Autonomous competence identification protocol

Tim Pechersky

June 27, 2024

Abstract

This paper proposes a novel protocol for designing ranking systems applicable to consensus-building protocols and decentralized autonomous organizations (DAOs). Leveraging recent cryptographic advancements and social science insights, the protocol facilitates autonomous decision-making in trustless environments based on agent interactions, addressing key challenges in autonomous organizations. We examine an existing precedent, originating as an easy-to-understand tabletop game, which demonstrates promising participation rates even among non-technical users. Our proposed implementations focus on defining interoperable and liquid voting weights for participants, facilitated in both computational and non-computational (social) networks. Additionally, we briefly review economic models for the practical utilization of such competence frameworks and game theoretic moments.

1 Introduction

The quest for consensus, a cornerstone of collective decision-making, has deep historical roots. From the ancient Chinese concept of *zhongyong* 中庸, advocating for moderation and balance in governance, to the Roman Republic's emphasis on *senatus consulta* (senate decrees) reached through deliberation and compromise, societies have long grappled with the challenge of aligning diverse perspectives towards a common goal. The study of these historical precedents continues to inform modern approaches to consensus [1] [2].

The pursuit of consensus, has gained renewed significance in the digital age. Originating from the Bitcoin whitepaper [3], blockchain technology fundamentally seeks consensus and establishes trustless systems through cryptographic signatures. While significant progress has been made in developing efficient Byzantine Fault Tolerance (BFT) algorithms for reaching consensus on verifiable data [4], the challenge of achieving consensus on subjective or non-deterministic matters within DAOs [5] remains a complex issue [6][7]. This has led some researchers to question the ability of autonomous organizations to overcome the hierarchical issues present in today's society [8] [9].

This paper addresses the gap between formally verifiable, automated consensus and subjective human decision-making. We propose a protocol that can achieve consensus even for subjective matters by qualifying participants based on their ability to represent a group's interests and intents. This protocol aims to provide a foundational building block for designing ranking systems applicable to both computational and social networks, and capable to address some of long standing governance issues such as agenda manipulation [10] problem.

Main objectives thus are to propose a methodology for creating a ranking system in a trustless environment, review attack vectors and resistance mechanisms, provide a case study of existing use-case and discuss potential economic models for the practical utilization of such competence frameworks. We begin by reviewing existing consensus mechanisms and their limitations, focusing on DAOs and their governance mechanisms. We then introduce our proposed protocol, followed by a discussion of its implementation and potential economic models. Finally, we present a case study of an existing use case and conclude with a discussion of future research directions.

2 Background

Decentralized Autonomous governance nor consensus protocols can be defined trough cyber-physical systems [11] methodology completely, nevertheless ultimately is an end goal for any autonomous governance is to operate CPS. In this context any kind of IT governance system can be seen trough methodology of

Cyber-Physical-Social-System (CPSS) [12].

Studies of management perspectives in cyber age introduce parallel management [13] ideas, management frameworks proposed to model DAOs as CPSS openly discuss need for multidimensional indexes and foundational models [14]. In order to support such grand design ambition, the DAO organizations must be able to show other metrics of their governance to provide the best possible performance. Additionally, as discussion for parallel management [13], there is a need for a robust mechanism for reinforcing the informational and intellectual capabilities of organizations, enabling them effectively benchmark performance of AI enabled agents against human in various tasks and aspects of governance and management.

In order to support quantities analysis of decentralization metric, Nakamoto Coefficient[15] was proposed, defined as *how many entities one would need to to be compromised to control entire system* it can be used as decentralization criteria.

Besides these new concepts, the traditional governance models long standing problems, such as agenda manipulation [10] that should be addressed well to ensure high reliability of organizations in autonomous systems.

2.1 Consensus Layer

Blockchain is a distributed and decentralized network that follows some particular consensus protocol in order to maintain continuous sequence, chain of blocks[16], where each new block consists of a digital records to a united ledger book. First introduced at launch of Bitcoin[3], since then grown to an industry where multiple approaches and protocols were developed and initial ability to write a records in to ledger book was elaborated to ability to write code in ledger records such that can change states of book itself. The blockchain governance plays a critical role in any blockchain protocol and can be summarized as consisting of Validators, Users, Governance Mechanisms and core developer community; In this context blockchain network is analogous to an organization, consisting validators (employees), protocols and governance structure whose activity result in services provided to users that also have to say their word by paying for using the protocol.

