Masterarbeit

Incentivizing Scientific Research Using a Reputation Scaled Proof of Stake Blockchain

by

Charan Annadurai

Supervisors:

Prof. Dr. rer. nat Erik Zenner

Prof. Dr. phil. M.Sc Andreas Schaad

Submitted in fulfilment of the requirements for the degree

Master of Science in Enterprise and IT Security

in the Enterprise and IT Security Department

Hochschule Offenburg

March 25, 2024

Abstract

Though the basic concept of a ledger that anyone can view and verify has been around for quite some time, today's blockchains bring much more to the table including a way to incentivize users. The coins given to the miner or validator were the first source of such incentive to make sure they fulfilled their duties. This thesis draws inspiration from other peer efforts and uses this same incentive to achieve certain goals. Primarily one where users are incentivised to discuss their opinions and find scientific or logical backing for their standpoint. While traditional chains form a consensus on a version of financial "truth", the same can be applied to ideological truths too. To achieve this, creating a modified or scaled proof of stake consensus mechanism is explored in this work. This new consensus mechanism is a Reputation Scaled - Proof of Stake. This reputation can be built over time by voting for the winning side consistently or by sticking to one's beliefs strongly. The thesis hopes to bridge the gap in current consensus algorithms and incentivize critical reasoning.

Declaration of Authorship

I, Charan Annadurai, declare that the dissertation, which I hereby submit for the degree *Master of Science in Enterprise and IT Security* at Hochschule Offenburg, is my own work and has not previously been submitted by me for a degree at this or any other tertiary institution.

Signed:

Date:

“So the Lord scattered them from there over all the earth, and they stopped building the city.”

The Tower of Babel - Genesis 11:8[1]

Acknowledgements

First and foremost my thanks to Prof. Dr. rer. nat Erik Zenner. I am grateful for his support and encouragement throughout this endeavour. His interest in my work inspired me to push my boundaries and work harder. The scrutiny he applied to my work has been invaluable in helping me to navigate challenges and build a stronger, more coherent thesis.

I extend my sincere appreciation to Prof. Dr. phil. M.Sc Andreas Schaad for his lectures on modelling systems and their requirements. They were crucial lessons that helped me in this journey. I also thank him for his tips on leveraging my thesis to enhance my resume and eventually find a worthy job.

I thank Deekshita for inspiring me to take up this problem and solve it. I also thank her for teaching me to use LateX efficiently. I extend my thanks to Nithilan P, Jeet A and Chandeep S for their invaluable opinions when my thesis was but a thought in my head. Special thanks to Aditya Nair for being the best roommate possible and keeping me company when I toiled through the nights. I also thank Harish R and Aditya for reminding me that it’s important to take breaks. I equally thank Joshua A and Daniel O for reminding me to get back to work. I am grateful for all my other friends who contributed in one way or another to help me complete this thesis.

Above all, my heartfelt thanks to my family, especially my mother, whose inspiration led me to pursue research and this master’s degree.

Lastly, I am grateful to all my teachers and professors who have played a part in my academic journey. Their contributions helped mould me into the person I am today.

Contents

Abstract i

Declaration of Authorship ii

Acknowledgements iv

1 Introduction 1
- 1.1 Echo Chambers and Lack of Diverse Exposure 1
  - 1.1.1 Misinformation - an Enabler 3
  - 1.1.2 The Human Mind - an Enabler 4
- 1.2 What are Decentralized Ledgers and Blockchain? 4
  - 1.2.1 Characteristics of a blockchain protocol 5
    - Public Key Cryptography and Hashing - Blockchain perspective 5
  - 1.2.2 Properties of the Blockchain Protocol 6
    - Common Prefix 6
    - Chain Quality 7
    - Chain Growth 7
  - 1.2.3 Consensus Mechanism 7
    - Proof of Work(PoW) 7
    - Proof of Stake(PoS) 8
    - Other Consensus Mechanisms Based on PoW 9
    - Other Consensus Mechanisms Based on PoS 9
  - 1.2.4 Other Consensus Mechanisms 10

2 Other Solutions 12
- 2.1 Battling Misinformation and Discord on Social Media 12
- 2.2 Decentralised Social Media 13

3 Overview of the proposed Solution 18
- 3.1 Introduction 18
  - 3.1.1 Reputation Scaled Proof of Stake Blockchain Which Incentivizes Scientific Research 18
    - Advantages 19
- 3.2 Proposal specifics 20
  - 3.2.1 System Overview and Requirements 20
    - Functional Requirements 20
    - Non-Functional Requirements 21
  - 3.2.2 Actors and Use Case 21
    - Delegates 21
    - Voters/Stakers 22
    - Experts 22

4 Implementation Details **24**

4.1 Use of smart contracts and Tokens . . . 24

4.2 Implementating a Proof of Stake Blockchain . . . 25

4.3 Transactions . . . 25

4.3.1 Transaction Pool . . . 29

4.4 Blocks and Blockchain . . . 29

4.5 Account Model . . . 30

4.6 Consensus - Reputation Scaled Proof of Stake . . . 31

4.6.1 Staking . . . 31

4.6.2 Forger Selection . . . 31

4.7 Consensus - Resolving Issues . . . 32

4.7.1 Buying in an Issue . . . 33

4.7.2 Discussion Forum . . . 33

4.7.3 Entering an Issue That is Already Bought . . . 34

4.7.4 Initial Voting . . . 34

4.7.5 Suggesting to Council . . . 34

Anonymous and Decentralized Qualification Verification . . . 34

4.7.6 Voting for the Council . . . 35

4.7.7 Final Vote . . . 35

4.7.8 Mathematical Modeling . . . 35

4.8 Incentive Scheme . . . 37

4.8.1 Delegate . . . 37

4.8.2 Expert . . . 38

4.8.3 Voters . . . 38

4.9 Conclusion . . . 38

5 Sample Use Case **40**

5.1 Introduction . . . 40

5.2 Wallet Creation . . . 40

5.3 Transaction Creation . . . 40

5.4 Final Output . . . 42

6 Suggestions and Addendum **44**

6.1 Core Belief Database or CBD . . . 44

6.1.1 Initial Questionnaire and Issue Alignment . . . 44

6.1.2 Issue-Based Survey and Dynamic Belief Adjustment . . . 44

6.1.3 Expert Privilege in Belief Modification . . . 45

6.1.4 Machine Learning and LLMs . . . 45

6.1.5 Polis . . . 45

6.2 Reopening Issues and Snowball Rewards . . . 46

6.3 Weight Reset . . . 46

6.4 Hardware Dependence . . . 46

6.5 Random Allocation of Stances . . . 46

7 Conclusion **48**

7.1 Ethical Considerations and Fairness . . . 48

7.1.1 Key Enablers . . . 49

7.1.2 Transparency and Decentralization . . . 49

7.1.3 Democratic Voting and Expert Council . . . 49

7.1.4 Introduction of randomness 50
7.2 Open Issues 50
7.2.1 Voter Apathy 50
7.2.2 Determination of Constants 51
7.3 Further Scope 51
7.4 Closing Remarks 51

A Intermediary Output Snippets **53**

Bibliography **67**

List of Figures

1.1 Average Ideological Diversity of content[3] 3

2.1 Social Media Functionality 14

3.1 Actors/Stakeholders and Use Cases 21

4.1 Activity/Flow Diagram 26
4.2 State Machine Diagram 32
4.3 Snippet of the Kialo Platform [45] 33

6.1 Snippet of the Polis Platform [58] 45

List of Tables

2.1 Advantages and Disadvantages of DeSo vs. Traditional Social Media 15
2.2 Comparison of DeSo Applications with Traditional Social Media . . . 16

4.1 Transaction Types and Their Validity Checks 27

5.1 Transactions As Part Of Sample Use Case 41

List of Abbreviations

DeSo	**De**centralized **So**cial Media
PoW	**P**roof **o**f **W**ork
PoS	**P**roof **o**f **S**take
UTXO	**U**nspent **T**ran**sac**tion **O**utput
DPoS	**D**elegated **P**roof **o**f **S**take
PoA	**P**roof **o**f **A**uthority
PoR	**P**roof **o**f **R**eputation
PoI	**P**roof **o**f **I**mportance
PoC	**P**roof **o**f **C**apacity
PoB	**P**roof **o**f **B**urn
PoET	**P**roof **o**f **E**lapsed **T**ime
ERC20	**E**thereum **R**equest for **C**omment 20
IPFS	**I**nter**P**lanetary **F**ile **S**ystem
dPoW	**d**elayed **P**roof **o**f **W**ork
ZKP	**Z**ero-**K**nowledge **P**roofs
TEE	**T**rusted **E**xecution **E**nvironment
LLM	**L**arge **L**anguage **M**odel
CBD	**C**ore **B**elief **D**atabase
TLS/SSL	**T**ransport **L**ayer **S**ecurity / **S**ecure **S**ockets **L**ayer
HTTPS	**H**yper**T**ext **T**ransfer **P**rotocol **S**ecure
CAPTCHA	**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

List of Symbols

D	Set containing all delegates, $D = \{d_1, d_2, \dots, d_N\}$.
W	Subset of D, containing winners $W = \{w_1, w_2, \dots, w_M\}$.
L	Subset of D, containing losers $L = D \setminus W$.
A_d	Amount contributed by delegate d.
T_w	Total amount contributed by winning delegates.
T_l	Total amount contributed by losing delegates.
R_w	Reward for a winning delegate.
α	Weight scale for adjustment, $\alpha > 3$.
β	Scale factor for council members' weight, $\beta = \frac{\alpha}{3}$.
γ	Scale factor for voters' weight who supported the winning stance, $\gamma = \frac{\alpha}{2}$.
S	Set of stances $S = \{s_1, s_2, \dots, s_k\}$.
V	Set of all eligible voters $V = \{v_1, v_2, \dots, v_n\}$.
Ω_{v_i}	Weight of voter v_i.
S_{v_i}	Stake voter has voted for.
C	Set of council members, where $C \subseteq V$.
Ω_{c_i}	Weight of council member c_i.
S_{c_i}	Stake council member has voted for.
$A_{s_i}^{(r)}$	Cumulative weight of stake s_i in round r.
N_v	Number of voters selected per round.
N_c	Number of council members selected per round.
ρ	Ratio of voters to council members per round, $\rho > 1$, $N_v > N_c$.
R	Number of rounds determined as $R = \left\lceil \frac{\lvert V \rvert}{N_v} \right\rceil$.
V_r	Subset of voters chosen randomly from V for round r.
C_r	Subset of council members chosen randomly from C for round r.
$\delta(x, y)$	Indicator function, equals 1 if $x = y$, otherwise 0.
$s_{\text{winner}}^{(r)}$	Winning stance of round r.
s_{final}	Final winning stance after all rounds.
B_i	A block in the blockchain, represented as a tuple $B_i = (D_i, h_i)$.
D_i	Set of transactions stored in block B_i.
h_i	Last block hash $h_i = H(B_{i-1})$

C_i, C_j	Chains owned by honest parties
μ	Ideal ratio of honest blocks within any segment of the blockchain.
τ	Growth rate of the blockchain.

To Dr. Logamadevi, my mother and one of the best researchers out there. . .

Chapter 1

Introduction

1.1 Echo Chambers and Lack of Diverse Exposure

The creation of the Internet changed communication and social networking forever. The Internet, as the name suggests, can itself be considered an extended social media. When the concept of social media was still novel, it was merely a simple platform for transferring messages[2]. It then evolved into something more complex, allowing users to convene, share and exchange. This was another step towards utopia. The next phase in the evolution of social media saw it change from a simple platform for personal communication and information exchange into a complex multi-faceted digital environment which supports multiple ecosystems pertaining to education, commerce, entertainment and gaming, cultural exchange, marketing and even politics. Unfortunately, with this subsequent evolution, the internet and social media inadvertently planted seeds of discord and isolated users[3]. The blame though unintentional lies with the concept of web personalization.

Web personalization is sometimes considered a necessary evil. The internet stopped being static at one point and started allowing users to upload content and not just consume it. This caused an abundance of available information. The ever-expanding quantity of information on the internet had surpassed consumer processing capabilities long ago. This resulted in users not being able to access the information they desired. This mandated the requirement of intelligent personalized applications that simplified the process of information access by taking into account the user's history, preferences and needs[4]. Though this seems innocent enough popular social media algorithms are driven by recommender systems which are based on this. Users are only shown media that they agree with and do not realize there are multiple fronts to the same issue[5]. In an interview with the Wall Street Journal, Former Google CEO Eric Schmidt while still in office talks about the future of web personalization,

> "The power of individual targeting – the technology will be so good it will be very hard for people to watch or consume something that has not in some sense been tailored for them" [6]

The issue worsens when people consider social media as a "reliable" source of news and information. Presently, the exposure of an average citizen to new information and news is almost monopolised by social media. Since the algorithms are designed to farm attention in the form of views and likes, the algorithm tends to show content that the consumer or user agrees with and very rarely shows content that the consumer would disagree with [7]. This creates small pockets and bubbles within which users are trapped. They are never exposed to anything outside this bubble such as alternate information or opposing views.

Even though this seems like it wouldn't have a big impact on the average citizen's life. Only when one considers how much social media has seeped into our daily lives, does one realize its true impact. Quoting the former chief technology officer at Xerox PARC, Mark Weiser

> "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." [8]

The impact of social media is everywhere. Most products even in grocery stores nowadays have "Follow us on these social media" printed on its back. Most successful political parties have their own IT wing or PR department. The same goes for companies which worry about their customer's views about them. Whole E-Commerce ecosystems survive purely using social media. Social Media affects everything we do, buy and use. This heavy influence when combined with the bubble or echo chambers which keep repeating or re-showing content that one agrees with eventually leads to political and social extremism. A report from Facebook stated that,

> “64% of the people who joined extremist groups on Facebook did so because the algorithms steered them there.” [5]

Cross-cutting content refers to the amount of alternating or opposing views a person is exposed to. Fig. 1.1 shows the amount of cross-cutting users are exposed to from different sources. The data and the graph are part of a study by Bakshy et al.[3] in 2015. Though the social media landscape has changed since then it remains relevant as an indicator of how users weren't incentivized enough to seek out opposing views. The sources in the graph are of four types,

1. Random - From Random sources users are bound to get 40% to 45% of content that is opposing in view. In case recommendation algorithms were random there would be a good percentage of exposure to "hard" content or content which consumers don't agree with

2. Potential Networks - These include opposing views or content from friends and friends of friends.

3. Exposed - This is the actual "hard" content that recommendation systems show users

4. Selected - This represents content that the users deliberately searched and selected or clicked on which was dissonant.

Fig. 1.1 shows the hard content users come across from different sources. It is not an accurate representation of how often an average user access this source. Neither do real-world users not actively seek out information from a source which is random nor do they specifically go search for "hard" information. This is due to a lack of incentive to do so.

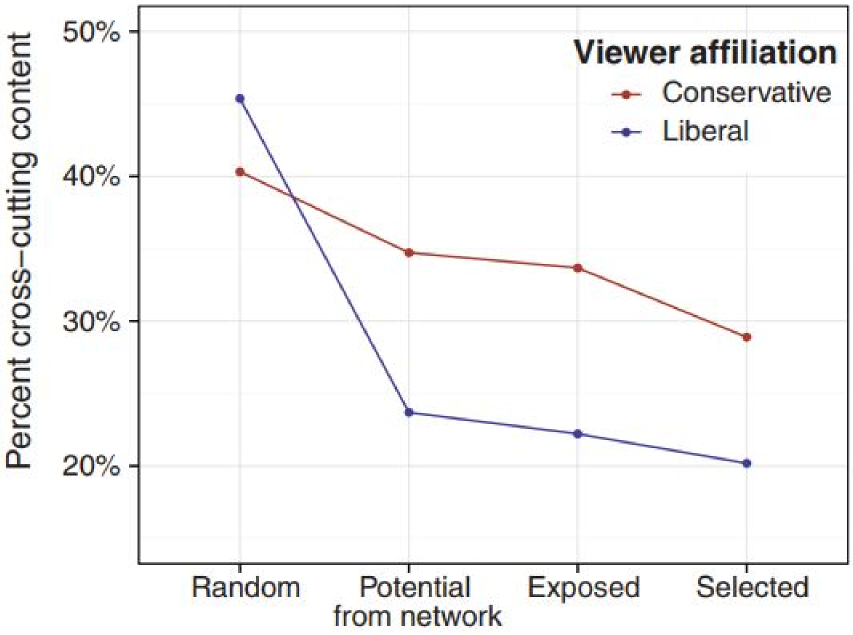


Figure 1.1: Average Ideological Diversity of content[3]

1.1.1 Misinformation - an Enabler

Misinformation acts as a powerful catalyst for discord on social media, driving wedges between individuals and communities. Misinformation mongers exploit pre-existing tensions and create new ones. Lazer et al provide some key differences between Misinformation, Disinformation and Fake news[9]:

- Misinformation - "False or misleading information"[9]
- Disinformation - "False information that is purposely spread to deceive people"[9]
- Fake News - "News that is fabricated information that mimics news media content in form but not in organizational process or intent."[9]

By rapidly broadcasting manipulated information that appeals to emotions, biases, or prejudices, malicious actors can disrupt rational discourse and amplify polarized opinions. Social media platforms enable such misinformation to travel rapidly, reaching a huge audience before corrections or fact-checks can be made. This often results in the cementing of false beliefs and causes more resistance to counterarguments. Misinformation mongers also exploit recommendation algorithms, as content that triggers strong emotional reactions is more likely to be shared, commented or in other ways interacted with and thus is recommended by the algorithm. Echo chambers are highly susceptible to misinformation, as the lack of diverse viewpoints prevents critical reasoning, scientific research and fact-checking[10][11][9].

1.1.2 The Human Mind - an Enabler

Though social media has fueled misinformation[12] this isn't new. People have throughout the ages formed opinions and never bothered to listen to the other side. Three major psychological biases are the reason for this,

- Confirmation bias is a fundamental psychological principle where individuals favour information that confirms their preexisting beliefs or notions[13], disregarding evidence to the contrary. This bias explains why echo chambers can be this effective, as individuals within these chambers are exposed only to confirming information.
- The Availability Heuristic suggests that people estimate the likelihood of an event based on how easily examples come to mind. On social media, misinformation that is emotional or widely shared becomes more "available" in our memory, leading to overestimation of its truth or prevalence[14].
- Cognitive Dissonance is a theory in psychology initially proposed by Festinger, it states our brain is hardwired to ignore information that is conflicting with the information we already possess[15].

These are psychological biases that this thesis aims to mitigate or at least weaken. The reason for these biases and the spread of misinformation is we aren't incentivised to discuss our opinions or even to find logical backing for or opposing views to their beliefs. Proper incentivization could be the key factor in this battle.

1.2 What are Decentralized Ledgers and Blockchain?

When systems are unreliable the reason can stem from two broad sources, either from the channel itself or from the nodes in the system. The former unreliability is modelled by the "Two Army Problem" while the latter is represented by the "Byzantine Generals Problem"[16]. The "Two Army Problem" is when two parts of an army are unable to communicate because messengers may not reach the other side i.e. unreliability of the channel. This is easily solved by implementing a timer. This timer starts when the message is sent and if an acknowledgement is not received in the specified time frame then the message is sent again. The "Byzantine Generals Problem" is much more complex, the problem is modelled when different parts of an army want to coordinate an attack against a city but one or more generals may be corrupt or have malicious intent. Only if all generals achieve consensus the attack will succeed. A corrupt general may relay false information to other generals or even produce malicious messages and blame it on the general relaying[17]. This authenticity issue is dealt with using simple public key encryption-enabled cryptographic signatures. This makes sure that even when a message is being relayed, receivers can make sure that the message is sent by the person it claims to be from. Though cryptography reduces the complexity of the problem it does not solve it completely. It is only effective if less than one-third of the generals are traitors[18]. This means that any traditional BFT algorithm requires $n \geq 3f + 1$ and $f + 1$ rounds, e.g., if you want to tolerate 3 failures(f), you need 4 rounds and 10 nodes(n) in total. Communication complexity $O(n^2)$.

