

POL106 (Contemporary Challenges to Democracy: Democracy in the Social Media Age)

The Decentralized Web: A Research Brief

By Filip Zaleski; 1008241500

2022.04.05

APA 7th Edition

Ins.: Ronald Deibert

T.A.: Yujia Shi

Introduction

In the aftermath of the French Revolution Alexis de Tocqueville, member of the French National Assembly, spoke that the reform was prompted by “a push for decentralization” away from the monarchy (Koritansky, 1975). As such the political ideology of decentralization was born. Much later, in 1992, Osborne and Gaebler published the bestselling *Reinventing Government* which proposed decentralist public administration strategies – this book was the cornerstone of ‘New Public Management’ and the groundwork of modern decentralist theories (Kamensky, 1996).

In modern times, decentralization relates to the process of redistributing the concentration of power or control away from a core agent or authority, towards several more local bodies (Boko, 2002). The widespread application of the idea across various academic fields has shaped different contextual modes decentralization. With regard to the internet, the “decentralized web” is the vision of a system of independent and interconnected computers that coincide to provide safe, censorship-resistant access to information and services (Barabas, Narula, & Zuckerman., 2017) and are free from central intermediaries like governments or businesses. In an op-ed for the REAL LIFE Magazine, Paris Marx invokes the dichotomy between the centralized and the decentralized web (Marx, 2021). According to him, the internet is currently more centralized than it is publicly acknowledged and decentralizing is desirable.

The thesis of this brief is deducted from a stream of research that outlines the positive and negative aspects of both centralized and decentralised systems. This paper will overview research categorized into four key perspectives that help to inform the debate: a more stable internet and the eradication of internet are two advantages of decentralization, whereas the ultimate need for policing and the risk of widening inequality are two drawbacks of that process.

Advantage #1 – A More Stable Internet

Blockchain technology consists of the ledger, a digital and anonymous database facilitating transactions, and the smart contract – a computer protocol that verifies and enforces rules akin to a physical contract (Mohanty, 2018). Blockchain is the trademark of the decentralization movement commonly dubbed ‘Web3’. It is the development of the blockchain that materialized dreams of a decentralized web, because alongside the introduction of the blockchain came the realization that the internet ought not play to the interest of the one controlling body, but can instead work with accordance to public interest. Public interest, in this case, is not just manifested in terms of an end to the exploitation of user data by big businesses (scrutinized later), but also in terms of dispersing the provision of infrastructure that creates the internet. The process of reducing the dependency on privately-supplied internet infrastructure in fact may enhance wider, societal wellbeing – as of now, not just commercially-used digital activities rely on corporate provision of infrastructure, but also governmental processes (Musiani, 2013).

A movement toward decreased dependency on private provision of infrastructure can lower the risk of a collapse or failure of the cyberspace. As it stands, the internet relies heavily on the performance and reliability of the six biggest tech companies – this addiction to the corporate world poses many ethical and practical considerations. For instance, in a massive outage of multiple server systems in October 2021, 3.5 billion people lost access to all of Facebook’s features (Patnaik, Mathews, & Dang., 2021). Evidently, this is a major vulnerability of the current centralised cyberspace and something Web3 promises to change. An example of a technology that aims to decentralize computing power and infrastructural dependence is the Golem Network (GLM), a platform that enables crowdsourced computational power from users with a surplus of computational resources. GLM allows for the leasing of idle hardware in a peer-to-peer method,

“democratizing” access to censorship-resistant processing (Janiuk, 2022). While this project requires further development and popularity within the public, it presently offers a vision for how the cyberspace could move away from intense corporate reliance.