The contrast between traditional organization and blockchain governance is CSP friendly automation. Such are designed to follow some determined rules of maintaining distributed ledger with no need for human stakeholder decision for a regular operations which are automated by running specific software applications (nodes) that act on behalf of stakeholder. These however work only well up to the point when the protocol changes are desired or some vulnerability happens which leads to stakeholder collective decision for stepping-off the protocol rules [17] for at least one block. Such occasions generally are called hard-forks and have specifics that coordinated consensus between node operators changes their protocol rules to move away from existing logic. The "fork" in context describes split of consensus in two possible ledger book states which are not compatible.
Consensus layer protocols also have the underlying node operator community which incentive driven and studies on Nash Equilibrium [18] are done while the real situation for Ethereum is that Miner Extracted Value is shown [19] as realistic thread to protocol level security that comes down to affecting applications such as decentralized exchanges. Same paper also observes that agents pursuing MEV can achieve cooperative equilibrium in terms of priority gas auctions.
"Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization research" [20] has shown that practical Nakamoto coefficient numbers in automated consensus engines such as PoS and Pow (Proof of Stake and Work accordingly) have stabilized on a very low numbers of less then 5 entities standing behind whole pool of validators and miners, and seem not to show any positive dynamics.

2.2 Application Layer

While research in CPSS field point out demand for DAOs as solution [12][13][14], the ability of DAOs to perform well and be competitive, however, is under question, as many research point out associated problems [7][8][9].
An empirical Study of On-Chain Governance conducted by Rainer Feichtinger et. al. [7] shows low Nakamoto coefficient numbers, however comparing it with Consensus Layer research [20] we can conclude there is a positive dynamic in the Nakamoto coefficient over time in DAOs, compared with absence of such for the consensus layer. Same research[7] also shown that analyzed DAOs Gini coefficients[21] are high, reaching 0.888-1 for direct holders and 0.667-0.980 range when counting delegates, also shown participation rate in DAOs are low. Out of four analyzed DAOs (Compound, Uniswap, ENS and Gitcoin), none of them are showing positive dynamics in

participation rate over time, and mean numbers for participation even amongst delegates are in range of 1.1-9.9% of total delegated accounts.

Another highlighted problem can be seen in the voting participation rates, which are low. For example, Compound DAO quorum requires only 400,000 [22] votes out of 10,00,000 total token supply [23], which is only 4%, yet in practice some of proposals fail to reach even this low threshold from the first time and have to re-submit [24][25]. To illustrate problem further some quorum requirements are illustrated in Table 1. Such low quorum requirements are directly explainable by a low participation rates, and already have a record of quorum attacks [26][27] precedents, that were exploiting this weakness, while contrary in high participation rate consensus layer systems, such as PoS and PoW, the financial incentives towards participation shown not just to negatively impact Nakamoto coefficients, but also have shown that any network node must be seen as rational-agent which may diverge from collective interest [19].

Table 1: DAO Minimal Quorums

Name of DAO	**Total Supply**	**Quorum**	**Threshold (%)**
Compound	10e6	400e3	4%
Uniswap	1e9	40e6	4%
ENS	100e6	1e6	1%
Arbitrum	10e9	300e6-500e6	3-5%
Lido	1e9	50e6	5%

as can be seen from 3

2.3 Comparing two above

DAOs ultimately are just an abstraction layer on top of Consensus, allowing blockchain users to abstract away from calculations intensity onto smart contract programming and therefore more versatile, dynamic governance systems that can rely on underlying consensus security guarantees. Difference however also lies in implementation specifics: while Consensus layers do provide participation incentives, the application layer organization might not propose such at all, instead providing a means to make a governance decisions that are profitable on their own.
Analyzing Nakamoto coefficient we can see a notable difference between Nakamoto coefficient in DAOs vs Consensus layer. One possible explanation for this phenomenon can be coined as "curse of money making money". It suggests that in order to ensure growth of Nakamoto coefficient, the ability to influence the system should grow at a rate that must be sub-linear in relation to entities efforts (investments), ensuring that no disproportionate compounding of power occurs. In other words, the growth of influence should not match or exceed a linear rate to prevent centralization, highlighting the necessity for mechanisms that enforce a diminishing increase in influence relative to investment or contribution (Fig. 1).