This problem when applied to financials, money and cryptocurrency produces another issue of double spending [19]. Double spending is when a person tries to duplicate a transaction and make it seem like a transaction is executed twice essentially paying the receiver twice. Even though it can be verified that the person them-self sent a request. This can only be solved if some verifier knows the whole history of how much money a person owns, has spent and received. The concept of a distributed ledger is born out of this necessity. A ledger where everyone can see how much money each person has and how much money a person has transferred to another person. Any independent verifier can verify whether or not this transaction is true. UTXO (unspent transaction outputs) model is what is used to strengthen this model. This makes sure that every transaction cites the source of its money. For example, A sends 10 cryptocurrencies to B. When B sends the same to C and D. He proves that he is sending 4 unspent cryptocurrencies that he got from A to C and 5 unspent cryptocurrencies to D[20].

A distributed ledger is still not the same as a blockchain. There are still some unresolved issues with this model. A can send money to B and C simultaneously to not allow them to confirm from other sources if the transaction is valid. A system which clubs together a certain number of transactions and verifies them is required which is by default system to reach a consensus. As discussed previously there also needs to be an incentive for some verifiers to do their duty.

1.2.1 Characteristics of a blockchain protocol

This section will seek to provide a better understanding of what constitutes a blockchain protocol and try to show why it works. A blockchain protocol has three major features,

1. Hash Chain: This is a data structure which is characterised by its property of being append-only
2. Consensus Protocol: A Mechanism to select the next miner or forger who will create and propose the next block.
3. Longest Chain rule: This is an agreed-upon standard set for all blockchains in case there are two conflicting versions of a blockchain. All users wait and accept the chain which is the longest which is the one which has the most suffixes

Public Key Cryptography and Hashing - Blockchain perspective

Before proceeding any further, we need to briefly delve into two essential components that enable the hash chain and blockchain protocol, the public key cryptography ecosystem and hashing. Public Key cryptography involves the creation of key pairs and secret sharing over insecure networks. The combined efforts of multiple researchers like, Whit Diffie, Martin Hellman and Ralph Merkle are credited with the ideation of public key cryptography. Asymmetric cryptography refers to the use of two keys instead of one. It is widely used, especially for TLS/SSL, which forms the basis for HTTPS[21]. A popular use case of public key Cryptography is for cryptographic signatures. When key pairs are created, one part is termed the private key which is a secret key that users do not share. A public key which is the later part of the key pair, can be derived from the private key. This public key is shared and is often used as an identifier for user profiles. When information is encrypted with one half of the key, the other half is used to decrypt it[21]. This property gives rise to some interesting cases. When information is encrypted using the public key of a certain person, only the intended receiver can read the message. When information is encrypted using a private key anyone can verify that the message was indeed sent by the person corresponding to a public key. Distributed ledgers use this to sign transactions[20].

Hashing is an irreversible process which transforms any given data into a fixed-length value. This data represents the sum of the original plaintext. An ideal hash function never produces the same output for two different inputs. But as the size of the hash output decreases the chances of producing the same output for two different inputs is higher[20]. Imagine a blockchain as a tower of bricks, where each new brick is placed on top of the previous ones. The critical feature ensuring the stability of this tower is a cryptographic "cement" known as a hash function. Each block in the chain contains its own hash and the hash of the block before it, linking them in a secure and unbreakable sequence.

A blockchain is comprised of a sequence of blocks, each securely linked to the previous one. Mathematically, a block (B) is represented as a tuple $B_i = (D_i, h_i)$, where:

- D_i is a vector of strings, representing the data or transactions stored in the block.
- h_i is a string derived from a cryptographic hash function H, such that $h_i = H(B_{i-1})$. This means that every block contains the hash of the previous blockB_{i-1}. This ensures each block is cryptographically linked to its predecessor[16].

The immediate issue in this is what h_i will the first block use? The first block, known as the genesis block B_0, is unique as it starts the chain. Its hash h_0 can be an arbitrary value, often chosen to be a timestamp or other unpredictable string for security reasons. The first blockchain, Bitcoin used the headline of the day it was started. There was no way anyone could have known it beforehand.

1.2.2 Properties of the Blockchain Protocol

The security of a blockchain is characterized by three essential properties, these can also be a measure of its functionality[22]:

Common Prefix

The common prefix property with parameter k ensures that if the last k blocks are ignored, any two chains will share a common sequence of blocks. Formally, for chains C_i and C_j owned by honest parties at rounds r_1 and r_2, respectively, we have:

$$C_i[: -k] \preceq C_j$$

This indicates that C_i is a prefix of C_j if we disregard the last k blocks of C_j.

This means that honest parties agree and are in complete consensus with a certain past version of the blockchain, even if the lengths of the chains are different[22].

Chain Quality

The chain quality property measures the integrity of the blockchain by ensuring a sufficient proportion of blocks are produced by honest nodes. Let $\mu \in (0,1)$ represent the ideal ratio of honest blocks and within any segment of k consecutive blocks in the chain:

For any segment of k blocks, the number of honest blocks should be $\geq \mu k$.

[22] Enforcing this quality necessitates a fair proportion of blocks are forged by honest users.

Chain Growth

The chain growth property ensures that the blockchain grows at a steady rate over time. Given two honest parties' chains C_i and C_j at rounds r_1 and r_2 with $r_2 > r_1 + s$, the length of C_j should be at least:

$$|C_j| \geq |C_i| + \tau \cdot s$$

where $\tau \in (0,1]$ represents the growth rate, ensuring the chain extends by at least $\tau \cdot s$ blocks over s rounds. This means that there must be a constant influx of transactions and proposed blocks[22].

1.2.3 Consensus Mechanism

In a blockchain transactions are clubbed together in a block and verified. Multiple blocks of transactions may be proposed but only one version can be accepted. So the system also needs a way to make sure only one version is accepted. In the first-ever cryptocurrency the "Bitcoin", this acceptance of a block was done by solving a hard mathematical problem and whoever solves it first would be able to make their block accepted. These blocks also need to be added to the previous block to create an infinite ledger. This means that these blocks are being chained to each other, essentially creating the blockchain. The way of verifying through mathematical problems is called proof of work[20]. There are other methods of verifying or reaching a consensus these are broadly called consensus mechanisms or consensus algorithms[23].

Proof of Work(PoW)

As discussed earlier, Bitcoin employs the Proof of Work mechanism to verify. When transactions are added to the block the verifiers now called miners, will have to add a number to the block and make sure when hashed the hash starts with at least a given number of zeroes. This is quite hard and is computationally demanding. To incentivize the miners to do this, the miners are allowed to give themselves a single bitcoin. It is along with this transaction and the hash of the previous block that the miners have to compute the new hash. This makes sure that with one block we can trace back the whole chain. Some chains also use a Merkle Root which contains the hash of all previous blocks[20]. Finding that one random number takes computation i.e. work and this is known as Proof of Work. Examples of chains which are based on Proof of Work include Bitcoin and Ethereum

For someone to perform malicious activities they would have to keep winning. After 6 consecutive blocks, the chances of winning all of them become extremely low, specifically 0.0002428[24]. It is accepted that if a transaction happened 6 blocks before then it is permanent as this means most people agree with the version on the chain. Attacks are still possible but one needs to own the major chunk of the computing power in the chain to accomplish that. Miners have also tried pooling their power and splitting rewards to increase their chances[20].

PoW faces some challenges. The most notable is its environmental impact.n The computational effort required for mining consumes a vast amount of electricity, leading to criticism regarding from environmental and sustainability activists. The competition for mining rewards has led to the centralization of mining power in the hands of a few who have formed mining pools potentially compromising the decentralized basis of a blockchain. This centralization impacts network security, as the accumulation of power increases the risk of 51% attacks too.[25]

Proof of Stake(PoS)

Proof of Stake is a consensus mechanism that is used in blockchain networks to validate transactions. It is an alternative to the resource-demanding Proof of Work. In PoS validators are chosen based on the amount of crypto-currency they are willing to stake as collateral[26]. Chosen validators can create new blocks and validate transactions. Staking is the process wherein participants are required to lock up a certain amount as collateral or stake. This stake is held in a separate wallet and cannot be moved or spent. The chances of being chosen are directly proportional to the amount staked. Even though validators who stake more have a higher probability, the validators are still chosen randomly. Validators who are chosen receive all the fees that are part of the block or node and their stake are released after a certain period of time[20].

The staked money does not get used up and is returned after a successful forging, but it is "frozen" and cannot be traded or utilized for other purposes. If they approve any fraudulent transaction or they fail to complete the validation then their stake is burned(this process is known as slashing)[27]. As long as the sum of all the transaction fees in the node is lesser than the amount staked, fraudulent validators have no incentive to cheat as they risk losing their stake.

Though proof of stake is better in some aspects, it isn't perfect. Attacks are still possible but only if a person owns a significant chunk of the coins in circulation. This means that for a non-colluding miner to enforce malicious transactions they would have to own 51% of the coins in the chain which is very expensive on popular chains. This means that in newer chains these attacks are easy and not expensive. This is why most chains try to start as Proof of Work chains and then go on to become Proof of Stake Chains. Ethereum 2.0 is one such endeavour[28].

The evolution from PoW to PoS is very significant in the blockchain community's ongoing efforts to balance efficiency and sustainability. Ethereum's transition to PoS through its Ethereum 2.0 upgrade represents this. By leveraging PoS, Ethereum seeks to reduce its energy footprint while increasing blockchain integrity and efficiency[28].

Proof of Stake initially looked like it favours users on the chain with more money This led to the exploration of some extra weights to reward loyalty. This resulted in the introduction of coinage [29]. This allows the value of a coin to increase based on the length of time it was staked. This is not a perfect solution as even the rich can do the same. There is still constant debate and research into alternate bases for consensus mechanisms.

Other Consensus Mechanisms Based on PoW

- Proof of Meaningful Work (PoMW)[30]- This is a highly appreciated variant of proof of work, since PoW is wasteful, PoMW derives from it and proposes that miners can use their computation power in order to support public scientific research projects(medical research, astrophysical simulation and chemical research). It is limited by the fact of having to choose different difficulty of problems in order to increase hardness over time.
- Delayed Proof of work(dPoW)[31] - This is a second-layer consensus mechanism that allows one blockchain to take advantage of the security provided through the hashing power of a secondary blockchain. Basically, a group of nodes on the dPoW chain called Notary nodes, add the data from their chain to a well-established PoW chain and get them validated there, On top of validating them on their own chain. This is especially useful for chains which have a small number of users and as such are more susceptible to 51% attacks. Attackers would have to face the combined hashing power of both chains in order to carry out malicious activity. This is a great security measure but is twice as wasteful as PoW. The Komodo chain uses this leveraging the Litecoin chain.

Other Consensus Mechanisms Based on PoS

- Delegated Proof of Stake(DPOS) -

  Sometimes after winning the in the PoS, the chosen validator fails to perform their task/ duty. Even though their stake is burnt, it still impacts the chain. One solution to this is to find backup validators but that is inefficient. Delegated Proof of Stake is yet another consensus mechanism which is used to address this specific issue. Instead of setting up a validator node themselves (which would require you to set up a machine which is always on and connected to the internet). One could use a voting mechanism to choose a delegate who will always be available to validate[29]. Each person has a fixed amount of votes proportional to the coins staked. One could also pool the staked coins and let someone else vote. No matter what when and if their delegate is chosen then the reward is split equally amongst all their voters. Delegates also deposit a bigger stake to have a chance to be on the electoral list. The election process is continuous, allowing stakeholders to vote delegates in or out based on their performance and contributions to the network.

An important quality of this chain is the number of nodes needed to reach consensus[20]. Since these nodes are significantly long-term nodes the confirmation time is much shorter and thus increases transaction throughput. This is also a truly democratic consensus protocol.

One of the primary concerns with DPOS is again centralization, as the consensus process is concentrated on a small group of delegates. These delegates would hold significant influence over the network. Another issue is if a significant amount of people do not participate [32]. An article written by WhiteBit and the Solar Chain calls this voter Apathy. This would result in a few select people deciding the future of the chain. There is also the risk of collusion as the delegates could collude for their self-interest rather than the chain's interest. Chains like Solar, EOS and TRON use DPOS[23]

- Proof of Authority (PoA) - Proof of Authority (PoA) is a consensus mechanism that relies on the identity and reputation of validators. PoA networks designate a limited number of approved validators, much like DPoS, who are responsible for creating new blocks and validating transactions[33].

  In a PoA system, validators are typically known entities, such as reputable individuals or organizations, who are selected based on their trustworthiness and expertise. Their identities are often publicly disclosed, adding a layer of accountability to the network. Since the number of validators is limited, consensus can be reached quickly, enabling faster transaction processing times. PoA networks are less susceptible to attacks such as 51% attacks since malicious actors would need to compromise a majority of the validators(Doxxed) to manipulate the network.

  Obviously, the major disadvantage PoA relies on a centralized group of validators, which might affect decentralization. The selection of validators and their continued reliability are crucial.

- ### 1.2.4 Other Consensus Mechanisms

- Proof of Reputation (PoR) - PoR mechanism is split into two distinct variants, dealing with individual users and enterprises, each leveraging reputation as a core element of transactional integrity and network participation.

  For individual users, PoR is characterized by a participatory model where users rate each other, and a user's reputation is determined by the average of ratings received[26]. These ratings are not uniform; they are weighted by the raters' own reputational scores, introducing a nuanced layer of trust whereby the influence of one's rating is directly proportional to their standing within the network. This model is a community-driven approach to trust. The influence of a participant is shaped by their contributions to the ecosystem.

In the enterprise variant, PoR is a more centralized model wherein a designated authority assesses and assigns reputations based on objective, quantifiable metrics such as market capitalization and brand significance. Such a model ensures that enterprises engage with the DeFi space on terms that reflect their real-world stature and influence[26].

- Proof of Importance (PoI)- PoI represents a consensus mechanism that transcends the traditional metrics of stake size. Instead, it uses engagement and transactional activity as deciding factors in determining a participant's influence on the network. Unlike mechanisms that solely prioritize wealth or computational power, PoI evaluates the quality of a participant's interactions within the ecosystem, such as the diversity and frequency of transactions, and the network of connections established through these activities. This approach incentivizes meaningful participation[34].

  However, PoI introduces potential vulnerabilities, as it may allow actors to artificially inflate their importance through automated transactions or bots, potentially compromising the system's integrity with lower monetary risk than required by Proof of Stake. This emphasizes the need for robust safeguards and continuous monitoring to detect and mitigate such strategies, ensuring that the mechanism effectively balances inclusivity and security.

- Proof of Capacity (PoC)- Also called Proof of Space, Miners allocate a non-trivial amount of memory or disk space to solve a challenge. This is not as wasteful as PoS since it uses a method called Plotting to pre-generate chunks of data containing all the computations necessary and mining only requires the reading of this[31]. This is limited by the fact that space is not as costly as work. This reduces the attack cost. Users can just store a huge amount of data and gain a significant advantage.

- Proof of Burn (PoB)- This is similar to Proof of Stake but instead of staking, it works more like PoW by sending the coins to an irrevocable wallet never to be accessed by anyone again. This process is called burning. This is limited again by the fact that the rich will get richer and there is a risk of deflation[31]

- Proof of Elapsed Time (PoET)[35]- Developed by Intel it leverages TEEs in order to make validators prove that they waited the allotted amount of time. It follows a lottery system that gives every node the same chance. All the nodes have to do is prove that they waited for the given random amount of time. This random time is generated by TEEs which are trusted execution environments and can be cryptographically attested as to their proper functionality. The validator allotted the least time will win the lottery.

This chapter highlights the current issues with popular social media and the limitations of current blockchain consensus mechanisms. The following chapters will discuss where these two problems meet and will proceed to try and solve both these broad issues.

Chapter 2

Other Solutions

2.1 Battling Misinformation and Discord on Social Media

Social media has allowed misinformation to sow discord in the community. This is a problem recognized by many researchers and some have come up with solutions before broadly they can be categorized into the following,

- Transparent Content Moderation Policies - Social Media Platforms must clearly outline what constitutes misinformation on their platform. This will increase trust among users about the platform

- Enhanced Algorithmic Detection - Social media platforms have started to employ advanced algorithms and artificial intelligence to detect and flag misinformation[36]. For example, Instagram shows a disclaimer on some posts[37] saying this might constitute misinformation. Some platforms also allow the users to download their data for them to analyse why they are shown what they are shown.

- Fact-Checking Partnerships- Some social media platforms like Twitter and Facebook have partnered with independent fact-checking organizations to verify information shared on their networks[9].

- Community and User Engagement - Social media platforms can leverage user engagement to combat misinformation. The reporting feature allows users to flag false information, which is then reviewed by the platform's AI or third-party fact-checkers. Online communities that promote critical discussion and share accurate information can help counteract the spread of falsehoods

- Strict Legal Action - Governments around the world are exploring regulatory measures and policies to crack down on misinformation mongers. Funke et al. provide an account of different cases of action taken by different countries around the world.[38].

- Empowering and Incentivizing Individuals - Providing incentives to users would motivate them to flag misinformation. This can be done in the form of a reputation score or in-platform content that the user can display on their profile[9].

- Cross Platform Initiatives - The same misinformation can be spammed across multiple social media platforms. Once a platform identifies one piece of misinformation it can then share it with other platforms and increase their chances of weeding out the same misinformation. Platforms can also share strategies and technology.

The above-mentioned solutions work well but there is still a certain amount of centralization. Governments and Social media Platforms can impose their biases and motivations and deem some information to be misinformation or fake news. This is a threat to freedom of speech. AI also has the same flaw. This issue can only be solved by providing proper incentives to perform research, think critically and consume "hard" content or information. Only two kinds of incentivization are effective when dealing with users who are capable to form and change opinions, money and reputation. Decentralized Ledgers technology and its applications can provide both of these.

2.2 Decentralised Social Media

Decentralized Social Media or DeSo are the culmination of the two fields discussed in Chapter 1. Traditional Social Media faces a lot of criticism for the control the company has over its users. Social media like X, Facebook and Instagram all have their community guidelines. They have the authority to ban user profiles and posts, essentially they have complete control over the user profiles. At the heart of decentralized social media is blockchain technology, which distributes data across a network of computers, making censorship and data manipulation democratic. It supports a model of content ownership and control that is different from the centralized versions which form the basis for traditional social media platforms. Some experts feel censorship resistance is not a progressive step. Finn Miller writing to the DailyCoin calls free speech a double-edged sword which can lead to DeSo applications becoming a breeding ground for hate speech and cyber bullying[39].

Kietzmann et al. define essential features of social media[2],Fig. 2.1 depicts the essential features. Concerning blockchain-based social media or DeSo they have taken on new meanings.

- Presence: Presence refers to how available users are on social media and to what extent users know if others are available. On the blockchain, you can see and ping active nodes. Nodes which propose block and listen for transactions are currently active.

- Sharing: This refers to the extent to which people share receive or consume content, generally, DeSo and Traditional Social Media do not differ much in this aspect

- Relationship: This represents how users relate to each other. Is there a hierarchy or are all users the same? For example in traditional social media, you would have verified and normal accounts. Verified accounts are considered more credible. Based on purpose too there might be different

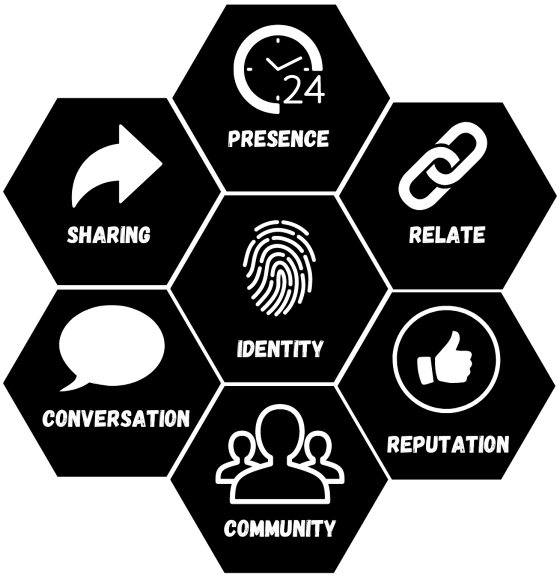


Figure 2.1: Social Media Functionality

roles, again in traditional social media there are content creators, moderators and users. In DeSo this can be modelled in the form of a reputation score or history

- Reputation: Though closely linked with Relationships, reputation is not always apparent. It refers to how much credibility or influence someone has on a certain social media. Verified accounts might not always hold that much influence. In DeSo this is based on the consensus mechanism employed.
- Identity: This is one aspect where there exists a stark difference between DeSo and Traditional Social Media. Traditional social media requires one to provide at least one source of identification seemingly as collateral. DeSo would be completely anonymised. Though there are criticisms about this aspect of DeSos, it continues to be the core principle.
- Conversation: This refers to the extent at which users are comfortable conversing with one another. If social media is toxic or filled with malicious actors, users will not readily converse with one another as the risk of starting a conversation is pretty significant. Another reason why users may be hesitant to start a conversation lies in how Identity is dealt with. For example, if a user wants to discuss something controversial that their friends wouldn’t agree with, they will be hesitant to do so for fear of real-life repercussions.
- Community: This refers to the extent to which users format and engage the community. This is also another aspect where DeSo and Popular Social Media do not differ much. Only in the fact that users will be more open to joining groups and communities if their identity is protected.

