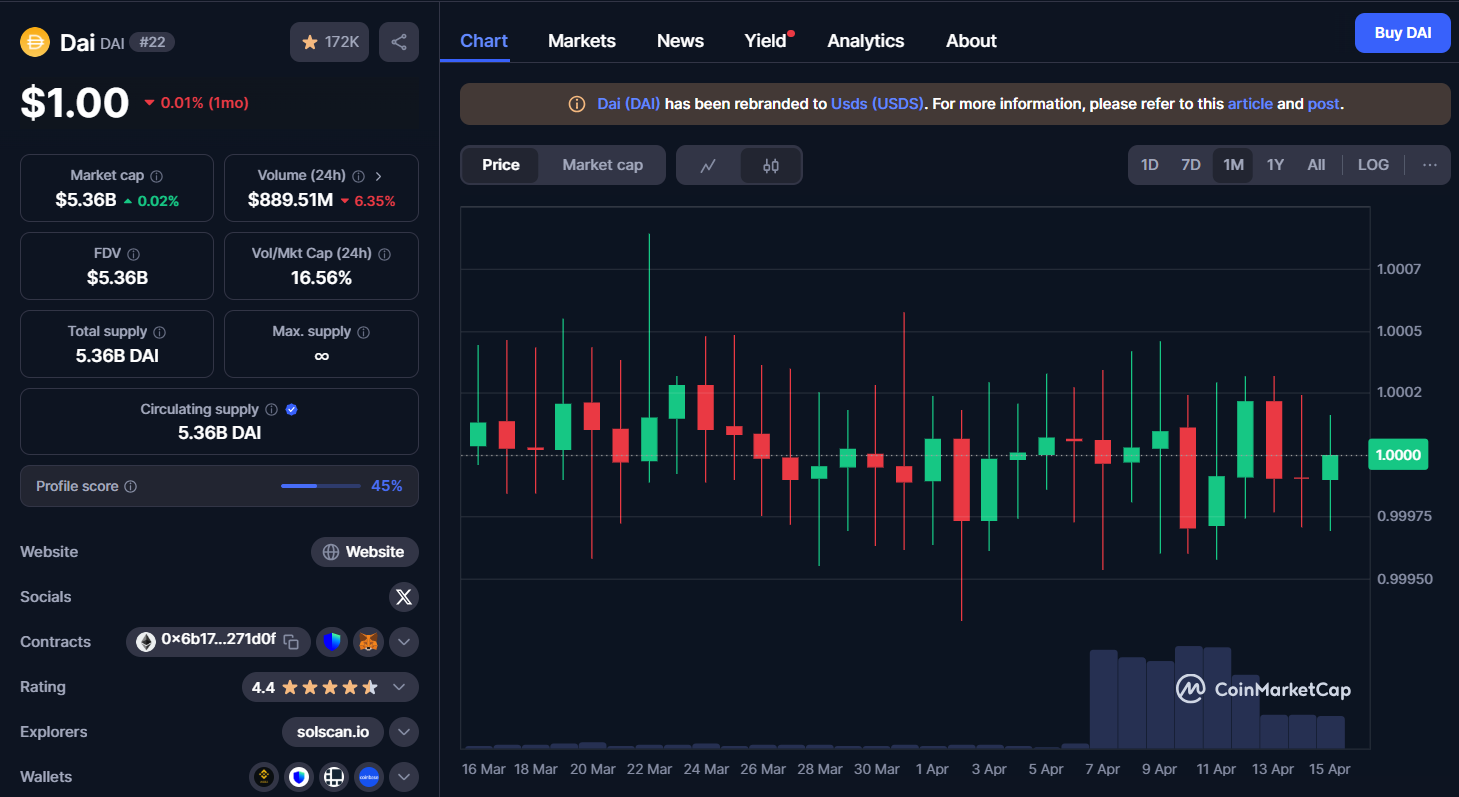
It is important to mention that this DAO project has no governance tokens and any other consensus mechanisms, it is DAO project that function by community consensus mechanism.

## Review of Literature

Decentralized Autonomous Organizations (DAOs) have become a very important of blockchain-based governance, as Vitalik Buterin 2014 {Reference No. 2} explained that DAO can eliminate centralized control through smart contracts that autonomously execute organizational rules because the DAO is built on the idea of decentralized decision making, where participants have direct control over governance through verified votes that on the blockchain.

