Voting Schemes in DAO Governance

Mar 2023

Qinxu Ding, Weibiao Xu, Zhiguo Wang, David Lee Kuo Chuen[*][†]

[*] ChartGPT, OpenAI. It assisted in some basic research and enhanced the flow of the thoughts in this article.
[1] [†] School of Business, Singapore University of Social Sciences.

Abstract: This article aims to provide a comprehensive overview of the different voting schemes used in DAO governance. We will examine the various features of these schemes and compare their differences. We propose a new hypothetical voting mechanism specifically designed for decentralized and permissionless DAO governance. This new scheme, which incorporates incentive designs, is intended to be more efficient than existing schemes and can be easily adapted to a permissioned scenario. Through this examination and proposal, we hope to contribute to the ongoing discourse on how to govern decentralized autonomous organizations effectively.

Keywords: Voting process, DAO, Governance

JEL codes: D02; D70; G30; Z0

1. Introduction

A decentralized autonomous organization (DAO) is an emerging legal organization structure (El Faqir et al., 2020; Hassan and De Filippi, 2021). It is not controlled by a single entity such as a government or central bank. It is decentralized among various members, such as computers, networks, and nodes. In contrast, governance used to be a concept in a centralized manner. It is to reflect some parties' decisions or views on others. A DAO is run according to computer codes rather than by a group of individuals. The rules and processes of the organization are encoded into a smart contract and are executed automatically. Typically, DAOs are decentralized and run on blockchain networks, meaning that they operate autonomously and are not controlled by a central authority.

On the other hand, governance refers to the process by which decisions are made, and rules are established in an organization. For blockchain and cryptocurrency, governance often refers to the process by which changes to a blockchain protocol or the rules of a cryptocurrency are proposed, debated, and implemented. This can include changes to the consensus algorithm, the addition of new features, or the allocation of funds. In summary, a DAO is a type of organization that is wholly run by a smart contract, whereas governance is the process of decision-making and rule-making for an organization. DAOs can use governance to make decisions. The way to embed the governance component into a DAO is a crucial issue and this must be decided initially. The governance scheme should incentivize the members to achieve a common goal to improve the DAO.

Current literature in management is mainly focusing on the relationship between DAOs and corporate governance. For example, many studies investigate how DAO could transform and improve corporate governance (Yermack, 2017; Kaal, 2019; Morrison, et. al, 2020). But we believe DAO governance per se is an interesting topic to investigate. DAO governance represents a new paradigm in organizational management, that is self-governance with a bunch of self-executed rules. The mechanism to achieve an agreement among humans in a democratically governed system is through voting and with the aim of reducing the centralization feature of governance (Zhao et al., 2022), allowing for a more equitable distribution of power among stakeholders.

In computer science, voting schemes are often studied under the subfields of cryptography, distributed systems, and algorithm design. They mainly focus on the concerns related to security or privacy for the voting designs (Chaum, 1981; Benaloh, 1987; Boyd, 1990; Fujioka et al., 1993; Sako and Killian, 1995; Cramer et al., 1997; Jakobsson et al., 2002, Neff, 2004; Sampigethaya and Poovendran, 2006; Ribeiro and Joaquim, 2012). For example, Neff (2004) introduces the MarkPldege (MP) technique to provide high "vote encryption assurance" to the voter. His research aims to assure the voter that the vote is encrypted.[3] Encrypting the votes ensures that they cannot be tampered with or changed during the voting period and makes it impossible to link a voter with their vote. This is important for maintaining the integrity of the voting process and ensuring that the results accurately reflect the will of the voters. Ribeiro and Joaquim (2012) extended and developed MarkPledge3 (MP3) to allow the voter to verify that her vote is correctly encrypted.

The existing discussions are either on the comparison between DAO governance and corporate governance or on specific technological implementations. However, there is little research covering efficiency, fairness, and self-motivated designs in the voting process mechanism. We fill the gap by looking into the practical voting schemes that are widely used in real applications and try to propose a new scheme from the perspective of design thinking.

2. DAO Voting Mechanisms

This section will review prevailing voting schemes used in DAO platforms. There are many types of practical voting schemes available in the DAO industry. Specifically, we will cover eight prevailing voting schemes: Token-based quorum voting, Quadratic voting, Weighted voting& Reputation-based voting, Knowledge-extractable voting, Multisig voting, Holographic consensus, Conviction voting, and Rage Quitting voting. A simple comparison will be presented in the end.

2.1 Token-based quorum voting

Quorum voting is a commonly used mechanism in DAO governance. For any given proposal, the participating voters in the voting process must exceed the certain pre-set threshold (e.g., 50% or 60%) of the total voters, or else the proposal will automatically be rejected. The threshold could vary according to protocols. After passing the threshold requirement or quorum, the proposal with higher votes will be approved. This ensures that a sufficient number of voters are participating in the decision-making process and also ensures that any proposal that is approved has the support of a significant portion of the community.

