Decentralized Autonomous Organisations (DAOS) in the Metaverse: The Future of Extremist Organisation?

Julia Ebner

The transition from Web 2.0 to Web 3.0 is likely to leverage the latest technological advances including AI, machine learning and blockchain technology. This might not only bring about a new interplay of the physical, virtual and augmented reality but could also fundamentally change the ways in which corporate entities, social communities and political movements organise themselves.

Decentralisation is a key property of the Metaverse. Policies, legal contracts and financial transactions that were traditionally the domain of governments, courts and banks might be replaced with smart contracts and financial transactions in blockchain. Cryptocurrencies can be used as a new medium of exchange outside of established banking systems, while non-fungible token (NFT) might serve as unique digital identifiers to certify ownership and authenticity. Taken together, these new forms of self-governance could lead to the explosion of so-called Decentralized Autonomous Organisations (DAOs) in the Metaverse.

Decentralized Autonomous Organisations (DAOs) are digital entities that are collaboratively governed without central leadership and operate based on blockchain (Jentzsch, 2016). As such, DAOs allow internet users to establish their own organisational structures, which no longer require the involvement of a third party in financial transactions and rulemaking. DAOs allow online communities to simplify their transactions and use a community-based approach to establish rules (World Economic Forum, 2023). However, as this study will explore, they might also give rise to new threats emerging from decentralised extremist mobilisation, pose a risk to minority rights, challenge the rule of law, and disrupt institutions that are currently considered fundamental pillars of our democratic systems.

Research Aim and Methods

The aim of this chapter is to explore potential ways in which DAOs could be exploited by extremist and anti-democratic actors. To what extent are extremist movements incentivised and able to make use of such new forms of self-governance? What are the types of threats that might emerge from anti-democratic or anti-minority DAOs?

To make progress on these research questions, the chapter reviews existing literature and summarises the findings from expert interviews and digital ethnographic research. More specifically, qualitative interviews were carried out with two leading experts on DAOs, a manual review of roughly 350 existing DAOs was performed, and exploratory digital ethnographic research was carried out across the extremist fringe platforms Odysee, Bitchute and Gab as well as the encrypted apps Telegram and Discord.[1]

The chapter will first provide an overview of DAOs, their relationship with the Metaverse and current use cases. It will then assess potential areas of misuse before providing an outlook of future trends, including key challenges and opportunities, and ideas for future research areas.

DAOs and the Metaverse

The next iteration of the internet, the Metaverse, is inherently tied to decentralised forms of communication, collaboration and finance. The metaverse is built on blockchain technology. Researchers have pointed out that collective governance and decentralised finance will likely be a key characteristic of the Metaverse (Chao et al., 2022; Goldberg & Schär, 2023; Tole & Aisyahrani, 2023). Ownership over an asset or "a piece of land" in the Metaverse would be governed by NFTs (Laeeq, 2022).

The World Economic Forum described DAOs as "an experiment to reimagine how we connect, collaborate and create" (World Economic Forum, 2023, p. 27). DAOs operate differently from traditional organisations in their allocation of resources, coordination of activities and decision-making processes. Code-driven and community-oriented structures allow stakeholders to be directly involved in governance and operations via voting systems (World Economic Forum, 2023). Decentraland is the

1 All quoted and referenced primary source content was documented and archived in the form of screenshots and can be made available to fellow researchers upon request.

first large-scale virtual world based on the architecture and premises of a DAO. With the aim of distributing power among its participating users, it operates on the Ethereum blockchain. The "residents" of Decentraland can initiate policy updates based on decentralised voting systems that are embedded in Decentraland DAO governance structure (Goldberg & Schär, 2023, p. 3).

There is an active ongoing debate about the legal status of DAOs. Proponents of DAOs have argued that smart contracts are self-executing codes on blockchain that can operate independently of legal systems. They point to lower transaction costs and reduce the need for intermediaries. However, more skeptical commentators have suggested that DAOs should be owned and/or operated by humans (Jentzsch, 2016, Mondoh et al., 2022). A more detailed discussion of existing efforts to regulate DAOs can be found in the final section of this chapter.