Research confirms the advantages of DAO {Reference No. 3} by reducing corruption and enhancing transparency, and enabling global interactions as anyone anywhere on earth can participate if a device and internet connection is provided.

Some case studies about DAO for example MakerDAO as it is one of the most important DAOs existed in crypto market with market cap of 1.16B$ at the time of writing this report and maker follows same principals of web3 project enhancing decentralization, transparency, and integrity meanwhile reducing scams and corruptions knowing that maker DAO governing the DAI stablecoin through on chain governance and DAI market cap is around 5.36B$ at the time writing this report.

  
{Reference No. 15}

  
{Reference No. 14}

But regardless of the improvements and developments of the DAO voting systems there are still limitations for example token centralization as most DAO voting systems suffer from centralization risk, as the more tokens a voter has the more voting power increases this makes a small number of voters control big members this will end up to plutocracy rather than democracy just like we are having now in different markets! So, a quadratic voting systems need to be developed to mitigate the influence and the power of whales.

Other point is that most of the DAO system are complex to use and many DAO interfaces are difficult to navigate and for the non-technical people voting process is unclear and difficult to be decided which of course this will create obstacles for global adoption.

## Methodology

This section will explain the three approaches to implementing the DAO voting system and tools and technologies used in building and testing the system.

Approach 1: non token weighted voting system  
token weighted voting system is one of the most common and is used by almost all of the voting systems in real life DAOs, but I have followed the non-token voting system for the following advantages:

Decentralization: because token weighted voting system will take voting power to the number of tokens the voter holds that means the richer the voter is the more voting power will have then we turn it to plutocracy rather than democracy.

Adoption: the voting power of all participants the same with easy interface and simple mechanism to vote will drive global adoption.

Less vulnerability to market manipulation: because having more voting power is as easy as buying tokens, and this is not allowed in the current DAO project system.

Approach 2: Non-Quadratic Voting or Delegated Voting  
in case of addressing the heavily invested people in the protocol that their voting power should be listened compare to the people are not heavily invested is by implementing quadratic voting model to allow users to cast multiple votes but at an increasing cost of casting n votes is proportional to tokens and in the case of the DAO project is ETH tokens or any token on Ethereum blockchain such as USDT, USDC, or even DAI but in the DAO project is determined on members added to the blockchain database and then their voting power will always equal to 1 regardless of how many tokens the participant holds.

1 participant = 1 voting power

The advantages of that are to reduce the dominance of whales and encourage thoughtful voting allocation with the limitation of is the decision of more votes will be determined by the owner of the contract and not by the voters.

Delegated voting model is also implemented so users can delegate their voting power to a representative that they trust, these representative vote on behalf of their delegators and delegation can be changed at any time via withdrawing the ETH that they have deposited into the smart contract pool knowing this model has also its pros and cons for example one of the advantages is that help build expert driven governance without centralization in voting or financing but the cons is that may lead to power accumulation among representatives and relies on integrity and knowledge of the delegators.

### Approach 3: Financial pool

Owner and members can create financial pool to receive and send money from/to anyone anywhere in the world knowing that participating in the pool or web3 wallet holdings of tokens does not increase the voting power, the approach is to move money in speed of light 24/7 so that the participants feel comfortable using the project. Only the owner of the pool can control the funds and able to execute the live piece of code on the blockchain.

|  |  |
| --- | --- |
| **Owner Privileges** | **Member Privileges** |
| Add new members to the DAO | Create new proposals for the DAO |
| Execute proposals after voting period | Vote on active proposals |
| Withdraw funds from the treasury | View detailed proposal information |
| All member privileges | Access treasury information |