[3] Vote encryption assurance, also known as end-to-end verifiable voting, is a method used to ensure the privacy and integrity of voting in electronic voting systems. It involves encrypting the votes before they are cast, and then decrypting them only after the voting period has ended. This allows for the voter to verify that their vote has been correctly recorded, while also maintaining the anonymity of their vote. It also allows for the public to verify that the vote counting was done correctly without exposing the individual votes. The use of encryption in voting systems is a key component in ensuring the security and transparency of the voting process.

This threshold can vary depending on the specific protocol. One of the advantages of this protocol is that it allows a proposal to be approved even if voter turnout is low, as long as a sufficient number of voters support the proposal, unlike the quorum voting. This protocol is used by several DAOs such as Compound, Curve, and Kleros, and it is gaining popularity due to its simplicity and the fact that it doesn't require reaching a quorum.

The threshold could be measured in terms of tokens, where voters must hold a certain amount of tokens to be eligible to vote, or it could be measured in terms of voter participation, where a certain percentage of eligible voters must participate in the voting process for a proposal to be considered. While pure token-based voting is a popular voting scheme in DAO governance, it has some issues. The major one is that voters who hold more tokens than others, could dominate the decision-making process, effectively giving them a disproportionate amount of influence. Additionally, the participant threshold required for this protocol can be costly and time-consuming as it requires a high voter turnout each time a proposal is put forward. Moreover, it is controversial to determine the optimal threshold level because an improper threshold will make the proposal too easy or too difficult to pass. Setting the threshold too high can make the decision-making process too restrictive, potentially leading to good proposals being rejected. On the other hand, setting the threshold too low can result in low-quality proposals being approved. It's important to find a balance in setting the threshold level to ensure that the decision-making process is fair and effective.

KyberDAO and Aave are examples adopting this voting scheme (Table 1).

Examples	Description
KyberDAO	KyberDAO is a decentralized exchange that allows users to trade cryptocurrencies. The platform operates through a DAO, in which token holders can vote on proposals related to the development and governance of the platform. The KyberDAO held the first public poll for the community on collecting the design of voting quorum/thresholds and participation incentivization methods.
Aave	Aave is a decentralized lending and borrowing platform that operates through a DAO. Token holders can vote on proposals related to the management and development of the platform. The number of votes required to pass a proposal is based on the number of tokens held by each voter.

Table 1 Examples for the applications of token-based quorum voting

2.2 Quadratic voting

Vitalik Buterin, the co-founder of Ethereum, has proposed a quadratic voting scheme as an alternative to the traditional "1 token 1 vote" and "1 person 1 vote" models. Unlike "1 token 1 vote" which gives a proportional voting power based on the number of tokens held and "1 person 1 vote" which allocates a single unit of voting power to each voter, quadratic voting allows voters to express the intensity of their preferences by allocating multiple units of voting power to a single proposal. This approach aims to strike a balance between giving each voter equal representation while also taking into account the economic stake that a voter holds in the DAO, and the level of importance they assign to a particular proposal.

Under the quadratic scheme, voters can buy tokens and use those tokens to gain greater voting power (Quarfoot et al. 2017). The scheme allows each voter to vote on the same proposals with multiple voting power but tries to avoid monopoly from single token holders. The voting power is increased by the square of the number of tokens, i.e., it needs N^2 for N votes from the same voter. For example, one vote needs one token. If the voter wants one more vote, it needs 2^2 =4 tokens. So the voting power is the square root of the token. It is costly for a single voter to dominate the voting process.

The quadratic voting scheme has several advantages over traditional voting mechanisms. This approach addresses some of the issues from traditional token-based voting, such as the potential for larger token holders to dominate the decision-making process and allows for a more nuanced representation of preferences. One of the main advantages is that it incentivizes voters to only vote on proposals that they are truly passionate about, as the cost of voting increases with the number of votes cast. This helps to avoid the problem of voters casting votes on proposals they are not truly invested in, which can lead to poor decision-making. Additionally, by allowing voters to express the intensity of their preferences, it helps to protect the voting rights of minorities, and ensures that even small groups can have a significant impact on governance.

However, there are also some potential downsides to this approach. One of the main criticisms is that voting power is still a function of wealth, which could lead to plutocracy, or rule by the wealthy. This is not in line with the principle of radical democracy that is often associated with blockchain technology. Moreover, this scheme needs a mechanism to verify the voter. Otherwise, a simple Sybil attack by bots or faking multiple identities will adversely affect the voting.

Gitcoin and BrightID are examples that adopted this voting scheme.