One another notable difference is in the security model. While relying on consensus engine enables security guarantees, the opposite side of that medal is that such application layer governance mechanisms have no similar alternative as consensus layer operators do with hard-fork ability. Even if community members agree on such decision in case exploit happens, there is no easy way to "split away" saving full state. The only known occasion of such successful split was The DAO Hack Hard-fork which was done very controversially at the protocol level. [17]. This is a substantial difference with consensus layers, where any participation requires a commitment that either requires to do work prior to a particular vote (PoW), or have assets at stake (PoS, Optimistic Rollups) that can be lost during due to any activity by operator against the protocol rules.
Lack of such ongoing commitment mechanisms in the application layer, brings in substantial security risks as governance attacks become less risky for the adversary [26][27]. Such risks led to solutions such as time-locks [28], and rage quit [29] methods giving individual stakeholders a last-resort options to leave the protocol (arguably) safely at the expense of delayed actions taken by the organizations.

While these solutions are effective in preventing funds loss, the reduce in reaction time by organization is not always acceptable. Need for prompt decision making is leads to empowering security players to run a privileged multi-signature wallets to run emergency stop or veto power over DAO protocols [30]. Fact of presence of such, centralizing actors makes

DAO frameworks to behave in non-autonomous way. The more general question is left open - how to appoint such privileged actions takers in an autonomous ways, ideally defining the privileges as a function of certainty in the actor?

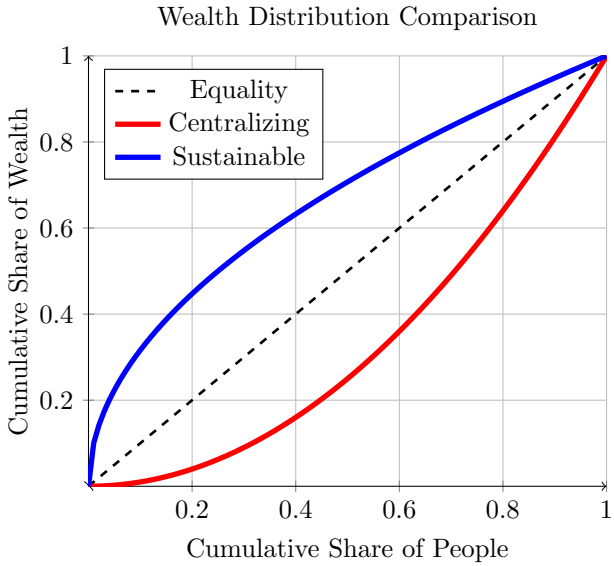

Figure 1: First Plot

Figure 1: Agent of Influence vs Efforts

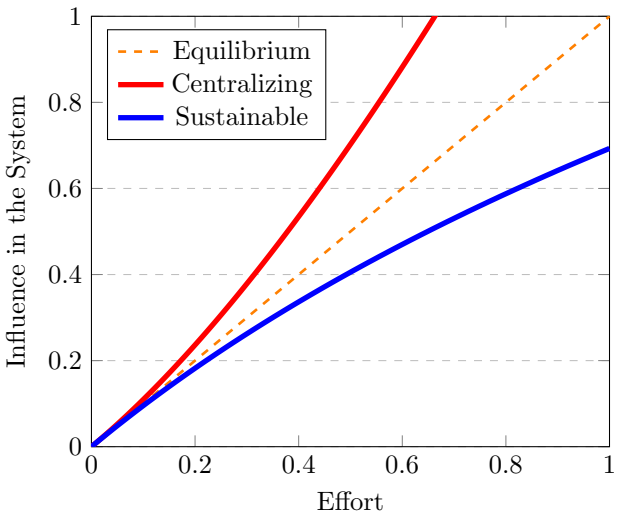

Figure 2: Second Plot

2.4 Recent cryptographic advancements

Recent cryptographic advancements have enabled the development of new governance and consensus mechanisms that may be used to address the challenges faced by DAOs. For example, the use of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) allows for the creation of verifiable and private voting systems that can be used to ensure the integrity of voting processes within DAOs [31], while MPC threshold-signature protocols can be used to create secure multi-party data signing process [32] and fully homomorphic encryption promises us soon ability to run fully private calculation directly on-chain [33].
Summing this section up, we can say that whatever new protocol is designed for governance, it is realistic to set requirements of privacy in voting and proposing process.

