The Internet Is Dead: Long Live the Internet

George Zarkadakis

Abstract Social exclusion, data exploitation, surveillance, and economic inequality on the web are mainly technological problems. The current web of centralized social media clouds delivers by design a winner-takes-all digital economy that stifles innovation and exacerbates power asymmetries between citizens, governments, and technology oligopolies. To fix the digital economy, we need a new, decentralized web where citizens are empowered to own their data, participate in disintermediated peer-to-peer marketplaces, and influence policy-making decisions by means of innovative applications of participatory and deliberative democracy. By reimagining “web 3.0” as a cloud commonwealth of networked virtual machines leveraging blockchains and sharing code, it is possible to design new digital business models where all stakeholders and participants, including users, can share the bounty of the Fourth Industrial Revolution fairly.

The internet is almost 50 years old.¹ It has transformed our world and has provided new and exciting opportunities to business, society, science, and individuals; but it has also ushered an era of greater inequality, surveillance, exclusion, and injustice. The first iteration of the internet (“web 1.0”) was a network of organizational servers where individual PCs were connected intermittently via dial-up modems. This evolved into the current mobile internet (“web 2.0”) that consists of many centralized social-network clouds that suck user data like black holes. As such, web 2.0 has enabled the land-grabbing business models of the Big Tech oligopolies. An unfair

Why do we need a new internet to democratize the digital economy and enhance participatory governance?

¹https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=January%201%2C%201983%20is%20considered,to%20communicate%20with%20each%20other.&text=ARPANET%20and%20the%20Defense%20Data,the%20birth%20of%20the%20Internet

G. Zarkadakis (✉)
Atlantic Council, Zug, Switzerland
e-mail: gzarkadakis@atlanticcouncil.org

distribution of power has thus emerged whereby our data are gathered, analyzed, and monetized by private companies while we accept cookies in a hurry. Today's digital economy is a rentier's wet dream come true. We have become serfs in the digital fiefdoms of the techno-oligarchs, tenants, instead of co-owners, of the enormous economic value that we generate through our digital avatars. Add the march of AI systems that automate our jobs, and what you get is the social contract of liberal democracy being torn to pieces. If we continue with business as usual, the future will be one of massive unemployment, dislocation, and the end of dreams. The Global Financial Crisis offered us a glimpse of what that means: populism, mistrust in democracy, conspiracy theories, polarization, hate, racism, and a dark replay of the 1930s. The COVID-19 pandemic has further exacerbated the political and economic asymmetries of a digital economy that works only for the few. "Working from home" sounds good until you realize that your job can now be outsourced anywhere in the world, at a much lower cost. Virtualization of work equals labor arbitrage enabled by web 2.0 and Zoom calls.

1 Perils of an Ornithopter Approach

Faced with the danger of their historical obliteration, democracies are gearing up for a fight. Proposals range from breaking up the tech oligopolies, taxing them more, expanding welfare to every citizen via a universal basic income, and enacting stricter data privacy laws. The defense strategy has a noble purpose: to reduce the power and influence of the techno-oligarchs.

But the usual means of defending democracy by legislating and regulating are insufficient and inefficient to deal with the magnitude and nature of this particular problem. Instead of a viable and sustainable solution, they will create new bottlenecks, more paperwork, more centralized control, and more loopholes to be exploited by influential and well-funded lobbies. At the end, regulation shifts power to governments, not citizens. We, the citizens, will be replacing one master with another. The strategy of increasing the role of the State in order to deal with inequality in the digital economy is wrong and will fail. Our problem is technological, not regulatory. Like the early aviators, we are trying to leave the ground using wings that cannot fly. And just as you cannot regulate an ornithopter to reach the stratosphere, so it is with the current internet: to make the digital economy fairer, trustworthy, and more inclusive, we need a different technology, another kind of internet.

But what would that "alternate" internet look like? And what should its fundamental building blocks be? Perhaps the best way to think about these questions is to begin by asking what is wrong with the current technology. I would like to argue that there are three main problem areas that we need to focus in order to reinvent the internet: data ownership (and its necessary corollary, digital identity), security, and disintermediation. Let's take those areas in turn and examine them further.

