Unstoppable DAOs for web3 disruption

Chotkan, Rowdy; Decouchant, Jérémie; Pouwelse, Johan

DOI
10.1145/3565383.3566112

Publication date
2022

Document Version
Final published version

Published in
DICG 2022 - Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good, Part of Middleware 2022

Unstoppable DAOs for Web3 Disruption

Rowdy Chotkan
Delft University of Technology
Delft, The Netherlands
R.M.Chotkan-1@tudelft.nl

Jérémie Decouchant
Delft University of Technology
Delft, The Netherlands
J.Decouchant@tudelft.nl

Johan Pouwelse
Delft University of Technology
Delft, The Netherlands
J.A.Pouwelse@tudelft.nl

ABSTRACT

Decentralised Autonomous Organisations (DAOs) have the capability of being a disruptive Web3 technology. Their usage of cryptographically secure distributed ledgers shows promise of replacing existing technical and financial intermediaries. However, this promise has not been fully materialised yet: existing attempts typically rely on centralisation as the required decentralised components do not exist or are not mature enough. We present our Web3 Deployment Experiment around a robust decentralised economy to address these issues. Our economy is unique due to the removal of all centralised components and governance. It is resilient against legal and economic attacks as no individual or organisation can compromise its functioning. We dub this characteristic *extreme decentralisation*. Similar to BitTorrent and Bitcoin, our extreme decentralisation DAOs carefully avoid single points of failure and are effectively unstoppable. Within our experiment around a music economy, we bypass all intermediaries in finance, technology, and the music industry itself with a direct donation to musicians. We demonstrate the viability of collective decision-making within our decentralised economy and present a set of principles for Web3 DAOs. Our implementation shows that the DAO ecosystem is fully deployable on smartphones, allowing anyone to create a DAO without reliance on central authorities or components.

CCS CONCEPTS

• **Networks** → **Peer-to-peer networks**; • **Security and privacy** → **Distributed systems security**; • **Computer systems organization** → **Peer-to-peer architectures**.

KEYWORDS

Decentralised Autonomous Organisation, Decentralised economy, Trustless infrastructure, Web3

ACM Reference Format:
Rowdy Chotkan, Jérémie Decouchant, and Johan Pouwelse. 2022. Unstoppable DAOs for Web3 Disruption. In *3rd International Workshop on Distributed Infrastructure for the Common Good (DICG '22), November 7, 2022, Quebec, QC, Canada.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3565383.3566112

DICG '22, November 7, 2022, Quebec, QC, Canada

ACM ISBN 978-1-4503-9928-9/22/11.
https://doi.org/10.1145/3565383.3566112

1 INTRODUCTION

Bitcoin solves the double spending problem without any trusted third party and is unstoppable in practice [10]. The ability for anyone to print their own money has disrupted the money creation monopoly of commercial banks. BitTorrent is a fully decentralised protocol that disrupted the broadcast monopoly of the content industry and is also unstoppable. The challenge we tackle in this work is to craft Distributed Autonomous Organisations (DAOs) as unstoppable as BitTorrent and Bitcoin.

A DAO is a system that enables a group of people to govern themselves and collectively manage some common goal or asset through a set of self-executing rules [9]. By applying extreme decentralisation, we design an ecosystem able to sustain DAOs with a novel cardinal feature – to be unstoppable. In practice, this equates to a socio-technical system that is resilient against legal and economic attacks as no individual or organisation can compromise its functioning.

DAOs are the natural economic element of Web3. Web3 is being touted as the future of the Internet. A future in which data is no longer in the grip of Big Tech, but liberated through decentralisation, distributed ledgers, and token economies. The vision for this new, ledger-based web is based on (extreme) decentralisation. With our DAOs, we demonstrate the feasibility of disrupting a Big Tech monopoly.

Our work combines the technologies from BitTorrent and Bitcoin into the communication (peer-to-peer) and financial (cryptocurrency) foundations together with a distributed ledger of our own design called TrustChain [13]. It represents a breakthrough for organising economic interaction in an adversarial environment. All prior DAO work has a vulnerable central element. To date, no implementation existed with fully decentralised governance, common treasury, et cetera. Our work is the first to achieve extreme decentralisation of all these essential DAO components.