These features point out that DeSo fulfils all the properties which are integral to traditional social media. DeSo can prove to be a strong alternative to tradition social media, especially given the fact that when we apply some of its other properties such as integrity and the ability to provide incentives.

Table 2.1: Advantages and Disadvantages of DeSo vs. Traditional Social Media

Advantages of DeSo	**Disadvantages of DeSo**
User Privacy and Control: DeSo platforms prioritize user privacy and data ownership.	**User Experience and Adoption Challenges:** DeSo platforms often lack the streamlined and aesthetic user experience of traditional social median[39].
Resistance to Censorship: DeSo platforms are less susceptible to censorship, allowing for a broader range of opinions.	**Content Moderation Challenges:** Decentralized governance makes it difficult to moderate harmful content.
Security and Immutability: Blockchain offers a secure and tamper-evident ledger for transactions, once information is stored on it it lasts forever.	**Scalability Issues:** DeSo platforms can face scalability issues, such as high transaction fees and slow processing times.
Incentivization and Monetization for Content Creators: Users and creators can be directly rewarded for their contributions via cryptocurrency or tokens.	**Fragmentation:** Users may be spread across multiple small networks with limited interoperability, reducing reach.
Reduced Platform Control and Bias: Without a central authority, there is a reduction in platform bias and manipulation.	**Economic and Market Volatility:** The use of cryptocurrencies as an incentive causes volatility, affecting income stability for creators.

Table 2.1 shows the advantages and disadvantages of DeSo over traditional social media.

Though there are some disadvantages such as the difficulty of censoring and verification they can be addressed with other modifications to consensus algorithms that are already in practice. There are already some DeSo applications gaining traction. Table 2.2 compiles information about some popular DeSo applications.

Some of the main features of the mentioned blockchains are discussed below,

- Mastodon - An equivalent of Twitter, Mastodon is a decentralized ad-free social network. Users control what they want to see there isn't any recommendation algorithm. It works by making use of multiple communities which act as servers. Each server can make its own rules. They also allow cross-server following and conversations[40].
- Minds - Minds works on the Ethereum network, it introduced its own token, the minds token which users can use to support content creators or

Table 2.2: Comparison of DeSo Applications with Traditional Social Media

DeSo Application	**Hosted On**	**Equivalent Traditional Media**
Mastodon	Dedicated Chain	Twitter(X)
Minds	Ethereum	Facebook/Twitter(X)
Steemit	Steem Blockchain	Reddit/Blogging Platforms
Akasha	Ethereum	General Social Media
DTube	IPFS	YouTube
Peepeth	Ethereum	Twitter(X)
Subsocial	Polkadot	YouTube/General Video Hosting
Indorse	Dedicated Chain	LinkedIn
Sapien Network	Ethereum	N/A

even promote their own content. It is censorship resistant advocating free speech and includes news feed group chats and direct messages[39].

- Steemit - Steemit enables blogging on the blockchain, allowing users to publish, upvote and comment. It incentivizes users to create quality content. Users are rewarded based on the reach and engagement their posts receive[41].

- Akasha - Built on the Ethereum blockchain, Akasha champions freedom of expression and data ownership, providing a secure and open environment for sharing ideas. It rewards users for engagement again using its native token AETH[40].

- DTube - DTube is an alternative to the popular video-sharing platform YouTube. The functionality is the same just that DTube leverages IPFS(Inter-Planetary File System) which is peer-to-peer content hosting/storing network. Content creators are also rewarded for engagement. Another important factor that makes DTube special is that its User Interface is very similar to traditional platforms. [42]

- Peepeth - Peepeth is hosted on the Ethereum Blockchain. It is a microblogging platform where posts adopt the immutability of blockchains. This promotes thoughtful and mindful engagement as anything and everything one says can never be taken back. It is ad-free but takes a 10% cut from any creators profit. It accepts tips and allows users one free "Ensō"(equivalent to a like or an upvote) per [42].

- Subsocial - Powered by Polkadot, Subsocial is another video hosting platform which allows monetization through ads. It also allows users to stake in favour of their favourite content creators at no cost to their balance[42][43].

- Indorse - Indorse is a decentralized professional networking platform an equivalent of LinkedIn, utilizing blockchain technology to reward users for sharing skills and activities [42].

- Sapien Network - The Sapien Network is a decentralized "nation". It is called a decentralized parliament. It even gives users a passport. It allows users to build Decentralized Autonomous Organizations or DAOs on the chain itself. Users can post proposals for their organizations on the chain gain funding for it and start them all within the ecosystem. This is a one-of-a-kind platform which is a DAO which allows you to create more DAOs. It enables DeSo-based E-commerce and normal social media posts which can serve as updates from DAOs[42].

Chapter 3

Overview of the proposed Solution

3.1 Introduction

The proposed thesis intends to provide incentivization in order to promote scientific discussion and critical thinking. This incentivization can be provided through blockchains. Meanwhile as noticed from Chapter Chapter 1, popular consensus mechanisms are flawed in one way or the other. This thesis proposes the design of a DeSo Platform along with a chain it is hosted on which aims to solve both these issues.

The proposed solution must ensure these two broad goals:

1. To create an environment that promotes and incentivizes critical thinking and debate. This can be further split into these sub-goals:
   - To be able to provide a fair incentive for discussions
   - Encourage users to invest in their opinions
   - Encourage users to find scientific backing for their opinions
   - Anonymize discussions as it will allow people to speak their minds but also tie in accountability
2. Provide an alternative to the popular consensus mechanism instead of directly relying on buying capacity or coins owned. This can be achieved by providing people with an opportunity to scale up their resources to match people with access to a lot of computing power or purchasing power.

It is clear from the subgoals that one problem can be solved with another. This forms the essence of the proposed solution.

3.1.1 Reputation Scaled Proof of Stake Blockchain Which Incentivizes Scientific Research

In a Reputation-Scaled Proof of Stake model, the ability of a participant to validate blocks and earn rewards is not just determined by their stake (i.e., the amount of cryptocurrency they are willing to lock up as collateral) but also by their "reputation" within the network. This acts as a weight that is used to multiply their Stake or scale their stake. The reputation score can have a positive or negative effect on the effective stake.

$$\textit{Effective Stake} = \textit{Staked Cryptocurrency} \times \textit{Reputation Score} \tag{3.1}$$

This reputation is a dynamic score which represents the user’s history. Specifically, the reputation score of the proposed solution would reflect how good the participant is at choosing the side which most people consider to be rational. This can in turn incentivize discussion and cause people to agree or disagree with views. The details of determining this reputation score will be discussed in a later subsection.

Advantages

1. **Increased Trust:** By considering reputation as a factor for forming consensus, the system rewards participants who consistently act in the network’s best interest.
2. **Promotion of Quality Participation:** The model incentivizes constructive discussions and critical reasoning, as such activities directly scale one’s ability to participate in the consensus process and earn rewards.
3. **Decentralization and Fairness:** This model can mitigate unintended centralization like in traditional PoS systems, where wealth concentration can lead to disproportionate control.
4. **Community Building:** A reputation-based system fosters a sense of community and mutual respect among participants. This reputation score may even be considered a standard or something to take pride in, further incentivizing a scientific temperament.
5. **Anonymised Discussions:** Though it is sometimes important to know what biases have led to a particular argument, according to the developers of the Kialo Platform and Psychologists like Brewer, more often than not since there is no prejudice involved arguments have a higher chance of sounding reasonable if it comes from an anonymised source. Usually on social media, usernames, posts and other information can cause people to dismiss arguments from people who seem different [44][45].

Disadvantages

1. **Potential for Gaming the System:** Any system based on scores and other subjective metrics is susceptible to manipulation. Participants might find ways to increase their reputation scores through strategic voting, meaning participants may be more likely to vote towards the winning side rather than the side they believe in.
2. **Inclusivity Concerns:** Newcomers might find it challenging to build their reputation. This might lead to a system where established users hold disproportionate control.

3. **Subjectivity and Disputes:** Reliance on community voting and discussion outcomes to determine reputation can lead to disputes over the fairness of scores and adjustments.
4. **Hate Speech and Cyberbullying:** As discussed earlier hate speech and Cyberbullying might become prevalent in this network.

The concept of using a reputation score can be very advantageous but sometimes using a reputation score may lead to a Majority Tyranny or the majority might lean towards unscientific decisions and believe in baseless and unscientific opinions. The goal of this thesis is not focused on the result but on the process itself. The emphasis lies on discussion and not on the result. The result is merely a way to encourage users to discuss and challenge themselves. Still, it is important to discuss ethical considerations in a thesis that leans a lot towards fairness. Discussing the specifics of the model first will help us better discuss the ethical considerations. It also allows us to define what is the scope of this and the extent of the implementation. As this thesis proceeds, the fairness of each process described will be discussed extensively, wherever necessary.

3.2 Proposal specifics

3.2.1 System Overview and Requirements

The proposed decentralized platform must facilitate a democratic system which aims to encourage rational discussion and reward critical thinking. The issue here is that critical thinking is not quantifiable. The result of a majority vote is the next closest quantifiable goal. This would adjust the reputation score and essentially change or update a participant's influence in the network. Drafting requirements for the proposed solution will help understand it better before proceeding to the solution.

Functional Requirements

1. The system must allow selected users to initiate narratives/issues on the platform.
2. The system must allow users to either support or oppose the view presented.
3. The system must allow users to register votes.
4. The system must balance majority views and scientific opinion.
   (a) The system must provide sufficient weight to Experts in the field.
   (b) The system should be able to anonymously verify the credentials of Experts
   (c) The system must also allow users to vote for a limited number of Experts to be on the council.
5. The system must incentivize users to engage in rational discourse.

(a) The system must reward or penalize the user based on the winning or losing side.

(b) The system must reward Experts no matter the result.

Non-Functional Requirements

1. The system must ensure the security of all data and transactions.
2. The system must ensure that the status of issues is reflected across all the nodes and is verifiable.
3. Transparent voting and reputation calculation is essential.
4. The system should proceed normally when there are no issues to be discussed
5. The system must be scalable and ensure fast transaction processing

These are the basic functional and non-functional requirements necessary to actualize a system that would help solve the issue of social discord and lack of scientific reasoning

3.2.2 Actors and Use Case

To fulfil the requirements mentioned above, this thesis proposes an ecosystem with three actors - Delegates, Voters and Experts. Each of them contributes to the consensus in their own way. They are motivated by different goals but are still incentivized to behave in the best interest of the system. Fig. 3.1 shows the different Delegates in a use case diagram.

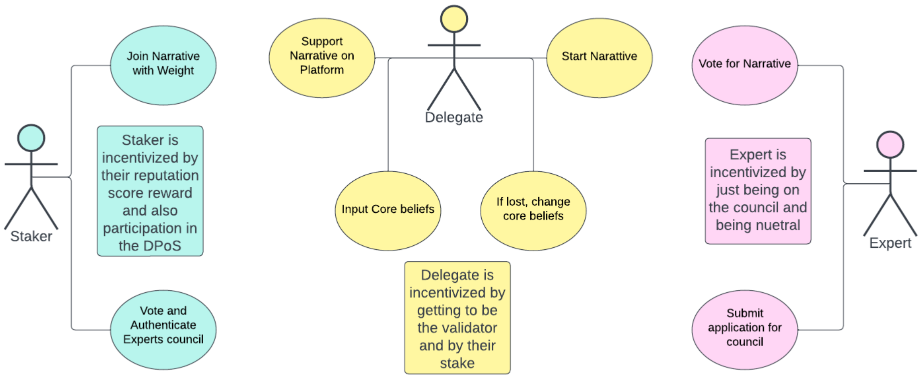

Join Narrative with Weight
Staker is incentivized by their reputation score reward and also participation in the DPoS
Staker
Vote and Authenticate Experts council
Support Narrative on Platform
Delegate
Start Narattive
Input Core beliefs
If lost, change core beliefs
Delegate is incentivized by getting to be the validator and by their stake
Vote for Narrative
Expert is incentivized by just being on the council and being nuetral
Expert
Submit application for council

Figure 3.1: Actors/Stakeholders and Use Cases

Delegates

The whole chain is built around these ’Delegates’, they are the crux and they decide the future of the chain. A decentralized system allows anyone with a certain amount of resources to become a delegate. They initiate discourse by championing issues for community discussion. They start the process by buying in an issue by staking some cryptocurrency on their chain. They are then provided with an issue ID which represents the issue and discussion. They can post information about it on the discussion forum attracting users and convincing them of their cause. The system can then have other Delegates who can either join the Issue/Narrative. Delegates can prove their identity by signing their messages with their private key proving to everyone that they are indeed the ones who invested in the issue they are championing.

Investing in the issue ensures accountability as it stops people from discussing trivial issues and only using the platform for issues that are significant and serious.

When buying in, Delegates formally lock in their stance on the blockchain. This immutable record serves as a commitment. After the voting process, Delegates who align with the consensus are rewarded, incentivizing the Delegates to find valid arguments for their side and put them forward in a convincing manner. Alternatively, Delegates whose positions are different from the community consensus are penalized through a stake loss and a loss in weight. winning Delegates can split the stakes of the losing stances and are also rewarded with an increased weight. This risk-reward mechanism drives Delegates to encourage rational debate amongst their Voters. Post-issue winning Delegates are also able to validate a block and split the reward with their users.

Voters/Stakers

As with any democratic process Voters or Stakers are the actors who hold the true power in the chain. Delegates would need to convince Voters to support them. Voters hear about an issue on the forum and register their initial vote which just from the face value of the issue. This helps them self-reflect on how their views and stances change as they come across new information. The initial vote also serves as a commitment to help vote for council members and participate in the final process. Any voter who participates in the initial voting and does not participate in the final vote will be penalized. The Voters then vote for Experts and add them to the council. Each stance would have a limited number of Experts so the Voters are forced to choose wisely. After electing the council Voters spend time discussing and reading arguments. After a stipulated amount of time has passed (typically represented by block count), they cast their final votes.

In case the voter’s stance aligns with the consensus they are rewarded with an increase in weight. They are also rewarded some money when their delegate validates a block later on. If the voter’s final stance is opposed to consensus their weights are decreased. This would encourage Voters to critically reason better.

Experts

Inside the ecosystem, Experts and the expert council play the same role that the judiciary plays in a democratic government[46][47].

> "As a non-political actor, the judiciary is supposed to base their decisions based on what is written in the law and not on what a politician tells them."[47]

Experts do not align with the majority and vote for the stance they feel is rational and scientific often considering their own research and experience. Experts bring to the table a level of specialized knowledge. They may or may not partake in the discussion. They suggest themselves on the chain and after verification and voting they are added to the council. Though the council is a much smaller subset than the rest of the Voters, they hold significant influence over the result. Post discussion the Experts are rewarded with crypto-currency just for being on the council. They also get a minor weight increase. This rewards the Experts for just being on the council and being true to their experience and research.

Chapter 4

Implementation Details

Since all the preliminary details are established, the next step is implementing the solution and fulfilling the requirements.

4.1 Use of smart contracts and Tokens

Most DeSo applications are hosted on established chains. Though they use these chains as a backbone they do not change the chain itself much and only use it for transactions. A major disadvantage to this is the gas fee in most chains. Gas fee is the fee transaction senders need to pay the validators to compensate for the resources for executing a smart contract[48]. The gas fee(which is a fractional denomination of the currency involved) is determined by network capacity. Scalability is another metric that is directly linked to gas fees. With the influx of a lot of transactions, it makes the chain take longer to process transactions.

Using an ERC20 token or other token also limits you in what you can do with the tokens. For example, ERC20 has only 6 basic functions which must be implemented in the suggested fashion[49]:

- `totalSupply`: Provides information about the total token supply.
- `balanceOf`: Returns the number of tokens that a specific address holds.
- `transfer`: Used to transfer tokens from the total supply to a user. something like an initial public offering.
- `transferFrom`: Used to transfer tokens from one user to another.
- `approve`: Lets a user approve another address to withdraw a specific amount of tokens from their account.
- `allowance`: Remaining number of tokens that an approved address is approved to withdraw from a user’s account.

Since this solution requires a lot of customization in the chain and would need to be scalable, implementing it from scratch is the better option. As for the programming language used, Python was the best option. Python was used as it is very versatile and has a very active community.

4.2 Implementating a Proof of Stake Blockchain

The first part of the implementation was to implement a proof of stake blockchain as the DeSo application can only be built on top of it. Inorder to do this once again it is necessary to formulate a set of functional requirements, this time to define the scope of the chain. This would be a proof of concept implementation(not be confused with any consensus mechanism) nevertheless, it will integrate all the basic functionality a proof of stake blockchain provides. Any extra security measures other than what is necessary for the basic definition and crucial concepts will not be implemented and are considered out of scope for this thesis.

1. The system must allow users to create new transactions and broadcast them.
    - The system must also allow users to maintain a transaction pool with unresolved transactions
2. The system must enable the creation of new blocks through the Proof of Stake consensus mechanism.
    - Creation of a new block must execute and validate the transactions.
3. Validators must be selected based on their stake and "participation" in the network.
    - Stake is scaled by user’s weight/reputation score.
    - Delegates must also be able to be considered validators.
4. The system should implement a method for validators to propose new blocks when chosen.
5. The blockchain must validate transactions and blocks according to predefined rules before appending or accepting them to their version of the chain.
6. The system must implement a reward mechanism for validators who successfully propose a new block.
7. Nodes must be able to join and leave the network and still follow the common prefix rule and ideally reach the same consensus after certain rounds
8. The system should provide a secure way to stake and unstake tokens.

These functional requirements must also be implemented along with the requirement listed in Chapter 3. The thesis will now proceed to discuss in detail, the implementation specifics. Fig. 4.1 represents the activity diagram for reference.

4.3 Transactions

The transaction class is the fundamental building block in the implementation. Each transaction has the following attributes:

- `senderPublicKey` This would represent the public key of the sender. This is the user who creates the transaction.