Examples	Description

Gitcoin	Gitcoin is a decentralized platform for funding open-source projects. Gitcoin uses QV for its quadratic funding mechanism, which allocates funds to projects based on the number of votes they receive from individual contributors. Contributors can allocate a budget of votes to different projects, with the number of votes for each project being the square root of the budget allocated.
BrightID	BrightID is a decentralized identity verification platform that aims to prevent sybil attacks (i.e. the creation of multiple fake identities) on decentralized networks. BrightID has incorporated quadratic voting into its platform to help incentivize users to participate in verification activities. In BrightID's quadratic voting system, users are given a certain number of tokens (called "Bright Tokens") that they can use to vote on proposals related to identity verification activities.

Table 2 Examples for the applications of quadratic voting

2.3 Weighted voting & reputation-based voting

Weighted voting refers to a voting system where each voter has a certain number of votes they can cast, and the weight of each vote is determined by the number of votes a voter has. This means that a voter with more votes has a greater influence on the outcome of the vote compared to a voter with fewer votes.

Reputation-based voting, on the other hand, is a voting system where the weight of a voter's vote is determined by their reputation or trustworthiness within the community. Voters are assigned a certain amount of reputation or influence based on factors such as their past contributions to the DAO, their level of engagement, or sometimes their stake in the DAO. This means that voters who are deemed more trustworthy or have a higher reputation within the community have a greater influence on the outcome of the vote compared to those with a lower reputation. This voting scheme usually weighs voters by considering the contributions a voter made rather than pure token holdings. Specifically, the voters with a track record are rewarded with a portable reputation, and the reputation will put more weight on their votes.

Under this mechanism, reputation instead of wealth has a significant effect. Track record is one measure of reputation. The length of time that users hold specific tokens could be also considered a measure of reputation or conviction or the alignment of interests. Reputation is like a credit accumulated by a timing process or contributions to DAO community. It is less likely to be transferred or traded. The reputation could be dynamic. For example, reputation could expire or diminish with time to avoid the effects of early easy-gainers and maintain fairness to all voters.

The weighted voting and reputation voting increase the difficulty of Sybil attacks, although the risk still exists. It is relatively more efficient and sustainable than token-based voting. Nevertheless, it could be challenging to build up a proper reputation system (Zhuang et al., 2019). BPC DAO and OrangeDAO are examples of adopting a reputation-based voting system.

Examples	Description
BPC DAO	The BPC DAO Voting Portal is an online application powered by Web3, which is being used by the BPC DAO to involve Ndau[4] holders in shaping the future of Ndau. Using this portal, all Ndau holders can suggest novel proposals and cast their votes on existing ones. The voting power of participants is calculated based on the amount of Ndau they own and their currency seat status, which is explained in the Ndau whitepaper. The voting process is designed to be weighted appropriately to guarantee equitable representation of all contributors.
OrangeDAO	OrangeDAO is collaborating with Snapshot to bring reputation-based voting to life. Snapshot has expansive DAO voting dataset while OrangeDAP has the capabilities to produce customizable reputation reports, resumes and NFTs. The combination can act as algorithm providers to create voting structures that more accurately reflect the sentiment of the community.

Table 3 Examples for the applications of weighted voting & reputation-based voting

2.4 Knowledge-extractable voting (KEV)

Knowledge-extractable voting is a type of voting system in which the knowledge or expertise of voters is taken into account when determining the outcome of a vote. This can be done by allowing voters to indicate their level of expertise on a given subject, or by using algorithms to assess the quality of their contributions to a discussion or debate.

The goal of knowledge-extractable voting is to ensure that decisions are made based on the collective wisdom of the group, rather than just the preferences of a small number of individuals. This voting scheme can be used in a variety of contexts, including online communities, decentralized autonomous organizations (DAOs), and other forms of collective decision-making. This knowledge-extractable voting scheme tries to allocate more weight to the vote from more knowledgeable experts. Under this scheme, the proposals will be categorized into different areas. Each area has a representative token. The token can be used

[4] Ndau aims to be the world's first adaptive digital currency, designed with a goal of a long-term store of value with staking income

to enhance the effect of the votes by putting more weight. In other words, the final voting outcome depends on a weighted average of the votes by using the knowledge tokens as weights.

KEV provides incentive schemes for voters to vote based on their expertise. The voters who use knowledge tokens as weights will be rewarded with more tokens if the proposal is passed. However, the tokens held will be reduced if the proposal fails. Therefore, voters without sufficient knowledge to judge the proposal are discouraged from voting. The knowledge tokens could not be transferred or traded. So, voters could not manage their voting effects by loopholes or other mechanisms that allowed them to increase their knowledge tokens.

This scheme is newly designed[5] and receiving attention in the industry. DIT Protocol (Decentralized Information Theory) is an example of using this voting scheme[6]. It is a decentralized protocol that aims to incentivize the creation and sharing of knowledge, by allowing users to vote on the quality and relevance of information. It is based on a reputation-based system, where users acquire reputation points by contributing valuable information, and can then use these points to vote on the relevance of other users' submissions. The DIT Protocol is intended to provide a decentralized and self-governing platform for knowledge sharing, where users can collectively curate and organize information.