Agents that execute cyber-attacks, financially motivated cybercrime, or cyber espionage make use of internet infrastructure and exploit means of cyber governance like content filtering or blocking measures to achieve mischievous actions (Raymond, 2016). Such activities not only pose risks to user privacy, but may have direct effects on the internet’s stability and interoperability; the ability of computer systems to exchange and make use of information. Many businesses’ easily-penetrable infrastructure or meager, centralized corporate security systems can lead to poorly-executed intrusions that may cause technical problems (Raymond, 2016). The increasing availability of such hacking technologies and spyware with single, centralized targets like Facebook leads to increased reception by actors with low levels of expertise, increasing the prominence of poorly executed disruptions. Furthermore, efforts by businesses to toughen down on intruders and “harden” communication platforms sacrifices the openness of such applications to users, leading to a network resembling a “cyber Westphalia” (Raymond, 2016). Escalating cycles of retaliation by corporate hosts often cause service interruptions that impact innocent third-party users such as student bodies. Web3 could mitigate the detriments of centralized internet infrastructure and computing by creating an untraceable, universal architecture of unbreachable data inaccessible to external actors (Fowler, 2021).

Advantage #2 – An End to Surveillance Capitalism

Decentralising the provision of computational infrastructure is a movement that brings the internet closer to its intended origins. Originally, the internet’s decentralised architecture became a manifestation of its ethos and purpose: to provide all users with the opportunity to publish and

share information without central intermediaries (Marx, 2021). The gradual public dependency on corporate infrastructure, however, allowed technology conglomerates to leverage abuses of user data and imperfections in website design on the provision of service. Easy exploitation of such vulnerabilities made platforms like Twitter or Facebook “vectors for disinformation and conspiracy, conditions that have altered democracy, perhaps forever” (Bogost, 2020).

The fact that digital technology companies have generated trillions of dollars of wealth and hugely contributed to the growth of many economies over the last forty years cannot be disputed. The principle of “permissionless innovation” under a profit-driven incentive has been central to the rapid global spread of the internet and its economic potential, though this same principle is responsible for the hindered stability and security of the global cyberspace (Raymond, 2016). Online advertising is responsible for shaping the internet into something Mike Liebhold, a senior fellow at the Institute for the Future, calls “a stalker economy” (Liebhold, 2016). Liebhold emphasizes that the dependence on ‘big tech’ has created a cyberspace laden with personal data mining, indefensible corruption of financial and identity networks, and an omnipresent infiltration of political and military hardware and software. Decentralizing the internet would not only end the cycle of abuse of user data, but also the pseudo-consensual nature of agreements between user and provider (Deibert, 2022).

The intrusive potential of surveillance capitalism and firms’ desire to create all-encompassing models of individuals compels providers to not only maximise their collection of information, but also surpass traditionally-viewed, ‘ethical’ types of consumer data (Zuboff, 2019). Shoshana Zuboff’s pivotal *The Age of Surveillance Capitalism* outlines the vicious, profit-driven cycle of acquiring increased quantities and types of user data through surveillance-friendly techniques, hidden default preferences, and unwitty site architecture that extracts user consent (Zuboff, 2019).

User data collection has also moved beyond digital statistics and into the physical world with location data, speech recordings, and measures of fitness activity (Zuboff, 2019). The commodification of personal data has occurred parallel to the erosion of privacy (Kasper, 2005), and modern-day online consumers often no longer have access to the data gathered about them. The desire to maximise payoff from data predictions has quickly turned into mechanisms actively influencing behaviours – it is at this point that surveillance capitalism undertakes a dark and “novel” character (Zuboff, 2019). Zuboff wrote about decentralized internet systems as plausible structures of resistance against the perils of surveillance capitalism (Zuboff, 2019). By enabling end-to-end interoperability between users, for instance, decentralized solutions allow private information to be shared securely, with users remaining in total control of their data (Shrestha, Vassileva, & Deters, 2020).

Decentralized networks and the applications built on top of them create opportunities for the redistribution of economic benefits of data monetization away from surveillance capitalists and towards the actual owners of data. Platforms such as GLM invoked earlier open up novel avenues for all users to generate alternative income from underutilized, unproductive, or inefficient assets such as computing power. Under GLM, user has the ability to lease out their computing infrastructure during inactive periods – employing such a system would be a way to redistribute the plethora of wealth currently held by technology conglomerates, as well as decreasing the reliance on corporate infrastructure. Alternate methods of monetizing data and correcting the surveillance capitalist norm of gathering revenue already exist. The *Brave* browser application prioritizes user control over data tracking, allowing users to reward publishers or content creators with money depending on the time spent on websites (Hayes, 2022). Such *Basic Attention Tokens* are one of the new currencies created by the growing decentralized economy fueled by the

blockchain, and offer an insight into a alternative revenue model – one free from corporate data abuse and privacy infringement.

