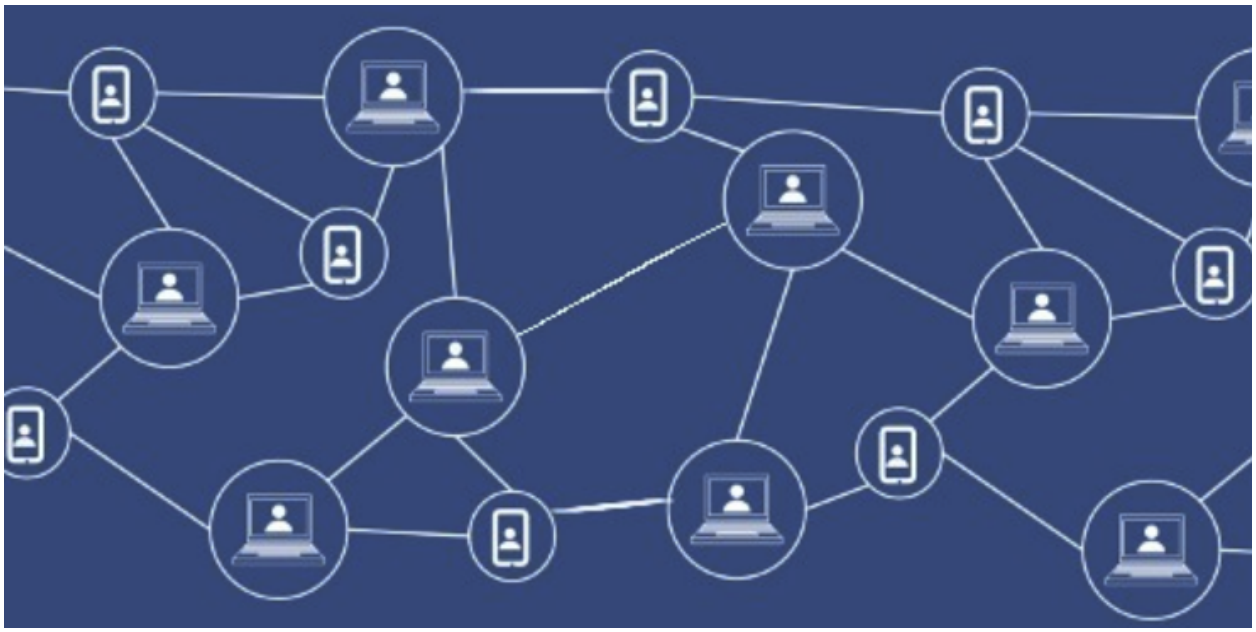
User privacy in DAOs

DAO analysis



Ignas Apšega

3620557

Version Control

Version	Date of change	Change description
0.1	18-09-2022	Start of the research about DAOs
0.2	11.10.2022	Started the research about DAO tooling
0.3	26-10-2022	Initial draft
0.4	27-10-2022	Added research based on research questions, strategies, and methods
0.5	28-10-2022	DAO tooling research added
0.6	29-10-2022	Added table of contents and fixed formatting
0.7	30-10-2022	Fixed research strategies
0.8	31-10-2022	Improved grammar
0.9	09-11-2022	1. Made main research question more explicit. 2. Fixed research methodologies. 3. Better explanation in: “3.4 is privacy really a problem within DAOs?” “3.5 What kind of data can be hidden to improve user experience in DAOs?” 3.6 What tools are there for improving privacy for DAOs? a) Added criteria of how these tools were researched 4. Added Advice section
1.0	21-11-2022	Decision Matrix for DAO tooling research
1.1	15-12-2022	1. Added Validator in the glossary. 2. More context and description on the Research Matrix of DAO tooling. 3. More explicit advice.
1.2	02-02-2023	1. Added some background on why 38% of blockchains projects are discontinued

1.3	22-02-2023	1. Added 2.2 Research Context (Page 11) 2. Added more context and articles for a. 3.3 What are the main activities in DAO people participate in? (Page 20) b. 3.4 Is privacy really a problem within DAOs? (Page 22) c. 3.5 What kind of data should be hidden for common actions of users in the DAOs? (Page 24) 3. Added knockout criteria for 3.6 What tools are there for improving user privacy in DAOs? (Page 25) 4. Added research matrix for 3.7 What techniques are there for improving the user privacy of DAOs? (Page 27) 5. New Conclusion
1.4	27-02-2023	1. Added more context about the questionnaire (Page 18, 19 and 20) 2. A conclusion after DAO tooling linking to techniques (Page 23) 3. Explicit conclusions for ZKP PoC (Page 24 and 25)

Table of Contents

1. Introduction

1.1 Purpose of the document

This document is part of the User Privacy in DAOs[1] research assignment. This document aims to showcase the research done on DAOs and their privacy problems and possible tooling to solve these problems.

1.2 Context

Tooling for DAOs is in active development. New improvements and solutions are introduced regularly. One of the main DAO features is that they want to be completely transparent. However, the members of the DAO may also want to stay anonymous and still be a part of this organization. In the DAOs, transparency comes from using smart contracts[2] on a blockchain[3].

The smart contracts are programmed in code that helps execute operations automatically when a set of criteria are met. While Ethereum[4] was the first blockchain to use smart contracts, nowadays, they are deployed on various other blockchains. Many blockchain networks operate as public databases, meaning anyone with an Internet connection can view a list of the network's transaction history, including smart contracts. This leads to the issue of low privacy because DAOs operate with these smart contracts that are public on the particular blockchain.

2. Research

2.1 Research Questions

The main research question for this document is -

“What are the best solutions to hide the data of DAO users for their most common actions?”

To answer this research question correctly, sub-questions must be derived from it:

- **What is a DAO?**
- **How do DAOs operate?**
- **What are the main activities in DAO people participate in?**
- **Is privacy really a problem within DAOs?**
- **What kind of data should be hidden for common actions of users in the DAOs?**
- **What tools are there for improving user privacy in DAOs?**
- **What techniques are there for improving the user privacy of DAOs?**

2.2 Research Context

Before starting with the research more context on the research questions has to be given:

What is a DAO?

To be able to research and answer the main research question. We have to understand what is a DAO. Thus, this question.

How do DAOs operate?

To have an even better understanding of what DAOs are. It is necessary to know how it operates. This will help underline the possible privacy problems of a user.

What are the main activities in DAO people participate in?

Researching this question helps us to identify which activities and actions a DAO user participates in. Thus, we would know what kind of privacy problems we might encounter.

