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 document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***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. Many of such organizations have already been deployed in the wild successfully. For instance, Uniswap, a decentralized exchange, reached transaction volumes to up to $85.5 billion in November 2021 [**uniswap˙volume?**]. It is used by hundreds of thousands of people to exchange currencies, and its token can be used to manage and alter the exchange's rules collectively. Prior to this, decentralized protocols such as BitTorrent and Wikipedia have enabled millions of individuals to collaborate in file sharing and information accumulation. Already, billions of users collaborate and consume information on Wikipedia. We anticipate that DAO technology will eventually mature and enable Big Tech alternatives.

Most deployed DAOs suffer from forms of centralisation in the governance structure and infrastructure. There is no real managerial decentralization. Even the currently second-largest DAO by market capitalisation, APE DAO, suffers from this through their initial token distribution, where 38% of the tokens were distributed to various founders which now have a disproportionate amount of voting power. Proposals are vetted by a centralized moderation team, and are all executed off-chain by the foundation members of the DAO. Another instance, Solend, one of the largest decentralized lending systems, was plagued by a second incident of concern. After a DAO vote, the development team took control of and liquidated the account of a "whale" with approximately $170 million worth of cryptocurrency, as it allegedly posed a systemic risk to the ecosystem at the time. In essence, 1% of the tokens might take 80% of the protocol's overall liquidity.

Proof-of-work and proof-of-stake blockchains, on which most DAOs run, suffer from centralisation problems. Cong et al. show that in the long run, due to centralized mining pools, Bitcoin will have a decentralized market structure [**cong2021decentralized?**]. Increased centralisation in mining will merely bring such blockchains back to square one relative to systems like PayPal and VISA. In addition, the current geographical centralisation of mining pools poses a threat to decentralization [**scharnowski2021bitcoin?**]. 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.

In addition, currently deployed DAOs suffer from the fact that current blockchains have very limited transaction output [**zhou˙solutions˙2020?**]. Bitcoin has a throughput of 7 transactions per second and Ethereum 18 transactions per seconds. Proof-of-work blockchains attempt to circumvent this by working with fewer miners which process more transactions, this however brings us back to square one to VISA-like systems. Proof-of-stake blockchains 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 present a new architecture for DAOs which is completely decentralized and scalable. We design, implement, and evaluate a prototype using this architecture for a DAO revolving around music, the Music DAO. This implementation only uses smartphones and is currently deployed live. We perform a real world test with users and perform an analysis on the performance of our voting mechanism. Academic decentralisation within a viable and sustainable DAO represents a key milestone in Web3 evolution. We believe an as-simple-as-possible DAO with very basic governance, membership voting, and treasury management is a key step forward.

This research contributes the following:

1) **Infrastructure design** We design and justify an infrastructure for DAOs which is completely decentralized and scalable. For this, we provide a set of technologies and principles that must be followed. We separate the settlement mechanism and validation of rules using multi-signature and thresh-hold signature schemes.
2) **Music DAO** We design and implement a real DAO which revolves around the music industry using our infrastructure. We use a combination of networks, including the TU Delft 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** We perform a real-life deployment test amongst a set of participants who work closely with DAOs. In addition, we do a set of performance tests on our voting and joining mechanism, to see what the performance in a real deployment is like.

II. Problem Description

The objective of this work is to design, implement and evaluate an architecture for an academically pure DAO with complete decentralization and scalability. Academic decentralization within a viable and sustainable DAO represents a key milestone in Web3 evolution. We believe an as-simple-as-possible DAO with very basic governance, membership voting, and treasury management is a key step forward.

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. The definition of a traditional organization is a group of individuals working toward a common objective, but whose rules are enforced by a central authority. Institutions, large technology companies, governments, and the legal system ensure that individuals can trust one another and cooperate. However, the centralization of these third parties brings with it a variety of issues. They are hierarchical in nature and suffer from a concentration of power in the hands of large shareholders who control the decision-making process. In other words, they are centralized in nature. They use this centralization to increase their efficiency. Internet and web 2.0 technologies have merely accelerated this development.

The aforementioned aspects resulting from centralized authorities are problematic for many reasons. They can at any time change the rules by which users interact. Users have no control over this decision-making. Furthermore, we can say that their interests do not align with the interests of the users, due to their profit-seeking behaviour. In addition to other problems, they use algorithms to maximize user retention rates in order to maximize profit, ignoring all social-economic problems, and abuse their user data.

Decentralized autonomous organizations (DAO) are a new form of organization which are both decentralized and autonomous. These organizations operate without a centralized authority. The 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 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 [**dao˙blog˙foundation?**]".

The main advantages of DAOs are thus summed by the following:

1) Efficiency: avoiding managerial overhead by replacing it with code
2) Decentralization: avoiding all the disadvantages which centralization brings such as corruption, collusion, profit as interest only

The challenge is to find a set of design primitives and technologies for a DAO which is actually completely decentralized and can scale. In addition, such a DAO should not only exist in theory, but also should be deployed in practice with no economic incentive mechanisms for the developer (such as transaction fees) built into the protocol.

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 [**dao˙memorial?**], 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 [**8836488?**]. 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 [**hassan2021decentralized?**]. 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.

The rest of the work in the field is mostly focused on governance issues and problems [**jentzsch2016decentralized?**] [**chohan2017decentralized?**].

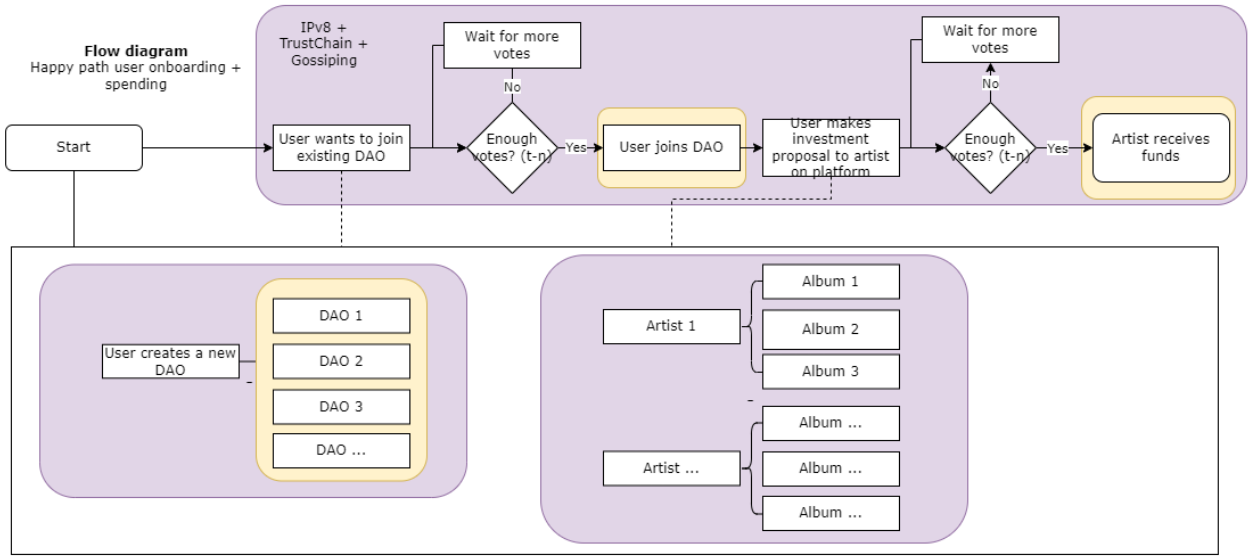

Fig. 1. Spending process

IV. A simple DAO architecture

One of the consequences of limited transaction output following from blockchain networks is that developers reach for other types of solutions, often centralised ones, in order to make their use-cases such as governance possible. Trivial solutions such as simply increasing the blockchain size inevitably lead to more bloated chains, which leads to a higher barrier for entry for new users wanting to support the network. Various other solutions have been proposed and are being worked on, such as layer-two solutions and proof-of-stake updates such as the current Ethereum upgrade.

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.

A. Consensus Layer

A blockchain is simply a linked list of blocks, which include a set of transactions, where every block contains the hash of the previous block. A transaction contains the information that is needed to change the state of something: be it a bookkeeping currency linked to addresses or the state of a smart-contract. All the nodes in a blockchain must agree on the state (and thus ordering) of the blockchain with a consensus mechanism. The state transitions of the transactions are thus checked by all nodes to see if they are valid. In the case of Bitcoin, this is ensured by a set-of-rules, namely that the chain with the most work done is regarded as the true chain. In addition to this, a consensus mechanism contains more parts such as economic incentives to not collude.

