Decentralisation
- Tech trends position statement

Decentralisation of the internet means widely distributing the control of the online data, information, interactions and experiences of users.
Under a decentralised internet, often referred to as 'DWeb' or 'Web 3.0', users are said to have more power because they can access online services and platforms without relying on a concentration of large technology companies that own or operate mainstream, centralised servers (the computer hardware and software that stores data).

While decentralisation can allow users to protect their information and control their online experiences, it can also make it more difficult to hold users (or the entities behind them) responsible for illegal and harmful content and conduct.

Background

One aim of decentralisation is to reduce the market dominance of technology companies by limiting their power to determine how users engage and interact online. It's also a way for users to address the power imbalance that has allowed digital platforms and services to trade in and profit from their data and information.

A decentralised internet would distribute responsibility for the storage and retrieval of data, along with decision-making about how it can be used. Control would be shared among communities of users, each with their own rules of governance defining the rights and obligations of its members.

While a fully decentralised internet is still only theoretical, there is growing interest within the tech community in developing decentralised platforms and services for messaging, file sharing and social networking.

Currently there are three main types of decentralised services.

Peer-to-peer (P2P) services

Peer-to-peer services allow users to share information directly with other computers on a network without going through a central server that may be moderated or regulated. Examples of popular P2P services include Napster, LimeWire and BitTorrent.

Blockchain-based services

Blockchain-based services use a 'trustless' system, which means that users place their trust in a type of database that packages information into 'blocks' that are 'chained' together chronologically. The chain is difficult to alter because whenever a new block is added, every computer in the network updates to reflect the new chain.

Any attempt to alter information already accepted in previous blocks can be detected by the rest of the network participants. No single person, group or authority controls the data or transactions.

This blockchain technology can be used to operate decentralised marketplaces and build programs and applications such as messaging services, games, social media services and storage platforms that do not allow data to be altered or deleted.

Federated services

Federated services are online networks that run on independent servers and operate autonomously. The services are open-source, which means any member can create a matrix of networks to share content and activities.

The governance of each matrix is controlled by everyone who uses it. The most popular example of this is Mastodon, which has attracted groups who hold extremist views (as seen when social media service Gab migrated to Mastodon in 2019). There are concerns that it may also protect networks which share material depicting, instructing or normalising child sexual abuse.

Positive uses

Decentralisation could improve the security, privacy and autonomy of online users by giving them greater control over their personal information and online experiences. For example, it would allow users to prevent technology companies from commercialising search preferences, purchase histories and location tracking to shape the user access to information, target them with advertising or make them accessible to other online marketers.

Decentralisation could also enhance freedom of expression, by removing the ability of technology companies and authorities to control who can connect and communicate online, as well as the content and conduct that is allowed. This could protect diversity of thoughts and opinions and reduce the risk of monitoring, tracking and targeting of at-risk or marginalised individuals or groups, including whistle-blowers and advocates for social change.

Risks

Mainstream services and platforms generally offer a degree of oversight and moderation of online conduct and content. They can use their control of centralised servers to remove or limit access to content, manage participation by users or accounts, and even block access to particular services or platforms.

However, decentralised services and platforms are typically created for the very purpose of being censorship-resistant and allowing users to determine for themselves what content they can access and what activities they can participate in. The absence of centralised servers and lack of central authority, along with the storage and distribution of data across many computers, makes it difficult to moderate or regulate decentralised services and platforms or enforce the removal of illegal and harmful content. For these reasons, there are concerns that a decentralised internet may become a haven for criminal activities and for users who have been removed from mainstream services and platforms.

Unchecked online environments could allow a range of harms from bullying, harassment, intimidation, discrimination and other abuses to grow, without providing any way for users to get help or for consequences to be imposed on those responsible. It would be up to the members of individual online communities on each service or platform – or part of it – to decide and apply standards in their own environment or across their networks.

eSafety's research and reporting trends show that online abuse is most often targeted at individuals and groups who are more at risk than others due to being socially, politically or financially marginalised. For these people, the inability to enforce standards for conduct and content within a decentralised internet may actually harm freedom of expression instead of improving it. The current trend towards decentralisation may push marginalised groups away from the services and platforms that would otherwise allow them to be seen and heard, deepening the existing digital divide between those who can access and enjoy the internet and those who cannot.

Using decentralised services may give users more control over their information and online experiences, but it also increases their own responsibility for understanding and operating in unregulated environments and keeping their personal information secure. They need to be aware of the risks and take steps to manage those so their safety is also protected, not just their privacy and security.