2.5 Proposed Protocol origins

Foundation for this research originates from existing precedent of a game that is played by small Lithuanian group of friends in chat messenger since 2017. This original game never had ambition to become a protocol or a system, but it was a fun way to spend time and exchange music ideas between friends-musicians who were all living in different countries and used it as mean to stay engaged. The game typically consists of 5 to 10 people, and series of rounds. Each round a player is assigned a role of a "game master". Participants send game master music compositions they like and game master compiles them into a playlist. The playlist is then shared with all participants, who vote on their favorite composition by sending their vote to the game master again. At the end of a turn, the game master reveals the proposer identities, as well as scores proposal based on votes. The game continues to the next round until total of hundred compositions are added to the playlist. Each round scores are aggregated per participant, yielding a final ranking.
Notably, the game has high agenda manipulation resistance, as every participant is required to make a proposal, in order to vote, which is contrary to traditional voting systems, where small group of proposers can pose a threat [10]. Also this game mechanics effectively coupes negative effects of proposals such as known as Hallo effect [34].
It also demonstrates some of the key features that are desirable in a governance protocol, such as high participation rates, user retention, while the only limit is that participants generally may be interested to par-

ticipate only in the specific field (music) or with a specific group of people.

It appears that participants in order to conduct a round must *i* submit a proposal, *ii* get proposals batch, *iii* submit a vote, resulting communication complexity $O(3n)$ per round

2.6 Summing up the context

From the issues identified in the background sections we can sum up that there are multiple problems that are faced both on network protocol level governance as well as on application layer built DAOs as well: Low participation rates, low Nakamoto coefficients, lack of application layer commitments, and lack of multidimensionality. We can also note that incentive based protocols cause centralization, yet decentralized organizations are not able to provide a commitment mechanism for participants, nor do they have truly autonomous way to appoint stakeholders purely from the mission it has, nor identify competent actors in the system to take prompt, time-critical actions.
We have discussed two different kinds of systems so far - based on consensus layer continuous proving and application layer share-holder voting and identified different problems of both of these kinds. We also outlined that already existing DAO precedent can show positive dynamics in Nakamoto coefficient when influence is sub-linear to efforts, compared to Consensus Layer systems that incentivize participants. We also outlined precedent of a game that has high participation rates and user retention (further elaborated in case study section).

3 Protocol Description

In order to enable deductive reasoning, we can outline specifications that a generic abstract organization must fulfill. Besides these, we preferably want to system to be compatible with existing solutions and technologies that allow data integrity, privacy and security, assuming that distributed ledger and multiparty computation signing may be combined to cover these problems.
We are seeking for protocol that is:
Mission aligned: Organization members should actively participate in the decision-making process by the design of the protocol, their activity shall be directly impacting the organization goals and mission.
Highly performant: Ideally, every organization design shall automatically align participants in collaborative model, enabling everyone to do their best contribution towards shared direction. , with utilizing full potential of competitive performance provided by decentralized autonomous methodology.
Centralization resilient: Protocol should be designed in a way that over time dependency on single actors shall be reduced, Nakamoto coefficient shall increase, promoting collaboration over competition for those aligned in automatic manner.
Multidimensionality: Protocol should enable multidimensional indexes and foundational models to be built on top of it, as well as promote working groups that can be more operative than a main governing body. At the global scale this should support automatically combining multiple DAOs in superset and enable establishing data, asset and control specific flows-controls.
Rational agent friendly: Protocol should be designed in a way that any network node must be seen as rational-agent which may diverge from collective interest or collude with others and still not able to reach influence over the system beyond what protocol accounts for.