To date, research into DAOs and the Metaverse remains scarce. However, in recent years there has been a notable rise in publications that investigate the trends and implications of DAOs for various sectors. For example, Chao et al. (2022) discuss the advantages and disadvantages of DAOs for non-profit organisations. While they argue that DAOs provide a "strong democratic system", they also caution that they "are not subject to legal, physical, or economic constraints" and are therefore capable of operating "outside the control of a single central authority or a single governing body" (Chao et al., 2022).

Mondoh et al. (2022) discuss whether DAOs might be the future of corporate governance, while Goldberg and Schär (2023) write that DAOs could disrupt the monopoly market structures in the technology sector. Their assessment is that "open standards and blockchain-based governance are a necessary but not a sufficient condition for a decentralized and neutral platform" (Goldberg & Schär, 2023). Meanwhile, Tole and Aiyahrani (2023) predict that the Metaverse and DAOs have the potential to revolutionise the education system. Through DAOs, they claim, "technology courses, certificates, and more can become automated and authenticated on the blockchain" (Tole & Aisyahrani, 2023, p. 1). DAOs could provide the basis for what they call "Metaversity", whereby the necessary infrastructure is provided for decentralised learning centers that have incentive structures and tailored courses in place (Tole & Aisyahrani, 2023, p. 3).

Most recently, computer scientists provided an in-depth analysis of the genesis and evolution of DAOs, as well as their classification and ethical implications (Amhaz et al., 2024). Another large-scale study published in 2024

argued that DAOs "resemble early online communities", in particular open-source projects. The authors assessed the impact of several DAO properties, including voting mechanisms, on levels of decentralization (Sharma et al., 2024). Moreover, the United Kingdom's Law Commission published a scoping paper on DAOs, discussing the legal characterization of DAOs, liability of participants as well as questions around financial regulation and tax (HM Law Commission, 2024).

Current Use of DAOs

The current DAO ecosystem is highly diverse and growing at a fast pace. By December 2024, DAOs collectively manage over 40 billion dollars and count more than 11 million token holders across at least 13,000 entities (DeepDAO, 2024). DAOs exist across a range of industries such as finance, philanthropy and politics. A manual review of the 356 DAOs listed on the website Decentralist.com at the time of the analysis (July 2023), illustrates the highly diverse nature and purpose of DAOs. The descriptions and stipulated mission statements include social, activist, investment, gaming, media and collector aims (Decentralist, 2023). Some DAOs are clearly satirical in nature, including the Café DAO which aims "to replace Starbucks", the Doge DAO which wants to "make the Doge meme the most recognizable piece of art in the world" and the Hair DAO, "a decentralised asset manager solving hair loss".

By 2023, DAOs have primarily attracted entrepreneurs, libertarians, activists, pranksters and hobbyists. However, there are also activist and political DAOs. For example, Decentralist.com lists DAOs that are tied to the climate movement and Black Lives Matter community as well as social justice and anti-banking DAOs that want to tackle social inequality. Figure 1 provides an overview of the most common DAOs found on Decentralist:

