

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/358070926>

Towards Re-Decentralized Future of the Web: Privacy, Security and Technology Development

Article in *Acta Informatica Pragensia* · January 2022

DOI: 10.18267/j.aip.169

CITATIONS

0

READS

155

2 authors, including:



Stanislav Vojtíš

Prague University of Economics and Business

21 PUBLICATIONS 69 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



EasyMiner.eu - web framework for interpretable ml: associations, classification, anomaly detection [View project](#)

Towards Re-Decentralized Future of the Web: Privacy, Security and Technology Development

Stanislav Vojř , Jan Kučera

Faculty of Informatics and Statistics, Prague University of Economics and Business, W. Churchill Sq. 1938/4, 130 67 Prague 3, Czech Republic

Corresponding author: Stanislav Vojř (stanislav.vojir@vse.cz)

Abstract

The World Wide Web (the Web) has become part of people's daily lives. Although the Web, like the Internet itself, was designed as a decentralized network, hand in hand with the increase in its interactivity Web users gradually concentrated on a limited number of platforms. As a result, providers of these large international platforms have become centres of power that can easily influence users' behaviour and what information they can access. This paper is based on an integrative literature review and its aim is to describe the development of the Web from its beginnings to the present. This development is viewed from the perspective of centralization of the Web and the reactions that this centralization has provoked, especially the current trends towards the so-called re-decentralized Web. More specifically, the paper focuses on the privacy imperative that might act as a driving force for the re-decentralized Web, and on the technological innovations enabling development of truly decentralized platforms and applications. This paper contributes to the discussion of implications that a wider adoption of the re-decentralized Web could bring in the near future.

Keywords

Web 3.0; Decentralized Web; Re-decentralized Web; Blockchain; Internet studies; Cloud feudalism; Platform capitalism; Social informatics; Web communities.

Citation: Vojř, S., & Kučera, J. (2021). Towards Re-Decentralized Future of the Web: Privacy, Security and Technology Development. *Acta Informatica Pragensia*, 10(3), 349–369. <https://doi.org/10.18267/j.aip.169>

Special Issue Editors: Vasja Vehovar, University of Ljubljana, Slovenia
Zdenek Smutny, Prague University of Economics and Business, Czech Republic
Alice R. Robbin, Indiana University, USA

Academic Editor: Stanislava Mildeova, University of Finance and Administration, Czech Republic

Copyright: © 2021 by the author(s). Licensee Prague University of Economics and Business, Czech Republic.
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (CC BY).

1 Introduction

More than thirty years ago, the World Wide Web (WWW, shortly the Web) was introduced as a service designed for sharing information over the Internet (Hiremath and Kenchakkanavar, 2016). Since then, it has evolved into an indispensable part of the digital economy. From a service used by a limited number of institutions, it has evolved into a phenomenon used daily by masses in every part of the world. Despite the continuous development of the Web technologies, the importance of the Web to individuals, businesses, institutions and states today makes it an undeniable socio-economic phenomenon. This broader understanding of the Web reveals more diverse structures and dynamics than what could have been otherwise observed at just the technological level.

The Web was designed as a decentralized network. However, according to World Wide Web Foundation (2018) *“billions of people experience the World Wide Web through a small handful of huge companies”*. Large numbers of users, regardless of whether they are individuals, companies, or institutions, either use or interact with each other through platforms or services provided by a relatively small number of providers. For instance, search engines (e.g., Google, Bing), social networks (e.g., Facebook, Twitter, YouTube) or digital marketplaces (e.g., Amazon) represent such services provided by international companies that have been able to attract very large user bases. Barabas et al. (2017) point out that the Web *“needed to consolidate around a few curated service platforms in order to become practical for everyday people to use”*.

On the one hand, consolidation of the Web around a small number of platforms or services has helped to make the Web easier to use. On the other hand, because of this consolidation the Web *“centers on a small number of points of control”* (Barabas et al., 2017). As a result, the platform or service providers owning these points of control have developed significant power allowing them to influence, or even control, the Web's content and who can access it. Despite its decentralized technological architecture, the Web shows signs of centralization nowadays (Verborgh, 2020).

The aim of this paper is to discuss the current perspectives on one of the streams in the recent development of the Web which could be described as its re-decentralization (Barabas et al., 2017; Verborgh, 2020). More specifically, this paper tries to place the so-called re-decentralized Web in the context of the Web's evolution. Thus, the first objective of the paper is to describe how the Web has evolved from its initial idea and technical implementation to the socio-technical phenomenon as it is experienced today. The second objective of the paper is to discuss consequences of centralization of the Web. Our aim is not to provide a comprehensive overview of such consequences but rather to highlight some notable examples illustrating how centralization of the Web impacts individuals, organizations, or societies. As with any other action, centralization of the Web has triggered reaction. Therefore, the third objective of the paper is to describe initiatives that could be viewed as responses to centralization of the Web.

Research presented in this paper was inspired by an analytical report by Barabas et al. (2017) and by a research paper by Verborgh (2020). Compared to those works, this paper provides a more detailed description of the evolution of the Web and it tries to put the consequences of centralization of the Web, as well as responses to this phenomenon, in the context of this evolution. This paper also extends and updates the previously published conference paper by Vojíř, Smutný and Kučera (2020). Besides the above-mentioned perspective of the Web's evolution, the contribution of this paper lies in a wider range of activities, initiatives and technical solutions discussed herein.

The paper is organized as follows. The research methodology is described in the next section. Section 3 focuses on the evolution of the Web. The next two sections describe the centralization tendencies on the Web, their consequences and reactions caused by the centralization. Section 6 presents two main forces supporting re-decentralization of the Web. The last section presents the conclusions.

2 Research Methodology

Re-decentralized Web represents an effort to return to the original ideas of the Web as an open space, where everyone can freely publish their content and decide on use of their data (Verborgh, 2020). The re-decentralized Web can still be considered an emerging topic. Therefore, this paper is based on an integrative literature review. According to Torraco (2005), this style of research is particularly useful for new or emerging topics. The subject of the research is the Web and its evolution, which involves centralization and re-decentralization of the Web as two opposing tendencies. The research is also focused on consequences of centralization of the Web, and on responses to this tendency. These responses represent a wider context in which re-decentralization of the Web takes place.

The following citation and full-text databases were searched for the relevant literature: Web of Science, Scopus, Google Scholar, EBSCO, ACM Digital Library, and IEEE Xplore Digital Library. The databases were queried using the following keywords: re-decentralized web, decentralized web, re-decentralization, decentralized web, decentralization, decentralized technology, privacy, cryptography, Big Tech regulation, social web, society, web 2.0, web 3.0, blockchain applications, and web platform. These keywords were further expanded as more phenomena were identified (e.g., cloud feudalism, platform capitalism, deplatforming, Digital Markets Act). The research presented in this paper is based on the approach previously used in the conference paper of Vojříř et al. (2020). However, the scope of the research was extended significantly, additional key words were used and current trends were reflected.

The literature reviewed in the paper can be found in the reference section. The authors mainly focused on review articles and books relevant to the discussed phenomena. Because of the rapid development in the field of the Web, the research cannot be limited to a review of academic literature. Up-to-date information found on the open Web was also analysed, especially status information about relevant projects, activities of organizations and working groups, and information about relevant policies and regulations.

3 Evolution of the Web

Nowadays, the term "Web" is already well known. From the users' point of view, this is one of the most common uses of the Internet. From an economic and social point of view, the Web is an important environment in which people spend both their working and free time. In general, it can be said that the Web is a constantly growing and developing area, which is a subject of interest of commercial activities and research. The increase in the numbers of Web users is even exponential (Hiremath and Kenchakkanavar, 2016). A closer look at both popular and research publications reveals several attempts at describing evolution of the Web.

3.1 Web 1.0 and 2.0

Researchers usually mark the oldest variant of the Web as Web 1.0, although this mark was assigned to it only retrospectively. It is the Web based on the 1989 proposal by Sir Tim Burners-Lee. It is a "web of documents", in some cases also called a "web of companies". This phase is dated from its beginnings to about 2005. Web 1.0 can be characterized by a limited number of authors creating mostly static content. The aim of the Web in this phase was to distribute information (Hiremath and Kenchakkanavar, 2016; Shivalingaiah and Naik, 2008).

Compared to Web 1.0, the next step in its evolution, Web 2.0, can be defined as a "web of people" or a "network of people". A characteristic feature of this phase is an increasing involvement of users not only in browsing, but also in creation of web content. Although the work by DiNucci (1999) could possibly be the first work where the term "Web 2.0" was used, multiple authors (e.g., O'Reilly, 2005; Alexander, 2006; Hiremath and Kenchakkanavar, 2016) agree that the term "Web 2.0" was defined in 2004 during a conference brainstorming by Dale Dougherty (O'Reilly Media) and Craig Cline (MediaLive International).

At the same time, these authors agree that the definition of Web 2.0 is not unambiguous. The term "Web 2.0" was introduced in response to the changing nature of the Web that had started to be visible back then, but that had not been fully understood. A definition of Web 2.0 was expected to evolve to reflect the further development of Web 2.0.