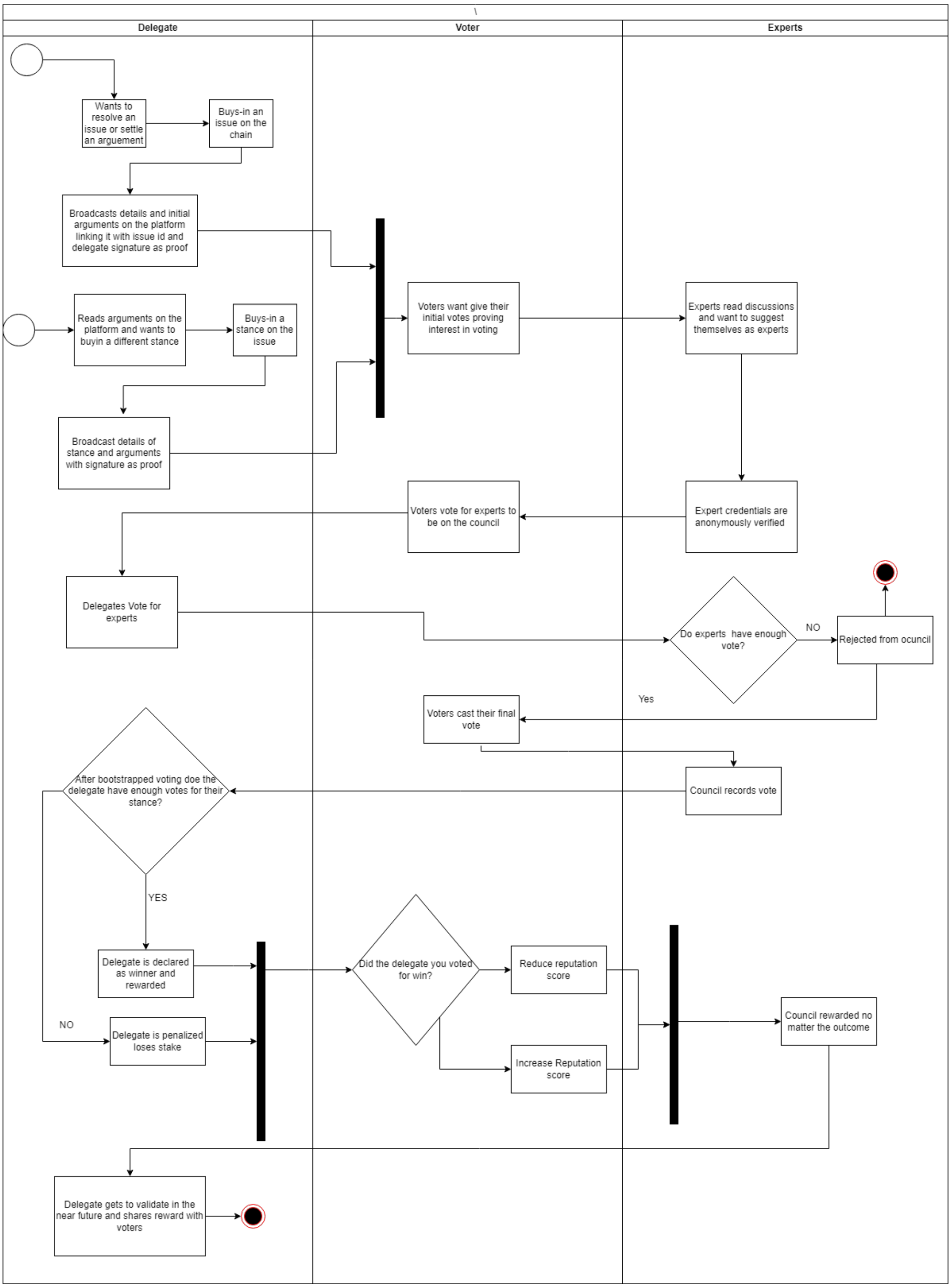

\
Delegate
Voter
Experts
Wants to resolve an issue or settle an arguement
Buys-in an issue on the chain
Broadcasts details and initial arguments on the platform linking it with issue id and delegate signature as proof
Reads arguments on the platform and wants to buyin a different stance
Buys-in a stance on the issue
Broadcast details of stance and arguments with signature as proof
Voters want give their initial votes proving interest in voting
Experts read discussions and want to suggest themselves as experts
Expert credentials are anonymously verified
Voters vote for experts to be on the council
Delegates Vote for experts
Do experts have enough vote?
NO
Rejected from ocuncil
Yes
Voters cast their final vote
Council records vote
After bootstrapped voting doe the delegate have enough votes for their stance?
YES
NO
Delegate is declared as winner and rewarded
Delegate is penalized loses stake
Did the delegate you voted for win?
Reduce reputation score
Increase Reputation score
Council rewarded no matter the outcome
Delegate gets to validate in the near future and shares reward with voters

Figure 4.1: Activity/Flow Diagram

- `receiverPublicKey` This represents the receiver of the transaction. This can in some cases be the same as the sender.
- `amount` This represents the amount transferred
- `timestamp` Represents the timestamp of when the transaction was created.

- `signature` This is the cryptographic signature of the sender, encrypting the whole payload of the transaction with their private key.
- `id` This is a UUID(Universally Unique IDentifier) generated by the creator such that this transaction cannot be repeated. Prevents double spending
- `type` This is where this implementation strays from the standard proof of stake implementation by using different types of transactions to ensure different functionality of the DeSo.
- `tag` This is a general-purpose field which is used to record the stance users want to vote for.

Table 4.1: Transaction Types and Their Validity Checks

Transaction Type	**Functionality**	**Validity Checks**
EXCHANGE	Allows cryptocurrency to be sent from the total supply to users.	Valid if initiated by the Genesis account.
TRANSFER	Transfers currency between users.	Sender must have sufficient balance.
STAKE	Users lock cryptocurrency as stake. This lets them compete to validate a new block.	Amount $\geq$ minimum amount; sender equals receiver.
RETURN	withdraw staked currency, affecting validation chances.	Receiver equals sender; the staked amount is sufficient.
BUYINFIRST	Initiates a new issue or proposal with a minimum stake.	stake $\geq$ minimum requirement.
BUYIN	Participates in an issue by staking.	Issue exists; stake $\geq$ minimum stake; sender not already a participant.
VOTE	Initial voting on an issue or proposal.	Issue exists; in INIT-VOTING stage; sender has not voted.
SUGGEST	Nominate oneself as an expert for the council.	Issue in COUNCIL-SUGGEST stage; sender not already suggested.
EXPERT-VOTE	Elect Experts to the council.	Issue in COUNCIL-VOTE stage; sender voted initially; expert already suggested.
FINAL VOTE	Locks in final stance on an issue for consensus.	Issue exists; in FINAL-VOTE stage; the sender hasn't locked in the vote.

The transaction class has functions which help with processing any object of this class. The payload function lets a user just pick the payload of the transaction(everything except the signature field). The transaction creator(sender) can encrypt the hash of this payload with their private key and add it to the signature. It also allows the nodes receiving the transaction to verify if the signature is valid by decrypting the signature using the sender's public key and comparing the hashes. Every time a transaction is received, a function is called to checks if the UUID is already used ina the transaction before preventing double-spending.

In a traditional Proof of Stake chain, a transaction would only be used to transfer crypto-currency from one account to another, but in this implementation, it is used to interact with the chain in multiple different ways. Table 4.1 shows short descriptions of each transaction type. Each transaction also has certain checks in place to see if it is covered (required before executing a transaction), these checks are shown next to each transaction type

The tag field is usually a dictionary and has two keys usually `issue_d` and `stance` this helps filter information and execute the transaction. This tag is not needed for some transaction types.

Code snippet 4.1 shows an example transaction object. This is a final vote transaction. So the sender and the receiver are the same public key and the amount is allowed to be set to zero. The tag represents a UUID equivalent to the issue and the stance key in the tag is used to register the final vote to the given stance.

Listing 4.1: Transaction example

```
{
"amount": 0,
"id": "231d29e5e3e111eea8e4982cbc0b3f0a",
"receiverPublicKey": "-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4
    AMIIBCQKCAQBms2NvW+1B23aaZD7mboBU CqUUhOmbK6WBq9glsG94sOmzsdo3Z5u/IYt2k2
    tdZrFUKLUZKabVH1lLxyO7YZgT K+M2ux4HnFQVvDEcEbwLPe3d6wFog01f3LTtiQxj+
    TFpQdUcQccHXmqhWlGvOCEn FpEf4sLtF8Bj16eZ2RPL7/nvweHEKEws+s7qzB4KVdb+4VoU0W2Et4
    eUuD/gknTp LLXozMcXjYEkiOhHKHftJveAClPQqsJT9i9tZgEC66Edjz64CyGJTmuEd0OJREtT o8
    Psi8p2kvrkzW/cMsnNDqKk5aQMfxKoxP1oTguymmcl/om0uvU7HKwBx+/ZXb4Z AgMBAAE= -----
    END PUBLIC KEY-----",
"senderPublicKey": "-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4
    AMIIBCQKCAQBms2NvW+1B23aaZD7mboBU CqUUhOmbK6WBq9glsG94sOmzsdo3Z5u/IYt2k2
    tdZrFUKLUZKabVH1lLxyO7YZgT K+M2ux4HnFQVvDEcEbwLPe3d6wFog01f3LTtiQxj+
    TFpQdUcQccHXmqhWlGvOCEn FpEf4sLtF8Bj16eZ2RPL7/nvweHEKEws+s7qzB4KVdb+4VoU0W2Et4
    eUuD/gknTp LLXozMcXjYEkiOhHKHftJveAClPQqsJT9i9tZgEC66Edjz64CyGJTmuEd0OJREtT o8
    Psi8p2kvrkzW/cMsnNDqKk5aQMfxKoxP1oTguymmcl/om0uvU7HKwBx+/ZXb4Z AgMBAAE= -----
    END PUBLIC KEY-----",
"signature": "310c2fcf87e9189d2f1cf0457e3b79234796eecd6728e9f0e24277a4d94a0c4f54
    feaed7765162e4fe21aa20465e0f66358670143655af91c6cb382da44587693fefea08f8865a6750
    0ca093df7bc7153f6a4b5bb16a0881b0f062e57fa1370bc628759bb7c81f9ec0b6a1ed6f781f842
    912ee134ee6061bf4463891cbb6b90048cf36dfaf905c1fba4d999f1af61e89aca37646d643e42e
    386659f6849fff08b89b85fd928f42485a2de7294d61ca94e7f72b01c09a8eb6c0b831030a3f55
    da64438371d8a7e5bee69eefc956140642a2c23291b4d242a2a39847b6ade5fe0ef9cfe4578e4
    efff807a185f40782042ab0e57ab4a737acd8b26b1118585f3584b",
"tag": {
```

```
"issue_id": "951a3bc5-9f04-3c94-5847-b09b0f7c3742",
"stance": 0
},
"timestamp": 1710626659.1324644,
"type": "FINAL-VOTE"
}
```

4.3.1 Transaction Pool

The transaction pool is a simple subclass which is a temporary place to store transactions until they are added to a block and eventually the blockchain. It is important as it signals to the blockchain that it has enough transactions to forge a block. After forging the transitions that are a part of a block are removed from the pool.

4.4 Blocks and Blockchain

The blockchain as discussed before is an append-only data structure which contains objects called blocks. These blocks are chained or linked to the blocks before by using the hash of the previous block in its header. Each block has the following attributes

- `transactions`: A list of transactions that are included in the block.
- `lastHash`: The hash of the previous block in the chain.
- `timestamp`: The time at which the block was forged.
- `forger`: The public key of the node that successfully validated the block.
- `signature`: A cryptographic signature generated by the forger's private key by hashing and encrypting the block(without the signature).
- `blockCount`: A number that represents the block's position within the blockchain. It increases with every block and can be used to check if the received block fits in next.
- `posHash` and `accHash`: Unique identifiers for the current state of the Proof of Stake mechanism and the account model. Inspired by the idea behind the Komodo chain[50] which uses Litecoin to double verify its transactions. These hashes are used to keep track of the weights of various users and the state of different issues currently. This helps increase the scalability of the chain as only transactions are validated and blocks contain the Consensus state and other information. The hashes would help validate the received information.

The genesis node would begin with generic the starting hashes "first hash". The last block hash changes with every block while the `posHash` and `accHash` change when there is a change in the respective objects. Code snippet 4.2 shows the second block of an example chain (with its transactions minimized).

Listing 4.2: Blockchain blocks example

```
"accHash": "8655bd572f3f5e48b77267b26f718867dadbbf01eda6b37079cb4c31539435f1",
"blockCount": 2,
"forger": "-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpQ2c9
    UvIiDOdU4i4yZG0Swyf2 8ylVMePPSTL0Lqh3Z8gcorYbMLEalUjXPIvuIcdRzjzVUDFt9wWPE4m0
    InaZH/ul USpEiWpX6zbkrcXsSnVg6v4gHROrYoE0ZkvmuVUAKr/KhXe3S6SN75WQABJG9Ew9 JhG1
    hlWvS9TiCqIr6QIDAQAB -----END PUBLIC KEY-----",
"lastHash": "4998e39f9f2e3867d653d2055e86a68a2a7f0228870350214ab5fb2e7a7c4e45",
"posHash": "0c6017eb13871480f691d021197d6226b30bab3876100e56f1ef64ffbc38f5ac",
"signature": "0417ca1374542fa424de7e934f8a68659920f96ad4bfc8a556440e31b583fdb795be2
    e9a69fc097ee829d6fee0a5b4d5f9a7c0a1b396f67345674e0cb68807f6e7e4133ccf9587fc64a9
    fbc0e63108dd1f9a93b1d44784ca75a11a1ca8e4f545756a71f7253430c2f40c769ff3bdf54feff
    028111975e515439ca55169a7fc85",
"timestamp": 1710626565.7212358,
"transactions": [3 items]
}
```

When receiving a block the validity of the following fields is also ensured:

- Block Count
- Last Block Hash
- Proof of Stake Hash
- Account Hash
- Validity of transactions
- Signature Validity
- Forger Validity

In case the Block Count is lesser the node requests the blockchain from the previous forger. This ensures requirement no.7 listed in Section 4.2 (Nodes must be able to join and leave the network). When receiving the blockchain this check is done for every block on the received chain.

The Proof of Stake object and the Account Model objects are both objects of the blockchain so when the blockchain is broadcasted/received the entire Proof of Stake object and the Account Model object are received.

4.5 Account Model

The account model is a very simple and basic class. It contains a list of account identifiers (public keys). It contains three other dictionaries which all use the account identifier as keys. The balance dictionary keeps track of an account balance and the weight dictionary maintains the weights. The `participatedIssues` dictionary keeps track of the issues participated. It also stores the history of balances and weights in another dictionary. The model has a function incorporated which will has the object along with a list of hashes of previous states. This is what is added to the account model hash in every block.

4.6 Consensus - Reputation Scaled Proof of Stake

Now that all the auxiliary information is defined, discussing how the core of this thesis is implemented will be a simpler task. The system would have to work in two different states. One that resolves the final stages of issues and another which is a scaled proof of the stake chain. It is important to understand that the base state is the scaled Proof of Stake and only once in a while issues are resolved. Before discussing the implementation of issue resolution, we discuss how Proof of Stake is implemented in the chain.

The first step in initializing the Proof of Stake process is to set a genesis node stake. This stake is constant. As there must at least be one Staker in order for the chain to function. The genesis node is the perfect candidate for this. One shortcoming of this is that the genesis node must always be online(at least until the chain gains popularity. Now it is imperative to discuss the execution of the `Stake` Transaction.

4.6.1 Staking

The `Stake` Transaction allows users to stake crypto-currency. The stake must be more than the reward gained by validating. If the stake is larger the transaction is accepted and executed. The sender and the receiver are the same wallets for staking. There is no need for a tag here. The stake is then recorded in the `ProofOfStake` object under the Stakers dictionary using the public key of the wallet as the dictionary key. Users can view their stake and their effective stake. See equation Eq. (3.1).

4.6.2 Forger Selection

Every time a new transaction is broadcasted or added to the transaction pool the forger function is called in every node. This triggers the creation of a `validatorLots` this is a dictionary with each account's effective stake. Then the system checks if there are any Delegates to be rewarded if not it proceeds to pick an account from the `validatorLots`. The chances of being chosen are weighted by the effective stake. This is achieved by normalizing the effective stake with respect to the total available stake. This normalized effective stake is considered to be the probability of being chosen.

Consider a set of validators $V = \{v_1, v_2, \ldots, v_n\}$, where each validator v_i has a stake s_i and an account weight a_i. The effective weight W_i for each validator v_i is given by the product of its stake and account weight:

$$W_i = s_i \times a_i, \quad \text{for } i = 1, 2, \ldots, n \tag{4.1}$$

The total effective weight T is the sum of the effective weights of all validators:

$$T = \sum_{i=1}^{n} W_i \tag{4.2}$$

The normalized weight w'_i for each validator v_i is then calculated as:

$$w'_i = \frac{W_i}{T}, \quad \text{for } i = 1, 2, \ldots, n \tag{4.3}$$

The selection of a winner validator, v_{winner}, is performed by randomly choosing a validator with probability proportional to its normalized weight.

$$\Pr(v_{\text{winner}} = v_i) = w'_i, \quad \text{for } i = 1, 2, \ldots, n \tag{4.4}$$

A slight hitch in the implementation was that this process is to be performed across all nodes. A true random function across all nodes will generate different results for different iterations. This would throw nodes out of consensus. Fortunately, python's random function allows setting a random seed. Random seeds initialize a pseudo-random generator making it random but predictable with a given seed. This bypasses the issue of multiple nodes using different random number generators. Moving forward all random functions will use a set seed. For this implementation, the seed will be based on the last block hash.

4.7 Consensus - Resolving Issues

This section will in detail discuss the issue resolution process. The consensus process is divided into stages as shown in Fig. 4.2. The first two states are triggered by transactions while the others are triggered based on block count which helps calculate the number of blocks that have been forged.

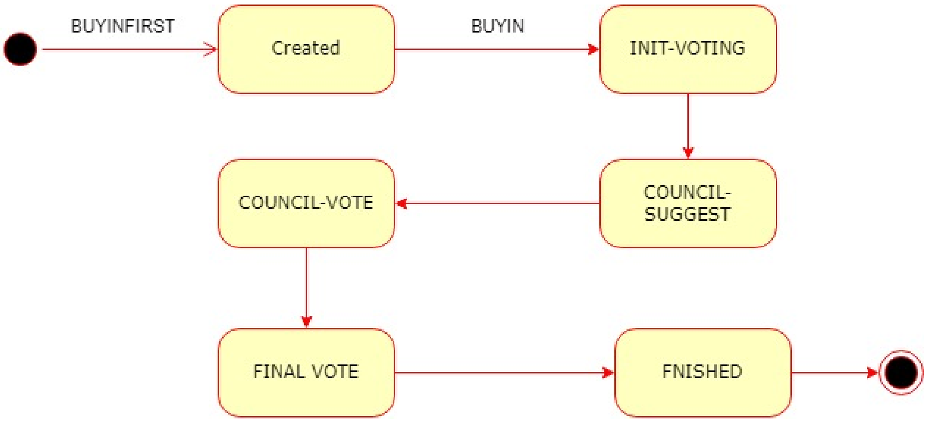


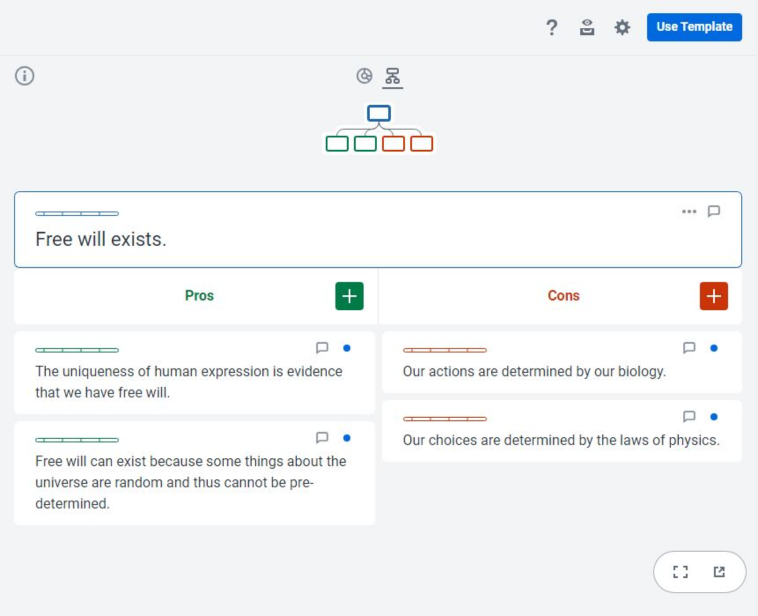
Figure 4.2: State Machine Diagram

4.7.1 Buying in an Issue

When a user wants to discuss an issue that they are passionate about or they are sure they have a lot of support they can buy in an issue on the chain using the `BUYINFIRST` transaction. There is a minimum buy-in amount set to start an issue. If the user has a sufficient account balance, the amount is staked in the issue and the issue is started. A random UUID is assigned to represent the issue and the Delegate who started the issue is assigned the stance 0. The delegate can then broadcast the issue on the discussion forum and put in their initial arguments. The delegate could on the platform hash and sign messages using their private key to prove that they are indeed the delegate who bought.

4.7.2 Discussion Forum

The discussion forum is an important part of the system but is out of scope for implementation as there are multiple forums available which encourage open discourse. One prominent forum that is a forerunner in enabling open discourse is Kialo[45].



Free will exists.

The uniqueness of human expression is evidence that we have free will.

Free will can exist because some things about the universe are random and thus cannot be pre-determined.

Our actions are determined by our biology.

Our choices are determined by the laws of physics.

Figure 4.3: Snippet of the Kialo Platform [45]

They allow discussion of issues in an anonymous and progressive manner. Each issue has two sides supporting and against. This can later be adapted to serve this implementation. The platform allows each of the supporting arguments to also be refuted or accepted. Again these supporting arguments can also be supported further or refuted. This creates a sort of recursive argument which allows users to explore, support or contend each fact used as part of the argument. This tree structure is very useful in allowing users to navigate complex discourse. The Kialo platform also recognizes possible duplicate entries and clubs them together. This is easier and only allows new arguments. The platform also allows users to rate relevancy. Arguments and statements which are voted highly relevant are displayed on top. Fig. 4.3 shows a snippet of the platform.