Tools and Technologies used to develop the DAO voting system

1. **Hardhat / Foundry:** development framework for compiling, testing and deploying smart contracts in localhost blockchain on my PC. Hardhat was used for its very simple typescript programming language and plugin support on VSCode and foundry was selected as well because it is fast, and it is native solidity tool as I have built smart contract using solidity.
2. **Solidity:** is the programming language that used to write the smart contract that been deployed on Ethereum blockchain
3. **Remix IDE:** to deploy smart contract to be stored on the blockchain and executed when conditions are met.
4. **MetaMask:** web3 wallet for development used to check the smart contract integrating and later the DAO project was developed to be suitable for all web3 wallets such as trust wallet as well.
5. **MegaETH:** test blockchain that is supported by Ethereum was used to deploy the contract and store it in its blocks
6. **Faucet:** ETH token provider for web3 wallets for testing purposes on only MegaETH test net.
7. **Node.Js:** for server-side scripting
8. **Next.Js:** frontend framework for users to interact with the smart contract
9. **Render.com:** for deploying the backend to interact with the smart contract
10. **GitHub:** for version control, store, and share the source code DAO project

## Findings

This section presents a comparative analysis of two voting approaches the non-token weighted voting mechanism and quadratic voting based on different key valuation metrics from research and technical experimentation and financial pool of web3 technology and sending money via blockchain wallets.

**Security**

Non-Token Weighted Voting Mechanism: this mechanism offers maximum security as it is applies the same voting power to all participants regards of participant token holding in contracts to token weighted voting mechanisms which anyone with money can buy tokens to have more voting power, the mechanism used in project dodge malicious actors from influencing the votes but on the other hand, its downside is that the participants who heavily invested will count their voting power as same as participants who are not invested or less invested which looks unfair.

Quadratic voting: it is more secure in sense of power distribution, but issues might pop up because of the complexity also without identity verification anyone anywhere can create web3 wallets for free a person can create as many web3 wallets as they want, and this may result to sybil attacks.

Financial pools are secured by the consensus mechanism of the nodes that running the blockchain {reference No. 4} this map shows how many nodes are running the blockchain, knowing that bitcoin is the most decentralized network on earth as there is no other network can match its decentralization and this, by nature, makes it the most secured blockchain, the money is held by the contract that deployed on the blockchain only the owner of the contract can withdraw the money to any address that the owner want and the transaction will be successful in speed of light to anyone anywhere in the world.

### Voter Participation

Non-Token Weighted Voting Mechanism: participation will be low when big token holdings feel their voting are not token weighted and same power vote as participants who hold no tokens, big token holdings feel their impact is negligible.

Quadratic voting: giving participants more value to all shareholders voices by adding them as members which will make decision making higher.

also, holdings in the pool does not change the voting power because the participations money in the pool will be controlled by the contract owner and does not gain any voting power to participants.

### Sybil Resistance

Non-Token Weighted Voting Mechanism: resilient to sybil attacks because it is not token weighted system which prevents token accumulation to gain voting power which will make it then resilient to sybil attacks.

Quadratic voting: sybil resistance depends on the presence on the identity layer, that’s why the project accepts voting power only to the members to prevent attack voting and changes to decision making. This is fixed by storing all the members on blockchain database and there is contact page if any participant wants to contact the owner to add more members to the blockchain database.

The blockchain ledger is resilient to any attack not only sybil attack, at the time of writing the report the market cap of BTC is 1.67T$ publicly available on the blockchain to everyone but no one can take it because the resources require to hack blockchain with this strength is way higher than the value of the whole blockchain multiple times.

A screenshot of a computer

AI-generated content may be incorrect.  
{Reference No. 13}

### Technical Complexity

Non-Token Weighted Voting Mechanism: from complexity perspective it is very simple to used solidity smart contract with gas cost that are very cheap which around 1 cent per transaction pretty much predictable and manageable.

Quadratic voting: requires more advanced mathematical logic and potential external verification layer. However, same gas cost and once adding as a member there will be no risk of implementation flaws.

Financial pool: it is like web3 wallet deployed and held on the blockchain in smart contract, the owner can control the pool only which makes it pretty much a simple logic.

It is good to mention that the project is built for the people, the project is modifiable and can be changed easily by deploying another smart contract on the same blockchain will result in changing the DAO project structure, and since it is for the people, in this case people ( early testers ) can decide if token or non-token weighted voting power is suitable for them the most and this decision can also be determine in transparent and public way with lower technical barriers. However, if there is interest in quadratic voting then in this case the DAO project has already implemented the members in the smart contract, more members possible to add by the owner especially for governance upgrades and sensitive community decisions.