This work makes the following contributions:

- *Architectural DAO principles* — We identify a set of architectural principles that are necessary for unstoppable economic interactions in an adversarial environment. They serve as a foundation for creating DAOs that are truly decentralised and unstoppable in nature.
- *Extreme Decentralisation DAOs* — We present our DAO architecture, operating without any central component or single point of failure. This economy allows any party to create a DAO and democratically manage collective funds. We combine direct peer-to-peer communication of the Trustchain [13] ledger with the transaction mechanism of Bitcoin. We meticulously avoid the need for a new speculative token and build everything on multi-signature transactions of Bitcoin Taproot [12]. Our DAOs are generic in nature and, in principle,

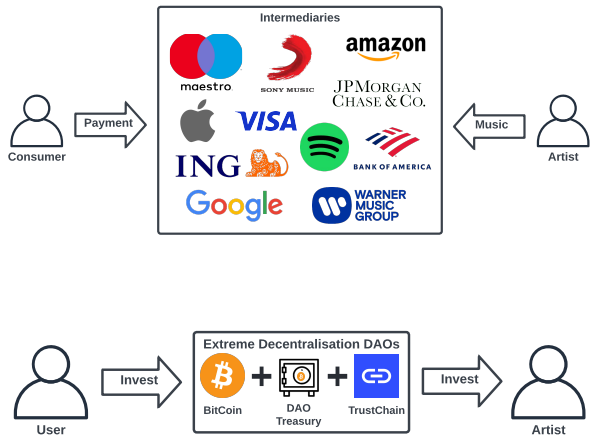

Figure 1: Contemporary music industry (a) dominated by intermediaries and (b) DAO-based music ecosystem with extreme decentralisation.

capable of disrupting any Big Tech monopoly using a Web3 alternative.

- *Web3 Deployment Experiment* — We build a Web3 application for the music industry on top of our unstoppable DAOs. In order to validate the disruptive potential of our technology, we report on a real experiment using our implementation. We enable direct investment into artists and remove all intermediaries from the value chain: payment processors, credit cards, banks, Big Tech, and music labels.

2 PROBLEM DESCRIPTION

Our goal is to devise a fully decentralised Web3 ecosystem that allows any user to create a decentralised autonomous organisation, without relying on any intermediary or central authority. We dub this principle *extreme decentralisation*: a truly free ecosystem in which equality is central, everybody is in control, and governance is democratic, whilst avoiding any single point of failure. Designing unstoppable DAOs and crafting disruptive Web3 applications is hindered by the open problem of creating an investment platform without any server or database, whilst still offering trustworthy services.

We specifically focus on the music industry to demonstrate our work. As illustrated in Figure 1, the music industry is currently dominated by intermediaries. Streaming platforms have caused the first wave of consolidation within that industry. The open question is whether financial actors can be replaced with fans directly rewarding artists and anybody investing in upcoming talent. Re-creating the function of various intermediaries within a DAO structure is an unexplored research topic. This problem goes beyond writing business logic in smart contracts. The challenge is to replace entire value chains with DAO and Web3 code. Wikipedia and Linux show that quality control within such public infrastructure is strenuous (something we address specifically using Trustchain).

Finally, smartphones are replacing the PC. The challenge is to create a DAO and Web3 platform without using any servers or clouds, and without any PC. The issue of how to pool unreliable donated smartphone resources in a peer-to-peer fashion to offer a reliable DAO service for mobile devices is unsolved.

3 ARCHITECTURAL PRINCIPLES

We present our architectural principles, built on top of the properties for decentralised finance proposed by Werner et al. [21]: non-custodial, permissionless, openly auditable, and composable. We identify the following set of principles vital for Web3 decentralised economies.