4.7.3 Entering an Issue That is Already Bought

After users hear about an issue on the forum if they do not agree with it, they can stake an equivalent or more amount on the chain and buy in an opposite stance / alternate stance. They can post a `BUYIN` with a tag which would contain the issue ID, if they want to join an already bought stance they can do that by adding the stance field too. If the user has sufficient balance it is then staked in that stance. Then the new delegate can also go on the platform and discuss providing their private key signature as proof.

4.7.4 Initial Voting

The initial voting is implemented using the `vote` transaction type. Everyone on the chain except the Delegates is allowed to vote. One account cannot vote for multiple stances and Delegates by default are considered to have voted for the stance they bought. Initial voting is a commitment. This allows only these select people to participate in the further stages. This can also be used for the rewarding purpose which will be discussed in a later section.

4.7.5 Suggesting to Council

Experts who notice that an issue could benefit from their expertise can also suggest themselves at the cost of no cryptocurrency. They would definitely have to prove their expertise. The Experts must try to prove their credentials anonymously. One option is to trust a central authority which can let Experts validate their credentials. Users can then go on to this platform and check if the delegate has the credentials they are claiming to. The platform could post anonymous credentials and certificates with redacted information. This sounds like a good option but unfortunately, this is against the principle of a decentralised system. This is another issue that has been researched a lot in the past decade. This issue falls under the umbrella of anonymous credential verification.

Anonymous and Decentralized Qualification Verification

Zero Knowledge Proofs are techniques which prove a statement without revealing any information about it[51][52]. Though it seems like an abstract concept, Zero Knowledge Proofs exist, especially one for this use case. Saleh et al. in 2020 proposed the use of Hyperledger Fabric to maintain and verify certificates[53]. Again the next year in 2021 they proposed another decentralized verification system that maintains privacy across different levels, such as Issuer(Universities), Owner(Students or in this case Experts) and Verifiers(Employers or in this case Voters on the chain)[54]. Other solutions also allow the issuing of certificates and verifying them decentrally[55][56]. A slight modification of any of these would work to anonymously or at least decentrally verify credentials. For example, these chains could provide an Asymmetric key pair to verified accounts and list the public key on their chain. Allowing users to check if the owner indeed has their credentials verified

4.7.6 Voting for the Council

Voters who voted initially on the issue are allowed to vote suggested Experts to the council. An expert needs to have a certain minimum amount of votes to be voted on to the council. Delegates can also vote for Experts. It is important to note that these votes are also affected by account weights and Voters can vote for more than one expert. The total number of Experts per issue is also limited. The size of the council is determined by the number of people who voted initially. The users must be stringent in their choices. Experts who have the most votes are voted into the council.

4.7.7 Final Vote

This is the most crucial part of the chain/system yet. The final vote needs to fulfil requirement 4 listed in Chapter 3, the system must balance majority views and scientific opinion. This means that even though the expert council is a smaller group than the Voters their influence must somehow be scaled to balance the majority.

To solve this the system proposes a bootstrapped voting system, which does the following,

1. Choose a certain number of Voters
2. Choose a certain smaller number of council members
3. Calculate the votes of this small sub-group
4. Repeat this process, with replacement for council members and without replacement for Voters
5. The process is repeated until all the Voters are exhausted.

4.7.8 Mathematical Modeling

Let,

$$
\begin{aligned}
S &= \{s_1, s_2, \ldots, s_k\}, \text{ Set of stances} \\
V &= \{v_1, v_2, \ldots, v_n\}, \text{ Set of all eligible Voters} \\
\Omega_{v_i} &= \text{ Weight of voter } v_i \\
S_{v_i} &= \text{ Stake voter has voted for} \\
C &= \{c_1, c_2, \ldots, c_m\}, \text{ Set of council members, where } C \subseteq V \\
\Omega_{c_i} &= \text{ Weight of council member } c_i \\
S_{c_i} &= \text{ Stake council member has voted for} \\
A_{s_i}^{(r)} &= \text{ Cumulative weight of stake } s_i \text{ in round r}
\end{aligned}
$$

$$N_v = \text{ Number of Voters selected per round}$$

$$N_c = \text{ Number of council members selected per round}$$

$$W = \{w_1, w_2, \ldots, w_r\}, \text{ Winning stances per round}$$

$$\rho = \frac{N_v}{N_c}, \text{ Ratio of Voters to council members per round}$$

$$\rho > 1, \quad N_v > N_c$$

The final voting process is as follows,

1. Initialization: $W = \emptyset$ and determining ρ. ρ is maintained above 1 as the system must still favour the majority but the larger the value the more it strays from the balance of expert/scientific opinion.

2. For each round until all Voters are represented or for R number of rounds:

   $$R = \left\lceil \frac{|V|}{N_v} \right\rceil, \text{Number of rounds}$$

   $$V_r \subset V, \quad |V_r| = \min(N_v, |V|), \quad V_r \text{ chosen randomly from } V,$$

   $$C_r \subset C, \quad |C_r| = \min\left(N_c, \left\lceil \frac{|V_r|}{\rho} \right\rceil\right), \quad C_r \text{ chosen randomly from } C,$$

   $$V = V \setminus V_r, \quad V_r \text{ is not replaced}$$

   Note: If for the last round of voting $|V_{\text{remaining}}| < N_v$, all remaining Voters are selected, and N_c is adjusted to maintain the ratio ρ, rounding N_c to the nearest higher Natural Number:

   - If $|V_{\text{remaining}}| < N_v$, then $V_r = V_{\text{remaining}}$.
   - The new N_c is calculated as $\min\left(N_c, \left\lceil \frac{|V_r|}{\rho} \right\rceil\right)$ to ensure ρ is maintained or adjusted according to the remaining Voters, rounded to the higher value to comply with $\rho > 1$.
   - n_v and n_c are the actual number of Voters and council members selected
   - Once again to maintain consensus the random number generator is initialized using the last block as seed.

   (a) Each participant casts weighted votes towards stances in S.

   $$A_{s_i}^{(r)} = \sum_{v \in V_r} \Omega_v \cdot \delta(S_v, s_i) + \sum_{c \in C_r} \Omega_c \cdot \delta(S_c, s_i) \tag{4.5}$$

   where $\delta(x, y)$ is defined as:

   $$\delta(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

(b) Determine the stance s_i with the highest cumulative weight in the round:

$$s_{\text{winner}}^{(r)} = \arg\max_{s_i \in S} A_{s_i}^{(r)}$$

Where:

- $S = \{s_1, s_2, \ldots, s_k\}$ represents the set of all possible stances.
- $A_{s_i}^{(r)}$ represents the cumulative weight of stance s_i in round r.
- $\arg\max$ function is used to select the stance s_i that maximizes the cumulative weight $A_{s_i}^{(r)}$.

(c) Update W with the winner of the round: $W = W \cup \{s_i\}$.

3. Determine the final winning stance s_{final} with the most wins across rounds:

$$s_{\text{final}} = \text{mode}(W)$$

4.8 Incentive Scheme

The Incentive scheme is different for different roles in the system. The goal of the incentive though is common to all actors regardless of their role. The goal is to encourage critical reasoning and ration discourse,

4.8.1 Delegate

The winning Delegates are rewarded with an increase in their weight while the losing Delegates get their weights scaled down. Winning Delegates also get to be the validator in the immediate future. The reward earned may also possibly be split amongst their Voters. Winning Delegates split the stake of the losing stances and share them according to their stance. This is modelled by the following equation,

- D: A set containing all Delegates, where $D = \{d_1, d_2, \ldots, d_N\}$.
- W: Subset of D, containing winners $W = \{w_1, w_2, \ldots, w_M\}$.
- L: Subset of D, containing losers $L = D \setminus W$.
- A_d: Amount contributed by delegate d.
- T_w: Total amount contributed by winning Delegates.
- T_l: Total amount contributed by losing Delegates.
- R_w: Reward for a winning delegate.
- α: Weight scale for adjustment, $\alpha > 3$.

1. Calculate the total amount contributed by winning Delegates (T_w) and losing Delegates (T_l):

$$T_w = \sum_{w \in W} A_w,$$

$$T_l = \sum_{l \in L} A_l.$$

2. For each losing delegate $l \in L$, divide their weight by α

3. For each winning delegate $w \in W$:

- Multiply their weight by α.
- Increase their balance by their contribution amount (A_w).
- Calculate their reward based on their contribution proportion to the total winning stake:

$$R_w = \left(\frac{A_w}{T_w}\right) \times T_l.$$

- Update their balance by R_w.

4.8.2 Expert

For each council member $c \in C$:

- Scale up their weight by β. Where β is modelled as

$$\beta = \frac{\alpha}{3} \tag{4.6}$$

- Update their balance by a fixed value, incorporating β for balancing.

4.8.3 Voters

For each voter who supported the winning stance, scale up their weight by γ, representing the adjustment. Where γ is modelled as

$$\gamma = \frac{\alpha}{2} \tag{4.7}$$

For each voter who supported the other stances, scale down their weight by γ.

4.9 Conclusion

All the above-given functionality is part of the proof of stake class which contains the data structure necessary for implementing the proposed consensus. The consensus is also verified using the PoS Hash discussed earlier as part of the Block and Blockchain section of this Chapter.

This chapter discussed the details of implementation of both a basic proof of stake and an issue resolution platform. Through thoughtful design, this chapter has laid down plans for a DeSo platform that promotes critical reasoning and is socially responsible as well as inclusive. The proposed solution makes full use of the potential of blockchain technology especially in revolutionizing online discourse making it democratic, transparent and meaningful.

Chapter 5

Sample Use Case

5.1 Introduction

This brief chapter will explain a very simple example use case of the implementation to better understand the proposed solution. The chapter for the sake of brevity would feature the inputs and the final output and try to connect the dots. The Appendices will contain all intermediary snippets for those who want to better understand the process. The example use case starts up four nodes each with a different key, one node using the Genesis key, one node using a Staker key which will represent a user trying to stake and win normally and two nodes using two different keys tagged Delegate1 and Delegate 2.

5.2 Wallet Creation

Wallets are created using the `Wallet` class by default a key pair is created for this but in case the user wants to provide a key pair they can do so by using the `Wallet.from Key()` function. For the use case, we create the following wallets:

- A **Genesis Wallet** to initiate the system and distribute the initial currency supply.
- Two **Delegate Wallets** representing users who will initiate and participate in issues.
- A **Staker Wallet** to represent a regular user participating in staking to validate transactions and blocks.
- Three **Voter Wallets** to represent users who will vote on issues bought by the Delegates.
- **Expert Wallets** to represent subject matter Experts who might be suggested and voted onto councils.
- Dummy wallets Alice and Bob to further block count.

5.3 Transaction Creation

Transactions are created to simulate various activities within the network, such as currency exchange, staking, issue creation, and voting. The `postTransaction` function encapsulates the process of creating and broadcasting transactions to the network. Depending on the type of transaction (`EXCHANGE`, `STAKE`, `BUYINFIRST`, etc.), different parameters may be required, including a `tag` for transactions related to issues and voting. Table 5.1 compiles the transactions used in this use case. Some transactions are skipped, because all they contribute to is block count progression and eventually issue stage progress. The sample use cases see one Staker staking some coins for a chance of getting validated. It then proceeds further when a delegate buys into an issue. Another delegate buys in an alternate stance. After which Voters vote for their initial stance. Initially, there are two Voters for Stance 1 and one voter for Stance 0. Then three council members suggest themselves and Voters then vote for them essentially adding them to the council. After a 'discussion' one voter changes their stance. Now there is one voter backing stance 1 and two Voters supporting stance 0. The Experts then vote for issues, in the same distribution two Experts for stance 0 and one expert for stance 1.

Table 5.1: Transactions As Part Of Sample Use Case

Block #	**Transaction Type**	**Details**
1	EXCHANGE EXCHANGE EXCHANGE	Genesis to Delegate1, 100 tokens Genesis to Delegate1, 100 tokens Genesis to Staker, 106 tokens
2	STAKE TRANSACTION TRANSACTION	Staker stakes 5 tokens Staker sends 50 tokens to Delegate1 Staker sends 1 token to Delegate1
3	BUYINFIRST EXCHANGE EXCHANGE	Delegate1 starts an issue with 104 tokens Genesis to Staker, 100 tokens Genesis to Staker, 100 tokens
4	EXCHANGE EXCHANGE BUYIN	Genesis to Delegate2, 201 tokens Genesis to Delegate2, 202 tokens Delegate2 buys into the issue, 106 tokens, stance 1
5	VOTE VOTE VOTE	Voter1 votes on the issue, stance 1 Voter2 votes on the issue, stance 1 Voter3 votes on the issue, stance 0
7	SUGGEST SUGGEST SUGGEST	Expert1 suggests themselves for the council Expert2 suggests themselves for the council Expert3 suggests themselves for the council
9	EXPERT-VOTE EXPERT-VOTE EXPERT-VOTE	Voter1 votes for Expert1 Voter2 votes for Expert2 Voter3 votes for Expert3
11	FINAL-VOTE FINAL-VOTE FINAL-VOTE	Voter1 final vote, stance 1 Voter2 final vote, stance 0 Voter3 final vote, stance 0
12	FINAL-VOTE FINAL-VOTE FINAL-VOTE	Expert1 final vote, stance 1 Expert2 final vote, stance 0 Expert3 final vote, stance 0

5.4 Final Output

The result of these interactions is observed in the blockchain's state changes, including the allocation of currency, the redistribution of stakes, the creation and resolution of issues, and the selection of validators.

Snippet 5.1 shows the issue resolution of the sample use case. As expected the result shows the winning stance is stance 0. An example bootstrapped round is shown to see how each round is executed. *winning_stances* list shows the winner of each round. The winning delegate of the issue also was able to forge Block number 13.

Listing 5.1: Issue example

```
{
"183d635e-8714-75a7-24fb-f056a60cc32a": {
"Final_winner": [
0
],
"all_voter_check": [5 items],
"all_Voters": [],
"blockCount": 12,
"bootstrapped_voting_results": {
"1": {
"stances": {
"0": 2,
"1": 1
},
"Voters": [3 items]
},
"2": {2 items},
"3": {2 items}
},
"council": [3 items],
"council_votes": {3 items},
"Delegates0": [1 item],
"Delegates1": [1 item],
"finalvote0": [3 items],
"finalvote1": [2 items],
"stage": "FINISHED",
"stance0": [2 items],
"stance1": [3 items],
"stances": [
0,
1
],
"suggested_Experts": {3 items},
"winning_stances": [
0,
0,
0
]
}
}
```

This chapter implements a sample use case of the chain. It explores the basic use of all transaction types and resolves each one. The issues created are resolved and the output is verified and confirmed to be as expected.

Chapter 6

Suggestions and Addendum

Gamification is the process of introducing mechanics, components, and concepts of game design into non-gaming environments to increase engagement, involvement, and motivation. Gamification is commonly used in digital platforms, especially decentralized systems, to leverage incentives, competition, accomplishments, and social connectivity to promote user interaction, contribution, and long-term commitment. Gamification poses certain issues that must be resolved to maintain the system's fairness and integrity, as it overemphasizes quantifiable results. The proposed system rewards a quantifiable result but in spirit must focus on critical reasoning a subjective definition. The system though implementing a lot of measures to enforce fairness still has some flaws. This section will explore some suggestions that will add to the solution and reinforce fairness.

6.1 Core Belief Database or CBD

A core belief Database or CBD is an additional suggestion to the proposed solution which helps weave an extra layer of fairness into the system

6.1.1 Initial Questionnaire and Issue Alignment

Upon joining the platform, users could be prompted to complete a questionnaire that assesses their knowledge and beliefs on fundamental scientific principles and historical facts. This initial engagement helps establish a baseline of core beliefs, ensuring that discussions are grounded in accepted realities. For instance, acknowledging the heliocentric model of the solar system becomes a prerequisite for engaging in discussions about the shape and dimensions of planet Earth.

6.1.2 Issue-Based Survey and Dynamic Belief Adjustment

Following participation in discussions or voting on issues, users could be surveyed about their reasoning. This post-engagement reflection encourages users to articulate their thought process, linking their stance back to their core beliefs. In cases where users find themselves on the losing side of a debate, the system could prompt them to reassess their core beliefs, offering an opportunity for learning and belief adjustment. Winners will not be allowed to change core beliefs and must stick to them or lose and change. This brings in a sense of commitment to an account and its history. Since Expert's core beliefs are a result of their education, they will not be able to change their beliefs easily.

6.1.3 Expert Privilege in Belief Modification

Experts would have the privilege to propose modifications or expansions to the CBD and instances in the CBD that are relevant to the current issue. This ensures that the database remains up-to-date with the latest scientific discoveries and historical understandings.

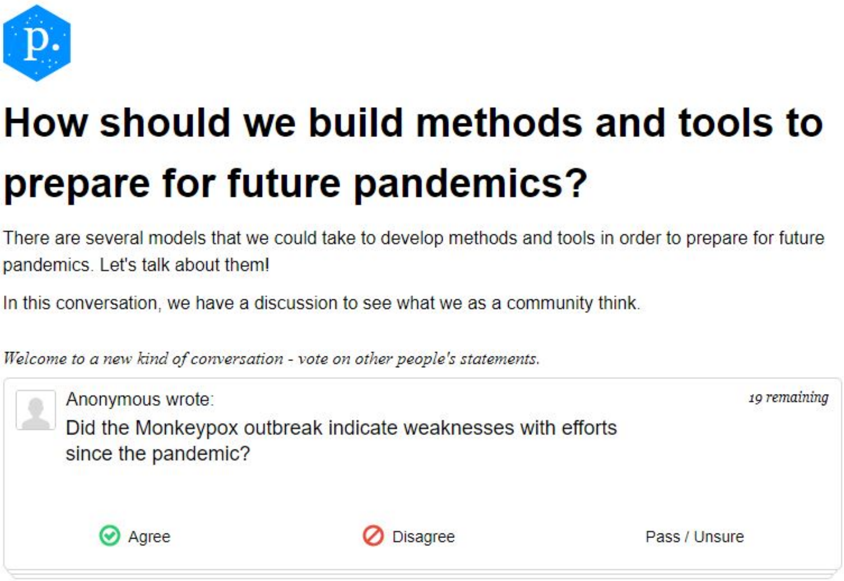
Database Expansion and Interconnectivity: The CBD is a growing and interconnected repository of knowledge. As issues are debated and resolved, the database expands, accommodating new findings and understandings. This dynamic nature of the CBD allows for the evolution of the platform's foundational beliefs, mirroring the fact that knowledge itself is not stagnant.

6.1.4 Machine Learning and LLMs

The development of Large Language Models (LLMs) has promise for improvements across various fields[57]. This includes the Core Belief Database (CBD), With their linguistic comprehension and capacity to produce logical, contextually relevant content, LLMs have the potential to both automate and improve the function of Experts inside the CBD framework. Experts will still maintain their role in issue resolution.

6.1.5 Polis

Polis is a participatory platform that combines real-time voting with machine learning to identify consensus among diverse groups. It's particularly adept at handling complex discussions, making it an ideal tool for enhancing the Core Belief Database (CBD)[58]. By leveraging Polis, the platform can ensure that the CBD remains a relevant and accurate source of knowledge.



How should we build methods and tools to prepare for future pandemics?

There are several models that we could take to develop methods and tools in order to prepare for future pandemics. Let's talk about them!

In this conversation, we have a discussion to see what we as a community think.

Welcome to a new kind of conversation - vote on other people's statements.

Anonymous wrote:

Did the Monkeypox outbreak indicate weaknesses with efforts since the pandemic?

Figure 6.1: Snippet of the Polis Platform [58]

Polis allows participants to express their agreement or disagreement with statements in real-time, providing immediate insights into the group's consensus or divisions. This could be detrimental to building and updating the CBD. Fig. 6.1 shows an example poll on the polis platform.

6.2 Reopening Issues and Snowball Rewards

Users who were on the losing side of an issue have the option to buy the reopening of an issue. This feature recognizes that new evidence, changes in societal values, or advancements in scientific understanding could significantly alter the context and conclusions of previously debated issues. After every loss, the cost to reopen an issue could drastically increase. This deters users from reopening issues without substantial evidence. On the other hand, continuously fighting for and sticking to a belief and finally winning could have a snowball effect on the reward meaning the reward might be worth all the reopening.

