Generic DAO primitives for Full Academic Decentralization and Scalability

Brian Planje
b.o.s.planje@student.tudelft.nl
Delft University of Technology
Delft, The Netherlands

***Abstract*—This thesis describes a new architecture for a completely decentralized and scalable decentralized autonomous organization based on multi-signature and thresh-hold signature schemes. To demonstrate the feasibility, we design, implement, evaluate, and deploy a DAO centered around music where artists can share their music in a decentralised manner and listeners can invest in artists using the DAO.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

Decentralized autonomous organizations (DAOs) are a mechanism for economic activity by an unbounded group of people within an adversarial environment. Numerous organizations have been deployed succesfully, demonstrating the potential for this mechanism to enable able a trustless and transparent ecosystem. For instance the decentralized exchange Uniswap, which is governed by a DAO, reached transaction volumes of up to $85.5 billion in November 2021 [5] and is controlled by a DAO. The token associated with the DAO is utilized for the collective management of its funds and modification of the exchange's protocols. Prior to the emergence of DAOs, partially decentralized protocols and platforms such as BitTorrent and Wikipedia enabled millions of individuals to collaborate in file sharing and information accumulation. The increasing emergence and popularity of decentralized protocols highlight their potential for fostering collaboration between individuals.

Despite wide deployment of DAOs, many of them exhibit forms of centralization in their governance structure and infrastructure. This centralization is reflected in the lack of true decentralized governance. For instance, the second-largest DAO by market capitalization, APE DAO, is characterized by an initial token distribution in which 38% of tokens were distributed to various founders, who now hold a disproportionate amount of voting power. Additionally, proposals in are vetted by a centralized moderation team, and all execution of proposals is carried out by the foundation members of the DAO. Another example is Solend, one of the largest decentralized lending systems. In 2022, there was an indicident where the development team took control of and liquidated the account of a whale with approximately $170 million worth of cryptocurrency. The team claimed it allegedly posed a systemic risk to the ecosystem at the time. This incident highlights the prevalence of centralized decision-making in many DAOs.

The root cause of the failure of contemporary DAOs to decentralise lies in the underlying blockchain. Proof-of-work and proof-of-stake have failed to scale, despite a full decade of attempts to boost transaction rates, without the loss of decentralisation. Attempts to circumvent this by working with fewer miners which process more transactions have resulted in systems akin to those of traditional authorities, such as VISA. Centralization might even be inevitable, with Cong et al. showing that in the long run, due to centralized mining pools, Bitcoin will have a centralized market structure [10]. Proof-of-stake distributed ledgers run the risk of reinstating a centralized elite. To validate the network, a substantial amount of capital must be placed at risk. This set of validators can then be subjected to regulatory pressure or collide with one another to alter transaction validation rules at the infrastructure layer. They run the risk of moving to a new centrality with a new elite, who can afford to buy enough tokens to put up to stake to validate the network.

In this paper, we propose a new architecture for DAOs which is completely decentralized and scalable. To demonstrate the feasibility of this architecture, we design, implement, and evaluate a prototype for a DAO centered around music, referred to as the Music DAO. This implementation solely utilizes smartphones and is currently live. We conduct a real-world test with users and analyze the performance of our voting mechanism. The results show that our proposed architecture is a viable and sustainable solution. We argue that pure academic decentralisation within a viable and sustainable DAO represents a key milestone in the evolution of Web3. We believe an as-simple-as-possible DAO with basic governance, membership voting, and treasury management is a key step forward in achieving this goal.

1) **A Simple DAO Architecture** We design and justify an infrastructure for DAOs which is completely decentralized and scalable. To achieve this, we propose a set of technologies and primitives that must be followed. In particular, we separate the settlement mechanism and validation of rules using multi-signature and thresh-hold signature schemes.
2) **Music DAO: a true decentralised DAO** We design and implement a real-world DAO that revolves around the music industry using the proposed infrastructure. We use a combination of networks, including the TU Delft

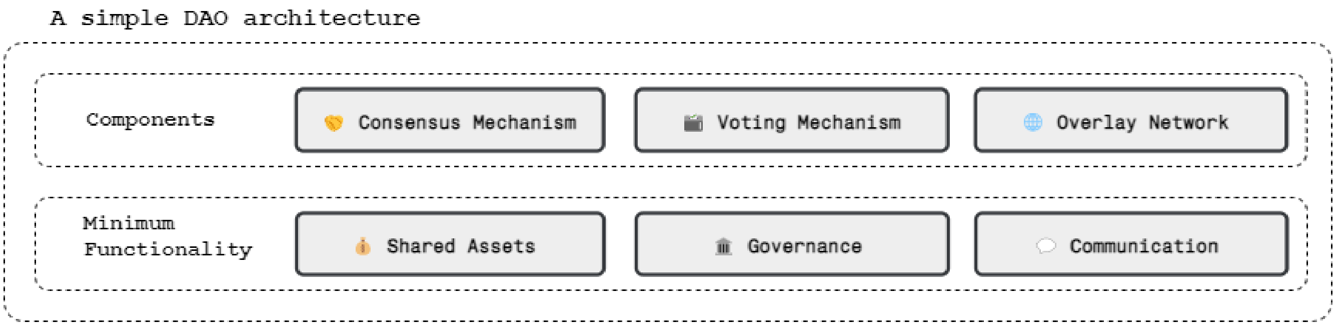

Fig. 1. A visual representation of the architecture of the simple DAO.

created IPv8, to create a music platform where artists can share music and receive funds from a flexible DAO crowdfund structure. This DAO runs on smartphones only, has no central components and is deployed on the Android Play store.