Drawback #1 – The Necessity for Policing

It is a reasonably intuitive statement that unregulated digital bodies, ones without a ‘centralised’ authority to maintain law, are prone to outbreaks of crime and corruption. Software champions using totally free speech and absolutely no censorship as their marketing agenda have many times seen the consequences of unregulated user exchange. In the dawn of the 2016 Presidential election, ‘4Chan’ users conspired on the platform and deliberately shut down Hilary Clinton’s phone lines, negatively impacting her campaign (Brandom, 2016). And it is not just malign, unregulated expression between users that decentralization may spur. Increasingly common investigations into cryptocurrency show that criminal bodies use digital currencies to launder dirty money, exploiting the anonymity of the blockchain (Irrera, 2020). In a journal article, David Davenport argues that contrary to the common doctrine of the decentralisation movement, ensuring universal anonymity to users poses risks to the ‘fabric of our society’ by dissolving accountability (Davenport, 2002). Davenport contends that unless individuals, firms, and governments can be held accountable, all users lose recourse to the law and hence subdue their freedom and order. The author importantly explains that accountability in democratic societies is the mechanism by which we punish misconduct and prevent future offenders from violating the rights of others – if users are to become anonymous and free of accountability, Web3 may cause virtual lawlessness.

Advocates of Web3 must begin to recognize that the eradication of a central authority with regulatory power has the trade-off in the form of increased freedom for criminal activities, though the effectiveness of regulation must improve. As Professor Ronald Deibert has stated, governments hitherto have performed poorly in regulating social media, though surveillance is necessary and

the public ought not be discouraged by the futility of recent government regulatory efforts (Deibert, 2022). If the internet is to head toward decentralization, governments should abandon the pervasion of users' data via digital espionage and create effective systems of policing that are un-invasive and compatible with contemporary visions of the internet. Already, state authorities seem to succeed in infiltrating blockchain technology – the FBI managed to track and intercept most of the Bitcoin ransom paid in the Colonial Pipeline ransomware attack of May 2021 (Perlroth, Griffith, & Benner., 2021).

The need for centralized oversight of the cyberspace is evident if law and order is to thrive. A government with neutral interest can achieve this cause. Nevertheless, many might find the prospect of governments controlling people's data to be somewhat Orwellian (Line et. al., 2020). Already, widespread surveys indicate that Americans' trust for both businesses and governments keeps decreasing ('Edelman', 2021). This is a grave obstacle in the formation of a healthy state-run monitoring system that is to be free of abusive corporate surveillance. If decentralization is to take a desirable, hybrid form, it seems that alongside the actual change in the structure of the cyberspace there must be a shift in public consensus that would accommodate the need for state monitoring. A government that wishes to regulate the internet must remain communicative with the public about its regulatory objectives and the means it will use to as to prevent public outlash and the abuse of state power (Bailey, 2012). As of now, the U.S. government has been isolating the public from regulatory discourse – a factor behind the recent ineffectiveness of digital regulation (Bailey, 2012).

Drawback #2 – The Risk of Widening Inequality

The common supposition that a decentralized web would rid the digital world of corruption and inequality requires more scrutiny than discourse commonly admits. In a peer-reviewed book