## Discussion of Findings

### Non-Token based vs Quadratic voting

In my opinion, I am favouring democracy over plutocracy. Non token voting based in not common in contracts to token-based voting power in real life projects, because in real life projects consider the investors, the more tokens the participant holds the more the participant invested in the project therefore the more voting power the participant will have, which also can creates voting manipulations as anyone with money can buy tokens and get more voting power to change the outcome of the proposals which it inherently supports plutocracy. On the other side non-token based is when all the participants get the same voting power regardless of the token holdings (investments) which this the project is based on for its simplicity, efficiency and DAO implementation therefore it inherently supports democracy. Quadratic voting provides a more democratic model but demands stronger identity and security mechanisms that’s why a contact us page was created to get more members to create a similar model to quadratic voting mechanism.

### Decentralization vs. Efficiency Trade-offs

Non token weighted system its priority is to be equal, but it is not fair as investors will have the same voting power to non-investors participants, but Token-weighted systems prioritize efficiency but compromise on equitable governance. In contrast, quadratic and delegated models favor decentralization but the cost of bigger of complexity and very slow execution speed as the model executions will depend on the owner of the deployed contract

### Scalability and User Adoption

The reason why most people don’t use web3 projects its because of its complexity, bad frontend integrations, and lack of scalability to achieve wild adoption the UI should be user friendly and suitable for all devices that’s how the DAO project was built as I have used Next.js and tailwind CSS stylings to give user best frontend experience when using the project because quadratic model could hinder participants from participating in the DAO especially if the UI is not user friendly.

The voting mechanism must balance complexity and user friends experience and non-token weighted voting power should scale easily by using web3 wallets such as MetaMask which I recommend and other wallets such as trust wallets.

### Smart Contract Risks and Audit Considerations

Implementing smart contract for both quadratic voting and non-token weighted voting mechanism is required for security purposes, but I have implemented and deployed only one smart contract as it can be develop in the future if the project gets to be worked by a team to develop its logic, the logic of the DAO project is simple and I have not considered security prospects, but of course, after findings I realized implementing two contracts for each is required for security. The project I implemented is non token voting mechanism with ability for the owner of the contract to add member acting as quadratic model via contract logic executions processes.

### P to P concept

Sending money to anyone anywhere in the world with no help of third party is revolutionary step to eliminate control of the big entities on us and that’s what my project is trying to achieve.

Anyone can create pool and anyone can fund the created pool, this pool works by making the owner withdrawing money to any person in the world and in speed of light with no need to third party at all, the owner (sender) and the receiver only and this finalized with no other entity included in the transaction, the transaction will be stored in the blockchain in a decentralized and distributed among the nodes by a specific consensus mechanism, in my DAO project case it is proof of stake consensus mechanism, in my opinion, this is the future of the money and database as no one will control, delay, or freeze transactions for silly reasons and most impressive part it is available 24/7 no bank holidays or weekends as it moves in speed of lights.

# Conclusion

This report explores my ability of implementing a decentralized blockchain voting mechanism with a DAO using blockchain technology and financial pool to send money anywhere to anyone in the world in speed of light via smart contract logic, three logics implemented in the DAO project, financial pool where the owner can select where the money to go in speed of light and two governance models non token based and quadratic model all this was analysed based on technical and security parameters.

While I have showed case that token weighted mechanism is common in the industry standard non token voting mechanism leans to democracy rather than plutocracy. On the other hand, quadratic model represents more democratic governance but slower and more complex.

This technology keep evolving rapidly as four years ago I was using different libraries and technologies to build the same what I built in this project, with experimentation across governance models, identity layers, and community engagement techniques such as fast smart contracts executions and send money in speed of light to anyone anywhere in the world as the purpose is to make the project convenient to use and simple.

This project ostensibly is in full development but in fact it is not as the project can be developed especially as the community grows more DAO structure possible to implement and more smart contracts deployment on the blockchain will be ideally to match the database and send and receive money among people in the same speed.