To be socially responsible, decentralised services and platforms must also commit to protecting the safety of users, not just their privacy and security. That means being aware of the safety risks in what they provide, informing users about those risks and taking steps to reduce or eliminate the risks.

Online safety solutions

There are a number of ways decentralised services and platforms can help to keep their users safe from online harms.

These include taking a Safety by Design approach when developing and operating new technologies and Web 3.0 infrastructure, and ensuring that robust moderation of conduct and content is possible before releasing products to the market.

Safety protections may include the following.

Community moderation and incentives

This is where an online community maintains a moderation policy based on agreed rules. Features such as voting systems can allow users to decide acceptable conduct and accessible content. Additionally, built-in incentives – such as micropayments or other rewards – may encourage positive behaviour and safer environments.

Opt-in governance

Opt-in governance can be used on blockchain networks to allow users to agree to community standards or rules, without the need for a central authority to manage the agreement. Because these agreements exist in a blockchain network, they are traceable and transparent. In theory, this means accountability and enforcement measures can be applied to terms of service breaches.

Identity verification

Verifying and storing a user's digital identity through a decentralised system can allow them to access different services and platforms with multiple identities and pseudonyms without having to reveal personal information to the technology companies that own and operate centralised servers. A socially responsible decentralised community could allow users to endorse content from digital identities or pseudonyms who they trust not to engage online in a harmful or abusive manner.

Content moderation

Decentralised services and platforms can be built using technology protocols that allow third party content moderation tools to function – for example, tools that scan for child sexual abuse material. Their operation would have to be agreed to by the community of users.

Recent coverage

Much of the recent coverage of decentralised services has focused on reducing the power of technology companies to make decisions about the content that can be hosted on their service.

- On 21 January 2021, the Verge reported on Twitter's Bluesky project, which focuses on developing an open and decentralised standard for social media.
- On 17 March 2021, The Conversation published an article on how decentralised social media services are resistant to censorship, giving users control over what accounts and content are allowed on a service or platform.
- On 14 May 2021, the Australian Strategic Policy Institute hosted a webinar, 'In-Conversation with Julie Inman Grant, eSafety Commissioner'. The webinar features discussion on decentralisation.

eSafety approach

eSafety recognises that decentralised systems may help to protect certain elements of privacy and security. Our focus is on working with industry and developers to ensure that decentralised services and platforms are aware of Safety by Design principles and adopt them, so the online safety risks of decentralisation are considered along with the benefits.

The potential for decentralisation to disproportionately impact at-risk individuals and groups is significant. The United Nations recognises digital access as a basic human right, so eSafety will continue to work with at-risk communities to ensure that all users can make the most of connecting online – including on decentralised services and platforms.

From an education standpoint, we recognise that people may require an advanced level of digital literacy to use decentralised services. Users need to understand that on most decentralised services and platforms they are responsible for keeping their account secure, and they may be required to enforce a community's rules.

We recognise that people will need more comprehensive education about how to stay safe on decentralised services and platforms as their use increases. eSafety aims to help people develop their digital literacy and build digital citizenship through comprehensive education resources.

As decentralisation is now a global trend, we will continue to work across borders to encourage greater international consistency and shared approaches to help counter online risks and harms on decentralised services and platforms.

Advice for using decentralised services

Many decentralised services and platforms may not be suitable for children, because there is an increased risk of encountering harmful and illegal conduct and content. As a starting point, parents and carers are advised to check whether the service or platform has safety features and minimum age requirements set out in its terms of use, as do many mainstream services and platforms.

Anyone using a decentralised service or platform built on a blockchain technology should be conscious that it may not be possible to remove content once they have posted it, so it is best to avoid posting any content or information they do not want preserved.

If someone seriously abuses or harms you or someone in your care, even if this is on a decentralised service, there are several steps you can take:

- **Collect and preserve evidence** using screenshots or similar methods (unless the shots show nude or sexual content or conduct of someone under 18 years old) then report the abuse to the community or moderator if a reporting and moderation process is available.
- **Block unwanted contact** – make use of any features a service or platform offers to protect yourself.
- **Report to eSafety** – we may be able to help with serious cyberbullying, image-based abuse and illegal or harmful content online, or connect you with support.
- **Seek further support** from an expert counselling service.

If you suspect online child sexual abuse or grooming by a sexual predator report it straightaway – even if it's on a decentralised service or platform – to the Australian Centre to Counter Child Exploitation (ACCCE) via the 'Report Abuse' button on accce.gov.au/report. Or report it anonymously to Crime Stoppers on 1800 333 000 or at crimestoppers.com.au.