Tuba Eldem*

Decentralisation as Resistance: Web3's Potential in Countering Digital Censorship and Redefining Cyber Sovereignty

Abstract

The Internet, initially celebrated as a bastion of freedom and openness, is increasingly becoming a domain of control, surveillance, and regulation by both states and private entities. The rise of state control and regulation of the Internet, along with the private sector's expanding control over information, poses significant challenges to the ideals of freedom and openness that once defined the Internet. This article examines the transformation in Internet governance from a state of minimal regulation to a heavily controlled environment by both governments and corporations and explores how the blockchain technology and decentralised architecture underlying Web3 promise to redefine Internet governance and resist censorship. Through a mixed-method approach that synthesises insights from computer science, political science, and legal studies, the paper argues that public blockchains challenge Internet Corporation for Assigned Names and Numbers' (ICANN) traditional control over DNS and significantly reduce the ability of centralised entities to exert control over content and communication, thereby enhancing freedom of expression and resisting censorship. The ability of Web3 to fully realise this potential is, however, dependent on overcoming complex technical and regulatory challenges.

Keywords: Web3, blockchain, Internet governance, digital censorship, cyber sovereignty, decentralisation, information controls

* Dr Tuba Eldem, PhD, Director of the Center for Cyberspace Studies (FBUCyber), Associate Professor of Political Science, Fenerbahce University. ORCID iD: 0000-0001-6264-255X.

I The Digital Westphalia: The Rise of Sovereign Controls in Cyberspace

Initially, the Internet was considered an autonomous space free from state regulation and intervention. Yet over the last two decades, information controls, which refer to mechanisms to monitor, manage and regulate the flow of information online, have significantly expanded thanks to the centralisation of power in governments and big corporations. Governments increasingly regulate flows of information to maintain national security, preserve cultural norms and uphold or impose certain moral standards. The evolution of state control of information is analysed according to three distinct generations, each marking a significant expansion in the scope and depth of governmental control.[1] The first Generation of 'Blocking and Filtering' is characterised by direct censorship tactics, such as blocking access to websites, filtering content based on keywords, and disrupting Internet services at the ISP (Internet Service Provider) level. Techniques such as IP blocking, DNS tampering and URL filtering are relatively straightforward and involve the interruption of the flow of information at various points within a country's Internet infrastructure. They are aimed to prevent users from accessing specific pieces of content or entire websites deemed undesirable by a government or authority. While China's Great Firewall is perhaps the most well-known example, several other countries, such as Russia,[2] Iran,[3] Saudi Arabia, the Gulf,[4] Egypt[5] and Turkey,[6] have all implemented similar strategies to regulate and restrict the flow

---

1 Ronald J. Deibert, Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 (3) Global Governance 339; Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010) DOI: https://doi.org/10.1163/19426720-01803006; Jonathan Clark and others, *The Shifting Landscape of Global Internet Censorship* (Berkman Klein Center for Internet and Society Research Publication 2017).

2 Gergely Gosztonyi, 'Special Models of Internet and Content Regulation in China and Russia' (2021) (2) ELTE Law Journal, 87–99, DOI: https://doi.org/10.54148/ELTELJ.2021.2.87; Julien Nocetti, 'Contest and Conquest: Russia and Global Internet Governance' (2015) 91 (1) International Affairs 111–130. https://doi.org/10.1111/1468-2346.12189; Nate Maréchal, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' (2017) 5 (1) Media and Communication 29–41, DOI: https://doi.org/10.17645/mac.v5i1.808

3 Orkideh Safshekan, 'Iran and the Global Politics of Internet Governance' (2017) 2 (2) Journal of Cyber Policy 266–284, DOI: https://doi.org/10.1080/23738871.2017.1360375

4 James Shires, *The Politics of Cybersecurity in the Middle East* (Oxford University Press 2022, Oxford) DOI: https://doi.org/10.1093/oso/9780197619964.001.0001; Ram Sundara Raman et al, 'Measuring the Deployment of Network Censorship Filters at Global Scale' (2020) Network and Distributed System Security Symposium (NDSS) <https://www.ndss-symposium.org/ndss-paper/measuring-the-deployment-of-network-censorship-filters-at-global-scale> accessed 15 October 2024.