For our DAO, we propose a much simpler, pragmatic solution based on the principle that only users of a ”smart-contract” should be responsible for the validation and storage of transactions.

A transaction consists of two elements:

1) A message that is valid on the blockchain that is used.
2) A valid group signature created by a thresh-hold signature scheme.

Transactions are defined as a message that is signed with a group signature created by a thresh-hold signature scheme. The group consists of all the members of the application. These messages are a valid transaction of the used blockchain, and can contain some state transition, such as the transfer of money from one address to another. Only end-users of the DAO store these transactions

In order to create a valid transaction, it must 1) be signed by at-least the thresh-hold amount and 2) be a valid transaction for the used blockchain. This in turn means that the group itself can be considered as the consensus set.

A client-side contract, or ”smart-contract”, is simply some logic that is run before a transaction is signed. All the data of previous transactions in the group is checked against the logic, in addition to the fact that it is checFed whether the transactions are actually present in the blockchain.

In the case of a DAO, we are concerned with voting on proposals in order to spend funds.

In our infrastructure, we define three types of functionalities a user can take on:

1) **Node running the blockchain network.** This is a node which participates in the consensus mechanism of the blockchain network that is used. In the Bitcoin network this for instance is a miner running a proof-of-work algorithm, and on Ethereum this can be a validator node staking Ethereum.
2) **End-user node.** This is a node which is an end-user of the application, but does not necessarily participate in the consensus mechanism of the used blockchain.

For our infrastructure we need a number of components:

1) **A blockchain network.** A secure, peer-to-pee
2) **A peer-to-peer overlay network.** A peer-to-peer overlay network is needed which connects the users of a ”smart-contract” with each other. It must offer identities and authenticated messaging.

The main advantage of this is that the rest of the nodes in the network do not need to run the transaction validation logic of all the users of an application. They only are concerned with verifying signatures of messages, which is much less expensive than running arbitrary code from a virtual machine such as the one available in the Ethereum Virtual Machine.

B. A peer-to-peer overlay network

A peer-to-peer communication solution is needed for individuals to communicate with each other on both a protocol level and on a organisatory level to coordinate activities in the DAO itself. The creation of proposals for instance must be communicated to all members. This information however does not neccesserily need to be stored in an immutable block-chain, since there is no relevant double-spendign attack possible. In other words, all communication that does not need to be stored forever needs such a solution.

C. Local-first data storage

Local first data storage is needed to store digital assets which are located in the DAO. Not all assets are simple ownership proofs or hashes, often times assets are media files or other documents. These types of assets are too expensive to be replicated completely on every node in a blockchain. The organization itself needs to hosts these assets, in such a way that every user contributes a part to this process.

D. Voting Mechanism using Threshold Signatures

V. Architecture

We present a generic and as simple as possible architecture for a DAO. 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 () components required.

A. Blockchain network

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 transactions and the hash of the previous block. This makes it hard 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 (often financial) incentives to determine which chain is favored and thus which ordering is used. In the case of Bitcoin Proof-of-Work is used, where the chain with the most work is preferred over the others.

The DAO consists of a collection of transactions which the members collectively make and need to agree upon, without trusting each other. The purpose of the blockchain is to make this possible. In the most generic case, this is the transfer of funds from a treasury after i.e. a voting procedure. In a more complex case, this can be some arbitrary logic from a ”smart-contract”.

B. Overlay Network

A peer-to-peer communication solution is needed for individuals to communicate with each other on both a protocol level and on a organisatory level to coordinate activities in the DAO itself. The creation of proposals for instance must be communicated to all members. This information however does not neccesserily need to be stored in an immutable block-chain, since there is no relevant double-spendign attack possible. In other words, all communication that does not need to be stored forever needs such a solution.

C. Local First Data Storage

Decentralized data storage solution is needed to store digital assets which are located in the DAO. Not all assets are simple ownership proofs or hashes, often times assets are media files or other documents. These types of assets are too expensive to be replicated completely on every node in a blockchain. The organization itself needs to hosts these assets, in such a way that every user contributes a part to this process.

D. Treasury

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-votecitewеyl2022decentralized 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.

A double-spend proof consensus layer is required to have users commit to collectively made decisions, such as the acceptance of a new DAO members or the spending of funds. For this, a DLT can be used which has a sound consensus mechanism with proper incentives. It is important for such a DLT to be decentralized, secure and performant. In practice is appears to be hard, as can be seen by the blockchain trillema [**8962150?**].

In this solution, we limit the need for on-chain storage and verification to a minimum, compared to traditional multi-sig solutions [CITE] or the solutions using smart-contracts. Only data which is required to have confidence in commitment of decisions is stored and verified on-chain. This allows us to remedy the throughput issues of DLTs such as Bitcoin.

Building upon the aformentioned primitives, we design the DAO such that it is a collection of UTXO (wallet) locked up by a Taproot script (described later) using the shared public key. Decisions in this DAO can be arbitrary, but for the management of funds we identify two decisions which are important. Namely, 1) the joining of the DAO 2) the spending of funds.

E. Thresh-hold Signatures

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. In a DAO, there are a

F. Voting Mechanism

1) (some voting mechanism is needed in order for governance to be possible)
2) (add requirements: flexibility, scalability, security)

G. Off-chain Scaling

1) (using thresh-hold signature schemes in order to decrease amount of work needed to be done on-chain)
2) (other scaling solutions possible too)

VI. Infrastructure

We propose an infrastructure for decentralized DAOs with the aim for the organization to be both decentralized and scalable. This design is based on a number of 1) functionalities and 2) generic technology solutions which can be swapped out with equivalent networks. We base our technologies on Rowdy et al. [] primitives on DAOs.

A. Technologies

Permission-less blockchain A double-spend proof consensus layer is required to have users commit to collectively made decisions, such as the acceptance of a new DAO members or the spending of funds. For this, a DLT can be used which as a sound consensus mechanism with proper incentives. It is important for such a DLT to be decentralized, secure and performant. In practice is appears to be hard, as can be seen by the blockchain trillema [**8962150?**].

Decentralized data storage solution A decentralized data storage solution is needed to store digital assets which are located in the DAO. Not all assets are simple ownership proofs or hashes, often times assets are media files or other documents. These types of assets are too expensive to be replicated completely on every node in a blockchain. The organization itself needs to hosts these assets, in such a way that every user contributes a part to this process.

Peer-to-peer communication solution A peer-to-peer communication solution is needed for individuals to communicate with each other on both a protocol level and on a organisatory level to coordinate activities in the DAO itself. The creation of proposals for instance must be communicated to all members. This information however does not necceserily need to be stored in an immutable block-chain, since there is no relevant double-spendign attack possible. In other words, all communication that does not need to be stored forever needs such a solution.

B. Functionalities

Treasury 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-votecite weyl2022decentralized 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.

A double-spend proof consensus layer is required to have users commit to collectively made decisions, such as the acceptance of a new DAO members or the spending of funds. For this, a DLT can be used which has a sound consensus mechanism with proper incentives. It is important for such a DLT to be decentralized, secure and performant. In practice is appears to be hard, as can be seen by the blockchain trillema [**8962150?**].

In this solution, we limit the need for on-chain storage and verification to a minimum, compared to traditional multi-sig solutions [CITE] or the solutions using smart-contracts. Only data which is required to have confidence in commitment of decisions is stored and verified on-chain. This allows us to remedy the throughput issues of DLTs such as Bitcoin.

Building upon the aformentioned primitives, we design the DAO such that it is a collection of UTXO (wallet) locked up by a Taproot script (described later) using the shared public key. Decisions in this DAO can be arbitrary, but for the management of funds we identify two decisions which are important. Namely, 1) the joining of the DAO 2) the spending of funds.

Digital Democracy Problem Locked up funds run the risk of being locked up forever if participants do not ever agree on a decision or if participants become in-active. We coin this the digital democracy problem. One solution to remedy this, which we use in our architecture, is the ability for an increasingly lower thresh-hold number of members to be required over time to spend the funds.

Funds are locked up using a specially constructed Taproot script. When members decide to construct a shared key, an additional set of shared keys is constructed as well using lower thresh-hold amounts. In the Taproot script hashed time locked contracts are combined with the different public keys over time. The public keys with lower thresh-holds will be locked with the time locks which are the largest. As time passes, smaller amount of participants will be able to unlock the funds in order to spend them.

Social Coordination

1)
2)

Voting Mechanism

Market Place

VII. Music DAO

We have created a proof-of-concept implementation of our infrastructure design to create a crowdfund DAO for music artists. This prototype implements all the technologies and functionality that we have specified. With this case study we show that dis-intermediation in the music industry is possible in practice [**torbensen2019tuning?**]. Our implementation is based on the zero-server-architecture stack [**pouwelse˙towards˙2020?**]]. It solely makes use of Android devices and no desktop computers. It uses IPv8/TrustChain [**otte2020trustchain?**] as the overlay network for communication between peers. In particular, the still immature Kotlin implementation of the protocol is since the app is Android based.

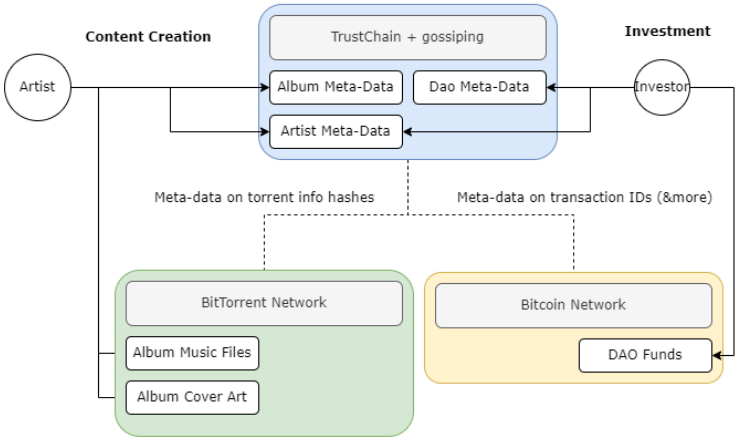

Fig. 2. Architectural components of the Music DAO

The Music DAO is managed by DAO participants who are both listeners and musicians, with the common goal of creating music, listening to music, and supporting musicians. The objective is to redistribute power back to end-users and away from large intermediaries such as record labels and streaming platforms, allowing artists to act as their own publisher, distributor, label and investment firm.

1) Zero-server infrastructure
2) No governance token [cite paper]
3) No platform specific token for financial value transfer
4) Permission-less
5) Every peer in network equal (ideally no federation)

The permission-less blockchain that is used is the Bitcoin network. It is one of the longest standing and most robust blockchain networks [cite]. The consensus mechanism and PoW have been unchanged since its inception and the price of an double-spend attack is very large (add dollar amount).

The decentralized data storage solution we have opted to use is the Bittorent protocol, along with its DHT discovery protocol.

We employ IPv8/Trust-Chain as our peer-to-peer communication solution. In this section, we organize and store items in users' personal ledgers. Using info-hashes of torrents and Bitcoin transaction hashes, respectively, these items are connected to the BitTorrent and Bitcoin networks.

Streaming of songs is handled by the BitTorrent protocol. Discoverability of such data will be done through the BitTorrent DHT protocol through querying info-hashes. Meta-data such as info-hashes are distributed using IPv8/TrustChain. Users can publish meta-data on their own chain, or, in case transactions with other users data will be published and signed by two users on both their chains.

To access any type of meta-data three strategies wil be used:

1. Passively gossiping data to other peers on the overlay
2. Querying a specific user for all their meta-data 3.

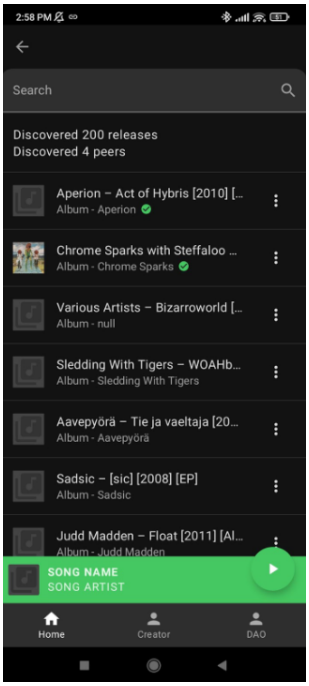

Fig. 3. The homepage of the application

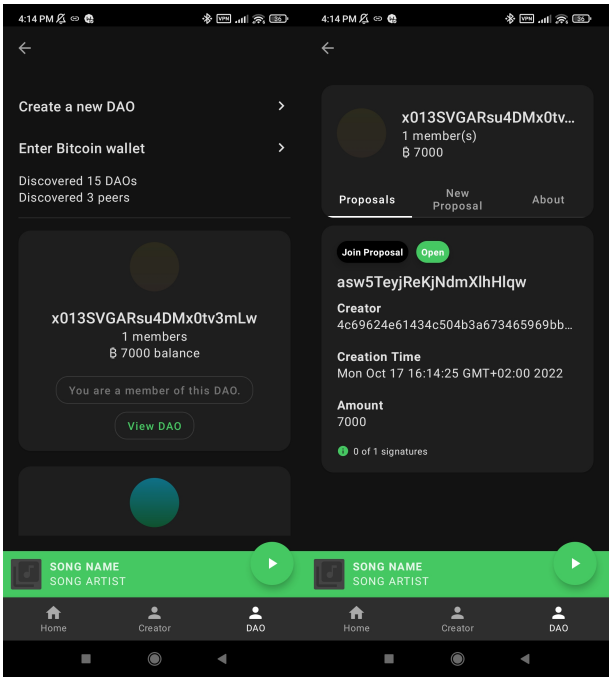

Fig. 4. The DAO screen

Querying random users in the overlay for a specific users meta-dat

Artists can set-up a crowdfund wallet within the DAO to request for funds from their listeners in return for a promise for music.

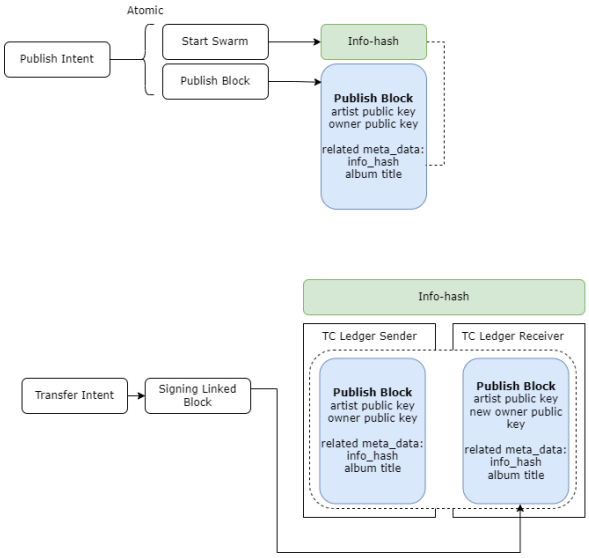

Fig. 5. The NFT protocol

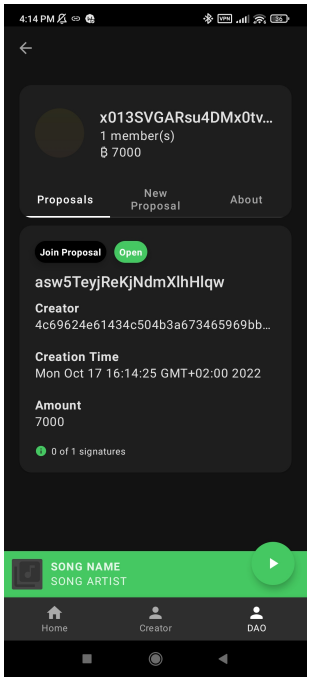

Fig. 6. The Bitcoin wallet

VIII. 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. Then we do an experimental analysis on the performance of the multi-signature voting scheme.

A. Real-life deployment test

B. 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.

The initial experiment will utilize actual phones. To measure the time between the creation of a DAO and the addition of a new member, a benchmark script is developed. All existing DAO members will be required to sign the new members into the DAO.

The second experiment will be done locally using a set of local IPv8 nodes running on a computer.

IX. Conclusion

Acknowledgment