Is privacy really a problem within DAOs?

It is important to double-check this and find facts proving the hypothesis.

What kind of data should be hidden for common actions of users in the DAOs?

To scope down the research and development it is required to know which data should be hidden from the user. By doing this, we will figure out what data we should hide in the Proof of Concept, thus having better time management for it.

What tools are there for improving user privacy in DAOs?

It is essential to check the available privacy tooling for DAOs. This will help to see if a solution already exists and if it does not we can still be inspired by current tooling. In addition, it should give a better overview of how DAOs operate.

What techniques are there for improving the user privacy of DAOs?

If there is no out-of-shelf tooling. We can check if there are techniques to bring privacy to the users such as libraries, plugins, programming languages, or blockchains.

2.3 Research strategy

For this research, mainly the strategies **Library** and **Field** were chosen. **Library** is done to explore what is already done and what guidelines and theories exist that could help. **Field** research is done to explore the application context

2.4 Research methods

Problem analysis

For **Field** research, mainly Problem analysis was chosen

Problem analysis - Before implementing solutions, an in-depth analysis of a problem has to be conducted. This research methodology was chosen to come up with the right research questions for the problem.

Interview

Interview - A questionnaire was made to understand the possible pain points of DAO users.

Library's research strategy has multiple research methods. But not all of them were used to conduct this research.

Available product analysis was used to answer most of the research questions. This research method helps to find what has already been done. This means already existing DAOs were researched, including how they operate.

Available product analysis

Literature study was used to research online literature to understand what DAO is, how it operates, and if it has any privacy problems.

Literature study

Research methodology	Research question
Field - Problem analysis, Interview	• What are the best solutions to hide the data of DAO users for their most common actions? • What is a DAO? • How do DAOs operate? • What are the main activities in DAO people participate in? • Is privacy really a problem within DAOs? • What kind of data should be hidden for common actions of users in the DAOs? • What tools are there for improving user privacy in DAOs? • What techniques are there for improving the user privacy of DAOs?
Library - Available product analysis, Literature study	• What is a DAO? • How do DAOs operate? • What are the main activities in DAO people participate in? • Is privacy really a problem within DAOs? • What kind of data should be hidden for common actions of users in the DAOs? • What tools are there for improving user privacy in DAOs? • What techniques are there for improving the user privacy of DAOs?

3. Research Results

3.1 What is a DAO?

After researching this question, the following results were found:

Firstly, to fully understand what Decentralized Autonomous Organization (DAO) is, we have to translate the acronym DAO:

- Decentralized - It means no central leadership.
- Autonomous - It is governed by smart contracts.
- Organization - It is a vehicle for agent coordination.

In short, DAO is a decentralized autonomous organization, a type of structure with no central authority. A DAO usually has its tokens[6] which members can own. Members of the DAO can vote for initiatives. There are multiple ways to measure vote weight, but most commonly, it is typically measured by the amount of DAO tokens a member holds. The backbone of a DAO is its smart contracts, which define the organization's rules and holds the group's treasury.

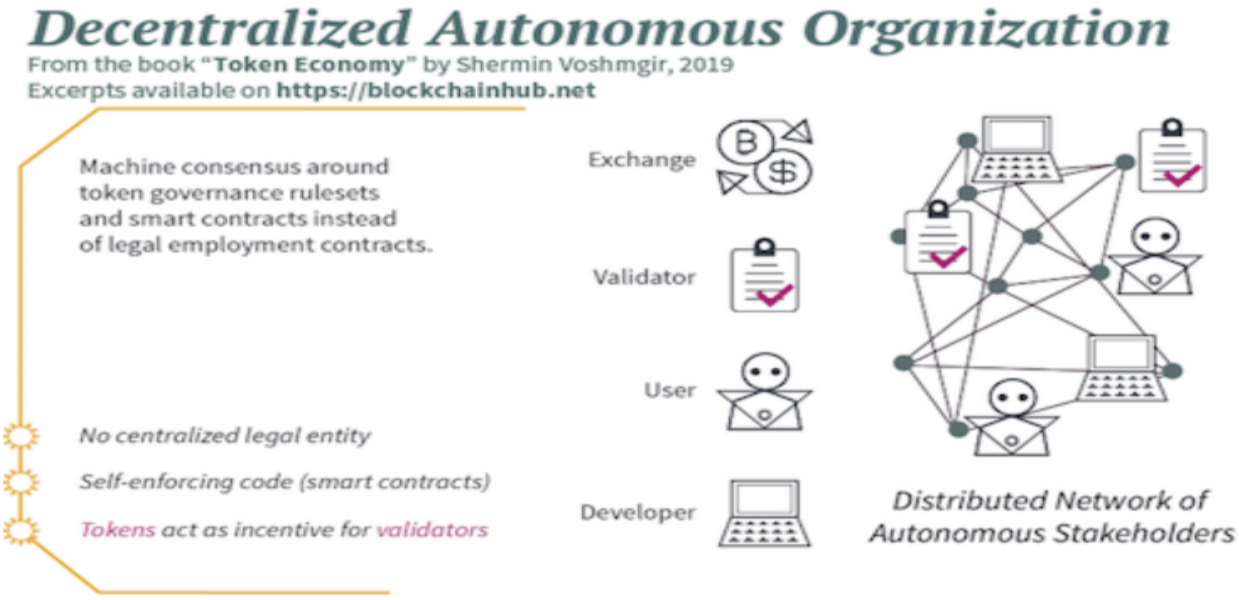


Figure 2. Decentralized Autonomous Organization (DAO). Source: [BlockchainHub]

Characteristics of a DAO:

- **DAOs are founded on a shared goal -** people with the same incentives gather to make a DAO.
- **Multi-sig Wallet** - is a digital wallet that operates with multi-signature addresses. This means that it requires more than one private key to sign and authorize a crypto transaction, or, in some cases, several different keys can be used to generate a signature.
- **Built-in treasury** - DAOs have raised funds - treasury. For example, during the initial stage, DAO can raise X amount of Bitcoin, which then can be used to pay the developers/workers in DAO. The treasury has to be governed.
- **Bottom-up governance -**
    - Democratic approach.
    - Willingness to solve problems.
    - Active collaboration.
    - An autonomy of collaborators in their choice of tools and how they organize themselves.
- **Trustless** - you don't have to trust a third party: a bank, a person, or any intermediary that could operate between you and your cryptocurrency transactions or holdings.
- **Membership via tokens[6]/NFT's[7]** - for example, if you have the most tokens, you have the biggest weight in votes/ if you do the most work, you will be rewarded. If you buy the NFT, you can join DAO.
- **DAO rules are hard-coded** - with the help of smart contracts.
- **Transparent** - you can see how DAO is set up and on what rules it is built on
- **Highly participatory** - DAOs are designed to allow/encourage you to participate. The more you participate, the more you are rewarded.
- **Decisions made via proposals** - for example, a proposal to spend some treasury funds to buy or do something.
- **Any stakeholder can propose an idea -** anyone who got into a DAO can propose any idea they have.
- **Members incentives aligned** - it would not be in your interest to act against it because you are a stakeholder in the DAO.
- **Can not be shut down (kind of)** - the code is set, up and running, and doing its thing. Unless you want to.

Types of DAO:

- **Grants DAOs** - Communities donate funds and use a DAO to vote on how that capital is allocated to various contributors in the form of governance proposals.
- **Protocol DAOs** - provided a framework for any network to issue a token that was owned and operated by its community.
- **Investment DAOs** - allow members to pool capital and invest in projects at their earliest stages.
- **Service DAOs** - from legal to creative, governance to marketing, development to treasury management, Service DAOs create funnels to contract web3[8] mercenaries.
- **Social DAOs** - focus on social capital over financial capital. Social DAOs are the natural evolution of group chats, where friends become co-workers.
- **Collector DAOs** - seek to curate which NFTs have long-term value.
- **Media DAOs** - share an outlet's open agenda to spread awareness and news.

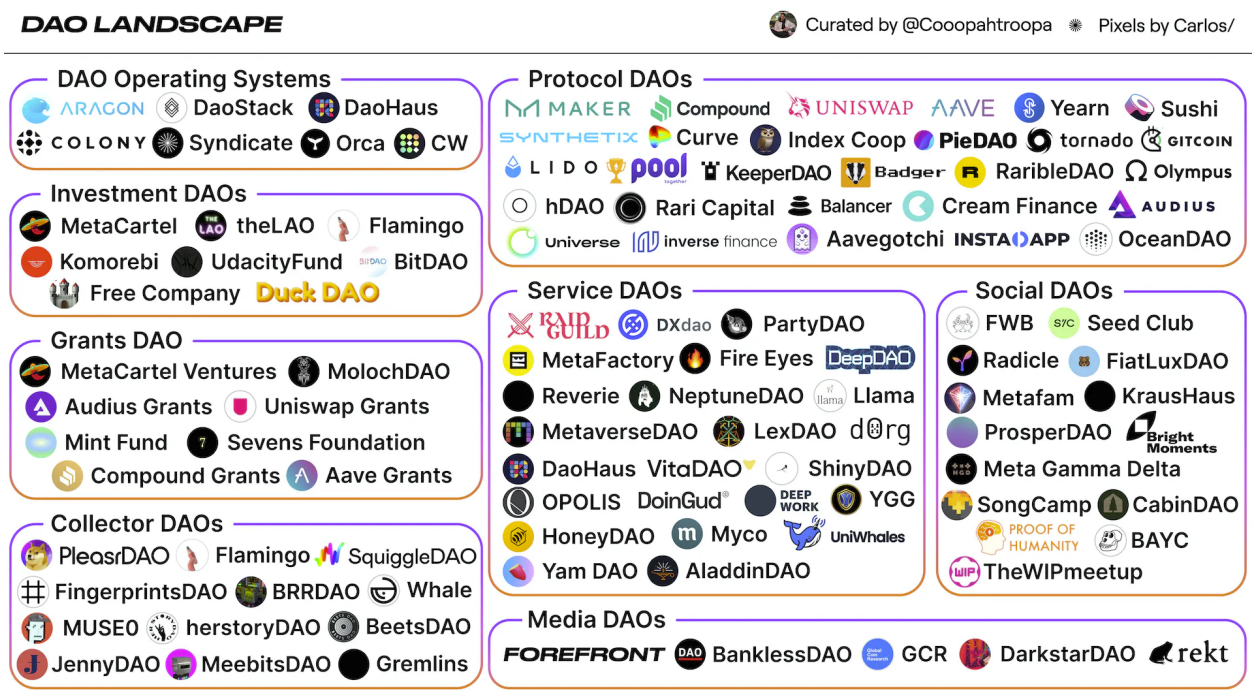


Figure 3. DAO Landscape. Source: [@CoopahTroopa]

3.2 How do DAOs operate?

To have a better understanding of What a DAO is. We have to understand how it operates

Principal/Agent Dilemma

Like any other organization, DAOs operate on principal and agent theory. It means that the principal-agent problem is also applicable. The problem refers to the conflict in interests and priorities that appears when one person or entity (the "agent") takes action on behalf of another person or entity (the "principal"). The problem worsens when there is a greater difference in interests and information between the principal and agent.

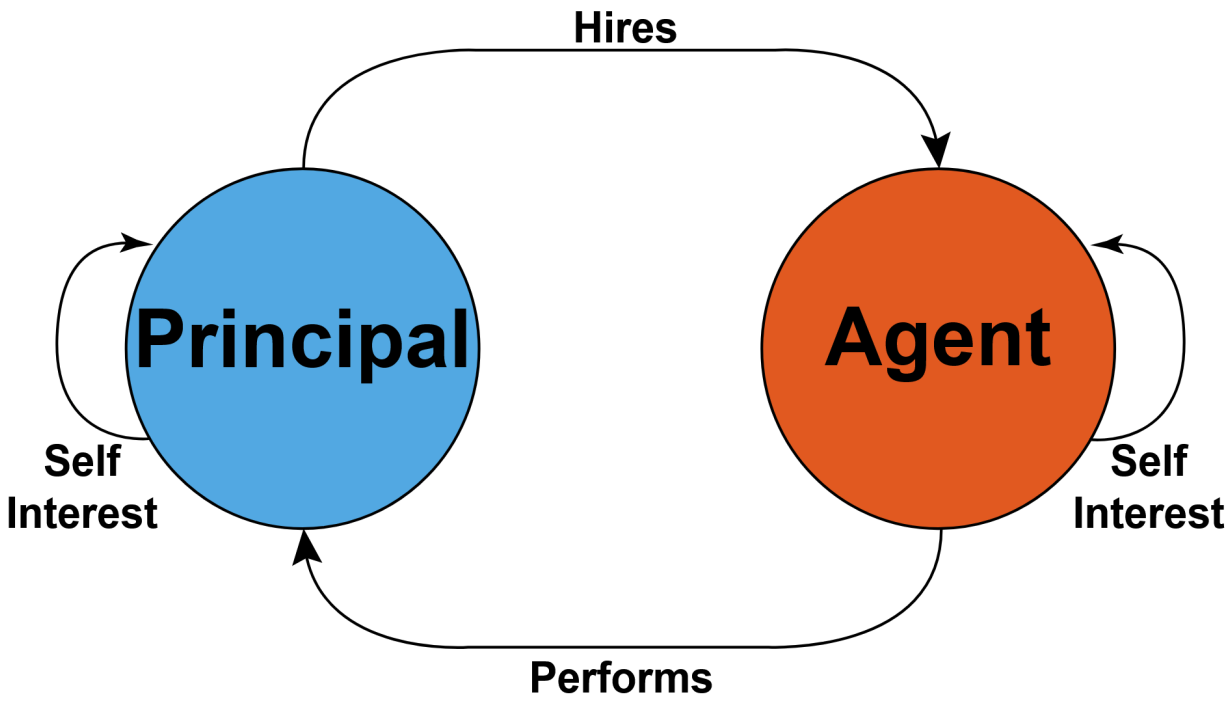


Figure 4. Principal-agent problem. Source: Wikipedia

DAOs solve this problem - they completely decentralize everything, and they remove that hierarchy and turn it into something completely different.

Participation in DAOs

This is a list of how people can participate in the DAOs:

- **Aligned incentives** - people join a particular DAO because they have a particular incentive
- **Verification via Collab.land[9]** - a tool to verify a member
- **Stake in DAO via tokens** - e.g., you might need to stake a specific amount of tokens to become a member. This number might rise each year.
- **Vote on proposals using Snapshot[10] -** is a decentralized governance platform that makes it easy to create and vote on proposals
- **Get rewarded (usually in tokens)** - if you participate, add value or do a task
- **More value you create, the more value you earn**.

Roles in the DAOs

There are many roles in the DAOs, but these are the most common:

- **Developer** - create code for the DAO. For example, improve smart contracts or build a tool that will be used internally.
- **Community Moderator** - Involves with dealing with information that is announced, dealing with spammers.
- **Create Content** - these people can write medium articles, create videos and etc.
- **Design Graphics** - can design websites, graphics for Content Creators, and overall make the DAO look good.
- **Website** - these people could create a DAO website and forum
- **Administration** - managing documents, keys, and flow of information from one place to another.
- **Treasury Manager -** to manage the funds of DAO.
- **Specialised DAO roles** - (i.e., legal, artist liaison, technical).

Ways of earning in the DAOs

There are many ways to earn in the DAOs. Usually, it is done via rewards. Rewards can mean various things, e.g., “pay for eligible work”. Pay means rewards in the form of liquid ownership. In other words, rewards should:

- **Liquid**: Be useful for rent and food

These rewards could be earned through methods such as

- **Full-time hire** - for example, AragonDAO has full-time positions such as Event Manager, People Operations Manager, and Senior Front-end Developer.
- **Grants** - apply for a grant to do a specific task that a DAO needs.
- **Bounties** - find bugs in the code.
- **Gigs** - make a small gig: website, video.

3.3 What are the main activities in DAO people participate in?

According to **Library** research, and articles -
“Decentralized Autonomous Organization (DAO): Definition, Purpose, and Example”

“Top Decentralized Autonomous Organization (DAO) Use Cases & Examples”

There are quite a few activities to do in the DAOs. However, the main activities in the DAOs are:

- **Making a proposal** - for example, SushiSwap[11] - a decentralized crypto exchange, had a proposal for electing - a “Sushi Head Chef”. Another example that happened was at Uniswap[12]. A proposal asked if Uniswap v3 should be deployed to another blockchain - Polygon.
- **Voting -** another very important activity of a user in the DAOs. Users can vote on the proposals, for example, with a simple - “yes or no”
- **Governance of treasury-** this activity is done with the help of smart contracts working on the blockchain. People usually vote on what could be done with the treasury or who could receive some of it as a reward/salary.

- **Communication -** the most common activity and one of the most important activities in the DAOs. People must communicate with each other and form small teams to work towards rewards and incentives. Usually, DAO communication and coordination are done via tools such as Discord[13] and Snapshot.

Worth to mention that most of these activities are on-chain[14]. Meaning that it is public for everyone to see what is happening within DAO, thus bringing some privacy problems