5 Bassant Hassib, James Shires, 'Manipulating uncertainty: cybersecurity politics in Egypt' (2021) 7 (1) Journal of Cybersecurity 1–16, DOI: https://doi.org/10.1093/cybsec/tyaa026

6 Tuba Eldem, 'The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security' (2019) 43 (5) International Journal of Public Administration 452–465, DOI: https://doi.org/10.1080/01900692.2019.1680689

of information online. The OpenNet Initiative conducted Internet filtering tests across over 70 nations, discovering signs of filtering in 45 countries.[7] This figure is probably growing rapidly as a growing number of countries are initiating content censorship related to child sexual exploitation, hate speech and terrorism-related content.

The second-generation controls saw deeper penetration by state agencies into the domestic sphere, enhancing their capacity to monitor and regulate the flow of information through a broad range of legal and regulatory measures. These methods often entail the participation or compliance of private sector entities, such as ISPs and social media platforms, and include the submission of content takedown requests, mandatory sharing of customer data and the enforcement of defamation and libel laws against online content.

The third generation of controls represents a qualitative leap in the strategies employed by states to manage, influence and control the information environment. This generation is characterised by an unprecedented expansion of state surveillance capabilities, both in-depth and reach, facilitated by technological advancements and the globalisation of data flows. Third-generation information controls have largely seen the expansion of the extraterritorial reach of state actors in cyberspace. Many states engaged in targeted surveillance, digital espionage and disinformation campaigns.[8] Russia has been involved in disinformation campaigns that have sought to influence elections and sow discord in other countries, notably in the events leading up to the 2016 US presidential election.[9] China has been reported to use advanced cyber capabilities not just for surveillance within their own borders but also for espionage and intellectual property theft from entities in the United States and other nations.[10] Many authoritarian states, such as the United Arab Emirates, Thailand and Saudi Arabia, have extended their extra-territorial intrusion largely thanks to the deployment of spyware technologies. An investigation by the New York Times revealed that NSO's dealings played a pivotal role in aiding former Israeli Prime Minister Benjamin Netanyahu to broker the Abraham Accords with Bahrain, Morocco and the UAE. Subsequently, these client states reportedly employed Pegasus not only to survey domestic opposition but also to engage in espionage against geopolitical adversaries.[11] The

---

7 https://opennet.net

8 Howard Nissenbaum, Bence Kollanyi, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' (2016) ArXiv, DOI: https://doi.org/10.48550/arXiv.1606.06356; Nigel Inkster, 'Information Warfare and the US Presidential Election' (2016) 58 (5) Survival 23–32, DOI: https://doi.org/10.1080/00396338.2016.1231527; Robert Chesney, Danielle Citron, 'Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics' (2019) Foreign Affairs 147–155.

9 Stephen McCombie, Adrian J. Uhlmann, Shane Morrison, 'The US 2016 Presidential Election & Russia's Troll Farms' (2020) 35 (1) Intelligence and National Security 95–114, DOI: https://doi.org/10.1080/02684527.2019.1673940

10 Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (eds), *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain* (Oxford University Press 2015, Oxford) DOI: https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

11 Ronald J. Deibert, 'The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy' (2023) Foreign Affairs <https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert> accessed 15 October 2024.

use of spyware has extended to democratic states such as Greece, Hungary, Poland, Spain and Mexico. These disclosures have revealed state-sponsored cyber espionage targeting journalists and political adversaries – blatant proof of the penetration of surveillance practices across both autocracies and democracies.

II Surveillance Capitalism and the Rise of Corporate Controls in Cyberspace

On the corporate side, the growing demand for these offensive tools has led to the rise of a lucrative market for advanced spyware, surveillance tech and services. The spyware industry, now valued at approximately $12 billion annually, has emboldened not only the prominent Israel-based NSO Group but also other Israeli firms like Cytrox, Cyberbit and Candiru, as well as former players like Italy's Hacking Team and the Anglo-German Gamma Group.[12] This proliferation reflects the broader trends in surveillance capitalism in which wealth and power are concentrated in the hands of a few tech giants who commodify and exploit personal data obtained through surveillance for profit.[13] In today's data economy, companies like Google, Facebook, Amazon and Apple have grown into colossal entities partly because of their ability to leverage vast amounts of data. The concentration of data, resources and decision-making power within a small number of large tech companies is considered to be creating a new form of techno-feudalism, where individuals have limited control over their data (akin to land in feudal times) and are dependent on tech platforms for access to digital services and economic opportunities.[14] According to the techno-feudal model, tech giants such as Google, Facebook and Amazon, which collect vast amounts of data to target users with advertisements more effectively, are seen as the new lords with control over digital resources, data and infrastructure. The Cambridge Analytica scandal is a blatant indicator of how such power dynamics operate in practice. Social media platforms, such as Facebook, compile intricate digital profiles of users by covertly observing their online behaviours. These detailed profiles, which capture individual preferences, interests, and even vulnerabilities, are then commoditised and sold to political interest groups without the users' consent. These groups employ the data to craft targeted campaigns that subtly manipulate public opinion and voter behaviour.[15] The Cambridge Analytica scandal

[12] Ronald J. Deibert, Louis W. Pauly, 'Mutual Entanglement and Complex Sovereignty in Cyberspace' in Didier Bigo, Engin Isin, Evelyn Ruppert, *Data Politics. Worlds, Subjects, Rights* (Routledge 2019, London) 81–99.

[13] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

[14] Yannis Varoufakis, *Technofeudalism: What Killed Capitalism* (Melville House 2024).

[15] Carole Cadwalladr, Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (17 March 2018) The Guardian <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 15 October 2024.

underscored the potential for massive data misuse in the absence of stringent privacy controls.

Tech giants have also gained significant prerogatives in determining what content is seen, shared and suppressed. The private sector's role in controlling information has expanded alongside the growth of digital platforms. Companies like Facebook, Twitter and YouTube not only control vast amounts of data but also control the infrastructure and platforms through which information is disseminated and transactions are conducted. This makes them important gatekeepers of information, with the power to amplify or suppress content through algorithms. They have important prerogatives in the areas of content moderation, de-platforming and algorithmic prioritisation, which are often criticised for being opaque, inconsistent and biased.[16]

The mounting concerns over centralised control, data commodification and the erosion of privacy have catalysed interest in alternative structures for the Internet – paving the way for the emergence of Web3. Characterised by its decentralised architecture and blockchain technology, Web3 is posited by its advocates as the future of the web, promising censorship resistance, enhanced security, transparency and user control, thus countering the monopolistic and surveillance-driven practices of traditional tech entities. This shift is seen as crucial in restoring self-sovereignty and enhancing user privacy, providing a robust framework that counters the centralised models that currently dominate the digital landscape.

The following section will explore the foundational principles of Web3, emphasising the pivotal technologies and initiatives that underpin this transformative shift. It will largely rely on insights gained from the participant observation of tech and thought leaders working in the area of Web3 and open-ended interviews conducted at the DevConnect conference in Istanbul in November 2023, where the leading tech experts and blockchain innovators shared their perspectives on the challenges and possibilities inherent in decentralised web technologies. This discussion will highlight how Web3 could lead to a censorship-resistant Internet and more participatory Internet governance structure while also recognising the significant challenges that must be overcome to fully realise a shift towards greater self-sovereignty and enhanced privacy.

III Web3: Envisioning the Future of the Internet

Web3 is a marketing concept coined by Ethereum co-founder Gavin Wood in 2014 and has attracted significant attention from cryptocurrency enthusiasts, major technology firms and

[16] Gergely Gosztonyi, *Censorship from Plato to Social Media: The Complexity of Social Media's Content Regulation and Moderation Practices* (Springer 2023, Cham) 111–119, DOI: https://doi.org/10.1007/978-3-031-46529-1_8

venture capital investors since 2021.[17] Proponents of Web3 usually explain it by comparing it with its earlier versions. The first, referred to as Web1, covered the early 1990s to the early 2000s. It was a read-only Internet site, and users were passive consumers of content, such as web pages or encyclopaedia entries. This era was characterised by static HTML pages with minimal user interaction. Web2 emerged around 2004 with the rise of social media platforms like Google and Facebook, leading to a more interactive era with user-generated content. However, the Web2 era was riddled with centralisation as network effects and economies of scale led to a few companies building extreme wealth based on user data and targeted advertising.[18] This centralisation and the numerous scandals that followed created a backlash against the manner in which personal data was handled, setting the stage for the development of Web3.

The cypherpunks, a countercultural group of software engineers, cryptographers and philosophers who emerged in the 1990s, laid much of the philosophical groundwork for Web3. Advocating for strong cryptography and privacy-enhancing technologies, they played a pivotal role in fostering the ideals of self-governance, individual freedom and self-sovereignty that are central to Web3.[19] The technical infrastructure of Web3 began to crystallise with Satoshi Nakamoto's introduction of blockchain technology in 2008 through Bitcoin. This innovation fostered a trustless, transparent and secure method for transaction recording and verification on a decentralised network. The momentum for Web3 continued to build with the launch of Ethereum in 2015, which led to smart contracts – self-executing contracts with terms directly written into code.[20] That same year, the InterPlanetary File System (IPFS) was developed, further advancing the Web3 vision by supporting decentralised storage and file-sharing across various applications.

The initial adoption of Web3 technologies was largely driven by the cryptocurrency community recognising the potential for decentralised finance (DeFi) platforms that operate independently of traditional banking systems. However, the implications of Web3 extend beyond DeFi, influencing sectors like social media and content delivery. These decentralised applications provide alternatives to traditional models, offering benefits in terms of data integrity, user sovereignty and resistance to censorship. The following section discusses the underlying technologies of Web3 and how they are likely to challenge Internet governance and counteract censorship.

---

17 Amanda Cassatt, *Web3 Marketing: A Handbook for the Next Internet Revolution* (Wiley 2023, New Jersey).

18 Thomas Stackpole, 'What Is Web3?' 10 May 2022, Harvard Business Review, https://hbr.org/2022/05/what-is-web3> accessed 15 October 2024.

19 Kelsie Nabben, 'Web3 as 'Self-Infrastructuring': The Challenge is How' (2023) (January–June) Big Data & Society 1–6, DOI: https://doi.org/10.1177/20539517231159002.

20 Andrew McAfee and others (eds), *Web3: The Insights You Need from Harvard Business Review* (Harvard Business Review Press 2023, Boston).

IV How Web3 Fights against Censorship and Reshapes Internet Governance

Web3, often synonymous with the decentralised web, leverages blockchain technology to create an Internet where applications and platforms operate on a decentralised network of computers rather than relying on central servers.[21] This decentralised, immutable and peer-to-peer nature of Blockchain is fundamental to Web3's resistance to censorship. Blockchains on which Web3 architecture is built operate as a type of database that distributes its data across many computers, where every entry, known as a 'transaction', is transparent to all users. This transparency ensures that any attempt at censorship is visible to all participants, who can then challenge and debate such actions. Second, blockchains are shared and decentralised, meaning that multiple copies of the blockchain exist simultaneously on different computers. Third, blockchains are immutable, which means that once data is recorded, it cannot be altered or removed. This structure makes it difficult for governments or other entities to suppress information or revise historical records. Finally, blockchains operate on the principle of disintermediation, where decisions are made through consensus among participants without the need for an intermediary. Content moderation policies work according to these consensus protocols, such as Proof of Work (PoW) and Proof of Stake (PoS), requiring approval from the network participants. This collective agreement is key to preventing any single party from individually changing data for purposes such as censorship or manipulation. The inherent difficulty of modifying any data already approved by consensus without the majority of the network's endorsement makes blockchain highly resistant to tampering.

A second way that Web3 fights censorship is by decentralising the hosting and storage of online content. In Web2, most websites and applications rely on centralised servers that are owned and operated by a single entity. This makes them easy targets for censorship by authorities that can block access to these servers or pressure the owners to remove or modify content. In Web3, however, content can be hosted and stored on distributed networks of nodes that are run by various users across the globe. This makes it harder for anyone to censor or manipulate specific content since even if some nodes are taken down or censored, the data remains accessible elsewhere in the network.[22]

Web3 introduces promising structural and functional innovations that complicate the ability of censors to directly interfere with content access and distribution. In Web2, censors typically block access to content by targeting specific servers or content delivery networks (CDNs), intercepting DNS requests, or employing IP-blocking censors. The decentralised

[21] Stackpole (n 18) 18.

[22] Will Scott, *Censorship Resistant Web Applications* (PhD thesis, University of Washington 2018); Adem E. Gencer and others, 'Decentralization in Bitcoin and Ethereum Networks' in Sarah Meiklejohn, Kazue Sako (eds), *Proceedings of the International Conference on Financial Cryptography and Data Security* (Springer 2018) 439–457, DOI: https://doi.org/10.1007/978-3-662-58387-6_24

architecture of Web3, involving decentralised naming systems and distributed file storage systems, complicates many of these conventional interference tactics. Decentralised naming systems such as Ethereum Name Service (ENS), Unstoppable Domains (UD) and Handshake (HNS) offer resilience against traditional DNS blocking and domain seizures by distributing control across a network of users. They also challenge the contemporary model of Internet governance. The current Internet infrastructure is predominantly centralised around ICANN, which manages 13 logical DNS root name servers. This centralisation makes Internet communications vulnerable to sophisticated censorship tactics like DNS and IP blocking.[23] In contrast, decentralised naming systems use distributed ledger technology to extend control widely among network participants. This greatly diminishes the centralised points of control that could be targeted for censorship or to restrict information access.[24]

Web3 also embraces distributed file storage systems, such as the InterPlanetary File System (IPFS), which disperses content across a network of nodes. Unlike conventional web protocols that locate content based on its location (URLs), IPFS uses a content-based addressing system where each piece of content is uniquely identified by a hash. Thus, as long as the content is hosted somewhere on the network, it remains accessible to anyone who knows its hash. This structure not only makes the web more resilient against censorship and server failures but also ensures that content cannot be easily removed or blocked by any single authority or organisation.[25] This was vividly demonstrated in situations like the censorship attempts in Turkey and Catalonia, where distributed mirror technologies and IPFS were used to bypass government-imposed Internet restrictions. For example, IPFS played a crucial role in counteracting Turkey's censorship of Wikipedia by hosting the entirety of Turkish Wikipedia on its network. This initiative was part of the Distributed Wikipedia Mirror project led by the IPFS team, which aimed to make Wikipedia available in a decentralised manner.[26] Similarly, during the 2017 Catalan independence referendum, activists and organisers used decentralised and blockchain technologies to circumvent censorship and ensure the integrity and confidentiality of the voting process. They used IPFS to spread referendum-related content through a decentralised network, ensuring accessibility despite government blocks. Blockchain was also critical for recording votes in an immutable ledger, which strengthened the security and reliability of the election results.

---

[23] Joseph L. Hall and others, *A Survey of Worldwide Censorship Techniques* (1 November 2023) Internet Research Task Force <https://www.rfc-editor.org/rfc/rfc9505.pdf> accessed 15 October 2024.

[24] Juan Benet, *'Preventing Digital Totalitarianism. Modern Orwellian States'* (presented at the DevConnect, Istanbul, 18 November 2023).

[25] Ibid. Dennis Trautwein et al, 'Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web' in *Proceedings of the ACM SIGCOMM 2022 Conference (SIGCOMM '22)* (Association for Computing Machinery 2022, New York) 739–752, DOI: https://doi.org/10.1145/3544216.3544232

[26] Arzu Geybullayeva, 'In Turkey, Mirror Websites Are Helping Users Reconnect to Wikipedia' (16 June 2017) The Wire <https://thewire.in/external-affairs/turkey-mirror-websites-helping-users-reconnect-wikipedia> accessed 15 October 2024; also see: Marcin Rataj, 'Distributed Wikipedia Mirror Update' (31 May 2021) IPFS Blog, <https://blog.ipfs.tech/2021-05-31-distributed-wikipedia-mirror-update> accessed 15 October 2024.

Decentralised applications enabled secure and transparent voting processes and made it challenging for the Spanish government to interfere.[27] This innovative use of technology not only safeguarded the referendum process but also demonstrated the potential of these tools in supporting democratic practices under restrictive conditions.

A third way Web3 challenges contemporary Internet governance and potentially reduces self-censorship is by providing users with greater anonymity and asserting their self-sovereignty and privacy through empowering user control over their digital identities and data. In the contemporary Web2 architecture, users often have to link their digital identities to personal information such as real names or phone numbers when creating accounts on social media platforms. This practice not only strips users of anonymity but also exposes them to extensive surveillance, tracking and profiling by platform operators and external entities. Furthermore, in this centralised system, the control over user data is largely in the hands of the platforms, which reserve the right to change, remove, or commodify user content according to their own terms and policies, often without obtaining explicit consent from the users.