Self-organising — Some form of overall order arises from local interactions between DAO participants. Self-organisation is not a characteristic that can be enforced, it *emerges* with a deliberate painstaking system design. Avoiding any central orchestrating entity is a necessary condition for organic growth and continued DAO evolution. Self-organisation also enables a minority to fork and evolve towards a different direction in a sustainable manner.

Zero-server — Augmenting the self-organisation principle is the zero-server principle: *no one* has a special role or distinctive function. No special servers, intermediaries, or superpowers may exist. An egalitarian approach at the lowest level aids the unstoppable characteristic.

Democratic — The ecosystem must be inherently democratic. Without democratic principles, an ecosystem would not be able to fairly reach a consensus on any matter. Even though we do not enforce any type of governance structure within the system, we believe that democracy is crucial to achieving self-regulation because some notion of order is required to achieve the common goals set out within a DAO.

Non-custodial — Individually held funds always remain under the full control of their owner (i.e., self-sovereign). In particular, the cryptographic keys belonging to a digital wallet are held by their actual owner. Similarly, the funds held by a DAO's community are also always under full collective community control. No contemporary DAO has this architecture principle and as a consequence, a vulnerable central element remains.

Permissionless — Disrupting existing monopolies without first obtaining their permission is essential. Web3 is only viable if permissionless innovation and shielding from lawyer-based attacks exist. Big Tech companies today may decide to *cancel* any voice, content, or financial fund without public consultation [16]. Our principles replace this approach with permissionless collective decision-making, leading to improved societal outcomes.

Trustless — Establish a *never trusted, always verified* model. Devoid of intermediaries, the system is inherently trustless as it does not require participants to trust others to not disrupt the workings of the ecosystem [17]. This principle is protected through the democratic nature of the ecosystem: any change brought upon an organisation must pass democratic polling in order to come into effect.

Openly auditable — The system must be verifiable. Given the trustless nature of the ecosystem, verifiability is required to guarantee fairness. Open auditability ensures that all outcomes are

verifiable. This leads to a system in which all can verify whether an output is valid.

Composable — The inner workings of the system are not fixed. They can be composed such that new functionalities can be realised. This allows for interoperability as well as flexibility in terms of infrastructure. This flexibility counteracts fixed behaviour within the ecosystem, as components can be composed such that they can provide new functionalities.

Modular — The infrastructure is modular. As a consequence, there exists no single point of failure nor is lock-in enforceable. Any service within the ecosystem can be replaced by another. This modular design enables availability, liveness, and upgradeability, ensuring that the design can stay robust and future-proof.

4 SYSTEM DESIGN

Our design is based on the interconnection of four components: (1) distributed ledgers; (2) treasury; (3) governance; and (4) digital identity. These components do not operate as independent processes, rather, they work in conjunction to achieve our envisioned functionalities for unstoppable DAOs. However, they can be regarded as *modular* and enable the *composable* nature of the architecture.

4.1 Distributed Ledgers

Distributed ledger technologies (DLTs) serve as our cornerstone. They enable the majority of the previously defined principles in the architecture. Their consensus mechanisms enable tamper-proof transactions and verifiability within the economy. We use both Bitcoin and a scalable ledger called TrustChain [13]. Bitcoin is used to perform multi-signature transactions using threshold signatures, whilst TrustChain is used for public key pinning and membership operations.

Our design inherently adheres to the majority of the architectural principles defined in section 3. More precisely, the ledgers are *permissionless*. Our design is also *trustless* as public key encryption enables anyone to verify the actions of others and, therefore, ignore invalid requests or other malicious interactions. The system is *openly auditable* as all interactions are recorded on the ledgers, allowing one to verify their validity at their own discretion. This building block of our design is also *modular* and adheres to the *zero-server* design philosophy as any of the two blockchains can be replaced by others and incorporate no required servers to interact with.