# Recommendations

Based on the findings the following actions are recommended especially if the community grows

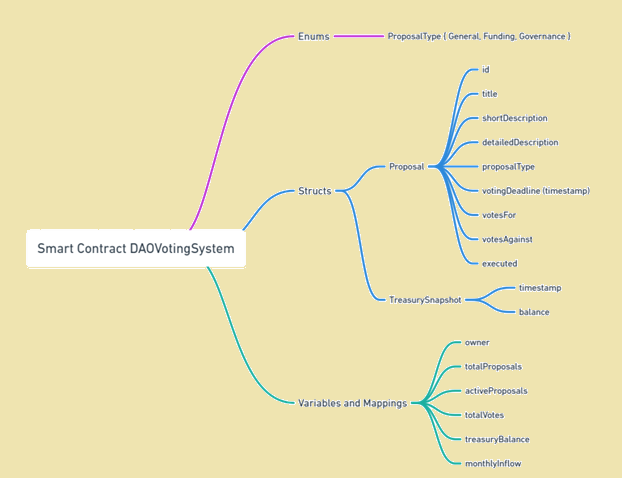
1. Adopt non token weighted voting mechanisms to make sure the development is going smoothly and for ease of participation for the participants
2. Make sure that off chain voting mechanisms are available to minimize gas fees by integrating snapshot of the smart contracts and enabling flexible vote strategies.
3. Implementation of the incremental development as project starts with limited governance scop and iteratively expanding based on the expansion of the community and its feedback.
4. Plan for future upgrades:

* create a secondary smart contract for quadratic model voting to meet the security requirements
* integrate NFTs for decentralized identity system
* zk-SNARKs for privacy preserving voting
* Quadratic or delegated voting mechanism is ideally recommended as the community matures.

# APPENDIX

A diagram of a company

AI-generated content may be incorrect. **Figure 1** – *DAO Voting System Workflow Diagram*

 **Figure 2 – *Mind Map of the DAOVotingSystem Smart Contract Components***

knowing the contract logic is structured around core components such as proposals, treasury snapshots, and DAO variables, as illustrated in Figure 2 above.

A screenshot of a black screen

AI-generated content may be incorrect.  
Figure 3 – *System overview of the DAOVotingSystem Smart Contract architecture, outlining roles (Owner, Member, External User), modules (Proposals, Treasury, Membership), and key events and interactions.*

# References

1. Aragon. (n.d.). *Aragon Whitepaper*. Retrieved from <https://aragon.org/whitepaper>
2. Buterin, V. (2014, May 6). *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*. Ethereum Blog. <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide>
3. CFTE. (2022). *The World's Top 5 Unbanked Countries Have More Than 60% of Their Population Without Bank Accounts*. Centre for Finance, Technology and Entrepreneurship. <https://blog.cfte.education/the-worlds-top-5-unbanked-countries-have-more-than-60-of-their-population-without-bank-accounts/>
4. DeXe. (n.d.). *Benefits of DAOs*. <https://www.dexe.io/blog/benefits-of-daos>
5. Ethereum Foundation. (n.d.). *Ethereum Whitepaper*. <https://ethereum.org/en/whitepaper/>
6. Lightning Network. (n.d.). *Nodes and Channels Map*. mempool.space. <https://mempool.space/graphs/lightning/nodes-channels-map>
7. OpenZeppelin. (n.d.). *Contracts and Security Audits*. <https://docs.openzeppelin.com/>
8. Snapshot. (n.d.). *Snapshot Documentation*. <https://docs.snapshot.org/>
9. DAOstack. (2018). *DAOstack Whitepaper*. <https://daostack.io/docs/>
10. Weyl, E. G., Posner, E. A., & Zhang, S. (2018). *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*. Princeton University Press. *(Referenced for Quadratic Voting)*
11. Atrakchi, E. (2024). *DAO Web3 Voting System* [GitHub Repository]. <https://github.com/EskandarAtrakchi/DAO-web3-voting-system>
12. Atrakchi, E. (2024). *DAO Web3 Voting System Demo* [Deployed Application]. <https://dao-web3-voting-system.onrender.com/>
13. CoinMarketCap. (n.d.). Bitcoin (BTC) Price, Charts, and Market Cap. Retrieved April 15, 2025, from <https://coinmarketcap.com/currencies/bitcoin/>
14. CoinMarketCap. (n.d.). Maker (MKR) Price, Charts, and Market Cap. Retrieved April 15, 2025, from <https://coinmarketcap.com/currencies/maker/>
15. CoinMarketCap. (n.d.). Multi-Collateral Dai (DAI) Price, Charts, and Market Cap. Retrieved April 15, 2025, from <https://coinmarketcap.com/currencies/multi-collateral-dai/>