3.1 Market value of competence

In order to support solving all of the objectives, we propose to specify, that outcome of protocol is a transferrable asset, that represents competence of the participant in a particular *subject*.
The *subject* in it's turn is to be described with the properties, such as text description, or unique resource identifiers assigned to it, which further may be used to point to a multidimensional representation of the subject by a third party tools, such as large-language-model that has a dimensionality concept within analyzed text already.
Transferability is an important aspect as this allows to accomplish multiple goals, starting with agent rational actions: even concepts of corruption and collusion can be seen as game-theoretic [35], are not necessarily bad [36], and can be seen trough definition of an intrinsic value of any transferable asset. Other words saying, we see personal competences in CPSS frameworks useful as a market value, that may be useful to trade. While this can me argued as a controversial statement, we can discuss that in the real world competence indeed is often traded in form of a investing time and money in education, relationships, that eventually form a social ranking. Since we declare as a requirement to have a compounding resistance, it forms a solid basis for building economic models

that penalize competence-market participants heavy enough, and the competence is not traded in a way that it can be easily bought by a single entity.
Transferability of value can be used by other protocols to define staking commitments, similarly as PoS consensus mechanisms do, eventually forming a rational economic model that would incentivize any participant to maintain his reputation.
The multidimensionality, supported by any semantics of subjects also benefit from free market economy, as it is expected to help arbitraging between different successful and largely adopted subjects that share same dimensionality. Nevertheless, for many software defined use cases of ownership within Account Abstraction[37] model, the assets could be made non-transferable, and still be used as a proof of competence of a specific account.
Providing a influence to compounding becomes a critical aspect part for such protocol, since we are relying to a free-market values and principally do not require any specific identity solution as a dependency to this protocol. Our foundational model for this resistance lies in extending 2.5 idea, to introduce *ranking ladder* (Fig. 3) that lets game winner to participate in next game with higher level of rewards only if it holds an asset of rank below. Each time participant produces a next level, his previous rank asset balance, that was used gets *exchanged*. This expected to create non-linear friction towards any sybil attack, allowing competent actors who are willing spend their time to participate in the game to be rewarded with advantage over any colluding company that is trying to game the system.

If every game does require to have some kind of commitment, such as participation fee, than is possible to prove that such ranking ladder would create non-linear friction for anyone trying to game the system.
Considering such fee, it directly follows that competence obtained by such game participation cannot be used to influence decisions whose total value is comparable with costs of obtaining competences. Assume situation that organizations total value locked is equal to TVL, it's obvious that if such organization is governed by a token, the total case of governance quorum attack shall be more expensive than TVL. In case if there is any additional token used as weight multiplier, than obtaining such weight multiplier should be at least as much as expensive as to do direct quorum attack.
Hence price relationship requirement between governing token and produced competence token can be defined. In case of linear proportional multiplier, that is

$$V_w = C * P$$

where Vw is vote weight, C is competence level and P is governance power, we can conclude that required price between competence level and governance power token can be defined by function

$$\$C_i \geq P * i$$

Where i is level of competence. Hence C_i qualification must by design cost something in governance power equivalent for each participant. In other words, there must be a *game price* defined that acts as resistance to gaining competence level from one side, while on the other side, our goal is to create high participation rates which imply a need for a low effort requirement. Solution for this is imposing minimum game size.

Assume we have N_{min} peers required to join the game, each of those must pay X_g price in order to join. Then for an attacker who tries to conduct a sybil attack it would cost

$$\$C(i) = X_g * N^i_{min}$$

At the same time, for the agent who is relying on his pure competence and wins each game, same cost would be only

$$\$C(i) = X_g * i$$

If adversary would try to optimize this around quorum attack internally in the voting, then his efforts could be minimized to

$$\$C(i) = X_g * N^i_q$$

where

$$N_q = \lfloor N_{min}/2 \rfloor + 1$$

From this it follows that for such system to be secure, the voting process should happen in larger groups as it will make it more difficult for malicious user to gain high ranking. On the other hand we want to keep games small enough to ensure that agents have sufficient ability to perform as small units. // This seems to be reasonable constraint, as it seems intuitive and inline with existing governance practice, that for lower TVL decisions can be done by small pods, while high TVL competences would require higher volume of engagement.
If attacker would try to reduce his cost even further, he could to reinforce his vote by having some limited number of sybil accounts voting for him, yet keeping that number below N_q and relying on a stochastic nature present in any voting process. For such case use of quadratic voting is proposed; If during individual round the scores are calculated using