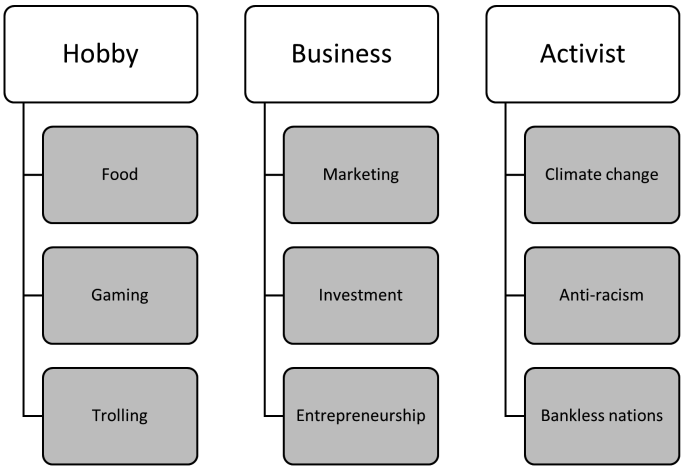

Figure 1: Overview of most common existing DAOs

While the review of existing DAOs did not identify any openly anti-democratic or anti-minority DAOs, some DAOs made use of alt-right codes and conspiracy myth references, or expressed support for far-right populist leaders. For example, the "Redacted Club DAO" claimed to be a secret network with the aim of "slaying" the "evil Meta Lizard King". The official Discord chat of the "Redacted Club DAO", which counted 850 members at the time of analysis, contained Pepe the Frog memes and references to "evil lizards" and "good rabbits". Another DAO, which was not listed on Decentralist, was called "Free Trump DAO". Its Twitter account described it as being "for Patriots" and serving as "a powerful tool that fights for freedom and liberty around the world." Its Telegram channel, which counted 474 members, was filled with Trump-glorifying memes, MAGA symbols and announcements such as "We're supporting Trump. Bring back Trump". There was also the "Trump DAO – the 47th U.S. President", which claimed to want to "raise money through the crypto to support Trump for 2024". The aim was to shape political campaigns by fundraising and giving complete anonymity to people who want to support Trump.

Extremist Incentives to Exploit DAOs

This sub-chapter used ethnographic research in extremist forums and chat groups to assess their conversations about DAOs. The analysis was

performed on the far-right fringe platforms Bitchute, Odysee and Gab as well as the encrypted apps Discord and Telegram. An exploratory discourse analysis was used, as the volume of content that is specifically focused on DAOs is still limited in extremist communities and therefore does not provide enough data points for statistical analysis.

A total of 85 pieces of content were identified across the analysed far-right fringe platforms, 46 on Odysee, 23 on Bitchute and 16 on Gab. Additionally, 100+ channels related to DAOs were detected on Telegram and Discord, including far-right extremist channels. While many of the posts on Odysee, Bitchute and Gab simply explain the characteristics and advantages of DAOs and how they might shape the Web 3.0, some of the detected conversations also reveal that there is much appetite for decentralised alternative forms of collaboration, communication and crowdfunding. Broadly speaking, the intent of far-right activists to use DAOs can be divided into two overarching types of incentives: practical and ideological motivations.

Important practical reasons are that DAOs can help users to circumvent monitoring, regulatory mechanisms and traditional institutions. For example, extremists may view them as useful to escape surveillance by security services, avoid perceived censorship by tech firms and find an alternative to frozen bank accounts. Many extremist and even terrorist movements already created their own cryptocurrencies and make use of anonymous bitcoin wallets. In particular, non-transparent cryptocurrencies such as Monero served extremists whose bank accounts have been frozen. Jihadists used cryptocurrencies as early as 2016 to fund violent activities (Irwin & Milad, 2016). In 2019, Treasury Secretary Steve Mnuchin warned that cryptocurrencies pose a national security threat, allowing malicious actors to fund criminal activities (Rappaport & Popper, 2019). While decentralised finance is already a trend among extremists, a shift to entirely decentralised forms of self-governance could be the next step (Krishnan, 2020). For example, Gab users highlighted that DAOs can help organisations to "unlock their full potential and usher in a new era of decentralized governance." The post continued: "Embrace the power of automation and embark on a journey of efficient and transparent decision-making within your DAO." Another one shared that DAOs may not be "capable of being subject to sanctions".

There are also ideological incentives that might lead extremists to use DAOs for their purposes. In particular, fundamental distrust in the establishment means that DAOs can be an appealing alternative. Users who believe that the "deep state" or the "global Jewish elites" control everything

from governments and big tech to the global banking system might prefer to set up their own technological, financial and logistical networks. For example, QAnon-related groups on Telegram were discussing the future of decentralized finance and how this might be an escape route to evade the U.S. federal banking system. DAOs also fit ultra-libertarian utopian visions of online worlds that are entirely unregulated, in which speech and actions are "truly free". "FREEDOM Meta-DAO" declared in its mission statement on Discord: "We believe in freedom of speech, privacy, and protection from cancel-culture bullying. Using a DAO as a service platform, we bring society together as a whole by removing borders and adaptation blockages." Finally, some users may be motivated by the outlook of creating their own digital state that operates based on their own rules, values and ideologies.

