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 blockchain-powered organizations that can run on their own without any central authority or management hierarchy [**?**]. These organisations have emerged in recent years as a result of Web 3.0 and permissionless blockchains. In the real world, some of these organizations tranasct billions worth of volume between its members. These new technologies facilitate the ability for individuals to reach consensus, removing the need for a trusted third-party. This allows individuals to directly co-orporate with each other, a DAO.

However, DAOs which are truly decentralized only exist in theory. Every technology claiming to be a DAO has central points of control and critically relies on central servers. [cite / give some examples]. Bitcoin and Bittorrent are the one of the few 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 [ref to related work].

The reason for this is two-fold. Firstly, achieving scalability while staying decentralized is still an unsolved problem [**?**]. Reaching consensus between participants is expensive due to communication overhead and often requires economic incentive. Secondly, contemporary DAOs are focused on speculation and earning money, and shortcuts such as centralization are used to achieve this goal. There is little focus on development on technologies that can make truly decentralized, scalable DAOs possible.

The objective of this work is to design, implement and evaluate an novel architecture for an academically pure DAO with academic decentralization focuses on while staying scalable. 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. The design of a novel architecture for an academically pure DAO with simple but fundamental primitives. An implementation of the architecture using completely decentralized technologies [cite zero-server-architecture stack]. An real-world performance evaluation of the architecture and a real-world test.

However, completely decentralized DAOs exist only in principle. Every technology claiming to be a DAO has centralized control and relies heavily on central servers. [cite / provide examples]. Bitcoin and Bittorrent are two instances of technological stacks that do not rely on centralized infrastructure. Many startups claim to provide a DAO with decentralisation. To some extent, all DAOs are still centralised [refer to related work].

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 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.

Traditional organizations are defined as a group of people working together with a particular purpose towards a collective goal. At the same time, people have individual interests and act in their own interest. Institutions, big-tech companies, governments, the court-of-law, make sure that people can trust each other and co-orporate. The centralization of these third-parties bring along a set of problems however. They are hierarchical in nature and suffer from power concentration of large share-holders which control decision making. In other words, they are are centralized in nature. They leverage this centralization for efficiency. The introduction of the internet and web 2.0 technologies have only accelerated this process.

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 au-

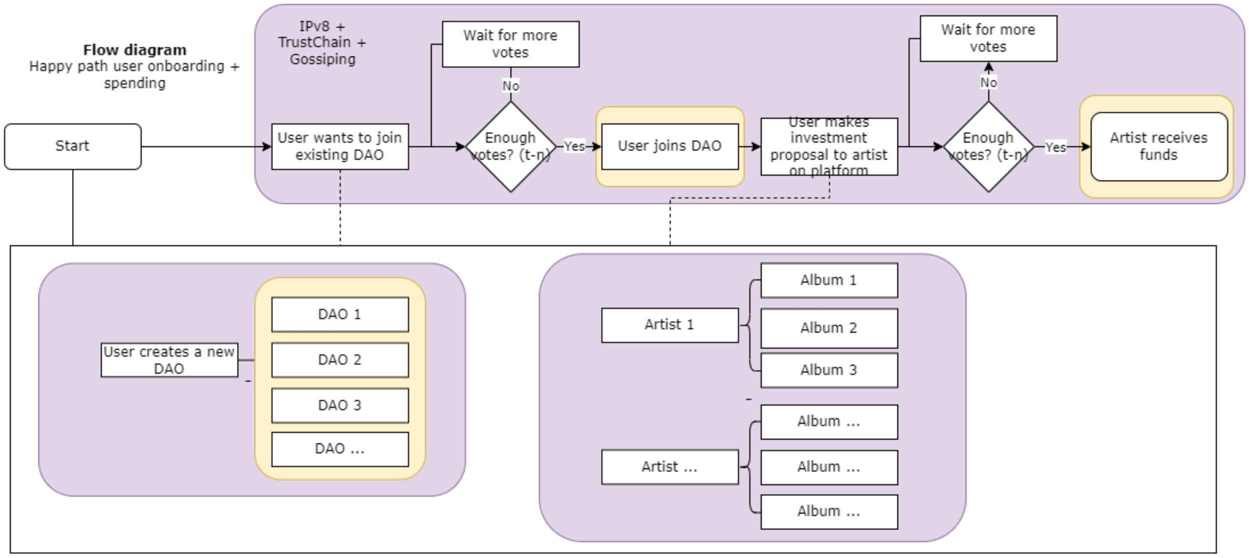


Fig. 1. Spending process

tonomous. 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 [**?**]”.

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

III. Related Work

IV. 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. [] primtives 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 [**?**].

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-voteciteweyl2022decentralized 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 [**?**].

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 us- ing 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 Voting Mechanism

Market Place

V. Music DAO Prototype

We have created a proof-of-concept implementation of our infrastructure design to create a crowdfund DAO for music artists. This prototype implemenets all of 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 [**?**]. Our implementation is based on the zero-server-architecture stack [**?**]]. It solely makes use of Android devices and no desktop computers. It uses IPv8/TrustChain [**?**] 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.

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

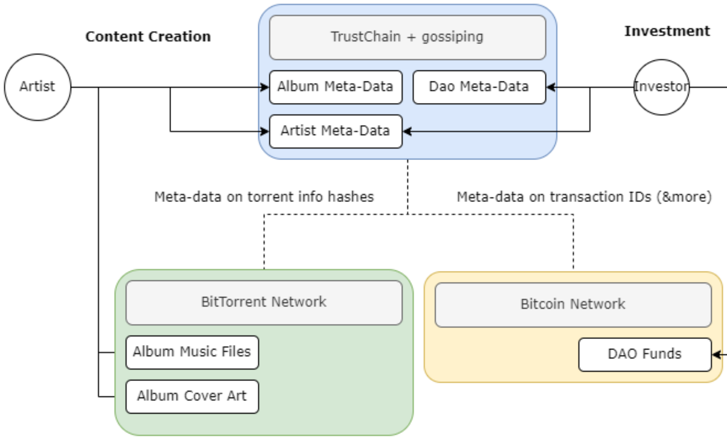
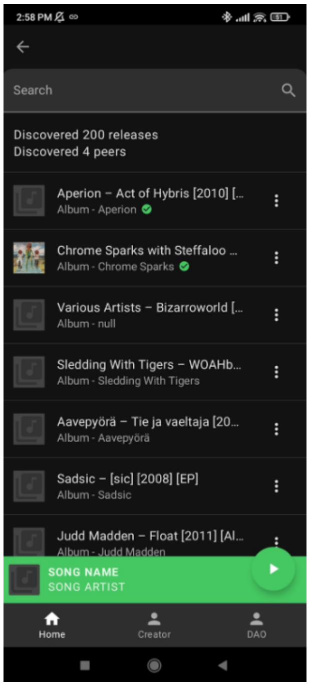


Fig. 2. Architectural components of the Music DAO



2:58 PM

Search

Discovered 200 releases
Discovered 4 peers

Aperion – Act of Hybris [2010] [...
Album - Aperion

Chrome Sparks with Steffaloo ...
Album - Chrome Sparks

Various Artists – Bizarroworld [...
Album - null

Sledding With Tigers – WOAHb...
Album - Sledding With Tigers

Aavepyörä – Tie ja vaeltaja [20...
Album - Aavepyörä

Sadsic – [sic] [2008] [EP]
Album - Sadsic

Judd Madden – Float [2011] [Al...
Album - Judd Madden

SONG NAME
SONG ARTIST

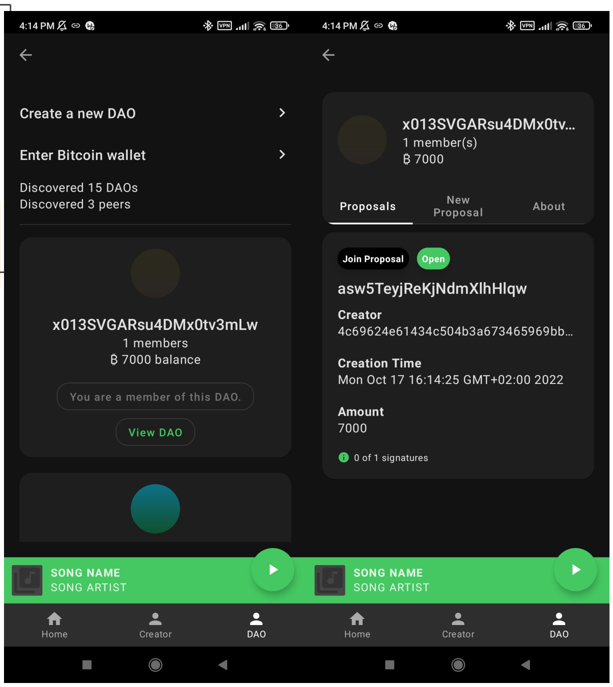
Fig. 3. The homepage of the application

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

VI. Evaluation Results

VII. Conclusion

Acknowledgment



4:14 PM

Create a new DAO

Enter Bitcoin wallet

Discovered 15 DAOs
Discovered 3 peers

x013SVGARsu4DMx0tv3mLw
1 members
₿ 7000 balance

You are a member of this DAO.

View DAO

4:14 PM

x013SVGARsu4DMx0tv...
1 member(s)
₿ 7000

asw5TeyjReKjNdmXlhHlqw

Creator
4c69624e61434c504b3a673465969bb...

Creation Time
Mon Oct 17 16:14:25 GMT+02:00 2022

Amount
7000

0 of 1 signatures

SONG NAME
SONG ARTIST

Fig. 4. The DAO screen

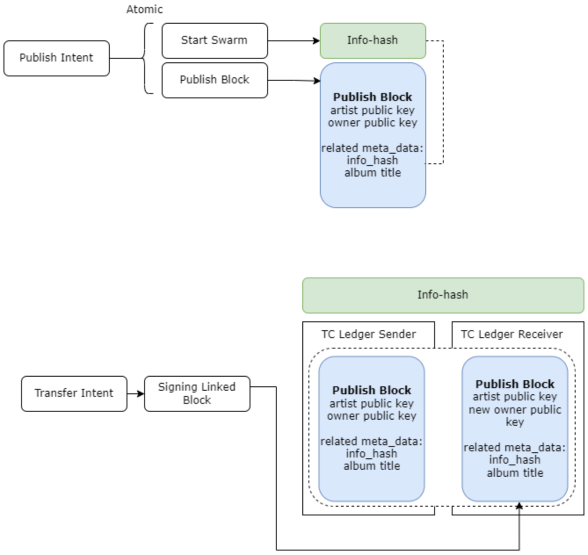
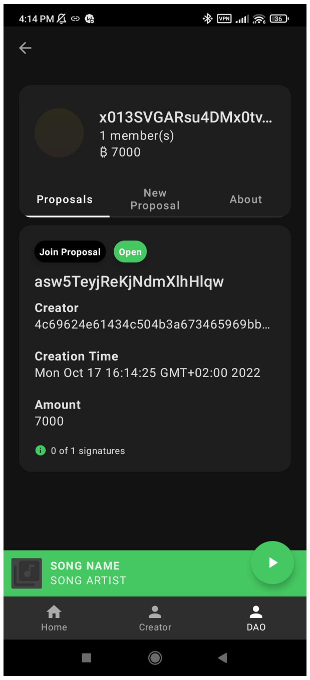


Fig. 5. The NFT protocol



x013SVGARsu4DMx0tv...
1 member(s)
Ƀ 7000

asw5TeyjReKjNdmXlhHlqw

Creator
4c69624e61434c504b3a673465969bb...

Creation Time
Mon Oct 17 16:14:25 GMT+02:00 2022

Amount
7000

0 of 1 signatures

SONG NAME
SONG ARTIST

Fig. 6. The Bitcoin wallet