3) **Evaluation** To evaluate the proposed infrastructure and implementation, we perform a real-life deployment test amongst a set of participants who work closely with DAOs. In addition, we perform a set of performance tests on our voting and joining mechanism to see assess the performance in a real-world deployment. The results of these tests provide insights into the feasibility and effectiveness of our proposed architecture and implementation

II. Problem Description

The goal of this study is to develop and deploy an academically pure decentralised DAO. We define a DAO as *a mechanism for economic activity by an unbounded group of people in a competitive environment devoid of infrastructure, leadership, and legal centralized authority.* An organisation which relies on no central intermediary nor central authority and one which is truly unstoppable.

In DAOs rules are transparent and enforced by an underlying decentralized protocol, such as a public blockchain. The rules of such organizations can be changed collectively by its members through the voting in a governance protocol. While such organizations are autonomous to an extent, they will still rely on human individuals to perform certain tasks. A alternative recent definition proposed by Vitalik, one of the founders of Ethereum, for DAOs is it is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do [11].

The need for pure academic decentralisation arises from the fact that any deviation from this leads to the mechanism inheriting the problems associated with centralized traditional organizations. In traditional organizations, individuals work towards a common objective, but the rules are enforced by a central authority. Third-parties such as institutions, large technology companies, governments, and legal systems ensure that individuals can trust one another and cooperate, providing efficiency gains through their top-down control. However, their interests may not align with the interest of the participants. They may alter the rules in alignment with their own interest or not follow them at all. Even if participants have some influence on this process, it often is outdated and slow (democracy) or relegated to a select wealthy group (share-holders). For example, commercial companies, such as big-tech companies, are ultimately primarily interested in maximizing their own profits. They often use increase user retention rate, at the expense of social and economic problems,. This problem is exacerbated when power becomes concentrated more among a small group of people.

In the field of decentralized autonomous organizations (DAOs), developing a mechanism that simultaneously achieves trust, pure academic decentralization, and scalability is a major challenge. Real DAOs only exist in theory. Every technology claiming to be a DAO has central points of control and critically relies on central servers. Bitcoin and Bittorrent are the only examples of technology stacks which are not reliant on central infrastructure. Numerous startups claim to offer a DAO with decentralisation. To date, all DAOs are still centralised to some extend. The problem is to actually engineer what has been dubbed the future of the firm. The challenge is to incrementally realise a new organisational method to coordinate socio-economic activities. In theory a true DAO will be more efficient than a traditional company, replace middleman with code, and scale beyond any work-from-home company operating on informal email exchanges. In principle, a DAO should be able to replace current Big Tech companies. This requires scalability beyond 1 billion contributing users. Irrefutable proof that a decentralised DAO is possible is the first near-term problem.

III. Related Work

The concept of DAOs in academia is relatively new, it has mostly been developed by open source developers in the blockchain sphere. One of the first deployed and successfully used DAOs was created in 2016 by Christoph Jentzsch and was called “The DAO”. The goal of the project was to create a new business model for non-profit enterprises. With an internal capital of 150 million
USD from 11.000 investors at its peak, it was extremely large

for its time. It however suffered from an exploit in the smart contract [2], after which the Ethereum blockchain was forked to return the money to investors.

There has been considerable effort invested in observing and researching the phenomenon of deployed DAOs. Shuai et al. have developed a comprehensive framework for DAOs that identifies their characteristics, problems, implementations, and upcoming trends [23]. In addition, they suggest a five-layer architecture for DAOs. They do not, however, give a concrete implementation of such a DAO utilizing the design.

Hassan et al. conducted a similar study with the objective of identifying the largest unresolved issues in DAO research [13]. They pose the questions of which DAO layers should be decentralized, to what extent a DAO should be autonomous, and whether a DAO should be considered a legal entity. The identification of these obstacles eases the entry of new researchers into the field.

IV. A Simple DAO Architecture

We propose a generic and simple as possible architecture for DAOs. We deliberately remove all unnecessary features and complexity in order to provide a flexible and strong building block. Our building block represents a milestone within the evolution of actual DAO realisations: it is the first to achieve hyper decentralisation. Our minimal function decomposition leads to the following three architectual primitives, the minimal functionality a DAO handling activity should have and the accompanying components which should be implemented. An overview of this decomposition can be found in Figure 1.