Practical Incentives	Ideological Incentives
Safe haven from surveillance by security services or journalists	Conspiracy myths about the establishment and financial institutions
Escape route from social media removal policies	Ultra-libertarianism and desire for unlimited free speech
Financial solution to frozen bank accounts	Creation of digital state or corporation according to own rules

Table 1: Overview of practical and ideological incentives

Most of the posts about DAOs on far-right websites were positive, however there were also a few warnings among the analysed pieces of content. For example, one user on Gab wrote that "though Blockchain technologies make traditional authoritarianism less likely, they make a new kind of authoritarianism, born of decentralized autonomous organizations (DAOs), more likely." The user continued: "By design and accident, DAOs will tend to develop into the computational equivalents of eusocial colony animals such as ants, bees, and termites. Once formed into such superorganisms, DAOs will exhibit emergent behaviors like swarming and collective intelligence." Indeed, the user pointed out that one of the risks is that "humans venturing into the DAOs' native habitat would then find themselves forced to live under the arbitrary will of not another human, but instead of a vast, mysterious hoard of nonhuman, and perhaps inhuman, entities."

Extremist Capabilities to Exploit DAOs

In this section, an analysis of potential areas for exploitation was performed based on a review of literature and interviews with two leading technology experts. The first interviewee was Carl Miller, the Director of the Centre for the Analysis of Social Media (CASM) at the think tank Demos who has long warned of potential threats emerging from the misuse of DAOs. The second interviewee was Christoph Jentzsch, a leading developer of the blockchain Ethereum and head behind "The DAO", which became one of the largest crowdfunding campaigns in history, raising over $150 million after launching in April 2016 via token sale, but was hacked soon later.

This sub-chapter addresses questions such as: Could trolling armies start cooperating via DAOs to launch election interference campaigns? What happens if anti-minority groups establish their own digital states in which they impose their own governing structures? Finally, how might terrorists leverage DAOs to fund and plot criminal activities and violent attacks?

DAOs can be used by movements to further their social, political and criminal objectives. Three potential threats were identified related to extremist and terrorist use of DAOs: 1.) influence campaigns, 2.) radicalisation of sympathisers, and 3.) attacks on political opponents. In all three potential threat areas, DAOs can be exploited in at least three ways on a tactical level: a.) by coordination and planning activities, b.) by crowdfunding and purchasing activities, and c.) by radicalisation and training activities. As such, they could change the nature of rebellion movements as well as their relative position of power, effectiveness and resilience to governmental countermeasures (Krishnan, 2020). Figures 2 and 3 summarise the potential threats as well as potential tactical exploitation areas associated with the use of DAOs by extremists and terrorists:

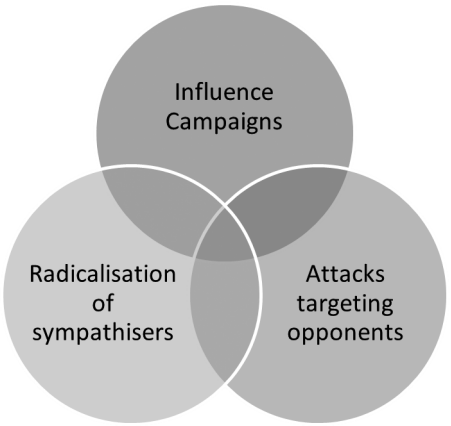

Figure 2: Overview of potential threats

Figure 3: Overview of potential tactical areas for exploitation

1 Influence Campaigns

One risk is that DAOs might be used in the future to carry out large-scale influence and election interference campaigns. Carl Miller told me that "beyond the speculative activities around crypto and NFTs, the deeper simmering experimentation around governance provided more fundamental challenges to the state and security." DAOs allow extremist groups to engage in deliberative and collective governance and decision-making in

ways where, according to Carl, it is a.) very unclear who is doing it, and b) hard for statutory security agencies to do anything about it. "As we gear up for the next U.S. presidential election, we might see DAOs being used for election campaigns," he warns. For example, Trump DAO could incentivise people to donate and participate in campaigns. "One could imagine a campaign being funded by tens of thousands of dark wallets that do not have clear links to real-world identities." Would this be recognised as electoral campaigning? Carl noted that the regulatory space in U.S. currently regulates at wallet level, not at DAO levels. However, these wallets can be fully anonymous. "There are already crypto-based gig sites where small jobs can be done anonymously based on crypto remuneration," Carl said. "In the future we might see gig workers being paid to run disinformation campaigns or stage protests."