Web 2.0 is characterized by a large number of users creating or changing content and by interactive behaviour of web applications. Previously, authors of papers mostly associated Web 2.0 with the use of blogs and content syndication using RSS (Shivalingaiah and Naik, 2008). From today's perspective, it can be stated that the "traditional" web blogs based on texts and wikis are no longer the prevalent form of newly created content, but they certainly continue to play a significant role. The traditional forms have been accompanied by other, especially shorter and more media-attractive, elements, especially video blogs and posts on social networks. Collective intelligence has become an important feature of the web content (O'Reilly, 2005; Singh and Gipti, 2011).

Sharing of user-selected links, comments, likes and similar ways to express emotions, content personalization and automatic selection of primarily displayed content led to the development of community thinking. The main actors of the Web are no longer individual companies with their presentations, but user groups and communities. Communication became the main goal of the web. Web 2.0 was also rather a social than a technological revolution (Coutinho and Bottentuit Jr., 2010; Solanki and Dongaonkar, 2016).

Creation of web content by most of its users leads to a very rapid increase in its volume. The sheer volume of content makes it impossible for the users to consume it all, and thus they are forced to choose only a fraction of the content. Prioritization of the newly created content is influenced by decisions of the community. Content popular among community members is more likely to be recommended to other members of the community, or to appear at the top of the search results. Therefore, community members not only create shared content, but through their behaviour and preferences they also participate on the selection process that strongly influences which content will be consumed. Some call this an "architecture of participation". Since content creation and consumption are tightly related, there is a significant centralization of the content and the users – creators and consumers of the content (also called prosumers) (Barassi and Treré, 2012; Król, 2020; Alexander, 2006).

Because of the community nature of Web 2.0, users naturally gather in only a few places on the Web. This concentration of users has positive, as well as significant negative consequences that are discussed in detail in Section 4.

3.2 Semantic web, Web 3.0

If Web 2.0 was aimed at people, the Web 3.0 should, according to many authors, be focused on its use by machines. The definition of the term Web 3.0 is attributed to John Markof, who associated it with the "social web", or to Sir Tim-Berners Lee, who associated it with the "semantic web" (Aghaei et al., 2012; Solanki and Dongaonkar, 2016).

Originally, a website as a fundamental element of the Web was designed to be readable by humans. However, this makes processing of websites by search engines and other software agents a nontrivial task. Therefore, the aim of the semantic web is to add new capabilities to the Web and make it machine-readable. Machine-readability could enable the Web to be turned into a word-wide database. In this context, Tim Berners-Lee (2007) also speaks about a "*giant global graph*". The semantic web is associated with development of semantic wikis and semantic social networks. Users should be able to create their profiles no matter where their data is stored. Therefore, the data should not be largely owned by specific companies. The companies should only use and represent them. Sometimes, Web 3.0 is also labelled as

the "*web of knowledge*" or the "*executable web*". It is also talked about "web-oriented architecture". The aim of a website in Web 3.0 is cooperation (Aghaei et al., 2012; Solanki and Dongaonkar, 2016).

Semantic web techniques such as linked data, interconnection of separate knowledge graphs, etc., could allow the Web to work as a global, yet distributed database. If Web 2.0 is associated with centralization of the Web, the techniques that are a fundamental part of the semantic web could help in re-decentralization of the Web. However, not every semantic web technique can contribute to the re-decentralization, because even a mere use of semantic tags for better SEO could be considered by some to be semantic web (Mavridis and Symeonidis, 2015).

To complete the picture of the term Web 3.0, alternative approaches to defining it should be mentioned. Some authors, e.g., Shivalingaiah and Naik (2008), Nath and Iswary (2015) or Bruwer and Rudman (2015), associate the third version of the Web with the concept of a "3D Web" represented by avatars moving in a virtual environment. However, other authors such as Patel K. (2013) or Khanzode and Sarode (2016) have designated the 3D Web as Web 5.0. Considering the current state of the Web, these past predictions of the Web's development were somewhat too optimistic. Nevertheless, there are some early indicators that the idea of the 3D Web is more than just a possible future direction of the Web's development. There are some virtual worlds that try to provide a 3D experience on the Web. These virtual worlds have been inspired by computer games, in which players control their characters (game avatars) moving around the virtual world. Decentraland presents itself as the "*first-ever virtual world owned by its users*" (Decentraland, 2021). Second Life (Linden Research, Inc., 2021) is an even older virtual 3D world. In 2003, it was the first virtual world without rules and with a functioning economy. Other similar projects can be found in the field of e-learning or online team cooperation. For example, in Gather Town (Gather Presence, Inc., 2021), users are represented by their avatars that can move in a predefined virtual world and that communicate with other avatars near them.

With regard to the semantic web, it should also be mentioned that the semantic web does not necessarily have to be marked as Web 3.0. Due to the ambiguous views and definitions of the versions or phases of the Web's development, semantic markup can also be attributed to Web 2.0. Some authors only regard applications that really understand data, such as search engines that respond with specific answers, not with a set of web links, as Web 3.0 applications. (Bruwer and Rudman, 2015; Wahlster et al., 2006)

Although Semantic Web and Web 3.0 technologies can help to decentralize the Web, some warnings about the potential risks resulting from machine-readability of data on the Web can also be found. The risks mentioned include personal data protection, the possibility of politicizing the Web, maximizing digital identities and the ability to suppress them more than with older versions of the Web. (Barassi and Tréré, 2012; Bruwer and Rudman, 2015)

3.3 Web 4.0 and beyond

Predicting future development is a challenge for many authors and researchers and it is not different in the Web domain. Several authors have presented different views on the possible future development of the Web, as well as on the labelling of its future versions.

The term "Web 4.0" is often presented as a synonym for a "symbiotic web". The symbiotic web builds upon the idea of a symbiosis between the human mind and machines (Aghaei et al., 2012). This symbiosis is associated with blending of the Web and the physical world (internet of things) or with voice assistants, or other interfaces that would allow humans to communicate with machines in natural language (Nath and Iswary, 2015; Patel K., 2013). Some authors went even further and suggested the use of mind-controlled Web interfaces (Solanki and Dongaonkar, 2016).

Visions presented by some authors expect the Web to evolve into a webOS – an operating system represented by the web ecosystem. All devices connected to the Web (e.g., symbionet) would be part of

this ecosystem, and users would live their lives through avatars in a virtual 3D environment. Some authors refer to this generation of the Web as Web 4.0, yet others have labelled it as Web 5.0. (Patel K., 2013; Solanki and Dongaonkar, 2016)

A different view on Web 5.0 was presented by Khanzode and Sarode (2016), who expect Web 5.0 to be built on personal servers and significantly decentralized.

An interesting idea was presented by Król (2020), who expects that the Web development could split into two partially separate branches. The first branch would be driven by cyber-biology thanks to which websites could become emotional and sensitive. Neurotechnology would allow the Web to read and interpret users' emotions. This branch is labelled as Web 5.0 by this author. The second branch would be driven by the further development of intelligent stand-alone agents. It expects that the Web would start to be composed of basically separate entities. Król (2020) labels this branch Web 6.0. The entities, intelligent virtual agents, could live in voluntary symbiosis with humans. He points out that the web technology should adapt to people and their changing behaviour, not vice versa.

3.4 What is the current version of the Web?

Regarding the versioning of the individual generations of the Web mentioned in the previous paragraphs, the question of what designation the current version of the website bears is certainly relevant. Considering the years in which the respective papers were published, it is possible to date the beginning of Web 2.0 and 3.0. However, it is difficult to tell whether the era of Web 1.0 or 2.0 is already over.

Even today, technologies and procedures developed for Web 1.0 are still important – for example, static company presentations and communication via e-mail. At the same time, elements associated with Web 2.0 (e.g., interactive websites or social networks) are actively used. Besides, Google (2021), for instance, tries to draw attention to the importance of structured data and the semantic markup on the Web (Schema.org Community Group, 2021). Search engines index Web 1.0, 2.0 also as 3.0 content (Mavridis and Symeonidis, 2015). With regard to this, Barassi and Treré (2012) point out that the individual versions of the Web cannot be understood as follow-up stages.

4 Centralization of the Web and Its Consequences

Without the Internet, there would be no Web. From a technical point of view, the Internet was designed as a decentralized computer network with many interconnected devices that, in most cases, can act as both data recipients and data providers. Theoretically, the environment of the Web and web services could also be decentralized. However, this is not the case. If the Web is viewed not as a system of servers serving content to clients, but as a system of interacting subjects, more centralized structures will be appeared. Especially with the development of Web 2.0, which brought about more centralization.

The Web is a complex socio-technical phenomenon (Barassi and Treré, 2012) that shows traits of centralization. This is true at least when publishing and searching for web content is considered (Barabas et al., 2017; Verborgh, 2020). The decentralized technology architecture of the Web does not seem to be a sufficient condition for a decentralized Web at all levels. Centralization of the Web includes or implies several problems, such as centralization of information retrieval and access to web content, the voluntary or involuntary consolidation of web users, and the business model based on monetization of user data. These consequences brought about by centralization of the Web are described in the following paragraphs. Responses to these consequences are described in Section 0.

4.1 Availability and accessibility of web content

One of the frequently repeated recommendations says that if a website does not appear on one of the first three pages of Google search results, no one will find it. Ledford (2015), for instance, points out that most

users click only on the first few links that appear in the search results. Although users can access websites directly if they know the corresponding URLs, due to the high competitiveness of the environment, it is necessary to deal with accesses from search engines. Therefore, search engines play a crucial role in access to the web content, and that is why the search engine optimization (SEO) attracts so much attention. The general principles of SEO are well known, and search engines are improving in the processing of new types of documents (e.g., semantic data; see Google Developers, 2021). However, the final algorithm is not public, and its results are not enforceable or controllable. Since search engines act as gateways to web content, removing a page from a search engine's index may have major consequences on discoverability of that web page. This puts search engines into a position in which they can influence what web pages are suggested, to whom and under which circumstances, reflected by keywords or queries. Therefore, some (e.g., Bratton, 2016) call search engines "centres of power", and Fioriglio (2015) raised the question of search neutrality.

Other services that can be clearly identified as centres of power are social networks. Social networks not only connect people online, but they also serve their users personalized content. Content personalization means that each user sees a different list of posts. Content personalization is often automated by algorithms that decide which pieces of content are displayed to which users. In this regard, some (e.g., Hofstetter, 2014; Fioriglio, 2015), talk about a dictatorship of algorithms that offer personalized content. Due to the huge volumes of content, displaying all the content to every user would result in an information overload. Similarly to search engines, the content personalization algorithms serve an important role in preventing this overload. However, there is a risk of direct or indirect censorship (Barabas et al., 2017). By amplifying or censoring certain types of posts, or posts containing certain keywords or images, social networks with large user bases can influence opinions of large numbers of people. Some have already expressed concerns that search engines and social networks could potentially influence electoral behaviour of their users (Barabas et al., 2017).

In addition to the creation of centres of power, there are also other significant consequences of centralization as well. Since most Web 2.0 user communities are active on only a relatively small number of platforms, these platforms and communities are vulnerable to state censorship. The "Great Firewall of China" can be served as an example. It is a very sophisticated solution that has been limiting and censoring web content for more than 600 million users since 2013 (Ensafi et al., 2015). To operate on the Chinese Internet, global companies must adapt to the Chinese regulations and policies. This can be illustrated with a case of Google, which discontinued offering the Web search in mainland China in 2010, allegedly due to cyber-attacks on Google and denial of search censorship (Tan and Tan, 2012). However, Google later worked on a censored search engine for China, but the development was halted after information on its development leaked to the public on 1st August 2018 (Charbonneau, 2019; Tiku, 2019).

4.2 Consolidation of users around platforms

Users access the Internet via services provided by Internet service providers. While there are many users, the number of the Internet service providers is limited. Neither the Internet nor the Web is a public property, but rather an ecosystem with many subjects with their own motivations and interests. The positions of service users and service providers are often not equal. Meinrath et al. (2011) characterized this situation as "digital feudalism".

As was already mentioned, Web 2.0 is largely community-oriented and social. Most users create micro-content (e.g., posts containing short texts, photos, etc.) that they want to share with their circles of friends or followers. This is often realized via social networks. For a social network, it is essential to reach a critical mass of users. Consolidation of the Web and its users and success of social networks often go hand in hand. Barabas et al. (2017) point out that it is not uncommon for people to start using a certain social

network because their friends are already there. It is not easy for users to switch from one social network to another, as they would also have to convince their friends to follow them to another social network.

Social networks have become an integral part of our lives and for many users social networks have become the dominant tool for communicating online. Therefore, a similar dependence of a user on a platform can be observed not only in the main social network applications (e.g., Facebook, Twitter, Twitch, YouTube, etc.) but also in other social networking services such as communicators. Built-in feedback mechanisms such as likes can also help to build a strong relationship between a user and the particular social network. Burke et al. (2010), Gallinari (2017) and others have studied the effects of social media on their users' self-perception. There is a positive correlation between the number of likes and the self-perception and social well-being of the social network user. To obtain a large number of likes, the users have to have their own group of "friends" active on the same social network.

If users become unwanted on a platform for any reason, their accounts can be blocked or even completely cancelled. This blocking or cancellation of user accounts is sometimes referred to as "deplatforming". Due to the imbalance of rights in the user-provider relationship, the user is then forced to find an alternative social network. As a result, migrating users would lose connections with at least some part of their communities. Even with celebrities, not all their followers or supporters are willing to migrate to other networks (Ali et al., 2021). The action to "deplatform Trump" can serve as a recent example of such termination of a user account. In January 2021, ex-president Trump's user accounts on social networks were blocked or even permanently banned after he published posts following the loss in the presidential election that were considered inciting unrest and hatred (Elias, 2021).

However, Web 2.0 is not just about social networks. Large numbers of users use cloud services provided by global companies, such as e-mail, calendar or office applications provided by Microsoft, Google, or Apple. All these companies try to interconnect their individual services to form one complex platform, but there is not much effort to interact with competitors' services. Migration from one platform to another can be difficult in some cases, or it might seem almost impossible in situations where a user has to collaborate with other users. If the interoperability between different providers' services is imperfect or non-existent, then the user is forced to keep using the platform or the service the other users are using. In this context, some also talk about the so-called "cloud feudalism" (Bratton, 2016), "Internet feudalism" (Liu et al., 2017), or "platform capitalism" (Srnicsek, 2017), where a platform means a set of interconnected services provided by a global company.

4.3 Monetization of data about users

For the for-profit web companies offering their products or services for free, monetization of data about their users can be an important part of their business model. There are several business models that these companies apply (Hayes and Graybeal, 2011), but for most of these business models knowing the preferences of users is either beneficial or even necessary. Companies operating on the Web (e.g., e-shops, social network providers) collect data about their users (personal data, behavioural data, etc.). This data is used to offer more relevant services and content to the users, and the provider can also use this data to better understand its customers and to gain competitive advantage (Fader, 2020). Providing a service or a product for free in exchange for the user data is a valid business model that can result in benefits for both the provider and the users. However, not every user is aware of this tradeoff when using services or products provided free of charge. For example, Marciano et al. (2020) quoted a study by the Italian Telecommunication and media regulator (AGCOM) according to which *"only 60% of users are actually aware of the implicit exchange of personal data when they download apps or have access to a digital platform"*.

In the discussion about centralization of the Web, usage of user data for targeting advertisements is one of the key topics because advertising is one of the major sources of revenue on the Web. Advertising systems, such as Google Ads, utilize user data to target advertisements displayed on websites or in search

results. Remarketing (also called retargeting) techniques allow advertisers to target advertisements at visitors of their websites even when they visit foreign websites (Google, 2021). Retargeting is effective in situations where the advertising system is used in many places. This could lead to consolidation of advertisers and website providers around the online advertising systems. Users can only be surprised why they see, for example, advertisements for goods that they viewed in an e-shop a few days ago when visiting a news website or a social network.

Advertising is also a major source of revenue for social networks. Again, the behaviour of users when browsing other websites is largely monitored (using tracking codes, or interactive elements of these social networks). However, this data can be combined with other data that a user generates when using a social network, such as the data about their relationships with other users or interactions on the social network. This allows social networks to develop rich user profiles of their users and to target advertisements according to the preferences of members of user communities (Tran, 2017; Windels et al., 2018).

In addition to the personalized advertising, user data collected by social networks can also be used for analysing behaviour of users. Identification of popular and important topics discussed in social networks could be a way to better understand societal concerns (Budak et al., 2011). However, the large user bases of social networks together with the possibility to analyse them, and subsequently to target them, can be misused. For example, in 2016 a campaign led with the contribution of the company Cambridge Analytica was executed in order to influence the US presidential elections (Alashri et al., 2016; Cadwalladr and Graham-Harrison, 2018; Wong, 2019).

5 Responses to Centralization of the Web

There is a growing concern about the current state of the Web and its future development. This can be illustrated by the fact that more than 1000 organizations backed a global activity called the Contract for the Web in the first month since its launch in November 2019 (World Wide Web Foundation, 2019). The aim of the Contract for the Web is to make the online world "*safe and empowering for everyone*" (World Wide Web Foundation, 2021). The Contract for the Web consists of nine principles that governments, companies and citizens should follow in order to ensure that the Internet and the Web are accessible and open, and that online privacy and data rights are respected and protected (World Wide Web Foundation, 2021). This activity does not target just the Web but also the Internet as its underlying infrastructure. It is also important to note that this activity stresses the need for action from both governments, companies and citizens as they all create and shape the Web.

This section provides a brief overview of the responses to centralization of the Web with a focus on regulation of large platforms. Technologies, privacy-oriented applications and alternatives to large, centralized platforms are described in Section 6.

5.1 Advocacy and fighting for the Web

Responses of individuals, organizations and companies to centralization of the Web have various forms and it is beyond the scope of this paper to list them all. Nevertheless, two very broad categories of such activities can be observed: fighting for the Web and development of alternatives to global Web platforms.

Quoting the principle 9 of the Contract for the Web (World Wide Web Foundation, 2021), the first of these two categories could be characterized as fighting for the Web. This category encompasses, again, a diverse range of activities. These activities include, but are not limited to, creating awareness regarding the issues and risks brought about by concentration of power in the hands of a small number of large platforms; influencing policymaking; conducting research or educating people about their rights and how to protect

them in the digital space in general, or on the Web in particular. The Electronic Frontiers Foundation¹ or the World Wide Web Foundation² could be named as examples of non-profit organizations whose activities fall within this category of responses to centralization of the Web. However, there are many other advocates fighting for the Web. For instance, the privacy-oriented search engine DuckDuckGo awarded donations to more than 20 other privacy and pro-competition organizations in 2021 (Spread Privacy, 2021).

The second of the broad categories of responses to centralization of the Web can be characterized as creating alternatives to the large platform providers, their products, and services. More details on this category of responses are provided in Section 6.2.

5.2 Regulation of large online platforms

According to the principles 1-3 of the Contract for the Web (World Wide Web Foundation, 2021), governments are expected to act by policymaking and by establishing legal and regulatory frameworks. Besides creating new regulations, governments have also responded by enforcing existing ones.

Regulation of digital markets and large online platforms such as Google or Facebook has attracted attention of both governments and researchers (e.g., Marciano et al., 2020; Sokol and Van Alstyne, 2021; Smyth, 2019; Weiss, 2020). Compared to industries such as television or telephone services, internet services and online platforms are viewed in the USA as free from significant federal regulation and operated under a system of self-governance. However, this does not mean that the internet services and online platforms are operated outside any legal framework because, for instance, the antitrust legislation or the legislation prohibiting unfair acts and practices still apply (Brannon, 2019). Because the algorithms built into online platforms require large amounts of data, including personal data, privacy protection regulation such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act represents a significant part of the legal framework regulating activities of online platforms. However, new regulations aimed at specific issues associated with the digital markets and especially large online platforms have been proposed in Europe (European Commission, 2020a; European Commission, 2020b), in the USA (Brannon, 2019) and in other countries such as the United Kingdom, Japan, Korea and India (Sokol and Van Alstyne, 2021).

At the EU level, two complementary regulations have been proposed that are aimed at dealing with some of the issues and risks associated with centralization of the Web: a Digital Markets Act (European Commission, 2020a) and a Digital Services Act (European Commission, 2020b). Primary objective of the Digital Markets Act is to set a harmonized EU-wide legal framework that should ensure *“contestable and fair markets in the digital sector”* (European Commission, 2020a). The objective of the Digital Services Act is to set harmonized rules on provision of intermediary services (transmission of information in a communication network, caching, hosting). More specifically, the Digital Services Act is aimed to set a legal framework for *“conditional exemption from liability of providers of intermediary services”*, and for *“specific due diligence obligations tailored to certain specific categories of providers of intermediary services”*, as well as rules on the implementation and enforcement of the Digital Services Act (European Commission, 2020b).

Both acts were proposed at the end of 2020, and at the time of writing of this paper they still have a status of a proposal. The aim of this paper is not to discuss the legal framework introduced by these regulations or to analyse the legal framework with the aim of drawing conclusions about their possible impacts on

¹ See, <https://www EFF.org>

² See, <https://webfoundation.org>

centralization of the Web. Nevertheless, the authors of this paper will discuss two aspects of the proposed regulations in order to demonstrate their relevance as responses to centralization of the Web.³

As mentioned above, search engines significantly influence what information is presented to users as responses to their queries (see, e.g., Fioriglio, 2015). The importance of algorithmic ranking, suggestions and prioritization of information is recognized in the proposed Digital Services Act. Article 29 of the Digital Service Act obliges very large platforms to inform the recipients of the service about the main parameters used in their recommender system, and to provide functionality that would allow the recipients of the service to select and to modify their preferences regarding the relative order of information presented to them (European Commission, 2020b).

Fioriglio (2015) also points out that search engines act as gatekeepers to digital information. The Digital Markets Act (European Commission, 2020a) is designed to regulate only a specific set of services listed in its Article 2, paragraph 2, called “*core platform services*”: online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating systems, cloud computing services and advertising services. The regulation would be applicable in situations where the core platform services are provided by “*gatekeepers*”. Conditions under which a provider of the core platform service would be considered as a gatekeeper are stated in the Article 3 of the Digital Markets Acts (European Commission, 2020a). Discussing these conditions is beyond the scope of this paper. However, the use of the term “*gatekeeper*” indicates recognition of the central role that large service and platform providers play.

Given the proposal status of the above-mentioned regulations, their impact on the Web is yet to be seen. However, some warn that regulations targeting large platforms and technology companies are not without their own risks. For instance, Sokol and Van Alstyne (2021) point out that growth of online platform providers and benefits for their users are driven by network effects and that the recommended changes to the antitrust laws in the USA could potentially undermine them, which can in turn negatively impact the users of the platforms. Marciano et al. (2020) argue that digital platform economy is complex, and that regulation of digital markets must consider the business model based on exchange of data for free services and the “*ability of reaching efficient outcomes similar to a perfect competition context, but—differently from perfect competition—obtained by internalising and exploiting information about preferences and willingness to pay of each customer*”. However, they add that what could be considered as positive from the efficiency perspective may not be desirable from a competitive and social perspective.

6 Different Shades of Re-Decentralized Web

As the previous sections suggest, the current state of the Web can be described as centralized. However, re-decentralization cannot be achieved in terms of initiatives and regulations alone. Similarly, it cannot be said that offering alternatives to existing global services will automatically lead to market fragmentation and the mentioned “centres of power” will be transformed into smaller, competing entities. However, the new, smaller entities can prevail, for example, by meeting the demand for more privacy for end users of the Web.

The re-decentralization can be viewed from several points of view. The main current trends could be characterized as the privacy imperative and the development of technologies for decentralized Web platforms and applications.

³ These two aspects should be viewed as examples. The legal framework set by the Digital Services Act and the Digital Markets Act would be more complex and cannot be reduced to the two points mentioned here.

6.1 User privacy

The right to privacy is one of the fundamental human rights (United Nations, n.d.). According to the Charter of Fundamental Rights of the European Union, individuals have an explicit right to the protection of personal data concerning them (European Union, 2000). Requirements to ensure anonymity and security of users are also in line with the ideas of Crypto Anarchy (May, 1992). However, due to the widespread adoption of the user tracking and monitoring, there is a growing importance of technologies that can help to protect these fundamental rights.

6.1.1 User tracking prevention

The first partial requirement for ensuring the privacy of users is to prevent tracking of their movement over the network. Everyone has certainly encountered the consequences of this tracking, for example in the field of advertising. Theoretically, the simplest solution to prevent tracking while browsing the Web content is to ban so-called third-party cookies. Many major web browsers already apply a certain degree of blocking. For example, Firefox turned on enhanced tracking protection in the autumn of 2019 (Wood, 2019). A similar effort can be registered with Google Chrome and browsers built on its open-source version Chromium. According to current plans, the date of their final ban is in 2023 (Bohn, 2021). However, Google is a big provider of advertising, and is trying to find a way to target it. This should be possible without identifying a specific user, using partial anonymization. The current, relatively controversial solution is a proposal of the technology “Federated Learning of Cohorts” – FLoC. FLoC should group web users according to their similarity and allow ads to be targeted according to the characteristics of these groups. Technically, however, the monitoring would be changed to first-party instead of third-party – data on user behaviour would be analysed directly by the browser. Anonymizing user data would certainly be beneficial (Langheinrich, 2021), but given the unfriendly acceptance of this proposal by other browsers, this would de facto contribute to increasing Google’s dominance (and thus centralization of power) in the field of advertising. Even FlocID could also be used for tracking (Rescorla, 2021).

Another level of user tracking prevention is hiding all network traffic by hiding the connection itself, or even moving web content to so-called Darknet. The best-known variant is the Tor Project (2021). Tor Browser not only blocks the common tracking mechanism, but it also allows the retrieval of Web content that is not addressable via common DNS servers. A specific of the Tor network is support for so-called “Onion services”. These allow accessing web content using alternative names derived from the encryption keys of the network nodes. (Burda et al., 2019) Research has appeared in recent years showing that the anonymity of Tor users may not be fully guaranteed due to the possibility of reconstructing of used private encryption keys (Kadianakis et al., 2018). However, the analysis (Sanchez-Rola et al., 2017) shows that a significant number of websites hidden in the Tor network use external resources, especially scripts, that can be used for the user tracking.

Another alternative for hiding network communication are also VPN networks and encryption of the content of communication. VPNs can be used to circumvent local restrictions on global services while limiting user tracking by hiding their true IP address. Examples of such networks are NordVPN (NordVPN.com, 2021), Browsec VPN (Browsec LLC, 2021) or VPN networks integrated in some antivirus and security solutions. ProtonVPN (Proton Technologies AG, 2021a) also integrates with the Tor anonymity network and also provides access to Onion websites. Browser creators also work on own solutions, e.g., Mozilla VPN (Mozilla Corporation, 2021).

When it comes to encrypting communications, most websites now use https security. This improves the security of transmission through network elements, but it is not sufficient to prevent all scanning of users’ content. Therefore, end-to-end encryption services are being developed. They concentrate not on static web content but on other web services – mainly e-mail and communicators. Examples are the encrypted

e-mail providers Tutanota (Tutao GmbH, 2021) or ProtonMail (Proton Technologies AG, 2021b). These solutions are also an aim of research (Kobeissi, 2018). An example from the category of communicators is Signal (Signal, 2021). This communicator became famous due to a tweet by Elon Musk on migrating his communication from WhatsApp to Signal in January 2021 (ETtech, 2021).

It can be said that, with conventional tools, a certain degree of anonymity can be achieved and users may be released from potential liability for their behaviour on the Web monitored by state institutions (Jordan, 2019; Zhuo et al., 2017; van Hardeveld et al., 2017).

6.1.2 Authentication, user identity

Although the privacy imperative is strong, identification of users is indispensable in many contexts. To use selected web service or platform, users need to be authenticated for access to their own data and for interactions between “anonymous” users. Anonymous authentication is the opposite of authentication guaranteed by the state or large institutions that join the online identity with a real person. In this regard, it was possible to register a new wave of pressure on anonymous online identifiers in connection with the tracking of people in the context of the COVID-19 pandemic (Halpin, 2020).

One of the variants of user identification can be found in the use of blockchain. For example, in the case of trade in cryptocurrencies, end “wallets” are marked with own identifiers, but these identifiers are not mappable to identities of real persons. Each user can generate their own wallets. The validity of transactions between wallets is verified by the community and recorded in the blockchain. Similar trends can be found in the field of authentication of users of web applications as well as on the Internet of Things (Durand et al., 2017). A subject of current research is the development of standardized protocols to ensure authentication – for example, the “DAuth protocol” based on Ethereum (Patel et al., 2019).

The “W3C Decentralized Identifier Working Group” plays an important role in the field of standardization (W3C, 2021). Its goal is to design a structure for Decentralized Identifiers (DID) by the end of 2021, as well as a relevant URI scheme and a set of requirements for the use of decentralized identifiers and their standardization. The proposal should lead to a generally valid “self-sovereign identity”. Nevertheless, regarding the collection of identities in directories, there are criticisms as to whether this proposal will not lead to “identity totalitarianism” (Halpin, 2020).

The activities of the W3C Working Group are not the only efforts to develop decentralized identities. Another example is the Decentralized Identity Web Directory (Decentralized Identity, 2021). In connection with the semantic web, identities cooperating with it are also developed, e.g. “webID” (Fáisca and Rogado, 2016).

6.1.3 Payment for services

In particular, the younger generations are aware that their right to use personal data is limited in favour of global platforms (de Andrade and Monteleone, 2013). On the other hand, from a web service provider's point of view, this is a kind of indirect payment for using its service. If this indirect payment will not be available, it will be necessary to look for new business models and for ways to enable direct payment for services. In case this will be done to prevent user tracking, anonymous payment methods must be supported. Therefore, it is impossible to use, for example, common payment gateways for payment cards. For the possibility of anonymous payments, cryptocurrencies become a phenomenon (Ban et al., 2019) – e.g., Bitcoin (Nakamoto, 2008) and its alternatives. There are several dozen actively traded and used cryptocurrencies – Ethereum, Litecoin, etc. (Binance, 2021), and more may occur.

From an economic point of view, cryptocurrencies can in principle be viewed as a commodity, while the price of cryptocurrencies is relatively volatile in many respects. Compared to stocks, investing in cryptocurrencies is relatively riskier (Lahmiri and Bekiros, 2020). Despite this instability and the

impossibility of a simple direct comparison with state-guaranteed currencies, cryptocurrencies are becoming increasingly popular, mainly due to their anonymity and independence from trust in the state.

There is also one interesting alternative that should be mentioned – Brave Browser. This browser places great emphasis on the user privacy while blocking data-grabbing ads and trackers. At the same time, however, it seeks to offer an alternative business model for web service providers. Brave Browser users are rewarded for watching ads with a crypto-currency BAT, which they can then use to support their favourite portal or service. (Brave, 2021)

Cryptocurrencies could be one way for the future of anonymous payments on the Web. However, at least in some countries, their future is highly uncertain as states seek to influence the cryptocurrency market, tax it, and at the same time prevent a simple capital outflow from the country (Xie, 2019). China has gone the farthest in restrictions for cryptocurrencies. After several partial bans, cryptocurrencies were banned completely this year. All cryptocurrency transactions are prohibited, also as providing of the related services. Official sources refer to ecology, but there will certainly be more reasons. The cryptocurrency ban on one of the largest markets also affects the global cryptocurrency trade, affecting, for example, the well-known cryptocurrency exchange Binance. (Wolf, 2021; Tidy, 2021)

6.2 Decentralized platforms and applications

In order to mark the Web as decentralized, it is not enough to imagine some alternative platforms to the main players on the market (e.g., an alternative to Facebook). It is necessary to give developers an opportunity to develop natively decentralized applications and users to have full control over their data. To meet these requirements, it is necessary to provide support for decentralized user authentication (already described in 6.1) and support for decentralized data storage and access to them. For this purpose, blockchain technologies are now increasingly used, often in cooperation with peer-to-peer networks. Alternatively, technologies known from the semantic web – RDF and Linked Data – are also used.

6.2.1 Decentralized social networks

Decentralized data storage and especially sharing of data among users is still problematic. As already mentioned in Section 4.2, people start to use a social network because their friends are already using it. Users usually do not want to share their own data with absolutely everyone. They want to share their data with members of their own social community. The problem is that users do not have control over how the social network itself uses their data and where the data is stored. Another solution can be found in decentralized social networks.

Probably the most popular of decentralized social network is Diaspora (Edwards, 2021). The users of this network have full control over their data and can choose a concrete server where to store them. Besides sharing content, users can contribute the computing resources, i.e., they can host a server used in this network (called a “pod”). Although Diaspora has been able to build a global availability as well as to attract attention of the research community, its popularity lacks behind its centralized counterparts (Bielenberg et al., 2012).

Another example of a popular decentralized social network is Mastodon, which is, according to the information on the official web, used by 4.4 million of users (Mastodon, 2021). Mastodon is an open source, distributed, microblogging platform. This consists of many instances on which users can register or create and host a new one. The individual nodes of the network are interconnected, the users can communicate with each other across the individual nodes. Theoretically, the communication is open also for other websites (independent of Mastodon) using the ActivityPub protocol. Nevertheless, *“10% of instances host almost half of the users, and certain categories exhibit remarkable reliance on a small set of instances”* (Raman et al., 2019). Re-decentralization of the web at the social level would probably require users and other web participants to change their behaviour (Vojř et al., 2020).

Furthermore, it is possible to find some smaller social networks centralizing their users in one place but using decentralized or blockchain technology for user authentication and for data storage. Examples of networks that use blockchain as part of their technology infrastructure are the blogging platform Steemit (2021), which uses a STEM cryptocurrency, the social network PeakD (2021), which uses HIVE blockchain, or the video streaming service DTube (2021), which is based on Avalon blockchain and the IPFS decentralized file storage protocol.

6.2.2 Distributed web pages

From the point of view of many users, anyone can host anything on the Web, but this is not the case. There are countries where even regular web services are blocked because they are not politically desirable (remember the text about the Great Firewall of China). Using new technologies of the decentralized web, websites can be hosted not only on regular servers that are easily hackable or disconnectable. The content of a website can be hosted on an independent network, divided among its individual users. This approach is a base for the functionality of ZeroNet. It is an open-source network that utilizes the BitTorrent network and Bitcoin Wallet as an authentication solution. The data hosting is based on the peer-to-peer principle and the websites can be found under .bit domain names using the Namecoin cryptocurrency. (ZeroNet, 2021)

Another notable technology platform for distributed websites under active development is the Safe Network (Safe Network, 2021). According to the information on the official website, this project should be just before the release of the first version. As with ZeroNet, this will be a serverless solution. The users need to download an application that allows access to Safe Network content. Then the application (in this case a specific web browser) also hosts some parts of the network data. At the same time, the Safe Network should also provide a new business model. For providing the storage and the connectivity, individual nodes will be rewarded with a cryptocurrency that drives the network.

6.2.3 Platforms for development of decentralized applications

Distributed storage of content is attractive for websites, social networks, but also for many other applications. In this area, many companies and initiatives see a potential future business advantage. For example, blockchain technology and smart contracts can be used not only for the cryptocurrency trade itself, but also for storing other, application data. The beginnings of further uses of smart contract technology relate to Ethereum. It is not only a cryptocurrency, but also an open-source computing platform, presented with Ethereum Virtual Machine (EVM). (Hirai, 2017; Ste, 2021) In addition, it enables financial contracts, bets, digital token issuance, decentralized file storage incentivization or voting systems (Buterin, 2016), and Ethereum blockchain is also used in the field of IoT (e.g., Huh et al., 2017). Similar functionality can be found in several frameworks that facilitate the development of decentralized applications, for example, Tron Network (TRON Foundation, 2018), which is a decentralized blockchain platform based on the Tron cryptocurrency.

Another alternative is Stacks (Stacks, 2021), based on Bitcoin. It is a framework facilitating the creation of decentralized applications. It supports user authentication, smart contracts as well as data storage using Gaia Storage. Similarly, the newly developed NEAR Protocol (NEAR Protocol, 2021) can be mentioned.

Another project that should not be overlooked is called Solid, developed by the MIT Decentralized Information Group led by Tim Berners-Lee and Lalana Kagal (Decentralized Information Group, 2021). Solid is a solution that allows user authentication using WebId or an identity provider of their choice and then storage of user data in decentralized "Solid Pods". This framework is used in dozens of different applications (Solid, 2021; Mansour et al., 2016).

Regards to the wide range of decentralized web technologies, it is also possible to come across projects addressing new technological challenges associated with the development of decentralized applications,

e.g., (de)centralized search in data on the decentralized web (Presearch.org Global Limited, 2021; Trattner et al., 2012) or interoperability between different blockchains (Web3 Foundation, 2021).

7 Conclusions

The aim of the paper was to describe how the Web has evolved over time and to present a view on its development from the perspective of centralization and the responses triggered by this centralization. From a technical solution for sharing information over the Internet, the Web has evolved into a socio-technical phenomenon. The Web is currently an integral part of lives of billions of people, and it affects their habits and social ties. In order to understand how the Web has evolved up to the present, and in which directions it could possibly develop in the future, the authors of this paper described versions of the Web and how these versions are perceived by different authors. It can be agreed with Barassi and Treré (2012) that the individual versions of the Web cannot be perceived as follow-up stages. Individual versions of the Web are associated with certain technologies; however, technologies associated with different versions of the Web are actively used.

As opposed to Web 1.0, Web 2.0 can be characterized by increased interactivity and significant involvement of users in creation of web content. Users are clustered around a relatively small number of platforms provided by large, global companies. This concentration of users itself is not necessarily negative, but the users often cannot fully control their data and they cannot easily transfer them between platforms due to technical barriers and network effects. This puts the platform providers in a powerful gatekeeper position where they can analyse also as influence behaviour of Web users.

Centralization of the Web around a small number of global platforms has provoked several reactions, either from organizations and initiatives seeking to restart the Web and re-decentralize it, or from states acting within existing legal frameworks, and also proposing new legislation aimed at regulating large online platforms. In the context of centralization and decentralization of the Web, online privacy has gained significant attention. An imperative to protect privacy in the digital world has already created opportunities for privacy-oriented applications and services such as web browsers, search engines or e-mail services to attract users. These privacy-oriented applications and services together with decentralized platforms and applications create alternatives to existing large platforms.

The General Data Protection Regulation (GDPR) or the California Consumer Privacy Act can be seen as regulatory responses to the privacy imperative. The Digital Markets Act and the Digital Services Act represent examples of newly proposed legislation aimed at regulating the digital markets. However, views on the impacts of these regulations on the digital markets are not unified. For instance, Marciano et al. (2020) argue that the business model based on exchange of data for free services should be considered, and that effects of the regulation positive from the competitive and social perspective could be negative from the efficiency perspective, and vice versa.

Technologies such as peer-to-peer networks or blockchain enable development of truly decentralized applications. However, availability of such technologies and applications will not immediately lead to a shift towards a more decentralized or re-decentralized Web. Technologies can act as an enabler of a re-decentralized Web; however, significant changes at the socio-economic level would be required as well. Companies developing and adopting these technologies would have to change or adapt their business models to keep profitable. Re-decentralization of the Web would also require a shift in user mindset and behaviour. Especially, increased awareness of how their data is monetized would have to go hand in hand with the increased preference to control who can access their data, and how and when the data can be used.

Future development of the Web will certainly be a subject of further research, not only from the technological perspective, but also from the sociological and psychological perspectives. Automated web

content processing powered by artificial intelligence, smart assistants, blending of the physical and the digital world, and the new regulations will bring new practical problems and research questions. One of the possible future directions in the development of the Web could be a highly decentralized Web where data would be stored in redundant decentralized nodes. This could go hand in hand with obligations to encrypt personal data that could be further amplified by the voice of the users who would appreciate real control over their data. From the regulatory point of view, these developments could add to the dilemmas arising from conflicts between the rights of individuals (e.g., the right to privacy) and legitimate interests of the society or states, such as the role of a state to ensure public safety and to enforce active legislation.

Additional Information and Declarations

Acknowledgements: We would like to thank to our colleague Zdeněk Smutný for his contribution to the original paper (Vojříř et al., 2020).

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: S.V.: Conceptualization, Investigation, Project administration, Writing – original draft. J.K.: Conceptualization, Investigation, Writing – original draft, Writing – review & editing.

References


- Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the World Wide Web: From Web 1.0 to Web 4.0. *International Journal of Web & Semantic Technology*, 3(1), 1–10. <https://doi.org/10.5121/ijwest.2012.3101>
- Alashri, S., Kandala, S. S., Bajaj, V., Ravi, R., Smith, K. L., & Desouza, K. C. (2016). An analysis of sentiments on Facebook during the 2016 US presidential election. In *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, (pp. 795–802). IEEE. <https://doi.org/10.1109/ASONAM.2016.7752329>
- Alexander, B. (2006). Web 2.0: A new wave of innovation for teaching and learning? *Educause review*, 41(2). <https://er.educause.edu/articles/2006/1/web-20-a-new-wave-of-innovation-for-teaching-and-learning>
- Ali, S., Saeed, M. H., Aldreabi, E., Blackburn, J., De Cristofaro, E., Zannettou, S., & Stringhini, G. (2021). Understanding the Effect of Deplatforming on Social Networks. In *13th ACM Web Science Conference 2021*, (pp. 187–195). <https://doi.org/10.1145/3447535.3462637>
- Ban, Z., Lansky, J., Mildeova, S., & Tesar, P. (2019). A Probe Survey of Bitcoin Transactions Through Analysis of Advertising in an On-Line Discussion. *Acta Informatica Pragensia*, 8(2), 112–131. <https://doi.org/10.18267/j.aip.127>
- Barabas, C., Narula, N., & Zuckerman, E. (2017). Defending Internet Freedom through Decentralization: Back to the Future? *The Center for Civic Media & The Digital Currency Initiative MIT Media Lab*. https://dci.mit.edu/s/decentralized_web.pdf
- Barassi, V., & Treré, E. (2012). Does Web 3.0 come after Web 2.0? Deconstructing theoretical assumptions through practice. *New Media & Society*, 14(8), 1269–1285. <https://doi.org/10.1177/1461444812445878>
- Berners-Lee, T. (2007). Giant global graph. *Decentralized Information Group*. <http://dig.csail.mit.edu/breadcrumbs/node/215>
- Bielenberg, A., Helm, L., Gentilucci, A., Stefanescu, D., & Zhang, H. (2012). The growth of Diaspora – A decentralized online social network in the wild. In *Proceedings of the IEEE INFOCOM Workshops* (pp. 13–18). IEEE. <https://doi.org/10.1109/infcomw.2012.6193476>
- Binance. (2021). *Buy & sell Crypto in minutes*. <https://www.binance.com/en>
- Bohn, D. (2021). Google delays blocking third-party cookies in Chrome until 2023. *The Verge*. <https://www.theverge.com/2021/6/24/22547339/google-chrome-cookiepocalypse-delayed-2023>
- Brannon, V. C. (2019). *Regulating Big Tech: Legal Implications*. <https://crsreports.congress.gov/product/pdf/LSB/LSB10309>
- Bratton, B. H. (2016). *The stack: On software and sovereignty*. MIT Press.
- Brave. (2021). Secure, Fast & Private Web Browser with Adblocker. *Brave Browser*. <https://brave.com/>
- Browsec LLC. (2021). *Browsec VPN*. <https://browsec.com/en/>
- Bruwer, R. H., & Rudman, R. (2015). Web 3.0: governance, risks and safeguards. *Journal of Applied Business Research*, 31(3), 1037–1056.
- Budak, C., Agrawal, D., & El Abbadi, A. (2011). Structural Trend Analysis for Online Social Networks. In *Proceedings of the VLDB Endowment* (pp. 646–656). VLDB Endowment. <https://doi.org/10.14778/2021017.2021022>
- Burda, P., Boot, C., & Allodi, L. (2019). Characterizing the redundancy of DarkWeb .onion services. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, (pp. 1–10). ACM. <https://doi.org/10.1145/3339252.3339273>

- Burke, M., Marlow, C., & Lento, T. (2010). Social network activity and social well-being. In *Proceedings of the SIGCHI conference on human factors in computing systems*, (pp.1909-1912). ACM. <https://doi.org/10.1145/1753326.1753613>
- Buterin, V. (2016). *Ethereum: Platform Review*. Opportunities and Challenges for Private and Consortium Blockchains.
- Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, 17 March 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Coutinho, C. P., & Bottentuit Jr, J. B. (2010). From web to web 2.0 and e-learning 2.0. In *Handbook of research on practices and outcomes in e-learning: Issues and trends* (pp. 19–37). IGI Global.
- de Andrade, N. N., & Monteleone, S. (2013). Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications. In S. Gutwirth, R. Leenes, P. de Hert, & Y. Pouillet (Eds.), *European Data Protection: Coming of Age* (pp. 119-144). Springer. https://doi.org/10.1007/978-94-007-5170-5_5
- Decentraland. (2021). *Welcome to Decentraland*. <https://decentraland.org/>
- Decentralized Identity. (2021). Decentralized Identity Web Directory. *Decentralized Identity*. <https://decentralized-id.com/>
- Decentralized Information Group. (2021). Decentralized Information Group. *Internet Policy Research Initiative at MIT*. <https://internetpolicy.mit.edu/research/decentralized-information-group/>
- DiNucci, D. (1999). Fragmented Future. *Print Magazine*, 53(4). http://www.darcyd.com/fragmented_future.pdf
- DTube. (2021). *How does D.Tube work?*. <https://d.tube#!/wiki/faq/how-does-dtube-work>
- Durand, A., Gremaud, P., & Pasquier, J. (2017). Decentralized web of trust and authentication for the internet of things. In *Proceedings of the Seventh International Conference on the Internet of Things* (Article No.: 27). ACM. <https://doi.org/10.1145/3131542.3140263>
- Edwards, B. H. (2021). *The Practice of Diaspora*. Harvard University Press.
- Elias, J. (2021). YouTube stands alone as other social media providers race to deplatform Trump. *CNBC*. <https://www.cnn.com/2021/01/16/youtube-slow-to-deplatform-trump-versus-facebook-twitter.html>
- Ensaifi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). Analyzing the Great Firewall of China Over Space and Time. *Proceedings on Privacy Enhancing Technologies*, 2015(1), 61–76. <https://doi.org/10.1515/popets-2015-0005>
- ETtech. (2021). Another Signal gains after Elon Musk's tweet. *The Economic Times*. <https://economictimes.indiatimes.com/tech/tech-bytes/another-signal-gains-after-elon-musks-tweet/articleshow/80234425.cms>
- European Commission. (2020a). Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0842>
- European Commission. (2020b). Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0825>
- European Union. (2000). *Charter of fundamental rights of the European Union*. https://www.europarl.europa.eu/charter/pdf/text_en.pdf
- Fader, P. (2020). *Customer centricity: Focus on the right customers for strategic advantage*. University of Pennsylvania Press.
- Faísca, J. G., & Rogado, J. Q. (2016). Decentralized Semantic Identity. In *Proceedings of the 12th International Conference on Semantic Systems*, (pp. 177-180). ACM. <https://doi.org/10.1145/2993318.2993348>
- Fioriglio, G. (2015). Freedom, Authority and Knowledge On Line: The Dictatorship of the Algorithm. *Revista Internacional Pensamiento Político*, 10, 395-410.
- Gallinari, E. (2017). "Likes" for Self-Love? The Effects of Social Media on Self-Perception. *Undergraduate Review*, 13, 100–105. http://vc.bridgew.edu/undergrad_rev/vol13/iss1/13
- Gather Presence, Inc. (2021). Gather | A better way to meet online. *Gather*. <https://www.gather.town/>
- Google. (2021). What are retargeting ads? A guide to customer retargeting. *Google Ads*. https://ads.google.com/intl/en_uk/home/resources/retargeting-ads/
- Google Developers. (2021). Understand how structured data works. *Google Search Central*. <https://developers.google.com/search/docs/advanced/structured-data/intro-structured-data>
- Halpin, H. (2020). A Critique of Immunity Passports and W3C Decentralized Identifiers. *arXiv:2012.00136v1*. <https://arxiv.org/abs/2012.00136>
- Hayes, J., & Graybeal, G. (2011). Synergizing Traditional Media and the Social Web for Monetization: A Modified Media Micropayment Model. *Journal of Media Business Studies*, 8(2), 19–44. <https://doi.org/10.1080/16522354.2011.11073521>
- Hirai, Y. (2017). Defining the ethereum virtual machine for interactive theorem provers. In *International Conference on Financial Cryptography and Data Security* (pp. 520-535). Springer. https://doi.org/10.1007/978-3-319-70278-0_33
- Hiremath, B. K., & Kenchakkanavar, A. Y. (2016). An alteration of the web 1.0, web 2.0 and web 3.0: a comparative study. *Imperial Journal of Interdisciplinary Research*, 2(4), 705–710.
- Hofstetter, Y. (2014). *Sie wissen alles: Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen*. C. Bertelsmann Verlag.

- Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)* (pp. 464-467). IEEE. <https://doi.org/10.23919/ICACT.2017.7890132>
- Charbonneau, M. (2019). Google executive confirms termination of china search engine project. *S&P Global Market Intelligence*. <https://www.spglobal.com/marketintelligence/en/news-insights/trending/SVMmJHVT2amR4nfdMuhr-g2>
- Jordan, T. (2019). Does online anonymity undermine the sense of personal responsibility? *Media, Culture & Society*, 41(4), 572–577. <https://doi.org/10.1177/0163443719842073>
- Kadianakis, G., Roberts, C. V., Roberts, L. M., & Winter, P. (2018). "Major key alert!" Anomalous keys in Tor relays. In S. Meiklejohn, & K. Sako (Ed.), *International Conference on Financial Cryptography and Data Security* (pp. 3-19). Springer. https://doi.org/10.1007/978-3-662-58387-6_1
- Khanzode, C. A., & Sarode, R. D. (2016). Evolution of the world wide web: from web 1.0 to 6.0. *International Journal of Digital Library Services*, 6(2), 1–11.
- Kobeissi, N. (2018). *An Analysis of the ProtonMail Cryptographic Architecture*. Cryptology ePrint Archive. <https://eprint.iacr.org/2018/1121.pdf>
- Król, K. (2020). Evolution of online mapping: from Web 1.0 to Web 6.0. *Geomatics, Landmanagement and Landscape*, 1, 33–51. <https://doi.org/10.15576/gll/2020.1.33>
- Lahmiri, S., & Bekiros, S. (2020). The impact of COVID-19 pandemic upon stability and sequential irregularity of equity and cryptocurrency markets. *Chaos, Solitons & Fractals*, 138, Article no. 109936. <https://doi.org/10.1016/j.chaos.2020.109936>
- Langheinrich, M. (2021). To FLoC or Not? *IEEE Pervasive Computing*, 20(2), 4–6. <https://doi.org/10.1109/MPRV.2021.3076812>
- Ledford, J. L. (2015). *Search engine optimization bible* (Vol. 584). John Wiley & Sons.
- Linden Research, Inc. (2021). *Second Life*. <https://secondlife.com/>
- Liu, T., Tariq, Z., Chen, J., & Raghavan, B. (2017). The barriers to overthrowing internet feudalism. In *Proceedings of the 16th ACM Workshop on Hot Topics in Networks*, (pp. 72-79). ACM. <https://doi.org/10.1145/3152434.3152454>
- Mansour, E., Sambra, A. V., Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., ... Berners-Lee, T. (2016). A Demonstration of the Solid Platform for Social Web Applications. In *Proceedings of the 25th International Conference Companion on World Wide Web* (pp. 223-226). ACM. <https://doi.org/10.1145/2872518.2890529>
- Marciano, A., Nicita, A., & Ramello, G. B. (2020). Big data and big techs: Understanding the value of information in platform capitalism. *European Journal of Law and Economics*, 50(3), 345-358. <https://doi.org/10.1007/s10657-020-09675-1>
- Mastodon. (2021). Giving social networking back to you. *Mastodon*. <https://joinmastodon.org/>
- Mavridis, T., & Symeonidis, A. L. (2015). Identifying valid search engine ranking factors in a Web 2.0 and Web 3.0 context for building efficient SEO mechanisms. *Engineering Applications of Artificial Intelligence*, 41, 75–91. <https://doi.org/10.1016/j.engappai.2015.02.002>
- May, T. (1992). *A Crypto Anarchist Manifesto*. <https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html>
- Meinrath, S. D., Losey, J. W., & Pickard, V. W. (2011). Digital Feudalism. *Advances in Computers*, 81, 237–287. <https://doi.org/10.1016/b978-0-12-385514-5.00005-7>
- Mozilla Corporation. (2021). *Mozilla VPN: Protect Your Entire Device*. <https://www.mozilla.org/en-US/products/vpn/>
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from <https://www.debr.io/article/21260.pdf>
- Nath, K., & Iswary, R. (2015). What comes after Web 3.0? Web 4.0 and the Future. In *Proceedings of the International Conference and Communication System (I3CS'15)*, (pp. 337-341). Shillong.
- NEAR Protocol. (2021). Infrastructure for Innovation. *NEAR Protocol*. <https://near.org/>
- NordVPN.com. (2021). *NordVPN*. <https://nordvpn.com/>
- O'Reilly, T. (2005). What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software. <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>
- Patel, K. (2013). Incremental Journey for World Wide Web: Introduced with Web 1.0 to Recent Web 5.0 – A Survey Paper. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(10), 410–417.
- Patel, S., Sahoo, A., Mohanta, B. K., Panda, S. S., & Jena, D. (2019). DAuth: A Decentralized Web Authentication System using Ethereum based Blockchain. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (VITECoN)*. IEEE. <https://doi.org/10.1109/vitecon.2019.8899393>
- PeakD. (2021). *About PeakD*. <https://peakd.com/about>
- Presearch.org Global Limited. (2021). *Presearch*. <https://presearch.org>
- Proton Technologies AG. (2021a). *Protect yourself online. ProtonVPN. Protect yourself online*. <https://protonvpn.com/>
- Proton Technologies AG. (2021b). *Secure email: ProtonMail is free encrypted email*. <https://protonmail.com/>
- Raman, A., Joglekar, S., Cristofaro, E. D., Sastry, N., & Tyson, G. (2019). Challenges in the decentralised web: The mastodon case. In *Proceedings of the Internet Measurement Conference*, (pp. 217-229). ACM. <https://doi.org/10.1145/3355369.3355572>
- Rescorla, E. (2021). *Privacy analysis of FLoC*. <https://blog.mozilla.org/en/mozilla/privacy-analysis-of-floc/>