In Web3, however, users can create pseudonymous or anonymous identities that are secured by cryptography and blockchain. They can also store their data and content on decentralised platforms that respect their privacy and self-sovereignty. Through blockchain-based naming systems, users can own and control their personal data associated with domain registrations without needing to reveal their identities publicly, which is often required in traditional DNS registrations. Users of decentralised naming systems have true ownership of their domains, unlike traditional DNS where the domain is essentially leased from a registrar. Once acquired, blockchain domains are controlled by the individual through private keys, meaning they cannot be revoked by a third party without access to those keys.[28] This empowerment extends to how data is used and shared, giving users full control over their online presence. This growing self-sovereignty over their data and anonymity could diminish self-censorship by reducing fears of being personally targeted for one's online activities.

In China, blockchain technology has already been used to counteract censorship. In 2018, an anonymous user implanted an open letter describing harassment by Peking University within an Ethereum transaction and subsequently shared it on the Ethereum

---

[27] Marta Poblet, 'Distributed, privacy-enhancing technologies in the 2017 Catalan referendum on independence: New tactics and models of participatory democracy' (2018) 23 (12) First Monday, DOI: https://doi.org/10.5210/fm.v23i12.9402; Manel Medina, 'Governmental Censorship of the Internet: Spanish vs. Catalans Case Study' (2020) 68 (4) Library Trends 561, DOI: https://doi.org/10.1353/lib.2020.0011; Vasilis Ververis and others, 'Understanding Internet Censorship in Europe: The Case of Spain' in N/A (eds), *Proceedings of the 13th ACM Web Science Conference* (Association for Computing Machinery 2021, New York). DOI: https://doi.org/10.1145/3447535.3462638

[28] Alex Preukschat, Drummond Reed, *Self-Sovereign Identity* (Manning Publications 2021, New York).

blockchain.[29] Despite censorship efforts on widely used centralised platforms like WeChat, the Chinese government could not remove the letter once it was uploaded to the Ethereum blockchain. This event not only underscores the resilience of public blockchains in protecting information but also signifies their ongoing role as a crucial tool for safeguarding free expression in the future.

Last but not least, proponents of Web3 argue that Web3 would address censorship through user empowerment and the enhancement of democratic governance and participation. On traditional Web2 platforms, decisions about content and user interaction are typically made by a small group of platform administrators or algorithms designed by a company, often leading to opaque and sometimes controversial moderation practices. Web3's governance model shifts control and decision-making from centralised authorities to the community of users. Web3 introduces a system where users directly influence the platforms and protocols they engage with. This is achieved through participatory governance mechanisms of blockchain-based decentralised autonomous organisations (DAOs), which enable transparent and trustless decision-making by allowing stakeholders to participate directly in governance processes within decentralised systems. DAOs are structures that utilise blockchains, digital assets and associated technology to allocate resources, coordinate activities and reach decisions. Defined as community-minded and code-driven hybrid organisations, DAOs are considered an alternative to traditional organisational forms through the publication of operational data to the general public and enabling members to participate in governance.[30] DAOs allow users to vote on initiatives, propose amendments, finance projects and receive incentives for their contributions to the digital ecosystem.[31] DAOs have experienced explosive growth – from a total value of treasuries at $380 million in January 2021 to an impressive $25.1 billion by December 2023, with participants increasing from 13,000 to 6.8 million.[32] This shift towards grassroots, community-led governance defies traditional hierarchical structures by encouraging inclusivity and collective decision-making. Thus, the transformative potential of Web3 lies not only in fostering censorship resistance but also in significantly reducing the barriers to democratic engagement and control over digital spaces, thereby democratising the Internet in true form.

---

[29] Keith Zhai, Lulu Yilun Chen, 'Chinese #metoo student use blockchain to fight censors' (24 April 2018) Bloomberg, <https://www.bloomberg.com/news/articles/2018-04-24/chinese-metoo-student-activists-use-blockchain-to-fight-censors?embedded-checkout=true> accessed 15 October 2024.

[30] World Economic Forum, *Decentralized Autonomous Organization Toolkit: Insight Report* (January 2023) <https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf> accessed 15 October 2024, 6.

[31] Jonathan Ruane, Andrew McAfee, 'What a DAO Can—and Can't—Do' in Andrew McAfeeand others (eds), *Web3: The Insights You Need from Harvard Business Review* (Harvard Business Review Press) 61.

[32] World Economic Forum (n 30) 6.