2 Radicalisation of Sympathisers

Another risk is that DAOs could facilitate radicalisation efforts undertaken by extremist groups. Carl noted that "the basic problem of extremists is that they are being denied the conventional, easiest ways of reaching people". For example, they find it hard to rent halls, to have Facebook groups, to raise money or get the word out. He continued "You could easily see a world where there are protocol-based alternatives or replacements for conventional organizational structures", allowing extremist movements to surmount collective action problems, create international coalitions and fundraise for their activities.

Extremist movements could potentially even create their own digital states, for example in the form of digital white ethnostates or cyber caliphates. In 2022, the former chief technology officer at Coinbase Balaji Srinivasan described in his book *The Network State* how DAOs could soon give rise to new forms of digital statehood. Any group of online users could decide to start their own country, with their own laws, social services and financial transactions (Srinivasan, 2022).

3 Attacking Political Opponents

Finally, DAOs might also serve as safe havens for the planning and plotting of violent terrorist attacks and cybercrimes. The circumvention of govern-

ment regulation and monitoring activities could make them particularly useful for violent extremist and criminal organisations. Moreover, white nationalist movements have long been advocating for decentralised structures and so-called "leaderless resistance" (Michael, 2012; Malone et al., 2022). Increasingly, jihadist organisations such as Islamic State and Al Qaeda have adopted similarly decentralised models of leadership. Researchers have argued that leaderless organisations are more resilient to disruptions and interventions than hierarchical organisations. They compared hierarchical organisations to spiders who will die when you cut off their head, while the equated leaderless organisations with starfish whose legs will regrow when you cut them off (Brafman & Beckstrom, pp. 19–29).

According to Christoph Jentzsch, the most notable difference between DAOs and traditional forms of organisations is that, unlike associations or co-operatives, DAOs cannot be outlawed and their assets or bank accounts cannot be frozen. "If you can get organised without relying on traditional infrastructure, this also means that you won't be controlled by traditional institutions. It would be difficult to intervene on a statutory level". Jentzsch argues that cash already provides an alternative route for clandestine groups to fundraise, hold or spend money. Yet, DAOs might make it easier to conduct international, anonymous operations.

DAOs could give rise to new forms of the dark market. It might even be possible for DAOs to facilitate an anonymous assassination market (Krishnan, 2020). Carl noted that there would probably be law enforcement responses to terrorist plots and other serious criminal activities, which could include "a mix of infiltration and subversion, and perhaps direct cyber offensive activity." DAOs would be resilient in some ways because they are decentralised and rely on smart contracts. However, they might also be more vulnerable to hacking offenses. "It's difficult for creators to know when they are safe from a hacking attack due to their complex structures," Carl explained.

Conclusions, Future Research and Challenges on the Horizon

DAOs bring both a range of challenges and opportunities for democratic culture in cyberspace. Advocates of DAOs have argued that these blockchain-based forms of self-governance promise enhanced security, transparency and trust and reduce transaction costs arising through inter-

mediaries. Meanwhile, this chapter has explored some of the key challenges and risk areas for national security and democracy.

The potential exploitation of DAOs for extremist or criminal purposes has not received enough attention in the research and policy communities. This chapter identified a range of ways in which DAOs might be misused by extremist movements in the future, which could challenge the rule of law, pose a threat to minority groups, and disrupt institutions that are currently considered fundamental pillars of democratic systems. More specifically, the study explored how extremist movements might tap into DAOs to plan, coordinate and launch influence and interference operations, radicalisation campaigns and violent attacks.

Risks associated with the misuse of DAOs for extremist and criminal purposes has not been on the radar of global policymakers. Many governments have started to develop or pass legal frameworks to regulate AI. However, few countries or regions have even recognised the existence of DAOs or considered regulating them. Technology expert Carl Miller said that "even though DAOs behave like companies, they are not registered as legal entities". As of 2024, there are only a few exceptions: The U.S. States Wyoming, Utah, Vermont and Tennessee, as well as Switzerland, Estonia, Malta, Gibraltar, and the Republic of the Marshall Islands have passed laws to legally recognise DAOs.