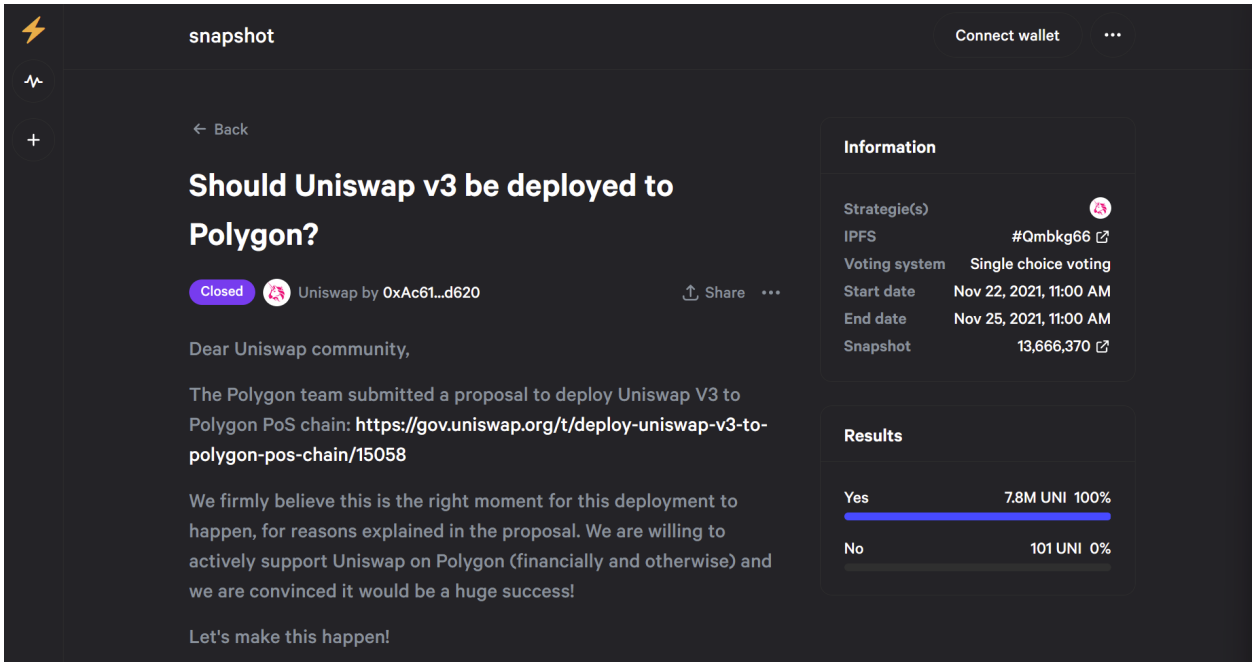


Figure 5. Proposal and Voting of Uniswap on Snapshot. Source: Snapshot

3.4 Is privacy really a problem within DAOs?

According to Teck Ming's research in 2019 - 38% of confidentiality and privacy, concerns are the reason some of the blockchain projects are discontinued. The report also revealed that the vast majority of blockchain experiments, proofs-of-concept, and trials do not pass to the next stage. While project launches are generally announced with great fanfare, including press releases, blog posts, and news articles, many end up being quietly abandoned with little to no public acknowledgment. Nonetheless, DAOs are still using blockchain for common actions which brings privacy issues. (Teck Ming (Terence) Tan, 2019, Jan 13, *Enterprise Blockchain: Permissioned Blockchain Current State of Adoption and Revenue Models,* https://www.oulu.fi/en/blogs/oulu-business-school/2019-enterprise-blockchain-permissioned-blockchain-current-state-adoption-and-revenue-models)

DAOs force absolute transparency. As mentioned before, more and more DAOs are going fully on-chain, meaning organizations' decisions and work are recorded on the blockchain. This presents many issues, such as off-chain coercion, problems with internal governance, and difficulties finding talent and bringing innovation. (Book 2022; “DAO Nation — Clay”).

- Firstly, without an anonymous voting process, individual stakeholders are at risk because malicious people can pursue stakeholders to influence their decisions, which may disrupt DAO and stakeholder interests. Without the ability to anonymize the voting, those malicious people can target individual stakeholders to influence decisions normally reserved for direct stakeholders, thus disrupting the typical alignment between DAO and stakeholder interests. This could be prevented if people could be anonymous - e.g., preventing them from being searched and found via real name and location. Moreover, a free and fair election aims to ensure that voters are not discriminated against. Yet, in the blockchain-based voting system, all the votes are public and can easily be tied back to a particular address - the user. This style of voting opens problems such as collusion and discrimination.
- Secondly, DAOs can face an unnecessarily limited talent pool for hiring if there are no flexible privacy options. It is because not every worker in the space prefers to have salary negotiations and salary flow publicly and transparently. In the early times of DAOs, it was popular to be a pseudo-anonymous worker, but it is unlikely that this will remain normal in the medium to long term.

- Thirdly, DAOs are at risk of discouraging innovation and experimentation by their developers. It is because the ability to recognize individual contributors on the blockchain is not an uncommon practice that may lead to unwanted individual consequences for work done by a developer in a particular DAO. This may discourage developers from doing risk-taking solutions that usually lead to technological breakthroughs in the space. For example, a new innovative blockchain emerges with the help of DAO stakeholders and their funding. However, if this new blockchain tends to be vulnerable and people start losing money, the first people to be blamed will be developers who tried to make something new and innovate the space, but with an element of privacy, this could be avoided.

Furthermore, a survey was conducted to investigate the level of privacy that users of DAOs have. This survey was supplied to the users of DAOs. The hypothesis was that DAO users lack privacy, and the purpose of the questionnaire was to confirm this theory. Although the sample size of respondents was small, the results of the survey suggest that user privacy within DAOs is a significant issue. The questionnaire revealed that many users feel that their personal information is not adequately protected. This raises important questions about the need for enhanced privacy measures within DAOs to ensure that user's sensitive information is adequately protected.

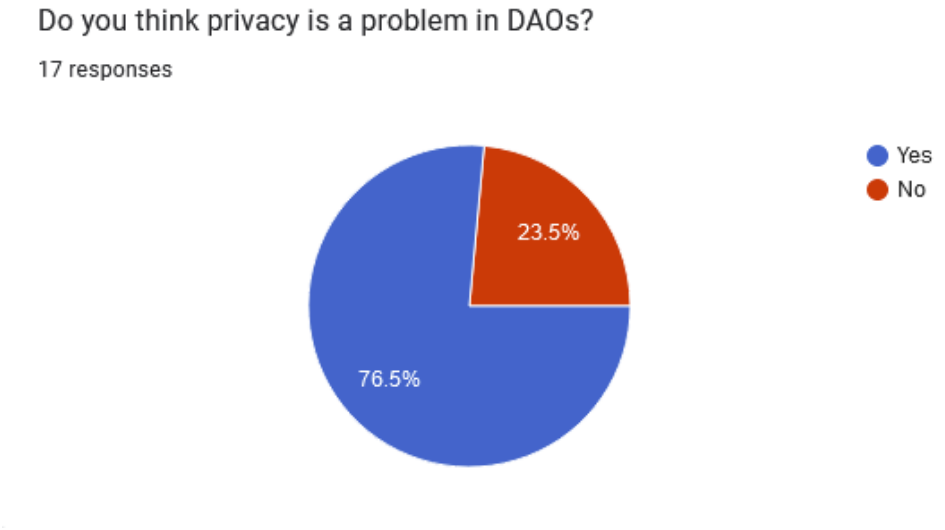


Figure 6. Online questionnaire: Is privacy a problem in DAOs?

According to the survey on user privacy in DAOs, the most common problem faced by users is discrimination. The transparency of user activities within DAOs, such as proposal issuers, voters, and received rewards, can lead to discriminatory practices and off-chain coercion.

The survey suggests that user privacy is crucial to ensuring fair and democratic decision-making within DAOs. By addressing privacy concerns, such as the protection of user identities and voting records, DAOs can promote inclusivity and diversity among their user base, leading to a more equitable and sustainable ecosystem.