V Unpacking the Challenges of Web3 Technologies

While Web3 offers substantial benefits in combating censorship and enhancing democratic governance, its broader adoption is not without challenges that stem from both technical difficulties and legal and regulatory uncertainties. One of the most pressing challenges for Web3 technologies, particularly blockchain-based systems, is scalability. Most decentralised networks struggle to handle large volumes of transactions quickly and efficiently compared to centralised systems. For instance, Ethereum, the backbone of many Web3 applications, can only process about 15-30 transactions per second in its current state, whereas a centralised system like Visa can handle thousands of transactions per second. Solutions are being explored but are complex to implement and have not yet been fully realised at scale. Another challenge is related to technical complexity and user accessibility. Web3's infrastructure and applications can be complex for the average user and require a certain level of technical proficiency. This can potentially limit its accessibility and widespread adoption. A third technical challenge is to ensure interoperability between different layers of Web3 and across different platforms within the same layer.[33]

Web3 also need to address a set of regulatory and legal challenges as it operates in an essentially vague regulatory environment. Many states are still struggling with how to deal with blockchain, distributed ledger technology, cryptocurrencies, DAOs, DeFi, non-fungible tokens (NFTs) and other aspects of Web3. The lack of clear and consistent legal frameworks across different jurisdictions is the greatest challenge. There are also different interpretations concerning the applicable law with respect to transactions and assets recorded on the blockchain. The application of anti-money laundering and counter-terrorism financing regulations to crypto transactions is another challenge for the regulators as the decentralised and anonymous nature of many blockchain transactions poses significant enforcement challenges.[34]

Additionally, while Web3 advocates for greater user privacy and control over data, the public nature of blockchain technology can paradoxically lead to privacy issues. For example, transactions on public blockchains are traceable and permanently recorded, which can expose user activities and balances to anyone who cares to look. Advanced cryptographic methods such as zero-knowledge proofs are perceived as potential solutions but are still complex and not yet widely implemented. Furthermore, the irreversible nature of blockchain may conflict with 'the right to be forgotten' upheld in the General Data Protection Regulation

[33] Jared Ronis, 'Understanding Ethereum's Layer 1 and Layer 2: Differences, Adoption, and Drawbacks' (Wilson Center, 13 October 2023) <https://www.wilsoncenter.org/article/understanding-ethereums-layer-1-and-layer-2-differences-adoption-and-drawbacks> accessed 15 October 2024.

[34] Ioannis Lianos and others, Regulating Blockchain: Techno-Social and Legal Challenges (Oxford University Press 2019, Oxford); Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill 2023, Leiden), DOI: http://doi.org/10.1163/9789004514850

(GDPR).[35] Addressing these challenges requires not only technological innovation and development but also collaboration between stakeholders, including developers, users, regulators and academics, to ensure that Web3 technologies can deliver on their promise of open, free and secure Internet.

VI Conclusion

The rise of information controls by both states and corporations has significantly impacted the landscape of freedom of expression and privacy on the Internet. Over the years, the expansion of centralised power in governance and corporate entities has led to sophisticated mechanisms to monitor, manage and regulate the flow of information online. This has resulted in a paradoxical situation where the Internet, once a bastion of free expression, has become a controlled environment where user data is extensively surveilled and manipulated for profit and power. The evolution of such controls and the risk of growing digital authoritarianism have facilitated the search for alternative models that can restore and protect the fundamental rights of users. Web3, characterised by decentralised blockchain technologies, offers a compelling alternative to the traditional, centralised models that dominate digital spaces. These technologies unsettle traditional data management by distributing transactions and data across a network, thus complicating any attempts at censorship, as in the case of the Turkish ban on Wikipedia or manipulation, as in the Catalan referendum in Spain. The integration of Web3 into mainstream use will, however, require overcoming a set of technical challenges, including scalability, accessibility, interoperability and privacy. Additionally, it will necessitate a concerted effort among a diverse group of stakeholders – developers, users, policymakers and academics – to collaborate in creating a regulatory and operational framework that supports the adoption and growth of decentralised technologies.

[35] The right to be forgotten, enshrined in Article 17 of the GDPR, grants individuals the authority to request the deletion or removal of their personal data under certain conditions. This provision empowers individuals to control their digital footprint by allowing them to erase their data when it is no longer necessary, unlawfully processed, or when they withdraw consent. This right is not, however, absolute and must be balanced against other rights and obligations, such as freedom of expression and legal requirements. See: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.