published by the World Bank, Manor (1999) wrote that in states characterised by powerful local elites, decentralization risks the capture of resources by those groups. The inegalitarian nature of the democratic world is currently supported by thorough multivariate research: a 2022 report by the World Inequality lab, a renowned institution at the Paris School of Economics, indicates that the globe's top 10% of earners own 76% of all wealth (Chancel et. al, n.d.). And inequality is rising each year. This inequality permeates the current state of the internet and, according to James Manor, there is no reason to believe it will not bedevil Web3. Warnings about an unequal future of the decentralized web can already be affirmed when looking at some decentralized technologies of today. In 2021, Sai et. al. underwent a research process measuring wealth distribution within eight major cryptocurrencies. The team's analysis demonstrates that despite the strong emphasis decentralization-based narrative behind cryptocurrencies, wealth inequality within these digital assets closely mirror the inequality present in real world economies. A subsidiary finding reveals that in the case of three cryptocurrencies analysed, less than 100 buyers own fifty one percent of the wealth, potentially signifying a security threat. Sai et. al.'s research helps in the observation that the 'free-market fundamentalist' doctrine of Web3 may be inadequate in countering wealth inequality online. This is a crucial discovery because one of the key objectives of Web3 is the reduction of the "digital divide", including the access and control of financial services, assets, and currencies (Harrisberg, 2021). The challenges of internet decentralization and inequality turn out to be intricate; on one hand, inequality is likely to persist – on the other, if elites find their dominance will be hindered by digital secession, they are likely not to support, and even oppose, efforts of such cause in the first place (Faguet, Fox, and Pöschl., 2014).

The detrimental impact of decentralized infrastructure on low-income communities is a risk certainly worth noting. Howson & de Vries (2022) outline that the "unsustainable trajectory" of

the blockchain disproportionately impacts poor and vulnerable communities where cryptocurrency miners and other actors take advantage of economic instabilities, frail regulation, cheap energy, and other resources. The researchers argue that if the adoption of publicly-sourced, energy-devouring assets like bitcoin is to continue rapidly increasing, a dramatic worsening of the climate crisis will loom. This, clearly, can deepen the struggle of impoverished communities that are always most severely influenced by climate change and already suffer “multiple dimensions of deprivation” (Howson & de Vries, 2022).

An increasing number of scholars are coming to the realization that a benign future for the internet is a future not with total decentralization but with considerable government intervention: with policing, as mentioned earlier, but also with the control of physical and digital technology. A 2018 special report for *The Economist* mentioned the warnings of Feng Xiang, a prominent legal scholar at Tsinghua University, who explained that if artificial intelligence (a pivotal driver of surveillance capitalism) is to be controlled entirely by free market forces, “it will inexorably result in a super-rich oligopoly of data billionaires” who will continue to reap the wealth (*‘The Economist’*, 2018). Xiang emphasises that this would hurt the labour market as well as increasing unemployment. As a solution, the scholar proposes a semi-centralised digital system in which the government would impartially ensure that “AI serves society instead of private capitalists”, maximizing benefit for all. The use of AI in fields like medicine (Ramesh et. al., 2004) should contain some level of government control as to allow an affordable presence of this technology in the vital health care sector. Another example is the educational system, where algorithms that calculate performance ought to be functional and neutral – the government can regulate and monitor this (Galaski, 2021). The enhancement of the government's role in the regulation and control of digital technology with the aim of preventing inequities in power is an interesting proposal for those Paris Marx called

'cyberoptimists'. It is yet another argument for why a regulatory vacuum under a decentralized web is undesirable.

Concluding Remarks

The intricacies of a switch to a decentralized internet are multiple – an issue involving virtually the entire world population and with such immense societal implications inevitably has both positive and negative interpretations. This brief helps to illuminate the principal perspectives one may encounter when scrutinizing the debate. The decreased reliance on corporate infrastructure and a possibility to eradicate the malicious repercussions of surveillance capitalism are certainly two strong arguments for a widespread support of Web3. However, the need for digital policing as well as the issue of rising inequality enabled by a decentralised cyberspace are risks that ought not to be ruled out. It is also critically important to remember that as much as the positive and negative aspects of the decentralization movement seem polarizing and severe, many key nuances and shortcomings of the current digital ecosystem as well as the structure and objectives of major players are not entirely understood (Alsahli, 2022). It is for this reason that more research and an intricate evaluation of the weaknesses of our digital spaces are necessary if society is to effectively decide on the future of the internet.