A. Architectual Primitives

All accompanying components should adhere to these architectural primitives in order to satisfy the definition of a decentralized autonomous organization.

Trustless Any decision made in the organization should not depend on any third-party or intermediary. The trust that the decisions are created in a fair manner according to a set of voting rules and the execution of the decisions should be established through cryptographic, verifiable means.

Permisionless Any person should have the opportunity available to participate or access in the organization, without needing any approval of intermediaries. They should not be discriminated based on factors which are not relevant for the workings of the DAO. This does however mean that members in the organization can still collectively decide to block or not allow a person in the organization.

Transparent All information regarding the organization, its decision making process and decisions made should be available to access for everyone, inside and outside the organization. Transparancy is important to instill confidence that the other primitives are adhered to, since they can be verified.

B. Architectual Minimum Functionality

The DAO must have a minimum set of functions which provide the ability for participants to coordinate economic activity among each other.

Shared Assets For a DAO to fund its activities and achieve its objectives, it must have some notion of shared assets. Although DAOs without any assets can rely on altruism to some extent, most of the time financial incentives are needed to make work possible in practice. An obvious choice for DAOs are crypto-currencies, as they conform to all three primitives we previously established.

Governance In order for a DAO to achieve its objectives in an orderly and "$fair$" manner, a set of government rules should be established which dictate how decisions are made in the organization. Generally, individuals who contribute more and take on responsibility should have more benefits in the decision making process than others. However, this primitive is often a matter of debate, and the concept of "$fairness$" in decision making is also an open research question. Nevertheless, it is essential to establish some form of governance to enable effective decision-making.

Communication In order to coordinate governance and other activities, participants need to able to communicate with one another. The communication protcol must be tamper-proof and authenticated, so that participants can hold each other accountable for any decisions they make in i.e. governance procedures. Furthermore, the conversations should be available to all participants, in order to uphold the primitive of transparancy. This will allow new participants to review the history of the DAO, thereby enabling them to make informed decisions that align with the objectives of the organization.

C. Architectural Components

To meet the minimum functional requirements of a DAO, it is necessary to define a basic set of components that should be present in the organization. These components can be interchanged with any other implementation that adheres to the requirements of the component.

Consensus Mechanism A secure, decentralized and immutable blockchain is essential to enable participants who do not trust each other to coordinate economic activity. The decisions made by the organization should be stored in such a ledger of trust. The blockchain acts as a foundation of trust upon which participants rely to enforce the existing rules of the DAO and possibly also provide a mechanism to change the rules according to a set of meta-rules, i.e. a vote to change the rules. It is important that such a blockchain must have the capabilities for validating transactions using at-least multi-signature and thresh-hold signature schemes in order to facilitate off-chain transaction settlements.

A blockchain network is a network wherein participants come to consensus on a set of transactions. The network ensures the 1) validity and 2) ordering of the transactions. Transactions are grouped in blocks, which contain a set of transactions and the hash of the previous block. This makes it difficult for the chain to be tampered with. In order to agree on the same chain (ordering of transactions), consensus mechanisms are used. These are a collection of rules and financial incentives that determine which chain is favored and thus which ordering is used. For instance. in the case of

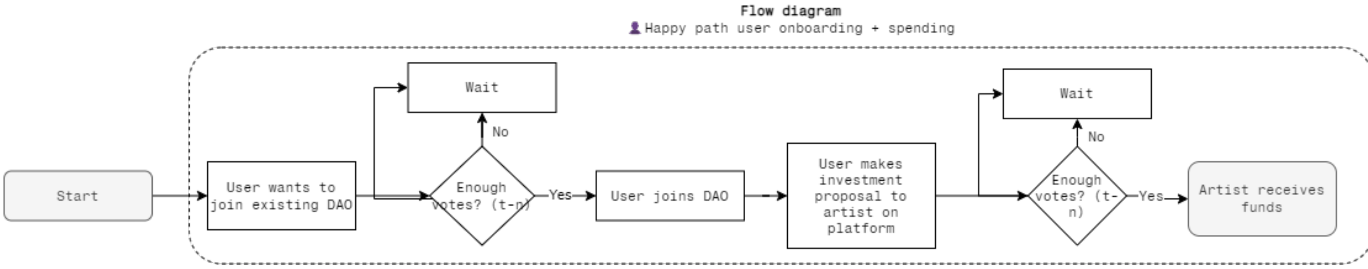

Fig. 2. Spending process

Voting Scheme	Private Keys	Interative	Message Complexity	Public Keys Published	Signatures Required	Signatures Published	Transactions Required	Total Transactions "Size"	
Smart Contracts	n		?	-	n	n	n*	O(n) * O(1)	
Naive MultiSig (OP_CHECKMULTISIG)	n		?	n	n	n	1	O(1) * O(n)	
Schnorr MuSig / MuSig2	n		?	1	n	1	1	O(1)	
Thresh-hold Sig	n	Yes	?	1	m ¡ n	1	1	O(1)	

TABLE I
COMPARISON SCHEMES OF VOTING MECHANISMS

Bitcoin, Proof-of-Work is utilized, where the chain with the most computational work is preferred over the others.