$$S_{given} = \sqrt{V_{credits\_given}}$$

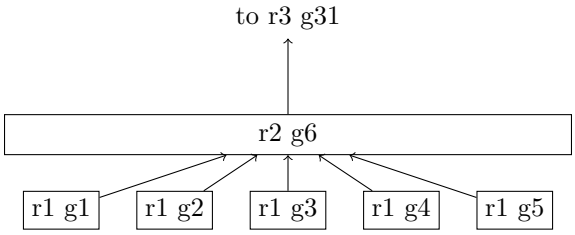

Figure 3: Diagram illustrating the rank ladder. With minimum participant requirements of 5, 30 games are required to create a rank 3 game. Strong candidate would need only 2 wins to reach it.

where S denotes score and V - vote, then the voting towards different candidates is incentivized. This still has to be observed in practice, the assumption however is that the higher level of peers are in game the harder to conduct such random dice game, as well as with higher rankings every participant will be skilled on his own ability to win and conduct decision making which is less likely to vote for non-competitive proposals.

Nevertheless, it is assumed that players also *must agree* on playing with each-other, while at any time it is guaranteed that only a handful of top-ranking players is possible even in theory - as the rank creation destroys the lower rank asset, leaders would have to wait until there is enough of high-ranking participants willing to compete with them. This requirement leaves us to the last, but not least requirement: High Participation rates. We argue that multidimensionality and free-market values will provide a way to ensure high participation rates, as participants will be able to participate in the decision-making process in a category that they are interested in, and that they are competent in, and lastly - are rewarded for being in. With a ranking ladder, and a multidimensional representation, this can be seen as a global framework for building education and helping young talents to discover their path by observing very well quantized data on their progress.
We may also suggest that this protocol functionally may be presented as simply a new way of talking, where each input - seen as valuable idea, and each vote - seen as a valuable feedback, and each game final, as actionable result.
In order to support such high participation rates, the user experience must be ensured as simple as possible, and the application must be designed in a way that it is easy to use and understand. In order for that, we require to have extensive metadata available for user experience purpose by the protocol as key requirement. For example, when participant sends in encrypted vote, or proposal - protocol shall be able to publicly announce that particular participant has submitted a vote, while not revealing the content of the vote nor the linkage to it after content is revealed for voting.

4 Implementation

Protocol particular implementation may vary depending on environment and requirements, however we can outline a generic implementation that can be used as a reference for further development.
The protocol can be implemented as a smart contract on a blockchain network, such as Ethereum, that allows participants to submit proposals, vote on proposals, and receive rewards based on their participation. Subject representing subject asset can be represented as semi-fungible asset, like ERC1155[38] standard interface on Ethereum, where each token id represents a rank level, and games that award such rank require a token of one below to be held in order to participate. Such token shall be created only as a result of competence identifying smart contract activity result. The competence identifying contract is a turn-based game where group must collect together and has a signer-key (game master), who is able to sign for a private inputs and keep personalities of participants hidden by either using MPC or zk-SNARKs protocol. The game master is responsible for collecting proposals and announcing fact of activity without disclosing the actor, then posting them as batch to a contract, collecting votes in a similar manner, without tell nor who, nor for whom votes, and finally revealing the results.

5 Case Study

Some rough statistical data could be gathered by analyzing groups activity and historical records, which

show that since 2017 total 17 games were played up to end of 2023. Each averaged for 13 turns, 8 participants and 3 month duration. Total amount of proposals and votes reaching 1700, as game is stopped at 100 songs playlist length. Total 34 participants joined it over course of years, out from which 22 players completed at least one full tournament and 15 completed at least two full tournaments. From original 6 players 3 still were playing at the moment of writing, with active user count 8 at latest game, showing steady with high user retention. Total amount of players not submitting a vote shown to be negligibly small, below 5% of all votes.
Even despite absence of any incentives beyond that participants are genuinely interested in the subject, and burden of having to be a game master occasionally which requires participants to do some effort, we can see exceptionally high user participation rates with average:

- participation rate of 95% for active users
- User retention for three month period of 65%
- User retention for two tournaments and roughly six month of 44%
- User retention after 72 month of 9%
- Average of 8 proposals and votes per participant per annum

The low absolute numbers however are explainable by user complex manual score calculation process and closed community by itself which never oriented itself towards big growth and hence let to do assertion that could be even higher on a well designed automated protocol.