2 Data Ownership and the Need of a Digital Identity

Data ownership is perhaps the biggest problem area of all. Ownership goes beyond self-sovereignty. It suggests property rights for the data, not just the right to allow permission for their use. We need to own our personal data as well as the data that we generate through our social interactions, actions, and choices. Our data is the most valuable resource in the digital economy. They are powering the AI algorithms that animate the wheels of the digital industries. When those algorithms finally replace us in the workplace, our data will be the only valuable resource for which we can legitimately claim a share in the bounty of the Fourth Industrial Revolution. Many initiatives, such as Sir Tim Berners-Lee's [Inrupt](#) project (Lohr 2021), are trying to work around the current web and provide ways for some degree of data ownership while building on existing web standards. However, by addressing only one of the three problem areas, they are only partial solutions. A more radical approach is necessary by establishing immutable, verifiable, digital identity systems as secure and trusted ways to identify every actor connected on the internet, including humans, appliances, sensors, robots, AIs, etc. Data generated by an actor would thus be associated with their digital identity and thus establish ownership rights. So, if I am a denizen of the alternate internet, I can decide what pieces of my data I will make available, to whom, and under what conditions. For example, if I need to interact with an application that requires my age, I will only allow that piece of data to be read by the application and nothing else. I can also decide on a price for giving access to my data to a third party, say to an advertising agency or a pharmaceutical company wishing to use my health records for medical research. Or I can decide to join a data cooperative, or a data trust (Zarkadakis 2020a), and pool my data with other people's data, include perhaps data from smart home appliances and smart city sensors, and thus exponentially increase the collective value of the "shared" data value chain. Digital identities can enable auditable data ownership from which we could engineer an equitable income for citizens in an AI-powered economy of material abundance. As we look for sustainable and meaningful funding for a universal basic income, data ownership based on digital identity may be the key solution. A "universal basic income" that is funded by economic activity would relieve governments from having to excessively tax and borrow. More importantly perhaps, it would be income earned, not "handed out," and as such would uphold – rather than demean – human dignity and self-respect.

3 Security

The current internet is highly susceptible to cyberattacks – such as Denial of Service (DoS) – because its architecture requires applications to be centralized and their data to be relayed via central servers, rather than exchanged directly between devices. Servers are thus single points of failure and attack that are candy for malevolent

hackers. Centralization of data in the current internet is also the cause of data breaches, regulatory fines, reputational risk, and consumer mistrust. Given these inherent shortcomings, the cyber security arms race is forever unwinnable. In the alternate internet, applications should be peer-to-peer, decentralized, and communicate directly with each other. They should run on virtual machines that use an operating system and communication protocol built on top of the fundamental TCP/IP protocol and run on the individual device, say a smartphone. If they fail, or are attacked, the damage will be minimal and restricted rather than spreading across the whole of the network. Moreover, such an operating system could render that alternate internet as a single, global computer, made up of billions of nodes. It will be the realization of the original internet dream: a completely decentralized and secure global network of trust, where there can be no surveillance.

4 Disintermediation

Security is not the only negative outcome of the centralized nature of web 2.0. All services are currently intermediated by default, and that includes essential services such as data storage and computing resources. It is the reason why [only four companies control 70% of the world's cloud infrastructure](#) (Cohen 2021). Regardless of what one may think of Donald Trump, the fact that Twitter, a private company, could silence a sitting US President ought to give pause to anyone who cares about free speech. Like Twitter, many other private social media platforms such as Facebook and YouTube have assumed the high office of unelected arbiters of what is true and permissible, replacing the role of legislatures, courts, and governments. Intermediation is also responsible for the fact that internet content can be monetized almost exclusively using an advertising business model, which is what social media platforms are exploiting in order to make their billions. If you are a content creator today, you need to satisfy advertisers with high numbers of followers and hits, which impacts both what content you can create and how you deliver it. The tiny minority of individual content creators who get this combination right and manage to earn some meaningful income from their work are then subject to the whims of the social media platforms that host their content. We must disintermediate and decentralize the internet if we want human creativity and innovation to flourish. In the alternate internet, content creators do not need the advertising industry to earn income; they can monetize their content in disintermediated, peer-to-peer markets, through micropayments paid to them directly by the consumers of their content. Moreover, infrastructure can also be disintermediated, and every node in the network can provide data and computing services and resources. A decentralized internet at global scale will provide new sources of income for billions of people. Just imagine anyone connecting to that internet via their smartphone or laptop and making available data storage and computing as part of a “cloud commonwealth.”

5 The Rise of a New, Decentralized Web

We are already witnessing the dawn of the new internet, often referred to as “web 3.0.” Distributed ledger technologies are providing new ways to establish disintermediated trust in peer-to-peer marketplaces, as well as new ways to reimagine money and financial assets. Smart contracts automate transactions and provide auditing on supply chains, banking, and insurance, while non-fungible tokens (NFTs) are transforming the internet of information into the internet of assets and enable content creators and digital artists to sell their creations, just as they would if they were made of atoms instead of bits.

In the web 3.0, individual users are connected directly, peer-to-peer, without centralized clouds. They may exchange content and other digital assets as NFTs that are executable applications. To achieve this, we must empower users with personal cloud computers (PC2), i.e., software-defined personal computers, to store and process their data. When users are ready to swap or trade their data, they can compile data into NFT capsules (encrypted, self-extracting, self-executing programs that encapsulate the data), much like people generate PDF files from Word documents today. And they will then share those capsules on a content delivering network running on a blockchain and verified by miners, instead of centralized cloud servers. The web 3.0 will, in effect, be a peer-to-peer web of personal cloud computers.

Many engineers and developers are already working on realizing the new internet. For example, the [Elastos Foundation](#) is developing a full range of tools and capabilities for web 3.0 application developers, so they may begin to code decentralized applications on the new web. All this is happening on open-source platforms in the true spirit of sharing knowledge and collaborating on projects. Which is exactly what is different in the mindset of the new digital world: success, innovation, and economic value can be derived from collaboration, not just competition, and from co-creating equitable ecosystems, not enforcing inequitable oligopolies.

6 Participatory Public and Private Governance

There is an additional prize to be won from transitioning from web 2.0 to web 3.0. A decentralized web based on digital identity, data ownership, and a peer-to-peer cloud commonwealth will bring new possibilities for digital business models that are inclusive and democratically governed, much like cooperatives of mutual ownership companies. Ethereum was first to experiment with “decentralized autonomous organizations” (DAOs) that can blend direct and representational democracy in private governance. However, similar models of democratic digital governance can also be adopted in the public domain by a city, a county, a region, or a nation state or in circumstances where citizens need to manage commons ([Zarkadakis 2020b](#), p. 140).

In a society where every citizen has a verifiable and decentralized digital identity, there can be no surveillance – state or private – only liberty and personal responsibility. Citizens can freely associate in the cyberspace, transact, create, innovate, debate, learn, and self-develop. Because their identity is verifiable and trusted, they are incentivized toward socially responsible behavior and consensus. The decentralized web 3.0 can be the foundation of a truly digital “polis” in cyberspace. In such a democratic polis, free citizens own their data and contribute through their interactions, knowledge, skills, networks, and choices to the creation of economic value in inclusive digital platforms, value that is then shared fairly among all those who have contributed on the basis of their contribution. Moreover, participatory forms of public governance can be enacted by institutionalizing citizen assemblies in liberal democracies and include citizen views and recommendations in the policy-making processes of legislatures. The future does not have to be a dystopia of oppression, surveillance, endemic penury, and dependency on central government control and welfare. A new internet of equitable opportunities can help us overcome the dire straits of societal polarization and injustice and let democracy, freedom, and liberty reclaim their civilizing influence on human nature.

References

- Cohen J. (2021) ‘Four Companies control 67% of the world’s cloud infrastructure’, *PC Magazine*, [online]. Available at: <https://uk.pcmag.com/old-cloud-infrastructure/131713/four-companies-control-67-of-the-worlds-cloud-infrastructure> (Accessed: 18 May 2021)
- Lohr, S. (2021) ‘He created the internet. Now he’s out to remake the digital world’, *New York Times*, [online]. Available at: <https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html> (Accessed: 18 May 2021)
- Zarkadakis, G. (2020a) ‘Data Trusts could be the key to better AI’, *Harvard Business Review*, [online]. Available at: <https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai> (Accessed: 18 May 2021)
- Zarkadakis, G. (2020b) *Cyber Republic: reinventing democracy in the age of intelligent machines*, Cambridge: MIT Press.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.