Voting Mechanism A voting mechanism is necessary in order to facilitate decision-making within in a DAO and allowing participants to come to reach on consensus on decisions that require a vote. This includes decisions on modification of existing rules, and decisions regarding current rules, such as the election of new members. The mechanism should be transparant and accesible to all members. The design of meta-rules should also be fair, however the definition of fairness is subjective and varies depending on the context and organization. This is still an unsolved problem and subject to ongoing research.

We propose a voting mechanism based on thresh-hold signature schemes. Thresh-hold signatures are a signature scheme where a minimum amount of partial signatures are combined in order to create a valid signature for a public key over a message. Each member possesses a shared public key. A secure Distributed Key Generation (DKG) protocol generates this key collectively using a predetermined threshold value. Members hold their respective portions of the corresponding private key. To sign a message, members of a t-n must participate in a thresh-hold signature signing protocol. A collective decision is simply the signing of an arbitrary message, since implicitly t-n members are required to sign a message that indicates t members have agreed on a proposal for a decision.

The implicit governance structure exhibited here is founded on the ownership of private key shares. A one-token-one-vote [25] model can be implemented using sybil-resistance mechanisms. In the absence of this restriction, a single user can create sybils to acquire additional shares based on the required criteria for membership. This can be desirable if, for instance, the members of the DAO wish to incentivize greater participation in the DAO (financial or otherwise), which can be rewarded with additional private key shares.

Overlay Network A peer-to-peer communication solution is necessary for enabling individuals to effectively communicate with each other and coordinate activities without intermediaries. This includes both protocol-level communication, as well as communication related to the organization's internal operations. The creation and dissemination of proposals for instance must be communicated among all members. This information however does not necceserily need to be stored in an immutable blockchain, since there is no relevant double-spending attack possible. Instead, a peer-to-peer communication solution would be sufficient for transmitting information that does not need to be permanently stored.

V. Voting Mechanism

In order to make decisions among a large number of participants possible, it is essential that there is some mechanism in place which off-loads the work from the blockchain. A typical blockchain which is actually decentralized and secure currently still has a small throughput. A trivial solution would be casting every vote in a proposal as a transaction on the blockchain. This would quickly become infeasible if the number of participants increase.

Our proposed scaling solution aims to address the issue of scalability by avoiding the need for transitioning between complex smart contract states on a blockchain with global

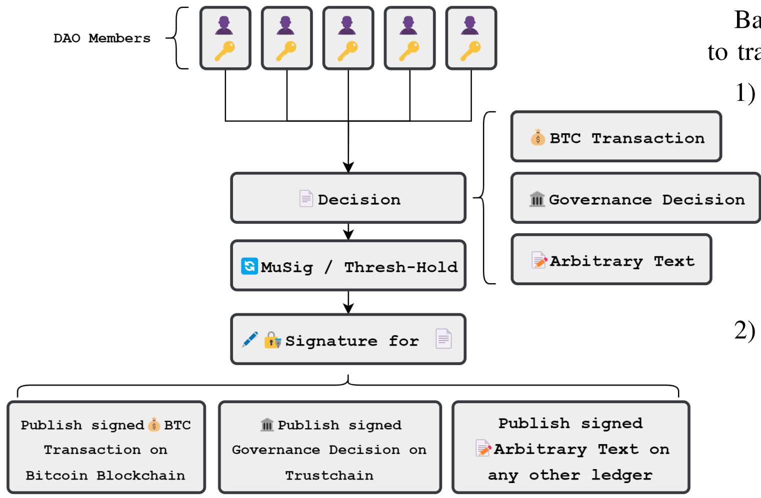

Fig. 3. The voting mechanism of the Simple DAO

consensus for making decisions. Instead, we leverage the use of threshold signature schemes among the DAO participants to achieve consensus on what state changes and decisions should be made. The key idea is only the relevant participants should validate whether the state transition rules have been followed, by participating in the group signature scheme for a particular proposed transaction. This approach reduces the complexity and computational requirements while still ensuring that decisions are made in a decentralized and trustless manner. By reducing the reliance on global consensus, we can improve the scalability and efficiency of the platform.

A. Blockchain Model

We make assumptions about how our blockchain works and provide some formal specification based on Al-Bassam's work [6]. We assume a blockchain model consisting of blocks $b_0, b_1..., b_n$. Every block contains a header h_i and a set of transactions $T_i = \{t_0...t_n\}$. This header contains a merkle root m_i of the set of transactions T_i.

All of the transactions are signed with a shared public key created by a thresh-hold signature scheme, of which the share keys are shared among the participants. The parameters of this signature scheme can be changed, a higher thresh-hold will require more participants to participate which increases the effort needed to commit fraud.