We also observed that collected playlists, ordered by high-score compositions, are of high quality and form a good representation of participants' preferences, while the winner of the tournament is often a participant that is able not simply propose a popular song, but to propose a song that is liked by many participants, including such aspects that participants will likely vote songs they hear for the first time (original ideas).

6 Conclusion

2 we are generalizing the proof based consensus mechanisms for social network interaction by viewing any network node as rational-agent which may diverge from collective interest [19] individually or collude with others. We propose BFT tolerance methodology that allows reaching effective consensus based on participant inputs, opinions and we can say that protocols reach an agreement in a trustless environment by qualifying the competence of the participants. Bitcoin miners are required to solve a cryptographic puzzle to prove their competence, or ethereum Proof of Stake consensus mechanism qualifies participants by their ability by ability to adhere to distributed ledger rules a nd stake their assets.
Similarly DAO participants are qualified by their ability to hold a token and participate in the voting process. Tokens held can be seen as analogy to stake in PoS consensus mechanism, incentivising participants to act in the best interest of the organization. The gap however exists between such automated protocols and DAO governance as organizations agenda may be much more arguable then a "simple" cryptographic puzzle, which despite any computational complexity it might have, most of the time can be formally verified to be correct. This becomes more emergent as the DAOs are becoming more complex and must take effective and prompt decisions in a trustless environment, which often leads to burden of complexity on users, while often a decision making process involves a fairly traditional board-level discussions within governance forum boards, which yields for doubts as researchers find blockchain-based governance systems likely not to solve problems of social.

The contrast between traditional organization and blockchain is that latter are set to follow some determined protocol of following consensus layer decisions in an autonomous way, therefore enabling CPS, there is no need for human stakeholder decision for a regular operations which are automated by running specific software applications (nodes) that maintain protocol on behalf of stakeholder. These however work only well up to the point when the protocol changes are desired or some vulnerability happens which leads to need for stepping-off the protocol rules for at least one block. Such occasions generally are called hard-forks and have specifics that coordinated consensus between node operators changes their protocol rules to move away from existing logic. The "fork" in context describes split of consensus in two possible ledger book states which are not compatible.

References

[1] X. Li, T. J. Andersen, and C. A. Hallin, "A zhong-yong perspective on balancing the top-down and bottom-up processes in strategy-making.," *Cross Cultural and Strategic Management*, vol. 26(3), 2019.

[2] F. Vervaet, *The High Command in the Roman Republic: The Principle of the Summum Imperium Auspiciumque from 509 to 19 BCE.* Historia, 2014.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] G. ZHANG and et. al, "Reaching consensus in the byzantine empire: A comprehensive review of bft consensus algorithms," *arXiv*, vol. 03181v3, no. 2204, 2023.

[5] S. Hassan and P. De Filippi, "Decentralized autonomous organization," *Internet policy review*, vol. 10, no. 2, 20 April 2021.

[6] S. Wang and et. al, "Decentralized autonomous organizations: Concept, model, and applications," *IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS*, vol. 6, no. 5, 2019.

[7] R. Feichtinger, R. Fritsch, Y. Vonlanthen, and R. Wattenhofer, "The hidden shortcomings of (d)aos – an empirical study of on-chain governance," *arXiv*, vol. 12125v2, no. 2302, Feb 2023.

[8] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?," *Available at SSRN: https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713*, 2016.

[9] X. Liu, "The illusion of democracy— why voting in decentralized autonomous organizations is doomed to fail," *NYU Law and Economics Research Paper*, vol. 13, no. 24, 2024.

[10] R. D. McKelvey, "Intransitivities in multidimensional voting models and some implications for agenda control," *Journal of Economic Theory*, vol. 12, no. 3, 1976.

[11] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pp. 363–369, 2008.

[12] F.-Y. Wang, M. Xiao Wang, L. Li, and L. Li, "Steps toward parallel intelligence," *IEEE/CAA JOURNAL OF AUTOMATICA SINICA*, vol. 3, no. 4, 2016.

[13] W. Fei-Yue, "Parallel management: The dao to smart ecological technology for complexity management intelligence," *ACTA AUTOMATICA SINICA*, vol. 48, no. 11, 2022.

[14] J. Li, R. Qin, and F.-Y. Wang, "The future of management: Dao to smart organizations and intelligent operations," *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS*, vol. 53, no. 6, 2023.

[15] B. S. S. et al., "Quantifying decentralization." https://news.earn.com/quantifying-decentalization-e39db233c28e, 2017 [Accessed Jun. 2024].

[16] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.

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

[18] N. Khan, T. Ahmad, A. Patel, and R. State, "Blockchain governance: An overview and prediction of optimal strategies using nash equilibrium," *arXiv:2003.09241 [cs.GT]*, 2020.

[19] P. Daian, S. Goldfeder, T. Kell, Y. Li, and X. Zhao, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," *arXiv*, vol. 05234v1, no. 1904, 2019.

[20] D. Grandjean, L. Heimbach, and R. Wattenhofer, "Ethereum proof-of-stake consensus layer: Participation and decentralization," *arXiv*, vol. 10777 [cs.DC], no. 2306, 2023 [Accessed Jun. 2024].

[21] L. Ceriani and P. Verme, "The origins of the gini index: extracts from variabilita e mutabilita (1912) by corrado gini," *The Journal of Economic Inequality*, vol. 3, no. 10, 2012.

[22] "Compound dao contract." Ethereum Network: 0xc0Da02939E1441F497fd74F78cE7Decb17B66529.

[23] "Compound token." Ethereum Network: 0xc00e94Cb662C3520282E6f5717214004A7f26888.

[24] Tally, "Compound dao proposal 232 voting page." https://www.tally.xyz/gov/compound/proposal/232, 2024.

[25] Tally, "Compound dao proposal 237 voting page." https://www.tally.xyz/gov/compound/proposal/237, 2024.

[26] A. Association, "Aragon association takes action to safeguard the mission of the aragon project and its community of builders." Web archive: https://web.archive.org/web/20240228120235/https://blog.aragon.org/aragon-repurposes-dao-to-ensure-treasury-serves-its-mission/, 2023.

[27] rhizoo.eth, "The rook dao story: Postmortem of the $25m governance takeover." https://www.bitget.com/news/detail/12560603820648, 2023.

[28] J. CURATOLO, "Protect your users with smart contract timelocks," *OpenZeppelin Blog: https://blog.openzeppelin.com/protect-your-users-with-smart-contract-timelocks*, 2021.

[29] A. Soleimani, A. Bhuptani, L. H. James Young, and R. Sethuram, "The moloch dao: Beating the tragedy of the commons using decentralized autonomous organizations," *https://raw.githubusercontent.com/MolochVentures/Whitepaper/master/Whitepaper.pdf*, 2019.

[30] J. Scharfman, "Decentralized autonomous organization (dao) fraud, hacks, and controversies," *The Cryptocurrency and Digital Asset Fraud Casebook*, vol. 2, 2024.

[31] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Scalable zero knowledge via cycles of elliptic curves." Cryptology ePrint Archive, Paper 2014/595, 2014. `https://eprint.iacr.org/2014/595`.

[32] J. Doerner, Y. Kondi, E. Lee, and abhi shelat, "Threshold ecdsa in three rounds," *IEEE S&P*, 2023.

[33] G. Zyskind, Y. Erez, T. Langer, I. Grossman, and L. Bondarevsky, "Fhe-rollups: Scaling confidential smart contracts on ethereum and beyond," 2023.

[34] B. Verhulst, M. Lodge, and H. Lavine, "The attractiveness halo: Why some candidates are perceived more favorably than others.." https://doi.org/10.1007/s10919-009-0084-z, 2010.

[35] J. Macrae, "Underdevelopment and the economics of corruption: A game theory approach," *World Development*, vol. 10, no. 8, 1982.

[36] N. H. Leff, "Economic development through bureaucratic corruption," *American Behavioral Scientist*, vol. 3, no. 8, 1964.

[37] Q. Wang and S. Chen, "Account abstraction, analysed," *arXiv [cs.CR]*, no. 2309.00448, 2023.

[38] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet, and R. Sandford, "Erc-1155: Multi token standard." `https://eips.ethereum.org/EIPS/eip-1155`, 2018. Accessed: 2023-10-04.