6.3 Weight Reset

In competitive gaming, rank resetting is a common practice where players' ranks are periodically reset, often coinciding with the start of a new season or competitive cycle. This approach ensures ongoing engagement and keeps the competitive environment dynamic and accessible to new and improving players. Drawing inspiration from this practice, the concept of rank or weight resetting can be adapted to the proposal. Resetting ranks or weights periodically motivates users to stay actively engaged with the platform, contributing to discussions and debates to maintain or improve their standing. Weights could be scaled down a bit and encourage users to spend time and effort building them again.

6.4 Hardware Dependence

Trusted Execution Environments (TEEs) offer a secure area within a main processor, ensuring that the code and data loaded inside the TEE are protected with respect to confidentiality and integrity[59]. Inspired by consensus mechanisms such as Proof of Elapsed Time (PoET)[35] and Proof of Luck[60], the use of TEEs can significantly mitigate issues related to the creation of multiple accounts, commonly referred to as Sybil attacks[61] and the operation of bots designed to manipulate voting or artificially inflate certain stances. Upon account creation or during critical actions like voting, the platform can utilize TEEs to conduct a secure verification process. The simple addition of a TEE check to the process increases the cost of attack significantly.

6.5 Random Allocation of Stances

Drawing inspiration from public defenders of the judiciary. The system could allow for random allocation of stances. For example, in case someone proposes an issue but doesn't have the means to back it up. The system could allow users to apply to be a public defender. Then the system could allot two stances randomly and reward the winner without the loser having to sacrifice anything. This could mean that sometimes people could be forced to find backing and arguments for stances that are against their beliefs. This helps users overcome their biases and

This chapter provides some suggestions that will improve the system but are out of scope for the current implementation. These suggestions would contribute towards making the system ’fairer’.

Chapter 7

Conclusion

In an era where misinformation runs rampant and social media have become the favoured platform for knowledge exchange and opinion formation, incentivizing scientific research and critical reasoning is of prime importance. This is an excellent way to get users to step out of their digital echo chambers which are a byproduct of algorithm-driven content. Moreover, existing blockchain consensus mechanisms while robust and revolutionary in their own sense show limitations. This thesis proposes a solution that tries to address both these issues. The previous chapters have explained the proposal in detail. This final chapter will discuss the ethical reasoning of the system, open issues and future scope.

7.1 Ethical Considerations and Fairness

Fairness is a subjective term and cannot really be defined but generally fairness in a sense points to impartiality i.e. treatment of everything and everyone as equals. How then can a system that by default increases and decreases the scores of its users be considered fair? This section will explore the fairness of the proposed system. A system which severely criticises social media algorithms for lack of fairness must put itself to the same scrutiny. In order to proceed further it is necessary to understand at least one facet of fairness. Researchers[62][63] and political Experts[64] suggest that fairness can be divided into three basic types:

- **Distributive Fairness** is the fairness of distribution of results when all involved parties have participated in the process that leads to the result. For the given system the result wouldn't be equal but might be considered fair as the results were based on the type of contribution.
- **Procedural Fairness** also known as process fairness deals with the process that determines the end result[63]. Jonathan Haidt says,

  > "People don't just care about whether they got a fair slice of the pie. That's "distributive fairness". They also care a great deal about whether open, honest, and impartial procedures were used to decide who got what."[64]

  This fairness drives the proposed solution. Even if the results aren't considered fair or if the end result is not considered to represent the 'truth', the process by which the incentives are determined would be considered fair.

> The judicial system is built on the same fairness. Even if the result may sometimes be alternate to what is true or fair. As long as the process is defined and impartial everyone considers it to be fair. A procedurally fair system must be bias-free, consistent and open to input.

The proposed solution might not embody distributive fairness but since the process is democratic, gives equal opportunity, is transparent and has optional participation it could definitely be considered procedurally fair. When people collaborate and reach a result fairness can take two forms or as Jonathan Haidt describes it, two buttons[64],

- People choose to 'press' the **Shared spoils** button when they feel the desire to share. This button is pressed more often when users feel that others contributed to their winning [64]. Delegates in the system and the users wouldn't mind sharing their rewards with people who voted for the winning stance. Normal Voters would even agree that since Delegates worked harder and risked more then they should be entitled to more rewards.
- People accept when the leader presses the **Shared sacrifice**. This is when to achieve a greater cause people will come together and risk or even sacrifice. When a delegate loses their stake people they convinced could even donate and share the sacrifice. This loyalty would help battle the fact that this system considered end result an alternative for rational discourse. Voters also accept losses when they are involved in a transparent process[64]

7.1.1 Key Enablers

The proposed system has certain practices that enable fairness, it is important to discuss why they are considered to enable fairness.

7.1.2 Transparency and Decentralization

Informational Fairness is a fairness metric that deals with a simple question, are explanations provided? This is a consideration under process fairness and is explored intensively in a field of Machine Learning known as XAI or eXplainable Artificial Intelligence [65]. The sole focus of this fairness metric is if the decisions can be traced or explained. Since the system is decentralized every is the decision maker but the decentralized system forces everyone to make the same decision in order to continue on the chain. This means that the whole process is as transparent as possible. Nodes know everything about the process and know that there are no biases involved in the system.

7.1.3 Democratic Voting and Expert Council

Though the Democratic process may have flaws most researchers agree that is the best available solution that can be balanced with auxiliary processes[66]. The introduction of Experts is yet another enabler that ties in with democratic voting. The majority might not always choose the scientifically reasonable decision. The introduction of Experts who vote after everyone has voted solves a lot of issues in the chain.

Primarily, the minority might not vote because they feel that their votes won't affect the result. The introduction of Experts gives a much-needed baseline that users must keep track of. For a lower value of ρ (the ratio which defines whether the system would lean more towards majority or expert opinion) the users in the system are incentivized to predict the voting style of the council or at least perform due diligence before voting.

Letting the Experts vote after normal Voters have voted further enables this. This practice also stops Voters from voting for the majority side. Because depending on the value of rho, the majority might still be the losing side.

7.1.4 Introduction of randomness

The selection of Voters and council members is a random choice(with the seed of the last block hash), this is done as it would add a layer of fairness to the system. Research points to the fact that people consider randomness to be fair[67]. Especially in a field known as Game Theory, randomness is considered fair. Game theory is a theoretical framework for modelling social situations. Research shows that people prefer random algorithms as they remove the need for intent. Only if an algorithm is deterministic is there an issue of fairness of intent. When there is no intent, algorithms have a better chance of being considered fair[68].

Even if fairness is a complicated and varied concept, it is clear that the suggested decentralized approach goes a long way toward accomplishing procedural justice. Through a focus on distributive justice, procedural justice, transparency, democratic engagement, and the integration of professional knowledge, the framework aims to achieve balance among the various dimensions of fairness. This equilibrium is essential in a decentralized setting when the objective is to guarantee a fair distribution of incentives.

7.2 Open Issues

Even if the suggested solutions mitigated a lot of potential issues there are still some issues that have to be left open-ended.

7.2.1 Voter Apathy

Voter apathy is the term used to describe situations in which eligible Voters in both traditional democratic procedures and decentralised systems decide not to participate in the voting process. There are a number of possible explanations for this low participation rate, such as a lack of interest in the topics up for a vote, a sense of powerlessness over the outcome, or discontent with the selections. A major problem with voter apathy is that it might result in decisions that are not truly reflective of the preferences of the entire community or user base.

Voter apathy in the proposed solution after consideration of the suggestions could only be because of a lack of popularity. This is something the solution cannot guarantee. Ultimately how many users use the chain and how many votes are unpredictable.

7.2.2 Determination of Constants

α is the incentive constant of the system. A fair determination of α, is important as too much or too little could throw the system off balance. Another constant that needs fair determination is ρ the majority-expert ratio. Both these constants would need to be determined after specific and extensive research spanning fields like game theory and statistics. The determination of these constants can also be dynamic. Raising a separate issue could help solve this problem in a democratic fashion.

7.3 Further Scope

This thesis is but the tip of the iceberg. The proposal is only an actualization of a small part of decentralized systems' potential to change society. Incentivization can be modelled to represent anything, even abstract concepts. As long as people put some sufficient measurable effort into the system, it can be measured and it has value when translated into crypto-currency or weights. Even this specific thesis could be improved in multiple ways as suggested by Chapter 6. There is much work to be done in this field and the same goes for this proposal. For example, the application of this could be modelled a bit differently to suit for use in academia. Decentralised voting systems and scaled consensus mechanisms hold much promise for the future.

There exists a lot of opportunity even beyond mere technical refinements. An avenue that could be explored involves evaluating how efficient this system could be in serving as a CAPTCHA. Initally even though all reputation scores start at the same baseline over time the thesis could clearly show the difference between users who chose randomly and users who make informed decisions. This could help weed out non-intelligent bots.

7.4 Closing Remarks

At its inception, the research was motivated by two pivotal questions: How can one incentivize the everyday citizen to engage in rational discourse? and How can we develop fairer consensus mechanisms? In exploring these two questions, the thesis navigated through multiple other questions and challenges like How can we ensure fairness in systems that are inherently majoritarian? Through systematic research and inspiration drawn from different facets of everyday life and governance, The thesis tried to answer all these questions. The main purpose of the thesis was to not just suggest but to also develop a minimally functional solution that proves that the concepts can be implemented.

Numerous factors seemed to enable misinformation and lack of interest in discourse, so much so that solving each separate issue wouldn't lead to any significant progress. The coupling of democratic voting mechanisms and the involvement of Experts emerged as a vital approach to balancing consensus mechanisms and incentivizing informed decision-making. The inclusion of randomness in the selection of Voters and council members introduced an additional layer of impartiality. The thesis explored and leveraged multiple aspects of decentralized ledgers in order to create a Decentralized social media that inherently incentivizes discussion. In this era of isolation and finding comfort in echo chambers this thesis provides people with the much-needed incentive to step out of their self-made boundaries. The proposed solution is not flawless but it answers some significant questions and opens new ones.

Though the explorations limited to this thesis have come to an end, the journey towards fairness in decentralized systems and social media is far from complete. The proposal hopes that it contributes in some small way to the advancement of knowledge and the betterment of society.

Appendix A

Intermediary Output Snippets

The step-by-step output of the sample use case will be shown here, starting with the state of the issue dictionary after initial creation,

Listing A.1: Output after Initial Creation of Issue

```
{
"6fff9fd6-ba00-630f-b5ae-ac58607e6b3e": {
"all_voters": [],
"blockCount": 2,
"council": [],
"council_votes": {},
"delegates0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"finalvote0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"stage": "CREATED",
"stance0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"stances": [
0
],
"suggested_experts": {}
}
}
```

The next output shows the chain after the staker who staked in Block 2 becomes the validator in Block 6.

Listing A.2: Output after Staker Becomes Validator

```
{
"blocks": [
{8 items},
{8 items},
{8 items},
{
"accHash": "8655bd572f3f5e48b77267b26f718867dadbbf01eda6b37079cb4c31539435f1",
"blockCount": 2,
"forger": "-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpQ2c9
    UvIiDOdU4i4yZG0Swyf2 8ylVMePPSTL0Lqh3Z8gcorYbMLEalUjXPIvuIcdRzjzVUDFt9wWPE4m0
    InaZH/ul USpEiWpX6zbkrcXsSnVg6v4gHROrYoE0ZkvmuVUAKr/KhXe3S6SN75WQABJG9Ew9 JhG1
    hlWvS9TiCqIr6QIDAQAB -----END PUBLIC KEY-----",
"lastHash": "fded3218bea504add7a622e6c64c3b843cbfdd0d3963150c2d86f9129fe1700d",
"posHash": "0c6017eb13871480f691d021197d6226b30bab3876100e56f1ef64ffbc38f5ac",
"signature": "108a9444178f85c40eb238e8da981c9a97f2bc1e856163df9c6058d6367dec2587640
    7b0793a852fda629cf5310590131427634169e940a9eb2ddad5ff4ea3afc2afba126f1a22697a11
    0d9225d1ae9f403160681780bcc7d9aa8c7b3c2d872e0a38d691067e9df04c659d0ca2936dad4e9
    b23a53240337602de6b14cee8cfec",
"timestamp": 1710978594.8515809,
"transactions": [
{
"amount": 5,
"id": "8975e609e71411ee917c982cbc0b3f0a",
"receiverPublicKey": "-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
    AMIIBCgKCAQEAxXRGQ4pQRfebUjSPAbL2 Dh1OaLXeCMWuI28TDKs9JD2r51s6zx8MEo288Kup0u43l
    9c5Hwq3tQzjM8K0g0x7 zfcclQaDIurWevzkgHDnH/bHDd6JLLGdX5/CBpwugnH60Rdv2HbqUvuXWS6
    Rmofo yiSNLlUVp/xqhFOW1u5BXDJ78pfF9c6zo2NVyOdPKAKP+lsw4Dh6GrtSEl7GYiO/ o35Dp57
    zzU9DmUEQNggkCUxxoOb7v/N93n7/S/+S9/prsNo9soruuOKVAEORoLYj uzjgzwiFlPLuPQrbaB5
    dFP3pnchxSioxE3oSIvdEleGXzDYFfJrucNi9bUDITs4c BQIDAQAB -----END PUBLIC KEY
    -----",
"senderPublicKey": "-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
    AMIIBCgKCAQEAxXRGQ4pQRfebUjSPAbL2 Dh1OaLXeCMWuI28TDKs9JD2r51s6zx8MEo288Kup0u43l
    9c5Hwq3tQzjM8K0g0x7 zfcclQaDIurWevzkgHDnH/bHDd6JLLGdX5/CBpwugnH60Rdv2HbqUvuXWS6
    Rmofo yiSNLlUVp/xqhFOW1u5BXDJ78pfF9c6zo2NVyOdPKAKP+lsw4Dh6GrtSEl7GYiO/ o35Dp57
    zzU9DmUEQNggkCUxxoOb7v/N93n7/S/+S9/prsNo9soruuOKVAEORoLYj uzjgzwiFlPLuPQrbaB5
    dFP3pnchxSioxE3oSIvdEleGXzDYFfJrucNi9bUDITs4c BQIDAQAB -----END PUBLIC KEY
    -----",
"signature": "46d441cdf83b36cfcee746b0d61958e4b35803716730e49e5be357b43d8b2dd832bbb
    00e7c3bf86eca1688e14ec02aef1208ca77b36049b3cfe27a18412f977f2840e9b57ad55ea7f95a
    4c3df3b4b0522f9407a19ad8a6cb17a297e53022961220fa0bd7671b97b96fa203a7b0051f00f94
    fa5778285240fc773af67ec4ebb71e80a4bc0495ff6893e4dddc993b4e10646242546e9792269
    ece1160eb9adac685dabb2dbbe4330a6325b680684b45c12c3b05fd3a4abf8765816783cf29a09
    ce03e181b4b222863d775a02583c3e1c21454dcaa6165b312eabf8504cc0be66a163625d960d989
    f0e8ce378a30e00d1675ac5f4866f2e724ac645018930e7ad65",
"timestamp": 1710978588.6631434,
"type": "STAKE"
},
{7 items},
{7 items}
]
},
{8 items},
{8 items},
{
"accHash": "29416e967d7862edf9aced70f0345faa2d5876fc33e75752a6bcdf4187ce4e5e",
"blockCount": 6,
"forger": "-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
    AMIIBCgKCAQEAxXRGQ4pQRfebUjSPAbL2 Dh1OaLXeCMWuI28TDKs9JD2r51s6zx8MEo288Kup0u43l
    9c5Hwq3tQzjM8K0g0x7 zfcclQaDIurWevzkgHDnH/bHDd6JLLGdX5/CBpwugnH60Rdv2HbqUvuXWS6
    Rmofo yiSNLlUVp/xqhFOW1u5BXDJ78pfF9c6zo2NVyOdPKAKP+lsw4Dh6GrtSEl7GYiO/ o35Dp57
    zzU9DmUEQNggkCUxxoOb7v/N93n7/S/+S9/prsNo9soruuOKVAEORoLYj uzjgzwiFlPLuPQrbaB5
    dFP3pnchxSioxE3oSIvdEleGXzDYFfJrucNi9bUDITs4c BQIDAQAB -----END PUBLIC KEY
    -----",
"lastHash": "458024665ceaaa103e6098ee4178373cb899a79c18b684f092cfdcfc5e7f45e7",
"posHash": "abf7fafc13a446d35e270ba54cc1b9669b227df544ad594744f21802fbc08e29",
"signature": "a1bee42df0f82328712197a47f5e02a813cfe28fff27d0fabf4c8c0375b16425af074
    88a0f1b2e282e0514aa2a955e6868ad47d07bccd21663e1337f9c0eb74033487e71aff127087ff0
    e1cc30997e5345609f6a0e6d06d29077393ac58ad41d9272fcbc6f508d849a71f0db6af0be0045a
    342b5b1753d5a07b114aed8edc1fcb35c32781ed962bd39133ab32806b45c4e2ff7fe32871ede1c
    6cd0f73a974efa2a27c4f238fcc600bbe434102e824097624e5885e091cec174cac2d5f5efa2f7d
    539b9f887593de57da989ee4dd0624d1b51ddae492871da108648616338f2bc068b388942186
    bacc632e82e32b5e23865fca3494c0d3be3668b09f76dbf5839",
"timestamp": 1710978601.0319316,
"transactions": [3 items]
}
}
```

This is the output after another delegate buys in an opposite stance,

Listing A.3: Output After a Total of Two Delegates Buyin

```
{
"6fff9fd6-ba00-630f-b5ae-ac58607e6b3e": {
"all_voters": [],
"blockCount": 3,
"council": [],
"council_votes": {},
"delegates0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"delegates1": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBP/tU1SlLd2
    EyjEC4Dwc0d kaUCD4WnsBaUmZo5Fh3ktPcQq9VVJbLF4EZ+tTXFFzSjhQl15isTz9SupPWum7YK
    juhUWeDPZ9MfMVOjR+6o4fc67h9NVxz8+gW5S0ceAQjEVrpUzCWQuWp7+M9PIaM0 WLuorccgHz8ib9
    Z1TjjPYEkodMs2jxT7sfGUlNCNcuBOPe797Rv5mdtbgrW3zEjF ZFO07GC6XwPcsMAa4jdBhtqnRW+
    RU08VwwP9dA+ITeOvxKYKpzidyI3lmYCSNFHy Oc50r/P2hwYdVvNJSjQHnQD0
    vUTjJjcCaDmdMvSEvnR4BgGvAqDnY31PFpFh15Ov AgMBAAE= -----END PUBLIC KEY-----"
],
"finalvote0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"finalvote1": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBP/tU1SlLd2
    EyjEC4Dwc0d kaUCD4WnsBaUmZo5Fh3ktPcQq9VVJbLF4EZ+tTXFFzSjhQl15isTz9SupPWum7YK
    juhUWeDPZ9MfMVOjR+6o4fc67h9NVxz8+gW5S0ceAQjEVrpUzCWQuWp7+M9PIaM0 WLuorccgHz8ib9
    Z1TjjPYEkodMs2jxT7sfGUlNCNcuBOPe797Rv5mdtbgrW3zEjF ZFO07GC6XwPcsMAa4jdBhtqnRW+
    RU08VwwP9dA+ITeOvxKYKpzidyI3lmYCSNFHy Oc50r/P2hwYdVvNJSjQHnQD0
    vUTjJjcCaDmdMvSEvnR4BgGvAqDnY31PFpFh15Ov AgMBAAE= -----END PUBLIC KEY-----"
],
"stage": "INIT-VOTING",
"stance0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"stance1": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBP/tU1SlLd2
    EyjEC4Dwc0d kaUCD4WnsBaUmZo5Fh3ktPcQq9VVJbLF4EZ+tTXFFzSjhQl15isTz9SupPWum7YK
    juhUWeDPZ9MfMVOjR+6o4fc67h9NVxz8+gW5S0ceAQjEVrpUzCWQuWp7+M9PIaM0 WLuorccgHz8ib9
    Z1TjjPYEkodMs2jxT7sfGUlNCNcuBOPe797Rv5mdtbgrW3zEjF ZFO07GC6XwPcsMAa4jdBhtqnRW+
    RU08VwwP9dA+ITeOvxKYKpzidyI3lmYCSNFHy Oc50r/P2hwYdVvNJSjQHnQD0
    vUTjJjcCaDmdMvSEvnR4BgGvAqDnY31PFpFh15Ov AgMBAAE= -----END PUBLIC KEY-----"
],
"stances": [
0,
1
],
"suggested_experts": {}
},
"541c89f7-51df-b2b4-1d99-119390bd7373": {
"all_voters": [],
"blockCount": 3,
"council": [],
"council_votes": {},
"delegates0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"finalvote0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"stage": "CREATED",
"stance0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----"
],
"stances": [
0
],
"suggested_experts": {}
}
}
```