- Rogers, R.** (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication*, 35(3), 213–229. <https://doi.org/10.1177/0267323120922066>
- Safe Network.** (2021). *We're Building The New Internet*. <https://safenetwork.tech/>
- Sanchez-Rola, I., Balzarotti, D., & Santos, I.** (2017). The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services. In *Proceedings of the 26th international conference on world wide web*, (pp. 1251-1260). ACM. <https://doi.org/10.1145/3038912.3052657>
- Shivalingaiah, D., & Naik, U.** (2008). Comparative Study of Web 1.0, Web 2.0 and Web 3.0. In *International CALIBER-2008*, (pp. 499-507). <https://ir.inflibnet.ac.in/bitstream/1944/1285/1/54.pdf>
- Schema.org Community Group.** (2021). *Schema.org*. <https://schema.org>
- Signal.** (2021). *Signal*. <https://signal.org/>
- Singh, K. P., & Gipti, D.** (2011). Technological March from Web 1.0 to Web 3.0: a comparative study. *Library Herald*, 49(2), 146–157.
- Smyth, S. M.** (2019). The facebook conundrum: Is it time to usher in a new era of regulation for big tech? *International Journal of Cyber Criminology*, 13(2), 578–595. <https://doi.org/10.5281/zenodo.3718955>
- Sokol, D. D., & Van Alstyne, M.** (2021). The rising risk of platform regulation. *MIT Sloan Management Review*, 62(2), 6A-10A.
- Solanki, M. R., & Dongaonkar, A.** (2016). A Journey of human comfort: web 1.0 to web 4.0. *International Journal of Research and Scientific Innovation*, 3(9), 124–134.
- Solid.** (2021). *Solid Applications*. <https://solidproject.org/apps>
- Spread Privacy.** (2021). *2021 DuckDuckGo Charitable Donations: \$1,000,000 to Privacy and Competition Organizations Around the World*. <https://spreadprivacy.com/2021-duckduckgo-donations/>
- Srnicek, N.** (2017). *Platform Capitalism*. Polity Press.
- Stacks.** (2021). *A better internet, built on Bitcoin*. <https://www.stacks.co/>
- Ste, J.** (2021). *Ethereum Virtual Machine (EVM)*. <https://ethereum.org/en/developers/docs/evm/>
- Steemit.** (2021). *Faq*. <https://steemit.com/faq.html>
- Tan, J., & Tan, A. E.** (2012). Business Under Threat, Technology Under Attack, Ethics Under Fire: The Experience of Google in China. *Journal of Business Ethics*, 110(4), 469–479. <https://doi.org/10.1007/s10551-012-1494-0>
- Tidy, J.** (2021). *US leads Bitcoin mining as China ban takes effect*. <https://www.bbc.com/news/technology-58896545>
- Tiku, N.** (2019). Three Years of Misery Inside Google, the Happiest Company in Tech. *Wired*. <https://www.wired.com/story/inside-google-three-years-misery-happiest-company-tech/>
- Tor Project.** (2021). Browse Privately. Explore Freely. *Tor Project | Anonymity Online*. <https://www.torproject.org/>
- Torraco, R. J.** (2005). Writing integrative literature reviews: Guidelines and examples. *Human resource development review*, 4(3), 356–367.
- Tran, T. P.** (2017). Personalized ads on Facebook: An effective marketing tool for online marketers. *Journal of Retailing and Consumer Services*, 39, 230–242. <https://doi.org/10.1016/j.jretconser.2017.06.010>
- Trattner, C., Singer, P., Helic, D., & Strohmaier, M.** (2012). Exploring the differences and similarities between hierarchical decentralized search and human navigation in information networks. In *Proceedings of the 12th International Conference on Knowledge Management and Knowledge Technologies* (pp. 1-8). ACM. <https://doi.org/10.1145/2362456.2362474>
- TRON Foundation.** (2018). *Tron - Advanced Decentralized Blockchain Platform*. https://tron.network/static/doc/white_paper_v_2_0.pdf
- Tutao GmbH.** (2021). *Secure email: Tutanota free encrypted email*. <https://tutanota.com/>
- United Nations.** (n.d.). *Universal Declaration of Human Rights*. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
- van Hardeveld, G. J., Webber, C., & O'Hara, K.** (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist*, 61(11), 1244–1266. <https://doi.org/10.1177/0002764217734271>
- Verborgh, R.** (2020). Re-decentralizing the Web, for good this time. In *Linking the World's Information: Tim Berners-Lee's Invention of the World Wide Web*. <https://ruben.verborgh.org/articles/redecentralizing-the-web>
- Vojř, S., Smutný, Z., & Kučera, J.** (2020). Social and Technical Aspects of Re-Decentralized Web. In *IDIMT-2020 Digitalized Economy, Society and Information Management* (pp. 107–116). Trauner Verlag. https://idimt.org/wp-content/uploads/2020/07/IDIMT_proceedings_2020.pdf
- W3C.** (2021). *Decentralized Identifier Working Group Charter*. <https://www.w3.org/2020/12/did-wg-charter.html>
- Wahlster, W., Dengel, A., Telekom, D., & Dengel, W.** (2006). Web 3.0: Convergence of web 2.0 and the semantic web. In *Technology Radar, Feature Paper*. Deutsche Telekom Laboratories.
- Web3 Foundation.** (2021). *Decentralized Web 3.0 Blockchain Interoperability Platform*. *Polkadot*. <https://polkadot.network/>
- Weiss, B.** (2020). Reframing antitrust law for big tech: Lessons from the german bundeskartellamt. *Federal Communications Law Journal*, 73(1), 193–217.

- Windels, K., Heo, J., Jeong, Y., Porter, L., Jung, A-Reum., & Wang, R.** (2018). My friend likes this brand: Do ads with social context attract more attention on social networking sites? *Computers in Human Behavior*, 84, 420–429. <https://doi.org/10.1016/j.chb.2018.02.036>
- Wolf, K.** (2021). Kolikrát ještě Čína zakáže bitcoin? A co si z toho vzít? *Forbes*. <https://forbes.cz/kolikrat-jeste-cina-zakaze-bitcoin-a-co-si-z-toho-vzit/>
- Wong, J. C.** (2019). The Cambridge Analytica scandal changed the world - but it didn't change Facebook. *The Guardian*. <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>
- Wood, M.** (2019). Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default. *The Mozilla Blog*. <https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/>
- World Wide Web Foundation.** (2018). *The Case #ForTheWeb*. <https://webfoundation.org/docs/2018/11/The-Case-For-The-Web-Report.pdf>
- World Wide Web Foundation.** (2019). *Over 1,000 organizations back the Contract for the Web in the first month*. <https://contractfortheweb.org/2019/12/20/over-1000-organizations-back-the-contract-for-the-Web-in-the-first-month/>
- World Wide Web Foundation.** (2021). *Contract for the Web*. <https://contractfortheweb.org>
- Xie, R.** (2019). Why China had to ban cryptocurrency but the US did not: A comparative analysis of regulations on crypto-markets between the US and China. *Washington University Global Studies Law Review*, 18(2), 457–492.
- ZeroNet.** (2021). Open, free and uncensorable websites, using Bitcoin cryptography and BitTorrent network. *ZeroNet*. <https://zeronet.io/>
- Zhuo, Z., Zhang, Y., Zhang, Z.-I., Zhang, X., & Zhang, J.** (2017). Website fingerprinting attack on anonymity networks based on profile hidden markov model. *IEEE Transactions on Information Forensics and Security*, 13(5), pp. 1081-1095. <https://doi.org/10.1109/tifs.2017.2762825>

Editorial record: The article has been peer-reviewed. First submission received on 21 October 2021. Revision received on 9 December 2021. Accepted for publication on 13 December 2021. The editor in charge of coordinating the peer-review of this manuscript and approving it for publication was Stanislava Mildeova .

Special Issue: Perspectives of Social Informatics.

Acta Informatica Pragensia is published by Prague University of Economics and Business, Czech Republic.

ISSN: 1805-4951