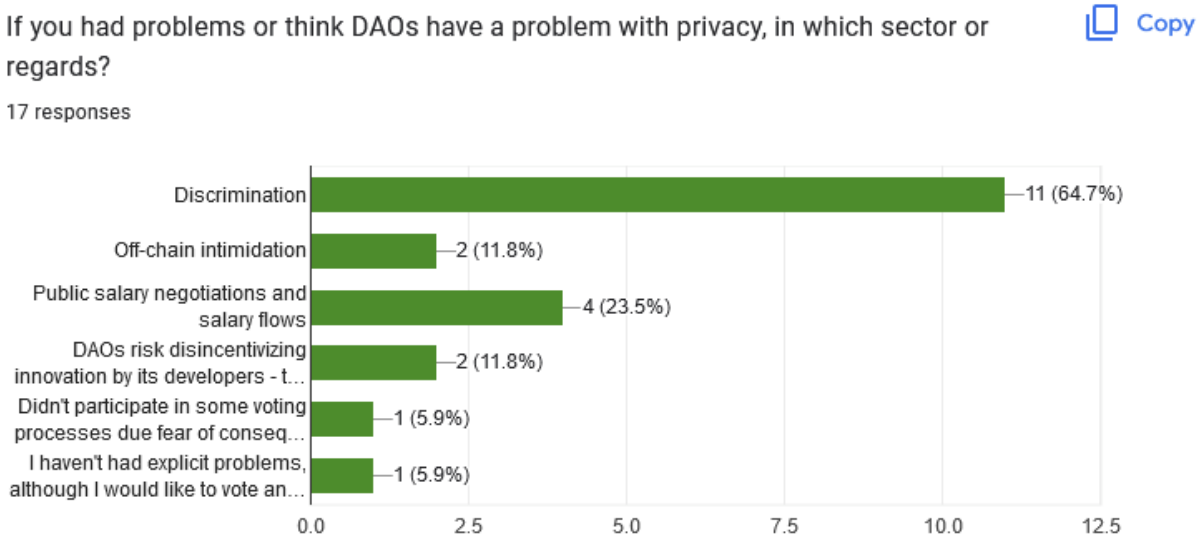


Figure 7. Online questionnaire: Is privacy a problem in DAOs?

3.5 What kind of data should be hidden for common actions of users in the DAOs?

This overlaps with the most common actions of users in DAOS. Ideally, it would be best if there was a possibility to hide most of the user data, which may include:

- The proposal issuers - to avoid discrimination and off-chain coercion.
- The people who vote for and against - to avoid discrimination and off-chain coercion.
- The received rewards and salaries - to attract developers and contributors to join DAO knowing that their salary inflows will be hidden from the entire public.
- Users' crypto wallet addresses - it would be nice to hide sender and receiver addresses from the public.

The survey on user privacy in DAOs revealed that the most common action within DAOs is voting, which raises concerns about user privacy. The transparency of voting records can lead to discriminatory practices and off-chain coercion. To address this issue, the survey suggests that voting records should be kept private to protect user identities and prevent the manipulation of voting outcomes.

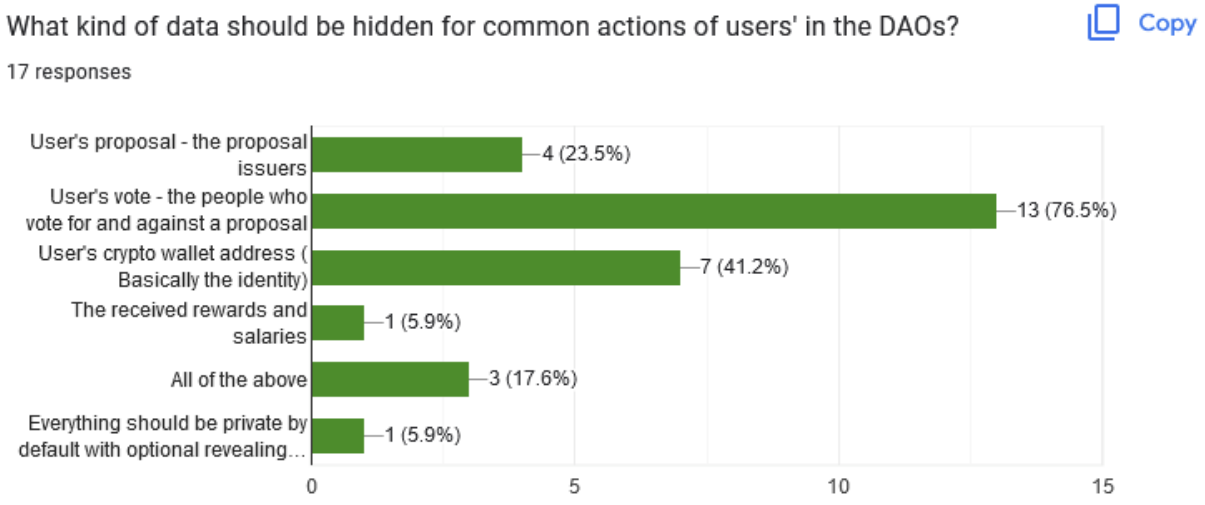


Figure 8. Online questionnaire: What kind of data should be hidden for common actions of users in the DAOs?

3.6 What tools are there for improving user privacy in DAOs?

To start with, criteria have to be defined on how DAO tools were researched. Mainly, it was looked into if the tools hide ***the users' voting in the DAOs***:

To continue, there are many tools for DAOs. In-depth research was done to find out if these tools help with privacy. In addition, it should give a better overview of how DAOs operate. This is the list of DAO tools researched:

- Aut - Expandable Community protocol, powering the next level of collective coordination in DAOs. It does so by adding Role-based Membership & Governance in Web3 Communities.
- Parcel - Treasury management to easily track and send payments.
- Utopia - Collaborative payroll and expense management for DAOs.
- Clarity - This is the most advanced DAO contribution platform. Share task boards & docs, manage access with tokens, receive bounty payouts, and build your contributor reputation.
- Snapshot - Off-chain voting platform for easy token-based governance.
- Coordinape - Coordination game to determine which contributors(s) deserve token rewards.
- SourceCred - Tracks community participation and rewards active members.
- Tally - Governance dashboard to track on-chain voting history across different protocols.
- Boardroom - Governance hub for token holder management to empower key decision-making.
- Sybil - Create and track on-chain governance delegation.

Research Matrix of DAO tooling

DAO tooling matrix was made with the idea to see if any of these tools could help with the privacy issue of ***users' voting in the DAOs***. In addition, it is good to check if the tooling has some sort of Identity feature because it could bring privacy.

Tool	Identity feature	Has voting mechanism	Knockout criteria
Aut	Non-Transferable NFT ID	+	**No Anonymous Voting**
Parcel	Your wallet address	+	**No Anonymous Voting**
Utopia	Your wallet address and first name, last name	+	**No Anonymous Voting**
Clarity	Your wallet address and nickname	+	**No Anonymous Voting**
Snapshot	Your wallet address	+	**No Anonymous Voting**
Coordinape	Your wallet address	+	**No Anonymous Voting**
SourceCred	Your wallet address - other social medias also linked	+	**No Anonymous Voting**
Tally	Your wallet address	+	**No Anonymous Voting**
Boardroom	Your wallet address	+	**No Anonymous Voting**
Sybil	Your wallet address and Twitter	+	**No Anonymous Voting**

To conclude, while several tools are available to assist with coordination and communication in DAOs, **none of these tools are solely dedicated to safeguarding users' privacy.** Instead, users' identities remain highly visible, with their real names and wallet addresses linked together. This lack of privacy-focused tooling means that we must explore alternatives to bring privacy to the blockchain, as DAOs operate on the blockchains. If we do not have tooling for DAO privacy, it is up to us to build it using privacy techniques on the blockchain. This highlights **the pressing need for the development of privacy tools that are tailored to the unique needs of DAOs**, ensuring that users' personal information remains protected in these decentralized environments.

3.7 What techniques are there for improving the user privacy of DAOs?

With the increasing adoption of DAOs, there is also a growing concern regarding the privacy of users who participate in these organizations. Privacy is an essential aspect of any decentralized system, and DAOs are no exception. In this context, various techniques have been proposed for improving the user privacy of DAOs. These techniques include encryption, zero-knowledge proofs, multi-party computation, and more.

Research Matrix of privacy techniques

Technique	Description	Advantages	Disadvantages	Example Use Cases	Knockout Criteria
Zero-Knowledge Proofs (ZKPs)	A cryptographic protocol that allows a prover to demonstrate knowledge of a secret without revealing the secret itself.	Can be used to verify transactions or computations without revealing sensitive data.	ZKPs can be computationally expensive to generate and verify.	Verifying transactions, voting, and data sharing.	N/A
Differential Privacy	A technique used to protect the privacy of individuals in a dataset by adding random noise to	Can be used to protect the identity of users in voting records or to	Differential privacy can be computationally expensive and may require	Data analysis and sharing of sensitive data within a DAO.	Not enough research, documentation, and development.

	prevent individual data points from being identifiable.	anonymize data in transaction logs.	significant expertise to implement.		
Anonymous Credentials	A technique that allows individuals to prove certain attributes or properties about themselves without revealing their identity.	Can be used to protect the privacy of users while still enabling them to participate in voting or decision-making processes.	Anonymous credentials may require significant expertise to implement and may be vulnerable to certain attacks.	Voting, decision-making processes, and identity verification.	Not enough research, documentation, and development.
Ring Signatures	A type of digital signature that allows a user to sign a message on behalf of a group without revealing which member of the group actually signed the message.	Can be used to protect the privacy of users in voting or other decision-making processes.	Ring signatures may be vulnerable to certain attacks and may not provide as strong security as other techniques.	Voting and decision-making processes where anonymity is desired.	Not enough research, documentation, and development.

Based on the updated research matrix and the current state of the field, Zero-Knowledge Proofs (ZKPs). It seems that they offer the most promising solution for addressing the privacy concerns of users within DAOs. ZKPs have been gaining significant attention and adoption in recent years, particularly in the blockchain and cryptocurrency communities. This growing interest in ZKPs has led to a wealth of research, documentation, and development related to the technique, with many open-source libraries and frameworks available for implementing them. While ZKPs does have some limitations, such as computational overhead and dependence on trusted setup, their unique features make them an ideal candidate for further research and development. Their ability to verify transactions and computations without revealing sensitive data is particularly valuable in a decentralized context, where privacy and security are critical concerns. However, to assess the full potential of ZKPs, a proof of concept must be developed to demonstrate their practical implementation in DAOs. Such proof of concept will enable us to evaluate the feasibility of ZKPs for safeguarding user privacy within decentralized organizations and inform future research and development in this field.

Conclusion

In conclusion, DAOs operate through a transparent, democratic, and decentralized blockchain network, where decision-making and governance occur in a decentralized manner. However, privacy concerns have been raised regarding the activities of users within DAOs. Research has revealed that several user actions require privacy, including

- Proposal issuers
- Voters
- Received rewards, and salaries
- Users' crypto wallet addresses.

The transparency of these activities may lead to discrimination, off-chain coercion, and a lack of participation from users. Specifically, the questionnaire concluded that users' votes should be kept private to ensure fair and democratic decision-making within DAOs.

Unfortunately, none of the current DAO tools offer privacy protection for voting. However, the promising technique of Zero-Knowledge Proofs (ZKPs) can provide a solution to privacy issues in DAOs. ZKPs enable the verification of transactions and computations without revealing sensitive data, making them a promising technique for enhancing privacy in DAOs. Despite some potential drawbacks, such as computational overhead and dependence on trusted setups, ZKPs are gaining significant attention and adoption within the blockchain and cryptocurrency communities, with many open-source libraries and frameworks available for implementing them.

Given the lack of privacy tools available for DAOs, it is crucial to develop our own privacy solutions using ZKP. This would require a proof of concept to demonstrate the feasibility of implementing ZKPs in DAOs and evaluate their potential for enhancing user privacy. As the blockchain and DAO ecosystem continue to grow and evolve, it is essential to prioritize research and development of new techniques for improving user privacy and ensuring the continued success of DAOs.

Citation and References

1. “AnonyVote: A DAO Tooling Platform for Anonymous Voting With ZK.” *Harmony forum*, 11 March 2022, https://talk.harmony.one/t/anonyvote-a-dao-tooling-platform-for-anonymous-voting-with-zk/13810. Accessed 28 October 2022.
2. “Blockchain Facts: What Is It, How It Works, and How It Can Be Used.” *Investopedia*, https://www.investopedia.com/terms/b/blockchain.asp. Accessed 26 October 2022.
3. Book, Adrien. “Everything Wrong With DAOs |.” *cult by Honeypot*, 5 July 2022, https://cult.honeypot.io/reads/everything-wrong-with-daos/. Accessed 27 October 2022.
4. “Collab.Land.” *Welcome to Collab.Land*, https://collab.land/. Accessed 26 October 2022.
5. “DAO Nation — Clay.” *Clay*, 16 August 2021, https://clay.mirror.xyz/DwJ60O0R1IyRiPAZFBw4L05L3fd8PPxWnzDNedKtOas. Accessed 27 October 2022.
6. “Ethereum.” *Wikipedia*, https://en.wikipedia.org/wiki/Ethereum. Accessed 26 October 2022.
7. Frankenfield, Jake. “What Are Crypto Tokens, and How Do They Work?” *Investopedia*, 20 May 2022, https://www.investopedia.com/terms/c/crypto-token.asp. Accessed 26 10 2022.
8. “Introduction to dapps | ethereum.org.” *Ethereum.org*, https://ethereum.org/en/developers/docs/dapps/. Accessed 28 October 2022.