Bibliography

- 2021 *Edelman Trust Barometer*. Edelman. (2021). Retrieved March 30, 2022, from <https://www.edelman.com/trust/2021-trust-barometer>
- Alsahli, A. (2022). Hawaii International Conference on System Sciences. In *ResearchGate*. Honolulu. Retrieved April 4, 2022, from https://www.researchgate.net/publication/357740344_Uncertainty_in_Digital_Platforms_and_Ecosystems_The_Dynamic_Interplay_Between_Knowledge_Problems.
- Bailey, R. (2012). Censoring the Internet: The New Intermediary Guidelines. *Economic and Political Weekly*, 47(5), 15–19. <https://doi.org/https://www.jstor.org/stable/41419840>
- Barabas, C. , Narula, N., & Zuckerman, E. (2017). Defending Internet Freedom through Decentralization: Back to the Future? *Media & Information Literacy*. Retrieved April 5, 2022, from http://dci.mit.edu/assets/papers/decentralized_web.pdf.
- Bogost, I. (2020, July 26). *So Much for the Decentralized Internet*. The Atlantic. Retrieved April 1, 2022, from <https://www.theatlantic.com/technology/archive/2020/07/twitter-hack-decentralized-internet/614593/>
- Boko, S. H. (2002). Decentralization: Definitions, Theories and Debate. *Decentralization and Reform in Africa*, 1–10. https://doi.org/10.1007/978-1-4615-1111-3_1
- Brandom, R. (2016, November 8). *4chan May Have Brought Down Pro-Clinton Phone Lines the Day Before the Election*. The Verge. Retrieved March 30, 2022, from <https://www.theverge.com/2016/11/8/13562868/4chan-clinton-election-hack-phone-dialer-ddos>
- Chancel, L., Piketty, T., Emmanuel Saez, & Zucman, G. (n.d.). *World Inequality Report 2022*. Retrieved March 31, 2022, from <https://wir2022.wid.world/>
- Davenport, D. (2002). Anonymity on the Internet: Why the Price May be Too High. *Communications of the ACM*, 45(4), 33–35. <https://doi.org/10.1145/505248.505267>
- Deibert, R. (2022, February 12). *Targeted Digital Espionage*. MyMedia. Retrieved March 30, 2022, from <https://play.library.utoronto.ca/watch/3402e5685f341ea5f4dcadd0d124df5>
- Deibert, R. (2022, January 21). *To Consent or Not*. MyMedia. Retrieved April 1, 2022, from <https://play.library.utoronto.ca/watch/022b9a5e9a187854996d6380adaa5384>
- The Economist Newspaper. (2018, June 28). *China has the World's Most Centralised Internet System*. The Economist - Special Report. Retrieved April 1, 2022, from <https://www.economist.com/special-report/2018/06/28/china-has-the-worlds-most-centralised-internet-system>