Now the next output is after voters vote their initial stance,

Listing A.4: Output After Initial Votes

```
{
"6fff9fd6-ba00-630f-b5ae-ac58607e6b3e": {
"all_voters": [3 items],
"blockCount": 5,
"council": [],
"council_votes": {},
"delegates0": [1 item],
"delegates1": [1 item],
"finalvote0": [1 item],
"finalvote1": [1 item],
"stage": "COUNCIL-SUGGEST",
"stance0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TuboоJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArtzc/
    YfuAXcVbBF54C9k ohAk9QZB4lUAO4wlnN+bkvKMohOlWUMrDJw0fAFxN1AqNiamItA+q/bzNajaAo4
    J NCtpUhUdSWmp0TiHffxAk8pWxeubv6xNxXkq5UrBR8DsQCto/k0X5wKG5omzqHaB jJciXul0Ooh0
    XFZcgS0rZUdpqQvUEdOub2UzR+SAXmAfzvBM7y8eHDvYMVeRGZsU YsbMy9Fs2
    jzXLkHeZKVAqyVbteLG4NuZYYvpj8gXlBlE5yU5I1s6czNwZIucbsdY Yn0mWnhy86
    jcKQbSMCUvaRzF7nPyVBC+cQ1d37yqWpFoYRZPD/ySYt5fWUIqzk+E TwIDAQAB -----END PUBLIC
     KEY-----"
],
"stance1": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBP/tU1SlLd2
    EyjEC4Dwc0d kaUCD4WnsBaUmZo5Fh3ktPcQq9VVJbLF4EZ+tTXFFzSjhQl15isTz9SupPWum7YK
    juhUWeDPZ9MfMVOjR+6o4fc67h9NVxz8+gW5S0ceAQjEVrpUzCWQuWp7+M9PIaM0 WLuorccgHz8ib9
    Z1TjjPYEkodMs2jxT7sfGUlNCNcuBOPe797Rv5mdtbgrW3zEjF ZFO07GC6XwPcsMAa4jdBhtqnRW+
    RU08VwwP9dA+ITeOvxKYKpzidyI3lmYCSNFHy Oc50r/P2hwYdVvNJSjQHnQD0
    vUTjJjcCaDmdMvSEvnR4BgGvAqDnY31PFpFh15Ov AgMBAAE= -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkkyJ+NS66
    jkNn83MZgEO cMnq2fg9saSOIy5meTRD/2h1h8PBHkU8QeytYVoACTn0i0nYuvZI7xkkJnDGrHIY V/
    UttpkZgDJMMTLr95MOGGVcd6eUoFiNXeWuCWJHk1ZBXd2+6rl4laBKdUyoLDOR u3RX1Xlp94
    rItXsvCI2NpKWbxIVq2y2zC+zfkA7w14VSUnXQwbS173sBJKENGvJK Q7WWOZ+iXDVhOIO/EXYBdKv7
    PIXDIDJD/lGC26Zux78+Zzwy0qpot5JBufHeVwnv HY2aMys3b9WgQuVueoXBYYBNdvFkJgt4V+Lc9
    ehngFlLsa2Wyaxe3LfZMBMlrogo dwIDAQAB -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBms2NvW+1B23
    aaZD7mboBU CqUUhOmbK6WBq9glsG94sOmzsdo3Z5u/IYt2k2tdZrFUKLUZKabVH1lLxyO7YZgT K+M
    2ux4HnFQVvDEcEbwLPe3d6wFog01f3LTtiQxj+TFpQdUcQccHXmqhWlGvOCEn FpEf4sLtF8Bj16eZ2
    RPL7/nvweHEKEws+s7qzB4KVdb+4VoU0W2Et4eUuD/gknTp
    LLXozMcXjYEkiOhHKHftJveAClPQqsJT9i9tZgEC66Edjz64CyGJTmuEd0OJREtT o8Psi8p2kvrkzW
    /cMsnNDqKk5aQMfxKoxP1oTguymmcl/om0uvU7HKwBx+/ZXb4Z AgMBAAE= -----END PUBLIC KEY
    -----"
],
"stances": [
0,
1
],
"suggested_experts": {}
}
}
```

The next process is experts suggesting and voting in experts,

Listing A.5: Output After Forming Council

```
{
"6fff9fd6-ba00-630f-b5ae-ac58607e6b3e": {
"all_voters": [6 items],
"blockCount": 9,
"council": [
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1HM6
    RFIHlZWjtDUbfO+s Vh4HmKYZA+2nKLw282p8I4+n+qjIKDyJDkoK1PH8jsr2xehSCQQQNXf61Yi1N5
    tc eu+HWncZEpgXpiIMXZArukvoEyJQI/Ti2lVfteKs8ZCxWRbjZj7sNmPsujbWDamC HLOaOd7QWz/
    BMEi0gpYKwHHt3qugK+FI/zmwCNKl9xiqIjDTtQUeexHPsdPAswOe KBpLkVIVK+Cl7xDq+fbYj5
    EcEKKTnTt/FuSLRMOKJRWZkxZxHODuMTxyA2ABubDB nzK/0sF7M6D9sk+/3KhZ/FVU9/fcqFA0DsI9
    Hpx/FakaikGtWS3Ol0MhHj+6Acz/ wwIDAQAB -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
    AMIIBCgKCAQEAvBERQXkyGJZFZS34fZ6g xHXqQR49Cwk2I+ycCpZrFZ4
    IfoWCZurtmWbvEvrqaPyjCbzYxDybVBroFD/J1X7s ukkfQ5ysTq19BC22yOH2P9YxzPzgmOkSnWP1
    wzeTSgHuXf7Zxr20iqdYdOSfJ4Tt vLoPbLx3ndMLAyLpe8tZPxFg8jFYKLaDQDNbnGdrG1NkJ/7
    Sagg464clVH7BqCIf 5CpZDlzoqsz3hI+mnQjPuR2iQxu4hlXlbaV9MRdX/z6j+p/wz9nGxTqHpnlmL
    8Py HO6ZoQFFLmLr5xXVB59sHzOmr2K7JLhFuUdJAV4zSFgx9vyb8cI0gM4igHuRqKWJ FQIDAQAB
    -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAi8PZim/1
    aAVDPDwh1DzL /6xKjBX3cRmn3JuGKVruxKiEjuQIm4x8973yhCJtePTSthvSkWXRiKI2VTkqpqHQ b
    8KKbnvNyOcSe++tRQRv0pyWUmK0JWzesr7jnK/bEeoAdpYBKvyartOvZLp9WCet 8t1MHyOi+qKV0
    Zxx7UsFm8/MKyAh5Lws5SkbNkXDvvQIOxeGHN1yHNCFxJIQALXi QJvFpldkYK2mE7De0gUEKasCBH9
    wiZTjfW6fi6bw+vLKK1nkAH07E2A2OcQ4xFWP hqHcej8zqa1qPCeSxr+IVn8YRrL+B8
    zfQDfhngCXaifnxVcIOWSLXKSYr35SXrgU QwIDAQAB -----END PUBLIC KEY-----"
],
"council_votes": {},
"delegates0": [1 item],
"delegates1": [1 item],
"finalvote0": [1 item],
"finalvote1": [1 item],
"stage": "FINAL-VOTE",
"stance0": [2 items],
"stance1": [3 items],
"stances": [2 items],
"suggested_experts": {
"-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1HM6RFIHlZWjtDUbfO+s
Vh4HmKYZA+2nKLw282p8I4+n+qjIKDyJDkoK1PH8jsr2xehSCQQQNXf61Yi1N5tc
eu+HWncZEpgXpiIMXZArukvoEyJQI/Ti2lVfteKs8ZCxWRbjZj7sNmPsujbWDamC
HLOaOd7QWz/BMEi0gpYKwHHt3qugK+FI/zmwCNKl9xiqIjDTtQUeexHPsdPAswOe
KBpLkVIVK+Cl7xDq+fbYj5EcEKKTnTt/FuSLRMOKJRWZkxZxHODuMTxyA2ABubDB
nzK/0sF7M6D9sk+/3KhZ/FVU9/fcqFA0DsI9Hpx/FakaikGtWS3Ol0MhHj+6Acz/
wwIDAQAB
-----END PUBLIC KEY-----": 1,
"-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAi8PZim/1aAVDPDwh1DzL
/6xKjBX3cRmn3JuGKVruxKiEjuQIm4x8973yhCJtePTSthvSkWXRiKI2VTkqpqHQ
b8KKbnvNyOcSe++tRQRv0pyWUmK0JWzesr7jnK/bEeoAdpYBKvyartOvZLp9WCet
8t1MHyOi+qKV0Zxx7UsFm8/MKyAh5Lws5SkbNkXDvvQIOxeGHN1yHNCFxJIQALXi
QJvFpldkYK2mE7De0gUEKasCBH9wiZTjfW6fi6bw+vLKK1nkAH07E2A2OcQ4xFWP
hqHcej8zqa1qPCeSxr+IVn8YRrL+B8zfQDfhngCXaifnxVcIOWSLXKSYr35SXrgU
QwIDAQAB
-----END PUBLIC KEY-----": 1,
"-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvBERQXkyGJZFZS34fZ6g
xHXqQR49Cwk2I+ycCpZrFZ4IfoWCZurtmWbvEvrqaPyjCbzYxDybVBroFD/J1X7s
ukkfQ5ysTq19BC22yOH2P9YxzPzgmOkSnWP1wzeTSgHuXf7Zxr20iqdYdOSfJ4Tt
vLoPbLx3ndMLAyLpe8tZPxFg8jFYKLaDQDNbnGdrG1NkJ/7Sagg464clVH7BqCIf
5CpZDlzoqsz3hI+mnQjPuR2iQxu4hlXlbaV9MRdX/z6j+p/wz9nGxTqHpnlmL8Py
HO6ZoQFFLmLr5xXVB59sHzOmr2K7JLhFuUdJAV4zSFgx9vyb8cI0gM4igHuRqKWJ
FQIDAQAB
-----END PUBLIC KEY-----": 1
}
}
}
```

Given below is the explained result of all the rounds and the final winner, interestingly enough since */rho* was very close to one even though the majority of councils voted for stance 0 and the majority of voters and delegates voted for stance 0 the winner of this iteration is stance 1.

Listing A.6: Output After Final Vote

```
{
"e53f80e0-a07e-7723-5baf-4940f71ecf06": {
"Final_winner": [
1
],
"all_voter_check": [5 items],
"all_voters": [],
"blockCount": 12,
"bootstrapped_voting_results": {
"1": {
"stances": {
"0": 1,
"1": 2
},
"voters": [
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkkyJ+NS66
    jkNn83MZgEO cMnq2fg9saSOIy5meTRD/2h1h8PBHkU8QeytYVoACTn0i0nYuvZI7xkkJnDGrHIY V/
    UttpkZgDJMMTLr95MOGGVcd6eUoFiNXeWuCWJHk1ZBXd2+6rl4laBKdUyoLDOR u3RX1Xlp94
    rItXsvCI2NpKWbxIVq2y2zC+zfkA7w14VSUnXQwbS173sBJKENGvJK Q7WWOZ+iXDVhOIO/EXYBdKv7
    PIXDIDJD/lGC26Zux78+Zzwy0qpot5JBufHeVwnv HY2aMys3b9WgQuVueoXBYYBNdvFkJgt4V+Lc9
    ehngFlLsa2Wyaxe3LfZMBMlrogo dwIDAQAB -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBms2NvW+1B23
    aaZD7mboBU CqUUhOmbK6WBq9glsG94sOmzsdo3Z5u/IYt2k2tdZrFUKLUZKabVH1lLxyO7YZgT K+M
    2ux4HnFQVvDEcEbwLPe3d6wFog01f3LTtiQxj+TFpQdUcQccHXmqhWlGvOCEn FpEf4sLtF8Bj16eZ2
    RPL7/nvweHEKEws+s7qzB4KVdb+4VoU0W2Et4eUuD/gknTp
    LLXozMcXjYEkiOhHKHftJveAClPQqsJT9i9tZgEC66Edjz64CyGJTmuEd0OJREtT o8Psi8p2kvrkzW
    /cMsnNDqKk5aQMfxKoxP1oTguymmcl/om0uvU7HKwBx+/ZXb4Z AgMBAAE= -----END PUBLIC KEY
    -----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1HM6
    RFIHlZWjtDUbfO+s Vh4HmKYZA+2nKLw282p8I4+n+qjIKDyJDkoK1PH8jsr2xehSCQQQNXf61Yi1N5
    tc eu+HWncZEpgXpiIMXZArukvoEyJQI/Ti2lVfteKs8ZCxWRbjZj7sNmPsujbWDamC HLOaOd7QWz/
    BMEi0gpYKwHHt3qugK+FI/zmwCNKl9xiqIjDTtQUeexHPsdPAswOe KBpLkVIVK+Cl7xDq+fbYj5
    EcEKKTnTt/FuSLRMOKJRWZkxZxHODuMTxyA2ABubDB nzK/0sF7M6D9sk+/3KhZ/FVU9/fcqFA0DsI9
    Hpx/FakaikGtWS3Ol0MhHj+6Acz/ wwIDAQAB -----END PUBLIC KEY-----"
]
},
"2": {
"stances": {
"0": 1,
"1": 2
},
"voters": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBP/tU1SlLd2
    EyjEC4Dwc0d kaUCD4WnsBaUmZo5Fh3ktPcQq9VVJbLF4EZ+tTXFFzSjhQl15isTz9SupPWum7YK
    juhUWeDPZ9MfMVOjR+6o4fc67h9NVxz8+gW5S0ceAQjEVrpUzCWQuWp7+M9PIaM0 WLuorccgHz8ib9
    Z1TjjPYEkodMs2jxT7sfGUlNCNcuBOPe797Rv5mdtbgrW3zEjF ZFO07GC6XwPcsMAa4jdBhtqnRW+
    RU08VwwP9dA+ITeOvxKYKpzidyI3lmYCSNFHy Oc50r/P2hwYdVvNJSjQHnQD0
    vUTjJjcCaDmdMvSEvnR4BgGvAqDnY31PFpFh15Ov AgMBAAE= -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1HM6
    RFIHlZWjtDUbfO+s Vh4HmKYZA+2nKLw282p8I4+n+qjIKDyJDkoK1PH8jsr2xehSCQQQNXf61Yi1N5
    tc eu+HWncZEpgXpiIMXZArukvoEyJQI/Ti2lVfteKs8ZCxWRbjZj7sNmPsujbWDamC HLOaOd7QWz/
    BMEi0gpYKwHHt3qugK+FI/zmwCNKl9xiqIjDTtQUeexHPsdPAswOe KBpLkVIVK+Cl7xDq+fbYj5
    EcEKKTnTt/FuSLRMOKJRWZkxZxHODuMTxyA2ABubDB nzK/0sF7M6D9sk+/3KhZ/FVU9/fcqFA0DsI9
    Hpx/FakaikGtWS3Ol0MhHj+6Acz/ wwIDAQAB -----END PUBLIC KEY-----"
]
},
"3": {
"stances": {
"0": 2,
"1": 1
},
"voters": [
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArtzc/
    YfuAXcVbBF54C9k ohAk9QZB4lUAO4wlnN+bkvKMohOlWUMrDJw0fAFxN1AqNiamItA+q/bzNajaAo4
    J NCtpUhUdSWmp0TiHffxAk8pWxeubv6xNxXkq5UrBR8DsQCto/k0X5wKG5omzqHaB jJciXul0Ooh0
    XFZcgS0rZUdpqQvUEdOub2UzR+SAXmAfzvBM7y8eHDvYMVeRGZsU YsbMy9Fs2
    jzXLkHeZKVAqyVbteLG4NuZYYvpj8gXlBlE5yU5I1s6czNwZIucbsdY Yn0mWnhy86
    jcKQbSMCUvaRzF7nPyVBC+cQ1d37yqWpFoYRZPD/ySYt5fWUIqzk+E TwIDAQAB -----END PUBLIC
     KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1HM6
    RFIHlZWjtDUbfO+s Vh4HmKYZA+2nKLw282p8I4+n+qjIKDyJDkoK1PH8jsr2xehSCQQQNXf61Yi1N5
    tc eu+HWncZEpgXpiIMXZArukvoEyJQI/Ti2lVfteKs8ZCxWRbjZj7sNmPsujbWDamC HLOaOd7QWz/
    BMEi0gpYKwHHt3qugK+FI/zmwCNKl9xiqIjDTtQUeexHPsdPAswOe KBpLkVIVK+Cl7xDq+fbYj5
    EcEKKTnTt/FuSLRMOKJRWZkxZxHODuMTxyA2ABubDB nzK/0sF7M6D9sk+/3KhZ/FVU9/fcqFA0DsI9
    Hpx/FakaikGtWS3Ol0MhHj+6Acz/ wwIDAQAB -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
    AMIIBCgKCAQEAvBERQXkyGJZFZS34fZ6g xHXqQR49Cwk2I+ycCpZrFZ4
    IfoWCZurtmWbvEvrqaPyjCbzYxDybVBroFD/J1X7s ukkfQ5ysTq19BC22yOH2P9YxzPzgmOkSnWP1
    wzeTSgHuXf7Zxr20iqdYdOSfJ4Tt vLoPbLx3ndMLAyLpe8tZPxFg8jFYKLaDQDNbnGdrG1NkJ/7
    Sagg464clVH7BqCIf 5CpZDlzoqsz3hI+mnQjPuR2iQxu4hlXlbaV9MRdX/z6j+p/wz9nGxTqHpnlmL
    8Py HO6ZoQFFLmLr5xXVB59sHzOmr2K7JLhFuUdJAV4zSFgx9vyb8cI0gM4igHuRqKWJ FQIDAQAB
    -----END PUBLIC KEY-----"
]
}
},
"council": [3 items],
"council_votes": {
"-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1HM6RFIHlZWjtDUbfO+s
Vh4HmKYZA+2nKLw282p8I4+n+qjIKDyJDkoK1PH8jsr2xehSCQQQNXf61Yi1N5tc
eu+HWncZEpgXpiIMXZArukvoEyJQI/Ti2lVfteKs8ZCxWRbjZj7sNmPsujbWDamC
HLOaOd7QWz/BMEi0gpYKwHHt3qugK+FI/zmwCNKl9xiqIjDTtQUeexHPsdPAswOe
KBpLkVIVK+Cl7xDq+fbYj5EcEKKTnTt/FuSLRMOKJRWZkxZxHODuMTxyA2ABubDB
nzK/0sF7M6D9sk+/3KhZ/FVU9/fcqFA0DsI9Hpx/FakaikGtWS3Ol0MhHj+6Acz/
wwIDAQAB
-----END PUBLIC KEY-----": 1,
"-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAi8PZim/1aAVDPDwh1DzL
/6xKjBX3cRmn3JuGKVruxKiEjuQIm4x8973yhCJtePTSthvSkWXRiKI2VTkqpqHQ
b8KKbnvNyOcSe++tRQRv0pyWUmK0JWzesr7jnK/bEeoAdpYBKvyartOvZLp9WCet
8t1MHyOi+qKV0Zxx7UsFm8/MKyAh5Lws5SkbNkXDvvQIOxeGHN1yHNCFxJIQALXi
QJvFpldkYK2mE7De0gUEKasCBH9wiZTjfW6fi6bw+vLKK1nkAH07E2A2OcQ4xFWP
hqHcej8zqa1qPCeSxr+IVn8YRrL+B8zfQDfhngCXaifnxVcIOWSLXKSYr35SXrgU
QwIDAQAB
-----END PUBLIC KEY-----": 0,
"-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvBERQXkyGJZFZS34fZ6g
xHXqQR49Cwk2I+ycCpZrFZ4IfoWCZurtmWbvEvrqaPyjCbzYxDybVBroFD/J1X7s
ukkfQ5ysTq19BC22yOH2P9YxzPzgmOkSnWP1wzeTSgHuXf7Zxr20iqdYdOSfJ4Tt
vLoPbLx3ndMLAyLpe8tZPxFg8jFYKLaDQDNbnGdrG1NkJ/7Sagg464clVH7BqCIf
5CpZDlzoqsz3hI+mnQjPuR2iQxu4hlXlbaV9MRdX/z6j+p/wz9nGxTqHpnlmL8Py
HO6ZoQFFLmLr5xXVB59sHzOmr2K7JLhFuUdJAV4zSFgx9vyb8cI0gM4igHuRqKWJ
FQIDAQAB
-----END PUBLIC KEY-----": 0
},
"delegates0": [1 item],
"delegates1": [1 item],
"finalvote0": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQB12TubooJB0V0
    92XgWNco3 sa5DqmW2Fb42hrlf+LZmgG1izKOb2m/cPA9wotiIR3dDKshi7P+T/K6Wm5ReDzgp v9uv
    3n6qBLfjwKPE0nVRLnYG6iEzqY+XhpRw36GLDQnebzA42Gt0SId6a4qmRfQB GBQ4/Pn9hG7JOFiV/3
    XKGJuck2BgK3S07aB0ERwugmSgvlitQ7oOyUtMBhrpMjvn tAnXjsQzjgJ1KVd2xqYTUjUUIy7b6
    QYpePxcjJJoUDA/4rLXbXsesgL1Af7EOzEg zlaDfnaIanu7O/8BXlKvTjFBTm1PqzW5Saa+sbZsyZd
    5CasEtyrvHh9/C3jYdkJN AgMBAAE= -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBms2NvW+1B23
    aaZD7mboBU CqUUhOmbK6WBq9glsG94sOmzsdo3Z5u/IYt2k2tdZrFUKLUZKabVH1lLxyO7YZgT K+M
    2ux4HnFQVvDEcEbwLPe3d6wFog01f3LTtiQxj+TFpQdUcQccHXmqhWlGvOCEn FpEf4sLtF8Bj16eZ2
    RPL7/nvweHEKEws+s7qzB4KVdb+4VoU0W2Et4eUuD/gknTp
    LLXozMcXjYEkiOhHKHftJveAClPQqsJT9i9tZgEC66Edjz64CyGJTmuEd0OJREtT o8Psi8p2kvrkzW
    /cMsnNDqKk5aQMfxKoxP1oTguymmcl/om0uvU7HKwBx+/ZXb4Z AgMBAAE= -----END PUBLIC KEY
    -----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArtzc/
    YfuAXcVbBF54C9k ohAk9QZB4lUAO4wlnN+bkvKMohOlWUMrDJw0fAFxN1AqNiamItA+q/bzNajaAo4
    J NCtpUhUdSWmp0TiHffxAk8pWxeubv6xNxXkq5UrBR8DsQCto/k0X5wKG5omzqHaB jJciXul0Ooh0
    XFZcgS0rZUdpqQvUEdOub2UzR+SAXmAfzvBM7y8eHDvYMVeRGZsU YsbMy9Fs2
    jzXLkHeZKVAqyVbteLG4NuZYYvpj8gXlBlE5yU5I1s6czNwZIucbsdY Yn0mWnhy86
    jcKQbSMCUvaRzF7nPyVBC+cQ1d37yqWpFoYRZPD/ySYt5fWUIqzk+E TwIDAQAB -----END PUBLIC
     KEY-----"
],
"finalvote1": [
"-----BEGIN PUBLIC KEY----- MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBP/tU1SlLd2
    EyjEC4Dwc0d kaUCD4WnsBaUmZo5Fh3ktPcQq9VVJbLF4EZ+tTXFFzSjhQl15isTz9SupPWum7YK
    juhUWeDPZ9MfMVOjR+6o4fc67h9NVxz8+gW5S0ceAQjEVrpUzCWQuWp7+M9PIaM0 WLuorccgHz8ib9
    Z1TjjPYEkodMs2jxT7sfGUlNCNcuBOPe797Rv5mdtbgrW3zEjF ZFO07GC6XwPcsMAa4jdBhtqnRW+
    RU08VwwP9dA+ITeOvxKYKpzidyI3lmYCSNFHy Oc50r/P2hwYdVvNJSjQHnQD0
    vUTjJjcCaDmdMvSEvnR4BgGvAqDnY31PFpFh15Ov AgMBAAE= -----END PUBLIC KEY-----",
"-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkkyJ+NS66
    jkNn83MZgEO cMnq2fg9saSOIy5meTRD/2h1h8PBHkU8QeytYVoACTn0i0nYuvZI7xkkJnDGrHIY V/
    UttpkZgDJMMTLr95MOGGVcd6eUoFiNXeWuCWJHk1ZBXd2+6rl4laBKdUyoLDOR u3RX1Xlp94
    rItXsvCI2NpKWbxIVq2y2zC+zfkA7w14VSUnXQwbS173sBJKENGvJK Q7WWOZ+iXDVhOIO/EXYBdKv7
    PIXDIDJD/lGC26Zux78+Zzwy0qpot5JBufHeVwnv HY2aMys3b9WgQuVueoXBYYBNdvFkJgt4V+Lc9
    ehngFlLsa2Wyaxe3LfZMBMlrogo dwIDAQAB -----END PUBLIC KEY-----"
],
"stage": "FINISHED",
"stance0": [2 items],
"stance1": [3 items],
"stances": [2 items],
"suggested_experts": {3 items},
"winning_stances": [
1,
1,
0
]
}
}
```

Bibliography

[1] *The Holy Bible International Version- Book of Genensis*, NIV. Biblica, 2011, vol. Genesis, 11:1–9.

[2] J. H. Kietzmann, K. Hermkens, I. P. McCarthy, and B. S. Silvestre, "Social media? get serious! understanding the functional building blocks of social media," *Business Horizons*, vol. 54, no. 3, pp. 241–251, May 2011. doi: 10.1016/j.bushor.2011.01.005.

[3] E. Bakshy, S. Messing, and L. A. Adamic, "Exposure to ideologically diverse news and opinion on facebook," *Science*, vol. 348, no. 6239, pp. 1130–1132, Jun. 2015. doi: 10.1126/science.aaa1160.

[4] S. Berkovsky and J. Freyne, "Web personalization and recommender systems," *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Aug. 2015. doi: 10.1145/2783258.2789995.

[5] N. Statt, *Facebook reportedly ignored its own research showing algorithms divided users*, May 2020. [Online]. Available: https://www.theverge.com/2020/5/26/21270659/facebook-division-news-feed-algorithms (visited on 12/20/2023).

[6] H. W. Jenkins, *Google and the search for the future - wsj*, Aug. 2010. [Online]. Available: https://www.wsj.com/articles/SB1000142405274870490110457542329409952 (visited on 11/16/2023).

[7] E. Pariser, *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin Books, 2012.

[8] M. Weiser, "The computer for the 21st century," *Scientific American*, vol. 265, no. 3, pp. 94–104, Sep. 1991. doi: 10.1038/scientificamerican0991-94.

[9] D. M. Lazer *et al.*, "The science of fake news," *Science*, vol. 359, no. 6380, pp. 1094–1096, Mar. 2018. doi: 10.1126/science.aao2998.

[10] M. E. Wojcieszak and D. C. Mutz, "Online groups and political discourse: Do online discussion spaces facilitate exposure to political disagreement?" *Journal of Communication*, vol. 59, no. 1, pp. 40–56, Mar. 2009. doi: 10.1111/j.1460-2466.2008.01403.x.

[11] H. Allcott and M. Gentzkow, *Social media and fake news in the 2016 election*, Jan. 2017. doi: 10.3386/w23089.

[12] J. Urakami, Y. Kim, H. Oura, and K. Seaborn, "Finding strategies against misinformation in social media: A qualitative study," *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 2022. doi: 10.1145/3491101.3519661.

[13] R. S. Nickerson, "Confirmation bias: A ubiquitous phenomenon in many guises.," *Review of General Psychology*, vol. 2, no. 2, pp. 175–220, 1998. doi: 10.1037//1089-2680.2.2.175.

[14] A. Tversky and D. Kahnema, "Availability: A heuristic for judging frequency and probability," *PsycEXTRA Dataset*, 1971. doi: 10.1037/e301722005-001.

[15] R. Westermann, "Festinger's theory of cognitive dissonance: A structuralist theory-net," *Structuralist Knowledge Representation*, pp. 189–217, Jan. 2000. doi: 10.1163/9789004457805_011.

[16] B. Warburg, B. Wagner, and T. Serres, *Basics of blockchain: A guide for building literacy in the economics, technology and business of Blockchain*. Animal Ventures, 2019.

[17] K.-C. Li, E. Bertino, X. Chen, and H. Jiang, *Essentials of blockchain technology*. CRC Press, Taylor and Francis Group, 2020.

[18] A. Y. Ogun, *Byzantine generals problem*, Sep. 2023. [Online]. Available: https://medium.com/@ayogun/byzantine-generals-problem-a47b33ef87fc (visited on 12/20/2023).

[19] G. O. Karame *et al.*, "Misbehavior in bitcoin," *ACM Transactions on Information and System Security*, vol. 18, no. 1, pp. 1–32, 2015. doi: 10.1145/2732196.

[20] B. Wu and B. Wu, *Blockchain for teens with case studies and examples of blockchain across various industries*. Apress, 2023.

[21] O. Goldreich, *Foundations of Cryptography*. Cambridge University Press, 2006.

[22] I. Bashir, *Mastering blockchain: Deeper insights into decentralization, cryptography, bitcoin, and popular blockchain frameworks*. Packt Publishing Ltd., 2017.

[23] S. M. Saad, R. Z. Radzi, and S. H. Othman, "Comparative analysis of the blockchain consensus algorithm between proof of stake and delegated proof of stake," *2021 International Conference on Data Science and Its Applications (ICoDSA)*, 2021. doi: 10.1109/icodsa53588.2021.9617549.

[24] S. Nakamoto, *Satoshi Nakamoto*, 2008.

[25] C. Zhang, C. Wu, and X. Wang, "Overview of blockchain consensus mechanism," *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, 2020. doi: 10.1145/3404512.3404522.

[26] M. S. Ferdous, M. J. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *Journal of Network and Computer Applications*, vol. 182, p. 103 035, 2021. doi: 10.1016/j.jnca.2021.103035.

[27] M.-S. Lee and K.-J. Kim, "Survey on blockchain evolution and proof-of-stake consensus algorithm," *International Journal of Engineering Trends and Technology*, vol. 69, no. 4, pp. 139–141, 2021. doi: 10.14445/22315381/ijett-v69i4p220.

[28] C. Smith, S. Richards, and A. K. Shin, *Ethereum roadmap*. [Online]. Available: https://ethereum.org/en/roadmap/ (visited on 12/23/2023).

[29] M. Chen, "Comparison on proof of work versus proof of stake and analysis on why ethereum converted to proof of stake," *Advances in Economics, Management and Political Sciences*, vol. 12, no. 1, pp. 200–204, 2023. doi: 10.54254/2754-1169/12/20230624.

[30] C. Walter, *Consensus*, 2019. [Online]. Available: https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-work/proof-of-meaningful-work-pomw (visited on 12/29/2023).

[31] K. Stadelmann, *Delayed proof of work (dpow) definition: Coinmarketcap*, Dec. 2022. [Online]. Available: https://coinmarketcap.com/academy/glossary/delayed-proof-of-work-dpow (visited on 12/27/2023).

[32] WhiteBIT and Solar, *What is delegated proof-of-stake?* Jun. 2023. [Online]. Available: https://blog.whitebit.com/en/what-is-delegated-proof-of-stake/#heading-6 (visited on 11/21/2023).

[33] M. Antolin, *What is proof-of-authority?* May 2023. [Online]. Available: https://www.coindesk.com/learn/what-is-proof-of-authority/ (visited on 12/27/2023).

[34] P. Khobragade and A. K. Turuk, "Blockchain consensus algorithms: A survey," *Lecture Notes in Networks and Systems*, pp. 198–210, 2023. doi: 10.1007/978-3-031-21229-1_19.

[35] T. I. Team and S. ANDERSON, *Proof of elapsed time (poet) definition, purposes, vs. pow*, Aug. 2023. [Online]. Available: https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp#:~:text=Proof%20of%20elapsed%20time%20(PoET)%20is%20a%20blockchain%20network%20consensus,following%20a%20fair%20lottery%20system. (visited on 12/29/2023).

[36] O. Seneviratne, "Blockchain for social good: Combating misinformation on the web with ai and blockchain," *14th ACM Web Science Conference 2022*, Jun. 2022. doi: 10.1145/3501247.3539016.

[37] Meta, *Why posts on instagram may be marked as false information*. [Online]. Available: https://help.instagram.com/388534952086572 (visited on 12/10/2023).

[38] D. Funke and D. Flamini, *A guide to anti-misinformation actions around the world*, Aug. 2019. [Online]. Available: https://www.poynter.org/ifcn/anti-misinformation-actions/ (visited on 12/10/2023).

[39] F. Miller, *Decentralized social media networks to join in 2024*, Dec. 2023. [Online]. Available: https://dailycoin.com/top-decentralized-social-media-networks/ (visited on 11/16/2023).

[40] S. Shyamson, *9 awesome decentralized social media platforms for 2023: Blocksurvey*, Jan. 2024. [Online]. Available: https://blocksurvey.io/web3-guides/decentralized-social-media-platforms (visited on 11/16/2023).

[41] S. Team, *A guide for newcomers*, Oct. 2020. [Online]. Available: https://steemit.com/guide/@steemitblog/steemit-a-guide-for-newcomers (visited on 12/10/2023).

[42] C. Staff, *An overview of the blockchain social media landscape*, Nov. 2023. [Online]. Available: https://www.gemini.com/cryptopedia/blockchain-social-media-decentralized-social-media#section-is-decentralized-social-media-the-future (visited on 12/10/2023).

[43] A. Siman, *A next gen content monetization platform*. [Online]. Available: https://subsocial.network/ (visited on 12/27/2023).

[44] M. B. Brewer, "The psychology of prejudice: Ingroup love and outgroup hate?" *Journal of Social Issues*, vol. 55, no. 3, pp. 429–444, Jan. 1999. doi: 10.1111/0022-4537.00126.

[45] Khai, *How students can benefit from anonymous discussions*, May 2023. [Online]. Available: https://www.kialo.com/tour.

[46] L. Neuburger, A. Clooney, H. Kennedy, and C. Yeginsu. [Online]. Available: https://www.unodc.org/dohadeclaration/en/news/2021/05/the-need-for-independent-judges-and-a-free-press-in-a-democracy.html (visited on 12/10/2023).

[47] E. Brooks, *What is the role of the judiciary? i liberties.eu*, Mar. 2023. [Online]. Available: https://www.liberties.eu/en/stories/role-of-judiciary/44724 (visited on 02/15/2023).

[48] E. RASURE and S. KVILHAUG, *Gas (ethereum): How gas fees work on the ethereum blockchain*, Sep. 2022. [Online]. Available: https://www.investopedia.com/terms/g/gas-ethereum.asp (visited on 01/11/2023).

[49] S. McKie, *The anatomy of erc20*, Oct. 2017. [Online]. Available: https://medium.com/blockchannel/the-anatomy-of-erc20-c9e5c5ff1d02 (visited on 01/11/2023).

[50] K. Team, *Komodo's dpow now supports litecoin notarizations for 51 attack protection*, Mar. 2022. [Online]. Available: https://komodoplatform.com/en/blog/dpow-litecoin-notarizations/ (visited on 12/29/2023).

[51] A. Zunino, *Council post: What are zero-knowledge proofs?* Feb. 2023. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2023/02/07/what-are-zero-knowledge-proofs/ (visited on 03/01/2023).

[52] L. Fortnow, "Review: Shafi goldwasser, silvio micali, charles rackoff, the knowledge complexity of interactive proof systems; oded goldreich, silvio micali, avi wigderson, j. gruska, b. rovan, j. wiedermann, proofs that release minimum knowledge; oded goldreich, rolf herken, randomness, interactive proofs, and zero-knowledge–a survey," *Journal of Symbolic Logic*, vol. 56, no. 3, pp. 1092–1094, Sep. 1991. doi: 10.2178/jsl/1183743759.

[53] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," in *Journal of Critical Reviews*, vol. 7, 2020, pp. 79–84. doi: 10.31838/jcr.07.03.13.

[54] O. S. Saleh, O. Ghazali, and N. B. Idris, "A new decentralized certification verification privacy control protocol," in *2021 3rd International Cyber Resilience Conference (CRC)*, 2021. doi: 10.1109/CRC50527.2021.9392485.

[55] R. Li and Y. Wu, "Blockchain based academic certificate authentication system overview," *IT Innovation Centre University of Birmingham*, 2018, Available: https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockc based-Academic-Certificate-Authentication-System-Overview.pdf.

[56] D. H. Nguyen, D. Nguyen-Duc, N. Huynh-Tuong, and H. A. Pham, "Cvss: A blockchainized certificate verifying support system," in *ACM International Conference Proceeding Series*, 2018, pp. 436–442. doi: 10.1145/3287921.3287968.

[57] N. Karanikolas *et al.*, "Large language models versus natural language understanding and generation," in *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics*, ser. PCI '23, <conf-loc>, <city>Lamia</city>, <country>Greece</country>, </conf-loc>: Association for Computing Machinery, 2024, pp. 278–290, isbn: 9798400716263. doi: 10.1145/3635059.3635104. [Online]. Available: https://doi.org/10.1145/3635059.3635104.

[58] Brook and C. Messinger, *Polis: Why and how to use it - ea forum*, Feb. 2023. [Online]. Available: https://forum.effectivealtruism.org/posts/9jxBki5YbS7XTnyQy/polis-why-and-how-to-use-it#:~:text=pol.is%20is%20the%20main,the%20tradition%20of%20nonviolent%20communication. (visited on 03/14/2023).

[59] J.-E. Ekberg, K. Kostiainen, and N. Asokan, "The untapped potential of trusted execution environments on mobile devices," *IEEE Security and Privacy*, vol. 12, no. 4, pp. 29–37, 2014. doi: 10.1109/msp.2014.38.

[60] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck," *Proceedings of the 1st Workshop on System Software for Trusted Execution*, Dec. 2016. doi: 10.1145/3007788.3007790.

[61] A. Bakar, A. Zouhair, and E. M. En-Naimi, "Review of vulnerabilities and countermeasures against sybil attacks on decentralized systems based on machine learning algorithms," in *Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security*, ser. NISS '23, <conf-loc>, <city>Larache</city>, <country>Morocco</country>, </conf-loc>: Association for Computing Machinery, 2023, isbn: 9798400700194. doi: 10.1145/3607720.3607751. [Online]. Available: https://doi.org/10.1145/3607720.3607751.

[62] W. E. Williams, *Fairness: Results versus process*, Oct. 1998. [Online]. Available: https://fee.org/articles/fairness-results-versus-process/ (visited on 03/03/2023).

[63] M. K. Lee *et al.*, "Procedural justice in algorithmic fairness: Leveraging transparency and outcome control for fair algorithmic mediation," vol. 3, no. CSCW, 2019. doi: 10.1145/3359284. [Online]. Available: https://doi.org/10.1145/3359284.

[64] J. Haidt, *What are the fairness buttons?* Oct. 2023. [Online]. Available: https://righteousmind.com/what-are-the-fairness-buttons/ (visited on 03/01/2023).

[65] H. Vainio-Pekka *et al.*, "The role of explainable ai in the research field of ai ethics," *ACM Transactions on Interactive Intelligent Systems*, vol. 13, no. 4, pp. 1–39, Dec. 2023. doi: 10.1145/3599974.

[66] A. K. Sen, "Democracy as a universal value," *Journal of Democracy*, vol. 10, no. 3, pp. 3–17, Jul. 1999. doi: 10.1353/jod.1999.0055.

[67] B. Güroğlu *et al.*, "Dissociable brain networks involved in development of fairness considerations: Understanding intentionality behind unfairness," *NeuroImage*, vol. 57, no. 2, pp. 634–641, Jul. 2011. doi: 10.1016/j.neuroimage.2011.04.032.

[68] J. H. Fowler and N. A. Christakis, "A random world is a fair world," *Proceedings of the National Academy of Sciences*, vol. 110, no. 7, pp. 2440–2441, Jan. 2013. doi: 10.1073/pnas.1222674110.