9. “On Chain Transactions (Cryptocurrency) Definition.” *Investopedia*, https://www.investopedia.com/terms/c/chain-transactions-cryptocurrency.asp. Accessed 26 October 2022.
10. Ouaddah, Aafaf. “Arithmetic Circuit.” *ScienceDirect*, 2019, https://www.sciencedirect.com/topics/engineering/arithmetic-circuit. Accessed 25 10 2022.
11. “Testnet.” *Wikipedia*, https://en.wikipedia.org/wiki/Testnet. Accessed 28 October 2022.
12. “Uniswap.” *Wikipedia*, https://en.wikipedia.org/wiki/Uniswap. Accessed 26 October 2022.
13. “Web3.” *Wikipedia*, https://en.wikipedia.org/wiki/Web3. Accessed 27 October 2022.
14. “Welcome to Snapshot!” *Home - snapshot*, https://docs.snapshot.org/. Accessed 26 October 2022.
15. “What are smart contracts on blockchain?” *IBM*, https://www.ibm.com/topics/smart-contracts. Accessed 26 October 2022.
16. “What is SushiSwap? (SUSHI).” *Kraken*, https://www.kraken.com/learn/what-is-sushiswap-sushi. Accessed 26 October 2022.
17. “Zero-knowledge proof.” *Wikipedia*, https://en.wikipedia.org/wiki/Zero-knowledge_proof. Accessed 27 October 2022.
18. “ZKU-Vote: Anonymous voting within DAO - zkDAO - Harmony Community Forum.” *Harmony forum*, 12 May 2022, https://talk.harmony.one/t/zku-vote-anonymous-voting-within-dao/18423. Accessed 28 October 2022.

Appendix

Term	Explanation
1. Decentralized Autonomous Organisation (DAO)	DAO, or Decentralised Autonomous Organisation, is an organization without any hierarchy among its members. A DAO also has a set of “rules” on how to manage its treasury (DAO’s money) and how to handle votings, which are essential for making decisions, and a DAO usually has its own Token (Cryptocurrency, in this case). All these aspects are described inside a DAO smart contract.
2. Smart Contract	Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met. (“What are smart contracts on the blockchain?”)
3. Blockchain	A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in a digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions.

	The innovation of a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. (“Blockchain Facts: What Is It, How It Works, and How It Can Be Used”)
4. Ethereum	Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform. Among cryptocurrencies, ether is second only to bitcoin in market capitalization. Ethereum was conceived in 2013 by programmer Vitalik Buterin (“Ethereum”)
5. The Development Oriented Triangulation (DOT)	The DOT framework can help to structure the research and communication about it. The Development Oriented Triangulation (DOT) framework consists of three levels: The "What" of your research (the domains), The "Why" of your research (the trade-offs), and The "How" of your research (the strategies and methods)
6. Token	A crypto token is a virtual currency token or a cryptocurrency denomination. It represents a tradable asset or utility that resides on its own blockchain and allows the holder to use it for investment or economic purposes. (Frankenfield)
7. Non-fungible token (NFT)	A unique digital identifier that cannot be copied, substituted, or subdivided, that is recorded in a blockchain, and that is used to certify authenticity and ownership. The ownership of an NFT is recorded in the blockchain and can be transferred by the owner, allowing NFTs to be sold and traded. NFTs can be created by anybody and require few or no coding skills to create. NFTs typically reference digital files such as photos, videos, and audio. Because NFTs are uniquely identifiable assets, they differ from cryptocurrencies, which are fungible.

8. WEB3	It is an idea for a new iteration of the World Wide Web that incorporates decentralization, blockchain technologies, and token-based economics. (“Web3”)
9. Collab.land	Collab. Land leverages the power of identity through cryptocurrency to create a social space unique to a specific network of humans. Once you add the bot to your Telegram group or Discord guild, it will manage your people for you. Depending on their token holdings, they will be allowed to join the community (“Collab.Land”)
10. Snapshot	It is a decentralized voting system. It provides flexibility on how voting power is calculated for a vote. Snapshot supports various voting types to cater to the needs of organizations. Creating proposals and voting on Snapshot is user-friendly and does not cost gas as the process is performed off-chain. (“Welcome to Snapshot!”)
11. SushiSwap	SushiSwap is a software running on Ethereum that seeks to incentivize a network of users to operate a platform where users can buy and sell crypto assets (“What is SushiSwap? (SUSHI)”)
12. Uniswap	Uniswap is a cryptocurrency exchange that uses a decentralized network protocol. Uniswap is also the name of the company that initially built the Uniswap protocol. The protocol facilitates automated transactions between cryptocurrency tokens on the Ethereum blockchain through the use of smart contracts. As of October 2020, Uniswap was estimated to be the largest decentralized exchange and the fourth-largest cryptocurrency exchange overall by daily trading volume. (“Uniswap”)
13. Discord	is an instant messaging social platform.

	Users can communicate with voice calls, video calls, text messaging, media, and files in private chats or as part of communities called "servers". A server is a collection of persistent chat rooms and voice channels that can be accessed via invite links.
14. On-chain	On-chain transactions refer to transactions that are recorded and verified on the blockchain. Off-chain transactions don't occur on the blockchain network but instead are transacted on another electronic system such as PayPal. (“On Chain Transactions (Cryptocurrency) Definition”)
15. Decentralized Application (dApp)	A decentralized application (dapp) is an application built on a decentralized network that combines a smart contract and a front-end user interface. On Ethereum, smart contracts are accessible and transparent – like open APIs – so your dapp can even include a smart contract that someone else has written. (“Introduction to dapps | ethereum.org”)
16. Testnet	In blockchain technology, a testnet is an instance of a blockchain powered by the same or a newer version of the underlying software to be used for testing and experimentation without risk to real funds or the main chain. (“Testnet”)
17. Mainnet	Mainnet is a term used to describe a working, fully-operational blockchain. A mainnet network has been fully deployed and is in production, like the Bitcoin and Ethereum blockchains. In a mainnet, cryptocurrency transactions are verified and recorded to the blockchain. In contrast to main nets, testnets aren’t ready for production or live use.
18. Zero-Knowledge Proofs (ZKP)	In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method

	by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information. ("Zero-knowledge proof")
19. Validator	It is a node in a proof-of-stake system responsible for storing data, processing transactions, and adding new blocks to the blockchain.