2.5 The multisig voting

Multisig voting is a voting mechanism where multiple signatures or approvals are required before a proposal can be executed. It is typically used as a security measure to ensure that a certain level of consensus is reached before any action is taken on the blockchain. In a multisig voting system, a group of users, known as signers, are required to sign off on a proposal before it can be implemented. This can help prevent a single person or group from making unilateral decisions and ensure that decisions are made through a more democratic process. Multisig voting is often used in the context of DAOs and other decentralized systems. Multisig Voting stipulates the members who will have a private key and the minimum number of key holders needed for a transaction to be approved (Petersen et al., 1995; Noizat, 2015). For example, a 7-of-10 multisig protocol would require seven out of ten parties to sign off on a transaction before it could be executed. This means that in a DAO with ten private

[5] https://hackernoon.com/knowledge-extractable-voting-for-blockchain-distributed-governance-radically-new-mechanisms-ed2ca47f065f
[6] https://www.ditcraft.io/dl/ditcraft_whitepaper.pdf

keys, the proposal would require the approval of at least seven key holders in order to pass. Then seven key holders are enough to govern the DAO.

Multisig voting is usually used to manage pooled DAO funds, and it requires a certain number of members to sign off for transferring actions. The mutli-signature fund management solutions can prevent any DAO member from moving funds on their own. Multisig voting requires a multi-signature wallet, which enables multiple owners to control their shared assets.

The main advantage of this voting scheme is its security. It provides a backup plan in case something goes wrong. It ensures that each transaction is thoroughly verified before it is completed.

This voting scheme is for some typical proposals, especially for fund management. It is not a general voting scheme for all types of proposals. It's often recommended for organizations that prefer advanced security and privacy. The scheme could be much faster if the multikey holders can sign efficiently. However, adding the extra signature requirements might also cause inefficiency for a transaction if the number of key holders is not quickly reached. Moreover, setting up a multisig wallet might require the members to have some basic technical knowledge. More importantly, it is also possible that the multi-sig key holders can collude to make decisions against the interests of the other DAO members. Gnosis Safe, Aragon Client DAOs and BitDAO (Table 4) are examples that used this voting scheme.

Examples	Description
Gnosis Safe	Gnosis Safe is a multi-sig wallet that allows users to securely store and manage their cryptocurrency assets. It is built on the Ethereum blockchain and utilizes smart contract technology to provide users with a user-friendly and secure way to manage their digital assets. The Gnosis Safe uses a multisig voting system, which means that multiple signatures are required to authorize a transaction. This is designed to provide an additional layer of security and prevent unauthorized access to user funds. Additionally, Gnosis Safe also provides users with a range of advanced features, such as support for ERC-20 and ERC-721 tokens, a customizable user interface, and integration with decentralized applications (dApps).

Aragon Client	Aragon Client is a decentralized application (dApp) built on the Ethereum blockchain that allows users to create and manage decentralized autonomous organizations (DAOs). It provides a user-friendly interface for creating and customizing DAOs, as well as tools for managing and voting on proposals within the organization. The Aragon Client is built on the Aragon Network, a platform for building decentralized organizations that aims to make it easy for anyone to create and manage a DAO. The Aragon Client is an open-source project and is governed by the Aragon Association, a non-profit organization that oversees the development and maintenance of the Aragon Network.
BitDAO	BitDAO supports builders of the decentralized economy. It is an open platform for proposals that are voted upon by BIT token holders, and is agnostic to chains and projects.

Table 4 Examples for the applications of multisig voting

2.6 Holographic Consensus

Holographic consensus is a proposed mechanism for achieving consensus in a decentralized system. The idea is that the consensus of a large number of low-power nodes can be inferred from the consensus of a smaller number of high-power nodes, similar to how the information on the boundary of a region is equivalent to the information inside the region[7]. The mechanism is also a variant of futarchy, which is based on the notion that the market participants are more efficient and smarter than the elected voters at predicting outcomes.[8] This allows for more efficient and scalable consensus compared to traditional methods. Holographic consensus is a governance mechanism initiated by DAOstack.

By staking their tokens, users can influence the direction and governance of the DAO, and may also be eligible for rewards or other benefits. The exact mechanics of staking in a DAO can vary depending on the specific organization, but generally involve holding and locking up a certain amount of tokens for a certain period of time in order to participate in the DAO's governance.

[7] Holographic principle states that the information on the boundary of a region is equivalent to the information inside the region. Imagine a holographic image, the information that creates the image is encoded on the boundary of the holographic film, this information is equivalent to the information of the whole image that is inside the film. In the context of consensus, the idea is that the consensus of a large number of low-power nodes in a decentralized system can be inferred from the consensus of a smaller number of high-power nodes. Just as the information on the boundary of a holographic film is equivalent to the information inside the film, the consensus of a small group of high-power nodes is equivalent to the consensus of the entire network of low-power nodes.