- Faguet, J.-P., & Pöschl Caroline. (2015). *Is Decentralization Good for Development?: Perspectives from Academics and Policy Makers*. Oxford University Press.
- Fowler, G. (2021, April 7). *Taking a Decentralized Approach to Cyber Security, Data Protection and Privacy*. Forbes. Retrieved April 4, 2022, from <https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/04/07/taking-a-decentralized-approach-to-cyber-security-data-protection-and-privacy/?sh=5d61398b5601>
- Galaski, J. (2021, September 8). *AI Regulation: Present Situation and Future Possibilities*. Liberties. Retrieved April 5, 2022, from <https://www.liberties.eu/en/stories/ai-regulation/43740>
- Harrisberg, K. (2021, December 3). *Bridging Africa's Digital Divide: The Rise of Community internet*. World Economic Forum. Retrieved April 1, 2022, from <https://www.weforum.org/agenda/2021/12/bridging-africas-digital-divide-the-rise-of-community-internet/>
- Hayes, A. (2022, February 14). *Basic Attention Token (BAT)*. Investopedia. Retrieved April 4, 2022, from <https://www.investopedia.com/terms/b/basic-attention-token.asp>
- Howson, P., & de Vries, A. (2022). Preying on the poor? opportunities and challenges for tackling the social and environmental threats of cryptocurrencies for vulnerable and low-income communities. *Energy Research & Social Science*, 84, 102394. <https://doi.org/10.1016/j.erss.2021.102394>
- Irrera, A. (2020, December 9). *Criminals getting smarter in use of digital currencies to Launder Money*. Future of Money. Retrieved March 30, 2022, from <https://www.reuters.com/article/crypto-currencies-criminals-idUSKBN28J1IX>
- Janiuk, P. (2022, March). *Golem Network: Peer-to-Peer Computing Power*. Cryptopedia. Retrieved April 1, 2022, from <https://www.gemini.com/cryptopedia/golem-network-peer-to-peer-computing-power>
- Kamensky, J. M. (1996). Role of the "Reinventing Government" Movement in Federal Management Reform. *Public Administration Review*, 56(3), 247–255. <https://doi.org/10.2307/976448>
- Kasper, D. V. (2005). The Evolution (Or Devolution) of Privacy. *Sociological Forum*, 20(1), 69–92. <https://doi.org/10.1007/s11206-005-1898-z>
- Koritansky, J. C. (1975). Decentralization and Civic Virtue in Tocqueville's "New Science of Politics." *Publius: The Journal of Federalism*, 5(3), 63–81. <https://doi.org/10.1093/oxfordjournals.pubjof.a038366>

- Liebhold, M. (2014). *Inventing a New Internet: Learning from Icarus*. Institute for the Future. Retrieved March 30, 2022, from <https://www.iftf.org/our-work/global-landscape/ten-year-forecast/inventing-a-new-internet/>
- Line, N. D., Dogru, T., El-Manstrly, D., Buoye, A., Malthouse, E., & Kandampully, J. (2020). Control, use and ownership of Big Data: A reciprocal view of customer big data value in the hospitality and tourism Industry. *Tourism Management*, 80, 104106. <https://doi.org/10.1016/j.tourman.2020.104106>
- Manor, J. (1999). *The Political Economy of Democratic Decentralization*. World Bank.
- Marx, P. (2021, July 26). *Reconnected*. REAL LIFE. Retrieved March 30, 2022, from <https://reallifemag.com/reconnected/>
- Mohanty, D. (2018). THE WORLD OF BLOCKCHAIN. *India International Centre Quarterly*, 45(3/4), 196–203. <https://doi.org/https://www.jstor.org/stable/45129865>
- Musiani, F. (2013). Dangerous Liaisons? Governments, Companies and Internet Governance. *Internet Policy Review*, 2(1). <https://doi.org/10.14763/2013.1.108>
- Patnaik, S., Mathews, E., & Dang, S. (2021, October 4). *Facebook blames 'faulty configuration change' for nearly six-hour outage*. Reuters. Retrieved April 1, 2022, from <https://www.reuters.com/article/facebook-outages-idCAKBN2GU1TV>
- Perlroth, N., Griffith, E., & Benner, K. (2021, June 9). *Pipeline Investigation Upends idea that Bitcoin is Untraceable*. The New York Times. Retrieved March 31, 2022, from <https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html>
- Ramesh, A. N., Kambhampati, C., Monson, J. R., & Drew, P. J. (2004). Artificial Intelligence in medicine. *Annals of The Royal College of Surgeons of England*, 86(5), 334–338. <https://doi.org/10.1308/147870804290>
- Raymond, M. (2016). Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot. *Strategic Studies Quarterly*, 10(4), 123–149. Retrieved April 4, 2022, from <https://www.jstor.org/stable/26271532>.
- Sai, A. R., Buckley, J., & Le Gear, A. (2021). Characterizing Wealth Inequality in Cryptocurrencies. *Frontiers in Blockchain*, 4. <https://doi.org/10.3389/fbloc.2021.730122>
- Shrestha, A. K., Vassileva, J., & Deters, R. (2020). A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives. *Frontiers in Blockchain*, 3. <https://doi.org/10.3389/fbloc.2020.497985>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs. Retrieved from

<https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/>.