4.2 Treasury

The DAO treasury represents the capital of an organisation. It is a component of our design that is facilitated by the used DLTs. We envision that the DAO treasuries are implemented as shared cryptocurrency wallets. These wallets hold the cryptocurrency belonging to the organisation and can only perform transactions when (a part of) the members provide their signature. They enable the *democratic* nature of our ecosystem and ensure it is *non-custodial*. Through this principle, all funds belonging to a DAO are managed directly by its community as no transaction can be made without the signature of (a part of) the members. In our prototype, this functionality is optimised through the use of threshold encryption. The application depends on the Bitcoin Taproot upgrade [12]. More specifically, we utilise Schnorr signatures [18] to create multi-signature Bitcoin wallets. These wallets enforce democracy within the decentralised organisations as threshold encryption ensures that a transfer is only executed when a specific number of members vouch for it.

4.3 Governance

Governance within the organisations is per principle democratic: transactions are only performed when a majority of its members vote in favour of it. This majority ruling is not only in use for monetary transfers but also for additions of new members and changes in parameters related to the DAO, e.g., changing the threshold within the encryption scheme or an entrance fee. The democracy within the community adheres to the one-person-one-vote model. Where existing DAOs typically use the one-token-one-vote model [22], favouring power to those holding the most amount of wealth. We argue that the one-person-one-vote model ensures fairness as power is distributed equally amongst members. This layer of our design ensures the *democratic* principle whilst also strengthening the *non-custodial* nature of the ecosystem. Furthermore, it aids in creating *self-organisation*: the governance structure allows all organisations to run independently of each other whilst also ensuring that the capital within the organisations is not in the hands of governments or other institutions. Both the power and the wealth are in the hands of the people.

4.4 Digital Identity

Without strong digital identity, attacking the democratic values of our ecosystem would be rather trivial. An adversary would be able to create Sybils [6] and join an organisation multiple times in order to possess the majority of the voting power. Thus, strong digital identity is required to prevent abuse. As traditional digital identities typically introduce central components [3], we argue that the use of Self-Sovereign Identity [20] provides the design with the security it requires whilst not introducing centralised components. Self-sovereign identities allow users to manage their own identities through credentials signed by relevant parties. This enables verification of relevant credentials without interacting with third parties.

5 EXTREME DECENTRALISATION DAOS

Our architecture operates in a fully decentralised setting. Participants of the network directly communicate with each other, in a peer-to-peer fashion. This network is maintained by the participants without central components. Communication channels are constructed independently. The network is permissionless and egalitarian, hence, all clients possess the same permissions. All participants use public key encryption and thus have a public key through which they can be identified.

The main logic of our Web3 model can be concretised into three interactions:

DAO creation — A user initiating a DAO performs the following procedure. First, the initiator decides the entrance fee f and the encryption threshold t. The entrance fee dictates the amount that

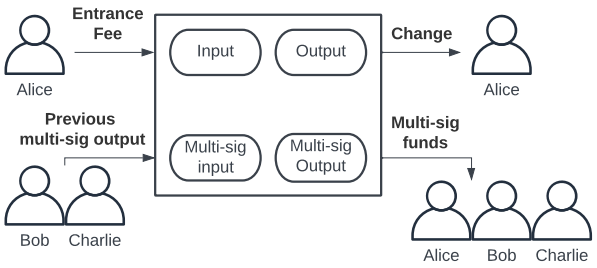

Figure 2: Transaction performed for new members

must be invested into the DAO in order to be eligible for membership. The threshold value represents the proportion of the members that must vote in favour of a proposal for it to be accepted, e.g., for membership or investment proposals. The initiator creates the DAO treasury by generating a multi-signature wallet for its own public key and the given threshold. Note that at this stage, the wallet type and threshold number do not matter as the initiator is the sole owner. Next, the initiator transfers the entrance fee to the generated DAO treasury and publishes information about the DAO to the ledger. In the application, a TrustChain block comprising the DAO's information is added to the initiator's personal ledger and is broadcast across the network. This information consists of the public treasury information, the list of current participants, the entrance fee amount, and the threshold value. These parameters are public as they are necessary for potential members to propose their joining.

DAO treasury deposits — A potential member aspiring to join the organisation runs the following procedure. The relevant information about the organisation is fetched from the distributed ledger on which it was published during the last update of the organisation. A new member generates a new multi-signature wallet for the existing DAO treasury, adding itself to the set of public keys of the current members P. Next, they create an unsigned transaction transferring the funds from the DAO's existing wallet to the new wallet whilst simultaneously transferring the entrance fee from a personal wallet. This leads to the transaction visualised in Figure 2, comprising both transfers in a single atomic transaction. The new member then proposes their joining by initiating a vote. They do so by multi-casting the unsigned transaction to the existing members. Members then perform a binary vote: they either vote in favour by providing the potential member with their partial signature for the transaction or reject the request. In case all signatures are received, the new member is able to sign the transaction, after which they broadcast it to the payment network. This leads to a replacement of the wallet in the DAO's treasury, transferring the capital to the multi-signature wallet containing the new member. Finally, the new member publishes the latest DAO information to the ledger. In case the voting procedure does not reach the threshold required for transfer, the potential member is unable to perform the transaction and thus does not become a part of the organisation.

Investing from a DAO's treasury — Performing investments from a DAO's treasury takes place in a similar fashion as the previous procedure. A member creates an unsigned transaction for transferring a specific amount n to an address a. This unsigned transaction is then proposed to the other members, which then execute the same voting mechanism. In case the number of received signatures surpasses the threshold, the proposer is able to sign the transaction by combining the signatures. The transaction is then broadcast over the payment network, transferring the funds from the DAO's treasury to the investment address.

6 IMPLEMENTATION & EXPERIMENT

We have created a fully functioning Android application that implements our principles and follows our system design. The application supports the discussed functionalities: users can create DAOs, invest in DAOs, perform voting, and make investments from DAOs. The Bitcoin token is used as DAO capital and as the currency of investments. Information about the DAOs is stored on TrustChain ledgers. The code of the application has been published on GitHub[1].

The application is implemented as a module in the TrustChain SuperApp [14]. With our open testing program, a few hundred Internet volunteers successfully used our work. Figure 3 showcases screenshots of the user interface and depicts the ability to join DAOs and vote on proposals. This project incorporates a TrustChain implementation as well as a communication protocol. Communication channels in this protocol are formed in a decentralised manner through NAT puncturing. Clients communicate peer-to-peer, allowing DAO members to communicate without intermediaries.

In the TrustChain blockchain, each user maintains a personal ledger. The blocks within these ledgers can be programmed to specific types, allowing for the identification of each organisation. TrustChain requires no proof-of-work nor global consensus, which

[1]https://github.com/Tribler/trustchain-superapp/tree/master/currencyii

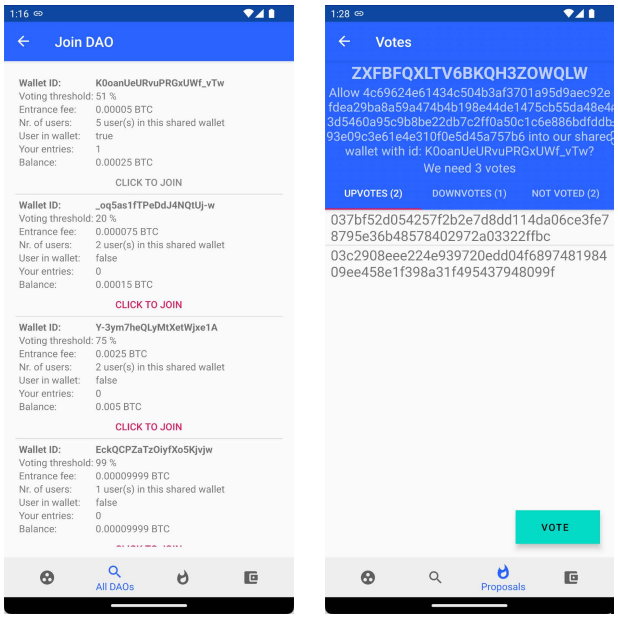

Figure 3: Our fully functioning Android prototype showcasing (a) DAOs within the network and (b) the decentralised voting mechanism.

serves the needs of an organisation comprised of selected members. Information about organisations is published on the ledger, allowing users to scan the network to find the latest information. This block contains the previously discussed information: the list of members, the entrance fee, the threshold value, and the address containing the funds of the organisation. As mentioned, the solution uses the Bitcoin blockchain with the Taproot upgrade [12]. This upgrade enables us to create multi-signature wallets using Schnorr signatures [18].

If we use the Nakamoto Coefficient [19] as an indicator of decentralisation, then our work rates significantly beyond the academic and industrial state-of-the-art (e.g. Bitcoin and Cardano). Our DAOs remove the need for a governance token by adhering to the one-person-one-vote model. Reliance on governance tokens would lead to a direct reliance on DLTs for governance, as is the case for existing DAOs (e.g., see MakerDAO [7] or Aave [8]). In our system, DLTs are merely used for capital, ensuring funds are transferred without the need for intermediaries. In a blockchain, mining pools are the cardinal vulnerability as only a few are needed to fully control it. Even in the instance that a used blockchain is compromised, the DAO and its governance are secure, merely the capital is at stake.

Using the communication protocol of the SuperApp in conjunction with the TrustChain ledger and the Bitcoin blockchain, our architecture achieves *extreme decentralisation* as neither single points of failure nor central components exist within the network.

6.1 Web3 Deployment Experiment

We set up an experiment that provides evidence for the viability of our Web3 DAOs. We do so by demonstrating its usability for the music industry. We performed an experiment in which we used five smartphones running our Android application. The implementation is capable of live Bitcoin transactions but currently lacks basic software quality assurance measures. As such, the experiment was conducted in the Bitcoin Regression Test Network.

A single client, serving as the artist, created a DAO. This DAO serves as a platform through which anyone can invest in the artist. The entrance fee gives each user the right to a vote within the organisation. The actual artist serves in principle no bigger role within an organisation created in our economy than any of the participants. However, they represent a common goal around which the participants want to create a community. Capital is invested by joining participants as well as through donations to the fund. This can be performed by members, outsiders, or even the artists themselves. This capital is then used as deemed fit by the participants. The actual spending is performed through democratic governance within the organisation as discussed in section 5. The goal is to grow the capital with the motive to support the artist. Interests make the organisation an investment opportunity for investors. Artists are incentivised through patronage from users as well as through the capital of the DAO that can support their ventures.

Next, the remaining clients joined the organisation. All transferring the required entrance fee to the DAO's treasury, updated by the latest joining member, and collecting signatures for signing the transactions, until all clients were connected to the organisation. Upon success, we doubled, using an unconnected wallet, the capital

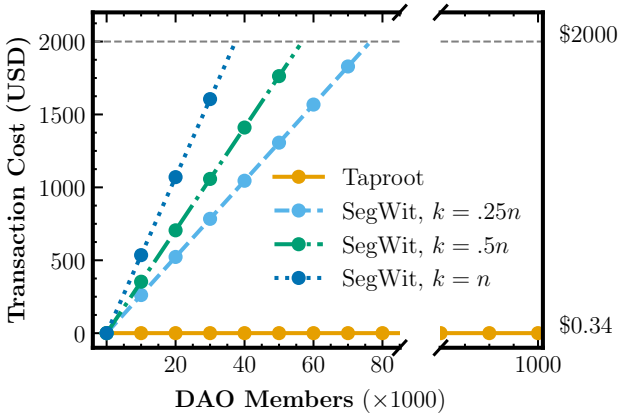

Figure 4: Transaction costs for governance decisions using the Bitcoin blockchain.

present in the treasury of the organisation. After this step, the organisation distributed the whole amount to the personal addresses of the investors as a paid-out interest.

This experiment showcases the usability of the main functionalities required for a functional organisation. Furthermore, it showcases the viability of making investments for common goals without any form of intermediaries or governing bodies. A direct investment was made into an artist's organisation, which is formed in a completely trustless network. We believe that our disruptive Web3 system is able to replace existing industries in a fully released setting. However, we encourage further experimentations to be able to draw definitive conclusions.

6.2 Cost of Governance Model

As discussed previously, the DAO treasury is implemented using Taproot [12]. This provides the solution with a considerable benefit versus multi-signature protocols using SegWit addresses [11]: Taproot addresses allow for multi-signature transactions through a single combined public key and aggregated signature. As a consequence, transaction costs do not grow with respect to the number of participants. Figure 4 showcases the cost associated with governance processes within DAOs, for both SegWit and Taproot addresses. The parameter k represents the number of signers in a k-of-n multi-signature wallet. The cost is based on a transaction fee of 10 Satoshi (with an exchange rate of 0.0002 USD) per vByte.

We find that for a DAO using SegWit, the used threshold has a direct impact on the number of members a DAO can have. The maximum block size of Bitcoin limits scalability. For instance, a DAO using a threshold of 50% for transactions is limited to around 56,000 members, assuming a single input and output per transaction. Regardless, the cost grows to 2,000 USD, as any transaction containing more signatures or signers exceeds the maximum block size.

These results show that modern Bitcoin Taproot is a necessary requirement for scalability, as the older SegWit does not scale. Our unstoppable DAO can achieve 1 million members with acceptable governance costs. Significant engineering effort remains to achieve

the order of magnitude of Big Tech with *billions* of users. The challenge is signature aggregation, which takes minutes or hours at this scale.

7 RELATED WORK

The field of Decentralised Autonomous Organisations is a relatively new research area. It has, however, been extensively explored in academia, and variations have been established in practice. DAOs such as Uniswap [1], Aave [8], or MakerDAO [7] have market capitalisations of billions of USD. However, the number of proposed ecosystems capable of creating DAOs is limited.

Aragon [2] allows the creation of a DAO using its templates. Aragon does not force any form of governance on their infrastructure and has a modular approach using smart contracts. DAOstack [5] is another Ethereum-based DAO infrastructure. However, while Aragon focuses on modularity, DAOstack focuses on the decision-making aspect through its unique holographic consensus mechanism. Colony [15] is a DAO framework that allows DAOs to be split up into specific purposes. These purposes are translated into tasks, which allow members to gain influence within the communities. As a consequence, power is divided among those that perform work within the community. DAOhaus [4] is a platform that allows the creation of DAOs with a special voting mechanism. In a DAO of this platform, proposers must pledge a certain amount of tokens and influence. Influence is a special currency held by members of such a community. In case any participant opposes the outcome of a proposal, they have the ability to *rage quit*, allowing them to opt out from the DAO.

All aforementioned platforms function on the Ethereum blockchain. Whilst this guarantees high availability, it also introduces a vast amount of overhead as each decision must reach a global consensus to be validated, while our system's outputs are only added to personal ledgers, greatly reducing the amount of processing power required. Furthermore, all previous works except Colony are relatively static solutions that do not allow much flexibility in terms of modularity or decision-making within the communities.

8 CONCLUSION

We provided a set of architectural principles that we identify as necessary for creating a truly decentralised Web3 infrastructure for Decentralised Autonomous Organisations, labelled *extreme decentralisation*. Our Extreme Decentralisation DAOs implement these principles, allowing any party to create a DAO without hindrance by central authorities or single points of failure. Participants establish communication channels independently and operate in an egalitarian permissionless network. As a result, we deem our DAOs to be as unstoppable as Bitcoin and BitTorrent in practice.

We created a functional prototype implementation for smartphones. This implementation was used to demonstrate our work by focusing on the music industry. Our experiment shows the possibility of direct artist investments through collective fund management, replacing all intermediary parties within the existing music industry.

Governance is shown to function through democratic decision-making. Anyone is able to create a DAO in our ecosystem, assign their own rules and make investments without regulation. Further external experiments are required independently of our work, however, we believe to have taken a great step towards disrupting current industries with unstoppable Web3 technology.

ACKNOWLEDGMENTS

This work was funded by NWO/TKI grant BLOCK.2019.004.

REFERENCES

[1] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. 2021. *Uniswap v3 core.* Technical Report. Uniswap Labs.
[2] Aragon Association. 2022. Aragon. https://aragon.org
[3] Rowdy Chotkan, Jérémie Decouchant, and Johan Pouwelse. 2022. Distributed Attestation Revocation in Self-Sovereign Identity. In *2022 IEEE 47th Conference on Local Computer Networks (LCN).* 414–421. https://doi.org/10.1109/LCN53696.2022.9843323
[4] DAOhaus. 2022. DAOhaus. https://daohaus.club
[5] DAOstack. 2018. *DAOstack: An Operating System for Collective Intelligence.* Technical Report. DAOstack.
[6] John R. Douceur. 2002. The Sybil Attack. In *Peer-to-Peer Systems*, Peter Druschel, Frans Kaashoek, and Antony Rowstron (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 251–260.
[7] Maker Foundation. 2020. *The Maker Protocol: MakerDAO's Mulfi-Collateral Dai (MCD) System.* Technical Report. Maker Foundation.
[8] Emilio Frangella and Lasse Herskind. 2022. *Aave V3 Technical Paper.* Technical Report. Aave. https://github.com/aave/aave-v3-core/blob/master/techpaper/Aave_V3_Technical_Paper.pdf
[9] Samer Hassan and Primavera De Filippi. 2021. Decentralized autonomous organization. *Internet Policy Review* 10, 2 (2021), 1–10.
[10] Yutaka Kurihara and Akio Fukushima. 2017. The market efficiency of Bitcoin: a weekly anomaly perspective. *Journal of Applied Finance and Banking* 7, 3 (2017), 57.
[11] Eric Lombrozo, Johnson Lau, and Pieter Wuille. 2015. BIP 141: Segregated Witness (Consensus layer). https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki
[12] Gregory Maxwell. 2018. Taproot: Privacy preserving switchable scripting. *Bitcoin development mailing list. Jan* 23 (2018), 98.
[13] Pim Otte, Martijn de Vos, and Johan Pouwelse. 2020. TrustChain: A Sybil-resistant scalable blockchain. *Future Generation Computer Systems* 107 (2020), 770–780.
[14] Johan Pouwelse. 2020. Towards the Science of Essential Decentralised Infrastructures. In *Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good* (Delft, Netherlands) *(DICG'20).* Association for Computing Machinery, New York, NY, USA, 1–6.
[15] Alex Rea, Aron Fischer, and Jack du Rose. 2018. *COLONY: Technical White Paper.* Technical Report. Colony Foundation Ltd. https://colony.io/whitepaper.pdf
[16] Richard Rogers. 2020. Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication* 35, 3 (2020), 213–229.
[17] Alexander Schaub, Rémi Bazin, Omar Hasan, and Lionel Brunie. 2016. A Trustless Privacy-Preserving Reputation System. In *ICT Systems Security and Privacy Protection*, Jaap-Henk Hoepman and Stefan Katzenbeisser (Eds.). Springer International Publishing, Cham, 398–411.
[18] Claus-Peter Schnorr. 1991. Efficient signature generation by smart cards. *Journal of cryptology* 4, 3 (1991), 161–174.
[19] Balaji S. Srinivasan and Lee Leland. 2017. Quantifying Decentralization. https://news.earn.com/quantifying-decentralization-e39db233c28e
[20] Quinten Stokkink and Johan Pouwelse. 2018. Deployment of a Blockchain-Based Self-Sovereign Identity. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).* 1336–1342. https://doi.org/10.1109/Cybermatics_2018.2018.00230
[21] Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. 2021. SoK: Decentralized Finance (DeFi). https://arxiv.org/abs/2101.08778
[22] Eric Glen Weyl, Puja Ohlhaver, and Vitalik Buterin. 2022. Decentralized society: Finding web3's soul. *SSRN Electronic Journal* (2022).