[8] https://blog.ethereum.org/2014/08/21/introduction-futarchy

Any user who satisfies reputation requirements could submit the proposals. But only the proposals with enough attention are more likely to be reviewed and voted. According to the voting mechanism, small groups will make decisions on behalf of the majority. An incentive is provided to align the interest between the voting group and the majority. However, DAOs are large organizations, and many proposals could be submitted. DAOstack brings in a cryptocurrency called GEN to select the proposal with the most potential for the voting group.

GEN can be used as a stake for or against a proposal. It is like a bet on the submitted proposals. The proposal with most GEN will catch the collective attention of the voters. If anyone stakes for the proposal and the proposal is passed, he/she can be awarded more GENs. However, if the proposal fails, the betting GEN will be taken. Therefore, in order to bet on the right proposal, the GEN stakers will investigate each proposal and make sure they bet on the most potential one. Thus, the one with the highest attention could be more likely to benefit the future of the DAO.

The GEN token is to tap the incentive structure for improving DAOstack ecosystem. Using GEN enables both stakers and voters to be in the same ecosystem, so they have the same interest in making DAOstack more useful and making GEN more valuable. Using other cryptocurrencies like Ether might deviate the purpose to other uses.

The staking system enables anyone with GEN to predict and choose most DAO-aligned proposals, so the proposal with top attention is more likely to be passed. The passing requirements could be dynamic according to the staking system. The proposal with high potential could be passed quickly with fewer votes than other proposals. Thus, a smaller group of voters could effectively vote for the whole voter group and make quick decisions with value alignment.

Holographic consensus has some potential benefits. For example, it can potentially scale to very large, decentralized organizations, as it allows for stakeholders to participate in decision-making without requiring a direct vote on every issue; It provides a transparent and auditable way for stakeholders to track decision-making in decentralized organizations. By allowing stakeholders to view the voting history and results, as well as the reasoning and arguments behind decisions, it can help to build trust and promote more accountable governance. Moreover, it can potentially increase voter engagement and participation by allowing stakeholders to delegate their voting power to trusted third parties or to participate in specific issue-based votes. This can help to promote a more active and engaged community of stakeholders in decentralized organizations. However, there is no free lunch. The drawback of this voting scheme could be the possibility that the one with high attention and influence might be due to some hype and the one with more valuable potential might thus be neglected.

DXdao, necDAO and DAOstack are examples (Table 5) that adopted this voting scheme.

Examples	Description
Dxdao	DXdao is a decentralized autonomous organization that operates a suite of DeFi protocols. The organization recently implemented holographic consensus voting to allow its token holders to participate in decision-making regarding the allocation of resources and the direction of the protocol.
necDAO	necDAO is built atop the DAOstack framework and uses holographic consensus through the alchemy interface.
DAOstack	DAOstack is a platform for building and managing decentralized autonomous organizations (DAOs) on the Ethereum blockchain. It provides a set of tools and frameworks that enable individuals and groups to collaborate and make decisions in a decentralized and transparent manner.

Table 5 Examples for the applications of holographic Consensus voting

2.7 Conviction Voting

Conviction voting is a newly developed voting scheme, which is based on both aggregated preference and time. It is designed to align the interests of token holders with the long-term success of the organization. In a conviction voting system, members of the community can vote on proposals by staking their tokens for a certain period of time. The longer the stake period, the more "conviction" a member has in their vote and the more weight their vote carries. This system is designed to incentivize community members to think carefully about the long-term implications of their vote and to discourage short-term thinking and speculation. By staking their tokens for a longer period of time, members signal that they are more confident in the proposal and that they believe it will be beneficial for the organization in the long run.

Examples	Description
Giveth	Giveth is a community-driven platform that uses Conviction voting to allocate funds and resources to various projects. With Conviction voting, Giveth allows stakeholders to allocate tokens to specific projects or causes, and the allocation of funds is based on the strength of conviction of stakeholders, rather than just their token holdings.

Common Stack	Common Stack is a DAO platform that uses Conviction voting to make decisions about the allocation of funds and resources. With Conviction voting, stakeholders can pledge their tokens to different initiatives, and the allocation of funds is based on the strength of conviction of each stakeholder.
MetaCartel	MetaCartel is a DAO platform that uses Conviction voting to make decisions about the allocation of funds and resources to various projects. With Conviction voting, stakeholders can pledge their tokens to specific initiatives, and the allocation of funds is based on the strength of conviction of each stakeholder.

Table 6 Examples for the applications of conviction voting

2.8 Rage Quitting Voting

Rage quitting is a term used to describe a phenomenon that can occur in decentralized autonomous organizations (DAOs) and other decentralized communities that use token-weighted voting systems. It refers to the scenario where a token holder, who is unhappy with the outcome of a vote or the direction of the organization, decides to withdraw their stake and sell their tokens, rather than continuing to support the organization. This can have a negative impact on the organization, as it can lead to a decrease in the value of the token, and it can also lead to a lack of participation in future votes.

Quitting voting is initiated by Moloch DAO and is well accepted by many DAOs using the DAOhaus platform. In a Moloch DAO, membership should be approved and permissioned by the existing full-share members. Upon approval, each member can hold either full shares or loot shares. The difference between these two shares is that the full share has both voting rights and "Ragequit" rights, while the loot share only has "Ragequit" rights. The "Ragequit" refers to a quitting mechanism for each member. The members can quit a DAO and redeem their shares in the grace period after the approval of the proposal if the approval does not align with their interests.

Proposals could be submitted by anybody (including non-members). However, they should be supported by at least one member for proceeding to the voting process. The voting process is simply collecting 'agree' or 'disagree' votes from the members and passing if the 'agree' is more than 'disagree'. It does not have a quorum requirement. In some DAOs with such a voting scheme, the vote is by default considered as 'agree' if the member does not vote for 'disagree'.

When the proposal is passed, there will be a grace period. Those who voted 'disagree', can withdraw their shares before the proposal's implementation. This is the "Ragequit" design so that some minor members are allowed to escape before an unwanted proposal that might represent the majority's tyranny. For example, suppose the majority members (say, 70%) would like to pass a proposal which benefits themselves (by exploiting the benefits of the rest 30% minority). In that case, the minority can protect their treasury with the "Ragequit" mechanism.

The advantages of the mechanism are sound. For example, it is a secure system against Sybil attacks as the voting is done within a permissioned group, and members are protected. It scales trustless coordination with more stakeholders than other voting mechanisms like Multisig.

The downside is that the mechanism takes time to approve any proposal, given that there is a grace period. If the proposal is in urgent need, this might not be efficient. To address this concern, Moloch DAO also introduces Minion as a supplement. Minions need a quorum, that there are sufficient "Agree votes" and no "Disagree" votes, to allow early execution on proposals without "Ragequit" and the grace period. However, this modification changes the security properties of a DAO's funds, especially when the stakes in the proposal are high enough. There is a trade-off between security and efficiency. To avoid rage quitting voting, organizations can implement different measures like reducing the token liquidation speed, or making it difficult to withdraw the stake, making sure that the token holder has to wait a certain period of time before they can withdraw the stake.

MetaCartel Ventures, MolochDAO and DAOhaus[9] are experimenting with this voting scheme (Table 7).

Examples	Description
MolochDAO	MolochDAO is a collective that funds Ethereum-based projects. In MolochDAO, members can rage quit if they disagree with a proposal that has passed by submitting a request to exit the DAO and retrieving their staked tokens.

[9] https://daohaus.mirror.xyz/U_JQtheSzdpRFqQwf9Ow3LgLNG0WMZ6ibAyrjWDu_fc

MetaCartel	MetaCartel is a DAO that funds Ethereum-based projects. In MetaCartel, members can also rage quit if they disagree with a proposal that has passed by withdrawing their funds from the DAO.
DAOhaus	DAOhaus is a decentralized autonomous organization (DAO) that operates on the Ethereum blockchain. In a DAO, decisions are made by token holders who vote on proposals using their tokens. Anyone who contributed funds can vote with their dollars if they don't like our direction.

Table 7 Examples for the applications of Rage Quitting Voting

2.9 Appraisal of the Schemes

We follow the literature to compare each voting system from five aspects as follows (Sampigethaya and Poovendran, 2005; Wu et al., 2014; López García, 2016).

Efficiency: Speed of selecting the potential proposals and approval of urgent proposals.

Fairness: Each voter has equal rights to vote.

Scalability: Ability to adjust storage, computation, and communication needs according to the number of voters.

Robustness: The resistance to attacks or collusion.

Incentive Schemes: Whether the design motivates the behavior of participants.

	Efficiency	Fairness	Scalability	Robustness	Incentive Schemes
Token-based Quorum voting	Medium	High	Low	Low	Not
Quadratic Voting	Medium	Low	Medium	Medium	Not
Weighted Voting & Reputation-based Voting	Medium	Low	Medium	High	Yes
Knowledge-extractable Voting	Medium	Low	Medium	High	Yes
The Multisig Voting	Medium	High	Low	Low	Not
Holographic Consensus	High	High	High	Medium	Yes
Conviction Voting	Low	Medium	Medium	High	Not
Rage Quitting Voting	Low	High	Medium	Medium	Not

Table 8 Comparison of listed schemes

The comparison in Table 8 is a relative appraisal. We can see that there is not any 'perfect' scheme. There are pros and cons for all the schemes. A compromise approach is to combine some voting schemes and tries to design a better one. We propose a new scheme with prominent features from Holographic consensus and conviction voting.

There could be other voting scheme concepts. For example, liquidity voting, a.k.a. proxy voting. The idea behind liquid voting is to align the interests of token holders with the interests of the DAO. By giving token holders more voting power in proportion to the number of tokens they hold, the system incentivizes them to hold onto their tokens and engage with the DAO, rather than selling them. This helps to ensure that the long-term health and success of the DAO is aligned with the interests of its token holders. Some of the voting schemes introduced in the paper could be a variant to the liquidity voting, e.g., quadratic liquidity voting is a hybrid scheme to apply the quadratic notion with a liquidity voting concept.

3. A New Voting Design Notion

This section proposes a new hypothetical voting mechanism for a purely decentralized and permissionless DAO governance. We focus on permissionless characteristics as it is more general. The design is to accelerate conviction voting with a Holographic mechanism.

We first define the voting member as the stakeholder of a DAO. The DAO governance power is represented as the stakes of all the resources. If we tokenize the resources, the address with at least one token stake is considered a member. The membership is permissionless, but the interest is aligned as it might be costly to obtain the token. To avoid excess voting power from vast new members or large-stake members, the basic voting process will follow conviction voting. Therefore, time and stake are both essential for passing the proposals, the same as traditional conviction voting.

For any proposal submitted, we dynamically introduce an estimated duration of the proposal (e.g., the average duration of recent proposals). If the proposal cannot be passed within this pre-estimated duration, it will fail automatically. In other words, we introduce a veto possibility into conviction voting.

We know that the downside of the conviction voting mechanism is that it takes time to approve an urgent proposal. To address this concern, we introduce a blind betting mechanism: Each member could choose whether to bet on any proposals with a certain number of their tokens. The betting is unseen to all the betters. If there are more betting tokens of "pass" than "veto", the governance power will be accelerated, and the proposal could be approved faster. If there are more betting tokens of "veto" than the "pass", the governance power will be slowed down, and the proposal could fail faster.

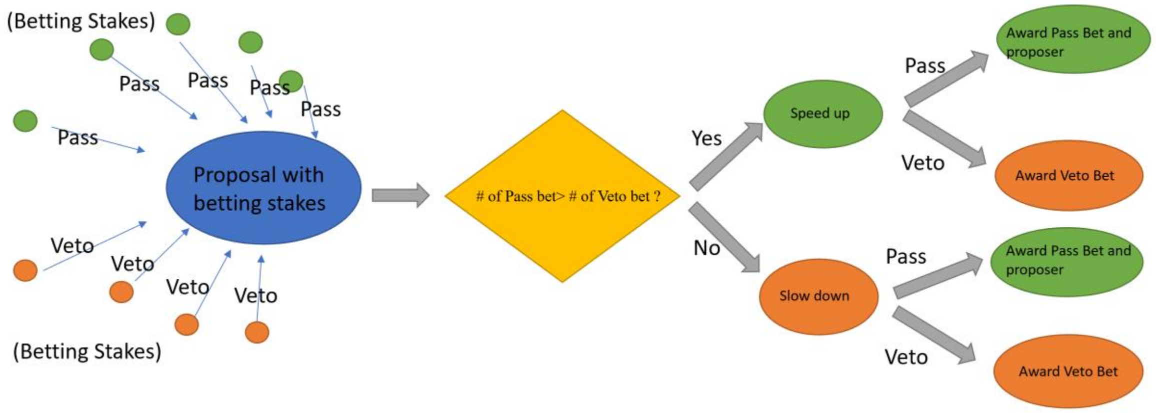

Figure 1 Voting and Rewarding Process

Incentive schemes are introduced in the betting process. If the proposal passes, the betting tokens of "veto" will be confiscated. Some of the confiscated amounts will be used to award the proposal submitter, and the rest will be distributed to the one with betting tokens of "pass" proportionally according to the bet. If the proposal fails, the " pass " betting tokens will be confiscated. However, there is no reward for the proposal submitter, and the confiscated tokens will be distributed to the one with betting tokens of "veto" proportionally according to the bet. Because it is a blind betting process, it is possible that there is only one way of betting, i.e., if all are betting "pass" or betting "Veto", then no rewards will be distributed. Nevertheless, the proposal will still be accelerated or slowed down.

Under the incentive schemes, everyone is incentivized to submit a good proposal that is more likely to pass and get rewarded. More importantly, the betting process provides incentives for voters to vote carefully if they place a bet on the proposal. Urgent and good proposals could be speeded up and approved faster. It is more efficient than a pure conviction voting mechanism.

The proposed scheme could be easily extended to a permissioned scenario. Permissioned cases are often used in a secure database with entry controls. It has restrictions on the users and voters, but this is irrelevant to this voting scheme per se.

4. Conclusion

We have reviewed several prevailing voting schemes and made a comparison among the schemes. There are pros and cons to each scheme we introduced. The schemes are mainly developed and implemented by DAO service platforms (Zhao et.al., 2022) such as Aragon, Moloch, DAOstack, and SubDAO[10].

The development of DAO is not only targeting a static organizational future. It should keep improving the organization constantly by absorbing good designs. Our hypothetical scheme has a better design incorporating key features from other schemes. However, it is not flawless and might face challenges in implementation. Nevertheless, we aim to inspire innovative design thinking. Because all the voting schemes are applied in DAO, they have also been widely used in social governance like elections or corporate governance. The research on the voting mechanism could be important for the decision-making of public issues, and any improvement or progress could have profound inspiration for realistic governance.

[10] SubDAO is a web3 protocol that helps manage digital assets through multi-sig and DAO.

Reference

Benaloh J. Verifiable secret-ballot elections, Ph.D. thesis, Yale University; 1987.

Boyd C. A new multiple key cipher and an improved voting scheme. In: Advances in cryptology – EUROCRYPT '89. Springer-Verlag; 1990. p. 617–25.

Cramer Ronald, Gennaro Rosario, Schoenmakers Berry. A secure and optimally efficient multi-authority election scheme. In: Advances in cryptology – EUROCRYPT '97. LNCS, vol. 1233. Springer-Verlag; 1997. p. 103–18.

DiRose, S., and M. Mansouri, 2018, Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations, 13th Annual Conference on System of Systems Engineering (SoSE), 2018, pp. 195-202, doi: 10.1109/SYSOSE.2018.8428782.

El Faqir, Y., Arroyo, J., & Hassan, S. An overview of decentralized autonomous organizations on the blockchain. Proceedings of the 16th International Symposium on Open Collaboration. 2020. doi:10.1145/3412569.3412579

Fujioka, A. Okamoto, T. Ohta, K. A practical secret voting scheme for large-scale elections. Advances in Cryptology, AUSCRYPT'92, Lecture Notes in Computer Science 718 (1993) 244– 251.

Hassan, S., De Filippi, P., Decentralized Autonomous Organization, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 2, pp. 1-10, 2021.https://doi.org/10.14763/2021.2.1556

López García, D. A., 2016, A flexible e-Voting scheme for debating tools, Computers & Security, Vol. 56, pages 50-62.

Jakobsson M, Juels A, Rivest R. Making mix nets robust for electronic voting by randomized partial checking. In: Proceedings of USENIX security '02 2002. p. 339–53.

Kaal, W.A., Blockchain-based corporate Governance. Stanford Journal of Blockchain Law & Policy(Online). 2021.

Morrison, R., Mazey, N.C.H.L. , Wingreen S.C., The DAO controversy: the case for a new Species of corporate Governance? Front.Blockchain, 3(25). 1-13. 2020. DOI: 10.3389/fbloc.2020.00025

Neff C A . Practical high certainty intent verification for encrypted votes 2004.

Noizat, Pierre. "Blockchain electronic vote." Handbook of digital currency. Academic Press, 2015. 453-461.

Petersen, H., P. Horster, and M. Michels. "Blind multisignature schemes and their relevance to electronic voting." 11th Annual Computer Security Applications Conference, IEEE Press. 1995.

Quarfoot, David, Douglas von Kohorn, Kevin Slavin, Rory Sutherland, David Goldstein, and Ellen Konar. "Quadratic Voting in the Wild: Real People, Real Votes." Public Choice 172 (1-2): 283–303. 2017.

Ribeiro C., Joaquim, R. An Efficient and Highly Sound Voter Verification Technique and Its Implementation. E-Voting and Identity, 3º Int. Conf. VoteID. 2012 Springer-Verlag. pp. 104–121.

Sako, K. & Kilian, J. Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth. In EUROCRYPT 1995, pages 393–403.

Sampigethaya, K. Poovendran, R. A framework and taxonomy for comparison of electronic voting schemes. Computers & Security 25 (2006) 137–153

Wu, Z. Y., Wu, J. C., Lin, S. C., & Wang, C. An electronic voting mechanism for fighting bribery and coercion. Journal of Network and Computer Applications 2014, 40, 139-150.

Yermack, D., Corporate Governance and Blockchains. Review of Finance, 21(1), 7–31. 2017. DOI: 10.1093/rof/rfw074

Youssef Faqir-Rhazoui, Javier Arroyo, and Samer Hassan. A scalable voting system: Validation of holographic consensus in Daostack. 2021, pp. 5557–5566. doi: 10.24251/hicss.2021.676

Zhao, X., Ai, P., Lai, F., Luo, X. (R.), & Benitez, J. Task management in decentralized autonomous organization. Journal of Operations Management, 68(6-7), 649– 674. 2022. https://doi.org/10.1002/joom.1179

Zhuang Q., Liu, Y., Chen, L., and Ai, Z., Proof of Reputation: A Reputation-based Consensus Protocol for Blockchain Based Systems. In Proceedings of the 1st International Electronics Communication Conference (IECC '19). Association for Computing Machinery, New York, NY, USA, 131–138. 2019. https://doi.org/10.1145/3343147.3343169