In this set of transactions, multiple types of information pertaining to the DAO can be stored. Most importantly, in a UTXO based blockchain, the transactions can lock up some financial value: the DAO treasury. The total locked up value c_i is equal to the treasury amount.

DAO Transitions

In order to make a decision in the DAO, its state needs to transition from one state to another. A new group signed transaction must be published to the blockchain. Anyone can propose to sign a new transaction. This transaction must follow 2 rules:

Based on these rules, there are two main ways for the state to transition:

1) Treasury re-allocation: this transaction transfer funds from the DAO treasury to an arbitrary address, to fund some type of economic activity.
   a) (1) a valid transaction from old outputs to a target input, with the rest of the funds sent to the DAO treasury
   b) (2) verify is empty
2) Thresh-hold signature inclusion: this transaction adds a new members to the DAO, by moving all the treasury funds from old locked up outputs, to a single new locked up output which is signed with a group signature where the new members is included. The new member should send sufficient coins as a entrance fee to the DAO treasury in the transaction.
   a) (1) a valid transaction where all funds are sent to the DAO treasury using the new key
   b) (2) verify should check whether the new members sent sufficient coins to the DAO treasury, before signing
3) Thresh-hold signature removal: this transaction removes a existing member to from the DAO, by moving all the treasury funds from old locked up outputs, to a single new locked up output which is signed with a group signature where the new members is excluded. If so desired, the DAO can choose to send some of the funds back to an address which is owned by the removed member.
   a) (1) a valid transaction where all funds are sent to the DAO treasury using the new key
   b) (2) verify is empty

B. Security Model

In this proposed architecture, the security model differs significantly from that of a smart contract platform run on a blockchain with global consensus. In a traditional blockchain, transactions are validated according to a set of rules that are determined by a group of miners. If 51% of all miners agree to, for example, commit fraud, it is possible for them to do so. In other words, the validator set consists of all the miner nodes in the network and the accompanying hash-rate.

In contrast, our security model rests on the number of particiapnts in the DAO that are part of the group signature group. If 51% of the people (or any other percentage, depending on the n-k threshold) want to commit fraud, it is possible for them to do so. The main advantage of this model is that the complexity of the client-side rules can be arbitrarily complex and is essentially free to compute, since we only need to verify the transaction on the client side. The other nodes in the network, which do not have anything to do with the DAO, do not have to validate the client-side rules. 51% of the DAO members can run the client-side rules, verify their correctness, and if they are valid, participate in the threshold signature

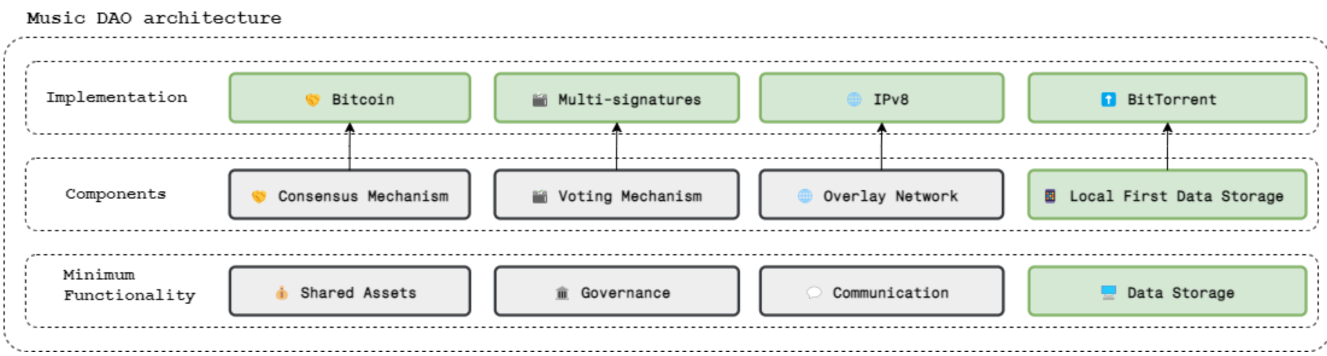

Fig. 4. A visual representation of the Music DAO based on the simple DAO.

scheme. If they do not verify, they can simply not participate, after which no signature will be created.

In this design, we do not rely on advanced turing-complete smart contract capabilities. Instead, we use a blockchain of choice, namely Bitcoin, which is simple and secure, and does not require advanced smart contract capabilities. In this way, we can achieve a high level of security and scalability, while keeping the complexity of the system at a minimum.

VI. Music DAO: a truly decentralised DAO

We have created an implementation of a DAO centered around music using our proposed architecture. This implementation uses all the specified architectual components and adheres to the architectural primitives that we have laid out in Section IV. In this section we describe its functionality, the implementation choices we made and any additional components we added.

The objective of the Music DAO is to enable artists to earn a living through music and to allow listeners to listen to their preferred music and support artists. While music platforms and labels also facilitate this process, these intermediaries often take a significant portion of the revenue, create platform lock-in for both artists and listeners, and have a disproportionate amount of power over artists [CITE].

In order to realize this objective, the DAO consists of two main components: the music platform, and the crowdfund platform. The music platform enables the dissemination and availability of music and it's meta-data. The crowdfund platform allows listeners to collectively manage funds, which they can use to fund new projects of their favorite artists.

Music Publishing Artists can publish music to the platform. Published music is shared on the IPv8 peer-to-peer overlay network. The music is first encoded to the correct format and an accompanying torrent file/torrent meta-data is created for the formatted data. This meta-data is then published on the personal trustchain of the user and gossiped around to other users. At the same time, the torrent file is published on the BitTorrent DHT network and is available to seed from the phone. Additional meta-data such as album art cover is also included in the published music and is displayed in the GUI.

Data Availability Listeners keep seeding a part of their music according to some type of a set of rules, for instance based on popularity. The optimization of this process is out of scope for this work. For this implementation, the most popular music and a selection of the less popular music (tail-end) is randomly selected and seeded.

Music Listening Different users on the network can receive the signed trustchain blocks and add them to their local storage of published music. They use the meta-data in the block to query the DHT network and download peer information to download the torrent from seeders. After the music has been downloaded, everything is verified, and the listener can listen to the music with the accompanying data.

The implementation is created using Kotlin and Android on the JVM platform. This allows for deployment on the Play Store and accessibility for hundreds of users. Cross-platform mobile application is outside the scope of our use case, due to many of our libraries not being available, such as our chosen overlay network IPv8. Android additionally provides extensive service APIs that allow services to continously run in the background, allowing for the upkeep of the network.

We chose to limit our implementation to smartphones only for several reasons, all of which align with our primitive of creating a permissionless system. Additionally, smartphones have a lower barrier to entry, as almost everyone has a phone, especially in developing countries, and not everyone has a PC. The zero-architecture server stack also supports the idea that smartphones are the superior device for maintaining and using P2P networks.

The use of BitTorrent in our implementation is due to its reliability and decentralization. BitTorrent has a proven track record of stability and security, with 19 years of incremental improvements to the protocol. While other technologies such as IPFS offer similar functionality, BitTorrent is more widely adopted and has a larger user base. By extracting torrent info hashes from the platform, we can facilitate mass seeding of the network, or allow users to download content using popular torrent clients without the need for our application. The use of the accompanying Distributed Hash Table (DHT) network in our implementation is to remove the need for tracker servers, which are centralized and may be taken down by law enforcement agencies. DHT networks are much harder to take down and only require a simple bootstrap node, which can be

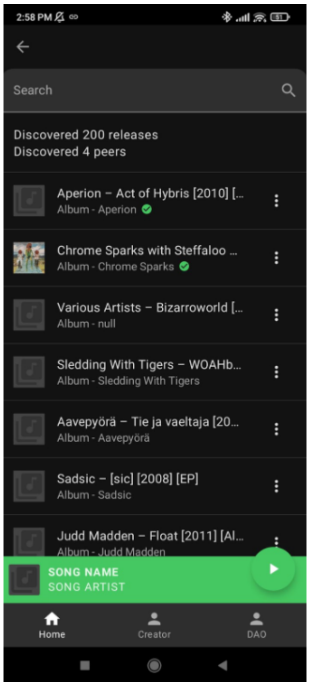

Fig. 5. Homepage of the Music DAO

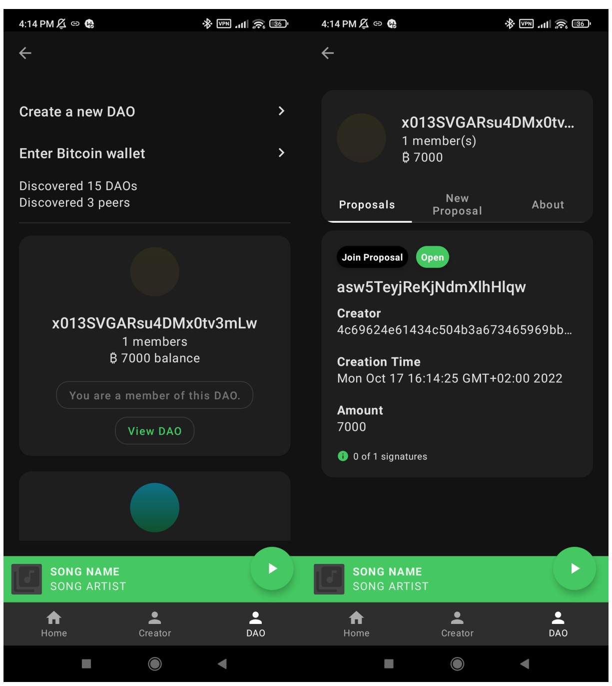

Fig. 6. All available DAOs in the Music DAO

any node with sufficient knowledge, after which you can get almost any swarm info about a info-hash in the network.

VII. Performance Evaluation

In the previous sections, we have discussed the infrastructure of our DAO and the design and implementation of the Music DAO. In this section, we will perform both a qualitative and quantitative evaluation of our DAO in terms of usability and performance. We deploy our DAO on the Android play store and do a real life usability test amongst a set of participants who work closely with DAOs. In order to evaluate the performance and scalability, we measure the performance of the joining scheme in a deployed setting using multiple phones. To evaluate the usability, we perform various experiences on time to discovery on listening and discovering DAOs.

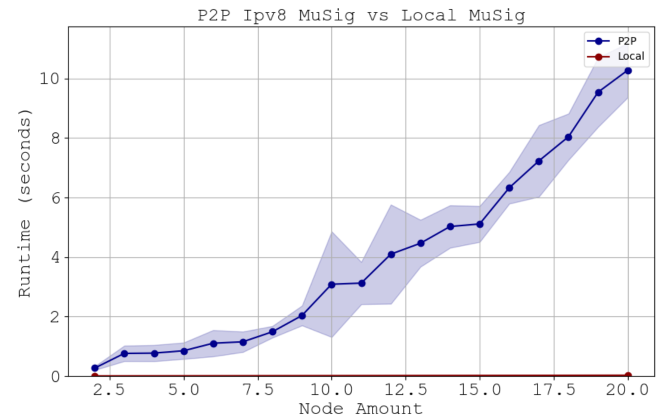

Fig. 7. Performance of our voting mechanism

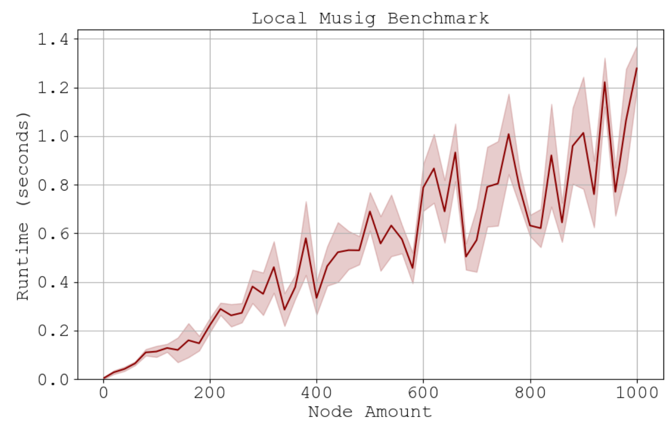

Fig. 8. Performance of our voting mechanism

A. Performance Experiment

For the performance experiment, we wish to determine whether the DAO can scale in a deployed, real-world environment. Specifically, we wish to examine how the voting mechanism scales with the number of voters. In a deployed environment, many factors are at play, including phone performance, network type and connectivity, and implementation of the various technology layers. With these experiments, the interaction between the IPv8 overlay network, the multi-signature scheme, and the Bitcoin network will be evaluated.

For our evaluation we closely analyze the multi-signature scheme MuSig first and foremost. For this evaluation, we want to analyze the performance of MuSig and get insight into a lower bound for our complete voting mechanism. To do this, we run the whole protocol in a single process on an Android emulator. We measure the time it takes for a number of nodes to collectively run the protocol, that is: create an aggregated public key, nonce and signature. The key generation of the individual nodes is not included in this measurement. The results can be found in 7.

The following evaluation measures MuSig implemented on top of a overlay network using IPv8. For this, a peer to peer protocol implementation was made which allows nodes to collectively sign arbitrary messages, solely with UDP messages. The evaluation was done on an Android emulator. On the emulator IPv8 nodes are started which each have an endpoint in the same network with different ports. The results can be found in 8. In this graph, the lower bound of MuSig running locally can be seen as well.

B. Usability Experiment: discovering music

We measure the time it takes for music to show up in the application using two phones using benchmark code within the application. One phone will act as a seeder and one phone will receive new releases. The phones are connected to the same local network. The experiment is run 10 times and the results can be found in Figure 9. All measurements end up being under two seconds, which is a reasonable time to wait. Notice that in a setting with more phones, this time will decrease due to more chance of releases being gossiped to the receiver phone. This thus can be interpreted as an upper bound.

C. Usability Experiment: discovering DAOs

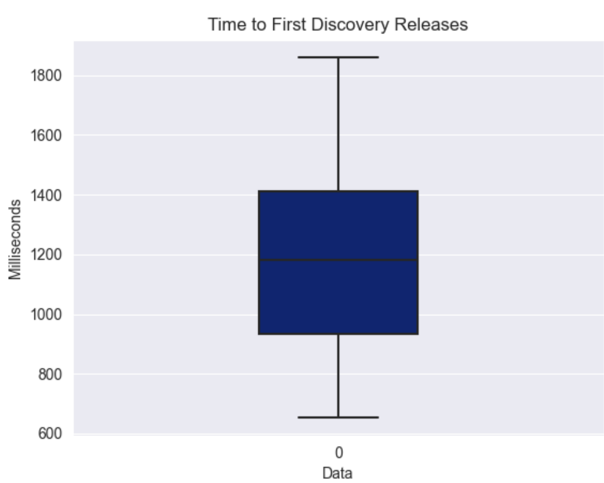

Fig. 9. Time to first discovery music

D. Real-life deployment test

In order to evaluate the usability of our tests, we have additionally do a real-life deployment test. Participants are given a presentation on DAOs and were subsequently provided access to the application, which is deployed on the Google Play Store. This allows us to gather valuable insight on the usability and user experience of our solution in a real-world setting.

VIII. Conclusion

In an increasingly connected world where big-tech and governments are centralizing power, decentralized autonomous organizations (DAOs) offer a bottom-up approach for collaboration on the internet. However, many DAOs suffer from issues caused by managerial and infrastructure centralization. In this work, we have proposed a simple and robust architecture for DAOs that allows for economic activity while maintaining complete decentralization. The Music DAO, which utilizes the most robust currently live-deployed networks, demonstrates the viability of this architecture, and our evaluations show that it is both scalable and user-friendly.

IX. Acknowledgment

References

[1] bips/bip-0340.mediawiki at master · bitcoin/bips — github.com. https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki. [Accessed 30-Jun-2022].

[2] A call for a temporary moratorium on the dao.

[3] Helium x2013; Introducing The Peopleapos;s Network — helium.com. https://www.helium.com/. [Accessed 30-Jun-2022].

[4] The state and future of Decentralized Autonomous Organizations (DAOs) including 6 leading examples - Ross Dawson.

[5] Uniswap combined metrics.

[6] Mustafa Al-Bassam. Lazyledger: A distributed data availability ledger with client-side smart contracts. *arXiv preprint arXiv:1905.09274*, 2019.

[7] Alireza Beikverdi and JooSeok Song. Trend of centralization in bitcoin's distributed network. In *2015 IEEE/ACIS 16th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD)*, pages 1–6. IEEE, 2015.

[8] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.

[9] Usman W Chohan. The decentralized autonomous organization and governance issues. *Available at SSRN 3082055*, 2017.

[10] Lin William Cong, Zhiguo He, and Jiasun Li. Decentralized mining in centralized pools. *The Review of Financial Studies*, 34(3):1191–1235, 2021.

[11] Ethereum Foundation. Daos, dacs, das and more: An incomplete terminology guide.

[12] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 3–16, 2016.

[13] Samer Hassan and Primavera De Filippi. Decentralized autonomous organization. *Internet Policy Review*, 10(2):1–10, 2021.

[14] Christoph Jentzsch. Decentralized autonomous organization to automate governance. *White paper, November*, 2016.

[15] Chelsea Komlo and Ian Goldberg. Frost: flexible round-optimized schnorr threshold signatures. In *International Conference on Selected Areas in Cryptography*, pages 34–65. Springer, 2020.

[16] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, Dec 2008.

[17] Pim Otte, Martijn de Vos, and Johan Pouwelse. Trustchain: A sybil-resistant scalable blockchain. *Future Generation Computer Systems*, 107:770–780, 2020.

[18] Johan Pouwelse. Towards the Science of Essential Decentralised Infrastructures. In *Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good*, pages 1–6, Delft Netherlands, December 2020. ACM.

[19] Stefan Scharnowski and Yanghua Shi. Bitcoin blackout: Proof-of-work and the centralization of mining. *Available at SSRN 3936787*, 2021.

[20] Jack Schickler. Sweden, EU Discussed Bitcoin Proof-of-Work Ban: Report — coindesk.com. https://www.coindesk.com/policy/2022/04/21/sweden-eu-discussed-bitcoin-proof-of-work-ban-report/. [Accessed 30-Jun-2022].

[21] William Stallings. *Handbook of computer-communications standards; Vol. 1: the open systems interconnection (OSI) model and OSI-related standards*. Macmillan Publishing Co., Inc., 1987.

[22] Alexandra Torbensen and Raffaele Ciriello. Tuning into blockchain: Challenges and opportunities of blockchain-based music platforms. In *Twenty-Seventh European Conference on Information Systems (ECIS2019), Stockholm-Uppsala, Sweden*, 2019.

[23] Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, and Fei-Yue Wang. Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems*, 6(5):870–878, 2019.

[24] Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, and Fei-Yue Wang. Decentralized Autonomous Organizations: Concept, Model, and Applications. *IEEE Transactions on Computational Social Systems*, 6(5):870–878, October 2019.

[25] E Glen Weyl, Puja Ohlhaver, and Vitalik Buterin. Decentralized society: Finding web3's soul. *Available at SSRN 4105763*, 2022.

[26] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. A Taxonomy of Blockchain-Based Systems for Architecture Design. In *2017 IEEE International Conference on Software Architecture (ICSA)*, pages 243–252, Gothenburg, Sweden, April 2017. IEEE.

[27] Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to scalability of blockchain: A survey. *IEEE Access*, 8:16440–16455, 2020.

[28] Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to Scalability of Blockchain: A Survey. *IEEE Access*, 8:16440–16455, 2020.