This chapter understands the potential risk areas of DAOs in the Metaverse. While this study focused on non-state actors, exploring emerging threats from hostile state actors might be another important area for future research. Studies could also use experimental methods and interviews with policymakers and law enforcement to map the threats landscape. "DAOs can be used by anyone: by charities, investment funds, but yes, they can also be used by terrorist organisations," Christoph Jentzsch argues. However, he believes that the positive cases of use significantly outweigh the negative ones. Future studies should investigate both the potential opportunities and challenges related to collective decision-making and self-governance, diversity and the protection of minorities, radicalisation and extremism in decentralized communities in the Metaverse. The positive ways in which DAOs can shape future democratic culture are just as poorly understood as the negative impact they could have on politics and society.

References

Amhaz, R., Bobenrieth, C., & Marz, M. (2014). The impact of decentralised autonomous organisations (DAO) on Society 5.0. In *5th International Conference on Machine Learning, IOT and Blockchain*. https://aircconline.com/csit/papers/vol14/csit140301.pdf

Brafman, O., & Beckstrom, R. A. (2007). *The starfish and the spider: The unstoppable power of leaderless organizations*. Penguin.

Chao, C.-H., Ting, I.-H., Tseng, Y.-J., Wang, B.-W., Wang, S.-H., Wang, Y.-Q., & Chen, M.-C. (2022). The study of decentralized autonomous organizations (DAO) in social network. In *Proceedings of the 9th Multidisciplinary International Social Networks Conference* (pp. 59–65).

Decentralist. (2023). The list of DAOs. *Decentralist*. https://www.decentralist.com/list-of-daos

DeepDAO. (2024). Organizations. *DeepDAO*. https://deepdao.io/organizations

Goldberg, M., & Schär, F. (2023). Metaverse governance: An empirical analysis of voting within decentralized autonomous organizations. *Journal of Business Research*, 160.

HM Government, Law Commission. (2024, July). *Decentralised autonomous organisations (DAOs): A scoping paper*. https://lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/#related

Irwin, A. S. M., & Milad, G. (2016). The use of crypto-currency in funding violent jihad. *Journal of Money Laundering Control*, 19(4), 411.

Jentzsch, C. (2016). *Decentralized autonomous organization to automate governance* [White paper].

Krishnan, A. (2020). Blockchain empowers social resistance and terrorism through decentralized autonomous organizations. *Journal of Strategic Security*, *13*(1).

Laeeq, K. (2022, February). *Metaverse: Why, How and What* [Presentation]. https://www.researchgate.net/publication/358505001_Metaverse_Why_How_and_What

Malone, I., Blasco, L., & Robinson, K. (2022, September). Fighting the Hydra: Combatting vulnerabilities in online leaderless resistance networks. *National Counterterrorism, Innovation, Technology and Education Center, U.S. Department of Homeland Security*. https://digitalcommons.unomaha.edu/nctereportsresearch/24/

Michael, G. (2012). *Lone wolf terror and the rise of leaderless resistance*. Vanderbilt University Press.

Mondoh, B. S., Johnson, S. M., Green, M., & Georgopoulos, A. (2022, June 23). Decentralised autonomous organisations: The future of corporate governance or an illusion? http://dx.doi.org/10.2139/ssrn.4144753

Rappaport, A., & Popper, N. (2019, July 15). Cryptocurrencies pose national security threat, Mnuchin said. *New York Times*. https://www.nytimes.com/2019/07/15/us/politics/mnuchin-facebook-libra-risk.html

Sharma, T., Potter, Y., Pongmala, K., Wang, H., Miller, A., Song, D., & Wang, Y. (2024). Future of algorithmic organization: Large scale analysis of decentralized autonomous organizations (DAOs). In *Proceedings of ACM* (New York, US). https://arxiv.org/pdf/2410.13095

Srinivasan, B. (2022). *The network state: How to start a new country*. Self-published.

Sutikno, T., & Aisyahrani, A. I. B. (2023). Non-fungible tokens, decentralized autonomous organizations, Web 3.0, and the metaverse in education: From university to metaversity. *Journal of Education and Learning*, 17(1), 1–5.

Venis, S. (2022, July 5). Could new countries be founded – on the internet? *The Guardian*. https://www.theguardian.com/commentisfree/2022/jul/05/could-new-countries-be-founded-on-the-internet

World Economic Forum. (2023, January). *Decentralized Autonomous Organizations Toolkit* [Insight Report]. https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf