Log out_
A Glossary of Technological Resistance and Decentralization_

Edited by:
Valeria Ferrari, Florian Idelberger, Andrea Leiter, Morshed Mannan, María-Cruz Valiente, Balázs Bodó_

Log out_
A Glossary of Technological Resistance and Decentralization_

Edited by:
Valeria Ferrari, Florian Idelberger, Andrea Leiter, Morshed Mannan, María-Cruz Valiente, Balázs Bodó_

Log Out. A Glossary of Technological Resistance and Decentralization

Editor of Printed Edition: Valeria Ferrari
Editing of Online Edition: Valeria Ferrari, Florian Idelberger, Andrea Leiter, Morshed Mannan, María-Cruz Valiente.
Advisory Board: Balázs Bodó, Primavera De Filippi, Aron Fischer, Samer Hassan, Björn Scheuermann, Monica Palmirani.
Copy Editor: Jack Wilson
Design: Andy Díaz Sánchez

Authors: Valeria Ferrari, Kelsie Nabben, Ellie Rennie, Aron Fischer, María-Cruz Valiente, Florian Tschorsch, Ingolf G. A. Pernice, Brett Scott, Jaya Klara Brekke, Wassim Zuhair Alsindi, André Ramiro, Ruy de Queiroz, Heleen Janssen, Jatinder Singh, Balázs Bodó, Roel Roscam Abbing, Cade Diehm, Shahed Warreth, Samer Hassan, Primavera De Filippi, Isabelle A. Zaugg, Anushah Hossain, Brendan Molloy, Daniel Villar-Onrubia, Victoria I. Marín, Laura Lotti, Florian Idelberger, Péter Mezei, Selwa Sweidan, Karlynne Ejercito, Tyng-Ruey Chuang, Rebecca C. Fan, Ming-Syuan Ho, Kalpana Tyagi, Michael Zargham, Gerd Beuster, Oliver Leistert, Theo Röhle, Ori Shimony, Ámbar Tenorio-Fornés, Alexandra Giannopoulou, Fennie Wang, Chris Wray, Giovanni Sileno, Francisco Javier Moreno Gálvez, Francisco Sierra Caballero, Indrek Ibrus, Ulrike Rohn, Nanna Bonde Thylstrup, Matthew Archer, Louis Ravn, Moritz Becker, Catalina Goanta, Alfa Yohanis, Vikas Jaiman, Visara Urovi.

ISBN: 9789083328225
Printer: Proefschriftspecialist

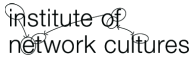
Contact
Institute of Network Cultures
Email: info@networkcultures.org
Web: www.networkcultures.org

A project of the *Blockchain and Society Policy Research Lab, Institute forInformation Law, University of Amsterdam* & *Internet Policy Review*. Published by the *Institute of Network Cultures* & the *Blockchain and Society Policy Research Lab, Institute for Information Law, University of Amsterdam*.

The project and the publication have received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681.

Web: https://blockchain-society.science/; https://www.ivir.nl/; https://policyreview.info/.

Published by the Institute of Network Cultures, Amsterdam, 2023.



Log out_
A Glossary of Technological Resistance and Decentralization_

TABLE OF CONTENTS_

The Glossary of Decentralized Techno-Social Systems_

Much academic research in social sciences and technology is focused on scrutinising the adverse effects of the current structure of the information economy on individual, social, cultural and political life, and on the global distribution of power. Critical efforts point at the enclosure of users within platform ecosystems and at the logics of data accumulation: how they compress individual autonomy and create hard to reverse power asymmetries. But thinking critically against such a heavily centralised, data-intensive digital economy also implies imagining possible alternatives.

Against the logics of information capitalism, which want users to be dumb and innovation centrally controlled, decentralised, privacy-enhancing technologies emerge, often from the peripheries of the internet, as tools for individual and collective emancipation and resistance.

Unlike 'big tech'-generated terminology, however, terms that originate in peripheral, subversive, resistant parts of the internet remain obscure, unheard-of or misunderstood by most people. If discourses are performative, the obscurity of these terms suggests that the alternative visions they propose are always already in the past, or in a future that struggles to materialize.

With a highly ideological charge, discourses on decentralised technologies have generated a wide vocabulary of context-specific terms that associate political, societal and technological issues in rather original ways. Just as any other subject, however, these technologies (as tools, as conceptual design, as symbols) are rooted in specific geographies, ideologies, gender relations, and reflect the biases encoded in these contexts. The related terminology is used and interpreted according to different purposes and pre- and/or mis- conceptions. This results in uninformed hypes, prejudices, lost opportunities for discussion.

This book brings together voices from various fields of intellectual inquiry, based on the idea that technological, legal and societal aspects of the information sphere are interlinked and co-dependent from each other. In order to tackle the existing gap in shared semantics, this glossary converges the efforts of experts from various disciplines to build a shared vocabulary on the social, technical, economic, political aspects of decentralised, distributed or sovereign technologies: artefacts which seek to challenge the

techno-social *status quo* by, for example, circumventing law enforcement, resisting surveillance, or being participative.

The idea of this glossary arose from the need for a workable, flexible and multidisciplinary resource for terminological clarity, which reflects instead of denying complexity. Situating the terms emerging through technology development in the wider context of multidisciplinary scientific, policy and political discourses, this glossary provides a conceptual toolkit for the study of the various political, economic, legal and technical struggles that decentralised, encryption-based, peer-to-peer technologies bring about and go through.

Choosing relevant technology-related terms and understanding them is to investigate their affordances within a given ecosystem of actors, discourses and systems of incentives. This requires an interdisciplinary, multi-layered approach that is attentive to the interlinkages between technological design nuances and socio-political, economic implications.

The glossary was envisioned as a long-term collaborative project, and as a work-in-progress, as new entries are periodically added over time. The present book collects the entries published on the Internet Policy Review between 2021 and 2023. Therefore, it represents the first volume of what hopefully will be a long-term, ever-evolving editorial collaboration, whose sources of inspiration and goals evolve with the evolving of the broader discussions on decentralized technologies.

Initiated by the Blockchain and Society Policy Research Lab (University of Amsterdam), in collaboration with P2P Models (Universidad Complutense de Madrid), Trust in Distributed Environments (Weizenbaum Institute for the Networked Society, Berlin) and Blockchain Gov teams (Centre National de la Recherche Scientifique, Paris), the project is backed by a solid academic network. However, it strives to exit the academic rooms, and it welcomes contributions from experts, activists and researchers whose perspective is crucial to this discussion.

Valeria Ferrari

Curating a glossary: the discomforts of indexing and defining_

Taxonomies, encyclopedias and glossaries are the legacy of an era - the enlightenment - when knowledge was thought to be describable and depictable in terms of dichotomies and hierarchies. This view of knowledge is assertive and exclusionary; it produces taxonomies and classifications that - as they expand and meet their limits – result to be inconsistent, arbitrary. Collecting, giving meaning and names to objects and phenomena, and organizing the information about them, are exercises of power. What, then, is the function, the utility and the legitimacy of making glossaries and encyclopedias today?

The idea of the Glossary of Decentralised Technosocial Systems arose from the need to define terms that - while being relevant to current discussions about power in the context of digital cultures - remain ill-defined and contested. But the definition of the scope, content and format of the Glossary triggered many questions about the usefulness, feasibility, necessity of such an effort.

What gives an editorial project the "authority" to select and define terms in ways that should be accepted by a broader community of researchers? How can our glossary include multiple and diverse academic and non academic voices, without losing coherence and soundness? How can the tension between terminological definition and dynamism be resolved?

To find possible answers to such questions, we looked at efforts that share some similarities to ours: projects that were inspirational to our initiative, and projects we discovered along the way. We invited the people behind some of these projects to discuss with us how they have addressed, solved or simply thought about these and other questions posed by the fascinating yet problematic task of organizing the terms that are relevant to a discourse.

We found many exciting collections, presenting different formats and sizes, different curatorial approaches and criteria of terms' selection. Le Abécédaire des architectures distribuée (Francesca Musiani, National Centre for Scientific Research), the Glossary of Platforms Law and Policy (Internet Governance Forum), A New AI Lexico (AI Now Institute),

Tecnologie del Dominio (Ippolita), the Posthuman Glossary (Rosi Braidotti & Maria Hlavajova), the Cyberfeminism Index (Mindy Seu) are some of the initiatives that inspire ours.

Looking at these parallel efforts is to reject the claim of universality usually associated with encyclopedic projects. It is also to recognize the importance of asking questions about authority, interdisciplinarity, plurality of approaches and temporal evolution of language, when mapping a discourse.

Gathering information overlaps with its production, with the involvement of those "experts" who are in a position to represent or report about the use and evolution of complex terms. Rather than giving definitive and crystalized answers about meaning, the Glossary is interested in tracing the negation behind its enduring construction and evolution, illuminating the power of multiple discourses and practices that compete in its definition.

This glossary, and in particular this volume, does not want to exhaust the list of terms that are relevant to the discourse on decentralized technologies. Rather, it hopes to broaden someone's vocabulary, literacy and imagination. It opens discussion, it triggers the reader to think of other possible terms, alternative definitions. It is a place from which the gaze can expand, searching for possible technological futures.

The curatorial experience of the two editions of the Glossary here collected showed that collective efforts are powerful; but it also showed that it is not always straightforward, nor frictionless, to unleash such collective power. I truly wished, and tried to architect, from the beginning, a more open, crowdsourced and distributed writing and editing process. I partially failed, and had to rely on some dear old academic editorial practices. I also wished this edition was less white, more explicitly feminist, richer in voices and languages. But these are all goals only partially achieved. These are goals we should keep striving for, not only in the context of this glossary but in any effort of knowledge creation and technological experimentation.

Valeria Ferrari

AD HOC NETWORK_

Kelsie Nabben_ Blockchain Innovation Hub, RMIT University, Australia.
Ellie Rennie_ School of Media and Communication, RMIT University, Australia.

There is no one set definition for the phrase "ad hoc networks". The term refers to the ability for members of a network to establish a network connection between devices. Ad hoc networks are relevant both in technical terms of certain network infrastructures, as well as in terms of the social, political and economic modes of self-organisation they enable. This requires people to combine software and hardware tools to set up peer-to-peer infrastructure that provides access to temporary information networks, as well as networking standards and policy frameworks. When long-standing, these can adapt to become local area networks. An example of an ad hoc network is a temporary cryptocurrency economy, such as a Decentralised Autonomous Organisation, which can connect people, information, and resources online and in person for a specific purpose.

Definition of the term_

"Ad hoc" is Latin for "to this" meaning "for this" or "for this purpose". The term "ad hoc network" refers to the ability for members of a network to establish a network connection between devices. Yet, ad hoc networks are relevant both in technical terms, as well as in terms of the social, political and economic modes of self-organisation they enable. They also depend on technical standards, as well as regulatory and policy frameworks in most settings.

A network can be described as ad hoc when it is self-provided and not reliant on an installed base of pre-existing infrastructure, except where it connects to external services (such as internet gateways). Thus, the attribute of "ad hoc" in a network often pertains to decentralised networks that do not rely on a central point of control. Instead, the network is comprised of "peers" in a network and each peer operates as a "node" to forward packets of data to other nodes.

Ad hoc networks require people to combine software and hardware tools to set up peer-to-peer infrastructure to provide access to temporary

communication networks. Today, smartphone applications can create ad hoc networks through native Bluetooth or WiFi capabilities. This enables new network architectures for access and coordination through digital infrastructure. When long-standing, these can adapt to become local area networks.

The combination of "ad hoc" networks with other technologies, such as blockchain, enables new social, economic, and political possibilities for self-organising. An example of an ad hoc network are temporary cryptocurrency economies which have proven adaptive and responsive for connecting people, information, and resources online, and in person, for time limited and specific purposes before disseminating. For example "Decentralised Autonomous Organisations" (DAOs), such as ConstitutionDAO, which collectively raised millions of dollars in an attempt to buy an original version of the U.S. Constitution, and UkraineDAO, which responded to raise millions of dollars in support of Ukrainian fighters in the conflict with Russia in a matter of days.

Origin_

Ad hoc networks would not have come about if it was not for a number of preceding developments in distributed communications networking research and development, unlicensed spectrum regulations, and open standards.

Distributed computing emerged in the 1960s as a potential solution for more resilient networks against the threat of military attack. While working for military research organisation RAND Corporation in the 1960s and 1970s, Paul Baran authored 13 seminal papers "On Distributed Communications" (RAND Corporation, n.d.). Baran is credited for inventing the idea of "distributed networks", that went on to inform some of the attributes of the internet and ad hoc networking (Yoo, 2018). Distributed networks require that all nodes be connected in a network by multiple links to make a system robust against physical attack. Through these ideas, "it is thus possible to visualise a new set of systems based upon a distributed organisation" (Baran, 1967, 21). The concepts of "packet switching" and "store and forward" data transfer were pioneered to make distributed networking possible. Baran proposed that data could be divided into individual packets termed "message blocks" that would

travel independently through a network and be reassembled once they reach their destination (which later became known as "packet switching", as termed by other independent, simultaneous inventors) (Yoo, 2018). The other fundamental innovation for distributed networking that applies to ad hoc networks is that network data traffic operates on a store and forward routing algorithm to eliminate the vulnerability of a single centralised point of control being targeted by a foreign attack and causing a communications failure across an entire network (Baran, 1967; 1965).

From these origins, ad hoc architecture matters as both a technical architecture and political means for resilience and self-governance, rather than relying on existing infrastructure or third-party provision of infrastructure, as per the example of DAOs.

Evolution_

Ad hoc networks have evolved in terms of usability, security, availability, complexity, and purpose.

Baran's propositions were fundamental for the architecture of the modern-day internet, which was originally an internal network or "intranet" that only authorised parties could access to share information called the Advanced Research Projects Agency Network (ARPANET) (Abbate, 1999). The concepts of "message blocks" and "store -and -forward" concepts laid the foundation for distributed networks to automatically select routes for multi-hop communication between any two nodes on the network. However, the principle of non-hierarchical distributed networking was not adopted in ARPANET, as the attribute of survivability of the network was not a priority (Abbate, 1999). This emission had consequences in the central points of control that manifested in modern day internet architecture, which peer-to-peer decentralised technologies such as public blockchain networks seek to address.

From the late 1960s, researchers at the University of Hawaii developed wireless networking innovations to allow them to send information across islands and to link to ARPANET. The ALOHAnet's random access techniques formed the basis of Wi-Fi and mobile networking (Abramson, 2009). By the 1970s, the packet radio network (PRNET) project was also underway under the sponsorship of the Defense Advanced Research

Projects Agency (DARPA), which is a digital radio communications method that can be used in mobile communications.

The regulatory foundations for legal ad hoc networks was laid by the decision by the US Federal Communications Commission in 1985 to allow unlicensed use of radiofrequency spectrum. This meant that people could access radio frequencies within specific frequency bands, as opposed to co-opting the radiofrequency of others (known as "spectrum piracy"). The wording of the ruling to allow "spread spectrum and other wideband emissions" (FCC, 1984) enabled free market and amateur innovation, resulting in the development of Wi-Fi and other wireless technologies. Without this decision — later replicated in other parts of the world — people would not be legally allowed to establish self-provided wireless networks. Open standards for hardware and software were also an important factor behind the research and development that led to ad hoc networks (Lemstra et al., 2011). For instance, open standards for Wi-Fi technologies enables Wi-Fi router electronics manufacturers to support wireless spectrum networking.

The emergence of personal computing devices such as laptops, local area network (LAN) routers, and smartphones routers have given rise to what is often referred to as "mobile ad hoc networks" (MANETS), which may use Wi-Fi, cellular, Bluetooth or other radio frequency technologies to establish connections between devices. "Ad hoc", in this context, means instances of temporal, networked infrastructure where a central router is not required. In distributed computing, the phrase "ad hoc digital infrastructure" is sometimes used to describe some mobile communication network protocols (Murthy, et. al., 2004; Legendre, et al., 2011).

These dynamic and adaptive networks enable a number of applications where existing infrastructure or a central node is not available, cannot be relied upon, or where scalability is an issue. They may also be used to alleviate digital exclusion by enabling users to share connectivity.

Applications for ad hoc networks_

There are a wide variety of applications of ad hoc networks, some of which are described in the section that follows.

Military_

Military or tactical MANETs are used by military units with emphasis on data rate, real-time requirement, fast rerouting during mobility, data security, radio range, and integration with existing systems (Toh, 2002). Military ad hoc networks offer rapid deployment, infrastructureless, no contact with fixed radio towers, robustness, security, and instant operation. Tactical networks can be formed during a mission and then disappear when the mission is over via mobile, Air Force Unmanned Aerial Vehicle (UAV), Navy ship, or robot.

Humanitarian_

Wireless, ad hoc networks provide communications connectivity in disaster scenarios in circumstances whereby existing infrastructure ceases to function effectively (such as earthquake, flood, storm, or fire), or in remote areas (Leiser et al., 2017). For example, a network run by the Red Hook Initiative, a public housing youth organisation in Brooklyn NY, continued to serve as a communications platform for residents during Hurricane Sandy when mobile telephony and internet services were down (Finlay, 2018).

Community wireless mesh networks_

A mesh network topology refers to a rich interconnection between nodes or devices, whereby each node in the network relays data to other nodes, forming a non-hierarchical network. The resilience of the network increases as more nodes are added, thus reducing dependency on any one connection. In some locales, communities have established community owned wireless mesh networks for internet connectivity, including NYC mesh, Toronto mesh, Freifunk, and GUIFI (NYC Mesh, n.d.; Toronto Mesh, n.d; Freifunk, n.d.; APCNews, 2018). Only one node needs to be connected to the internet for all to be able to access the internet as each node is able to relay data to any other node in the network. Mesh networks organically adapt as people join or leave, and are dynamic, meaning

they automatically reconfigure to guarantee connectivity (Navarro et al., 2018). These networks can be considered "ad hoc" insofar as people can come and go from the network, in definitional terms could transition from being an ad hoc network to a local area network, as hardware and network connection become more fixed, rather than dynamic.

Blockchain-based ad hoc networks_

Blockchains and cryptocurrencies are being used as ad hoc information networks for social coordination. These economic infrastructures are a means for people to transact (transfer value) in a "peer-to-peer" fashion without requiring a third-party service or central intermediary, such as a bank (Nakamoto, 2008, 1). Some scholars have proposed that temporary blockchain networks are a type of "pop up economy" (Rennie, 2019). The organisational framework of "Decentralised Autonomous Organisations" (DAOs) also demonstrates ad hoc, blockchain-based coordination.

One such instance of a "pop-up economy" was the not-for-profit Oxfam's use of the cryptocurrency stablecoin Dai for emergency cash transfers in Vanuatu (Rust, 2019). Oxfam's goal was to trial cash-based aid that could support local economies during disaster relief efforts. Oxfam and their technology partners worked with local vendors to received payments via "Near Field Communication" (NFC) cards that had been distributed to local residents.

Decentralised Autonomous Organisations (DAO), are also a kind of community that can form around a specific objective via network technologies to form an ad hoc network. For example, "Friends with Benefits" is an international social interest DAO that communicates online in a group chat but also holds pop up "in real life" parties and events (Ryce, 2021). "ConstitutionDAO" was a group of people that collectively pooled funds in a failed attempt to purchase an original copy of the United States Constitution (Brown, 2021). A number of funding DAOs have also formed as temporary funding organisations to pool resources and support a common cause, such as in response to the crisis in Ukraine and to subsidise the legal fees to free internet activist Julian Assange (Gottsengen, 2022). DAOs have enabled the rapid, ad hoc mobilisation and direction of resources in a decentralised manner, without relying on a central authority for response coordination.

Coexisting uses and meanings_

Within the discipline of computer science, ad hoc refers to "the capability that members of a network have to build routing information and forward data units from one location to another in the network" (Barbeau and Kranakis, 2007, 63).

In computer networking, an ad hoc network is a self-configured wireless network that allows each wireless node to dynamically forward and receive data. Devices can connect "on the fly" to create a network and share data without certain pre-existing infrastructure, such as a network router. The devices themselves act as the network equipment, creating a network between them.

Ad hoc networks are often referred to as "on the fly", temporary networks (Feeney et al., 2001). Yet, this is not entirely accurate as establishing and maintaining a network can require significant planning and expertise. The maintenance requirements of ad hoc networks demonstrates what Susan Leigh Star referred to as the mundane nature of infrastructure (1999).

Ad hoc infrastructure and ad hoc networks matter because they create opportunities for civic self-organisation. Modular, ad hoc, distributed, cryptographically secure networks are being erected, maintained and dismantled by groups to serve specific ideological purposes and needs, such as censorship resistance (although it should not be assumed that all ad hoc networks are censorship resistant, temporality and encryption can be some avenues for groups to pursue this attribute against perceived threats). . These adaptive, temporary, technology-enabled economies politically and socially challenge the ideological underpinnings of existing institutions through independence, obfuscation, and subversion (Poblet, 2018). An example of the repurposing of ad hoc networking infrastructure for political purposes is the use of the music festival connectivity mobile application "Bridgefy" in Myanmar, when the internet was throttled to censor information during protests (Potkin and Pang, 2021).

Issues currently associated with the term_

There are some issues associated with the concept of "ad hoc" networking. This includes the dependencies between hardware, software, and policy and standards frameworks, network maintenance, and digital inclusion which are addressed below.

The use of ad hoc networks for tethering devices is now commonplace. While this on the fly user practice seems straightforward, ad hoc technologies are better conceived as a suite of nested infrastructures, including specific hardware and software requirements combined with policy frameworks and standards. When some of these components are missing or broken, ad hoc networks may be rendered untenable or unsafe in particular contexts.

Mesh networks in particular have been championed as an alternative to commercially provided internet and telephony services in areas where affordability is a barrier to connectivity. Yet, ad hoc networks can be cumbersome to establish and maintain in terms of expertise and resources,as well as broader context expectations and limitations of ad hoc networks as a technical or socio-political solution. Such networks require a significant amount of skills and labour to establish and maintain -resources that are more likely to be present in affluent areas (Powell, 2008). Where mesh networks are used to provide internet services they are also dependent on backhaul service providers, which typically require a contract or agreement with a commercial company or municipal government. Regulatory conditions may impede ad hoc networks by making users liable for the activities of others on the network or requiring the retention of metadata for policing (Giovanella, 2016). Some ad hoc networks can also not be fit-for-purpose for the applications that people adopt. For example, during the Occupy Wall st protests, spontaneous ad hoc networks were not sufficient to provide continuous service (Baccelli, 2012). In disaster scenarios, resilience is largely attributed to community capacity to prepare, respond, and recover, as well as the capabilities afforded by communications infrastructure (Norris et al., 2008).

In some respects, ad hoc networks can create opportunities for digital inclusion. For example, ad hoc networks can allow multiple people to

share one internet connection in remote or rural areas, provide free or cheaper access, or extend connectivity to areas previously beyond range, depending on the devices and geography of the network. On the other hand, ad hoc networks also possess elements of digital exclusion. For example, establishing and maintaining a network can require access to specific hardware or a pre-existing infrastructure, such as a mobile network, satellite, or router. Participation can also require a certain level of digital literacy. In some cases, such as the political examples mentioned above, exclusion of unwanted participants could be considered a feature, not an issue.

Conclusion_

At its most basic definition, the term "ad hoc network" refers to the ability for members of a network to establish a network connection between devices. Yet, this capability is representative of a broader socio technical phenomenon, as ad hoc networks are enablers of social organisation and innovation. Ad hoc networks require communities of people to combine software and hardware tools, as well as standards, and regulatory and policy frameworks.

In this piece, we have explored the origins and history of developments in "ad hoc networks", demonstrated the co-existing uses and meaning of the term "ad hoc" across the disciplines of computer science and the social sciences, and then related this to examples of current technological developments and applications. We then explored co-existing meanings and uses, as well as issues and limitations of access, maintenance, and inclusion and exclusion. Finally, we demonstrated some ways in which the combination of "ad hoc" networks with other technologies enable new social, economic, and political possibilities for self-organising, such as communications during protests, pop-up economies, and DAOs.

This brief history and context of ad hoc networks has outlined the technical requirements, as well as the communities, standards, and socio-political needs and purposes of ad hoc networks. This shows how the development of technology networks are embedded in socio-political dynamics in the ways that people use technology and media for technological innovation.

References_

- Abbate, J. (1999). *Inventing the Internet*. MIT Press.
- Abramson, N. (2009). The AlohaNet: Surfing the wireless data. *IEEE Communications Magazine*, *47*(12), 21–25. https://doi.org/10.1109/MCOM.2009.5350363
- APCNews. (2018, March 12). *Guifi.net: Accessible and affordable 5G network architecture*. Association for Progressive Communications. https://www.apc.org/en/news/guifinet-accessible-and-affordable-5g-network-architecture.
- Baccelli, E. (2012). *IP-disruptive wireless networking: Integration in the Internet*. Université Pierre et Marie Curie. https://tel.archives-ouvertes.fr/tel-00770791
- Baran, P. (1965). *A briefing on the distributed adaptive message-block network*. RAND Corporation. https://www.rand.org/pubs/papers/P3127.html
- Baran, P. (1967). *Some remarks on digital distributed communications networks*. RAND Corporation. https://www.rand.org/pubs/papers/P3536.html
- Baraniuk, C. (2014, June 14). FireChat warns Iraqis that messaging app won't protect privacy. *WIRED*. https://web.archive.org/web/20150917061844/http://www.wired.co.uk/news/archive/2014-06/25/firechat
- Barbeau, M., & Kranakis, E. (2007). *Principles of ad-hoc networking*. John Wiley & Sons.
- Brown, A. (2021). *Crypto investors lose out in $43.2 million sale of rare copy of U.S.* Forbes. https://www.forbes.com/sites/abrambrown/2021/11/18/constitution -dao-crypto-ether-constitutional-sothebys-sale-auction/?sh=54efaeb66ad4.
- FCC. (1984). Further Notice of Inquiry and Notice of Proposed Rule Making adopted regarding authorization of spread spectrum and other wideband emissions not presently provided for in FCC Rules and Regulations Notice of Proposed Rulemaking. General Docket #: FCC-81–413. In *Federal Communications Commission Reports: Advance Reports* (pp. 380–401). Federal Communications Commission.
- Fenney, L. M., Ahlgren, B., & Westerlund, A. (2001). Spontaneous networking: An application oriented approach to ad-hoc networking. *IEEE Communications*. https://doi.org/10.1109/35.925687
- Finlay, A. (2018). Cutting a line of sight for community connectivity. In

A.P.C.-I.D.R.C. (Ed.), *Global Information Society Watch 2018: Community Networks* (pp. 59–63). https://www.apc.org/sites/default/files/2018_community_networks.pdf

- Freifunk. (n.d.). *What is Freifunk about? How to join us?* Freifunk. https://freifunk.net/en/
- Giovanella, F. (2016). Community networks: Legal issues, possible solutions and a way forward in the European Context. In L. Belli (Ed.), *Community connectivity: Building the Internet from scratch: Annual report of the UN IGF Dynamic Coalition on Community Connectivity* (pp. 111–122). FGV Direito Rio. http://hdl.handle.net/10438/17528
- Gottsengen, W. (2022). *New DAO Raises $3M in ETH for Ukrainian Army*. CoinDesk. https://www.coindesk.com/tech/2022/02/27/new-dao-raises-3-million-in-eth-for-ukrainian-army/.
- Legendre, F., Hossmann, T., Sutton, F., & Plattner, B. (2011). 30 years of wireless Ad Hoc networking research: What about humanitarian and disaster relief solutions? What are we still missing? *Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief (ACWR'11*, 217–217. https://doi.org/10.1145/2185216.2185279
- Lemstra, W., Hayes, V., & Groenewegen, J. (Eds.). (2011). *The innovation journey of Wi-Fi: The road to global success*. Cambridge University Press.
- Lieser, P., Alvarez, F., Gardner-Stephen, P., Hollick, M., & Boehnstedt, D. (2017). Architecture for responsive emergency communications networks. *2017 IEEE Global Humanitarian Technology Conference (GHTC)*, 1–9. https://doi.org/10.1109/GHTC.2017.8239239
- Murthy, C. S. R., & Manoj, B. S. (2004). *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall/PTR.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.
- Navarro, L., Maccari, L., & Lo Cigno, R. (2018). At the limits of the network: Technology options for community. In A.P.C.-I.D.R.C. (Ed.), *Global Information Society Watch 2018: Community Networks* (pp. 13–20). https://www.apc.org/sites/default/files/2018_community_networks.pdf
- Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology*, *41*(1–2), 127–150. https://doi.org/10.1007/s10464-007-9156-6

- NYC Mesh. (n.d.). *Join our community network!* https://www.nycmesh.net/
- Poblet, M. (2018). Distributed, privacy-enhancing technologies in the 2017 Catalan referendum on independence: New tactics and models of participatory democracy. *First Monday*. https://doi.org/1583508256
- Potkin, F., & Pang, J. (2021). *Offline message app downloaded over million times after Myanmar coup*. Reuters. https://www.reuters.com/article/us-myanmar-politics-bridgefy-idUSKBN2A22H0.
- Powell, A. (2008). WiFi publics: Producing community and technology. *Information, Communication & Society*, *11*(8), 1068–1088. https://doi.org/10.1080/13691180802258746
- RAND Corporation. (n.d.). *Paul Baran* [RAND Corporation]. https://www.rand.org/pubs/authors/b/baran_paul.html
- Rennie, E. (2019). One night in the blockchain economy [Medium]. *Altcoin Magazine*.https://medium.com/the-capitalone-night-in-the-blockchain-economy-d6eeea1d2cdf.
- Rust, B. (2019). *Unblocked cash: Piloting accelerated cash transfers in Vanuatu* [Report]. Oxfam Australia. https://policy-practice.oxfam.org/resources/unblocked-cash-piloting-accelerated-cash-transfer-delivery-in-vanuatu-620926/.
- Ryce, A. (2021). Decentralized autonomous organizations and the promise of utopia. *RA Magazine*. https://ra.co/features/3914.
- Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, *43*(3), 377–391. https://doi.org/10.1177/00027649921955326
- Toh, C. K., Lee, E. C., & Ramos, N. A. (2004). Next-generation tactical ad hoc mobile wireless networks. *Technology Review Journal*, *125*(SB).
- Toronto Mesh. (n.d.). *Toronto Mesh*. https://tomesh.net/
- Yoo, C. S. (2018). Paul Baran, network theory, and the past, present, and future of the Internet. *Colorado Technology Law Journal*, *17*(1), 161–186.

BLOCKCHAIN GOVERNANCE_

Aron Fischer, Colony, New York, United States.
María-Cruz Valiente, Universidad Complutense de Madrid, Spain.

Blockchain governance can be regarded as the integration of norms and culture, the laws and the code, the people and the institutions that facilitate coordination and together determine a given organisation.

Origin and competing definitions_

The importance of governance is well recognised in the information technology (IT) industry (ITSM Library, 2008) and this term is widely used in academic, economic and policy debates. In the blockchain space, this term has been tightly linked to *Decentralised Autonomous Organisations* (DAOs) (Buterin, 2013). Unfortunately, there is no common understanding, or generally accepted formal definition of *governance*, when associated with blockchain-based technologies. In pursuit of a formalisation of this term, before going more deeply into its evolution in the context of blockchain technology, we will briefly chart out a few common definitions.

The origins and most common approaches to governance are thoroughly dealt with by Hufty (2011), and as stated by Bevir (2011), at the most general level, governance can be associated with *"theories and issues of social coordination and the nature of all patterns of rule".* The Oxford English Dictionary defines governance as *"the action or fact of governing a nation, a person, an activity, one's desires, etc.; direction, rule; regulation."* In an economics context, governance is defined as *"the use of institutions, structures of authority and collaboration to allocate resources and coordinate the effort and activity in society or in the economy"* (Bell, 2002).

On the other hand, from an IT *perspective*, governance is composed of the leadership and the set of structures and processes that guarantee that the IT of an organisation provides support and extends the organisation's strategy and objectives in a manner that is focused on achieving a better alignment between the business and IT (van Bon, de Jong & Pieper, 2008). In contrast, Margaret Blair notes that corporate governance is *"the whole set of legal, cultural, and institutional arrangements that determine what publicly*

traded corporations can do, who controls them, how that control is exercised, and how the risks and returns from the activities they undertake are allocated" (1995, p. 3), as quoted in Clarke (2012). However, the meaning of corporate governance could vary considerably according to the values, institutions, culture and objectives pursued by each organisation as well as the corporate governance system in the jurisdiction where the corporation is registered (Pollman, 2019; Norbäck & Persson, 2009). Corporate governance is not just about accountability, and it has an important role enabling strategising, value creation and innovation, as highlighted by Kraakman et al. (2017).

In this context, Morell (2014) presents the term *community governance* which is defined as the direction, control and coordination of a dynamic process, which evolves over time and manages several aspects of power classified by eight interrelated categories, from 'cultural principles/social norms' and 'formal rules or policies', to 'infrastructure provision'.

Academic review of the term in the blockchain domain_

Despite the gap in literature due to the lack of a formal, comprehensive and holistic definition of what governance means in different domains, we can find several papers focused on governance whose approaches are applied or could be applied to blockchain technology.

For example, Reijers et al. (2016) explore how blockchain technology enables the configuration of specific forms of political organisation using the Ethereum network as a case study, based on the idea that the blockchain can act as a legal framework that provides the basis for online interactions of any kind in terms of governance.

Similarly, Davidson et al. (2016) share the idea that by eliminating the need for trust of agreed contracts through consensus and transparency, blockchains enable a new type of governance for autonomous organisations with the legal coordination properties of a market. Further, the governance attached to these decentralised autonomous organisations could be implemented as blockchain-based software systems through smart contracts (i.e., small pieces of code deployed on the blockchain) (De Filippi & Wright, 2018). Although the fact that the blockchain is operated autonomously,

could itself raise problems for corporate governance, such as corporate record-keeping and the maintenance and upgrading of blockchains themselves (Yermack, 2017).

Another approach is the use of notions of governance of the commons derived from the study of natural resources, particularly the work of the Nobel-laureate Elinor Ostrom (1990) as the basis for blockchain-based self-governance (Rozas et al., 2018). They identify and conceptualise six affordances that blockchains may provide including tokenisation, formalisation and decentralisation of rules, autonomous automatisation, decentralisation of power over the infrastructure, increase in transparency and codification of trust.

Data governance is another less explored approach presented by Micheli et al. (2020). In their work, governance is defined as the power relations between all the actors affected by, or having an effect on, the way data is accessed, controlled, shared and used, the various socio-technical arrangements set in place to generate value from data, and how such value is redistributed between actors.

Finally, in another line of research, Karjalainen (2020) presents an informative survey of governance models in blockchain-based decentralised networks. It is worth highlighting that consensus mechanisms inherent in blockchain transactions have been excluded from this study.

Usage of the term 'blockchain governance'_

We find relevant visions of governance in the context of blockchain, for instance, in the works presented by Finck (2018) and Reijers et al. (2018). However, as mentioned earlier, the academic research for *blockchain governance* is still somewhat sparse (see also: Pelt et al., 2020), and while governance is a much discussed topic at blockchain conferences, such as Ethereum Devcon, the annual conference for all Ethereum developers, researchers, thinkers, and makers (DevCon Archive, n.d.); *Community Ethereum Development Conference* (EDCON, n.d.); *Ethereum Community Conference* (ETHCC, n.d.); and DAOfest, an event series focused on advancing the technology and adoption of decentralised governance globally (DAOfest, n.d.), the written record still comprises mostly blog posts and social media entries of dubious quality.

As stated previously, all governance is ultimately a social construct, comprising not simply laws (or bylaws), but also norms, culture, institutions, and individuals. Despite impassioned claims to the contrary, this is no different in regard to blockchains.

To understand the (mis-)usage of the notion of *blockchain governance*, we must first consider what specifically blockchains bring to the table: they enable systems in which adherence to procedure is automatically enforced, relying neither on norms nor a legal system, and leaving no room for individual discretion. This strict separation of enforceable procedure on the one hand and norms and discretion on the other is genuinely novel, but its import is exaggerated. Among the more enthusiastic supporters of blockchain technology, we observe a tendency to wilfully ignore all questions of norms and culture and equate *governance* entirely with coded procedures (*code is law*). Once all governance is reduced to procedure, it is hard to resist the claim that blockchains change everything.

This mixture of confusion and hubris is exemplified nicely in Singh (2020), who introduces "standard" governance as being either *direct governance* or *representative governance*, thus conflating governance with voting procedures, and asserting that everything is different with the blockchain: *"We can broadly categorize the governance types into two major categories: Standard Governance and Blockchain Governance"* (n.p.).

A further ambiguity stems from the fact that *blockchain governance* is used in two related but distinct contexts — governance of the chain itself vs governance using the chain. Additionally, usage in the first context is further complicated by the highly polarised and politicised nature of the blockchain space where we observe different factions reinterpreting and redefining the phrase to fit their outlook.

In this first usage, *blockchain governance* refers to *governance of the blockchain* (i.e. the specific question of making consensus-relevant changes to the software running a blockchain). *Consensus relevance* here means a change to the internal rules of the blockchain that must be applied (i.e., software must be updated) by all relevant participants in the blockchain network such as cryptocurrency exchanges, wallet software providers, miners, and users. If a large enough portion of the network does not apply the

changes, then the network splits into two: those following the new rules and those following the old rules — this is called a *hard fork*[1].

Examples of this approach include: (i) Curran (2020), who uses *blockchain governance* to vaguely mean whatever process leads to consensus-relevant changes in the software, and hard forks are hailed as a safety valve for users to choose their own fork if things go awry; and (ii) Rajarshi (2020), where governance is conflated with voting procedures, and hard forks are hailed as enabling *"much more flexibility in operation than traditional structures"* because *"a user is free to choose which blockchain to follow."*

In this context, we typically observe the introduction of a strict separation of governance into *off-chain governance* and *on-chain governance*.

The main idea of *on-chain governance* is to use coded procedures within a blockchain that represent voting procedures by which decisions about consensus-relevant software upgrades are mediated through the consensus system itself. Usage of the term in industry is neatly summarised by Frankenfield (2018): *"On-chain governance is a system for managing and implementing changes to cryptocurrency blockchains. In this type of governance, rules for instituting changes are encoded into the blockchain protocol. Developers propose changes through code updates and each node votes on whether to accept or reject the proposed change".*

Proponents of this way of doing things disparage the off-chain (human) world as being outdated in its reliance on people, norms, and culture to achieve *governance*, specifically alleging that procedures might be ill-defined or opaque: "off-chain collectives that organize over phone calls or at conferences, which either leads to shadow hierarchies where only a few, unwritten people make decisions" (Petrowski, 2020, n.p.). Central to this line of thought is that anything on-chain is transparent and thus fair, and anything off-chain is hidden and potentially nefarious. This stands in contrast to the Bitcoin notion that *all* consensus relevant changes are bad because they represent human involvement and in as much as code is law, they are breaking the law (De Filippi & Wright, 2018). On-chain governance, they argue, only aids and abets such law breaking; arguing that the goal is not coordinated updates to the network, but immutability.

The other context in which *blockchain governance* is used ignores the previous question entirely and focuses on using the blockchain to achieve governance.

It presupposes the existence of a functioning blockchain network such as Ethereum, which can be leveraged to deploy smart contracts that encode the procedures of a decision-making paradigm. The blockchain is used to force/guarantee adherence to procedure, but the decisions being made have nothing to do with the blockchain itself (i.e., upgrading, avoiding hard forks). Rather, the goal of this form of *on-chain* governance is to enable the creation and operation of DAOs (i.e., organisations whose bylaws are written in code and enforced by the blockchain).

Once a DAO has been deployed to a blockchain, its rules can no longer be changed — short of a hard fork of the underlying network. Envisioning the need for future changes, DAO authors must incorporate the rules-for-changing-the-rules in the original deployment. We may think of this as analogous to an ordinary legislative process, coupled with a process for amending the constitution that the legislation is based on.

Current prominent examples of DAO platforms such as Aragon (Aragon, n.d.) and Daostack (DAOstack, n.d.) place heavy emphasis on a process in which proposals — usually to reallocate cryptocurrency funds — are put forward, a voting procedure then determines passage of the proposal, and eventually the funds are moved. This all happens on the blockchain, though off-chain communication and discussion are alluded to. Other examples such as Colony (Rea et al, 2020) take a more holistic view of governance, involving primarily off-chain interactions between human beings to come up with ideas and make decisions, and usage of the blockchain is reserved for enforcement, as opposed to decision making, whenever this is feasible.

It is worth noting that all DAO projects are ultimately a mixture of off-chain and on-chain elements, echoing the idea that even with blockchains and cryptocurrencies, governance consists of more than coded procedures.

Conclusion_

As we have seen, the concept of *blockchain governance* is still under development and it can be understood differently depending on the domain of the application area under discussion.

In a broad sense, *blockchain governance* can be regarded as the integration of norms and culture, the laws and the code, the people and the institutions that facilitate coordination and together determine a given organisation. Importantly it refers to the entirety of motivations, rules, and activities that feed into the establishment of choices and subsequently deciding on them, and includes, but is not limited to, any coded on-chain rules that guide these processes. However, *blockchain governance* also refers to two distinct dimensions: off-chain governance vs on-chain governance.

When referring strictly to smart contracts, one should specify that one is referring specifically to the on-chain elements of the governance system in question. Further care should also be taken to clarify whether one is talking about governance of a blockchain's own consensus relevant rules, or whether the governance system in question is merely using a blockchain to enforce on-chain rules in an otherwise unrelated off-chain domain.

References_

- *Aragon*. (n.d.). https://aragon.org/
- Bell, S. (2002). *Economic governance and institutional dynamics*. Oxford University Press.
- Bevir, M. (Ed.). (2011). *The SAGE handbook of governance*. SAGE. https://doi.org/10.4135/9781446200964
- Blair, M. M. (1995). *Ownership and Control: Rethinking Corporate Governance for the Twenty-First Century*. Brookings Institution Press.
- Buterin, V. (2013). *Ethereum whitepaper: A next-generation smart contract and decentralized application platform* [White Paper]. https://ethereum.org/en /whitepaper/
- Clarke, T., & Branson, D. (Eds.). (2012). *The SAGE handbook of corporate governance*. SAGE Publications.
- Curran, B. (2020, July 30). *What is Blockchain Governance? Complete Beginner's Guide*. Blockonomi.https://blockonomi.com/blockchain-governance/
- *DAOfest*. (n.d.). https://daofest.io
- *DAOstack*. (n.d.). https://daostack.org/
- Davidson, S., De Filippi, P., & Potts, J. (2016). *Economics of Blockchain*. https://doi.org/10.2139/ssrn.2744751
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of*

code. Harvard University Press.
- *DevCon Archive: The annual conference for all Ethereum developers, researchers, thinkers, and makers*. (n.d.). https://archive.devcon.org/
- *EDCON: Community Ethereum Development Conference*. (n.d.). https://edcon.io/
- *EthCC: Ethereum Community Conference*. (n.d.). https://ethcc.io/
- Finck, M. (2019). *Blockchain regulation and governance in europe*. Cambridge University Press. https://doi.org/10.1017/9781108609708
- Frankenfield, J. (2018). *On-Chain Governance*. Investopedia. https://web.archive.org/web/20200224034437/https://www.investopedia.com/terms/o/onchain-governance.asp
- Hufty, M. (2011). Governance: Exploring Four Approaches and Their Relevance to Research. In U. Wiesmann (Ed.), *Research for Sustainable Development: Foundations, Experiences, and Perspectives* (pp. 165–183). Geographica Bernensia. http://nccr-north-south.ch/Upload/8_Hufty.pdf
- ITSM Library. (2008). *IT Service Management Global Best Practices* (Vol. 1). Van Haren Publishing.
- Karjalainen, R. (2020). *Governance in Decentralized Networks*. https://doi.org/10.2139/ssrn.3551099
- Kraakman, R., Armour, J., Davies, P., Enriques, L., Hansmann, H., Hertig, G., Hopt, K., Kanda, H., Pargendler, M., Ringe, W.-G., & Rock, E. (2017). *The Anatomy of Corporate Law: A Comparative and Functional Approach*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198739630.001.0001
- Micheli, M. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2). https://doi.org/10.1177/20539517 20948087
- Morell, M. F. (2014). Governance of Online Creation Communities for the Building of Digital Commons: Viewed through the Framework of Institutional Analysis and Development. In B. M. Frischmann, M. J. Madison, & K. J. Strandburg (Eds.), *Governing Knowledge Commons* (pp. 281–312). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199972036.003.0009
- Norbäck, P.-J., & Persson, L. (2009). The Organization of the Innovation Industry: Entrepreneurs, Venture Capitalists, and Oligopolists. *Journal of the European Economic Association*, *7*(6), 1261–1290. https://doi.org/10.1162/JEEA.2009.7.6.1261
- Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions*

for Collective Action. Cambridge University Press. https://books.google.co.uk/books?id=4xg6oUobMz4C

- Pelt, R., Jansen, S., Baars, D., & Overbeek, S. (2020). Defining Blockchain Governance: A Framework for Analysis and Comparison. *Information Systems Management*, *38*(1), 21–41. https://doi.org/10.1080/10580530.2020.1720046
- Petrowski, J. (2020, June). *Polkadot Governance*. Polkadot. https://polkadot.network/polkadot-governance/
- Pollman, E. (2019). Startup Governance. *University of Pennsylvania Law Review*, *168*(1), 155. https://scholarship.law.upenn.edu/faculty_scholarship/2135/
- Rajarshi, M. (2020). *What is Blockchain Governance: Ultimate Beginner's Guide*. Blockgeeks. https://blockgeeks.com/guides/what-is-blockchain-governance-ultimate-beginners-guide/
- Rea, A., Kronovet, D., Fischer, A., & du Rose, J. (2020). *Colony* [White Paper]. https://colony.io/whitepaper.pdf
- Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. *Ledger*, *1*, 134–151. https://doi.org/10.5195/ledger.2016.62
- Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Vélez, A. C., & Orgad, L. (2018). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi*. https://doi.org/10.1007/s11245-018-9626-5
- Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2018). *When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance*. https://eprints.ucm.es/id/eprint/59643/1/SSRN-id3272329.pdf
- Singh, N. (2020, August 19). *Blockchain Governance Principles: Everything You Need To Know*. 101 Blockchains. https://101blockchains.com/blockchain-governance/
- van Bon, J., de Jong, A., & Pieper, M. (Eds.). (2008). *IT service management global best practices* (Vol. 1). Van Haren.
- Yermack, D. (2017). Corporate Governance and Blockchains. *Review of Finance*, *21*(1), 7–31.[https://doi.org/10.1093/rof/rfw074

Endnotes_

1. This term itself is not well defined. Thus *hard fork* may refer to a network split where different actors in the network follow different rules, whether due to an update that was not universally installed or due to a software flaw; but it is also used to describe a successful network upgrade that could have led to a split but did not.

BLOCKCHAIN-BASED TECHNOLOGIES_

María-Cruz Valiente, Universidad Complutense de Madrid, Spain.
Florian Tschorsch, Distributed Security Infrastructures, Technical University Berlin, Berlin.

Blockchain-based technologies can be understood as a distributed network of computers, ideally organised in a decentralised way, mutually agreeing on a common state while tolerating failures (incl. malicious behaviour) to some extent.

Definition_

Blockchain-based technologies can be understood as a distributed network of computers, ideally organised in a decentralised way, mutually agreeing on a common state while tolerating failures (incl. malicious behaviour) to some extent.

Origin and evolution of the term_

In recent years, blockchain(-based) technologies have attracted the interest of a wide variety of actors and stimulated a large amount of academic research. The topic is increasingly part of academic and public debates. Unfortunately, there is neither a formal definition nor a common understanding of what *blockchain-based technologies* means, that is, what properties and technical features the term implies. Therefore, a good understanding of the term *blockchain* is needed to design, develop, and manage such technologies effectively, especially also for researchers and society concerned with the intention to use and their actual usage. The main question that needs to be answered is: what fundamental requirements have to be met in order for a proposal or solution to be classified as blockchain technology?

According to the literature, there are several concepts and aspects to be taken into account when defining the inherent properties associated with blockchain technologies. The main attempts to define the notion of blockchain technologies can be summarised as follows: a network composed of decentralised databases or distributed computing nodes

sharing a global data structure to record chronologically connected blocks of transactions, which use cryptographic techniques and distributed consensus that lead to secure, transparent and immutable distributed ledgers (García-Barriocanal et al., 2017, p. 39; Governatori et al., 2018, pp. 385 ff; Iansiti & Lakhani, 2017). The network executes smart contracts (i.e., a programme) as transactions (Staples et al., 2017), and should provide trust, anonymity, security, and data integrity without requiring any third party controlling the process (Janssen et al., 2020).

The complex relationships between all the aspects concerned with governance, business information (namely business processes), and technical issues that must be taken into account in the adoption process of blockchain technologies are presented in the work of Janssen et al. (2020).

In summary, we observe that the meaning of the word *blockchain* is and remains controversial. It has no standard technical definition. Rather it is used as a loose umbrella term to refer to systems that bear resemblance to the Bitcoin protocol, or more generally the Nakamoto Consensus (Narayanan & Clark, 2017). At the same time, blockchain technologies are influenced by other research areas and existing technologies, e.g., peer-to-peer networks, fault tolerance, distributed timestamping, and cryptography (Tschorsch & Scheuermann, 2016; Narayanan & Clark, 2017). In order to facilitate an unambiguous understanding of blockchains, they have been classified as a subset of *Distributed Ledger Technologies* (DLTs). Hence, DLT becomes the technical accurate term, referring to consensus of replicated data in a peer-to-peer network.

Issues currently associated with the term_

Blockchain technology originally emerged to support new forms of digital money. It was first proposed in the birth of *Bitcoin* by Satoshi Nakamoto in 2008 and presented at a time where the trust in banks and other financial institutions was at a low due to the world-wide financial crisis. In short, Bitcoin can be defined as the first and (at the time of writing) most popular cryptocurrency. It consists of a digital currency (i.e., bitcoin) and online payments (i.e., the Bitcoin network), which operates independently of a central bank (Swan, 2015). In this way, Karlstrøm (2014) defends that payments performed through Bitcoin avoid the services of a middleman, such as commercial banks, lawyers, and notaries, which

destabilises adopted state monopolies on the production and verification of money and transactions. Since the blockchain records every single change made in the network (first and foremost to reject double spends), Bitcoin probably became the most transparent financial system. In the following, we look beyond Bitcoin to convey the technological diversity with respect to blockchains. By doing this, we intend to emphasise the difficulties to capture this technology in a single definition.

By the end of 2013, Vitalik Buterin created *Ethereum*, a general-purpose blockchain-based distributed computing technology (Buterin, 2014). Using Ethereum, developers can create web applications known as *decentralized applications* (dapps) without knowledge about the underlying mechanisms, such as peer-to-peer networks and blockchain in general.

However, eleven years have passed since the invention of Bitcoin and seven years since Ethereum was first presented and no widely accepted definition for blockchain technology exists yet. A prime example to highlight the ambiguity of the term *blockchain* is the tension between so-called *permissionless* and *permissioned blockchains*. *Permissionless blockchains*, such as Bitcoin, do not require a permission to contribute to the consensus. The permission to generate a new block is organised in a completely decentralised manner. In contrast, permissioned blockchains, such as Hyperledger, define a closed group of nodes, who can contribute to the consensus. This group is often determined by a central entity. In the literature, both are referred to as blockchains. While permissionless blockchains are clearly in line with the Nakamoto consensus, permissioned blockchains exhibit more resemblance to the area of Byzantine fault tolerance (Lamport, Shostak, & Pease, 2019). Agreement protocols offering this particular type of fault tolerance typically require a well-defined distributed system. Such ambiguities between permissionless and permissioned blockchains and many more misconceptions motivated articles that explore suitable application domains of blockchains by trying to give an answer to the question "do you need a blockchain?" (Wüst & Gervais, 2018). This dissonance clearly emphasises the issues that we observe with the definition of the term blockchain.

Conclusion_

Blockchains are supposed to offer diverse technological possibilities. With a range of use cases that go far beyond virtual currencies applications, they are proposed as a technological means to achieve trust, security, and privacy. After more than a decade of research and experimentation, however, the utility of blockchains seems to be circumscribed to few use cases, with cryptocurrencies still representing their most relevant application.

The value proposition of blockchain seems to be that of offering a global, open and censorship-resistant network for peer-to-peer transactions. Its key innovation is the deployment of consensus algorithms that offer reasonable security in open peer-to-peer networks. The main characteristics attributed to blockchain-based technologies include: (i) decentralised consensus, i.e., no central entity or third party is responsible for decision-making; (ii) immutable archive, i.e., an ordered list of transactions that cannot be removed or altered; (iii) transparency and verifiability, i.e., all recorded entries can be accessed and verified locally; (iv) resilience to failure, i.e., the system can handle Byzantine failure up to a certain threshold.

The term *blockchain* remains vague, even controversial. Sometimes, the term 'blockchain technology' instead of 'blockchain' is preferred in order to remark that blockchain is concerned about computers or technical aspects. Often, the term is used merely to point at the ideologies that have been attached to it, with imprecise references to technological specifications. This makes it difficult to classify a given application as blockchain-based technology. While not clearly defined, blockchains typically exhibit a resemblance to Bitcoin, which is commonly considered its archetypal example, repeating its technical characteristics or following similar goals. From a purely technical point of view, blockchains are a type of DLT. Therefore, they can be understood as a distributed network of computers, ideally organised in a decentralised way, mutually agreeing on a common state while tolerating failures (incl. malicious behaviour) to some extent.

References_

- Buterin, V. (2014, January 23). Ethereum: A Next-Generation Cryptocurrency And Decentralized Application Platform. *Bitcoin Magazine*. https://bitcoinmagazine.com/business/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211
- García-Barriocanal, E., Sánchez-Alonso, S., & Sicilia, M.-A. (2017). Deploying Metadata on Blockchain Technologies. In E. Garoufallou, S. Virkus, R. Siatri, & D. Koutsomiha (Eds.), *Metadata and Semantic Research* (pp. 38–49). Springer International Publishing. https://doi.org/10.1007/978-3-319-70863-8_4
- Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, *26*, 377–409. https://doi.org/10.1007/s10506-018-9223-3
- Iansiti, M., & Lakhani, K. R. (2017, January). The Truth About Blockchain. *Harvard Business Review*, *95*, 118–127. https://hbr.org/2017/01/the-truth-about-blockchain
- Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, *50*, 302–309. https://doi.org/10.1016/j.ijinfomgt.2019.08.012
- Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Journal of Social Theory*, *15*(1), 23–36. https://doi.org/10.1080/1600910X.2013.870083
- Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In *Concurrency: The Works of Leslie Lamport* (pp. 203–226). https://doi.org/10.1145/3335772.3335936
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, *60*(12), 36–45. https://doi.org/10.1145/3132259
- Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A. B., Weber, I., Xu, X., & Zhu, J. (2017). *Risks and opportunities for systems using blockchain and smart contracts* [Technical report]. Data61 (CSIRO). https://doi.org/10.4225/08/596E5AB7917BC

- Swan, M. (2015). *Blockchain: Blueprint for a new economy* (First edition.). O'Reilly.
- Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3). https://doi.org/10.1109/COMST.2016.2535718
- Wüst, K., & Gervais, A. (2018). Do you need a blockchain? *Crypto Valley Conference on Blockchain Technology (CVCBT 2018)*. https://doi.org/10.1109/CVCBT.2018.00011

CRYPTOCURRENCY_

Ingolf G. A. Pernice, Weizenbaum Institute, Berlin, Germany.
Brett Scott, Independent, Berlin, Germany.

A cryptocurrency system can be understood as a system intended for the issuance of tokens which are intended to be used as a general or limited-purpose medium-of-exchange, and which are accounted for using an often collectively-maintained digital ledger making use of cryptography to replace trust in institutions to varying extents. Against such a backdrop, the singular term cryptocurrency can mean a token, intended to be used as a general or limited-purpose medium-of-exchange, issued via a cryptocurrency system.

Definition_

A cryptocurrency system can be understood as a system intended for the issuance of tokens which are intended to be used as a general or limited-purpose medium-of-exchange, and which are accounted for using an often collectively-maintained digital ledger making use of cryptography to replace trust in institutions to varying extents. Against such a backdrop, the singular term cryptocurrency can mean a token, intended to be used as a general or limited-purpose medium-of-exchange, issued via a cryptocurrency system.

Origin and evolution of the term_

The term *cryptocurrency* entered public usage with the surge of Bitcoin in 2008 — a protocol aimed at enabling a network of people connected together via peer-to-peer digital communications infrastructure to issue digital tokens and transfer them between themselves whilst securing the process through cryptography (Nakamoto, 2008). While the original proposition did not use the term *cryptocurrency*, Nakamoto presented the project as a peer-to-peer 'currency' in a network and cryptography mailing list (Nakamoto, 2009).The term 'cryptocurrency', however, soon gained traction in online-chatter (compare HXN (2009) and print media (e.g., Davis, 2011).[1] An early distinction was made between the protocol-using the capitalised term *Bitcoin*-and the tokens, which used the lower-case term *bitcoin*. New bitcoins are 'written into existence' by a network participant

(a so-called miner) who has succeeded in transforming the format of a bundle of proposed transactions (of previously issued bitcoins, along with a single request to issue new ones as a reward) in such a way that the bundle can be hitched to a chain of previously hitched bundles.

The remainder of this section attempts to explain how this protocol, and immediate descendants, might have shaped the term *cryptocurrency*.

The role of cryptography in early cryptocurrencies_

The word stem *crypto* within the term *cryptocurrency* might be seen as surrogate for *cryptography*, but could also have emerged from the cypherpunk movement, who identified "anonymous cash and other untraceable payment systems" (De Filippi & Wright, 2018, p. 19) as enabling feature within a *crypto-anarchy* (Ludlow, 2001, p. 4). Bitcoin's mission of leveraging "cryptographic proof instead of trust" (Nakamoto, 2008, p. 1) resonates with the above. The exact protocol specifications of Bitcoin and its descendants are summarised in Scheuermann and Tschorsch (2016). Cryptography enters its architecture in various ways. A few examples are the integrity of, and consensus on a joint transaction history as well as the authorisation setup for sending tokens. However, the use of the surrogate *crypto* for Bitcoin is slightly arbitrary in the sense that earlier attempts at creating digital currencies (compare e.g. Chaum, 1988) relied heavily on cryptographic techniques as well. Nevertheless, it might seem justified by the fact that cryptography plays a far more central role for Bitcoin than it does for national currencies.

Monetary characteristics of early cryptocurrencies_

Loosely speaking, the modern fiat monetary system consists of physical and digital credits — issued by state central banks, state treasuries, and private commercial banks — which circulate under a legal system that guarantees their redemption. The number of credits expands through issuance, after which they can be transferred in the course of exchange among those who use them, before being retired when they are returned to the issuers. This composite system of expandable-contractable credits is what we refer to as 'money' in everyday parlance. In this context, the term *cryptocurrency* is controversial, because — from its inception — the name has simply *assumed* that the tokens are money tokens. The controversy is

amplified by the fact that enthusiasts sometimes use the term performatively to make the normative point that crypto tokens 'should be money', or — alternatively — to deny that what we currently call 'money' is in fact money. One strategy to negotiate these language politics is to initially strip the money assumption from the tokens by giving them the generic name *crypto-tokens*, and then listing their uncontroversial characteristics to compare them with fiat credits.

Tokens of early cryptocurrencies are *data objects* created through accounting, much like the act of typing out the number '1' creates the mental image of a 'thing'. This is what is referred to as a 'token', but they are 'blank tokens'. An example of a blank token in the physical world might be a clear plastic token with no inscription or rights attached to it. Bitcoin tokens, similarly, are *empty signifier*s, somewhat like the digital equivalent of blank physical tokens, but with strict supply limits.[2] These blank digital tokens however, are promoted with a name and branded logo that serves as a mental image for them, without which they would be almost entirely featureless. The tokens can be said to be *digital bearer instruments*, in the sense that transfers can only be initiated by the possessor of a private key that can unlock an 'unspent transaction output'. The 'bearer-instrument-like' nature is one reason why cryptocurrency sometimes gets referred to as 'digital cash' (physical cash being the bearer-instrument form of fiat currency). The tokens move around — Bitcoin and some of its descendants are processing hundreds of thousands of transfers of tokens every day (compare Hileman and Rauchs, 2017). Furthermore, they have a *price* measured in fiat currency and their tokens can be split into smaller pieces, or combined into larger ones. The fact that split-able and lump-able tokens with a fiat currency price can be moved gives the system a 'moneylike' feeling, and — under a shallow definition of money as *something that is issued and moved around in association with commerce* — the term *cryptocurrency* feels loosely plausible in everyday conversation.

Most 'purchases' conducted with bitcoin tokens, however, take the form of *countertrade*. The token, priced in fiat currency, is compared to a good or service, priced in fiat currency, and from this comparison of two fiat currency prices emerges an exchange ratio between the token and the good or service. This is the conceptual equivalent of superimposing a pair of two-way fiat currency transactions over each other and cancelling

out the money flows, giving the residual appearance of the crypto-token being used as 'money' to 'pay' for a good or service.

Nevertheless, Bitcoin is used primarily for speculation (Baur, 2018) — buying the token with fiat currency with an intention to resell it for fiat currency — rather than using it to countertrade ('pay') for goods and services. This speculation (compare, among others, Yermack, 2015; Glaser et al., 2014; or Cheah, 2015) drives volatility in the fiat currency price of tokens, which — when analysed through the lens of the conventional 'functions of money' paradigm favoured by economic textbooks (money as a medium-of-exchange, a store-of-value and a unit-of-account), poses problems for the 'moneyness' of the tokens. Not only are they not widely accepted in exchange for goods and services, but they are not widely used to price things, and attempts to provide prices are unintuitive[3] (Yermack, 2015). They also struggle to consistently 'store value', if we interpret that to mean 'maintain stable purchasing power' (which in the case of Bitcoin means 'maintain fiat price and countertrade ratios'). Put simply, while a person can generally predict how many bags of sugar US$ 100 will command in a month, they will be very uncertain as to how much sugar they can obtain through Bitcoin countertrade in a month.

Issues currently associated with the term_

Beyond these debates about the validity of the original use of the term *cryptocurrency*, the term has been destabilised by the proliferation of alterations to traditional cryptocurrency systems. The role of cryptography and 'moneyness' implied by the diverse token designs varies considerably and will be discussed in the remainder of the section.

The role of cryptography in today's cryptocurrencies_

A useful classification of projects from a technical standpoint involves rights for writing and reading transaction records. Peters et al. (2016) introduced a popular categorisation that can be used to classify the underlying infrastructure of cryptocurrency systems along the dimension "public" vs. "private" and "permissioned" vs. "permissionless". In public-permissionless systems every participant in the network (node) can read transactions and write others to the ledger. For public-permissioned systems, only authorised nodes can write. In private permissioned systems, finally,

even reading is restricted to authorised nodes. The more "private" and "permissioned" in its underlying infrastructure a system is, the further it is from the cypherpunk vision.

An example of a recent development trend holding true to the aim of replacing trust by cryptographic proof found in archetypal cryptocurrencies (compare Nakamoto, 2008; and Genkin et al., 2018) are so-called privacy-preserving cryptocurrencies or 'privacy coins' (e.g., Zcash, n.d.; Monero, n.d.). They are closely related to archetypal cryptocurrencies and replicate their public-permissionless setup of rights to read and write. As "alternative cryptocurrencies designed with the goal of providing stronger privacy guarantees than Bitcoin" (Genkin et al., 2018) they even *increase* the use of cryptography to ensure anonymity. As a consequence of their focus on privacy, however, they are leading to rising concerns with respect to anti-money-laundering and law enforcement (compare Tziakouris, 2020; or Ferrari, 2020).

The broad trajectory in recent years, however, has been to *decrease* the centrality of cryptography in the respective implementations. Even permissioned payment systems run by corporations but still called *cryptocurrencies* entered the stage.[4] Eyal (2017) concludes that "if attendees at recent blockchain events are any indication, cryptocurrencies have caught the attention of the mainstream financial technology (FinTech) sector" (Eyal, 2017, p. 39). With traditional business starting to experiment with the technology inspired by Bitcoin, system requirements — and with it the respective security setups and use of cryptography — changed. The economic design for these more centralised payment systems led to the reestablishment of trusted third parties or intermediaries for token creation to a certain degree.

While many novel *cryptocurrencies* are far from the crypto-anarchist roots of archetypal token designs, the general idea of the replacement of trust in institutions or their internal governance mechanisms by cryptography still plays a role in all *cryptocurrency* designs. However, given that even fiat bank payments use cryptography for *security*, mere reliance on cryptography for security should not enter a definition of cryptocurrencies.[5]

Monetary characteristics of today's cryptocurrencies_

Early cryptocurrencies had the declared intent of creating 'digital cash' or currency (see section 1.1.), but the proliferation of crypto token forms have destabilised how this is conceptualised. Not all development strands feature the objective of proposing general purpose monetary tokens.

First-layer tokens (e.g. Ether) that underlie smart contract platforms[6] (e.g. Ethereum), and informally even second-layer tokens (tokens running on respective platform) are called *cryptocurrencies*, but they exist first and foremost to activate smart contracts rather than aiming to provide a payment solution for goods and services more generally (see Bartoletti, 2017). Nevertheless, this more 'limited purpose' focus can be a strength, insofar as smart contract activation can be seen as a *real service* accessible via possession of the token, thereby 'anchoring' the tokens into a 'real economy', albeit one in cyberspace.

However, also 'general purpose' tokens are marked by changes. A response to the inherent instability in prices of archetypal cryptocurrency was the advent of 'stablecoins', which try to solve the issue of high volatility in purchasing power of Bitcoin and its descendants (Pernice, 2019). Stablecoins are tethered or pegged to fiat currencies, or 'backed' in some way with assets that have fiat currency prices. They are thus no longer 'blank' empty signifiers, and contain some reference point that is easier to estimate and communicate. There are very different types of stablecoins, and recently several frameworks have tried to unify and abstract existing stabilisation techniques (e.g., Bullmann et al., 2019; Pernice et al., 2019; Moin et al., 2020; Sidorenko, 2019; Clark et al., 2020). A national currency can be 'tokenized' by issuing a digital promise for it on a blockchain system, and such tokenised funds might indeed be categorised as a "new form of electronic money" (Blandin et al., 2019) falling under the respective regulations for e-money, anti money laundering and counter terrorist financing regulations. This might ensure "moneyness" at least from a legal standpoint. With more complex stablecoin designs the legal case is not always clear, but from an economic standpoint their stability in purchasing power might contribute to an increase in their adoption as money in the future. Stablecoins, for now however, haven't seen mainstream adoption in retail markets yet (Bullmann et al., 2019).

Conclusion_

Many scientific publications simply assume the meaning of the term *cryptocurrency* to be common knowledge or, at most, sketch it roughly.[7] Instead, we followed the evolution of the term starting with Bitcoin to define what *cryptocurrency* is understood as today. The neologism *cryptocurrency* is unstable in its meaning, and is applied to systems with diverse technical architectures and governance systems. Nevertheless, one way to unify the diverse uses of the term is to define it by some common intent among those who claim it, rather than by the diverse means via which that intent is enacted, and regardless of whether the intent is achieved in practice. We find that cryptocurrency systems are unified by being intended to host a *general or limited-purpose medium-of-exchange*, a cryptocurrency, using infrastructure that replaces trust in institutions by cryptography to varying degrees.

To make the term more useful in public discourse, *cryptocurrency* should be coupled with specifying classifications from economic (e.g., Bullmann et al., 2019; Pernice et al., 2019; Moin et al., 2020; Clark et al., 2020), governance (e.g., Ziolkowski et al., 2020; Beck et al., 2018; Hacker, 2019) or technological (e.g., Cachin and Vukoli, 2017; Peters et al., 2016) points of view.

References_

- Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. *ArXiv*. https://arxiv.org/abs/1710.10377
- Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *Computer Science & Information Technology*, *7*(10),1-6. https://doi.org/10.5121/csit.2017.71011
- Bartoletti, M., & Pompianu, L. (2017). An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, & M. Jakobsson (Eds.), *Financial Cryptography and Data Security* (pp. 494–509). Springer International Publishing. https://doi.org/10.1007/978-3-319-70278-0_31
- Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets,*

Institutions and Money, *54*, 177–189. https://doi.org/10.1016/j.intfin.2017.12.004

- Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10). https://aisel.aisnet.org/jais/vol19/iss10/1
- Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., & Cloud, K. (2019). *Global cryptoasset regulatory landscape study* [Report]. Cambridge Centre for Alternative Finance, University of Cambridge. https://econpapers.repec.org/RePEc:jbs:altfin:-201904-gcrls
- Bullmann, D., Klemm, J., & Pinna, A. (2019). *In search for stability in crypto-assets: Are stablecoins the solution?* (Paper No. 230; Occasional Paper Series). European Central Bank. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf
- Cachin, C., & Vukolić, M. (2017). Blockchain Consensus Protocols in the Wild (Keynote Talk). In *31st International Symposium on Distributed Computing (DISC 2017)* (pp. 1:1–1:16). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. https://doi.org/10.4230/LIPIcs.DISC.2017.1
- Chaum, D., Fiat, A., & Naor, M. (1988). Untraceable Electronic Cash. In S. Goldwasser (Ed.), *Advances in Cryptology — CRYPTO' 88* (pp. 319–327). Springer. https://doi.org/10.1007/0-387-34799-2_25
- Cheah, E. T., & Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, *130*, 32–36. https://doi.org/10.1016/j.econlet.2015.02.029
- Chu, J., Chan, S., Nadarajah, S., & Osterrieder, J. (2017). GARCH modelling of cryptocurrencies. *Journal of Risk and Financial Management*, *10*(4), 17. https://doi.org/10.3390/jrfm10040017
- Clark, J., Demirag, D., & Moosavi, S. (2020). Demystifying Stablecoins: Cryptography meets monetary policy. *Queue*, *18*(1), 39–60. https://doi.org/10.1145/3387945.3388781
- Davis, J. (2011, October 3). The crypto-currency. *The New Yorker*, *87*. https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Cambridge, Massachusetts: Harvard University Press. https://doi.org/10.2307/j.ctv2867sp

- *Diem*. (n.d.). Retrieved 19 May 2023, from https://www.diem.com/en-us/
- Eyal, I. (2017). Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer*, *50*(9), 38-49.https://doi.org/10.1109/MC.2017.3571042
- Ferrari, V. (2020). The regulation of crypto-assets in the EU – investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law*, *27*(3), 325–342. https://doi.org/10.1177/1023263X20911538
- Genkin, D., Papadopoulos, D., & Papamanthou, C. (2018). Privacy in Decentralized Cryptocurrencies. *Communications of the ACM*, *61*(6), 78–88. https://doi.org/10.1145/3132696
- Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014, June 7). Bitcoin-asset or currency? Revealing users' hidden intentions. *ECIS 2014 Proceedings*. European Conference on Information Systems. https://aisel.aisnet.org/ecis2014/proceedings/track10/15
- Hacker, P. (2019). Corporate Governance for Complex Cryptocurrencies?: A Framework for Stability and Decision Making in Blockchain-Based Organizations. In P. Hacker, *Regulating Blockchain* (pp. 140–166). Oxford University Press. https://doi.org/10.1093/oso/9780198842187.003.0008
- Härdle, W. K., Harvey, C. R., & Reule, R. C. G. (2020). Understanding Cryptocurrencies. *Journal of Financial Econometrics*, *18*(2), 181–208. https://doi.org/10.1093/jjfinec/nbz033
- Hileman, G., & Rauchs, M. (2017). *Global cryptocurrency benchmarking study* [Report]. Cambridge Centre for Alternative Finance, University of Cambridge. https://ideas.repec.org/b/jbs/altfin/201704-gcbs.html
- HXN [в^{3}ан]. (2009, September 24). This is really interesting: Bitcoin, the p2p cryptocurrency. Http://bitcoin.sourceforge.net/ [Tweet]. *@hxn*. https://twitter.com/hxn/status/4334116324
- Lansky, J. (2018). Possible state approaches to cryptocurrencies. *Journal of Systems Integration*, *9*(1), 19–31. https://doi.org/10.20470/jsi.v9i1.335
- Ludlow, P. (Ed.). (2001). *Crypto anarchy, cyberstates, and pirate utopias*. Cambridge, Massachusetts: MIT Press. https://doi.org/10.7551/mitpress/2229.001.0001
- Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract

applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, *35*(8), 2337-2354. https://doi.org/10.1016/j.tele.2018.10.004

- Moin, A., Sekniqi, K., & Sirer, E. G. (2020). SoK: A Classification Framework for Stablecoin Designs. In J. Bonneau & N. Heninger (Eds.), *Financial Cryptography and Data Security* (pp. 174–197). Springer International Publishing. https://doi.org/10.1007/978-3-030-51280-4_11
- Monero. (n.d.). *Monero Research Lab*. Monero. https://web.getmonero.org/resources/research-lab/
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- Nakamoto, S. (2009, February 11). *Bitcoin open source implementation of P2P currency* [Forum post]. P2P Foundation Post. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source
- Peters, G. W., & Panayi, E. (2016). Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century* (pp. 239–278). Springer International Publishing. https://doi.org/10.1007/978-3-319-42448-4_13
- Pernice, I. G., Henningsen, S., Proskalovich, R., Florian, M., Elendner, H., & Scheuermann, B. (2019, June). Monetary stabilization in cryptocurrencies–design approaches and open questions. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 47-59). IEEE. https://doi.org/10.1109/CVCBT.2019.00011
- Popper, N., & Isaac, M. (2020, April 16). Facebook-Backed Libra Cryptocurrency Project Is Scaled Back. *The New York Times*. https://www.nytimes.com/2020/04/16/technology/facebook-libra-cryptocurrency.html
- Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718
- Sidorenko, E. L. (2019). Stablecoin as a New Financial Instrument. In S. I. Ashmarina, M. Vochozka, & V. V. Mantulenko (Eds.), *Digital Age: Chances, Challenges and Future* (pp. 630–638). Springer International Publishing. https://doi.org/10.1007/978-3-030-27015-5_75

- Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero. *Journal of Economics and Financial Analysis*, *2*(2), 1–27. https://mpra.ub.uni-muenchen.de/85036/
- Tziakouris, G. (2018). Cryptocurrencies — A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective. *IEEE Security & Privacy*, *16*(4), 92–94. https://doi.org/10.1109/msp.2018.3111243
- White, L. H. (2015). The Market for Cryptocurrencies. *Cato Journal*, *35*(2), 383–402. https://ideas.repec.org/a/cto/journl/v35y2015i2p383-402.html
- Yermack, D. (2015). Is Bitcoin a Real Currency? An Economic Appraisal. In D. Lee Kuo Chen (Ed.), *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (pp. 31–43). Academic Press. http://doi.org/10.1016/b978-0-12-802117-0.00002-3
- Zcash. (n.d.). *How it works*. Zcash. https://z.cash/technology/
- Ziolkowski, R., Miscione, G., & Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems*, *37*(2), 316-348.
- https://doi.org/10.1080/07421222.2020.1759974

Endnotes_

1. An online search on Google Trends and Google Ngrams indicated that the term *cryptocurrency* was not used before the inception of Bitcoin.
2. Note that the notion of a "blank token" refers here to economic intuition rather than technical implementation. In Bitcoin and its descendents no "coins" exist, but only transaction outputs that are transferable and arbitrarily divisible.
3. Usual consumer goods priced in Bitcoin, for example, are represented by tiny decimal numbers.
4. Compare e.g. Diem (n.d.) and their reception in the press e.g. New York Times (Popper & Isaac, 2020).
5. We would have liked to rely on the unifying element of blockchain-based technology (which supposedly amalgamates all the cryptographic tools of a cryptocurrency) here. However, noting that this term is similarly unclear and vague as the term to define, we abstained from that step.

6. A summary of the research around smart contract platforms is given in Macrinici et al. (2018) while Bartoletti et al. (2017) and Alharby et al. (2017) review different platforms. While generally similar to cryptocurrency systems, their tokens are part of the security setup and used as medium-of-exchange between smart contracts.
7. The meaning of *cryptocurrency* is outlined briefly in White (2014), Lansky (2018), Aggarwal (2018), Chu et al. (2017), Sovbetov (2018) and Härdle et al. (2020).

CRYPTOECONOMICS_

Jaya Klara Brekke, Department of Geography,
Durham University, United Kingdom.
Wassim Zuhair Alsindi, Media Lab,
Massachusetts Institute of Technology,
United States.

Cryptoeconomics describes an interdisciplinary, emergent and experimental field that draws on ideas and concepts from economics, game theory and related disciplines in the design of peer-to-peer cryptographic systems. Cryptoeconomic systems try to guarantee certain kinds of information security properties using incentives and/or penalties to regulate the distribution of efforts, goods and services in new digital economies. Cryptoeconomics is an embryonic field at present and can be taken to include several areas of focus: information security engineering, mechanism design, token engineering and market design. This portmanteau of cryptography and economics raises questions regarding the epistemic novelty of cryptoeconomics, as distinct from its constituent components.

Definition_

Cryptoeconomics describes an interdisciplinary, emergent and experimental field that draws on ideas and concepts from economics, game theory and related disciplines in the design of peer-to-peer cryptographic systems. Cryptoeconomic systems try to guarantee certain kinds of information security properties using incentives and/or penalties to regulate the distribution of efforts, goods and services in new digital economies.

Cryptoeconomics is an embryonic field at present and can be taken to include several areas of focus: information security engineering, mechanism design, token engineering and market design. This portmanteau of cryptography and economics raises questions regarding the epistemic novelty of cryptoeconomics, as distinct from its constituent components.

Origin_

The term *cryptoeconomics* entered casual usage in the formative years of the Ethereum developer community in 2014-5. The phrase is typically attributed to Vitalik Buterin with the earliest public usage being in a

2015 talk by Vlad Zamfir entitled "What is Cryptoeconomics" (Zamfir, 2015). For Buterin, the aim of cryptoeconomics is "as a methodology for building systems that try to guarantee certain kinds of information security properties" (Buterin, 2017, pp. 46-56). While for Zamfir, the focus is more broadly on the distribution of efforts, goods and services in new digital economies: "A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols" (Zamfir, 2015, 00:00:58). The term is uncommon amongst Bitcoin developers, but is occasionally used to discuss adversarial scenarios such as state-sponsored defensive mining and transaction censorship (Voskuill, 2018).

Cryptoeconomics was coined by the Ethereum community but was initially inspired by the use of economic incentives in the Bitcoin protocol (Nakamoto, 2008). Bitcoin mining is designed with the intention that it would be more profitable and attractive to contribute to the network than to attack it. With the development of Ethereum as the first successful general-purpose blockchain protocol, the idea of using economic incentives was also generalised as an approach to achieve a broad variety of behavioural and information security outcomes for decentralised systems. This has led to experimentation with the use of cryptographic techniques and incentives in organisational, financial, market and monetary experiments (Davidson et al., 2016; Halaburda et al., 2018; Voshmgir, 2019).

Motivation for the development of cryptoeconomics arises from the need to solve specific information security, organisational and economic problems that manifest in cryptographic systems. Examples include incentive alignment between stakeholder participants in permissionless networks and developing viable alternative approaches to distributed consensus other than proof-of-work, which is also commonly referred to as blockchain mining. In this sense, the portmanteau cryptoeconomics (or crypto-economics) as a combination of cryptography and economics raises an interesting question regarding epistemic reducibility. Can cryptoeconomics be fully deconvoluted — in other words, retro-synthesised — into its constituent namesakes; is it a mere combination or greater than the sum of its parts? A particular respondent's answer might fall along the lines of their proclivity towards general-purpose blockchain networks and / or proof-of-work.

The aforementioned affinity to *decentralisation* as an axiomatic aim and primary concept originates from a longer history of the development of peer-to-peer systems as a means to establish autonomous networks (Brekke, 2020). With the invention of Bitcoin, economic ideas were added to the toolbox of computer engineers developing leaderless systems. For some, the motivation was to enable economic autonomy and fair distribution of efforts and rewards within such decentralised networks, what scholar of money and the internet Swartz calls *infrastructural mutualism*. For others, the promise of provably scarce and unforgeable virtual commodities — *digital metallism* — was the main attraction (Swartz, 2018). Adherents to the digital metallist ideology often draw upon economic and monetary concepts typically associated with libertarianism and the US far right (Golumbia, 2016).

Evolution_

Over time there has been a broadening in the scope of what can be considered *cryptoeconomics* as the variety of consensus systems and token types has proliferated. The different approaches to cryptoeconomics are beginning to settle into distinct layers of a cryptoeconomic 'stack': 'layer 1' referring to the information security of a network protocol such as proof-of-work and proof-of-stake; and 'layer 2' referring to the token, market or mechanism capacities offered by emerging cryptoeconomic platforms (Alsindi, 2019).

In recent years a number of networks affording general-purpose computation with facile smart contracting and token creation capabilities have emerged. This layer 2 cryptoeconomics entails the creation of notionally valuable economic assets without being connected to the underlying security properties of the network substrate; for example ERC20-type Ethereum tokens, Non-Fungible Tokens (NFTs) and more recently Decentralised Finance (DeFi) synthetic tokens. Whilst having notional economic value, these assets provide negligible security benefits to the base layer of the network: the abstracted non-native assets of 'layer 2' may increase the incentive to attack 'layer 1', as has been discussed in relation to ledger forks (Alsindi, 2019), Initial Coin Offering launches and sudden market-moving events are seen regularly in the hyper financialised DeFi sector (Daian et al., 2019). The scope and definition of cryptoeconomics is still undergoing *epistemic formation* (0x Salon & Alsindi, 2020) and thus entails specific areas of focus:

Information security engineering: Where the primary focus of the cryptoeconomic endeavour is on the security properties for peer-to-peer 'layer 1' protocols.

Mechanism design: Where the focus is specifically on the use of incentives for behavioural engineering of *rational agents* in a game theoretical setting (Brown-Cohen et al., 2018).

Token engineering: Where the primary focus is on the functionality and properties exhibited by tokens used in a system. Tokens might for example grant token holders specific rights (such as service access or voting privileges as commonly encountered with the ERC-20 pseudo-standard), be *fungible* or *non-fungible* such as NFTs, be generated and distributed through mining, or through *airdrops*. Different token designs are understood to encourage different types of behaviours and organisational properties (Voshmgir, 2019).

Market design: Where the focus is on employing blockchain protocols and tokens in order to experiment with new kinds of markets that generate specific types of outcomes. For example, *bonding curves* determine the price of tokens depending on the supply or other factors, with an aim to influence the behaviour of investors (Titcomb, 2019).

Issues currently associated with the term_

Cryptoeconomics is generally understood to combine cryptographic techniques and economics. However, much of the field of cryptoeconomics *"shows an interesting but also alarming characteristic: its underlying economics is remarkably conventional and conservative"* (Virtanen et al., 2018). Out of the long-standing and broad fields of economics and associated fields of political economy, monetary theory, finance and social study of finance, most literature on cryptoeconomics takes an overly formalist approach to the contested field of game theory (Green & Viljoen, 2020). Virtanen et al. (2018, n.p.) quote a revealing tweet from the influential Nick Szabo: *"An economist or programmer who hasn't studied much computer science, including cryptography, but guesses about it, cannot design or build a long-term successful cryptocurrency. A computer scientist and programmer who hasn't studied much economics, but applies common sense, can."* This means that the potential of cryptoeconomic approaches may be more reformist than revolutionary;

"in spite of their noble intentions, these projects do not in fact break with the current financial paradigm" (Lotti, 2016, p. 105).

More recent characterisations of cryptoeconomics take a broader societal outlook, for example focusing on the economics of new organisational forms (Davidson et al., 2016), the design of *economic space* (Virtanen et al., 2018), or on economic and monetary design that draws on mutual credit systems (Brock et al., 2018) and *commons* approaches (De Filippi & Hassan, 2015; Catlow, 2019). There is, in other words, much broader economic experimentation taking place with and through peer-to-peer cryptographic systems, however, those explicitly labelled *cryptoeconomic* often imply narrow and formalist approaches limited to Austrian school economics, right wing monetary ideas and game theory, especially apparent in the usage of the term in reference to Bitcoin (Golumbia, 2016; Voskuill, 2018).

One of the ongoing challenges encountered in cryptoeconomics is inherent to *mechanism design* and *market design* economics more generally (Ossandón, 2019). Namely the contradiction between the promise of deterministic outcomes in theory and the complex, emergent behaviours and effects of the systems in real deployments. On the one hand, the market design approach in cryptoeconomics promises to deliver specific properties (information security or behavioural outcomes). But on the other hand, the simple rules of the systems designs produce complexity and unintended outcomes (Voshmgir & Zargham, 2019). A contradiction off-handedly commented on by Ethereum developer Floersch when discussing the Casper proof-of-stake approach: *"[W]e have this complex behavior emerging from really simple economic rules, and this actually not specific to Casper by any means, this is any protocol that are messing around with economics"* (Floersch, 2017, pp. 12-18).

This contradiction — of emergent complexity and unintended effects — is nevertheless "productive" for those seeking to promote economic approaches to social problems: the promise of deterministic outcomes makes the models convincing and attractive from a formalist perspective (Green & Viljoen, 2020), while the complexity obscures any "failures" of the design (Nik-Khah & Mirowski, 2019). These shortcomings are instead relegated to being a problem "of the social" or "with humans" or that the implementation was not sufficiently faithful to the protocol, or even that the protocol implementation was not being expansive or

radical enough. This contradiction is extensively covered in political economic and economic history and comprises one of the main critiques of the Austrian school of economics in particular (Mirowski & Nik-Khah, 2018; Heilbroner, 1998), what is also called the *performative* aspects of economics. From an information security perspective, the incorporation of economic incentives into protocol design in this sense radically increases the complexity of peer-to-peer systems, and correspondingly also leads to an increased attack surface and wider variety of hypothetical vulnerabilities (Alsindi, 2019).

Conclusion_

In summary, cryptoeconomics refers to an emerging field that employs economic concepts in the design of peer-to-peer cryptographic systems. The origins of the field lie in specific information security problems arising out of such systems. Competing approaches draw from a much wider field of economic and political economic thinking, including mutual credit systems and commons frameworks, in order to address questions of organisation and societal outcomes more broadly.

References_

- 0x Salon, & Alsindi, W. Z. (2020). *0x002 Report: Trespasser Theory: Aside on Cryptoeconomic Systems — A case study in attempted epistemic formation?* [Report]. 0x Salon. https://doi.org/10.21428/49968aaa.9160a130#aside-on-cryptoeconomic-systems---a-case-study-in-attempted-epistemic-formation
- Alsindi, W. Z. (2019). *TokenSpace: A Conceptual Framework for Cryptographic Asset Taxonomies*. Parallel Industries. https://doi.org/10.21428/0004054f.ccff3c19
- Brekke, J. K. (2020). Hacker-engineers and Their Economies: The Political Economy of Decentralised Networks and 'Cryptoeconomics'. *New Political Economy*. https://doi.org/10.1080/13563467.2020.1806223
- Brock, A., Atkinson, D., Friedman, E., Harris-Braun, E., Mcguire, E., Russell, J. M., Perrin, N., Luck, N., & Harris-Braun, W. (2017). *Holo Green Paper* [White Paper]. Holo. https://files.holo.host/2017/12/Holo-Green-Paper.pdf
- Brown-Cohen, J., Narayanan, A., Psomas, C., & Weinberg, S. M.

(2018). Formal Barriers to Longest-Chain Proof-of-Stake Protocols. *ArXiv*. https://arxiv.org/abs/1809.06528
- Buterin, V. (2017). *Introduction to Cryptoeconomics, Ethereum Foundation* [Talk]. https://youtu.be/pKqdjaH1dRo
- Catlow, R. (2019). Decentralisation and Commoning the Arts. *Free/ Libre, Technologies, Arts and the Commons. Unconference Proceedings*, 50–55. http://www.unrf.ac.cy/files/unconference-proceedings-phygital.pdf#page=50
- Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *ArXiv*. https://arxiv.org/abs/1904.05234
- Davidson, S., De Filippi, P., & Potts, J. (2016). *Economics of Blockchain*. https://doi.org/10.2139/ssrn.2744751
- De Filippi, P., & Hassan, P. (2015). Measuring Value in the Commons-Based Ecosystem: Bridging the Gap Between the Commons and the Market. In G. Lovink, N. Tkacz, & P. De Vries (Eds.), *MoneyLab Reader: An Intervention in Digital Economy* (pp. 74–91). Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2015/04/MoneyLab_reader.pdf#page=76
- Floersch, K. (2017). *Casper Proof of Stake* [Talk]. Cryptoeconomics and Security Conference, Berkeley. https://youtu.be/ycF0WFHY5kc.
- Golumbia, D. (2016). *The politics of Bitcoin. Software as right-wing extremism.* University of Minnesota Press.
- Green, B., & Viljoen, S. (2020). Algorithmic Realism: Expanding the Boundaries of Algorithmic Thought. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT '20)*, 19–31. https://doi.org/10.1145/3351095.3372840
- Halaburda, H., Haeringer, G., Gans, J., & Gandal, N. (2018). *The Microeconomics of Cryptocurrencies* (Research Paper No. 2018-10–02). NYU Stern School of Business, Baruch College Zicklin School of Business. https://doi.org/10.2139/ssrn.3274331
- Heilbroner, R. (1998). The self-deception of economics. *Critical Review*, *12*(1–2), 139–150. https://doi.org/10.1080/08913819808443490
- Lotti, L. (2016). Contemporary art, capitalization and the blockchain: On the autonomy and automation of art's value. *Finance and Society*, *2*(2), 96. https://doi.org/10.2218/finsoc.v2i2.1724
- Mirowski, P., & Nik-Khah, E. (2018). *The Knowledge We Have Lost*

In Information – The History Of Information in Modern Economics. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190270056.001.0001

- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- Nik-Khah, E., & Mirowski, P. (2019). On Going the Market One Better: Economic Market Design and the Contradictions of Building Markets for Public Purposes. *Economy and Society*, *48*(2), 268–294. https://doi.org/10.1080/03085147.2019.1576431
- Ossandón, J. (2019). Notes on Market Design and Economic Sociology. *Economic Sociology*, *20*(2), 31–39. http://hdl.handle.net/10419/200967
- Swartz, L. (2018). What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies*, *32*(4), 623–650. https://doi.org/10.1080/09502386.2017.1416420
- Titcomb, A. (2019). Deep Dive: Augmented Bonding Curves [Blog post]. *Giveth Medium*. https://medium.com/giveth/deep-dive-augmented-bonding-curves-3f1f7c1fa751
- Virtanen, A., Lee, B., Wosnitzer, R., & Bryan, D. (2018). Economics Back into Cryptoeconomics [Blog post]. *Econaut Medium*. https://medium.com/econaut/economics-back-into-cryptoeconomics-20471f5ceeea
- Voshmgir, S. (2019). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. BlockchainHub Berlin.
- Voshmgir, S., & Zargham, M. (2019). *Foundations of Cryptoeconomic Systems* [Working Paper]. Institute for Cryptoeconomics, Vienna University of Economics and Business. https://epub.wu.ac.at/7309/
- Voskuill, E. (2018). *Cryptoeconomics* [Wiki Page]. The Bitcoin Development Library. https://github.com/libbitcoin/libbitcoin-system/wiki/Cryptoeconomics
- Zamfir, V. (2015). *What Is Cryptoeconomics?* Cryptocurrency Research Group Cryptoeconomicon. https://youtu.be/9lw3s7iGUXQ?t=58

CYPHERPUNK_

André Ramiro, Law and Technology Research Institute of Recife (IP.rec), Brazil.
Ruy de Queiroz, Federal University of Pernambuco, Recife, Brazil.

Cypherpunk refers to social movements, individuals, institutions, technologies, and political actions that, with a decentralised approach, defend, support, offer, code, or rely on strong encryption systems in order to re-shape social, political, or economic asymmetries. Based on a literature review that encompassed the last thirty years, bringing together iconic manifestos, seminal works on Internet social movements, as well as contemporary academic research developments, the entry offers a sedimentation of the significance of cypherpunk phenomena. It argues that "cypherpunk" constitutes a socio technical expression of the promotion of rights through cryptography, meaning that it can be considered to have a broader area of incidence. Therefore, going further in order to give elasticity to the term, the entry covers not only the diversity of political rationale behind the development, promotion and reliance on encryption, but also to classify the variety of expressions of cypherpunk beyond individuals and collectives, but also organisations and technologies that constitute contemporary networks of political participation.

Origins_

In the 1980s, the computer industry was becoming the provider of the main apparatus central to private interconnected management systems and by extension to the United States government's administration. Beyond the optimisation of private and public services, sociopolitical concerns regarding privacy and data protection were already being addressed and gaining space among scholars and activists questioning the necessity of compulsory identification, unnecessary data collection and the formation of data centres, archives and dossiers about individuals (Lyon, 1994; Zuboff, 1988; Burhnham, 1983). The *chilling effect,* which reduces the expression potential of individuals, was potentially growing among civil society (Lyon, 1992).

In parallel, despite the broadening of computer industry and its necessity to provide secure hardware and software that would equip the

private sector, the restrictive administrative rules towards domestic use and exportation of encryption (initially listed as a war munition) was imposing an obsolete regulation because the continuing technological development required state-of-the-art security (Diffie & Landau, 2001). This distrust of data collection plus the anachronistic regulation resulted in the advocacy of encrypted technologies becoming to symbolise, at once, a market necessity and a resistance against growing surveillance ecosystems.

The latter was a central concern of a 1985's article, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, by computer scientist and cryptographer David Chaum. He dreamed of a transaction model in which, through a strong and reliable encryption system, privacy would be preserved. The premise was that:

"[c]omputerization is robbing individuals of the ability to monitor and control the ways information about them is used. (...) The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions" (Chaum, 1985).

Therefore, for Chaum and for the subsequent cypherpunk movement, the conclusion is that it would be necessary to implement decentralised public-key encryption systems (Diffie & Hellman, 1976; Rivest, Shamir & Adleman, 1978), in order to disrupt this fast-marching problem.

In 1988, influenced by Chaum's ideas and pushing the ideology forward, electronic engineer Timothy May, a then former Intel employee, distributed flyers of a first draft of what would become the *Crypto Anarchist Manifesto.* The manifesto was officially published in 1992 (May, 1992). In that same year, May and Eric Hughes gathered a group of cryptographers, mathematicians, engineers, and hackers for meetings to discuss how encryption communication systems could overcome state surveillance. According to Levy (2001), Jude Milhon, influenced by authors such as Neal Stephenson and William Gibson — known for cyberpunk novels with technological immersive scenarios, and rebellious characters — baptised them "cypherpunks" (a word-play with *cipher*, the central code of an encryption system). The group then adopted the label.

Although Tim May could be considered the most prolific cypherpunk ideologist near the origin of the movement, and close to anarchist beliefs, it is crucial to place him among a varying spectrum of political views within the movement's first founders. Eric Hughes (1993) has published the iconic *A Cypherpunk's Manifesto,* stating that "cypherpunks write code (...) deplore regulations on cryptography" and "are actively engaged in making the networks safer for privacy". The publication was a landmark for also establishing the concept of "cypherpunk" at the time, and it explored the value of privacy within personal data dynamics (for example, anonymization protocols) in expanded connected ecosystems. Then it highlighted the centrality of encryption for the society to achieve a reliable "social contract". John Gilmore (1991), in a paper called "Privacy, Technology, and the Open Society" introduced at the First Conference on Computers, Freedom, and Privacy that year, predicted much of what would be explored by Eric Hughes two years later by combining emerging Internet rights, with a focus on data protection, to the full deployment of strong encryption:

"What if we could build a society where the information was never collected? (...) That's the kind of society I want to build. I want a guarantee — with physics and mathematics, not with laws — that we can give ourselves things like real privacy of personal communications. Encryption strong enough that even the NSA can't break it" (Gilmore, 1991).

After its inception the term was further crystallised by the creation of the "*Cypherpunk Mailing List",* a forum-like discussion space with nearly a thousand people in the 1990s (Manne, 2011; Greenberg, 2012). The mailing list encompassed a range of people that went from anarcho-capitalists to socialists, leftists to rightists, political scientists and lawyers to developers and cryptographers (Rid, 2016), making it nearly impossible to classify the cypherpunks in one single class, under one stakeholder, or political box. Still, the mailing list gained traction and there was a shared understanding and strategy discussions in opposition to regulatory limitations of domestic use and exportation of encryption products, as well as against major national surveillance programs that would undermine communications secrecy in that decade.

Evolution of the term from a chronological perspective_

From a chronological perspective, the wide selection of definitions on the *cypherpunk* spectrum can draw a rich mosaic of interpretations since its baptism back in 1992.

Taking from the first two manifestos mentioned before, Levy (1993; 1994; 2001) offers a continuous documentation of the cypherpunk's first decade. As a description, the author states that they were "cryptographers with an attitude", "a loose confederation of computer hackers, hardware engineers and high-tech rabble-rousers" that "assumed that cryptography is a liberating tool, empowering individuals to protect communications from the Government". Levy's approach offers special attention to their involvement in the 1990's Crypto Wars and their advocacy towards the weakening of government regulations for civilian use of encryption.

In 2006, the term *Cypherpunk* was added to the Oxford English Dictionary as "a person who uses encryption when accessing a computer network in order to ensure privacy, especially from government authorities" (Lexico, 2021). Colin Bennett (2008), in his well known ethnography about narratives and agendas of privacy advocates around the world, credits the cypherpunks as the principal example of the assemblage between *privacy-enhancing technologies* and the notion of anonymous communications to avoid law enforcement interests. The available definitions gained new dimensions with the advent of WikiLeaks (further discussed below), with Greenberg (2012) and Assange (2012) expanding its social and historical meaning to cover a whistleblowing movement that values secure communication spaces — thus encrypted — in order to report on government and private corporation's abuses.

The notion that cryptography rearranges power is directly shared by the cryptographer Phillip Rogaway, an explorer of the political dimensions of encryption and author of a seminal essay entitled "The Moral Character of Cryptographic Work" (2015). After giving an overview about the connections between technoscientific production and social values, for too long denied by scientists (including cryptographers), Rogaway states that cypherpunks have "long worked the nexus of cryptography and politics" To him, not cryptographers, but cypherpunks are normally the strongest advocates of cryptography: they are "cryptographers with values".

In addition, in a book dedicated to tell the story of cybernetics' main ideas, from Norbert Wiener's first theories of automated control systems to contemporary political techno-dilemmas, Rid (2016) also gives great attention to libertarian movements within, with focus on the cypherpunks. The author relates the movement to the "unshakable cybernetic faith in the machine", that "combined Wiener's hubristic vision of the rise of the machines with [Stewart] Brand's unflinching belief that computers and networked communities would make the world a better place", although adding a crucial key element: cryptography, which would provide the necessary personal empowerment.

Regarding the narratives mobilised by cypherpunks, Hellegren (2016; 2017) introduces the notion of "*crypto-discourses*" to analyse how a rationale was articulated to define "Internet freedom", by having the state as the antagonist actor. The author recalls the concept of *crypto-freedom* from Coleman and Golub (2008), "to refer to a partially fixed construction of meaning that establishes a relationship between encryption and a negative conception of freedom". In other words, "freedom" (or the use of encryption for that matter), to cypherpunks, would necessarily encompass acts to oppose the state's power. It didn't include a public call for an eventual obligation of the state to ensure encryption-derived rights such as privacy or freedom of expression.

Finally, Jarvis (2021) more recently echos that the concept of freedom is "not entirely fixed", arguing that, for example, although Tim May's initial insights were somewhat influential, his conception of freedom did not comprehend the whole variety of political tendencies within the cypherpunk community, as stated before. They were a highly educated, mostly libertarian community, permeated by *some* aspects of anarchism derived from societal disaffiliation inherited from counterculture circles, influencing generations of digital privacy activists responsible for challenging today's surveillance programs.

The idea of cypherpunk goes beyond individuals_

The creation of the mailing list played a central role, and it anticipated the threats to encryption to come. The two main policies were the *Clipper Chip* and "key escrow" proposals by the United States federal government, according to which backdoors would be implemented in

encrypted communication systems and a decryption key copy should be escrowed to the government (Kehl; Wilson; Bankston, 2015). The time around these proposals is broadly known as the first *Crypto Wars,* and the proposals have frequently resurfaced in one form or another.

Resisting those policies took a cypherpunk approach by existing as a technosocial *quasi*-organized movement[1] and as an emailing network. But from an institutional perspective, it is possible to credit entities such as the then recently created Electronic Frontier Foundation — co-founded by one of the central figures to the cypherpunk early articulations, John Gilmore — as a cypherpunk organisation, a structured institutional front, with legal powers, to engage in court battles and public advocacy for encryption freedom.

If the cypherpunks' defence of encryption — as a tool to enforce effective secrecy for civil communication and privacy regarding individual's data in transactions — was so far seen as an essential resource to keep away government and private corporations' eyes and ears, an additional layer to its meaning could be perceived within the WikiLeaks movement. The ideology represented by Julian Assange (Assange *et al*. 2012), reaffirms not only the use of strong encryption to protect private communications between two parties, but strengthens the notion of using encrypted communication channels to report on abuse, release secret government information with potential public interest and scandals connected to private corporations. It brings the notion of the protection from identification and the message's content security to whistleblowers. In the words of their model, "privacy for the weak, transparency for the powerful." As a result, WikiLeaks can be considered a *cypherpunk organisation* (Anderson, 2020), adding the element of securely reporting government and corporate abuse to the cypherpunk spectrum.

Further, the symbolization of the cypherpunk spectrum is not identified only in individuals, groups, and constituted organisations, but the phenomenon's technical dimension is materialised in the basic element of digital technologies: code. The cypherpunks' defence of encryption was not only a theoretical or law-based activism for human rights, but was coded into software at the very beginning of its activity. In 1991, when *Pretty Good Privacy* (PGP) was published as a strong encryption resource to private communications, it was a fundamental inspiration to

the cypherpunk movement. According to its creator, Philip Zimmermann (1999), it was a 1991's surveillance draft bill focusing on backdoors to private communications that made him publish PGP for free in order to popularise the use of strong encryption, so that it would be impossible to revert the situation, for example, by unpublishing the software (Levy, 2001; Greenberg, 2012). It was a strategic intervention in the technological culture, provoking social change. Therefore, PGP can also be qualified as a *cypherpunk technology*. The same interpretation reaches other decentralised technological expressions, such as Bitcoin, conceived in 2008 — see Pernice and Scott (2021), bridging early cypherpunk elaborations to current cryptocurrency models — and the The Onion Router (TOR), launched in 2002, and currently maintained by The Tor Project.

It's also worth noting the greater geographical decentralisation of the cypherpunk movement brought by WikiLeaks. If most of the cypherpunk movement in the nineties took place in the United States, there has been a diffusion of whistleblowing movements around the world, coinciding with the advancement and the popularisation of encrypted communication channels. That is reflected in the central role of Julian Assange and figures like Jérémie Zimmerman (Quadrature du Net, from France) and Andy Müller-Maguhn (Chaos Computer Club, from Germany) for the cypherpunk movement. Manne (2011) notes that, for Assange, laws regarding Internet control tended to be harmonised worldwide due to globalisation — meaning a great risk if the laws were inclined to restrict human rights — and, in parallel, to combat this, political actions must be taken on a global scale in order to provoke social change — which happened to be the *modus operandi* of WikiLeaks, helping the spread of the cypherpunk ethos.

Literature has also made it possible to stretch the elasticity of the term "cypherpunk" further by advancing the idea of "cypherpunk" being a characterisation of sociotechnical phenomena beyond individuals. This characterisation brought political dimensions to encryption itself by categorising different types of encryption according to their socio technical purpose. As an illustration, in the taxonomy proposed by Arvind Narayanan (2013), the term "crypto" deserves its own classification according to its purpose. *Crypto for security* would be designed to protect electronic transactions in the context of economic development; "*crypto for privacy*" would be sub-categorized in two others: "*pragmatic crypto*",

which aims to "keep the same level of privacy that we had in the analog world", and "*cypherpunk crypto*", that sees in cryptography an engine that inexorably re-shapes economic, social and political power structures.

Finally, the notion that *cypherpunk* can also be instrumental to qualify technologies is sustained by Nabben (2020). In the field of ethnography, she argues, there hasn't been a proper definition to classify *decentralised information infrastructures*, such as blockchain, nowadays best illustrated by cryptocurrency ecosystems. Defined by being *participatory*, *permissionless*, and *encrypted*, these infrastructures could produce digital assets categorised under the heading of *cypherpunk*.

Conclusion_

Along with the development of actors and technosocial structures regarding encryption, for the last thirty years the term *cypherpunk* has been used to describe different contexts. Originally used as an adjective to characterise individuals that used encryption as a way to perform social and political change, the term now can be understood as a qualification to individuals, groups, entities and techniques that fulfil its foremost vision: claiming and safeguarding rights and freedoms through encryption, with encryption as the basic and ultimate element. Therefore, it can be asserted that ***cypherpunk*** *refers to social movements, individuals, institutions, technologies, and political actions that, with a decentralised approach, defend, support, offer, code, or rely on strong encryption systems in order to re-shape social, political, or economic asymmetries.*

References_

- Abelson, H. (2015). *Keys Under doormats: Mandating insecurity by requiring government access to all data and communications* [Report]. Massachusetts Institute of Technology. http://hdl.handle.net/1721.1/97690
- Anderson, P. D. (2020). Privacy for the weak, transparency for the powerful: The cypherpunk ethics of Julian Assange. *Ethics and Information Technology*, *23*, 295–308.
- Assange, J. (2012). *Cypherpunks: Freedom and the Future of the Internet*. OR Books.
- Bennett, C. (2008). *The Privacy Advocates: Resisting the Spread of*

Surveillance. MIT Press.
- Burnham, D. (1983). *The Rise of the Computer State: The Threat to Our Freedoms, Our Ethics and Our Democratic Process*. Random House Inc.
- Chaum, D. (1985). Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*, *28*(10). https://dl.acm.org/doi/10.1145/4372.4373
- Coleman, G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3). https://doi.org/10.1177/1463499608093814
- Diffie, W., & Hellman, M. (1976). New directions on Cryptography. *IEEE Transactions on Information Theory*, *22*(6). https://ee.stanford.edu/~hellman/publications/24.pdf
- Diffie, W., & Landau, S. (2001). The export of cryptography in the 20th and the 21st centuries. In *The History of Information Security* (pp. 725–736). Elsevier. https://doi.org/10.1016/B978-044451608-4/50027-4
- Gilmore, J. (1991, March 28). *Privacy, Technology, and the Open Society.* First Conference on Computers, Freedom, and Privacy.
- Greenberg, A. (2012). *This Machine Kills Secrets: How WikiLeakers, Cypherpunks and Hacktivists Aim to Free the World's Information*. Dutton.
- Hellegren, I. (2016). Deciphering Crypto-Discourse: Articulations of Internet Freedom in Relation to The State. *11th Annual GigaNet Symposium*. http://dx.doi.org/10.2139/ssrn.2909373
- Hellegren, Z. I. (2017). A history of crypto-discourse: Encryption as a site of struggles to define internet freedom. *Internet Histories*, *1*(4), 285–311. https://doi.org/10.1080/24701475.2017.1387466
- Hughes, E. (1993). *A Cypherpunk's Manifesto*. https://www.activism.net/cypherpunk/manifesto.html
- Jarvis, C. (2021). Cypherpunk ideology: Objectives, profiles, and influences. *Internet Histories*. https://doi.org/10.1080/24701475.2021.1935547
- Kehl, D., Wilson, A., & Bankson, K. (2015). *Doomed to repeat history? Lesson from the crypto war of the 1990* [Report]. Open Technology Institute, New America. https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/
- Levy, S. (1992). Crypto Rebels. *WIRED*. https://www.wired.com/1993/02/crypto-rebels/
- Levy, S. (1995). *The Cypherpunks vs. Uncle Sam* (L. Hoffman, Ed.). Institute for Computer and Telecommunications Systems Policy

and Department of Electrical Engineering and Computer Science.
- Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. Penguin Books.
- LEXICO. (2006). *Cypherpunk*. LEXICO Powered by Oxford. https://www.lexico.com/definition/cypherpunk
- Lyon, D. (1992). The new surveillance: Electronic technologies and the maximum security society. *Crime, Law and Social Change*, *18*(1–2). https://doi.org/10.1007/BF00230629
- Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press.
- Manne, R. (2011). The cypherpunk revolutionary. *The Monthly*. https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary#mtr
- May, T. (1992). *The Crypto Anarchist Manifesto*. https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html
- Nabben, K. (2020). 'An ethnography of decentralised information infrastructure': Adopting cypherpunk nomenclature to categorise the unique attributes of decentralised technologies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3752531
- Narayanan, A. (2013). What Happened to the Crypto Dream? *IEEE Security and Privacy Magazine*. https://www.cs.princeton.edu/~arvindn/publications/crypto-dream-part1.pdf
- Pernice, I., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1561
- Rid, T. (2017). *Rise of the Machines: A Cybernetic History*.
- Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342
- Rogaway, P. (2015). *The moral character of cryptographic work* (Report No. 2015/1162). Cryptology ePrint Archive.
- Zimmermn, P. (1999). *Why I Wrote PGP*. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html
- Zubhoff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power*. Basic Books, Inc. Publishers.

Endnotes_

1. “The only thing they all shared was an understanding of the political significance of cryptography and the willingness to fight for privacy and unfettered freedom in cyberspace”, says Manne (2011).

DATA INTERMEDIARY_

Heleen Janssen, Institute for Information Law, University of Amsterdam, Netherlands.
Jatinder Singh, Compliant and Accountable Systems Research Group, Computer Science & Technology, University of Cambridge, United Kingdom.

Data intermediaries serve as a mediator between those who wish to make their data available, and those who seek to leverage that data. The intermediary works to govern the data in specific ways, and provides some degree of confidence regarding how the data will be used.

A data intermediary serves as a mediator between those who wish to make their data available, and those who seek to leverage that data. The intermediary works to govern the data in specific ways, and provides some degree of confidence regarding how the data will be used.

Data intermediaries form part of a data processing ecosystem. This includes the *intermediary*, often an organisation (of some form), as well as two other key categories of stakeholder:[1] *data suppliers* who are those individuals, communities, or enterprises that make their data available, and *third parties* referring to those interested in using (processing) supplier data.

Context and description_

The concept has emerged in the context of 'big data', and the increasing interest in data analytics and machine learning (Hardjono & Pentland, 2019; Stalla-Bourdillon et al., 2020; Micheli et al., 2021). Deep concerns however exist regarding opaque data practices, surveillance practices, and the systemic power and information asymmetries inherent to the current data processing ecosystems (Edelman, 2018), where organisations reap the value and benefit of data and its processing, rather than the people to whom the data pertains (Zuboff, 2015; Beer, 2017; Kitchin, 2017). Data intermediaries respond by attempting to help rebalance the relationships between those producing or with rights over data, and those seeking to use that data by offering an alternative approach to the data processing.

The data intermediary is a nascent, yet emerging concept, with the terminology still *in flux*. An intermediary's role, operation and the actions it will undertake, as well as its governance and incentive structures are very context sensitive. That is, how data intermediaries form and operate, largely depends on their purposes, the nature of suppliers and third parties they engage with, the intermediary's relationships with the suppliers and third parties involved, the data used, the means used to operate the intermediary (and whether these require a technical expertise), and so forth (see Terminologies below).

Intermediaries can be proposed for a range of purposes and relationships, including by non-profits (for instance a data trust), private organisations (for instance data marketplaces), or public institutions (for instance in contexts where the public sector seeks to share data with businesses). Their business model, incentive structures, interests and governance concerns depend on the type of organisation, the purposes it pursues and the sector where it operates. A charity data intermediary might receive subsidies for enabling the sharing of health data between the public and researchers for public health purposes, whereas a commercial data intermediary might perhaps ask a third-party entrance fee for engaging with the intermediary's ecosystem. Some communities may wish to pool their data to advance particular interests for that group, or for a broader common good (Hartman et al., 2021), as might for instance happen in a research knowledge commons (Wong & Henderson, 2020).

Each data intermediary typically involves data governance measures for ensuring that data is only accessed and used as/when appropriate, giving some degree of assurance, guarantee and confidence that the rights and/or other interests of the stakeholders are properly respected and maintained – all in alignment with the intermediary's aim (see 'Governance Structures' below).

Purpose and practical usages_

Intermediaries have been suggested as a way to try and tackle a range of concerns. Many proposals for data intermediaries aim in some way at countering the consolidation of power given corporate data capture and

data-driven business models (Delacroix & Lawrence, 2019; Blankertz, 2020; RadicalxChange).

Often discussed are intermediaries that aim at one or more of the following:

- protecting the interests and rights of data suppliers (Reed et al, 2019; Delacroix & Lawrence, 2019; Ada Lovelace 2021; GPAI/Aapti/ODI 2021);
- rebalancing power asymmetries in data exchanges, by encouraging and empowering the data suppliers to play an active role in setting the terms of data use (GPAI/Aapti/ODI 2021);
- supporting individuals in managing their data, including helping in managing consent (Crabtree et al., 2018; Data Governance Act 2020; Ada Lovelace, 2021; Centre for Data Ethics and Innovation 2021), and in exercising their data rights (Delacroix & Lawrence, 2019; Ada Lovelace, 2021);
- enabling collective bargaining power (Hardjono & Pentland, 2019; Ruhaak, 2019; Delacroix & Lawrence, 2019);
- enabling suppliers to monetise or otherwise extract value from their data (Ng & Haddadi, 2018; ODI, 2019; Mulgan & Straub, 2019; Benthall & Goldenfein, 2021);
- allowing the pooling of data for particular aims, e.g. for research purposes (Ausloos & Veale, 2020), investigative journalism purposes (Mahieu & Ausloos, 2020) or for the broader public interest (Scassa, 2020; see also 'data altruism' - Data Governance Act 2020; Ada Lovelace, 2021); or
- enabling the sharing of public data that is made available by governments, whereby the intermediary facilitates businesses access to that data (European Data Portal, 2019).

The above represents but a few broad categories regarding intermediary aims and example contexts in which they might be used; as the concept of the data intermediary is still developing, a variety of other purposes will likely emerge.

In terms of specific applications, data intermediaries have already been suggested and/or used in the context of the sharing of public sector data (Scassa, 2020); in the pooling of data for medical research (Centre for Data Ethics and Innovation, 2021); to enforce corporate compliance with

rights, including those around employment (ACDU; WorkerinfoExchange) and data (MyDataDoneRight) or to assist in identifying discriminatory practices in credit scores (OpenSchufa).

Governance structures_

An intermediary's governance mechanisms are generally proposed such that they operate in such a way that they allow for an intermediary's transparent and accountable data processing towards the other stakeholders.

Proposed data governance mechanisms include those legal, such as fiduciary duties, where intermediaries are legally obliged to act in supplier interests (Edwards, 2004; O'Hara, 2019; Delacroix & Lawrence, 2019; Ada Lovelace, 2021; GPAI/Aapti/ODI 2021), and contractual mechanisms, creating environments where data is governed under agreed terms in a controlled way (Reed et al., 2019; Micheli et al., 2020; Ada Lovelace, 2021; GPAI/Aapti/ODI 2021). Technology-backed mechanisms may also be used to allow for stakeholders to manage, monitor and control how data is accessed, used, shared, or kept in a secure manner (De Montjoye et al., 2014; Crabtree et al., 2018; Janssen et al., 2020).

These legal and technical measures can, in combination, work to provide, for example, the control and audit measures to ensure that data protection rights or trade secrets are complied with, and that data is only shared or used by third parties as appropriate. Third parties, in turn, will want assurances that the data aggregate shared aligns with supplier's agreements, and the law more generally.

The power structures associated with data intermediaries can vary, for example, where the intermediary holds supplier data and performs computation over that data supplier data (i.e. taking more a 'centralised approach' to data processing), or with the suppliers holding their own data, with suppliers themselves performing computation over their data, after which the results are shared, where the intermediary works to broker and coordinate such activities (a more 'decentralised' approach to data processing).

The specifics of the governance measures employed will vary depending on the nature, aims and purpose of the intermediary, and the stakeholder rights and interests involved.

Terminologies_

The term 'data intermediary', while being broad and all-encompassing, is about governance in the stakeholder interest. A range of terms have been used to describe intermediaries, which often relate to their governance structure. Common examples include:

data trusts, in which the intermediary will take on responsibility to steward supplier data for agreed purposes. Data trusts may be based on fiduciary duties to act in the suppliers' interests (Edwards, 2004; Hall & Pesenti, 2017; O'Hara, 2019; Delacroix & Lawrence, 2019; GPAI/Aapti/ODI 2021), and/or be based on a contractual or statutory legal obligations (ODI, 2018; Reed et al., 2019; Ada Lovelace, 2021; GPAI/Aapti/ODI 2021);

data commons, with members voluntarily 'pooling' their data for the benefit of a specific community (Wong & Henderson, 2020; Hartman et al. 2020), or for the general public interest Data Governance Act;

data cooperatives, often referring to a data intermediary owned and democratically controlled by its members who delegate control over data about them (Hartman et al., 2020);

data collaboratives, where participants from different sectors – including private companies, research institutions, and government agencies – can exchange data and data expertise to help solve public problems (S. Verhulst & D. Sangokoya, 2015);

personal information management systems (see 'PIMS' in this glossary), where technology-backed systems offer data suppliers means to mediate, monitor and control how their data is accessed, used, or shared (Janssen et al., 2020);

data marketplaces, data brokers or trusted third parties that work to allow the trading of data (Ng & Haddadi, 2018; Dataswift-HubofAllThings, which is also a PIMS).

From these examples we see that data intermediaries are an emerging concept, as both the terminologies and the approaches are not only still developing, but that they may also overlap.

Debate_

Ongoing discussions about data intermediaries include conversations and the development of research questions about, amongst other, how the governance structure of a data intermediary fits the purposes it pursues; whether a centralised or a decentralised approach to the data processing is appropriate for the specific intermediary's purposes, and the stakeholders involved; whether data intermediaries can, where that applies, lawfully act on behalf of the suppliers, and how such mandates relate to the supplier's rights and interests; the domains and sectors where intermediaries should be explored; the relationship between data intermediaries and personal information management systems, personal data stores and other technical infrastructures; what type of intermediary fits a certain category of suppliers (e.g. computer literate, or not), as well as questions of what robust data governance is appropriate in a specific type of data intermediary; questions of who controls and enforces the data intermediary's operations and compliance; and of who exercises oversight over the landscape with data intermediaries more broadly; and more fundamentally, whether and to what extent data intermediaries can be trusted all together.

Conclusion_

Data intermediaries serve as a mediator between those who wish to make their data available, and those who seek to leverage that data. The intermediary works to govern the data in specific ways, and provide some degree of confidence regarding how the data will be used, in particular with regards to the rights and interests of those whose data is involved. Data intermediaries are a nascent, but rapidly developing concept, which lends itself for many data sharing contexts. How an intermediary operates, and the nature of its governance mechanisms, will likely depend on the specifics of the context in which it seeks to operate.

References_

- Ada Lovelace Institute. (2021). *Exploring legal mechanisms for data stewardship* [Report]. https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/
- Ausloos, J., & Veale, M. (2021). Researching with data rights. *Technology and Regulation*, 136-157 Pages. https://doi.org/10.26116/

TECHREG.2020.010
– Beer, D. (2017). The social power of algorithms. *Information, Communication & Society*, *20*(1), 1–13. https://doi.org/10.1080/1369118X.2016.1216147
– Benthall, S., & Goldenfein, J. (2021). Artificial intelligence and the purpose of social systems. *Proceedings of the 2021 AAAI/ACM Conference on AI Ethics and Society (AIES '21*, 1–10. https://ssrn.com/abstract=3850456
• Blankertz, A. (2020). *Designing data trusts. Why we need to test consumer data trusts now* [Policy brief]. Stiftung Neue Verantwortung, Think Tank für die Gesellschaft im technologischen Wandel. https://www.stiftung-nv.de/en/publication/designing-data-trusts-why-we-need-test-consumer-data-trusts-now
– Centre for Data Ethics and Innovation. (2021). *Unlocking the value of data* [Report]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf
– Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., Amar, Y., Mortier, R., Li, Q., Moore, J., Wang, L., Yadav, P., Zhao, J., Brown, A., Urquhart, L., & McAuley, D. (2018). Building accountability into the Internet of Things: The IoT Databox model. *Journal of Reliable Intelligent Environments*, *4*(1), 39–55. https://doi.org/10.1007/s40860-018-0054-5
– de Montjoye, Y.-A., Shmueli, E., Wang, S. S., & Pentland, A. S. (2014). openPDS: Protecting the Privacy of Metadata through SafeAnswers. *PLoS ONE*, *9*(7), e98790. https://doi.org/10.1371/journal.pone.0098790
– Delacroix, S., & Lawrence, N. (2019). Bottom-up data Trusts: Disturbing the "one size fits all" approach to data governance. *International Data Privacy Law*, *9*(4), 236–252. https://doi.org/10.1093/idpl/ipz014
– Edelman. (2018). *Edelman trust barometer 2018 — UK findings*. https://www.edelman.co.uk/research/edelman-trust-barometer-2018-uk-findings
– E.D.P.B.-E.D.P.S. (2021). *Joint Opinion 3/2021 on the proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en
– Edwards, L. (2004). The problem with privacy. A modest proposal.

International Review of Law Computers & Technology, *18*(3), 313–346. https://ssrn.com/abstract=1857536

- European Commission. (2020). *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (COM/2020/767 final)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
- European Data Portal. (2019). *Open data maturity report 2019*. European Data Portal. https://data.europa.eu/sites/default/files/open_data_maturity_report_2019.pdf
- Global Partnership on Artificial Intelligence (GPAI), Aapti Institute, & Open Data Institute. (2021). *Enabling data sharing for social benefit through data trusts* [Report]. https://gpai.ai/projects/data-governance/data-trusts/enabling-data-sharing-for-social-benefit-through-data-trusts.pdf
- Hall, W., & Pesenti, J. (2017). *Growing the Artificial Intelligence Industry in the UK* [Report]. UK Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy.
- Hardjono, T., & Pentland, A. (2019). *Data cooperatives: Towards a foundation for decentralized personal data management*. https://doi.org/10.48550/ARXIV.1905.08819
- Hartman, T. (2020). Public perceptions of good data management: Findings from a UK-based survey. *Big Data & Society*, 1–16. https://doi.org/10.1177/2053951720935616
- Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020). Decentralised data processing: Personal data stores and the GDPR. *International Data Privacy Law*, *10*(4), 356–384. https://doi.org/10.2139/ssrn.3570895
- Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, *20*(1), 14–29. https://doi.org/10.1080/1369118X.2016.1154087
- Mahieu, R., & Ausloos, J. (2020). *Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access* [Preprint]. LawArXiv. https://doi.org/10.31228/osf.io/b5dwm
- Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 205395172094808. https://doi.org/10.1177/2053951720948087
- Mulgan, G., & Straub, V. (2019). *The new ecosystem of trust: How data trusts, collaboratives and cooperatives can help govern data for the maximum of public benefit* [Report]. Nesta. https://www.nesta.org.uk/blog/

new-ecosystem-trust/
- Ng, I., & Haddadi, H. (2018). Decentralised AI has the potential to upend the online economy. *WIRED*. https://www.wired.co.uk/article/decentralised-artificial-intelligence
- O'Hara, K. (2019). Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship. *WSI White Paper*, *1*. https://doi.org/10.5258/SOTON/WSI-WP001
- Pistor, K. (2020). Rule by data: The end of markets? *Law & Contemporary Problems*, *83*, 101–124.
- Reed, C., B.P.E. Solicitors, & Pinsent Masons. (2019). *Data trusts: Legal and governance considerations*. Open Data Institute. http://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf
- Ruhaak, A. (2019). Data trusts: Why, what and how. *Medium*. https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34
- Scassa, T. (2020). Designing data governance for data sharing. *Technology and Regulation*, 44-56 Pages. https://doi.org/10.26116/TECHREG.2020.005
- Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L., & Simperl, E. (2020). Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy*, *2*, e4. https://doi.org/10.1017/dap.2020.1
- Wong, J., & Henderson, T. (2020). Co-creating autonomy: Group data protection and individual self-determination within a data commons. *International Journal of Digital Curation*, *15*(1), 16. https://doi.org/10.2218/ijdc.v15i1.714
- Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Endnotes_

1. Note this is the terminology that we use; in this space, the terminology tends to vary.

DECENTRALISATION IN THE BLOCKCHAIN SPACE_

Balázs Bodó, Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands.
Jaya Klara Brekke, Department of Geography, Durham University, United Kingdom.
Jaap-Henk Hoepman, Institute for Computing and Information Sciences, Radboud University, Nijmegen, Netherlands.

The rapidly evolving blockchain technology space has put decentralisation back into the focus of the design of techno-social systems, and the role of decentralised technological infrastructures in achieving particular social, economic, or political goals. In this entry we address how blockchains and distributed ledgers think about decentralisation.

Decentralised network topologies_

A network is made of nodes, and edges, or interconnections between the members of the network. There are many different metrics with which one can describe the topology of a network (Bondy and Murty, 2008). In the following we define the centralised — decentralised — distributed nature of a network according to the number of edges a node has. In a distributed network every node has roughly the same number of edges, and there are more than one routes in which nodes can connect with each other. This means that the topology of the network does not contain nodes in central or privileged positions, or if there are hierarchies built into the network, each node belongs to more than one hierarchy. This gives distributed networks a special property: the failure of a few nodes (even if they are chosen on purpose) still leaves the network connected, allowing all nodes to communicate with each other (albeit over a possibly much longer path than in the original network).

Though often used as synonyms, decentralised and distributed networks are not the same. Decentralised networks are built from a hierarchy of nodes, and nodes at the bottom of the hierarchy have only a single connection to the network. Failure of a few nodes in a decentralised network still leaves several connected components of nodes that will be able to communicate with each other (but not with nodes in a different component).

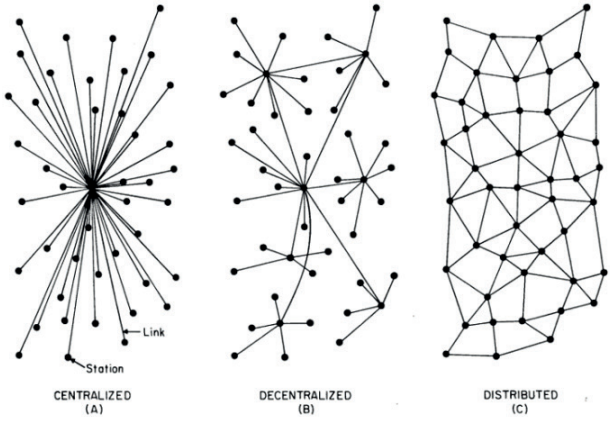


Figure 1: Various network topologies (Baran, 1964)

The degree of decentralisation and distributedness varies from network to network. In general networks that are more distributed are more resilient to the failure of individual nodes or loss of connection between them. This resilience applies to both concrete and virtual networks i.e physical network infrastructures (such as the routers, cables, backbones, WIFI hotspots of the internet), and virtual networks running on the physical layer, such as blockchain networks, or file sharing networks.

Initially designed to be a Cold War resilient distributed network, the internet is in fact a *decentralised* network. Consequently, there are multiple stakeholders, and multiple physical as well as virtual bottlenecks where the network is controllable, or vulnerable to surveillance, and failure (Forte et al., 2009; Kaiser, 2019; Kastelein, 2016; Snowden, 2019). Likewise, while the TCP/IP protocol envisaged a network in which each node (user, machine) could be both an information sender and receiver, in practice, highly centralised virtual networks emerged in knowledge production, communication, or commerce. The recent wave of re-decentralisation (Redecentralize, 2020) tries to address the centralisation of the virtual layers — often assuming this will lead to decentralisation in other dimensions including power and political control (Buterin, 2017).

Advantages and disadvantages of decentralisation_

Different network topologies come with particular advantages and disadvantages, that vary with the degree of centralisation, and the ways networks become more or less distributed over time. Distributed networks are more resilient to failure but incur a cost to maintain coordination. Centralised networks are much easier to maintain, but the central node can be a performance bottleneck and a single point of failure.

	COSTS	BENEFITS
DISTRIBUTED	Costs of maintaining individual nodes (security, connectivity, bandwidth, etc)	Higher resilience
	Cost of network coordination	Lack of nodes with unilateral control power
CENTRALISED	Central nodes can unilaterally set the conditions for using the network	Higher efficiency
	Lower resilience of the network, in particular the vulnerability of the network to the failure of the central nodes.	Lower cost of coordination

Table 1: Summary of the main costs and benefits associated with distributed and centralised networks

In distributed networks, each node has a wide range of responsibilities and associated costs. A distributed network is only operational if there is a coordination mechanism between the nodes.

In the absence of robust solutions to the problems of *coordination* and *fault tolerance*, Lamport et al (2019) have noted, a distributed system is only a network "in which the failure of a computer you didn't even know existed can render your own computer unusable".

Coordination problems must address, for example, how nodes reach each other (as in the internet routing system); how to deal with competition and race conditions (when multiple nodes want to use the same limited resource, such as a network printer); or how the system's operational and development processes are governed (Katzenbach and Ulbricht, 2019). These issues are usually resolved through the protocols which describe the basic rules and operation of a decentralised system (Galloway, 2004). On the other hand, updates to the protocol requires governance frameworks, which so far has not been successfully encoded in the protocol itself. G*overnance frameworks*, which might be equally distributed, remain experimental (Arruñada and Garicano, 2018; Atzori, 2017; De Filippi and Loveluck, 2016). Most of the distributed applications and services have bare-bones, generic governance frameworks. Governance, however, entails more than, for example, an infrastructure of secure voting. Effective participation in the governance mechanisms of a distributed social, political, economic system also requires substantive investment from the individual in terms of knowledge, time, attention, engagement.

The problem of fault-tolerance has to do with failures and attacks[1], and ensures that the overall network remains functional and continues to work to achieve its overarching goal while some of its components fail. Attacks that are particular to distributed and decentralised systems include DDoS (Distributed Denial of Service)[2] and Sybil attacks[3]. Distributed architectures are designed to be tolerant of the failure of a relatively high number (typically 30-50%) of all nodes in a network[4]. But Troncoso et al. (2017) also showed that decentralisation, done naively, may multiply the 'attack vectors', and security risks, not least the breach of privacy. Distributed architectures might also be worse in terms of availability and information integrity, as the failure of nodes may have a fundamental impact on these properties.

In distributed networks, individual nodes must also take care of their own security, and availability. Distributed networks also have issues with efficiency, such as the transaction throughput of blockchain systems, or the bandwidth and latency in the TOR routing network.

In return, when done right, distributed networks offer higher resilience. There is also a lower risk of any central actors taking control, or exercising unilateral power over the network. For this reason, decentralised network topologies are also used to achieve privacy, censorship resistance, availability, and information integrity information security properties (Hoepman, 2014; Troncoso et al., 2017).

In centralised systems coordination is taken care of by central actors who can specialise, and this leads to efficiency gains. There are costs to this, however, including making the network more vulnerable to the failure, or the abusive behaviour of that central node. Since network transactions run through a specific server, this grants those who control that server significant powers to observe, manipulate or cut off traffic (Troncoso et al., 2017), as well as to control, censor, tax, limit or boost particular social interactions, economic transactions, information exchange among network participants, and unilaterally set the conditions of interactions within the network.

To illustrate this cost-benefit calculus consider the privacy protecting TOR network. TOR is able to give reasonable levels of privacy at the cost of using a distributed network to route messages with lower speeds, and larger latency. These costs are seemingly too large for everyday users who are willing to settle for lower levels of privacy. On the other hand, for political dissidents who fear government retribution, journalists, whose integrity depends on their ability to protect their sources, and other groups for whom strong privacy is essential, the cost-benefit analysis justifies the higher costs of using this distributed network.

Both the costs and the benefits of using distributed network topologies are dynamic in nature, and are heavily dependent on factors both internal and external to the network (Marlinspike, 2016). For example, the unresolved problem of distributed governance often creates a certain structurelessness in the social, political dimensions of distributed networks. As Freeman (1972) or De Filippi and Loveluck (2016) pointed out,

seemingly unstructured social networks risk informal centralisation of their governance. In fact, blockchain networks have highly centralised forms of governance (Azouvi, Maller, and Meiklejohn, 2018; De Filippi, 2019; De Filippi and Loveluck, 2016; Musiani, Mallard, and Méadel, 2017; Reijers, O'Brolcháin, and Haynes, 2016). Blockchain networks may also suffer from centralisation in other dimensions of power. For instance, the *proof-of-work* (PoW) protocol randomly assigns a miner node to validate the latest batch of transactions for a relatively large reward to minimise the risk of a malicious miner hijacking the transaction ledger. The corresponding low chance of being rewarded forced miners to aggregate into a handful of coordinated mining pools, which control the vast share of this critical resource in an otherwise physically, geographically distributed network. The alternative approach, *proof-of-stake* (PoS) requires that those who wish to validate transactions stake their decisions with hard (crypto)cash: the larger the stake, the larger the validating power. PoS may remove mining pools, but creates another form of centralised power, namely that of capital. On the other hand, the increasing legal pressure on P2P file sharing networks, in particular on central nodes, pushed these projects towards increasingly distributed architectures, such as bittorrent networks, with distributed hash tables (Giblin, 2011). These dynamics push most systems to be decentralised, rather than fully distributed or centralised, as decentralised networks have some of the costs and benefits of both, depending on the particular level of centralisation and the particular context.

Distributed systems in practice_

While distributedness, as we have noted earlier, has been proposed as a general template for both the physical and the virtual digital networks, truly distributed networks only established themselves in particular niche applications, due to their particular cost-benefit balance.

P2P systems: P2P networks collectively make a resource (computation, storage) available among all nodes in the network. Examples of peer-to-peer computation networks are Seti@Home[5] and Folding@home.[6] Napster, Kazaa, or the bittorrent networks are peer-to-peer storage and file sharing networks, used to distribute copyrighted works under conditions of limited legal access (Johns, 2010; Patry, 2009). The peer-to-peer nature of these networks made it much harder to censor them

and to take down material that infringed on copyrights (Buford, Yu, and Lua, 2009).

Distributed ledgers are distributed data structures where a set of bookkeeping nodes (sometimes called miners), interconnected by a peer-to-peer network, collectively maintain a global state without centralised control (Narayanan et al., 2016). Bitcoin (Nakamoto, 2008) was the first distributed ledger, inventing *blockchain* as the data structure to store transaction histories of digital tokens capable of digitally representing units of value. Ethereum generalised the distributed ledger from recording transactions to instead process code and store the state of the network. Bookkeeping nodes maintain consensus on the list of executed transactions and their effect on the global state, as long as a specified fraction of the bookkeeping nodes is honest and active.

Secure multiparty computation allows several participants to collectively compute a common output, which is based on each of their private inputs. Instead of sending the private inputs to one central coordinator (that would therefore learn the values of all private inputs), the algorithm to compute the value is distributed and the computation is done on the devices of the participants themselves, thus ensuring that their inputs remain private (Cramer, Damgard, and Nielsen, 2015; Yao, 1982).

Decentralisation as a social template_

Distributed networks have brought experimentation with new coordination mechanisms, new ways to manage risks, and failures, lowering transaction costs and removing central powerful positions in technical terms. Proponents of disintermediation hope that these same logics provide new tools for horizontal social coordination, and the removal of political, economic, or social intermediary institutions, previously fulfilling those tasks (Schneider 2019).

The centralisation/decentralisation dichotomy is often framed in terms of power asymmetries, where distributed architectures are proposed as an alternative to authoritarian, coercive forms of political power. This dichotomy rests on a number of assumptions about power, and often does not fully account for the ways that, in practice, decentralisation in one dimension might produce or be enabled by centralisation in

another. In terms of economics, distributed digital networks often align with the concept of perfectly competitive markets, designed to prevent the emergence of entities in a monopoly position, whether information, resource, or other monopoly (Brekke, 2020). Yet in practice, markets tend to rely heavily on a regulatory body to ensure fair competition. Distributed ledger technologies (DLT) have also offered a possible technical solution to the loss of trust in institutional actors (Bodó, 2020), by setting up networks with little reliance on trusted third parties, and minimising the need to have trust in interpersonal relations (Werbach, 2018). Yet in practice, DLT brings along new kinds of intermediaries, from interface designers and wallet developers, to exchanges, miners, full nodes and core developers, therefore requiring new forms of accountability methods.

The recent popularity of distributed technical networks raised important questions about the preferred modes of social, political, or economic organisation. Digital innovation changes the costs and benefits of coordination and collaboration (Benkler, 2006). This highlights questions about the roles that intermediaries play in those relations (Sen and King, 2003). For example, cryptocurrency technology may have successfully demonstrated that there is no need for a centralised intermediary to keep accounts, or even run an asset exchange. However, that is not the only function of banks and exchanges. Trust generation, due diligence, risk assessment, conflict resolution, rules provision, accountability, insurance, protection, stability, continuity, and education are arguably also core functions of the banking system, offered in conjunction with the bookkeeping function. A second set of questions address the various layers which constitute a complex techno-social system, and the fact that a distributed topology at one layer, may not produce, require, or allow a distributed form of organisation at the other. In fact, often highly centralised governance is a precondition of a distributed system to function, as is currently the case in blockchain based systems. Another example would be the role of governments to ensure fair and open competition on various markets, such as anti-trust regulation, or in politics.

Conclusion_

Decentralised and distributed modes of organisation are well defined in computer science discourses and denote a particular network topology.

Even there, they can be understood either as an engineering *principle*, a design *aim*, or an aspirational *claim*. In the decentralisation discourse these three dimensions are often conflated without merit. A decentralised network design might not produce decentralising effects and might not either necessarily be decentralised in its actual deployment.

When the technical decentralisation discourse starts to include social, political, or economic dimensions, the risk of confusion may be even larger, and the potential harms of mistaking a distributed system for something it is not, even more dangerous. Individual autonomy, the reduction of power asymmetries, the elimination of market monopolies, direct involvement in decision making, solidarity among members of voluntary associations are eternal human ambitions. It is unclear whether such aims can now suddenly be achieved by particular engineering solutions. An uncritical view on decentralisation as an omnipotent organisational template may crowd out alternative approaches to creating resilient, trustworthy, equitable, fault resistant technical, social, political or economic modes of organisation.

References_

- Arruñada, B., & Garicano, L. (2018). *Blockchain: The Birth of Decentralized Governance* (Working Paper No. 1038). Barcelona Graduate School of Economics. https://ideas.repec.org/p/bge/wpaper/1038.html
- Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 1–37. https://doi.org/10.22495/jgr_v6_i1_p5
- Azouvi, S., Maller, M., & Meiklejohn, S. (2018). Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance. *22nd International Conference on Financial Cryptography and Data Security*. https://fc18.ifca.ai/bitcoin/papers/bitcoin18-final13.pdf
- Baran, P. (1964). On distributed communications networks. *IEEE Transactions on Communications Systems*, *12*(1), 1–9. https://doi.org/10.1109/TCOM.1964.1088883
- Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.
- Bodó, B. (2020). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*. https://doi.org/10.1177/1461444820939922
- Bondy, J. A., & Murty, U. S. R. (2008). *Graph theory*. Springer.

- Brekke, J. K. (2020). Hacker-engineers and Their Economies: The Political Economy of Decentralised Networks and 'Cryptoeconomics'. *New Political Economy*. https://doi.org/10.1080/13563467.2020.1806223
- Buford, J. F., Yu, H. H., & Lua, E. K. (2009). *P2P networking and applications*. Elsevier.
- Buterin, V. (2017). *The Meaning of Decentralization* [Blog post]. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
- Cramer, R., Damgard, I. B., & Nielsen, J. B. (2015). *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press. https://doi.org/10.1017/CBO9781107337756
- De Filippi, P. (2019). *Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream*. https://hal.archives-ouvertes.fr/hal-02445179
- De Filippi, P., & Loveluck, B. (2016). The invisible politics of Bitcoin: Governance crisis of a decentralised infrastructure. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.427
- Fischer, M. J., Lynch, N. A., & Paterson, M. S. (1985). Impossibility of distributed consensus with one faulty process. *Journal of the ACM*, *32*(2), 374–382. https://doi.org/10.1145/3149.214121
- Forte, A., Larco, V., & Bruckman, A. (2009). Decentralization in Wikipedia Governance. *Journal of Management Information Systems*, *26*(1), 49–72. https://doi.org/10.2753/MIS0742-1222260103
- Freeman, J. (1972). The tyranny of structurelessness. *Berkeley Journal of Sociology*, 151–164. https://www.jstor.org/stable/41035187
- Galloway, A. R. (2004). *Protocol: How control exists after decentralization*. MIT Press.
- Giblin, R. (2011). *Code Wars: 10 Years of P2P Software Litigation*. Edward Elgar Publishing.
- Hoepman, J.-H. (2014). Privacy design strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Eds.), *Proceedings of the 29th ICT Systems Security and Privacy Protection Conference* (Vol. 428, pp. 446–459). Springer. https://doi.org/10.1007/978-3-642-55415-5_38
- Johns, A. (2010). *Piracy: The Intellectual Property Wars from Gutenberg to Gates*. University Of Chicago Press.

- Kaiser, B. (2019). *Targeted: My inside story of Cambridge Analytica and how Trump, Brexit and Facebook broke democracy*. HarperCollins.
- Kastelein, R. (2016, June). World Wide Web Creator Tim Berners-Lee Wants to Decentralise the Internet with P2P and Blockchain Technologies. *BlockchainNews*. https://www.the-blockchain.com/2016/06/12/world-wide -web-creator -tim -berners -lee -wants -recreate-internet-blockchain/
- Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1424
- Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In *Concurrency: The Works of Leslie Lamport* (pp. 203–226). https://doi.org/10.1145/3335772.3335936
- Marlinspike, M. (2016). Reflections: The ecosystem is moving [Blog post]. *Signal*. https://signal.org/blog/the-ecosystem-is-moving/
- Méadel, C., Mallard, A., & Musiani, F. (2017). Governing what wasn't meant to be governed: A controversy-based approach to the study of Bitcoin governance. In *Bitcoin and Beyond* (pp. 133–156). https://doi.org/10.4324/9781315211909-7
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies*. Princeton University Press.
- Patry, W. F. (2009). *Moral panics and the copyright wars*. Oxford University Press.
- Redecentralize. (2020). *Redecentralize*. https://redecentralize.org/
- Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. *Ledger*, *1*, 134–151. https://doi.org/10.5195/ledger.2016.62
- Schneider, N. (2019). Decentralization: An incomplete ambition. *Journal of Cultural Economy*, *12*(4), 265–285. https://doi.org/10.1080/17530350.2019.1589553
- Sen, R., & King, R. C. (2003). Revisit the Debate on Intermediation, Disintermediation and Reintermediation due to E-commerce. *Electronic Markets*, *13*(2), 153–162. https://doi.org/10.1080/1019678032000067181
- Snowden, E. (2019). *Permanent Record*. Pan Macmillan.
- Troncoso, C., Isaakidis, M., Danezis, G., & Halpin, H. (2017). Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments. *Proceedings on Privacy Enhancing Technologies*,

2017(4), 404–426. https://doi.org/10.1515/popets-2017-0056
– Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.
– Yao, A. C. (1982). Protocols for secure computations. *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, 160–164.

Endnotes_

1. Failure can mean multiple things: the unavailability of a node; the unreliable, unexpected, or unaccounted for behaviour; and any malicious, manipulative or destructive behaviour. Failures can happen for a number of reasons: stochastic processes which may equally affect any node in a network due to their intrinsic properties; failures in some of the underlying layers: energy failures, environmental force majeure; as well as failures due to attacks by malicious actors.
2. ADDoS attack is when the bandwidth of a network is overloaded by flooding it with traffic coming from a distributed set of nodes.
3. A Sybil attack is when some actor/s create/s many nodes such that the network seems distributed, when in actual fact it might be controlled by a single or small set of actors.
4. The so-called Byzantine Agreement protocols allow a system to agree on a common output even if at most one-third of the members are faulty (in the Byzantine sense, meaning that they are malicious) (Lamport, Shostak, and Pease, 2019). But this is only the case under certain conditions. In particular, fully asynchronous systems (where there is no bound on the time it can take for a message to arrive or the time a node may take to complete a step) defy solutions to the Byzantine Agreement problem (Fischer, Lynch, and Paterson, 1985). This highly theoretical line of research re-emerged with the birth of Bitcoin and the subsequent explosion of distributed ledger technologies that exactly needed what Byzantine Agreement offered: reaching agreement on the global order of transactions, when faced with potentially malicious adversaries.
5. Started in 1999, its aim is detecting intelligent life outside Earth, see https://setiathome.berkeley.edu
6. Started in 2020, its aim is to simulate protein dynamics, see https://foldingathome.org

DECENTRALISED SOCIAL MEDIA_

Roel Roscam Abbing, School of Arts & Communication, Malmö University, Malmö, Sweden.
Cade Diehm, New Design Congress, Berlin, Germany.
Shahed Warreth, Cyber Threats Research Centre, Swansea University, Swansea, Wales, UK.

Social media platforms allow users to create digital identities, interact with other users, post and discover content. On mainstream social media platforms, aspects of the platform are centralised under the control of one umbrella. Decentralised social media are designed around the distribution of one or more aspects required to make social media function. Architecturally, these are data storage, content distribution, discovery, identity mechanisms and networking topology. Socially, these are their governance and revenue models. This article identifies and discusses three general types of decentralised social media grouped by architecture: federated, peer-to-peer, blockchain-based. Examples of each are discussed, along with a general description of their functioning and governance. Finally, the entry provides a general discussion of the drivers and issues around decentralised social media.

Definition_

Decentralised social media can generally be categorised as federated, peer-to-peer (P2P) and blockchain-based. These platforms are designed around the distribution of one or more of the following: data storage, content distribution, discovery, identity mechanisms, governance and moderation, revenue models and network topology. Different drivers exist for decentralised social media, ranging from historical concerns over centralised power structures to more contemporary concerns about centralised platforms' content moderation policies.

Historically, there have been few formal definitions of what constitutes social media. In different academic fields, different nomenclature such as social network sites or online social networks have been used to talk about what is colloquially referred to as social media, with as many as

six types proposed (Aichner & Jacob, 2015; McCay-Peet & Quan-Haase, 2017). Essential shared characteristics have been identified, as well as the need to distinguish between the different typologies of these platforms, such as microblogging or image sharing. While the typologies shift the type of content, the essential mechanisms are similar.

The core feature of social media is the social graph, which allows users to create profiles; establish connections to other users and interact with them; publish content; and receive feedback on this content (boyd & Ellison, 2007). Content publishing is the central social media activity, and is either made publicly available to all on the web or to specific groupings, such as users of the platform or accepted lists of followers. The content and the user's profile can be interacted with by following, commenting, reposting or leaving precoded reactions such as likes. On a technical level, social media platforms handle data storage; content discovery; identity establishment; addressing; and authentication. On a sociotechnical level, they also handle revenue models and content moderation (Gillespie, 2018).

Origins and evolution_

Contemporarily and colloquially, decentralisation is closely tied to the discourse around blockchain technologies, but has functioned as a critique of centralised power structures since the advent of computer networking, operating as a cultural, normative and technical logic (Russell, 2014). Networks, and in particular the Internet, are imagined to flatten power hierarchies and be democratising agents (Bory, 2020; Baran, 1964).

With regard to web technology, on which the majority of platforms are built, the dangers of centralising social functions has long been a concern, even prior to centralisation's emergence (Halpin, 2018). Consequently, the web engineering community has tried to decentralise key aspects of the social web through the creation of open standards, including identity provisioning (DNS, XDI, OpenID); authentication (OAuth); machine-readable web page metadata (RDF, XML, Microformats, Open Graph); and content transportation (RSS, ATOM, XMPP, ActivityPub). These efforts have had mixed results, partly because of internecine strife between different standards competing to solve similar issues (Halpin, 2018). Moreover, standards bodies such as the World Wide Web Consortium

(W3C) and the Internet Engineering Task Force (IETF) have approached decentralisation technically and without considering economic, political and social issues.

While some standards have not been widely adopted, others have paradoxically helped cement the market dominance of mainstream, centralised platforms like Facebook and Google as they have co-authored and embraced key aspects of these standards. For instance, while the metadata standard RDF was not widely adopted, it inspired Facebook's Open Graph protocol (Halpin, 2018). By adding Facebook's 'Like' button, web pages are readable by social media platforms in a standardised way, and provide features like rich link previews, giving Facebook the ability to track users even when they are logged out. Similarly, OAuth was developed to securely identify users on one website using data from another. While this theoretically enabled a decentralisation of identity mechanisms, in practice it helped consolidate the position of Facebook and Google as the de facto identity providers through the 'Login with Facebook' and 'Login with Google' buttons (Halpin, 2018).

Nevertheless, the open protocols resulting from these standardisation processes also laid the technical foundations for decentralised social media. Besides academic experiments with decentralised social network architectures such as the Friend-of-a-Friend project, the first decentralised social media to get some degree of traction and publicity were partly or wholly based on these protocols. Subsequent decentralised social media projects all make use of these standards in one way or another.

Coexisting uses, meanings and types_

Decentralisation has been characterised by the fuzziness of the term's usage and is thus in need of further characterisation and contextualisation (Bodó et al., 2021; Schneider, 2019; Troncoso et al., 2017). This section will provide avenues to characterise decentralisation in social media architecturally and culturally, and it introduces several examples of decentralised platforms, categorising them into the following: *federated*, *peer-to-peer* and *blockchain-based*.

The term decentralisation evokes its binary opposite, centralisation. However, in practice, centralised and decentralised systems are better

understood as existing on a spectrum (Graber, 2021). With regards to social media, centralisation is used to discuss architectures where all aspects of a social media system are under one umbrella, including content moderation. This is the case in the aforementioned centralised platforms where all users are provided with identity, authentication, data storage, addressing and governance from the same provider. On the other end of the spectrum, one can find peer-to-peer (P2P) architectures, where all users of the system connect directly to each other and are their own sources for addressing, data storage, identity and governance. Each topological configuration has distinct advantages and drawbacks when it comes to aspects such as privacy, scalability, usability and persistence (Troncoso et al., 2017).

Limiting the assessment of centralisation and decentralisation to network topology is an oversight. Moreover, decentralisation also operates as a rhetorical and cultural logic with multiple drivers. Schneider (2019, p. 2) argues that decentralisation, while discussed technically, is used to refer to a social order. Specifically, he identifies 'three interlocking legacies' for decentralisation discourse: early computer networks, political theory and the blockchain. Similarly, Bodó et al. (2021), outline drivers ranging from information security concerns to concerns over power asymmetries and desires for political and economic disintermediation**.** In recent years, the content moderation policies of social media platforms have also been a driver for decentralisation. This is addressed in the governance and content moderation section.

Federated_

Federated systems include the earliest attempts to create decentralised social media such as identi.ca, GNU Social and Diaspora, as well as recent projects such as Mastodon and PeerTube. Federated systems all rely on open web standards and are open source, and decentralise through online federation. Hosting providers ('instances') interoperate with other instances, allowing interaction between different instances. Different federated platforms are also interoperable with one another to varying degrees, similar to email, leading users to refer to them as the Fediverse (federated universe) (La Cava et al., 2021; Fediverse Network, 2020; Mansoux & Roscam Abbing, 2020). None of the federated projects follow a for-profit model, and are thus heavily reliant on donations, sponsorship, grants and volunteer labour.

The experience of the network is dependent on the instance you are part of as each instance takes care of data storage, content discovery, identity establishment, addressing and authentication. Since there is no global state for all messages and users, content discovery is contingent on the connections that an instance has established, which in turn depends on user-to-user connections. Therefore, what one can view also depends on what instance one is on, creating a pressure to establish connections with as many instances as possible. Moreover, if an instance disappears, the data of all users on that instance also disappears. Some projects such as Mastodon (2020) and Hubzilla (n.d.) allow users to migrate from one instance to another. For security and privacy, users are thus reliant on the administrative team behind each instance, as is the case with centralised social media.

Peer-to-peer_

While peer-to-peer (P2P) systems have received significant attention in academic literature in the past (see Masinde & Graffi, 2020 for an extensive discussion), few have developed past the prototype stage and seen much adoption. Secure Scuttlebutt (SSB) and Briar are two examples with an active userbase.

SSB is based on the so-called gossip protocol, wherein users receive an identity and corresponding set of encryption keys which are tied to their device. Users establish contact with other users' devices, and receive and forward data in the network to users they know directly (Kermarrec et al., 2020; Tarr et al., 2019). However, one's data is propagated into the network only when they are followed. This means all users are potentially part of the infrastructure required to propagate data through the network, and that users collectively take care of data storage, content discovery and identity establishment. While in theory the network can be solely based on direct user-to-user interactions, in practice it is heavily reliant on so-called 'pubs', wherein the servers are also part of the peer network and always online, thereby providing better speed, consistency and reliability (Troncoso et al., 2017, p. 311). SSB's underlying mechanism is replicated append-only logs, meaning deletion of information is not possible as all changes must be propagated through the network (Tschudin, 2019). Histories of changes such as following someone, subscribing to a topic or changing display names are also permanent. SSB's funding is mostly

derived from sponsorship and grants, but in some cases there is venture capital investment.

Similarly, Briar allows for private and group messaging in addition to the creation and subscription to blogs and message boards. Unlike SSB, Briar relies explicitly on direct interaction between users outside of the app. Data storage, content discovery and identity establishment are therefore based on device-to-device interactions, while their authoring and publication interfaces mirror those of other platforms. At their core, P2P platforms such as Briar are examples in which the underlying social graph is fully disconnected from a centralised source, and publication or other functionality rely entirely on alternative methods for discovery, mirroring, content display and other core functionality.

Blockchain-based_

Blockchain-based technologies are 'a distributed network of computers, ideally organised in a decentralised way, mutually agreeing on a common state while tolerating failures (incl. malicious behaviour) to some extent' (Valiente & Tschorsch, 2021). Blockchain-based social media feature cryptocurrencies which are usually created specifically for the platform and are derivatives of, for example, the Ethereum blockchain. Some are pegged to fiat currencies, usually the US dollar. Blockchain is an anonymised public ledger of all transactions, meaning anyone can look up the details of any transaction if they have the associated address or transaction hash. No transaction can be deleted or removed.

On blockchain-based platforms, cryptocurrencies are used for the monetisation of content and site governance, and are central to both the identity and revenue models of these platforms. Blockchain-based social media projects, like Minds (Ottman et al., 2018) and Steemit (Steem, 2017) are centralised in a single organisation which takes care of functions such as content discovery, identity establishment, addressing and authentication. Blockchain-based platforms have become synonymous with decentralisation in mainstream discourse due to their lenient terms of service and content moderation (Warreth, 2020). The scope of prohibited content is narrower as many of these platforms are a response to centralised platforms' content moderation policies. As such, content is stored on the blockchain or through a distributed storage system. Notably, Web3,

which is built on the Ethereum blockchain, seeks to build a new internet on blockchains, including social media, gaming and more (Roose, 2022). Examples of blockchain-based platforms include Minds (Ottman et al., 2018) and Steemit (Steem, 2017). However, Web3 has been deemed responsible for the 'the hyperfinancialization of all human existence' (Diehl, 2021).

Issues associated with the term_

Governance and content moderation_

Many decentralised social media platforms arose in response to the centralisation and therefore the power asymmetry of mainstream social media (Diehm, 2020), particularly with regards to content moderation. As platforms' content guidelines and the regulations governing them have changed, the (in)ability of communities to define what is acceptable has been a major driver for decentralised social media. As a result, users have migrated to other platforms or started new ones, though most have proven to be temporary or unsuccessful (Bodó et al., 2021; Edwards & Boellstorff, 2021; Warreth, 2020).

The perceived deplatforming of right-wing content from centralised platforms has led to increased interest in decentralised social media (Van Dijck et al., 2021; Barrett & Sims, 2021; Bevensee, 2020). One example is Gab, a platform based on Mastodon, with the ability to define one's own content moderation policy. Additionally, using federated software such as Mastodon allows for the use of the Fediverse's third-party mobile apps, which forms part of an explicit strategy to avoid deplatforming through the removal of branded apps (Van Dijck et al., 2021, p. 11). Similarly, Minds has attracted a notable extreme right user base, while supporters of the Islamic State and Al Qaeda have also promoted it (Popper, 2021; Rajendra-Nicolucci & Zuckerman, 2021, p. 31; Europol, 2021). Minds has stated that it allows extremist content in order to 'de-radicalize' users (Makuch & Pearson, 2019).

There are some examples of collective governance and moderation, including the Fediverse mobilising to collectively block Gab when it joined (Caelin, 2022). In the case of SSB, the use of codes of conduct and aesthetic signalling through imagery and language by developers, early adopters and advocates specifically aims to deter adoption by the

extreme right (Bevensee, 2020, pp. 15-16). However, users are responsible for making their own decisions about blocking others. The act of one account blocking another is propagated through the network, which can indicate to others to also block the account (Kermarrec et al., 2020; Tarr et al., 2019). It is important to note that while such platforms bring greater transparency, their immutable nature means even truly objectionable content, such as child sexual abuse material, cannot be removed (Diehl, 2021).

Multi-stakeholder open standards model_

Abbate (2000, p. 179) states that 'protocols are politics by other means', meaning parties working on technical standards use those standards to further their agenda (see also DeNardis, 2009, p. 10). Meanwhile, ten Oever (2021) demonstrates that much of internet standardisation is voluntary, and adherence is therefore based on strongly embodied norms and principles which can be easily undone. Halpin (2018) outlines the paradox of the multistakeholder open standards model, where work aimed towards the decentralisation of the web further enabled its centralisation. However, the same processes and technologies also enabled larger decentralised social networks to emerge. As such, this work is critical but vulnerable to corporate capture. This can happen not only through "Embrace, Extend, Extinguish" (Simcoe & Watson, 2019, p. 6) but also through the accumulation of a majority stake of a tokenised governance model, a form of Sybil attack which blockchains are uniquely vulnerable to. One such example of this is documented in the case of Steem (Rajendra-Nicolucci & Zuckerman, 2021, pp. 33-35).

As corporate initiatives to standardise decentralised social media emerge, it is worth questioning whether it is realistic to expect this model to yield different results than it has historically. A further question arises about whether a new or unified standard built from scratch and driven by a single party is favourable over building on existing protocols and established multi-stakeholder forums. Finally, it is worth noting that such technologies are often built in the West, and exported elsewhere with 'the belief that every social problem has a technological solution', akin to a white saviour. Cryptocurrencies in particular have been touted as revolutionalising poorer countries, in a mindset dubbed crypto-colonialism, echoing history (Ottenhof, 2021).

Conclusion_

Several types of social media exist, with centrally controlled platforms being the most widely known. Centralised and decentralised platforms exist on a spectrum, and are designed around the following: data storage, content distribution, discovery, identity mechanisms, governance and moderation, revenue models and network topology. While there have been several attempts to create open standards to ensure a decentralised internet, the importance of several providers has nonetheless solidified, thereby reinforcing centralised systems.

Nevertheless, several decentralised platforms have shown promise, but have not yet gained widespread adoption. One particular driver for their adoption is the content moderation policies of centralised platforms. Decentralised social media are seen as an alternative to the power asymmetry of centralised platforms, offering users autonomy and greater control over the content they see. Regardless, these technologies bring their own concerns, most notably with respect to their immutability and the monetisation of socialising. Moreover, the multi-stakeholder open standards model risks creating further centralised systems, despite their stated objectives.

References_

- Abbate, J. (1999). *Inventing the internet*. MIT Press. https://dl.acm.org/doi/10.5555/309692
- Aichner, T., & Jacob, F. (2015). Measuring the degree of corporate social media use. *International Journal of Market Research*, *57*(2), 257–276. https://doi.org/10.2501/IJMR-2015-018
- Baran, P. (1964). On distributed communications networks. *IEEE Transactions on Communications Systems*, *12*(1), 1–9. https://doi.org/10.1109/TCOM.1964.1088883
- Barrett, P. M., & Sims, J. G. (2021). *False accusation: The unfounded claim that social media companies censor conservatives* (pp. 1–24) [Report]. NYU Stern Center for Business and Human Rights. https://bhr.stern.nyu.edu/bias-report-release-page
- Bevensee, E. & Rebellious Data LLC. (2020). *The decentralized web of hate. White supremacists are starting to use peer-to-peer technology. Are we prepared?* (pp. 1–21). https://rebelliousdata.com/p2p/

- Bodó, B., Brekke, J. K., & Hoepman, J.-H. (2021). Decentralisation: A multidisciplinary perspective. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1563
- Bory, P. (2020). *The internet myth: From the internet imaginary to network ideologies*. University of Westminister Press. https://doi.org/10.2307/j.ctv12fw7sn
- Boyd, danah m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x
- Caelin, D. (2022). Decentralized networks vs the trolls. In H. Mahmoudi, M. H. Allen, & K. Seaman (Eds.), *Fundamental challenges to global peace and security: The future of humanity* (pp. 143–168). Palgrave Macmillan.
- DeNardis, L. (2009). *Protocol politics: The globalization of internet governance*. The MIT Press. https://doi.org/10.7551/mitpress/9780262042574.001.0001
- Diehl, S. (2021, December 4). Web3 is bullshit [Blog post]. *Stephen Diehl*. https://www.stephendiehl.com/blog/web3-bullshit.html
- Diehm, C. (2020). *This is fine: Optimism and emergency in the P2P network*. New Design Congress. https://newdesigncongress.org/en/pub/this-is-fine
- Edwards, E. J., & Boellstorff, T. (2021). Migration, non-use, and the 'Tumblrpocalypse': Towards a unified theory of digital exodus. *Media, Culture & Society*, *43*(3), 582–592. https://doi.org/10.1177/0163443720968461
- Europol. (2021). *Online jihadist propaganda: 2018 in review* (pp. 1–28) [Report]. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/cms/sites/default/files/documents/online_jihadist_propaganda_-_2018_in_review_0.pdf
- Fediverse Network. (2020, May 26). *Instances*. Internet Archive. https://web.archive.org/web/20200526120548/https://fediverse.network/.
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press. https://doi.org/10.12987/9780300235029
- Graber, J. (2021). *Ecosystem Review* (pp. 1–59). https://ipfs.io/ipfs/QmdFrru4PyHzXGZztEPnYToBR3QovD7fkC1HSyty22LzfD

- Halpin, H. (2018). Decentralizing the social web. *INSCI'2018- 5th International Conference 'Internet Science', October 2018*. https://hal.inria.fr/hal-01966561
- Hubzilla. (n.d.). *Help: Zot_protocol*. https://hubzilla.org/help/en/developer/zot_protocol
- Kermarrec, A.-M., Lavoie, E., & Tschudin, C. (2020). Gossiping with append-only logs in Secure-Scuttlebutt. *DICG'20: Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good*, 19–24. https://doi.org/10.1145/3428662.3428794
- La Cava, L., Greco, S., & Tagarelli, A. (2021). Understanding the growth of the Fediverse through the lens of Mastodon. *Applied Network Science*, *6*(1), 64. https://doi.org/10.1007/s41109-021-00392-5
- Makuch, B., & Pearson, J. (2019, May 28). Minds, the 'Anti-Facebook', has no idea what to do about all the neo-nazis. *Motherboard. Tech by Vice*. https://www.vice. com/en/article/wjvp8y/minds-the-anti-facebook -has-no-idea-what-to-do-about-all-the-neo-nazis
- Mansoux, A., & Roscam Abbing, R. (2020). Seven theses on the Fediverse and the becoming of FLOSS. In K. Gansing & I. Luchs (Eds.), *The eternal network: The ends and becomings of network culture* (pp. 124–140). Institute for Network Cultures & transmediale e.V. https://monoskop.org/images/c/cc/Mansoux_Aymeric_Abbing_Roel_Roscam_2020_Seven_Theses_on_the_Fediverse_and_the_Becoming_of_FLOSS.pdf
- Masinde, N., & Graffi, K. (2020). Peer-to-peer-based social networks: A comprehensive survey. *SN Computer Science*, *1*(5), 299. https://doi.org/10.1007/s42979-020-00315-8
- Mastodon. (2020). *Moving or leaving accounts*. http://docs.joinmastodon.org/user/moving/
- McCay-Peet, L., & Quan-Haase, A. (2017). What is social media and what questions can social media research help us answer? In L. Sloan & A. Quan-Haase (Eds.), *The SAGE handbook of social media research methods* (pp. 13–26). SAGE.
- Ottenhof, L. (2021, June 29). Crypto-colonialists use the most vulnerable people in the world as guinea pigs. *Motherboard. Tech by Vice*. https://www.vice.com/en/article/wx5zz9/crypto-colonialists-use-the-most-vulnerable-people-in-the-world-as-guinea-pigs
- Ottman, B., Harding, M., Ottman, J., & Ottman, J. (2018). *Minds: The crypto social network. Whitepaper v0.5* (pp. 1–34) [White paper]. https://www.minds.com/static/en/assets/documents/Whitepaper-v0.5.pdf

- Popper, N. (2021, January 26). They found a way to limit big tech's power: Using the design of Bitcoin. *The New York Times*. https://www.nytimes.com/2021/01/26/technology/big-tech-power-bitcoin.html
- Rajendra-Nicolucci, C., & Zuckerman, E. (2021). *An illustrated field guide to social media*. Knight First Amendment Institute Columbia University. https://knightcolumbia.org/blog/an-illustrated-field-guide-to-social-media
- Roose, K. (2022, March 18). What is web3? The latecomer's guide to crypto. *The New York Times*. https://www.nytimes.com/interactive/2022/03/18/technology/web3-definition-internet.html
- Russell, A. L. (2014). *Open standards and the digital age: History, ideology, and networks* (1st ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139856553
- Schneider, N. (2019). Decentralization: An incomplete ambition. *Journal of Cultural Economy*, *12*(4), 265–285. https://doi.org/10.1080/17530350.2019.1589553
- Simcoe, T., & Watson, J. (2019). Forking, fragmentation, and splintering. *Strategy Science*, *4*(4), 283–297. https://doi.org/10.1287/stsc.2019.0094
- Steem. (2017). *Steem: An incentivized, blockchain-based, public content platform* (pp. 1–32) [White paper]. https://steem.com/SteemWhitePaper.pdf
- Tarr, D., Lavoie, E., Meyer, A., & Tschudin, C. (2019). Secure Scuttlebutt: An identity-centric protocol for subjective and decentralized applications. *ICN'19: Proceedings of the 6th ACM Conference on Information-Centric Networking*, 1–11. https://doi.org/10.1145/3357150.3357396
- ten Oever, N. (2021). "This is not how we imagined it": Technological affordances, economic drivers, and the internet architecture imaginary. *New Media & Society*, *23*(2), 344–362. https://doi.org/10.1177/1461444820929320
- Troncoso, C., Isaakidis, M., Danezis, G., & Halpin, H. (2017). Systematizing decentralization and privacy: Lessons from 15 years of research and deployments. *Proceedings on Privacy Enhancing Technologies*, *2017*(4), 404–426. https://doi.org/10.1515/popets-2017-0056
- Tschudin, C. (2019). A broadcast-only communication model based on replicated append-only logs. *ACM SIGCOMM Computer Communication Review*, *49*(2), 37–43. https://doi.org/10.1145/3336937.3336943
- Valiente, M.-C., & Tschorsch, F. (2021). Blockchain-based technologies. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1552

– Van Dijck, J., de Winkel, T., & Schäfer, M. T. (2021). Deplatformization and the governance of the platform ecosystem. *New Media & Society*, 146144482110456. https://doi.org/10.1177/14614448211045662
– Warreth, S. (2020). *Comparing far right and jihadi use of crowdfunding, cryptocurrencies, and blockchain technology: Accessibility, geography, ideology* [Master's Thesis, Swansea University]. http://dx.doi.org/10.13140/RG.2.2.27543.09123

DAO (DECENTRALIZED AUTONOMOUS ORGANIZATION)_

Samer Hassan, Universidad Complutense de Madrid, Spain. Harvard University's Berkman Klein Center for Internet and Society, United States.
Primavera De Filippi, CERSA, CNRS, Paris, France. Harvard. University's Berkman Klein Center for Internet and Society, United States.

A DAO is a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralised (i.e., independent from central control).

Origin and evolution of the term_

Organisation theory has abundant literature on decentralised organisations of several kinds (Shubik, 1962; Beckhard, 1966; Freeland & Baker, 1975). Yet, the first references to actual Decentralized Autonomous Organization (DAO) only emerged in the 1990s to describe multi-agent systems in an internet-of-things (IoT) environment (Dilger, 1997) or nonviolent decentralised action in the counter-globalisation social movement (Schneider, 2014).

However, the modern meaning of DAOs can be traced back to the earlier concept of a Decentralized Autonomous Corporation (DAC), coined a few years after the appearance of Bitcoin (Nakamoto, 2008). The DAC concept was used mostly informally in online forums and chats by early cryptocurrency enthusiasts, using both "decentralized" and "distributed" autonomous corporations interchangeably. It was only in 2013 that the term became more widely adopted, and publicly discussed in a variety of websites (S. Larimer, 2013; D. Larimer, 2013), in particular by the co-founder of Bitcoin Magazine Vitalik Buterin[1] (Buterin, 2013).

DACs were described as a new corporate governance form, using tokenised tradable shares as a means of providing dividends to shareholders. Such corporations were described as "incorruptible", running "without any human involvement" and with "publicly auditable" bylaws as "open

source software distributed across the computers of their stakeholders" (S. Larimer, 2013). According to this definition, anyone could become a stakeholder in a DAC by simply "buying stock in the company or being paid in that stock to provide services for the company". As a result, the owners of a DAC stock would be entitled to "a share of its profits, participation in its growth, and/or a say in how it is run". (ibid). Such a definition reflects the maximalist view of many blockchain advocates considering that "DACs don't need regulation" because "you don't want to regulate them, and happily you can't" (ibid).

The term was inherently linked to corporate governance and therefore was too restrictive for many blockchain-based applications with a more general purpose. Thus, several alternatives to the term appeared, leading to the emergence of decentralized applications (dapps) (Johnston, 2013), and later to the generalisation of DAOs as a replacement for DACs (Buterin, 2014).

While some argue that Bitcoin is effectively the first DAO (Buterin, 2014; Hsieh et al., 2018), the term is today understood as referring not to a blockchain network in and of itself, but rather to organisations deployed as smart contracts on top of an existing blockchain network. Although there have been several attempts at instantiating a DAO on the Ethereum blockchain (Tufnell, 2014), the first DAO that attracted widespread attention is a 2016 venture capital fund confusingly called "TheDAO" (DuPont, 2017). Despite the short-life of the experiment[2], TheDAO has inspired a variety of new DAOs (e.g., MolochDAO, MetaCartel), including several platforms aimed at facilitating DAO deployment with a DAO-as-a-service model, such as Aragon, DAOstack, Colony or DAOhaus.

The DAO concept has enabled other derived terms: the term Decentralized Collaborative Organization (DCO) is typically referred as a DAO with strengthened collaborative aspects (Hall, 2015; Schiener, 2015; Davidson, De Filippi, & Potts, 2018); a more elaborate concept derived from those attempts is Distributed Cooperative Organization (DisCO), which highlights its co-op and democratic nature (Troncoso & Ultratel, 2019).

Definitions in the field_

There are multiple coexisting definitions of DAOs in use within the industry. The most relevant are the following:

– Buterin, in the Ethereum white paper (Ethereum, 2013, p. 23), defines a DAO as a "virtual entity that has a certain set of members or shareholders which [...] have the right to spend the entity's funds and modify its code". That is, the aim is to replicate "the legal trappings of a traditional company or nonprofit but using only cryptographic blockchain technology for enforcement" (ibid).

– Some of the most popular DAO platforms, such as DAOstack and Aragon define a DAO similarly as "a network of stakeholders with no central governing body" (https://daostack.io), "which is regulated by a set of automatically enforceable rules on a public blockchain" (https://aragon.org/dao). Conversely, other DAO platforms have opted to use a different terminology as a proxy to a DAO, such as the "colonies" of Colony (https://colony.io) or DAOhaus' "magic internet communities" (http://daohaus.club).

In the academic literature on DAOs, although some works avoid picking a definition (Norta et al., 2015) or refer to industry definitions (DiRose & Mansouri, 2018), multiple attempts have been made at providing a specific definition of DAOs. Most of these definitions include the following distinctive characteristics:

– DAOs enable people to coordinate and self-govern themselves online.[3] Although no mention is made as to the minimum size of the group, the term "organization" is generally understood to refer to an entity comprising multiple people acting towards a common goal[4], rather than a legally registered organisation.
– A DAO source code is deployed in a blockchain with smart contract capabilities like Ethereum — arguably always a public[5] blockchain.
– A DAO's smart contract code specifies the rules for interaction among people[6] — although it is unclear to which extent there may be other governance mechanisms that can affect or overrule such code.[7]
– Since these rules are defined using smart contracts, they are self-executed independently of the will of the parties.[8]
– The DAO governance should remain independent from central control:[9] e.g. some definitions specifically refer to self-governed (De Filippi & Hassan, 2018), self-organising (Singh & Kim, 2019), peer-to-peer and democratic control (Hsieh et al., 2018).

– Since they rely on a blockchain, DAOs inherit some of its properties, such as transparency, cryptographic security, and decentralisation.[10]

Current open discussions_

While the academic literature on DAOs is still fairly limited, there is a significant number of papers from the field of computer sciences focusing on blockchain technology as a technical platform for building new blockchain-based business models, such as decentralised exchanges (Lin et al., 2019; Bansal et al., 2019) or market-based platforms such as prediction markets (Clark et al., 2014) that operate as decentralised organisations with automated governance (Jentzsch, 2016; Singh & Kim, 2019). Yet, a DAO can be deployed to fulfill many different types of functions. A DAO can, for example, be used to create a virtual entity that operates as a crowd-funding platform, a ride-sharing platform, a fully automated company, or a fully automated decision-making apparatus. It is therefore important to understand that a DAO is not a particular type of business model or a particular type of organisation, but a concept that can be used to refer to a wide variety of things.

In terms of governance, diverse scholars recently started investigating the opportunities of blockchain technology and smart contracts to experiment with open and distributed governance structures (Leonhard, 2017; Rozas et al., 2018; Hsieh et al., 2018; Jones, 2019), along with the challenges and limitations of doing so (Garrod, 2016; DuPont, 2017; Scott et al., 2017; Chohan, 2017; Verstreate, 2018; Minn, 2019; Hutten, 2019). There is also an emerging body of literature from the field of economic and legal theory concerning DAOs. While most of these works focus on the new opportunities of decentralised blockchain-based organisations in the realm of economics and governance (Davidson et al., 2016, 2018; Sims, 2019; Rikken et al., 2019; Kaal, 2020), others focus on the legal issues of DAOs from either a theoretical (De Filippi & Wright, 2018; Reijers et al.. 2018) or practical perspective (Rodrigues, 2018; Werbach, 2018; Riva, 2019).

The political discourse around DAOs is more pronounced, at least in the context of many existing blockchain communities (Scott, 2015; Swartz, 2017; DuPont, 2019). Various authors have pointed out that DAOs could be used to further economic and political decentralisation in ways that may enable a more democratic and participatory form of governance

(Swan, 2015; Atzori, 2015; Allen et al., 2017; Tapscott & Tapscott, 2017). However, as the limitations of blockchain-based governance came into light, especially in the aftermath of the aforementioned TheDAO hack (DuPont, 2017; Reijers et al., 2018; Mehar et al., 2019), the public discourse around DAOs has shifted from describing DAOs as a technical solution to a governance problem (Jentzsch, 2016; Voshmgir, 2017) to a discussion on how DAOs could change the nature of economic and political governance in general (Davidson et al., 2016; Beck et al., 2018; Zwitter & Hazenberg, 2020; De Filippi et al., 2020).

The use of the term "decentralized autonomous organization" or DAO is now fairly established in the blockchain space, yet there are still many misconceptions and unresolved issues in the discussion around the term.

(1) First of all, with regard to the "decentralization" aspect of a DAO, it is unclear whether decentralisation only needs to be established on the infrastructural layer (i.e. at the level of the underlying blockchain-based network) or whether it also needs to be implemented at the governance level (i.e. the DAO should not be controlled by any centralised actor or group of actors).

(2) Second, it is unclear whether a DAO must be fully autonomous and fully automated (i.e. the DAO should operate without any human intervention whatsoever), or whether the concept of "autonomy" should be interpreted in a weaker sense, (i.e. while the DAO, as an organisation, may require the participation of its members, its governance should not be dependent on the whims of a small group of actors).

(3) Third, there are some debates as to when the community of actors interacting with a smart contract can be regarded as an actual "organization" (independently of any legal recognition). For instance, it is unclear whether the mere act of transacting with a smart contract qualifies as an organisational activity, or whether a stronger degree of involvement is necessary, such as having a governance model or collective interactions amongst participants.

The latter has triggered important discussions in the blockchain and legal field, as regards whether a DAO could be considered as an entity separate from the human entities that operate it (i.e. as a legal person) or whether

it can only be considered as an entity when it is identified as such by the law (i.e. the law should identify a DAO as a legal person for the DAO to be considered as such). Yet, the common understanding today is that the "autonomous" nature of a DAO is incompatible with the notion of legal personhood, as legal personhood can only be established if there is one or more identified actors responsible for the actions of a particular entity. The discussion on whether a DAO should be recognised as a legal person has important implications in the legal field, as it can determine the extent to which a DAO can be considered as a separate legal entity from its human actors, and therefore the extent to which these actors can be shielded from the liabilities of the DAO.

References_

- Allen, D. W., Berg, C., Lane, A. M., & Potts, J. (2017). *The economics of crypto-democracy*. 26th International Joint Conference on Artificial Intelligence, Melbourne. https://doi.org/10.2139/ssrn.2973050
- Atzori, M. (2015). *Blockchain technology and decentralized governance: Is the state still necessary?* https://doi.org/10.2139/ssrn.2709713
- Bansal, G., Hasija, V., Chamola, V., Kumar, N., & Guizani, M. (2019, December). Smart Stock Exchange Market: A Secure Predictive Decentralized Model. *2019 IEEE Global Communications Conference (GLOBECOM)*. https://doi.org/10.1109/GLOBECOM38437.2019.9013787
- Beck, R. (2018). Beyond bitcoin: The rise of blockchain world. *Computer*, *51*(2), 54–58. https://doi.org/10.1109/MC.2018.1451660
- Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10). https://aisel.aisnet.org/jais/vol19/iss10/1
- Beckhard, R. (1966). An Organization Improvement Program in a Decentralized Organization. *The Journal of Applied Behavioral Science*, *2*(1), 3–25. https://doi.org/10.1177/002188636600200102
- Buterin, V. (2013a). *Ethereum whitepaper: A next-generation smart contract and decentralized application platform* [White Paper]. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
- Buterin, V. (2013b, September 13). Bootstrapping A Decentralized

Autonomous Corporation: Part I. *Bitcoin Magazine*. https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274

- Buterin, V. (2014, May 6). DAOs, DACs, DAs and More: An Incomplete Terminology Guide [Blog post]. *Ethereum Foundation Blog*. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/
- Chohan, U. (2017). *The Decentralized Autonomous Organization and Governance Issues* (Notes on the 21st Century) [Discussion Paper]. University of New South Wales. https://doi.org/10.2139/ssrn.3082055
- Clark, J., Bonneau, J., Felten, E. W., Kroll, J. A., Miller, A., & Narayanan, A. (2014, June). *On decentralizing prediction markets and order books*. 13th Annual Workshop on the Economics of Information Security, Pennsylvania State University. https://econinfosec.org/archive/weis2014/papers/Clark-WEIS2014.pdf
- Davidson, S., De Filippi, P., & Potts, J. (2016a). *Disrupting governance: The new institutional economics of distributed ledger technology*. https://dx.doi.org/10.2139/ssrn.2811995
- Davidson, S., De Filippi, P., & Potts, J. (2016b). *Economics of Blockchain*. https://doi.org/10.2139/ssrn.2744751
- Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, *14*(4), 639–658. https://doi.org/10.1017/S1744137417000200
- De Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, *21*(12). https://doi.org/10.5210/fm.v21i12.7113
- De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*. https://doi.org/10.1016/j.techsoc.2020.101284
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
- Dilger, W. (1997). Decentralized autonomous organization of the intelligent home according to the principle of the immune system'. *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, 351–356. https://doi.org/10.1109/ICSMC.1997.625775
- DiRose, S., & Mansouri, M. (2018). Comparison and analysis of

governance mechanisms employed by blockchain-based distributed autonomous organizations. *2018 13th Annual Conference on System of Systems Engineering (SoSE)*, 195–202. https://doi.org/10.1109/SYSOSE.2018.8428782

- DuPont, Q. (2018). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In M. Campbell-Verduyn (Ed.), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (pp. 157–177). Routledge. https://doi.org/10.4324/9781315211909-8
- DuPont, Q. (2019). *Cryptocurrencies and blockchains*. John Wiley & Sons.
- El Faqir, Y., Arroyo, J., & Hassan, S. (2020). An overview of decentralized autonomous organizations on the blockchain. *Proceedings of the 16th International Symposium on Open Collaboration*, 1–8. https://doi.org/10.1145/3412569.3412579
- Franklin, S., & Graesser, A. (1996). Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents'. In *International Workshop on Agent Theories, Architectures, and Languages* (pp. 21–35). Springer. https://doi.org/10.1007/BFb0013570
- Freeland, J. R., & Baker, N. R. (1975). Goal partitioning in a hierarchical organization. *Omega*, *3*(6), 673–688. https://doi.org/10.1016/0305-0483(75)90070-5
- Garrod, J. Z. (2016). The real world of the decentralized autonomous society. *TripleC: Communication, Capitalism & Critique*, *14*(1), 62–77. https://doi.org/10.31269/triplec.v14i1.692
- Hall, J. (2015). The Future of Organization, Deep Code [Blog post]. *Deep Code Medium*. https://medium.com/deep-code/the-future-of-organization - b26219e5fc95
- Hsieh, Y. Y., Vergne, J. P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. *Journal of Organization Design*, *7*(1), 1–16. https://doi.org/10.1186/s41469-018-0038-1
- Hütten, M. (2019). The soft spot of hard code: Blockchain technology, network governance and pitfalls of technological utopianism. *Global Networks*, *19*(3), 329–348. https://doi.org/10.1111/glob.12217
- Jentzsch, C. (2016). *Decentralized autonomous organization to automate governance* [White Paper].
- Johnston, D. (2013). *The General Theory of Decentralized Applications, Dapps*.

David Johnston CEO. https://github.com/DavidJohnstonCEO/DecentralizedApplications
- Jones, K. (2019). Blockchain in or as governance? Evolutions in experimentation, social impacts, and prefigurative practice in the blockchain and DAO space. *Information Polity*, *24*(4), 469–486. https://doi.org/10.3233/IP-190157
- Kaal, W. A. (2020). Decentralized Corporate Governance via Blockchain Technology. *Annals of Corporate Governance*, *5*(2), 101–147. https://doi.org/10.1561/109.00000025
- Larimer, D. (2013a). *Bitcoin and the Three Laws of Robotics.* [Blog post]. Let's Talk Bitcoin. https://letstalkbitcoin.com/blog/post/bitcoin-and-the-three-laws-of-robotics
- Larimer, D. (2013b). DAC Revisited. Lets Talk Bitcoin [Blog post]. *Let's Talk Bitcoin*. https://letstalkbitcoin.com/blog/post/dac-revisited
- Leonhard, R. (2017). *Corporate Governance on Ethereum's Blockchain*. https://dx.doi.org/10.2139/ssrn.2977522
- Lin, L. X., Budish, E., Cong, L. W., He, Z., Bergquist, J. H., Panesir, M. S., & Wu, H. (2019). Deconstructing Decentralized Exchanges. *Stanford Journal of Blockchain Law & Policy*.
- Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology (JCIT*, *21*(1), 19–32. https://doi.org/10.4018/JCIT.2019010102
- Minn, K. T. (2019). Towards Enhanced Oversight of" Self-Governing" Decentralized Autonomous Organizations: Case Study of the DAO and Its Shortcomings. *NYU J. Intell. Prop. & Ent. L*, *9*, 139.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system'*.
- Norta, A., Othman, A. B., & Taveter, K. (2015). Conflict-resolution lifecycles for governed decentralized autonomous organization collaboration. *Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, 244–257. https://doi.org/10.1145/2846012.2846052
- Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Vélez, A. C., & Orgad, L. (2018). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi*. https://doi.org/10.1007/s11245-018-9626-5
- Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of

blockchain and decentralized autonomous organizations. *Information Polity*, *Preprint*, 1–21. https://doi.org/10.3233/IP-190154

- Riva, S. (2019). *Decentralized Autonomous Organizations (DAOs) as Subjects of Law–the Recognition of DAOs in the Swiss Legal Order* [Master's Thesis].
- Rodrigues, U. R. (2018). Law and the Blockchain. *Iowa L. Rev*, *104*, 679.
- Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2018). *When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance*. https://eprints.ucm.es/id/eprint/59643/1/SSRN-id3272329.pdf
- Schiener, D. (2015). Reposium: The future of Wikipedia as a DCO. *Medium*. https://medium.com/@DomSchiener/reposium-dco-the-future-of-wikipedia-4be080cfa027
- Schneider, N. (2014). *Are You Ready to Trust a Decentralized Autonomous Organization?. Shareable*. https://www.shareable.net/are-you-ready-to-trust-a-decentralized-autonomous-organization/
- Scott, B. (2015). *Visions of a techno-leviathan: The politics of the bitcoin blockchain*.
- Scott, B., Loonam, J., & Kumar, V. (2017). Exploring the rise of blockchain technology: Towards distributed collaborative organizations. *Strategic Change*, *26*(5), 423–428. https://doi.org/10.1002/jsc.2142
- Shubik, M. (1962). Incentives, Decentralized Control, the Assignment of Joint Costs and Internal Pricing'. *Management Science*, 325–343. https://doi.org/10.1287/mnsc.8.3.325
- Sims, A. (2019). *Blockchain and Decentralised Autonomous Organisations (DAOs): The Evolution of Companies?* https://dx.doi.org/10.2139/ssrn.3524674
- Singh, M., & Kim, S. (2019). Blockchain technology for decentralized autonomous organizations. In *Advances in Computers* (Vol. 115, pp. 115–140). Elsevier. https://doi.org/10.1016/bs.adcom.2019.06.001
- Swartz, L. (2017). *Blockchain dreams: Imagining techno-economic alternatives after Bitcoin. Another economy is possible: Culture and economy in a time of crisis*.
- Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review*, *58*(2), 10.
- Troncoso, S., & Utratel, A. M. (2019). *If I Only Had a Heart: A DisCO Manifesto*. DisCO. https://disco.coop/manifesto/
- Tufnell, N. (2014). *Bitcloud wants to replace the internet*. https://www.

wired.co.uk/article/bitcloud
- Verstraete, M. (2018). The Stakes of Smart Contracts. *Loyola University Chicago Law Journal*, *ue 50*.
- Voshmgir, S. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, *26*(5), 499–509. https://doi.org/10.1002/jsc.2150
- Werbach, K. (2018). Trust, but verify: Why the blockchain needs the law. *Berkeley Tech. LJ*, *33*, 487. https://doi.org/10.15779/Z38H41JM9N
- Zwitter, A., & Hazenberg, J. (2020). Decentralized Network Governance: Blockchain Technology and the Future of Regulation. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2020.00012

Endnotes_

1. Vitalik Buterin would later co-found the Ethereum platform in 2014.
2. This open-source project attracted 11,000 investors and USD$ 150 million, where the funds were operated by the code implemented, theoretically safe from managerial corruption. However, a bug in its code enabled vulnerabilities exploited by an attacker who stole USD$ 50 million, requiring a fork in the Ethereum blockchain to restore the funds.
3. See e.g. Singh and Kim (2019, p. 119) who describe a DAO as a "a novel scalable, self-organizing coordination on the blockchain, controlled by smart contracts".
4. See e.g. El Faqir, Arroyo, and Hassan (2020, p. 2) according to whom a DAO is made up of "people with common goals that join under a blockchain infrastructure that enforces a set of shared rules".
5. See e.g. Hsieh et al. (2018, p. 2) claiming that a DAO should be deployed on a "public network".
6. See e.g. De Filippi and Hassan (2018, p. 12), describing a DAO as a"self-governed organization controlled only and exclusively by an incorruptible set of rules, implemented under the form of a smart contract".
7. See e.g. Singh & Kim (2019, p. 119)'s definition of a DAO as "an organization whose essential operations are automated agreeing to rules and principles assigned in code without human involvement". However, this definition is put into question by Reijers, Wuisman, Mannan, De Filippi and colleagues (Reijers et al., 2018) distinguishing between "on-chain" and "off-chain" governance in the governance structure of DAOs.

8. See also De Filippi & Wright (2018, p. 146), according to whom a DAO "represents the most advanced state of automation, where a blockchain-based organization is run not by humans or group consensus, but rather entirely by smart contracts, algorithms, and deterministic code".
9. See e.g. Hsieh et al. (2018, p. 2) describing DAOs as "non-hierarchical organizations that perform and record routine tasks on a peer-to-peer, cryptographically secure, public network, and rely on the voluntary contributions of their internal stakeholders to operate, manage, and evolve the organization through a democratic consultation process".
10. "A decentralized, transparent, and secure system for operation and governance among independent participants" which "can run autonomously" (Beck, 2018, p. 57).

DIGITAL SCARCITY_

Jaya Klara Brekke, Department of Geography, Durham University, United Kingdom.
Aron Fischer, Colony, New York, United States.

Digital Scarcity is a credibly maintained limitation, imposed through software, of digital information, goods or services that may be accessed and used entirely digitally.

The history of digital scarcity_

Some of the earliest uses of the term *digital scarcity* stem from the early 2000s and describe the scarcity of access to IT resources and the underlying physical resources that computers and networks rely on — i.e. "the scarcity of the digital" (Weinberger, 2003; Hammersley, 2003; Chaudhry & Shipp, 2005). In one prominent example, legal restrictions on access to radio frequencies stymied the growth of communications networks at the beginning of this century — and activists and network operators bemoaned the resulting *digital scarcity* (Weinberger, 2003; Hammersley, 2003). The explosive growth of mobile telephony and the widespread demand for digital services on mobile devices led to public auctions of radio spectrum usage rights in order to alleviate this particular form of legally imposed scarcity (Wikipedia contributors, 2021). *Digital scarcity*, as referring to the availability of IT resources, has also described issues of accessibility due to forms of marginalisation (the *digital divide*), including lack of access because of disabilities. In this specific context, the term *digital scarcity* is used to describe "the dearth of accessible technological and other resources, lack of political will to address the problem, and general ignorance about digital access" (Chaudhry & Shipp, 2005, sect. 6, para. 10).

As internet access has become more widespread, and as an increasing amount of content is consumed digitally (text, news, music), the usage of the phrase has shifted. Digital scarcity now refers to the imposition of limits and conditions on availability and access to digital content. Digital information can be easily copied and is by nature not scarce or rivalrous; it can be shared at next to no cost, with no reduction in availability or quality: 'Digital reproduction frustrates notions of originality' (O'Dwyer, 2020, p. 874). As assets that were previously scarce or rivalrous (e.g.,

number of copies of a book or record) became increasingly digital, this led to no end of difficulties in the realm of copyright enforcement (Perzanowski & Schultz, 2016). In this context, *digital scarcity* describes limitations set on the access to data, in order to protect business models that depend on scarcity, as well as in the development of new forms of digital markets and economies.

Copyright-based industries for example, seek to impose digital scarcity to prevent copying of data. In the case of music, the value to the customer is clear, but scarcity needs to be maintained in order to protect industry profits. In the words of Warner Music Group chairman Edgar Bronfman: "Music is ubiquitous to a degree that also I think is probably not helpful for the industry" (Resnikoff, 2007). On the other hand, manipulating (perceptions of) scarcity is used *a priori* as a marketing tool in order to create demand for digital goods and services (Fortin, 2007). This (pre-bitcoin) notion of scarcity is perhaps best summed up in the following: "*One key to the success of digital goods business models is to maintain the scarcity of the digital goods. Since digital goods are digital, they cost nothing to copy. Free copies of digital goods would reduce demand for paying for the same item. In a closed system, it is easier to maintain scarcity. The company controls the supply of all digital goods completely.*" (Lightspeed Venture Capital Partners, 2008).

The rise of the internet, and the ease with which data could be copied, led to movements of digital activists seeking to open the access to information entirely ('information wants to be free'). These movements often clashed with intellectual property and copyright-based industries (Dahlstrom et al., 2006; Swartz, 2016), and these clashes in turn informed much of the development of peer-to-peer systems that would enable circumvention of the copyright industry, and free access to information (Oram, 2001; Andersson, 2011). Arguments were put forward that nothing digital is genuinely scarce and that any imposed scarcity is not just artificial, but also objectionable. "In digital goods, scarcity doesn't exist" and "the economics of scarcity doesn't apply digitally" (Masnik, 2006a). Virtual goods are only scarce by design and, as such are scarce by choice, and "that's a recipe for trouble" (Masnik, 2006b; see also Knowles, Castronova, and Ross, 2015, p. 242).

If we look beyond mere data, there *are* digital resources that are inherently limited, such as bandwidth or short domain names. Short domain names

for instance (using the English alphabet) are scarce due to the limitations of the alphabet, and may sell for millions of dollars (WP02); but scarcity of top-level-domains (such as .com, .org, .luxe, or .io) is artificially created and maintained by the Internet Assigned Numbers Authority (IANA) and the Internet Corporation for Assigned Names and Numbers (ICANN). Sometimes the creation of digital scarcity is accidental and its maintenance is due to a failure in governance. A prominent example is the dearth of IPv4 (Internet Protocol version 4) addresses (Rodriguez, 2012). The looming shortage has been apparent since the 1990s, and yet the coordinated migration to the newer IPv6 has yet to be achieved on a large scale.

Bandwidth meanwhile is a hotly contested commodity and the ability to impose artificial scarcity on specific customers or types of content is subject to intense legal wrangling (Smith, 2010). Indeed, the imposition of limitations on bandwidth has been used as a means to clamp down on peer-to-peer file sharing or to degrade performance of a competitor's services, known as *throttling*. In response, the notion of 'net neutrality' emerged as part of a campaign aiming to protect the free flow of data and ensure that internet providers are not legally allowed to limit internet access based on content or source or usage (Wu, 2003; for an overview, see Finley, 2020).

Digital scarcity in the age of blockchains_

In the context of the Bitcoin blockchain, *digital scarcity* refers to the limitation on the total supply of bitcoin. In contrast to the previous meaning, access to data is not restricted, and indeed the network relies on the blockchain data being freely available for anyone to copy in order to function securely. What determines a specific *bitcoin* is thus not its uniqueness as a piece of data, but rather its function as a verified entry in a distributed ledger.

It should also be noted that while both the cryptocurrency ether (on the Ethereum blockchain) and bitcoin (on the Bitcoin blockchain) are finite. The total amount of ether rises linearly whereas the total amount of bitcoin rises at a linear rate that is then halved every four years, so that the total number of bitcoins asymptotically approaches 21 million. As both blockchains enable finite transfers of a finite amount of digital currency, and the total amount in question grows only (sub-)linearly, they

both exhibit digital scarcity and are not subject to uncontrolled inflation brought about by an out-of-control increase in money supply.

There is a further aspect of scarcity inherent in Bitcoin (and indeed any blockchain). Just as the bitcoin supply is limited to 21 million, so too is the Bitcoin network limited to seven transactions per second. These are both examples of digital scarcity, but while the former limit is entirely arbitrary and determined in protocol designs, the latter cannot be arbitrarily raised as it is bounded by bandwidth and processing constraints.

In the digital realm, data can be copied, databases re-indexed and values of variables can be changed — at least in principle. As the copyright battles of the 1990s and early 2000s made clear, maintaining digital data scarcity by preventing copies is nearly impossible. Copying data is just too easy and ubiquitous. However, establishing *referential* scarcity, where references are ledger/database entries (and the referents are anything from cryptocurrencies to *cryptokitties*), is possible as long as it can be credibly established that the scarcity will be maintained and the rules adhered to. The crucial aspect of referential scarcity is not control over data availability, but control over manipulation of the data in question. This was the innovation of Bitcoin and the invention of the blockchain as a decentralised ledger technology.

With the invention of Bitcoin, digital scarcity could be established without the need for a central entity to enforce it. Instead, the network uses cryptographic hash cycles (mining) in order to agree on, maintain and enforce a record of valid transaction data. Cryptocurrencies are not the first databases with finite number entries, but they are the first in which changes to the entries cannot be forced by the entities providing the computing infrastructure. The notion that centralised control over a database is necessary to ensure digital scarcity was thus overturned.[1]

As more advanced and general-purpose blockchain networks such as Ethereum appeared, the scope for scarce ledger entries grew. Aside from scarcity of cryptocurrencies and currency-like 'tokens', a new class of 'unique digital items' known as *non fungible tokens*, or NFTs have appeared. These range from formal claims of ownership over a real-world (offline) asset, to purely digital collectibles (see, for example, Serada, Sihvonen, and Harviainen, 2020).

The rise of NFTs has led to experiments with new types of digital property where 'the broader intention does not appear to be to reduce the circulation and reproduction of the work, but instead to create titles and derivatives from its use and circulation' (O'Dwyer, 2020, p. 876). This for example implies producing a digital 'original' where its source and provenance is considered important enough to be able to acquire value as a 'unique' digital object, but where 'copies' can nevertheless circulate freely. However, there are considerable doubts about whether the possibilities afforded by distributed ledgers for new forms of digital scarcity will challenge much of the economic dynamics of property rights, or financial speculation and benefit producers of digital goods (Zeilinger, 2018; Lotti, 2016).

Issues currently associated with the term_

At the time of writing, the culture around blockchains is still young, and it remains highly politicised and polarised. This polarisation contributes to the confusion surrounding *digital scarcity* as it relates to ideas of value. Proponents of Bitcoin in particular argue that it is the limited supply of bitcoins (and that alone) that gives them 'intrinsic' value whereas supporters of other blockchains (such as Ethereum, Cardano, Polkadot) argue that utility of the network, its 'extrinsic' value, is far more important. From their perspective, the limited performance of blockchain networks, which to the Bitcoin network is a feature, in fact inhibits the usability of the network and therefore growth of value.

In the context of the Bitcoin blockchain, *digital scarcity* tends to refer to the limitation on the total supply of bitcoin. The single-minded focus on Bitcoin's supply is not without precedent. New bitcoins are created in a staggered process, intended to replicate the dynamics of gold — it is increasingly hard to find, and the total supply is limited. Media theorist Golumbia (2016) traces these ideas in Bitcoin via the Austrian school of economics to right-of-centre US monetary ideas (and hard right conspiracy theories) that view the governance of money supply with deep suspicion. This line of thought views the government's very purpose as being the theft of ordinary people's wealth by printing money and causing hyperinflation. The broader consensus however is that good monetary governance, rather than no governance, is key to addressing not only hyperinflation but also other economic concerns. The correlation of hyperinflation with money supply draws on the Quantity Theory of

Money (QTM). There are several real world examples of hyperinflation, from Zimbabwe (Ncube, 2019) to video games (Earle, 2013; Knowles et al., 2015, p. 248). But where proponents draw on QTM as a reason for absolute monetary and digital currency scarcity, critics — most notably of the school of Modern Monetary Theory, argue that money supply is not the main issue of concern, but rather how the supply is governed and what it is directed towards (Kelton, 2020).

Conclusion_

Digital scarcity describes a credibly maintained limitation, imposed through software, of digital information, goods or services that may be accessed and used entirely digitally. This includes limitations to entries in a ledger or database (including cryptocurrency entries in a blockchain or top-level domains in the Domain Name System), as well as limitations in access to computing resources such as network addresses, bandwidth, or (again in the context of blockchains) transactions-per-second, wherever these limits go beyond the physical limits imposed by hardware. The motivations for engineering digital scarcity tend to be in order to support business models that profit from scarcity or uniqueness in the digital realm.

Older usage of the term includes physical limitations in processing power and bandwidth, and limitations in physical access to computing devices and computing services. Since in such cases, scarcity is not imposed through software, it is included in the history of the term but not in the current definition.

References_

- Andersson, J. (2011). The origins and impacts of the Swedish file-sharing movement: A case study. *Critical Studies in Peer Production (CSPP)*, *1*(1), 1–18. http://urn.kb.se/resolve?urn=urn:nbn:se:sh:diva-22494
- Chaudhry, V., & Shipp, T. (2005). Rethinking the digital divide in relation to visual disability in India and the United States: Towards a paradigm of 'Information Inequity'. *Disability Studies Quarterly*, *25*(2). https://doi.org/10.18061/dsq.v25i2.553
- Earle, P. C. (2013). A Virtual Weimar: Hyperinflation in a Video Game World [Blog post]. *Mises Institute, Mises Daily Articles*. https://mises.org/library/virtual-weimar-hyperinflation-video-game-world

- Finley, K. (2020, May). The WIRED guide to net neutrality. *WIRED*. https://www.wired.com/story/guide-net-neutrality/
- Fortin, M. (2007). Digital Scarcity: Does It Still Convert? Personal Blog [Blog post]. *Michel Fortin's Blog*. https://web.archive.org/web/20071217220308/https://michelfortin.com/digital-scarcity-does-it-still-convert/
- Golumbia, D. (2016). *The politics of Bitcoin. Software as right-wing extremism.* University of Minnesota Press.
- Hammersley, B. (2003, July 10). Radio active revolution. *The Guardian*. https://www.theguardian.com/technology/2003/jul/10/onlinesupplement2
- Kelton, S. (2020). *The deficit myth, modern monetary theory and the birth of the people's economy*. John Murray.
- Knowles, I., Castronova, E., & Ross, T. (2015). Video games, virtual worlds and economics. In R. G. Picard & S. S. Wildman (Eds.), *Handbook on the Economics of the Media*. https://doi.org/10.4337/9780857938893.00018
- Liew, J. (2008, January 28). Three use cases for virtual goods [Blog post]. *Lightspeed Venture Capital Partners*. https://lsvp.wordpress.com/2008/01/28/three-use-cases-for-virtual-goods/
- Lotti, L. (2016). Contemporary art, capitalization and the blockchain: On the autonomy and automation of art's value. *Finance and Society*, *2*(2), 96. https://doi.org/10.2218/finsoc.v2i2.1724
- Masnik, M. (2006a). Economics of abundance getting some well deserved attention. In *Techdirt*. https://www.techdirt.com/articles/20061026/102329.shtml
- Masnik, M. (2006b). In a world where everything is digital, economics gets screwy fast. In *Techdirt*. https://www.techdirt.com/articles/20061114/181724.shtml
- Ncube, M. (2019, August 28). Introducing a new currency was Zimbabwe's only viable option. *Financial Times*. https://www.ft.com/content/f3e298c2-c8e7-11e9-a1f4-3669401ba76f
- O'Dwyer, R. (2019). Limited edition: Producing artificial scarcity for digital art on the blockchain and its implications for the cultural industries. November 20, 2018. *Convergence: The International Journal of Research into New Media Technologies*, *26*(4), 874–894. https://doi.org/10.1177/1354856518795097
- Oram, A. (Ed.). (2001). *Peer-to-peer: Harnessing the benefits of a disruptive technology* (1st ed.). O'Reilly.

- Perzanowski, A., & Schultz, J. (2016). *The end of ownership: Personal property in the digital economy*. MIT Press. https://doi.org/10.7551/mitpress/9780262035019.001.0001
- Resnikoff, P. (2007, August 8). Bronfman ponders digital scarcity, retreads strategy. *Digital Music News*. https://www.digitalmusicnews.com/2007/08/08/warner-2/
- Rodriguez, R. (2012, November). IPv4 scarcity [Blog post]. *Internet Society*. https://www.internetsociety.org/blog/2012/11/ipv4-scarcity/
- Roemer, R., Schear, N., Dahlstrom, D., & Farrington, N. (2006). *Piracy in the digital age*. University of Washington, Computer Science & Engineering. https://courses.cs.washington.edu/courses/csep590a/06au/projects/digital-piracy.pdf
- Serada, A., Sihvonen, T., & Harviainen, J. T. (2020). CryptoKitties and the new ludic economy: How blockchain introduces value, ownership, and scarcity in digital gaming. *Games and Culture*. https://doi.org/10.1177/1555412019898305
- See also conference proceedings: http://www.digra.org/digital-library/publications/cryptokitties-and-the-new-ludic-economy-how-blockchain-introduces-value-ownership-and-scarcity-in-the-digital-world/
- Smith, C. E. (2010). Net neutrality, full throttle: Regulation of broadband internet service following the Comcast/Bittorrent dispute. *Santa Clara Law Review*, *50*(2), 569–605. https://digitalcommons.law.scu.edu/lawreview/vol50/iss2/7/
- Swartz, A., & Lessig, L. (2016). *The boy who could change the world: The writings of Aaron Swartz*. Verso.
- Weinberger, D. (2003, March 13). The myth of interference. *Salon*. https://www.salon.com/2003/03/12/spectrum/
- Wikipedia contributors. (2021a). Sex.com. In *Wikipedia*. Wikimedia Foundation. https://en.wikipedia.org/w/index.php?title=Sex.com&oldid=1013006654#History
- Wikipedia contributors. (2021b). Spectrum auction. In *Wikipedia*. Wikimedia Foundation. https://en.wikipedia.org/w/index.php?title=Spectrum_auction&oldid=1015746929
- Wu, T. (2003). Network neutrality, broadband discrimination columbia law school scholarship archive. *Journal of Telecommunications and High Technology Law*, *2*, 141–179. https://scholarship.law.columbia.edu/faculty_scholarship/1281/

– Zeilinger, M. (2018). Digital art as "Monetised graphics": Enforcing intellectual property on the blockchain. *Philosophy & Technology*, *31*(1), 15–41. https://doi.org/10.1007/s13347-016-0243-1

Endnotes_

1. Meanwhile, in some cases centralised control does not guarantee the maintenance of digital scarcity either. This is evident not least from the Diablo 3 game: although the publisher — Blizzard Entertainment — nominally had complete control over all aspects of the game, they could not forestall runaway hyperinflation in the in-game economy (Mises, 2013).

DIGITALLY-DISADVANTAGED LANGUAGES_

Isabelle A. Zaugg, Institute for Comparative Literature and Society, Columbia University, New York City, United States.
Anushah Hossain, University of California Berkeley, United States.
Brendan Molloy, Independent researcher, Göteborg, Sweden.

Digitally-disadvantaged languages face multiple inequities in the digital sphere including gaps in digital support that obstruct access for speakers, poorly-designed digital tools that negatively affect the integrity of languages and writing systems, and unique vulnerabilities to surveillance harms for speaker communities. This term captures the acutely uneven digital playing field for speakers of the world's 7000+ languages.

Origin & evolution of the term_

The term originates with Mark Davis, president and co-founder of the Unicode Consortium, a nonprofit that maintains and publishes the Unicode Standard.[1] In 2015, Davis said, "The vast majority of the world's living languages, close to 98 percent, are 'digitally disadvantaged' — meaning they are not supported on the most popular devices, operating systems, browsers and mobile applications" (Unicode, 2015, n.p.). Computational linguist András Kornai (2013) similarly estimates that at most 5% of the 7000+ languages in use today will achieve "digital vitality," while the other 95% face "digital extinction". Gaps in language access are one facet of the *digital divide* (Zaugg, 2020).

Critical digital studies scholar and co-author Isabelle Zaugg utilises the term *digitally-disadvantaged languages* in her work on language justice in the digital sphere (2017; 2019a; 2019b; 2020; forthcoming). Zaugg (forthcoming) proposes that *digitally-disadvantaged language* communities face three primary challenges: 1) gaps in equitable access; 2) digital tools that negatively impact the integrity of their languages, scripts and writing systems,[2] and knowledge systems; and 3) vulnerability to harm through digital surveillance and under-moderation of language content.

Digitally-disadvantaged languages overlaps and extends upon adjacent terms used in geopolitics and computational linguistics, i.e., natural language processing (NLP). While the category of *digitally-disadvantaged languages* includes many if not all minoritised languages, Indigenous languages, oral languages, signed languages, and endangered languages, it also includes many national and widely-spoken languages that enjoy robust intergenerational transmission.[3] There is no sharp line that delineates whether a language is *digitally-disadvantaged.* Rather, the term captures a relative degree of disadvantage as compared to the handful of languages that enjoy the most comprehensive digital support and wider political advantages. That said, there are stark differences between the levels of support for languages such as English, Chinese, Spanish, and Arabic and even widely-spoken national and regional languages such as Amharic, Bulgarian, Tamil, Swahili, or Cebuano. However, *digitally-disadvantaged* is not a static state; it is possible for a language to "digitally ascend" (Kornai, 2013) through wide-reaching efforts to create digital support for the language and foster digital use among speakers. Cherokee, Amharic, Manding languages written in N'Ko, Fulani written in Adlam, and Sámi are a few languages whose digital ascent has been hastened by concerted advocacy efforts.

The term also overlaps with and contrasts against *low resource* or *under-resourced languages*, NLP terms that refer to languages with sparse data available for analysis. A language may be *digitally-disadvantaged* in part because digital corpora are unavailable to develop machine translation and search functions. Digital corpora often do not exist due to lack of basic digital support like fonts and keyboards that allow speakers to develop online content — a vicious cycle. By focusing on resource deficits, NLP terms shift focus away from how power has shaped the techno-social imbalances that have rendered the vast majority of languages *low resource* in the first place.

In contrast, the term *digitally-disadvantaged languages* captures how languages' digital marginalisation represents how wider linguistic power dynamics map onto the digital sphere. The fact that the earliest digital technologies were developed in the US and UK laid the foundation for English to become the best-supported and default means of digital communication in many contexts (Zaugg, 2017). Illustratively, the QWERTY Latin character layout remains the default keyboard all over the world, leading many to

write even well-supported languages like Arabic in a transliterated Latin form such as "Arabizi" (Zaugg, 2019a). The global spread of digital tools and systems including QWERTY keyboards, ASCII,[4] ICANN oversight of the originally Latin character-only domain name system,[5] and default English auto-correct have all contributed to the "logic" that English is the global *lingua franca*, and the Latin alphabet the most modern, rational, and universal script.[6] This "logic" in turn builds upon US and UK imperial power that laid the groundwork for the "digital revolution" as well as first brought English and the Latin script to far flung corners of the globe.

Digital advantage for English and the Latin script - and to a lesser degree other dominant languages and scripts - has created a paradigm in which many bilingual or multilingual speakers of *digitally-disadvantaged languages* become habituated to consuming and sharing content in a dominant "bully" language or script.[7] Many *digitally-disadvantaged language* speakers do not imagine that the digital sphere could be equally hospitable to their mother tongue and native script as it is to English and Latin (Benjamin, 2016). Unfortunately, gaps in digital support and use may be contributing to many of these languages' extinction as speakers increasingly use "bully" languages on and offline. Shockingly, 50-90% of language diversity is slated to be lost this century (Romaine, 2015); inequities in the digital sphere appear to be a factor in this shift (Kornai, 2013; Zaugg, 2017; Zaugg, 2019a; Zaugg, 2020).

The route out of *digitally-disadvantaged* status is "full stack support"[8] (Loomis, Pandey, and Zaugg, 2017). This term, used among technologists, designates comprehensive digital support for a language from basic levels like fonts and keyboards to sophisticated NLP tools. Achieving full stack support requires numerous steps, from documenting the language, submitting its script for inclusion in the Unicode Standard,[9] and designing fonts, to building input methods such as virtual keyboards (Loomis et al., 2017; *Indigenous Languages: Zero to Digital*, 2019). Text must be translated and interfaces localised so menu headers and dates follow the correct conventions. Advocates must lobby software vendors to include support for their language at the operating system and application levels.[10] High-level technical affordances require NLP research and include optical character recognition, spell-check, text-to-speech, and search capabilities. Developing full stack support can take years or decades, requiring the coordination of many stakeholders. Even under ideal conditions — a

large speaker community with a base of committed language advocates and technologists — challenges in reaching full stack support abound due to commercial, technical, and political hurdles.

Equitable access_

Equity, versus equality, acknowledges that each language community has unique circumstances and requires an allocation of resources and efforts to match, including potentially refusal of digital support. Issues with equitable access can fall anywhere on the "stack," from fonts to support on popular social media platforms. For example, while Indic scripts are encoded within the Unicode Standard, disproportionately few Indic fonts exist, due in part to the technical difficulty of engineering such fonts and the historically low commercial interest in Indian markets. Support by major software vendors has also followed political and commercial interests, from prioritising national and "commercially-viable" scripts in early editions of the Unicode Standard (Zaugg, 2017), to the targeting by software localization vendors of Europe and Japan through the late 20th century (Oo, 2018).

Even for languages where typographic access is not a barrier, a major issue is a lack of integration methods through a "digital re-colonization" supposedly driven by market conditions. Modern operating systems are becoming black boxes with limited extensibility and few supported languages. For example, Google's Chrome OS has no means to recognise languages beyond its pre-existing repertoire. For Sami students in Norway who are required to use Chrome OS laptops, a workaround had to be implemented to enable Sami keyboard access,[11] with no mechanism for enabling proofing tools. iOS and Android require manual maintenance of separate keyboard apps, with limited operating system integration. It is presently not possible to provide a high-quality user experience for *digitally-advantaged language* speakers on these platforms.

Many *digitally-disadvantaged language* communities include passionate advocates who have led grassroots efforts to develop fonts, keyboards, and word processing software for their languages and scripts (Zaugg, 2017; Zaugg, 2019a; Zaugg, 2020; Zaugg, forthcoming; Scannell, 2008; Bansal, 2021; Coffey, 2021; Kohari, 2021; Rosenberg, 2011; Wadell, 2016). The challenges of lobbying major software vendors for technical support have

led some communities to embrace free and open-source software instead (Bailey, 2016). User communities have created fonts using free tools like FontForge and libraries such as Pango and HarfBuzz. Virtual keyboards are created using KeyMan or kbdgen, and content translated using platforms such as Weblate or Pontoon. In the absence of high-quality support within operating systems, some have localised Linux desktops and applications. A suite of advanced NLP tools is also available as free and open-source software, enlarging possibilities for decentralised efforts by communities (Littauer, 2018).

Peer production can assist with reinvigorating *digitally-disadvantaged languages*. Organisations such as Divvun[12] provide open source tools to enable spell- and grammar checking, keyboard layouts and additional necessities for high-quality digital functionality for Sámi and other Uralic languages. Once baseline tools exist, organic communities arise to create content on Wikipedia, Twitter and other platforms. Non-profit and international efforts, such as the University of California, Berkeley's Script Encoding Initiative, and UNESCO projects such as those associated with the 2019 UN Declaration of the Year of Indigenous Languages,[13] are also working to widen access; but it is an uphill battle, as what constitutes"full stack support" grows with each new digital innovation.

Language and script integrity_

While some efforts to support *digitally-disadvantaged languages* are well-grounded, others are based on superficial knowledge of languages and writing systems (Zaugg, forthcoming). A virtual keyboard is only useful if it includes all the characters a language utilises, and ideally has a layout optimised for the most commonly used characters, etc. A well-designed font that incorporates calligraphic traditions can elevate a script's readability and status; a poorly designed font can signal its devaluation compared to font-rich scripts such as Latin (Leddy, 2018). Tools such as auto-correct, spell-check, and predictive typing can speed input, but can also degrade a language's orthography, honorifics, and patterns of respectful address if developed without appropriate care.

A significant trend within NLP is reliance on "big data" approaches to solve language access issues, such as generating text-to-speech engines or automatic translation. This exacerbates the disadvantage of *low-resource*

languages, as dominant languages receive better quality tools as the bulk of cultural discourse already exists in these languages. Optimistically, new approaches such as "transfer learning" may allow using higher-resourced languages to train models for lower-resourced languages. However, to avoid building linguistically-damaging or unwanted tools, computational linguists should commit to "decolonizing NLP" by only developing tools in partnership with and led by the interests of language communities (Bird, 2020).

Surveillance vulnerabilities_

Even when *digitally-disadvantaged languages* achieve a baseline of digital support, knock-on challenges remain. For example, social media platforms do not adequately moderate content in these languages (Zaugg, 2019b; Fick & Dave, 2019; Martin & Sinpeng, 2021; Marinescu, 2021). Facebook in particular has failed to moderate hate speech and fake news in *digitally-disadvantaged languages*, leading to real world harms across the globe (Adegoke & BBC Africa Eye, 2018; Stevenson, 2018; Taye & Pallero, 2020).

Given that *digitally-disadvantaged languages* have a smaller mass of digitised content, data mining puts these communities at higher risk relative to dominant languages. The smaller the corpus, the higher the chance that individual privacy of community members will be invaded. Finding the balance between technological solutions and social responsibility is challenging. Ensuring that users are not surveilled, while simultaneously improving language tool quality, requires consent-based measures significantly beyond those provided by laws and regulations like GDPR. Privacy-protections are critical for *digitally-disadvantaged language* communities; surveillance capitalism will likely lead to disproportionately negative outcomes in these communities, as many are uniquely vulnerable to state, NGO, and corporate harms (Zaugg, 2019b). For example, digital tools have been used to surveil the Rohingya in Myanmar and Bangladesh (Aziz, 2021; Ortega, 2021), while U.S. Customs and Border Protection surreptitiously collects migrants' cell phone conversations and social media posts, using them to inform asylum decisions at the US-Mexico border (Korkmaz, 2020).

Some *digitally-disadvantaged languages* are of "strategic interest" to governments, and tools such as machine translation are built through

military-intelligence funding to aid surveillance. Amandalynne Paullada (2021, n.p.) reminds us that a push for militarised surveillance is "precisely what fostered the development of machine translation technology in the mid-20th century" and its deployment today extends this tradition of "exerting power over subordinate groups." Efforts towards digital justice for *digitally-disadvantaged language* communities must balance the fact that increased digital support for a language also increases its speaker community's legibility to surveilling actors, benevolent or malevolent. These languages require design solutions that maintain data privacy, sovereignty,[14] and safety within the digital sphere.

Conclusion_

Digitally-disadvantaged languages face multiple inequities in the digital sphere, including gaps in digital support that obstruct access for speakers, poorly-designed digital tools that negatively affect the integrity of languages and writing systems, and unique vulnerabilities to surveillance harms for speaker communities. The term can bridge the work of a wide range of stakeholders who seek to study, discuss, and address language equity in the digital sphere, including scholars, NLP researchers, technologists, speaker communities, and language advocates.

References_

- Adegoke, Y. (2018, November 13). Like. Share. Kill. Nigerian police say "fake news" on Facebook is killing people. *BBC News*. https://www.bbc.co.uk/news/resources/idt-sh/nigeria_fake_news
- Aziz, A. (2021). A repertoire of everyday resistance and technological (in)security: Constructing the Rohingya diaspora and transnational identity politics on social media. *AoIR Selected Papers of Internet Research*. https:// spir.aoir.org/ojs/index.php/spir/article/view/11859/10248.
- Bailey, D. (2016). Software localization: Open Source as a major tool for digital multilingualism. In L. Vannini & H. L. Crosnier (Eds.), *Net.Lang: Towards the Multilingual Cyberspace*. https://unesdoc.unesco.org/ark:/48223/pf0000216692.
- Bansal, V. (2021). *Forget emoji, the real Unicode drama is over an endangered Indian script* [Report]. Rest of World. https://restofworld.org/2021/tulu-unicode-script/

- Benjamin, M. (2016, May 23). *Digital language diversity: Seeking the value proposition*. 2nd Workshop on Collaboration and Computing for Under-Resourced Languages, Portoroz, Slovenia. https://infoscience.epfl.ch/record/222525?ln=en
- Bird, S. (2020). Decolonising speech and language technology. *Proceedings of the 28th International Conference on Computational Linguistics*, 3504–3519. https://www.aclweb.org/anthology/2020.coling-main.313
- Coffey, D. (2021, April 28). Māori are trying to save their language from Big Tech. *WIRED*. https://www.wired.co.uk/article/maori-language-tech
- Fick, M., & Dave, P. (2019, April 23). Facebook's flood of languages leave it struggling to monitor content. *Reuters*. https://www.reuters.com/article/us-facebook-languages-insight-idUSKCN1RZ0DW
- Grubin, D. (2015, January 25). *Language Matters with Bob Holman*. David Grubin Productions Inc. and Pacific Islanders in Communications.
- *Indigenous languages: Zero to digital: A guide to bring your language online*. (2019). Translation Commons. https://drive.google.com/file/d/1JB6nXz6kpqcXfKaZR3VEYvrC9M2x7qOj/view.
- Kohari, A. (2021, February 9). *Meet the people fighting to keep a language alive online*. Rest of World. https://restofworld.org/2021/bringing-urdu-into-the-digital-age/
- Korkmaz, E. E. (2020, December 8). Refugees are at risk from dystopian "smart border" technology. *The Conversation*. https://theconversation.com/refugees-are-at-risk-from-dystopian-smart-border-technology-145500
- Kornai, A. (2013). Digital language death. *PLoS ONE*, *8*(10), e77056. https://doi.org/10.1371/journal.pone.0077056
- Leddy, M. (2018, May 29). Beyond "Graphic design is my Passion": Decolonizing Typography and Reclaiming Identity (II of II. *Explorations in Global Language Justice*. https://languagejustice.wordpress.com/2018/05/29/beyond-graphic-design-is-my-passion-decolonizing-typography-and-reclaiming-identity-ii-of-ii/
- Littauer, R. (2018). *Open source code and low resource languages* [Master's Thesis, Saarland University Department of Computational Linguistics]. https://raw.githubusercontent.com/RichardLitt/thesis/master/single-thesis.pdf
- Liu, L. H. (2015). Scripts in motion: Writing as Imperial technology, past and present. *PMLA*, *130*(2), 375–383.

- Loomis, S. R., Pandey, A., & Zaugg, I. (2017, June 6). Full Stack Language Enablement. *Steven R. Loomis*. https://srl295.github.io/2017/06/06/full-stack-enablement/
- Marinescu, D. (2021, September 8). Facebook's Content Moderation Language Barrier. *New America*. http://newamerica.org/the-thread/facebooks-content-moderation-language-barrier/
- Martin, F. R., & Sinpeng, A. (2021, July 5). Facebook's failure to pay attention to non-English languages is allowing hate speech to flourish. *The Conversation*. http://theconversation.com/facebooks-failure-to-pay-attention-to-non-english-languages-is-allowing-hate-speech-to-flourish-163723
- Oo, M. T. (2018, September 19). A brief history and evolution of IT localization. *Translation Royale*. https://www.translationroyale.com/history-of-it-localization/
- Ortega, A. (2021, March 23). Myanmar and the oppressive side of the digital revolution. *The Globalist*. https://www.theglobalist.com/myanmar-dictatorship-surveillance-technology/
- Paullada, A. (2021, July 31). Machine Translation Shifts Power. *The Gradient*. https://thegradient.pub/machine-translation-shifts-power/
- Romaine, S. (2015). The global extinction of languages and its consequences for cultural diversity. In H. F. Marten (Ed.), *Cultural and Linguistic Minorities in the Russian Federation and the European Union* (pp. 31–46). Springer International Publishing.
- Rosenberg, T. (2011, December 9). Everyone Speaks Text Message. *The New York Times Magazine*. http://www.nytimes.com/2011/12/11/magazine/everyone-speaks-text-message.html
- Rousseau, J.-J. (Ed.). (1986). *On the origin of language*. University of Chicago Press.
- Scannell, K. P. (2008). *Free software for Indigenous languages* [Thesis, Saint Louis University]. https://cs.slu.edu/~scannell/pub/ili.pdf
- Sinclair, K. (2021, June 16). The Twitch streamers fighting to keep minority languages alive. *The Verge*. https://www.theverge.com/2021/6/16/22533319/twitch-streamers-minority-languages-basque-gaelic
- Stevenson, A. (2018, November 6). Facebook Admits It Was Used to Incite Violence in Myanmar. *The New York Times*. https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html
- Taye, B., & Pallero, J. (2020, July 27). *Open letter to Facebook on violence-inciting speech: Act now to protect Ethiopians*. Access Now. https://www.accessnow.org/open-letter-to-facebook-protect-ethiopians/

- Unicode. (2015, December 16). Unicode launches adopt-a-character campaign to support the world's "digitally disadvantaged" living languages. *The Unicode Blog*. http://blog.unicode.org/2015/12/unicode-launches-adopt-character.html
- Wadell, K. (2016, November 16). The alphabet that will save a people from disappearing. *The Atlantic*.
- Zaugg, I. A. (2017). *Digitizing ethiopic: Coding for linguistic continuity in the face of digital extinction* [PhD dissertation, American University]. http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqm&rft_dat=xri:pqdiss:10599782
- Zaugg, I. A. (2019a). *Imagining a multilingual cyberspace*. Nesta. https://findingctrl.nesta.org.uk/imagining-a-multilingual-cyberspace/
- Zaugg, I. A. (2019b, December 4). Digital surveillance and digitally-disadvantaged language communities. *International Conference Language Technologies for All*. https://lt4all.elra.info/media/papers/O8/188.pdf
- Zaugg, I. A. (2020). Digital inequality and language diversity: An Ethiopic case study. In M. Ragnedda & A. Gladkova (Eds.), *Digital Inequalities in the Global South* (pp. 247–267). Springer International Publishing. https://doi.org/10.1007/978-3-030-32706-4_12
- Zaugg, I. A. (forthcoming). Global Language Justice: Ecology, Diversity, Digital Vitality. In L. H. Liu, A. Rao, C. A. Silverman (Eds.), *Lifeworld of Languages*. Columbia University Press.

Endnotes_

1. The Unicode Standard is a character coding system designed to support interoperable exchange and consistent representation of text in the world's writing systems on digital devices, providing a foundation for a multilingual digital sphere.
2. A language is a shared means of communication, while a script is the collection of written characters used to write a language. A language's writing system incorporates a script and a set of rules regarding its use. Languages and scripts do not have a one-to-one or static relationship. Some languages, such as Kazakh, Mongolian, and Urdu, are written in multiple scripts. Many languages share a script, although the rules of their writing systems may differ. More than 1000 languages are written in the Latin script, including English, French, Czech, Kazakh, Nahuatl, Tagalog, Vietnamese, and Igbo; Hindi, Nepali, Marathi, Bodi, and Konkani are

among languages written in the Devanagari script; Bulgarian, Kazakh, Russian, Tajik are written in the Cyrllic script; while Chinese, Korean, Japanese, Vietnamese, and Miao are written in the Hanzi script.

3. Marked by a high EGIDS score (Ethnologue, n.d.)

4. The American Standard Code for Information Interexchange, widely known as ASCII, assigned the Latin letters, numbers, and other characters common to American English to the 256 slots available in the 8-bit code. ASCII was the predominant character encoding standard pre-Unicode and is still used by many websites and devices today.

5. ICANN, or the Internet Corporation for Assigned Names and Numbers, is a U.S nonprofit and multi-stakeholder group that maintains the central repository for IP addresses and helps coordinate their supply while also managing the domain name system.

6. This digital "logic" perpetuates supremacist theories such as Jean-Jacques Rousseau's hypothesis in *On the Origin of Language* that "the depicting of objects is appropriate to a savage people; signs of words and of propositions, to a barbaric people; and the alphabet to civilised people" (1966, p. 17, as quoted in Lydia Liu, 2015, p. 380).

7. Poet Bob Holman calls dominant languages that push out mother tongues "bully" languages (Grubin, 2015).

8. "Full-stack support" is similar to Kornai's (2013) definition of "digital vitality," but the difference is that Kornai's definition encompasses both digital support and digital use. This is an important distinction because digital support does not necessarily lead to digital use of a language; long-standing lack of digital support may in fact incentivize bilingual/multilingual speakers to utilise a dominant, well-supported language for digital communication, such that these habits may be irreversible even if digital supports for their mother tongue later exist. In this context, it is possible for a language to be *digitally-disadvantaged* while also being well-supported.

9. Unicode inclusion itself often requires extensive historical research, documentation, and resolution of differences in character representation, etc. (Zaugg, 2017; Bansal, 2021).

10. Users on the popular streaming platform Twitch complained, for example, about the lack of Indigenous language tags available to help them find other members of their language communities, e.g. Basque and Gaelic (Sinclair, 2021). One example of lobbying working is Apple's attempts to support the *nastaʿlīq* script used to write Urdu (Kohari, 2021).

11. The workaround was to add the keyboard as a variant under the majority language, as well as to write the necessary operating system extension to implement the actual keyboard functionality as well (i.e., the ability for a key press to input the necessary key input).
12. <https://divvun.org>, funded by the Sámi Parliament of Norway
13. For example, see the International Conference Language Technologies for All (LT4All): Enabling Linguistic Diversity and Multilingualism Worldwide held in December 2019. Furthermore, the UN proclaimed 2022-2032 as the International Decade of Indigenous Languages (IDIL2022-2032), with UNESCO the lead organizer; expanding digital support for Indigenous languages will continue to be a focus.
14. For example, the Māori non-profit Te Hiku Media is working to build language tools for their community while keeping their annotated audio data, which can be used to develop automatic speech recognition and speech-to-text tools, out of the hands of corporate actors (Coffey, 2021).

INDEPENDENTLY-HOSTED WEB PUBLISHING_

Daniel Villar-Onrubia, Disruptive Media Learning Lab, Coventry University, United Kingdom.
Victoria I. Marín, University of Lleida, Spain.

Definition_

The term *independently-hosted* is used here to describe online publishing practices that utilise the World Wide Web (hereafter the Web) as a *decentralised* socio-technical system, where individuals and communities operate as the owners or controllers of the online infrastructures they use in order to share content. Such practices may be adopted as an alternative of, or as a complement to, the use of centralised content-sharing systems that belong to and are entirely operated by third parties. The term "publishing" is used here in a rather inclusive way and refers to the act of making content available online, rather than being restricted to the editorial processes that characterise, for instance, academic publishing.

It involves the use of server space, usually obtained from a web hosting provider, to create a static website or to install a content management system (CMS) such as WordPress.org in order to create a *self-hosted* site. On the contrary, a site that is not hosted independently could be exemplified by the use of a website builder entirely operated and controlled by a third party.

Origin and evolution_

Independently-hosted web publishing is part and parcel of the Web as an information sharing infrastructure, with the first website and web server established in 1990 (CERN, n.d.). While the Web was originally pitched as a solution to the problem of information loss at CERN, it was more generally envisioned as a system to help scientists share and access information from distributed locations across the world (Berners-Lee et al., 1994; Berners-Lee, 1990). It was very soon adopted in other contexts, permeating other realms of life quicker than any other information and communication technology had ever done before, resulting in an exponential growth of internet users that went from

less than 1% of the global population in 1990 to almost 50% in 2017 (International Telecommunication Union World Telecommunication, n.d.).

As revealed by Bory et al. (2016), throughout the decade of the 1990s, the discourse of the "founding fathers" of the web shifted from originally depicting their invention as: "a technological tool made by servers and based on existing data which could be useful for specialised users", to claiming that it was envisioned as "a new medium useful for all the people owning personal communication devices (computers) that would profit of a new living and global system of shared knowledge" (Bory et al., 2016, p. 1068-1069).

By the mid-1990s, the Web had already expanded well beyond academia. At that time, what the net artist and theorist Olia Lialina (2005) calls the "vernacular web" started to flourish when people, acting as amateur web designers, learnt to express themselves in the incipient online public sphere. In that context, long before social media was established as a concept, new forms of social networking emerged as websites connected to each other by means of hyperlinks, often listed as favourite links and sometimes forming circular clusters and virtual communities known as web-rings (Casey, 1998; Hess, 2007). While Geocities contributed to the rise of the vernacular web by enabling users, for the first time, to "create their own web pages without having to worry about the intimidating acronym soup of FTP, HTML, and the like" (Milligan, 2017, p. 137), much of that happened by means of independently-hosted websites and domain names purchased by their owners.

Issues currently associated with the term_

Over the last three decades the Web has experienced significant socio-technical changes, and beyond those shifts, a mythology of radical transformation embodied in the "discourse of versions" (Allen, 2013), from 1.0 to 2.0 and so on, has become widely accepted. However, the basic architectural principles underpinning the Web have remained fundamentally unchanged. As Kenneth Goldsmith, the founder of UbuWeb, a veteran website amassing avant-garde materials since 1996, reminds us:

"There's a commonly held idea that it is impossible to be independent on the web anymore…What we tend to forget is that the bedrock architecture of the web is the same as it was decades ago. Everything I did twenty years

ago on UbuWeb I still do today in an identical way, using the identical programmes, languages and tools. What was possible for UbuWeb in the beginning is still possible today" (Goldsmith, 2020, p. 22).

Openness and *decentralisation* are two core principles of that architecture. In April 1993 CERN put the key software components of the Web (the basic line-mode client, the basic server and the library of common code) in the Public Domain and a new version of the server software was released as Open Source in November 1994: "CERN would retain the copyright to protect the software from appropriation as well as to secure attribution, but would grant to anyone the perpetual and irrevocable right to use and modify it, freely and at no cost" (Smith & Flückiger, n.d.).

Beyond software licensing, openness is a broad concept often used to characterise other aspects of the Web. In this regard, the term 'Open Web' highlights both the practices and technical dimensions of the Web that make it operate as a global public resource "by and for *all* its users, not select gatekeepers or governments" (Surman, 2017). As a set of normative principles or values, it advocates for a Web that is accessible to as many people as possible and ensures interoperability, as opposed to practices and platforms that delimit access by establishing siloed systems (Behrenshausen, 2017).

High levels of decentralisation, aspiring to yield a distributed network topology (Bodò et al. 2021), were key to ensuring that anyone with access to the Web could start using it (e.g. to publish content online) without having to seek permission from a gatekeeper (Berners-Lee, 1999). However, centralisation dynamics have been increasingly defining both the Web and the internet for a while now, materialising as a handful of disproportionally large actors and sites that attract most of the attention and have the power to influence online visibility (Benkler, 2006; World Wide Web Foundation, 2018). At the same time, many of those big players operate much like walled gardens, rather than following the principles of the Open Web.

Even though anyone with access to a networked computer – firewalls permitting – can still access information, share content and collaborate across boundaries beyond those walled gardens, in the current online landscape we often do these things through centralised, private, closed

platforms built on top of the Web (e.g. most social media platforms), rather than working with open online infrastructures owned or controlled by ourselves (e.g. independently-hosted web publishing).

Several concepts, practices, technologies and communities have emerged to challenge the increasingly centralised topology of the modern Web. This has happened through imagining, materialising and promoting alternative – or at least complementary – ways of inhabiting the Web that do not rely primarily on private online infrastructures.

For web publishing in particular, centralisation trends mean that users tend to rely on platforms that are heavily controlled by others. Companies offering web publishing platforms usually work with proprietary systems with limited interoperability by design, meaning that it is not easy for users, or at all possible, to migrate a site to another system.

We propose 'independently-hosted web publishing' as a term that can appropriately describe "affirmative disruption" (Hall, 2016) in relation to practices enabling a diverse range of individuals, collectives and initiatives to adopt alternatives to centralised modes of sharing content online. As it is not an established term within neither the academic literature nor common parlance, in the next section we discuss some related concepts and systems that may involve independently-hosted web publishing.

Related concepts_

Media practices involving information and communication infrastructures established or controlled by users and grassroot communities, instead of third parties (whether the state or commercial entities), are far from new. Indeed, they predate both the Web and the internet. In this regard, by mobilising such alternative infrastructures, *emancipatory communication* seeks "to circumvent the politics of enclosure and control enacted by states, regulators, and corporations" (Milan, 2019 , p. 1). Classic examples span across analogue and digital media, from print media and pirate radio stations to activist web-based initiatives, such as the Independent Media Center (Indymedia) network of grassroot journalism made of local groups around the globe (Pickard, 2016).

Autonomy, as in autonomous media (Langlois & Dubois, 2005), is another relevant term to describe practices based on the creation and use of information and communication technologies that are independent from dominant institutions. Likewise, Temporary Autonomous Zones (TAZ) was a highly influential concept within the cyberculture and net art scenes of the 1990s (Sastre, 2020; Sellars, 2010).

The increasingly centralised topology of the Web has been met with calls for alternatives that enable some level of autonomy from hegemonic online infrastructures. The idea of *Public Service Internet* platforms is one of those alternatives, where "users manage their data, download and re-use their self-curated data for reuse on other platforms [… which] minimise and decentralise data storage and have no need to monetise and monitor Internet use" (Fuchs & Unterberger, 2021, p. 13).

Likewise, free and open source communities have developed a number of federated and decentralised social networking and content-sharing systems, such as Diaspora, Hubzilla, Peertube or Pixelfed. One of the most prominent examples is Mastodon, positioned as an alternative to Twitter that allows communities to host an instance of the software in servers they control while still allowing interaction across instances thanks to its federated nature (Raman et al., 2019; Zulli et al., 2020). The fact of not being driven by profit-generation, while being sustained by voluntary contributions from their communities – instead of selling targeted advertisement or relying on venture capital investments – takes personal data collection out of the equation. At the same time, the decentralised and open source nature of these systems, where anyone can host an instance, may protect their communities from the kinds of losses experienced by users of the many commercial platforms that have gone out of business over the last decades (e.g. Geocities, Wikispaces or Google + to name just a few).

In this context, establishing an independently-hosted web domain can be understood as another way for individuals, and collectives, to gain more agency and control over their online presence and to enhance their autonomy from centralising forces. That is the premise of the *IndieWeb* movement (Finley, 2013; Gillmor, 2014), initiated in 2011 as a "people-focused alternative to the *corporate web*" and "based on the principles of owning your domain, using it as your primary identity, to publish (sic)

on your own site (optionally syndicate elsewhere), and own your data" (IndieWeb, 2021).

The IndieWeb effectively advocates for independently-hosted web publishing as opposed to relying on web building platforms such as Google Sites, SquareSpace, Tumblr, Wix or even WordPress.com – just to mention a few services that are active these days, but the same logic would apply to platforms that were popular in the past and are not longer operating, such as Geocities or Posterous.

Beyond proposing a new label for what can be regarded as relatively old practices, the IndieWeb community supports the integration of independently-hosted websites with the siloed platforms that make up the social media ecosystem, developing technologies that enable "the practice of posting content on your own site first, then publishing copies or sharing links to third parties (like social media silos) with original post links to provide viewers a path to directly interacting with your content" (IndieWeb, 2021).

In the realm of education, other terms have been proposed to advocate for the adoption of similar practices with the aim of enhancing digital competence and autonomy. For example, Campbell talks about *personal cyberinfrastructures* when he suggests providing students with hosting space and their own domain as soon as they start their studies:

Suppose that when students matriculate, they are assigned their own web servers […] As part of the first-year orientation, each student would pick a domain name […] students would build out their digital presences in an environment made of the medium of the web itself. […] In short, students would build a personal cyberinfrastructure — one they would continue to modify and extend throughout their college career — and beyond. (Campbell, 2013, p. 101–102)

These are also the ideas underpinning the concept of a *Domain of One's Own* (Udell, 2012; Watters, 2016a). Inspired by Virginia Woolf's claim that the independence enabled by a private room is one of the essential material conditions required for being an author (Woolf, 1931), similar thinking was applied to life in the digital age when coining this phrase to refer to "the practice of giving students, faculty, and staff the opportunity

to obtain a domain with hosted web space of their own" (Groom et al., 2019). Therefore, the word *domain* in that phrase does not refer to just domain names, as independently-hosted web publishing is also inherent to the concept. The premise is that it may "empower teachers and students to engage in digital literacies while maintaining ownership over their digital identities" (O'Byrne & Pytash, 2017, p. 499).

Also within academia, it is worth noting a number of open source software development initiatives that enable scholars and institutions to adopt independently-hosted (academic) web publishing practices. Projects like the Open Journal System, Manifold or Scalar are based on a distributed model that allow anyone to download and deploy the software (Maxwell et al., 2019), offering an alternative to the commercial entities that dominate the scholarly communication ecosystem.

Conceptual limitations_

Ownership and decentralisation are key aspects to the notion of independently-hosted web publishing and the related terms discussed above. However, the accuracy of both properties might be questioned due to the fact that in most cases such websites actually live in facilities that are still operated by third parties, usually not even in the infrastructures of the hosting providers contracted by the websites' owners but in data centres that belong to other companies, which might well be one of those big players responsible for the centralising trends that define the Web these days (e.g. Amazon). Likewise, domain names are not actually bought in perpetuity, but leased over a period of time, so at best they can be conceived as temporary (whether more or less durable), rather than permanent, autonomous zones.

Addressing some of these points, Watters (2016b) argued that the idea of *owning* a domain and hosting space should be understood in the context of a post-ownership and subscription economy. Instead of the legal implications of ownership associated with the notion of *property*, she argues that in this context the verb *to own* should be interpreted as "to have authority and control". After all, even if it is the kind of control that comes with *lease* instead of property, it offers a higher degree of ownership and autonomy than online infrastructures completely governed by third parties.

Conclusion_

Independently-hosted web publishing practices entail the use of websites made available online through infrastructures that – despite being usually outsourced to a hosting provider – are largely controlled by the website's owners, allowing them to make substantial architectural decisions. Most importantly, they can seamlessly transfer their activity to alternative infrastructures at any time. This usually involves owning a domain name too and its independence from fixed infrastructures enables decentralised forms of communication, by not requiring them to rely on the platforms that dominate content sharing in the modern Web. The term *independent* is considered more appropriate than *self*, as in self-hosted, considering the latter can give the wrong impression that it only refers to situations where the owners of a website decided to physically host it on hardware that is physically controlled and managed by them.

References_

- Behrenshausen, B. (2017). *What is the open web?* Year of Open https://web.archive.org/web/20220107102856/https://www.yearofopen.org /november-open-perspective -what-is-open-web/what-is-the-open-web -bryan-behrenshausen-writer-and-editor-red-hat/
- Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.
- Berners-Lee, T. (1990). *Information Management: A Proposal*. C.E.R.N. http://cds.cern.ch/record/369245/files/dd-89-001.pdf
- Berners-Lee, T. (1999). *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor* (1st ed). HarperSanFrancisco.
- Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H. F., & Secret, A. (1994). The World-Wide Web. *Communications of the ACM*, *37*(8), 76–82. https://doi.org/10.1145/179606.179671
- Bodó, B., Brekke, J. K., & Hoepman, J.-H. (2021). Decentralisation: A multidisciplinary perspective. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1563
- Bory, P., Benecchi, E., & Balbi, G. (2016). How the Web was told: Continuity and change in the founding fathers' narratives on the origins of the World Wide Web. *New Media & Society*, *18*(7), 1066–1087. https://doi.org/10.1177/1461444816643788
- Campbell, G. (2013). A Personal Cyberinfrastructure. In D. J. Cohen

& T. Scheinfeldt (Eds.), *Hacking the Academy: New Approaches to Scholarship and Teaching from Digital Humanities* (pp. 100–103). University of Michigan Press. https://doi.org/10.2307/j.ctv65swj3

- Casey, C. (1998). Web rings: An alternative to search engines. *College & Research Libraries News*, *59*(10), 761–763. https://doi.org/10.5860/crln.59.10.761
- CERN. (n.d.). *A short history of the Web*. CERN. https://web.archive.org/web/20190330111012/https://home.cern/science/computing/birth-web/short-history-web
- Cohen, D. J., & Scheinfeldt, T. (Eds.) (2013). *Hacking the Academy: New Approaches to Scholarship and Teaching from Digital Humanities*. University of Michigan Press. https://doi.org/10.2307/j.ctv65swj3
- Finley, K. (2013). Meet the hackers who want to jailbreak the Internet. *WIRED*. https://www.wired.com/2013/08/indie-web/
- Fuchs, C., & Unterberger, K. (Eds.) (2021). *The Public Service Media and Public Service Internet Manifesto*. University of Westminster Press. https://doi.org/10.16997/book60
- Gillmor, D. (2014, April 25). Welcome to the Indie web movement. *Slate Magazine*. https://slate.com/technology/2014/04/indiewebcamps-create-tools-for-a-new-internet.html
- Goldsmith, K. (2020). *Duchamp Is My Lawyer: The Polemics, Pragmatics, and Poetics of UbuWeb*. Columbia University Press.
- Groom, J., Taub-Pervizpour, L., Richard, S., Long-Wheeler, K., & Burtis, M. (2019). *7 things you should know about a domain of one's own* [Report]. https://library.educause.edu/resources/2019/10/7-things-you-should-know-about-a-domain-of-ones-own
- Hall, G. (2016). *The Uberfication of the University*. University of Minnesota Press.
- Hess, A. (2007). In digital remembrance: Vernacular memory and the rhetorical construction of web memorials. *Media, Culture & Society*, *29*(5), 812–830. https://doi.org/10.1177/0163443707080539
- IndieWeb. (2021a). *POSSE*. IndieWeb. https://web.archive.org/web/20210908045307/https://indieweb.org/POSSE
- IndieWeb. (2021b). *What is the IndieWeb?* IndieWeb. https://web.archive.org/web/20210909125917/https://indieweb.org/
- International Telecommunication Union (ITU) World Telecommunication. (n.d.). *Individuals using the Internet (% of population) — ICT Indicators Database*. The World Bank. https: //data.worldbank.org/indicator/IT.NET.USER ZS?end=2019&start=1990&view=

chart&year=2020
- Langlois, A., & Dubois, F. (Eds.). (2005). *Autonomous Media: Activating Resistance & Dissent*. Cumulus Press.
- Lialina, O. (2005). The vernacular web. *A Minima*, *11*, 158–187.
- Maxwell, J. W., Hanson, E., Desai, L., Tiampo, C., O'Donnell, K., Ketheeswaran, A., Sun, M., Walter, E., & Michelle, E. (2019). *Mind the Gap: A Landscape Analysis of Open Source Publishing Tools and Platforms* (1st ed.). PubPub. https://doi.org/10.21428/6bc8b38c.2e2f6c3f
- Milan, S. (2019). Emancipatory Communication. In R. Hobbs & P. Mihailidis (Eds.), *The International Encyclopedia of Media Literacy* (1st ed., p. 1–6). Wiley. https://doi.org/10.1002/9781118978238.ieml0062
- Milligan, I. (2017). Welcome to the web: The online community of GeoCities. In N. Brügger (Ed.), *The Web as History*. UCL Press. https://doi.org/10.14324/111.9781911307563
- O'Byrne, W. I., & Pytash, K. E. (2017). Becoming literate digitally in a digitally literate environment of their own. *Journal of Adolescent & Adult Literacy*, *60*(5), 499–504. https://doi.org/10.1002/jaal.595
- Pickard, V. W. (2006). United yet autonomous: Indymedia and the struggle to sustain a radical democratic network. *Media, Culture & Society*, *28*(3), 315–336. https://doi.org/10.1177/0163443706061685
- Raman, A., Joglekar, S., Cristofaro, E. D., Sastry, N., & Tyson, G. (2019). Challenges in the decentralised web: The Mastodon case. *Proceedings of the Internet Measurement Conference*, 217–229. https://doi.org/10.1145/3355369.3355572
- Sastre, P. (Ed.). (2020). *Manifiestos sobre el arte y la red, 1990-1999*. Exit Publicaciones.
- Sellars, S. (2010). Hakim Bey: Repopulating the temporary autonomous zone. *Journal for the Study of Radicalism*, *4*(2), 83–108. https://www.jstor.org/stable/41887659
- Smith, T., & Flückiger, F. (n.d.). *Licensing the Web for everyone*. CERN. https://web.archive.org/web/20190330110617/https://home.cern/science/computing/birth-web/licensing-web
- Surman, M. (2017). *What is the open web and why is it important?* Year of Open. https://web.archive.org/web/20220107103127/https://www.yearofopen.org/november-open-perspective-what-is-open-web/what-is-the-open-web-and-why-is-it-important-submitted-by-mark-surman-executive-director-of-the-mozilla-foundation/
- Udell, J. (2012). A Domain of One's Own. *WIRED*. https://www.wired.com/insights/2012/07/a-domain-of-ones-own/

- Watters, A. (2016a). *A domain of one's own in a post-ownership society*. Hacked Education. https://web.archive.org/web/20190521155252/http://hackeducation.com/2016/08/23/domains
- Watters, A. (2016b). *Claim Your Domain and Own Your Online Presence*. Solution Tree Press.
- Woolf, V. (1931). *A Room of One's Own*. Hogarth Press.
- World Wide Web Foundation. (2018). *The case #ForTheWeb* [Report]. World Wide Web Foundation. http://webfoundation.org/docs/2018/11/The-Case-For-The-Web-Report.pdf
- Zulli, D., Liu, M., & Gehl, R. (2020). Rethinking the "social" in "social media": Insights into topology, abstraction, and scale on the Mastodon social network. *New Media & Society*, *22*(7), 1188–1205. https://doi.org/10.1177/1461444820912533

MINING_

Wassim Zuhair Alsindi, Media Lab,
Massachusetts Institute of Technology,
United States.
Laura Lotti, Independent, Berlin, Germany.

In the context of blockchain networks, mining describes a permissionless process intended to ensure the global consistency of a decentralised ledger. Mining requires the consumption of a costly computational resource to participate in a probabilistic competition that confers specific privileges to a node. These privileges typically relate to the proposal of a new block, including the identity and order of transactions contained within. Mining is incentivised via an algorithmically regulated provision of rewards, usually in the form of newly generated coins and/or transaction fees.

Origin_

Cryptocurrency mining was initially understood to refer to processes incorporating proof-of-work (PoW) (i.e., the spending of costly computational resources such as central processing unit (CPU) cycles via a mechanism originally developed to mitigate spam) (Dwork & Naor, 1992; Back, 2002). PoW is usually a permissionless process (i.e., anyone can partake) with miners' identities unknown (anonymous/pseudonymous). Precursor digital money projects such as Bit Gold and b-money (Szabo, 2005; Dai, 1998) proposed the use of PoW-type mechanisms to avoid resource exhaustion and message flooding attacks or Sybil attacks from large numbers of dishonest *sockpuppet* nodes (Douceur, 2002).

While the Bitcoin Whitepaper (Nakamoto, 2008a) did not refer to PoW explicitly as mining, reference was made to the gold mining analogy. The term was used colloquially in online forums and chatrooms including BitcoinTalk and IRC (Internet Relay Chat, a long-running instant messaging protocol) as far back as 2010. Indeed, the source code of the first version of the Bitcoin software referred to the process of generating coins as mining (Nakamoto, 2009).

The chain selection heuristic which uses PoW to ensure the eventual network-wide consistency of the Bitcoin ledger is referred to as Nakamoto

Consensus. This requires a 51% majority of "work" to reach agreement on the latest valid block and a *"guarantee that all honest parties output the same sequence of blocks throughout the execution of the protocol"* (Kiffer et al., 2018, p. 1). Blockchains grow in height incrementally as new candidate blocks are constructed by miners and added to the canonical chain. In PoW-based networks this takes place through the combination of nonces (i.e., an arbitrary variable which is progressively iterated) with the proposed block header to generate hashes which are then compared against the network-determined difficulty of finding a block. The miner chooses the identity and order of transactions contained within a proposed candidate block and this has potential economic implications including front-running and re-ordering of transactions (Daian et al., 2019).

The mining process is mediated by a *difficulty adjustment* feedback mechanism, which periodically recalibrates the effective probability of finding a valid block so as to maintain the network's target inter-block times. Should the hash of a candidate block be found that satisfies the network's difficulty requirements, the miner will announce it to the network and fellow network participants will confirm the validity of the block. Within the block, the miner may claim a so-called *mining subsidy* or *block reward* by including a transaction payable to themselves, in addition to any mining fees paid by transactions included.

The key cryptographic component of Bitcoin mining is the SHA-256 hash puzzle. Hashing refers to a one-way deterministic process that converts an input of arbitrary length to one of fixed length. An ideal cryptocurrency hashing algorithm must have the following properties (Narayanan a& Clark, 2017): (i) it is difficult to compute so that shortcuts or undue advantages are not available to participants; (ii) cost is parameterisable so that the energetic expenditure required to mine a valid block is not fixed over time; and (iii) it is trivially easy to verify the correctness of the hashed output from the input material. Since cryptographic hash functions are deterministic (i.e., given a fixed block with a fixed nonce — and a broad subset of possible hash values satisfying the difficulty requirements exist), it is entirely plausible that more than one valid candidate block may be found by competing miners at very similar times. In such an eventuality there begins a block propagation competition *per se* which allows the network to reach agreement on the latest state of the transaction ledger.

The class of hashing algorithms used in cryptocurrency mining today are considered to be potentially vulnerable to cryptographic attacks by quantum computers, resulting from the ability of quantum systems to search possibility spaces more efficiently than their classical counterparts. Increasingly sophisticated hardware and algorithms such as Shor's (1994) and Grover's (1996) collectively threaten the integrity of key mathematical assumptions for public-key cryptography such as the hardness of integer factorisation problem, the discrete logarithm problem and the elliptic-curve discrete logarithm problem. Quantum-resistant cryptographic schemes have already been proposed for Bitcoin (Ruffing, 2019), however these would require contentious protocol upgrades.

Since there can only be one block with a particular height in a blockchain, should multiple candidates emerge the prospect of a persistent network partition known as a *fork* arises if subsets of the population of validating nodes do not overwhelmingly agree on the latest block. Such partitions may be short-lived in the case of *stale blocks* such as "orphans" and "uncles" (terms used with respect to Bitcoin and Ethereum mining respectively)[1] which represent discarded timelines as the canonical chain built upon another candidate block. In other cases, a fork can happen due to a malicious attack, such as a "51% attack" — when a nefarious actor manages to take control of the majority of hashing power and is able to modify the order of transactions or reverse the transactions that they themselves made, leading to double-spending (i.e., spending the same digital coins twice).

Combining these various elements, we can take the original meaning of cryptocurrency mining to be a *thermoeconomic*[2] process employing PoW and a parameterisable feedback mechanism (difficulty adjustment) with direct incentives provided by block rewards from an algorithmically regulated network-level issuance schedule alongside transaction fees.

Evolution_

Since Bitcoin's PoW, the range of activities falling under the nominal banner of mining has broadened substantially over time.

A number of alternative PoW strategies have emerged in recent years, at first hypothetical and subsequently observed in the wild, which afford

favourable game-theoretic outcomes by deviating from *honest* mining behaviour as originally intended by the Bitcoin protocol (Eyal & Sirer, 2018, Grunspan & Pérez-Marco, 2018). *Selfish mining*, also known as block withholding, may be conducted by a miner who finds a valid block but instead of immediately broadcasting to peers, the block is withheld and kept secret. The miner then begins to search for a valid block atop the previous clandestine block, with the aim of finding a valid second block (and then announcing the first secret block) before another participant finds an alternative valid first block. It has been claimed that this adversarial strategy is more beneficial than honest mining for a sufficiently well-resourced miner.

With the development of the field, the processes at the core of decentralised consensus have become unbundled and abstracted from the materiality of computational work, while at the same time capital and other exogenous resources have become more integrated. One popular approach to this virtualisation of work is *staking*, which involves locking (i.e., rendering illiquid) some form of collateral in a protocol and being rewarded for participating in network consensus proportionally to the amount staked. Since it extends and further virtualises the novelty of Bitcoin's consensus model, staking via proof-of-stake (PoS) has also been called "generalised mining" or "mining 2.0" (Brukhman, 2018). In fact, staking was initially proposed as a less computationally-intensive alternative to PoW to prevent double-spending in base layer chains such as Ethereum (King & Nadal, 2012), but the model has found broad application in 'layer-2' cryptoeconomic protocols (Brekke & Alsindi, 2021), made possible by smart contracts. An area in which staking has found significant application in layer-2 protocols is *Decentralised Finance* (DeFi), in which *liquidity mining* is currently (at the time of writing) a popular term used to describe the incentivised provision of collateral and liquidity for the most disparate financial activities: lending, borrowing, insurance, synthetic derivatives, and governance over the risk parameters of a decentralised bank.

Issues currently associated with the term_

Critiques of the mining metaphor_

The analogy between PoW-secured digital currency and gold has been widely discussed. In general it echoes the desirable commodity money characteristics prized by adherents to modern libertarian ideals or the Austrian School of Economics (Alsindi, 2019), among which is Szabo's

concept of *unforgeable costliness* (Szabo, 2008) relating to the inelasticity of supply of Bitcoin (and most subsequent PoW cryptocurrencies). The strict resource scarcity that arises from Bitcoin's algorithmically regulated issuance schedule and the analogy with gold mining have become expressions of the *digital metallism* that characterises Bitcoin's discourse (Maurer et al., 2013).

Swartz (2018) further differentiates between *digital metallism* and *infrastructural mutualism*, that is, two techno-economic imaginaries stemming from the cryptoanarcho-libertarian and cypherpunk subcultures, respectively. Here mining, and the diverse meanings that emerged around this misnomer, illustrate the tensions between these two positions, which ultimately led to an ideological fork of the Bitcoin network in mid-2017: *"Digital metallists understood the act of mining as an opportunity to extract the greatest amount of Bitcoins to be used as a store of speculative value, whereas infrastructural mutualists saw mining as an act of collaboration to produce a shared privacy-protecting payment network*" (Swartz, 2018, p. 12).

These divergent ideologies profoundly influenced the development of the blockchain ecosystem beyond Bitcoin. Here we could argue that Satoshi Nakamoto and Hal Finney were much more in line with the infrastructural mutualism vision; early message logs exist where the two earliest known Bitcoin network participants were hopeful that solely altruistic behaviour could be encouraged as a community ethos (Nakamoto, 2008b). However, at the core of the process of mining is neither the minting of new coins, nor the access to decentralised economic flows *per se*, but the assurance of settlement through decentralised consensus (Antonopolous, 2018; Carter, 2019). In Bitcoin and other PoW chains, this assurance comes from the distribution of the computational power used to search for blocks, whereas in staking protocols it is a matter of economic distribution so that, in principle, no single actor is able to accumulate more than 51% of the *proving resource* (i.e., hashrate for PoW and token supply for PoS).

Ecological and thermodynamic critiques_

As the term mining is now used to describe cryptoeconomic processes as well as thermoeconomic ones, the previously strained analogy now appears to be a pure simulacrum (Baudrillard, 1981). PoW mining is by necessity an energetically costly process, consisting of irreversible computation

(Landuaer, 1961). At the time of writing, Bitcoin electricity consumption is estimated to be over 120 TWh per year, approximately equivalent to that of Norway or Pakistan (Cambridge Centre for Alternative Finance, 2021). Proofs-of-useful-work such as those used in cryptocurrencies such as Primecoin (King, 2013) have been proposed as more eco-friendly alternatives to Bitcoin-type PoW. In reality, useful work may not reduce the overall thermodynamic footprint of a cryptocurrency, as the effective worth of the useful work may simply be treated as a universal discount by all mining participants (Sztorc, 2015).

It has been proposed that Bitcoin liberates stranded, illiquid energy and the majority of PoW mining employs renewable energy from geothermal and hydroelectric sources far from population centres (Bendiksen & Gibbons, 2019). However, the insensitivity of PoW cryptocurrencies to the energy sources used to secure them has led to criticism as to their inability to mitigate their ecological externalities. PoS systems are less resource-intensive but, by replacing a real (costly) resource with a virtual one, they become vulnerable to attack vectors leveraging costless simulation (i.e., "nothing-at-stake") of alternative malicious ledger timelines such as long-range attacks (Brown-Cohen et al., 2018).

Conclusion_

In the context of blockchain networks, *mining* describes a permissionless process intended to ensure the global consistency of a decentralised ledger. Mining requires the consumption of a costly computational resource to participate in a probabilistic competition that confers specific privileges to a node. These privileges typically relate to the proposal of a new block, including the identity and order of transactions contained within. It is incentivised via an algorithmically regulated provision of rewards, usually in the form of newly generated coins and/or transaction fees. Initially understood to refer to processes incorporating PoW, over time the term mining has come to describe a wider array of mechanisms for achieving peer-to-peer consensus. One such "generalised mining" method is staking some form of collateral in a protocol and being rewarded for participating in network consensus. As more blockchains are adopting PoS and the term is used to describe cryptoeconomic processes as well as thermoeconomic ones, the original "gold mining" analogy has become increasingly exhausted.

Acknowledgements_

The authors would like to thank Yuval Kogman, Anil Bawa-Cavia and Sam Hart for helpful feedback during the preparation of this article.

References_

–
– Alsindi, W. Z. (2019). *TokenSpace: A Conceptual Framework for Cryptographic Asset Taxonomies*. Parallel Industries. https://doi.org/10.21428/0004054f.ccff3c19
– Antonopolous, A. (2018). The Bitcoin Network. In *Mastering Bitcoin* (2nd ed.). https://github.com/bitcoinbook/bitcoinbook
– Back, A. (2002). *Hashcash — A denial of service counter measure*. http://www.hashcash.org/papers/hashcash.pdf.
– Baudrillard, J. (1981). *Simulacra et Simulation*. Éditions Galilée.
– Bendiksen, C., & Gibbons, S. (2019). *The Bitcoin Mining Network: Trends, Average Creation Costs, Electricity Consumption & Sources* [White Paper]. CoinShares Research. https://coinshares.com/research/bitcoin-mining-network-december-2019
– Brekke, J. K., & Alsindi, W. Z. (2021). Cryptoeconomics. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1553
– Brown-Cohen, J., Narayanan, A., Psomas, C., & Weinberg, S. M. (2018). Formal Barriers to Longest-Chain Proof-of-Stake Protocols. *ArXiv*. https://arxiv.org/abs/1809.06528
– Brukhman, J. (2018, October 30). *Generalized Mining and the Third-Party Economy: An Introduction & Primer* [Talk]. Prague Blockchain Week, Prague. https://youtu.be/ceex9CN2YZU
– Cambridge Centre for Alternative Finance. (2021). *Cambridge Bitcoin Electricity Consumption Index*. University of Cambridge, Judge Business School, Cambridge Centre for Alternative Finance. https://www.cbeci.org/
– Carter, N. (2019). It's the settlement assurances, stupid! [Blog post]. *Medium, Nic Carter*. https://medium.com/@nic__carter/its-the-settlement-assurances-stupid-5dcd1c3f4e41
– Dai, W. (1998). *B-money*. Wei Dai. http://www.weidai.com/bmoney.txt
– Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. *2020 IEEE Symposium on Security and Privacy (SP)*, 910–927.

https://doi.org/10.1109/SP40000.2020.00040
- Douceur, J. R. (2002). The Sybil Attack. In P. Druschel, F. Kaashoek, & A. Rowstron (Eds.), *Peer-to-Peer Systems* (pp. 251–260). Springer. https://doi.org/10.1007/3-540-45748-8_24
- Dwork, C., & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. In E. F. Brickell (Ed.), *Advances in Cryptology — CRYPTO' 92* (pp. 139–147). Springer. https://doi.org/10.1007/3-540-48071-4_10
- Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), 95–102. https://doi.org/10.1145/3212998
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing*, 212–219. https://doi.org/10.1145/237814.237866
- Grunspan, C., & Pérez-Marco, R. (2018). On profitability of selfish mining. *ArXiv*. https://arxiv.org/abs/1805.08281
- Kiffer, L., Rajaraman, R., & Shelat, A. (2018). A Better Method to Analyze Blockchain Consistency. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18*, 729–744. https://doi.org/10.1145/3243734.3243814
- King, S. (2013). *Primecoin: Cryptocurrency with Prime Number Proof-of-Work* [White Paper]. Primecoin. https://primecoin.io/bin/primecoin-paper.pdf
- King, S., & Nadal, S. (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* [White Paper]. Peercoin.
- Landauer, D. (1961). Irreversibility and Heat Generation in the Computing Process. *IBM Journal*, *5*(3), 183–191. https://doi.org/10.1147/rd.53.0183
- Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": The practical materiality of Bitcoin. *Social Semiotics*, *23*(2), 261–277. https://doi.org/10.1080/10350330.2013.777594
- Nakamoto, S. (2008a). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- Nakamoto, S. (2008b, November 14). *Cryptography Mailing List "Bitcoin P2P e-cash paper"*. https://satoshi.nakamotoinstitute.org/emails/cryptography/12/
- Nakamoto, S. (2009). *Bitcoin* (0.1.5 Alpha) [Computer software]. https://github.com/bitcoin/bitcoin/tree/ 4405b78d6059e536c36974088a8e d 4d9f0f29898

- Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, *60*(12), 36–45. https://doi.org/10.1145/3132259
- Ruffing, T. (2019). *Cryptography for Bitcoin and Friends* [PhD Thesis]. Universität des Saarlandes.
- Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700
- Swartz, L. (2018). What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies*, *32*(4), 623–650. https://doi.org/10.1080/09502386.2017.1416420
- Szabo, N. (2005). Bit gold [Blog post]. *Unenumerated*. https://unenumerated.blogspot.com/2005/12/bit-gold.html
- Sztorc, P. (2015). Nothing is Cheaper than Proof of Work [Blog post]. *Truthcoin*. https://www.truthcoin.info/blog/pow-cheapest/

Endnotes_

1. The term *uncle* is associated primarily with Ethereum-based networks, as a partial subsidy is allocated to orphaned blocks and therefore acts as a consolation prize for producing a valid block which does not become part of the canonical chain.
2. A portmanteau of *thermodynamic* and *economic*, not associated with the heterodox field of thermoeconomics.

NFTs (NON-FUNGIBLE TOKENS)_

Florian Idelberger, Law, European University Institute, Italy.
Péter Mezei, Institute of Comparative Law, University of Szeged, Hungary.

Blockchain-based NFTs (non-fungible tokens) are uniquely identifiable digital representations of physical or digital items. Usually, the tokens are indivisible into smaller units. NFTs represent structured metadata referring to physical or digital objects. The tokens act as separate identifiers and are often not tied to the objects. Their proponents claim they further the interoperable commercialisation of digital or physical goods.

Origin and evolution_

Already back in 2012-2013, hashes of files or other data were incorporated into the Bitcoin blockchain to prove existence or authenticity from a specific point in time (de Beauchesne, 2021). This development was built upon to create so-called 'Colored Coins', tokens that are uniquely identified by adding metadata to Bitcoin transactions, and Namecoin, a separate blockchain that deploys tokens for registering domain names, to establish an alternative, decentralised top-level domain name system (*Namecoin*, 2022). A further experiment was Counterparty, which featured expanded capabilities for more general-purpose applications of NFTs on the Bitcoin blockchain and the first blockchain-based trading cards (Portion.io, 2021).

The details of most current non-fungible tokens (NFTs) are described in a technical standard called ERC-721 (*ERC-721 Non-Fungible Token Standard*, 2018). This standard describes the required metadata of the NFT and the executable functions the underlying smart contract has to support to work with existing infrastructure such as trading websites and other interfaces. The standard refers to the Ethereum blockchain, the most popular one as of writing, but many other implementations are based on the Ethereum standard. ERC-721 is based on an Ethereum Improvement Proposal (EIP) and was finalised in 2018, shortly after Cryptokitties (CryptoKitties, 2021), a game to collect and multiply digital cats, first became popular in 2017.

From 2018 on, the projects and companies expanded even more and diversified their operations. NFTs started reaching the fine art market regarding pricing, with Beeples 'First 5000 Days' selling for 69 million (Christie's, 2021). Shortly thereafter, they were diversified further with the minting of, e.g. tweets (Howcroft, 2021), newspaper covers (The Economist, 2021) and even law review articles (Newsham, 2021). Fueled by venture capital, cryptocurrency investments and hype, marketplaces and surrounding infrastructure expanded massively (Mattei, 2021). At the end of 2021, a developer tokenised 'Cryptogotchis', the most expensive Tamagotchi clone ever (*Cryptogotchi Home*, 2021). As a result of this expansion, there have also been music songs, physical objects, academic papers, and much more put into NFTs. Sometimes these were just experiments, some were founders or investors looking for their own niche, yet others claim this process of tokenisation will bring about a new property system.

As the evolution continued, the art world has been drawn into cooperations between established art world institutions like Art Basel and technology companies. These cooperations are partly driven by profit motives with cryptocurrency proponents promising improved artist remuneration, disintermediation and easier compliance with upcoming anti-money-laundering regulations (Brown, 2021; Ryan, 2021).

Creation_

Minting is the act of creating an NFT. In this process, a user creates a new set of NFT data by sending a transaction to an underlying smart contract that supports NFTs, as described in ERC-721. It is assigned a blockchain contract address and a tokenId, which in combination form a globally unique identifier. Additional metadata can be (optionally) added. Crucially, the tokenised work is not necessary for minting, and not even a hash of the work has to be stored in the NFT (Guadamuz, 2021c; Bodó et al., forthcoming, 2022).

There are three main types of NFTs, based on how they relate to the digital or physical asset they represent. First, for certain NFTs, the work is uploaded to the blockchain; this, for example, can happen with code generating art or vector art. This type of NFT is relatively rare due to the high costs of storing data on the blockchain. Secondly, other NFTs incorporate

ownership rights, either by specifying them in the NFTs metadata or via a reference to external terms and conditions (such as on Mintable); in both cases, ownership can be transferred via blockchain transactions (Foo, 2021). Finally, the most used type of NFTs do not confer any rights or favour a commons-based licence such as CC0, which also does not confer rights on the token owner, as rights are granted publicly (Guadamuz, 2021b).

Issues_

NFTs raise several issues, the most relevant of which are the uncertainty about the legal rights and economic benefits they confer and the environmental impact of the underlying blockchain technology.

The ease of creating 'digital editions' of either art or collectables in an open and economically liquid network made for value transfer has partially opened up new revenue streams for artists, museums (Willis, 2021) and companies. Some proponents also argue that "NFTs might be able to democratise art" (Gibson, 2021), as they allow a broad spectrum of people to disseminate their born-digital art and to be remunerated for such dissemination. Contrary to claims from NFT projects, however, there is currently no evidence that it improves artists' struggles to earn a living (with some notable exceptions) compared to other forms of online monetisation (Dash, 2021; Ryan, 2021).

From a copyright perspective, NFTs do not work to provide a living for many artists, as they are freely accessible, and thus already established artists and those who can grow a following (especially among crypto natives) are the ones that thrive (Bruner, 2021). Compared to other popular content such as streaming services, NFTs are not protected by digital rights management and thus can be enjoyed by anyone and many people at the same time. This 'non-rivalrous nature' only works for artists with clout and networks by creating artificial scarcity (Brekke & Fischer, 2021) via artificially limiting not the work but the reference to it. Nevertheless, the art itself can still be enjoyed and copied by anyone. In the absence of property rights, an NFT is essentially often only a unique global identifier for a reference to a work (Moringiello & Odinet, forthcoming).

As a result, on the one side, NFT proponents describe these bits of metadata as the start of a new economic system and the liberation of the art and

the artists from the oppressive forces of the art market, whereas opponents and sceptics see it as capitalism in overdrive due to the commoditisation and securitisation of art (Ryan, 2021). Commoditisation refers to treating art as yet another tradeable good instead of something with its own value independent of money. Securitisation refers to turning everything into a financial instrument for financial speculation, which then also allows fractionalisation (splitting into shares) of an asset. (Rabouin, 2021). Decrying rampant fraud and speculation, NFTs' opponents claim that the economic models used by NFT projects do not offer any non-capitalist incentives such as a fairer economic system (Ivie, 2021; Moringiello & Odinet, forthcoming).

Regarding the environmental concerns, most NFTs today exist on proof-of-work blockchains which require vast amounts of energy to power their security and functioning, which is criticised due to their environmental footprint. There are proof-of-stake based blockchains or second layer systems either in development or already available to alleviate the environmental impact. However, for now, the amount of energy required is an essential argument against NFTs, same as with many public blockchains (Alsindi & Lotti, 2021).

Other technical and socio-legal issues raised by NFTs are that of disappearing links ('link rot') and allegations of fraud and money laundering. With many NFTs containing only a link to the tokenised content, "link rot" is a pressing concern. This term describes the situation where the hyperlink no longer points to its target because it is no longer available through the corresponding hosting service. In the case of a decentralised storage system such as IPFS, it is dependent on someone sharing this via their node or paying for 'pinning' as a service (Kastrenakes, 2021). Finally, there have also been allegations of money laundering. Specific projects, especially those featuring collectables, have sometimes disappeared right after selling all their generated NFTs (Department of Justice, 2022). These cast any positive aspects of NFTs into doubt (Teitelbaum, 2022; Bodó et al., forthcoming, 2022).

Copyright-related aspects of NFTs_

NFTs and copyright law have two significant zones of interaction. The first is related to the 'minting' when NFTs are created, and the second is focused on the dissemination of the digitised works.

Without any doubt, the *content behind the NFT* can be subject to copyright protection. The threshold of originality (whether a work is original enough to be protected by copyright) is the prerequisite of protection under copyright law (of the European Union), and this threshold is low under the case law of the Court of Justice of the European Union (Bodó et al., 2022, forthcoming). Hence, even pixel-based art (e.g. CryptoPunks) can meet such requirements. Likewise, plenty of other traditional copyright concepts remain applicable for tokenised digital artworks, e.g. moral rights protect authors against misappropriation; other examples are "copyfraud" cases (that is, minting by non-owners of artworks) (Guadamuz, 2021a) and traditional licensing mechanisms.

The use of the tokens referencing a copyrighted work leads to more substantial copyright challenges. First, posting a digital image on a website (e.g. OpenSea) can infringe on the economic right of making available to the public by the author. (In the European Union, Article 3 of the InfoSoc Directive grants this right to authors and related rights holders with respect to on-demand use). Second, it is far from certain that the offering for "sale" of the NFT itself represents a "use" in a traditional copyright sense. It is plausible that the transfer of NFTs does not fit into the right of distribution, as distribution is relevant mainly for the transfer of ownership of tangible copies of works. Offering access to digital copies is instead treated as the making available of that copy to the public. The CJEU's judgement confirmed this in the Tom Kabinet case (*C-163/18 Tom Kabinet*, 2019). The same judgement concluded that the doctrine of exhaustion should remain inapplicable in the digital domain for works other than software (Bodó et al., forthcoming, 2022).

A source of tension between the NFT world and copyright laws is the misleading use of copyright-related terminology. The use of copyright terminology creates the illusion that NFTs naturally incorporate property rights. Furthermore, claims of authenticity are made based on links to a work even when no legal connection between such work and the token is

established (Moringiello & Odinet, forthcoming, p. 24). The acquisition of ownership interests is seldom associated with acquiring a token, and platforms often make no efforts to verify authenticity. There is even a project that allows automated 'cloning' of an NFT by minting it yourself (*Knockoff NFTs*, 2021).

With NFTs, sellers can set their own terms. These terms can consist in traditional transfer of rights, possibility to use the NFT to unlock additional content, or a 'digital resale royalty'. Such rights can be granted either via traditional licensing agreement or by attaching additional terms to the NFT. In any case, creators and owners of NFTs are in a powerful position to control the fate of their creations (Lapatoura, 2021, p. 171).

There have been attempts even before the rise in popularity of NFTs to use blockchain-based systems for a registration system for copyrighted works — but all failed (Bodó et al., 2018) Some were too early (ascribe), others were just experiments (Ujo), and existing stakeholders such as collecting societies and publishers likely have little to gain from making their licensing more transparent. However, for consumers and smaller artists, transparency about who earns how much could be very beneficial. In a recent development, the Italian collecting society SIAE plans to launch NFTs for the creators it represents on Algorand, an alternative blockchain with higher throughput and much-reduced energy needs. It is unknown how this plays out and what the benefits are, especially as the most significant issues for collecting societies are finding infringement and enforcement (Bodó et al., forthcoming, 2022)

Lastly, a public policy issue is the minting of public domain works. Such tokenisation might not be prohibited, as the original work is not necessary for the minting. Still, it invokes a strong reaction in parts of society when profits are made in such a way off public or free works (Guadamuz, 2021c).

Conclusion_

NFTs give their holders the illusion of ownership; in other words, they are a "cryptographically signed receipt that you own a unique version of a work" (Guadamuz, 2021c). However, the possession of an NFT does not necessarily confer any legal right over the digital or physical object that the NFT refers to. Several proposals have been advanced to

overcome this limitation to the concept of NFT. Some instantiations try to forego the law in favour of technical solutions, sticking to the idea that 'code is law'; others try to strike a balance between the legal and the technical dimension, incorporating aspects of copyright law into the metadata of the NFT or in accompanying documentation; finally, others propose to incorporate the actual work into the underlying smart contract. While many commentators are critical at this point (Ryan, 2021), others, like Fairfield, see the potential of NFTs as forms of 'unique digital property', reestablishing personal property rights that have been lost to user agreements and other instruments of uneven bargaining power (Fairfield, 2021).

References_

- Alsindi, W. Z., & Lotti, L. (2021). Mining. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1551
- Bodó, B., Gervais, D., & Quintais, J. P. (2018). Blockchain and smart contracts: The missing link in copyright licensing? *International Journal of Law and Information Technology*, *26*(4), 311–336. https://doi.org/10.1093/ijlit/eay014
- Bodó, B., Giannopoulou, A., Quintais, J. P., & Mezei, P. (2022). The Rise of NFTs: These Aren't the Droids You're Looking For. *European Intellectual Property Review*, *44*(5). https://ssrn.com/abstract=4000423
- Brekke, J. K., & Alsindi, W. Z. (2021). Cryptoeconomics. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1553
- Brekke, J. K., & Fischer, A. (2021). Digital scarcity. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1548
- Brown, K. (2021, September 21). *NFTs Make Their Debut at Art Basel, Where Collectors Are Curious — And a Bit Confused — About the New Art Medium*. Artnet News. https://news.artnet.com/market/nfts-art-basel-2011438/amp-page
- Bruner, R. (2021, September 7). Teen artists are making millions on NFTs. How are they doing it? *Time*. https://time.com/6093982/nft-art-teens-money/
- *C-163/18 Tom Kabinet, ECLI:EU:C:2019:1111*. (2019). European Court of Justice. https://curia.europa.eu/juris/document/document.jsf?text=&docid=221807&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=23536823
- Christie's. (2021, November 3). *Beeple (b. 1981), EVERYDAYS: THE*

FIRST 5000 DAYS. Christie's. https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924
- *Cryptogotchi Home*. (2021). Cryptogotchi. https://cryptogotchi.app/
- CryptoKitties. (2021). *CryptoKitties | Collect and breed digital cats!* CryptoKitties. https://www.cryptokitties.co
- Dash, A. (2021, April 2). NFTs weren't supposed to end like this. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2021/04/nfts-werent-supposed-end-like/618488/
- de Beauchesne, Q. (2021, July). *NFT Month — History of NFTs*. Ownest.Io. https://archive.ph/izPW9
- De Mattei, S. E. (2021, September 28). *2021 Has Been the Year of the NFT. But What Exactly Is an NFT?* Art News. https://www.artnews.com/art-news/news/nft-guide-1234614447/
- Department of Justice. (2022). *Two defendants charged in Non-Fungible Token ("NFT") fraud And money laundering scheme*. Department of Justice U.S. Attorney's Office Southern District of New York. https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0
- *ERC-721 Non-Fungible Token Standard*. (2018, June 24). Ethereum. Org. https://ethereum.org
- Fairfield, J. (2021). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal, Forthcoming*. https://papers.ssrn.com/abstract=3821102
- Foo, T. (n.d.). *How Do NFT Copyrights Work?* Mintable. https://web.archive.org/web/20211125163520/https://editorial.mintable.app/2021/08/27/how-do-nft-copyrights-work/
- Gibson, J. (2021). The thousand-and-second tale of NFTs, as foretold by Edgar Allan Poe. *Queen Mary Journal of Intellectual Property*, *11*(3), 249–269. https://doi.org/10.4337/qmjip.2021.03.00
- Guadamuz, A. (2021a, March 14). Copyfraud and copyright infringement in NFTs. *TechnoLlama*. https://www.technollama.co.uk/copyrfraud-and-copyright-infringement-in-nfts
- Guadamuz, A. (2021b, March 28). What do you buy when you buy an NFT? *TechnoLlama*. https://www.technollama.co.uk/what-do-you-buy-when-you-buy-an-nft
- Guadamuz, A. (2021c). The treachery of images: Non-fungible tokens and copyright. *Journal of Intellectual Property Law & Practice*, *16*(12), 1367–1385. https://doi.org/10.1093/jiplp/jpab152
- Howcroft, E. (2021, March 22). Twitter boss Jack Dorsey's first tweet

sold for $2.9 million as an NFT. *Reuters*. https://www.reuters.com/article/us-twitter-dorsey-nft-idUSKBN2BE2KJ

- Ivie, D. (2021). Brian Eno elegantly eviscerates NFTs. *Vulture*. https://www.vulture.com/2021/12/brian-eno-on-nfts-and-capitalist-assholes.html
- Kastrenakes, J. (2021, March 25). Your million-dollar NFT can break tomorrow if you're not careful. *The Verge*. https://www.theverge.com/2021/3/25/22349242/nft-metadata-explained-art-crypto-urls-links-ipfs
- *Knockoff NFTs*. (2021). Knockoff NFTs. https://www.knockoff.lol/#/
- Lapatoura, I. (2021). Creative digital assets as NFTs: A new means for giving artists their power back? *Entertainment Law Review*, *32*(6), 169–172.
- Moringiello, J. M., & Odinet, C. K. (2021). The property law of tokens. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3928901
- *Namecoin*. (2022, January). Namecoin. https://www.namecoin.org/
- Newsham, J. (2021, October 2). A law professor made $65,000 selling NFTs of papers he writes in his bathtub. Here's how he set his prices and what he's doing with the money. *Business Insider*. https://www.businessinsider.com/law-professor-made-65000-selling-nfts-how-he-did-it-2021-10
- Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1561
- Pinto-Gutiérrez, C., Gaitán, S., Jaramillo, D., & Velasquez, S. (2022). The NFT Hype: What Draws Attention to Non-Fungible Tokens? *Mathematics*, *10*(3), 335. https://doi.org/10.3390/math10030335
- Portion.io. (2021, July 27). The History of NFTs & How They Got Started. *Portionio Blog*. https://blog.portion.io/the-history-of-nfts-how-they-got-started/#:~:text=The%20idea%20of%20NFTs%20emerged,%2C%20even%20equities%2C%20and%20bonds.
- Rabouin, D. (2021, October 4). Should You Invest in Little Bits of Paintings, Cars, and Comedians? *Vox*. https://www.vox.com/the-goods/22700655/cryptocurrency-invest-nft-whiskey-playboy
- Ryan, T. R. (2021, December 2). *Will the Artworld's NFT Wars End in Utopia or Dystopia?* Art Review. https://artreview.com/will-the-artworld-nft-wars-end-in-utopia-or-dystopia/
- Teitelbaum, D. E., Tessler, L., Teager, K. S., & Park, C. K. K. (n.d.). *Treasury Study of Money Laundering Risks in the Art World Focuses on NFTs*. Sidley Austin LLP. https://www.lexology.com/library/

detail.aspx?g=ae38077d-119f-4f2f-afdd-00a04a3f4180
– Why we are selling our cover as an NFT: How we set it up — And decided it was worth doing. (2021, October 21). *The Economist*. https://www.economist.com/the-economist-explains/2021/10/21/why-we-are-selling-our-cover-as-an-nft
– Willis, S. (2021). Crypto millionaires' love of NFTs is a boon for the aging art market — But galleries may miss out. *Fortune*. https://fortune.com/2021/04/14/nft-non-fungible-token-art-crypto-art-market -galleries-auction-houses/

NON-USER_

Selwa Sweidan, Department of Media Arts and Practice, University of Southern California, United States.
Karlynne Ejercito, Department of American Studies and Ethnicity, University of Southern California, United States.

A "non-user," as the name suggests, refers to an individual who does not use a given product or system. Critical work on non-use elaborates a range of applications for the term we consider here. The variations of non-use under discussion encompass both voluntary and involuntary cases of non-use.

Context for non-user discourse_

What broadly comprises "non-user discourse" is derived from user discourse. Commentary about the "user" originated in systems design, which emerged in the United States and Europe as part of a wider effort to advance the development of military technologies. As computing systems evolved, so too did the "user" for whom these technologies were designed.

Early data processing systems originally responded to the needs of information intensive industries. User organisations in both public and private sectors oriented the design of information technologies to enhance the productive capacities of their respective operations (Yates, 1993). It is within the context of user-organisation that innovation studies introduced the concept of "lead users" into user discourse. Research focused on single industries identified the "lead user" as an individual who proposes key innovations from outside the industry (Oudshoorn & Pinch 2003, p. 541; von Hippel, 2007; Graham, 2006). What distinguishes the lead user from ordinary users is a set of skills that exceed the given functions of a particular device (von Hippel, 1976).

As demand for micro-electronics and personal computers surged in the 1980s, "user-centred" design and "user experience" re-oriented the design of systems to accommodate individual consumers (Oudshoorn &

Pinch, 2003). With the convergence of information and communication technologies, models of human computer interaction turn their attention from the single user tethered to a single device to multiple users distributed across large networks.

In contrast to their predecessors, these products incorporated the "holistic study of users from the viewpoint of the user" rather than the system (Dervin & Nilan, 1986; & Hartel 2007, p. 2; White & McCain, 1998). Harnessing cognitive psychology to improve how systems were designed, the study of "user experience" deepened the existing view of users by taking into account the "emotions, beliefs, preferences, perceptions, physical and psychological responses, behaviours, and accomplishments" (ISO, 2009) that condition human computer interaction (Rheinfrank, 1995).

Research on users in human-machine interaction, information science, and cognitive psychology (Cooper & Bowers, 1995; Kosara et al., 2003; von Hippel, 2005) since then, has provided a basis for critical work in the field of science, technology and society (STS). It is within this context that discourse on non-users takes shape.

Variations of non-use_

From the standpoint of HCI, non-users are a technical designation for "potential users" (Satchel & Dourish, 2012, p. 9). Implicit in HCI's model of non-use are a set of assumptions that elicit much debate outside the field. Studies in STS identify a range of cases for non-use: resistance, rejection, exclusion, expulsion, lagging adoption, disenchantment, disenfranchisement, displacement and disinterest (Wyatt et al., 2002; Satchell & Dourish, 2009).

This spectrum of negative actions captures what makes non-use particularly difficult to define in positive terms. Because non-use is not observable in the way uses are, the study of it presents a formidable challenge for how scholars approach the topic (Dourish, 2001, p. 56; Treem, 2014). For the purposes of this glossary entry, we organise the different types of non-use into two primary categories. The first encompasses cases of voluntary non-use, while the second circumscribes examples of involuntary non-use.

Voluntary non-use_

Opting-out of use is a singular action which belies a complex of subjective considerations and varies in relation to economic conditions and ideological commitments (Brubaker, Ananny et al., 2016).

Insofar as voluntary non-use presumes a certain degree of individual choice, it refers to a set of economic conditions specific to market-based capitalism. Non-users who terminate their engagement with one company, for example, may opt into a platform belonging to a competitor. Scholarship on the attention economy (Crary, 2001) expands on the subjective dimensions intrinsic in the economic model of consumer choice. Such scholarship examines how individual attention is structured by the products and services which compete for it (Crawford, 2015; Davenport, 2001).

Organised boycotts present a collectivised form of voluntary non-use. In these cases, a set of political and ethical commitments lend a social form to the decisions of individual non-users who reject the products of a given entity. This non-use as a form of consumer activism is based on the voluntary rejection of a user technology (Wyatt et al., 2002). The duration and degree to which non-users participate in the boycott varies: some partially and temporarily suspend use, while others may completely and permanently terminate their use of a particular good or service altogether.

Individual cases of non-use that are not principally motivated by political concerns have their origins in nineteenth century bourgeois culture. With the expansion of cities and industrial processes came a rich body of literature that broadly envisioned different means of withdrawal from the increasingly oppressive conditions intrinsic to modernity. Technology's relationship to nature and the rationalisation of society has long preoccupied critics of modernity, who consider the political subjects industrial development reciprocally determines (Marx, 1964; Kracauer, 1924). Risk assessment made on an individual basis underlies more recent examples of voluntary non-use that are motivated by concerns about public health. "Internet addiction" was officially declared a public health issue in China as early as 2008, when an uptick in searches for the term "digital detox" coincided with the launch of the first iPhone (Jiang, 2014). "Digital detox" posits a solution to problems of over-connectivity

(Syvertsen & Enli, 2019) that applies the moral rhetoric of contemporary wellness regimes (Madsen, 2015) to the digital age (Syvertsen & Enli, 2019).

Involuntary non-use_

Cases of non-use which are involuntary present a much more elusive object of research than the examples of voluntary non-use outlined in the previous section. Nevertheless, secondary literature on compulsory non-use can be subdivided into three different units of analysis: infrastructural, structural, and individual.

Discrepancies in access function as a point of departure for work on involuntary non-use at the infrastructural level. By examining differences in access among various populations, this research shows how historically marginalised populations have been disproportionately affected by lack of internet access. The extent to which race, gender, and class play a role in the distribution of access to digital technologies is the source of much debate among social scientists (Dewan & Riggins, 2005; DiMaggio et al., 2004).

Lack of access to content and different platforms as a result of mandates is a form of involuntary non-use that takes place at the structural level. These cases tend to presume a centralised structure of authority, such as the corporation or state, which has the capacity to revoke content and prioritise the use of certain systems.

In certain cases, individuals may fall under the category of involuntary non-users because of a gap between their skills and those required to navigate advanced information systems. Without the appropriate skills, these individuals attain non-user status. Debates over digital literacy are of central relevance to users (and non-users) of decentralised systems insofar as their accessibility determines who can and cannot be considered a user. One challenge decentralised computing infrastructures face is the creation of end-user-friendly systems. (Gervais et al., 2014). In prioritising technological design over usability, decentralised systems can be prohibitively difficult to use — even as they impact economic, civic, and social opportunities for users and non-users alike (DiMaggio et al., 2004). Potential users who cannot engage in decentralised platforms may consequently be "left behind," thus becoming involuntary non-users.

Further, users may have difficulty leaving centralised platforms for less mainstream, less easily accessible decentralised alternatives. In other words, digital literacy impacts not only who is able to use decentralised systems, but also, who has the choice to swap their usage of centralised systems for decentralised ones. Here it is important to note that scholars who research digital literacy emphasise the importance of studying population segments, and disaggregating digital literacy and non-use.

Issues related to non-use_

Voluntary and involuntary cases of non-use present a number of issues that range in practical and theoretical significance.

Where access to user technology is assumed, issues related to non-use take on practical considerations. The transfer of data from centralised platforms to alternative ones for example raises a problem concerning "portability." Users who opt out of one platform sometimes encounter difficulties with transporting their data as a result of conflicting proprietary arrangements. A solution to this problem may be found in open standards, which considers how user data may be portable, by enabling system interoperability (Barbas et al., 2017).

Determining who counts as a non-user remains largely contingent on how users themselves are defined. In HCI, the question of whether the user assumed in user-centred design can accommodate the diversity of interactions between humans and computers is a source of much debate (Baumer & Brubaker, 2017). One side of it maintains that by flattening the full range of human activity into "systems, interfaces, design practices, and discourse" (Baumer and Brubaker, 2017, p. 6291), user centred design posits an inherently exclusionary model of human computer interaction. Though HCI acknowledges its cultural specificity, certain methods central to the field nevertheless continue to employ a universalist approach which assumes an omniscient creator (Philip et al., 2012).

In calling attention to normative conceptions of user at work in popular narratives about technological development (Oldenziel, 2001; Star, 1991), feminist and postcolonial critiques of technoscience challenged prevailing definitions of the user and non-user by attending to positions which have historically been excluded from these narratives. This discourse focuses

on the wider conditions of uneven development that have shaped who designers and engineers assumed to be the user (MacKenzie & Wajcman, 1999; Williams et al., 2005).

Anti-universalist methods which have emerged in response to these debates apply decolonial critiques of knowledge and artefact production to the design of HCI (Johnson, 1998; Suchman, 2002). How the global division of labour is gendered and racialized in the technological imagination is the object of considerable research in STS (Oudshoorn & Pinch, 2003). Expanding the frame of HCI to geographies and peoples beyond the industrial north provincializes dominant narratives about innovation, which have long been weaponized against indigenous movements in newly industrialising countries across the global south (Chakrabarty, 2000; Mignolo, 2007). Although HCI theoretically recognizes the cultural specificity of designed products, a number of design processes and methods remain universalist in their approach (Philip et al., 2012) by assuming the ability to design for one user at the exclusion of many others. Adapting anthropocenic and decolonial critiques to HCI design, designers have increasingly turned to methods which aim to decentre the human, and attend to subaltern modes of knowledge production (Tunstall, 2020; Schultz, 2018). In centreing human agents, user and non-user discourse minimises the non-human agents that shape and are shaped by use. Actor-network theory (ANT) (Latour, 2005) provides one alternative to this human-centred framework through a definition of the user which extends to animals, plants, minerals and cities typically outside the core interaction between human and machines. ANT encompasses technological deterministic views of user-technology relations and social constructionist approaches to technology, by attending to how agency is distributed among humans, non-humans, and the technologies which mediate their relationship. This conceptualization places the user as an agent within relational networks aligns with anthropocenic debates, and calls for rethinking systems and technological approaches that concentrate the authority over these networks in human agents who comprise only one aspect of them (Light et al., 2017).

Conclusion_

In conclusion, non-use belies a complex of subjective considerations, which we sort in two primary categories: voluntary and involuntary cases of non-use. Attending to the non-user presents an opportunity to contextualise user agency, and access. Whereas systems design adopted a centralised model of human computer interaction as its basic unit of analysis, non-user discourse accounts for a more diverse range of interactions.

References_

- Barabas, C., Narula, N., & Zuckerman, E. (2017, September 8). Decentralised social networks sound great. Too bad they'll never work. *WIRED*. https://www.wired.com/story/decentralized-social-networks-sound-great-too-bad-theyll-never-work/
- Baumer, E. P. S., & Brubaker, J. R. (2017). Post-userism. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 6291–6303. https://doi.org/10.1145/3025453.3025740
- Benkler, Y. (2016). Degrees of freedom, dimensions of power. *Daedalus*, *145*(1), 18–32. https://doi.org/10.1162/DAED_a_00362
- Brubaker, J. R., Ananny, M., & Crawford, K. (2016). Departing glances: A sociotechnical account of 'leaving' Grindr. *New Media & Society*, *18*(3), 373–390. https://doi.org/10.1177/1461444814542311
- Bush, V. (1948). As we may think. *The Atlantic*.
- Central Government Portal. (2008). 我国首个《网络成瘾临床诊断标准》通过专家论证 *(Country's first "Clinical Diagnostic Criteria for Internet Addiction" passed expert demonstration)*.
- Chakrabarty, D. (2000). Subaltern studies and postcolonial historiography. *Nepantla: Views from South*, *1*(1), 9–32.
- Cooper, G., & Bowers, J. (1995). Representing the user: Notes on the disciplinary rhetoric of human-computer. The social and interactional dimensions of human-computer interfaces. In P. J. Thomas (Ed.), *The Social and Interactional Dimensions of Human-Computer Interfaces* (pp. 67–106). Cambridge University Press.
- Coutard, O. (Ed.). (2002). *The Governance of Large Technical Systems*. Routledge.
- Crary, J. (2001). *Suspensions of Perception: Attention, Spectacle, and Modern*

Culture. MIT Press.
- Crawford, M. B. (2015). Introduction: Attention as a cultural problem. In *The World Beyond Your Head: On Becoming an Individual in an Age of Distraction*. Farrar, Straus and Giroux.
- Davenport, T. H., & Beck, J. C. (2001). *The Attention Economy: Understanding the New Currency of Business*. Harvard Business School Press.
- Dervin, B., & Nilan, M. (1986). Information needs and uses. *Annual Review of Information Science and Technology*, *21*, 3–33.
- Dewan, S., & Riggins, F. J. (2005). The digital divide: Current and future research directions. *Journal of the Association for Information Systems*, *6*(2), 298–337.
- DiMaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). Digital inequality: From unequal access to differentiated use. In K. M. Neckerman (Ed.), *Social inequality*. Russell Sage Foundation.
- Dourish, P. (2001). Process descriptions as organisational accounting devices: The dual use of workflow technologies. *Proceedings of the 2001 International ACM SIGGROUP Conference on Supporting Group Work - GROUP '01*, 52. https://doi.org/10.1145/500286.500297
- Dourish, P., & Mainwaring, S. D. (2012). Ubicomp's colonial impulse. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, 133. https://doi.org/10.1145/2370216.2370238
- Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is Bitcoin a decentralized currency? *IEEE Security & Privacy*, *12*(3), 54–60. https://doi.org/10.1109/MSP.2014.49
- Goodin, T. (2018). *Off: Your digital detox for a better life*. Abrams. https://www.overdrive.com/search?q=448CC5C3-82D3- 4702-8C5F-30109EED9AC7
- Graham, M. B. W. (2006). Comment: Exploring the Context of Use. *Enterprise & Society*, *7*(3), 456–461. https://doi.org/10.1017/S1467222700004341
- International Organisation for Standardisation (ISO). (2009). *ISO 9241-210:2010 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems*.
- Jiang, Q. (2014). *Internet addiction among young people in China: Internet connectedness, online gaming, and academic performance decrement*.
- Johnson, R. R. (1998). *User-centered technology: A rhetorical theory for computers and other mundane artifacts*. SUNY Press.
- Kosara, R., Healey, C. G., Interrante, V., Laidlaw, D. H., & Ware, C.

(2003). Thoughts on user studies: Why, how, and when. *IEEE Computer Graphics and Applications*, *23*(4), 20–25. https://doi.org/10.1109/MCG.2003.1210860

- Kracauer, S., & Levin, T. Y. (1995). Boredom. In *The Mass Ornament: Weimar essays*. Harvard University Press.
- Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford university press.
- Low, C. (2020). *Accessibility in tech improved in 2020, but more must be done*. Engadget. https://www.engadget.com/accessibility-in-tech-2020-150002855.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ 29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAB1mniJhfdvluBKHyU7WgmH0vChPpNU9Imj2S_1OsjNw8SYZVWVAazfGik-zzFJ6e-hdfO150-HuB9ANzKlPGm2sBTYkEN_gyKVhTSEKinwiE2Fd6ZPAsiXwKEDS80GBPtYmotNi-tX0ePaNNaNx7jYlEatlfFUHSDbCIap_narn
- MacKenzie, D., & Wajcman, J. (1999). *The Social Shaping of Technology*. Open University Press.
- Madsen, O. J. (2015). *Optimizing the Self: Social Representations of Self-Help*. Routledge.
- Manley, J. (2020, November 26). The ethics of rebooting the dead. Wired. *WIRED*. https://www.wired.com/story/ethics-reviving-dead-with-tech/
- Marwick, A. (2011). If you don't like it, don't use it. It's that simple. *Social Media Collective Research Blog*. http://socialmediacollective.org/2011/08/11/if-you-dont-like-it-dont-use-it-its-that-simple-orly/
- Mignolo, W. D. (2007). Delinking: The rhetoric of modernity, the logic of coloniality and the grammar of de-coloniality. *Cultural Studies*, *21*(2–3), 449–514. https://doi.org/10.1080/09502380601162647
- Oudshoorn, N., & Pinch, T. (Eds.). (2003). *How Users Matter: The Co-construction of Users and Technologies*. MIT Press.
- Perrin, A., & Atske, S. (2021). *Americans with disabilities less likely than those without to own some digital devices* [Report]. Pew Research Center. https://www.pewresearch.org/fact-tank/2021/09/10/americans-with-disabilities-less-likely-than-those-without-to-own-some-digital-devices/.
- Philip, K., Irani, L., & Dourish, P. (2012). Postcolonial computing: A tactical survey. *Science, Technology, & Human Values*, *37*(1), 3–29. https://doi.org/10.1177/0162243910389594
- Rheinfrank, J. (1995). A conversation with Don Norman. *Interactions*,

2(2), 47–55. https://doi.org/10.1145/205350.205357
- Satchell, C., & Dourish, P. (2009). Beyond the user: Use and non-use in HCI. *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group on Design: Open 24/7 - OZCHI '09*, 9. https://doi.org/10.1145/1738826.1738829
- Schultz, T. (2018). Mapping Indigenous futures: Decolonising techno-colonising designs. *Strategic Design Research Journal*, *11*(2), 79–91. https://doi.org/10.4013/sdrj.2018.112.04
- Star, S. L. (1991). Power, technology and the phenomenology of conventions: On being allergic to onions. In J. Law (Ed.), *A Sociology of Monsters: Essays on Power, Technology and Domination* (pp. 26-55 ,). Routledge.
- Suchman, L. (2002). Located Accountabilities in Technology Production. *Scand. J. Inf. Syst*, *14, 2*, 91–105.
- Syvertsen, T., & Enli, G. (2020). Digital detox: Media resistance and the promise of authenticity. *Convergence: The International Journal of Research into New Media Technologies*, *26*(5–6), 1269–1283. https://doi.org/10.1177/1354856519847325
- Talja, S., & Hartel, J. (2007). Revisiting the user-centred turn in information science research: An intellectual history perspective. *Information Research*, *12*(4), 12–14.
- Treem, J. W. (2014). Technology non-use as avoiding accountability. In E. P. S. Baumer, M. G. Ames, J. R. Brubaker, J. Burrell, & P. Dourish (Eds.), *CHI '14 Extended Abstracts on Human Factors in Computing Systems* (pp. 65–68). ACM. https://dl.acm.org/doi/10.1145/2559206.2559224
- Trevisan, F. (2018). *Disability Rights Advocacy Online: Voice, Empowerment and Global Connectivity* (First issued in paperback). Routledge, Taylor & Francis Group.
- Tuhiwai Smith, L. (2021). Chapter 2; Research through Imperial Eyes. In *Decolonizing Methodologies: Research and Indigenous Peoples*. Zed Books. https://doi.org/10.5040/9781350225282
- Tunstall, E. D., Gunn, W., Otto, T., & Smith, R. C. (2020). Decolonizing design innovation: Design anthropology, critical anthropology, and indigenous knowledge. In *Design Anthropology Theory and Practice* (pp. 232–250). Routledge.
- von Hippel, E. (1976). The dominant role of users in the scientific instrument innovation process. *Research Policy*, *5*(3), 212–239. https://doi.org/10.1016/0048-7333(76)90028-7
- von Hippel, E. (2005). *Democratizing Innovation*. MIT Press.

- von Hippel, E. (2007). Horizontal innovation networks — By and for users. *Industrial and Corporate Change*, *16*(2), 293–315. https://doi.org/10.1093/icc/dtm005
- White, H. D., & McCain, K. W. (1998). Visualising a discipline: An author co-citation analysis of information science, 1972-1995. *Journal of the American Society for Information Science*, *49*(4), 327–355.
- Williams, R., Stewart, J., & Slack, R. (2005). *Social learning in technological innovation: Experimenting with information and communication technologies*. Edward Elgar Pub.
- Wilson, T. D. (1981). On user studies and information needs. *Journal of Documentation*, *37*(1), 3–15. https://doi.org/10.1108/eb026702
- Wyatt, S. (2003). Non-users also matter: The construction of users and non-users of the Internet. In N. Oudshoorn & T. Pinch (Eds.), *How Users Matter: The Co-construction of Users and Technologies*. MIT Press.
- Wyatt, S., Thomas, G., & Terranova, T. (2002). They came, they surfed, they went back to the beach: Conceptualising use and non-use of the Internet. In S. Woolgar (Ed.), *Virtual society? Technology, cyberbole, reality*. Oxford University Press.
- Yates, J. (1993). *Control through communication: The rise of system in American management* (Johns Hopkins paperbacks ed). Johns Hopkins Univ. Press.
- Zhao, Z., Laga, N., & Crespi, N. (2009). A survey of user generated service. *2009 IEEE International Conference on Network Infrastructure and Digital Content*, 241–246.

OPENNESS_

Tyng-Ruey Chuang, Institute of Information Science, Academia Sinica, Taiwan.
Rebecca C. Fan, Research Center for Information Technology Innovation, Academia Sinica, Taiwan.
Ming-Syuan Ho, Research Center for Information Technology Innovation, Academia Sinica, Taiwan.
Kalpana Tyagi, Maastricht University, Netherlands.

Openness is contextual. Openness implies access to resources that are otherwise closed or restricted in degrees; it can also refer to a more participatory mode of production. The nature and extent of openness depend on the context and/or disciplinary domain. Earlier usage of the term open was in the context of computer systems. For example, in networked systems of computers, 'openness' refers to enabling protocols that connect previously closed systems so that they can communicate with each other. Beyond that, openness has been used to imply a spectrum of meanings, notably since the campaign for open source software development populated the term 'open' and its suggested notions of 'openness' as freedom, entitlement, or norm. As a social form of organising, 'openness' suggests a way of sharing resources. In the corporate context, 'openness' refers to more active involvement of stakeholders in the process of value creation.

Coexisting uses and meanings_

In the 1980s, Open Systems Interconnection (OSI) released the OSI Reference Model, a set of standards for independent but interoperable computer networks (ISO, n.d.; Russell, 2013). This seven-layered network model offers a set of protocols for communication on and in between the layers. Openness, as in this OSI model, refers to the capability of working with "black box" systems of different vendors in the network. Such a model may be deemed open in the sense that it not only connects closed systems but it also remains vendor-neutral.

To achieve interoperability, information systems must follow formalised standard specifications. An open standard is one such specification that

is freely and publicly available for all to implement. According to the Open Source Initiative, an open standard must be detailed enough to allow interoperable implementations. As per the World Wide Web Consortium (W3C, 2007), the development of the specification must be transparent, open, and impartial. Open here means that anybody can participate. These requirements are also found in "The Modern Paradigm for Standards" (OpenStand, n.d.), a joint statement affirmed by the Internet Society, Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), W3C, and the IEEE Standards Association. Furthermore, all essential patents that are open must be licenced royalty-free or be covered by a promise of non-assertion when practiced by open source software (Open Source Initiative, 2006).

When a computer system's internal operation is not revealed to the outside, even though others may still interoperate with it, it is a closed system. When the software operating a computer system is publicly made available in a source code format, it is open source software. In the 1970s, source code was openly shared without much restriction until corporate entities started restricting redistribution of the source code of their products. In response, libre software and open source development emerged in the 1980s and 1990s to ensure that source code sharing remained a viable common practice. The Free Software Foundation and the Open Source Initiative were the key actors. The Free Software Foundation, by using the GNU General Public License, emphasises the freedoms the users must have in using their software, including the right to distribute, modify, and re-distribute the source code of the software and its modification (Free Software Foundation, 2007; 2021). The Open Source Initiative (2007) developed and released the Open Source Definition to establish a set of criteria that must be met before a software package can be called open source. The Open Source Initiative maintains a list of software licences conforming to the Open Source Definition. These are the open source licences recognised by the open source community at large.

Other public licences have also been devised to facilitate sharing. For example, open content licences have been applied to creative works that may be subject to copyrights and/or *sui generis* database rights. Examples of such open content licences include the Creative Commons Licenses

and the Open Database License. By definition, a piece of work can only be considered open if it is in the public domain or is distributed under an open (content) licence. The Open Definition of Open Knowledge Foundation further specifies the specific conditions that a licence must satisfy to be called an open licence, such as compatibility with other open licences (Open Knowledge Foundation, n.d.-b).

Issues currently associated with the term_

'Openness' evokes various connotations in socio-technical contexts, including but not limited to interoperability between computer systems in a network as well as the freedom of users to access, modify, and (re)distribute source code, expressive works, or datasets. It also suggests a participatory and interdependent mode of (co)production; sharing tangible and intangible resources; greater civic engagement as well as greater accountability of the duty-bearers; alternative governance models; a socio-cultural movement against enclosure and monopoly; an organisational paradigm characterised by dissolving boundaries or reducing barriers to facilitate innovation, amongst others.

The prime example that has generated much academic and business interest in the participatory mode of production or peer production is the Free/Libre Open Source Software (F/LOSS) development that emerged in the 1980s. Although neither the word 'participation' nor 'participatory' appeared prominently in the open software licences released by the key actors of F/LOSS. This participatory mode of production makes the (co) creation more community-based with a communal sense of ownership. It should be noted that open participation in the F/LOSS context mostly refers to contribution but not necessarily to governance, which is another issue (Raymond, 1998; Kreiss et al., 2011).

Beyond open participation and mode of production, diverse conceptions and disparate phenomena in the name of open can also be found elsewhere, one of which is the emerging phenomenon of Open Science that gained prominence in the mid-2000s. Here, the meaning of 'open' ranged widely, from advocating open access to existing scientific publications to suggesting open availability of scientific data, to a more open process of peer review, or opening up participation by "non-scientists" in research and knowledge production (Mirowski, 2018).

Another usage is Open Government. It has an older history than the previous terms discussed so far. Open Government, which is closely related to participatory government, first emerged around the 1950s in the US and was used by reformists to criticise the then opaque government in the post-World War II era (Yu, 2012; Wirtz and Birkmeyer, 2015). The term can be seen as a synonym for "accountable government" or "transparency government" and it implies how citizens shall have public access to previously undisclosed government information. In more recent years, innovations in digital technology also brought civic "participation" or civic "engagement" into the connotation of open government. For example, the OECD defines open government as "a culture of governance that promotes the principles of transparency, integrity, accountability and stakeholder participation in support of democracy and inclusive growth" (OECD, 2016). The Open Government Partnership, a multilateral organisation, also identifies "effective participation" as the first principle of open government (Burle et al., 2016).

Following the emergence of open government initiatives in the US and worldwide (Kitchin, 2014), as well as open-related movements facilitated by the enabling tool of the internet for data sharing (Yu, 2012), the term Open Data gained prominence. Although the origin of this term can be traced back to discussions in science policy in the 1970s (Yu, 2012), it did not gain momentum until the initiative for open data in the late 2000s. The word 'open' in Open Data emphasises free access to public sector information. Hence, it is often used as a synonym for Open Government Data. The W3C, the World Bank, and the European Union principally agree that Open Data must be freely accessible, reusable by everyone, and based on open licences (Open Knowledge Foundation, n.d.-a).

In public policy, the term Open Internet is often associated with the debates on net neutrality. Its usage can be traced back to the FCC Open Internet Order of 2010 in the US, while the Telecommunications Act of 1996 foresaw the Internet as an open platform for competitive information services. The term refers to how the Internet's architectural design and operation made it technically decentralised. For example, the layered nature of the Internet ensures that the modification of one layer of the Internet does not impact the other layers. The end-to-end design principle places the power and functionality of the network at its edge. The Internet Protocols ensure that the network can convey a packet

of data without knowing its content. This ensures there is "no central gatekeeper to exert control over the Internet" (Cerf, 2009). As such, its architecture enables different devices to connect to the networks, and the networks can interoperate with one another (West, 2016).

By extension and in the human context, Open Internet has been used to refer to the freedom for all to communicate over the network. In this sense, 'openness' advocates lowering the cost of access to increase affordability for the population at large (West, 2016).

In the corporate world, openness refers to the engagement of stakeholders across the value chain (Chesbrough, 2003). To enable open innovation, firms, customers, universities and start-ups readily collaborate with one another and use a more open business model. A business model is how the firm, based on its long-term vision, operates on a daily basis (Tyagi, 2020). The concept of 'openness' and the structure of an enterprise are closely interwoven. Viewed from this perspective, 'openness' is a "higher-order concept" (Schlagwein et al., 2017). This implies easy access to resources, open processes, and overall, a "democratic" opening up of the production process.

Openness herein refers to the process of "democratisation of innovation", whereby one sees a continuous feedback loop amongst the firms, its products and its consumers. Herein, one sees continuous interaction between the users and the firm, whereby users continuously feed into research and development (R&D) and the production process to create better and more innovative products, that in turn are widely adopted, manufactured, and further improved by the firms (von Hippel, 2005). Moreover, repeat iterations and interactions amongst creators and users over prolonged periods of time create these fine innovations. This is not to underplay the contribution of the individual inventor, it is to emphasise that the heroic individual inventor is but one key in the process of innovation.

Interestingly many of the revolutionising technologies that we see today, developed outside the patent system. As the systems developed, for example, as in the case of aviation, aggressive patenting activity put a cap on the group innovation activity (Bessen & Nuvolari, 2011). Overall, this indicates a complex interplay between patents, knowledge sharing, and open innovation. Complex products and systems (CoPS) refers to a

complex, high-value goods such as aircraft engines, telecommunications, and flight simulators. In light of high levels of customisation and post-purchase personalised requirements, such systems are designed in an open and accessible manner. The design here is the enabler of efficient allocation of tasks amongst the network of suppliers, and in that respect facilitates open innovation (Acha, 2008).

Existing misconceptions and biases_

Paradoxically, while openness may be used to invoke ideals like inclusiveness, equity, liberty, or transparency, the term does not necessarily lead to the implementation of such ideals or the assumed goodness of such ideals.

For example, two issues have generated debates in the public discourse and academia about F/LOSS projects: gender gap and governance. While the F/LOSS movement is known for its inclusive and collaborative working style, an Open Source Survey shows that only 3% of the total contributors are female (Github, 2017). Lee and Carver (2019) identified sexism as the key problem alongside male-dominating perspectives that created obstacles for gender-balanced contribution. On governance, when examined through a sociological lens of bureaucracy, notably Max Weber's account, it shows how the governance mechanisms of participatory or peer production championed by F/LOSS projects might not be as liberal or liberating as many theorists suggest (Kreiss et al., 2011).

Furthermore, Openness often suggests a particular kind of transparency that focuses on the exposure of politicians and bureaucrats for public scrutiny. However, as legal scholar Roberts (2015) argued, a call for transparency is not always about more openness but can be a call for the openness of a new type or a new focus as the architecture of the government changes, such as its size and complexity. Such openness sometimes provokes new worries about administrative changes. In such cases, the demand for openness is not simply about more transparency but the overhaul of oversight mechanisms to keep up with transformations in the bureaucracy.

Beyond the above ideals, certain adversarial practices have been identified by scholars and practitioners as Openwashing. Thorne (2009) who coined the term defines it as "to spin a product or company as open, although it is not." As more commercial products, services, and resources are

calling themselves 'open' but doing the opposite, the term has gradually been devalued or lost its meaning. While such practices of Openwashing have generated much criticism (World Wide Web Foundation, 2016; Heimstädt, 2017), Pomerantz and Peek (2016) offered a positive take by suggesting how it increased awareness about the term 'open' and prompted practitioner communities to develop more strict criteria to define what it means to be 'open'.

Conclusion_

As our search for definition underscores, openness is contextual. The motivations for designing or practicing openness in the digital realm tend to be enabling or supporting better communication between previously closed systems and to increase capability for the greater number to benefit. In other words, the drive is to scale up. Such enabling and capability-enhancing function and meaning can imply access to resources that are otherwise closed or restricted in degrees; it can also refer to a more participatory and interdependent mode of production.

The nature and extent of openness depend on the context and/or the disciplinary domain. Paradoxical as it may sound, openness does not necessarily lead to inclusiveness or equity, even though it may be used to invoke such ideals.

References_

- Acha, V. (2008). Open by design: The role of design in open innovation. *Academy of Management Proceedings*, *2008*(1), 1–6. https://doi.org/10.5465/ambpp.2008.33653210
- Bessen, J., & Nuvolari, A. (2011). Knowledge sharing among inventors: Some historical perspectives. *LEM Paper Series*, *2011*(21). https://ideas.repec.org/p/ssa/lemwps/2011-21.html
- Burle, C., Bellix, L., & Machado, J. (2016). *How about defining open government principles?* Open Government Partnership. https://www.opengovpartnership.org/stories/how-about-defining-open-government - principles/
- Cerf, V. (2009). The open Internet: What it is, and why it matters. *Telecommunications Journal of Australia*, *59*(2), 18.1-18.10. https://doi.org/10.2104/tja09018

- Chesbrough, H. W. (2003). *Open innovation: The new imperative for creating and profiting from technology*. Harvard Business School Press.
- Free Software Foundation. (2007, June 29). *The GNU General Public License v3.0*. GNU Operating System. https://www.gnu.org/licenses/gpl-3.0.en.html
- Free Software Foundation. (2021, February 2). *What is Free Software? Version 1.169*. GNU Operating System. https://www.gnu.org/philosophy/free-sw.en.html
- GitHub. (2017). *Open Source Survey*. GitHub. https://opensourcesurvey.org/2017/
- Heimstädt, M. (2017). Openwashing: A decoupling perspective on organizational transparency. *Technological Forecasting and Social Change*, *125*, 77–86. https://doi.org/10.1016/j.techfore.2017.03.037
- Hippel, E. (2005). *Democratizing Innovation*. The MIT Press.
- International Organization for Standardization. (n.d.). *35.100 — Open Systems Interconnection (OSI)*. https://www.iso.org/ics/35.100/x/
- Kitchin, R. (2014). *The Data Revolution: Big data, Open data, Data Infrastructures and Their Consequences*. SAGE Publications.
- Kreiss, D., Finn, M., & Turner, F. (2011). The limits of peer production: Some reminders from Max Weber for the network society. *New Media & Society*, *13*(2), 243–259. https://doi.org/10.1177/1461444810370951
- Lee, A., & Carver, J. C. (2019). FLOSS participants' perceptions about gender and inclusiveness: A survey. *2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE)*, 677–687. https://doi.org/10.1109/ICSE.2019.00077
- Mirowski, P. (2018). The future(s) of open science. *Social Studies of Science*, *48*(2), 171–203. https://doi.org/10.1177/0306312718772086
- OECD. (2016). *Open Government: The Global Context and the Way Forward*. OECD. https://doi.org/10.1787/9789264268104-en
- Open Knowledge Foundation. (n.d.). *Open Definition 2.1*. Open Data Handbook. https://opendefinition.org/od/2.1/en/
- Open Knowledge Foundation. (n.d.). *What is Open Data?* Open Data Handbook. http://opendatahandbook.org/guide/en/what-is-open-data/
- Open Source Initiative. (2006, July 24). *Open Standards Requirement for Software*. Opensource.Org. https://opensource.org/osr
- Open Source Initiative. (2007, March 22). *The Open Source Definition*. Opensource.Org. https://opensource.org/osd

- OpenStand. (n.d.). *The Modern Standards Paradigm — Five Key Principles*. OpenStand. https://open-stand.org/about-us/principles/
- Pomerantz, J., & Peek, R. (2016). Fifty shades of open. *First Monday*. https://doi.org/10.5210/fm.v21i5.6360
- Raymond, E. S. (1998). Homesteading the noosphere. *First Monday*, *3*(10). https://doi.org/10.5210/fm.v3i10.621
- Roberts, A. S. (2015). Too much transparency? How critics of openness misunderstand administrative development. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2601356
- Russell, A. L. (2013). The internet that wasn't. *IEEE Spectrum*, *50*(8), 39–43. https://doi.org/10.1109/MSPEC.2013.6565559
- Schlagwein, D., Conboy, K., Feller, J., Leimeister, J. M., & Morgan, L. (2017). "Openness" with and without Information technology: A framework and a brief history. *Journal of Information Technology*, *32*(4), 297–305. https://doi.org/10.1057/s41265-017-0049-3
- Thorne, M. (2009). *Openwashing*. https://michellethorne.cc/2009/03/openwashing/
- Tyagi, K. (2019). Merger control in the telecom industry: A landscape transformed. *Journal of Business Strategy*, *41*(6), 3–9. https://doi.org/10.1108/JBS-10-2018-0173
- West, J. (2016). *A framework for understanding internet openness*. Global Commission on Internet Governance Paper Series. https://www.cigionline.org/publications/framework-understanding-internet-openness/
- Wirtz, B. W., & Birkmeyer, S. (2015). Open government: Origin, development, and conceptual perspectives. *International Journal of Public Administration*, *38*(5), 381–396. https://doi.org/10.1080/01900692.2014.942735
- World Wide Web Consortium (W3C). (2007). *Definition of Open Standards*. World Wide Web Consortium (W3C). https://www.w3.org/2005/09/dd-osd.html
- World Wide Web Foundation. (2016). *Open data barometer: ODB global report third edition* [Report]. The World Wide Web Foundation. https://opendatabarometer.org/3rdedition/report/
- Yu, H., & Robinson, D. G. (2012). The new ambiguity of "open government." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2012489

PERMISSIONLESSNESS_

Kelsie Nabben, Blockchain Innovation Hub, RMIT University, Australia.
Michael Zargham, BlockScience, Inc., United States.

A technosocial system is deemed *permissionless* if it is possible to participate in the use, development, and governance of that system or infrastructure without requiring permission from an authority, by adhering to publicly stated procedures. "Permissionlessness" is a term often used in association with public blockchains. In this glossary entry, we explore the origins, evolution, and coexisting uses and meanings of the term "permissionless" to contextualise it. We argue that a technosocial system is deemed permissionless if it is possible to participate in the use, development, and governance of that system or infrastructure without requiring permission from an authority, by adhering to publicly stated procedures. This term is much more broadly applicable then just blockchain systems although it is relevant to decentralized systems. It can be conceptualised as a technical attribute, an ideology, and a cultural value, and links to the access, control, governance, entry and exit of an open information system.

Origin_

The term 'permission' comes from the Latin word 'permissio' — the act of permitting, in granting formal consent or authorisation (American Heritage Dictionary, 2000). In law, "permission" refers to the authority to act, as expressed or implied (Bouvier, 1856). The antithesis, 'permissionless', means without permission, or the ability to act without requiring another to allow that action. The notion of "permissionlessness" in relation to distributed technologies is both a technical attribute, and ideology, and a cultural value that emerged with the early internet.

In a technical context, *permissionlessness* refers to the open technical specifications in the network layer of the underlying protocols of the internet that avoids the cost of "permissioning" when transmitting data packets. The higher-level protocols for displaying websites also adhered to open specifications ("Hypertext Transfer Protocol" or HTTP). This innovation means that anyone is free to read, write, and share digital

information across interactive links without needing to seek permission from a central authority or gatekeeper, whereas prior to this, people were limited to local intranets on private networks. A culture of open source software development whereby anyone can verify or modify the underlying codebase helped enable permissionless protocols and innovation (Raymond, 2000).

The technical attributes of permissionless systems interplay with ideological values around freedom and anti-authoritarianism. For example, the "Cypherpunk" contributors to the technical developments and political ideology of decentralised digital infrastructure state "We're free individuals, able to say what we wish, meet in secret meetings without the permission of the government, and learn anything we wish to" (May, 1992).In a sociological context, permissionlessness is also a cultural value that emerged in early internet culture. "Permissionless innovation" is a counterculture value from the 1960s and 1970s about no central ownership or control, and not having to ask anyone for permission (Naughton, 2014; Web Foundation, 2017). Computer scientist and credited inventor of the World Wide Web, Tim Burners-Lee states that the internet is a force for free and open creativity outside of walled gardens: "It was all based on there being no central authority that you had to go to to ask permission" (Brooker, 2018). Digital networked infrastructures can be described as both social and technical, as "infrastructures for communication, cooperation and common value creation…allow for permission-less interlinking of human co-operators and their technological aids" (Kostakis and Bauwens, 2014, 55). An ideological purity towards free access to decentralised technologies developed in parallel to these technical capabilities, with some arguing that "true distributed networks are permission-less" and "not dependent on powerful obligatory hubs" (Bauwens, 2009). 'Permissionlessness' has come to broadly refer to anyone being able to *use* the infrastructure as common property with no selection process to participation.

These technical and cultural values were strongly amplified by adherents to influential technology communities, such as the free-software and open-source software movements (Stallman, 2002; Raymond, 2000). In these movements, the source code for computer programmes is available for users to modify it for their own use. Some principles of "permissionlessness" have also been defended against political and regulatory institutions by organizations such as the Electronic Frontier Foundation (EFF), which was

formed in 1990 to define and protect internet based civil liberties, such as open access to "Pretty Good Privacy" (PGP) digital encryption to rallying against bans on cryptocurrencies (Electronic Frontier Foundation, 2021).

Evolution_

Permissionless protocols have required, and also enabled new forms of social organisation and governance to evolve, including "Transmission Control Protocol and the Internet Protocol" or TCP/IP, and "Simple Mail Transfer Protocol" or SMTP. An important evolution in permissionless distributed technologies is the establishment and continuous development of standards to govern permissionless systems and allow them to scale. Although the foundation of permissionless systems is free access for anyone, permissionless systems still need to be governed at higher levels of the technology stack to manage unintended, negative consequences of free access. For example, the 'World Wide Web Consortium' (W3C), directed by Tim Burners-Lee, was founded in 1994 to develop open standards to ensure the long-term growth of the Web (W3C, 2021). These consensus-based standards offer recommendations to guide the technical specifications of how the system architecture should be developed.

Another example whereby permissionless systems still require governance mechanisms to function in practice is The Simple Mail Transfer Protocol (SMTP). SMTP is the protocol that facilitates email. A negative externality of permissionless email is the ability for anyone to freely send unsolicited junk mail, or 'spam' (Brunton, 2013). Spam is an example of the unintended consequence of open information networks that requires innovation in the governance of undesirable behaviour. This limitation of the base layer permissionless protocol is managed through governance mechanisms. This issue of spam in SMTP is solved by credentialing authorities that enforce processes and norms around automatically filtering incoming emails at higher levels of the technology stack. Modern email servers will reject or at least deprioritize messages that come from addresses on untrusted domains or which lack certificates from a relevant certificate authority by marking them as 'junk'. Although it involved institutions, some level of intervention, and in some ways partial censorship, this up-stack governance to manage the negative consequences of access to the system helps to ensure the ideal of permissionlessness can persist, as long as governance is polycentric, rather than monocentric. SMTP is arguably

a failed example of permissionlessness, as access to the global network is gated by access to the internet and the rules of access control are not clearly specified. This demonstrates how permissionless protocols have adapted over time to develop and incorporate governance mechanisms and processes to manage negative externalities. The sophistication and automation of these processes is constantly evolving.

Permissionless technological infrastructure was essential for the social evolution of the participatory systems that followed. The countercultural ideologies of the early internet influenced blockchain communities (Brunton, 2019). A resurgence of technical, cultural, and scholarly interest in 'permissionless' information infrastructures emerged in the wake of the Bitcoin whitepaper in 2008. Although the whitepaper does not mention "permissionless" directly, it makes numerous references to the ideals of the early internet and further develops these ideas of independence for "trust minimization" and "peer-to-peer" transactions without central intermediaries (Nakatomo, 2008). Bitcoin further mitigated the "Byzantine agreement problem", for agreement in distributed open networks (Lamport, Shostak, & Pease, 1982; Sherman et al., 2018). The ability to coordinate payments without intermediaries inspired an explosion in distributed consensus mechanism research in the field of computer science and economics (Xiao et al., 2020; Neudecker & Hartenstein, 2019). The explosion in innovation and development of public blockchains has led to the resurgence of the technical attribute and cultural value of "permissionless" networks.

"Decentralised Autonomous Organisations" (or "DAOs") represent a more recent class of "permissionless" organisation for participatory, technology-mediated systems that share a common goal (Larimer, 2013; Buterin, 2017). Within blockchain communities, DAOs are understood as a blockchain-based system that enables people to govern themselves, independent from central control (Hassan & De Filippi, 2021). DAOs refer to technologically mediated institutions, in the broad sense of the term, that are 'decentralised', as in "distributed away from a central authoritative location or group" (Merriam-Webster, 2021), and 'autonomous', as in "independent or self-governing" (Voshmgir et al., 2021). DAOs which are freely accessible to anyone to participate are an instantiation of 'permissionless' human-machine organisation at its logical extreme, and perhaps an evolution of the goals of the permissionless Web that more

explicitly incorporate permissionless approaches to governance. There are also other approaches beyond DAOs towards how information infrastructure-enabled coordination of value and social organisation among communities can be structured, such as protocol cooperatives and distributed cooperative organisations (Bauwens & Pazaitis, 2019; Mannan, 2020).

Coexisting uses and meanings_

The concepts of "permissionless" and "participatory" frequently appear together and are related. Although they frequently appear together, and are sometimes used interchangeably, they are not the same thing.

Permissionless is characterised by not needing permission to participate. These systems have a permissive boundary, meaning that no organisation mediates or controls access. Participatory systems are characterised by the ability to participate in a system in one or more ways. A common use of the term participatory is *participatory governance*, "which puts emphasis on democratic engagement, in particular through deliberative practices" (Fischer, 2012). Participation in an organisation operating and maintaining a digital infrastructure can include participation in multiple levels of the system, including (i) use of the infrastructure, (ii) contributing to the infrastructure's development, or (iii) engaging in governance of the infrastructure. Systems that are permissionless are necessarily participatory, yet those that are participatory are not always permissionless. Exclusivity can be a value proposition in participatory systems that are permissioned. An example of this is a semi-permissioned blockchain consensus mechanism, where only an approved set of validators can participate in governing the network. Different network architectures have various trade-offs and are fit for purpose in different cases. The context and purpose of a system, including who it serves must be clearly articulated to determine if permissionlessness is a useful attribute (Nabben, 2021). Conversely, permissionless systems may wish to consider the ways in which stakeholders participate.

Issues currently associated with the term_

There are five key issues with the term permissionless, including anarchy, censorship-resistance, exit, forking, and generationalisation, which we address in turn.

Anarchy: permissionless systems or communities does not mean the absence of rules of governance or lawlessness, but rather changing the architecture of a network to remove gatekeepers and hierarchy in accessing the network (Lessig, 2009). Activities in an anarchic network are still constrained within a surface of action and operate within the bounds of existing norms, including technical standards defined by the protocol, operational practices, and local laws (Daigle, 2014). Yet, being governed by norms and the rules of a protocol does not mean that selfish value-extraction is not possible if people can identify ways to exploit the system (Olson, 1965).

Censorship-resistance: permissionless at the technical level prevents banning someone from a digital network (or deplatforming) for any reason besides not adhering to the rules specified by the protocol (Ali et al., 2021). However, permissionless does not mean that you cannot be excluded for violating the protocol (e.g., when other nodes in a peer-to-peer network blacklist or drop connection to disconnect you from the network). In a social system, this equates to being kicked out of the community if the rules or norms of the community are violated repeatedly, through mechanisms such as graduated sanctions (Ostrom, 2005).

Exit: permissionless systems, whether cultural or technical, are defined by adherence to certain rules and norms. Those rules and norms themselves may change over time, or participants' preferences for following those rules or norms may change. In the presence of these changes a participant is faced with the options of Exit, Voice and Loyalty (Dowding, 2016). Permissionless systems that have a high cost of exit may be more effective at retaining participants, or this could work adversely, and retain undesirable participants. A particular manifestation of this concept as code is the 'rage-quit' mechanism popularized by MolochDAO, which allows participants to take their funds and exit the DAO if they disagree with a governance decision (de la Rouviere, 2021).

Forking: forking is an extreme manifestation of the permissionless ideal in all three layers (use, creation, governance) of a digital infrastructure. In both technical and cultural contexts, it is possible for disagreements to emerge regarding a particular standard, rule or norm which render two or more subgroups of digital network participants at odds. An example of this is a split in the Ethereum blockchain community following the

hack of a joint investment project called "The DAO" (DuPont, 2017). Some people believed the blockchain record of transactions should be wound back to recover the funds, while others wanted to respect the "immutable" ethos of public blockchains. This led to a "fork" of the protocol and community into what we know today as Ethereum, and Ethereum Classic. The resulting forking process is a technical mechanism to resolve a community impasse by copying the software code and dividing the community of participants. This can occur without permission of the original entity. It can be interpreted as exit on a scale large enough that a new similar entity is formed, despite, or in-spite, of the existence of the original entity.

Generalisation: the term 'permissionless' has become an ideological and cultural catchcry which is applied so generally that it loses its original meaning. It has evolved from its specific application in the technical architecture of open networking to mean 'all things that are without permission'.

Conclusion_

We have shown that "permissionlessness" can be conceptualised as a technical attribute, an ideology, and a cultural value. In practice, any functioning institution, including an institution that constitutes a digital infrastructure must have boundaries (Ostrom, 2005). Permissionless infrastructures are institutions where participation arises from an actor choosing to enter those boundaries, rather than an external authority or institution choosing to admit them. In contrast, participation is necessary but not sufficient for a system to be permissionless. An institution encompassing a digital infrastructure includes participation by way of (i) use of the infrastructure, (ii) contributing to the infrastructure's development, or (iii) engaging in governance of the infrastructure. In order for an infrastructure to be deemed fully *permissionless* in the strongest sense of the word, it must be possible to participate in its use, development, and governance without requiring permission from an authority, by adhering to publicly stated procedures.

References_

- 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. *13th ACM Web Science Conference*, 187–195.
- Bauwens, M. (2009). Class and capital in peer production. *Capital & Class*, *33*(1), 121–141. https://doi.org/10.1177/030981680909700107
- Bauwens, M., & Pazaitis, A. (2019). *P2P Accounting for Planetary Survival: Towards a P2P Infrastructure for a Socially-Just Circular Society*. P2P Foundation, Guerrilla Foundation and Schoepflin Foundation. https://commonstransition.org/wp-content/uploads/2019/09/AccountingForPlanetarySurvival_defx-2.pdf.
- Bouvier, J. (1856). Permission. In *A Law Dictionary, Adapted to the Constitution and Laws of the United States. By John Bouvier.* https://legal-dictionary.thefreedictionary.com/permission
- Brooker, K. (2018, July 1). I was devastated: Tim Berners-Lee, the man who created the world wide web, has some regrets. *Vanity Fair*. https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets#:~:text=August%202018%20Issue-,%E2%80%9CI%20Was%20Devastated%E2%80%9D%3A%20Tim%20Berners%2DLee%2C%20the,a%20plan%20to%20fix%20it.
- Brunton, F. (2019). *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*. Princeton University Press.
- Brunton, F. (2013). *Spam: A Shadow History of the Internet*. The MIT Press.
- Buterin, V. (2017). The Meaning of Decentralization' [Medium]. *@VitalikButerin*. https://medium.com/@VitalikButerin/i-invented-the-term-in-2013-and-daniel-larimer-came-up-with-dacs-s-organization-corporation-a-ef86db1524d5.
- Daigle, L. (2014). Permissionless innovation – openness, not anarchy. *Internet Society*. https://www.internetsociety.org/blog/2014/04/permissionless-innovation-openness-not-anarchy/.
- de la Rouviere, S. (2021). The Moloch DAO: collapsing the firm. *Medium*. https://medium.com/@simondlr/the-moloch-dao-collapsing-the-firm-2a800b3aa2e7.
- Dictionary, M.-W. (2021). *Decentralization*. Merriam-Webster. https://www.merriam-webster.com/dictionary/decentralization.
- Dowding, K. (2016). Albert O. Hirschman, Exit, Voice and Loyalty:

Responses to Decline in Firms, Organizations, and States. In M. Lodge, E. C. Page, & S. J. Balla (Eds.), *The Oxford Handbook of Classics in Public Policy and Administration* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199646135.013.30

- DuPont, Q. (2017). Experiments in algorithmic governance. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains and global governance*. Routledge, Taylor & Francis Group.
- Electronic Frontier Foundation. (2021). *About EFF*. Electronic Frontier Foundation. https://www.eff.org/about
- Fischer, F. (2012). *Participatory Governance: From Theory To Practice*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199560530.013.0032
- Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1556
- Kostakis, V., & Bauwens, M. (2014). *Network Society and Future Scenarios for a Collaborative Economy*. Palgrave Macmillan.
- Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176
- Larimer, D. (2013). The hidden costs of Bitcoin. *LTB Network*. https://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security#.UjtiUt9xy0w.
- Lessig, L. (2009). Against transparency: The perils of openness in government. *The New Republic*. https://newrepublic.com/article/70097/against-transparency.
- Mannan, M. (2020). *Everything old is new again: Evaluating the legal and governance structures of shared-services platform cooperatives*. Institute for Cooperative Digital Economy and the Platform Cooperativism Consortium. https://archive.org/details/morshed-mannan-single -web/mode/1up.
- May, T. C. (1991). *Communication with cypherpunks@toad.com, "Paranoia and Cypherpunks."* https://cypherpunks.venona.com/raw/cyp-1992.txt.
- Nabben, K. (2021). Blockchain security as "people security": Applying sociotechnical security to blockchain technology. *Frontiers in Computer Science*, *2*, 599406. https://doi.org/10.3389/fcomp.2020.599406
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.Org. https://bitcoin.org/en/bitcoin-paper.
- Naughton, J. (2014). 25 things you might not know about the web

on its 25th birthday. *The Guardian*. https://www.theguardian.com/technology/2014/mar/09/25-years-web-tim-berners-lee.
- Neudecker, T., & Hartenstein, H. (2019). Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & Tutorials*, *21*(1), 838–857. https://doi.org/10.1109/COMST.2018.2852480
- Olson, M. C. (1965). *The Logic of Collective Action: Public Goods and the Theory of Groups*. Harvard University Press.
- Ostrom, E. (2005). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.
- Permission. (2000). In *American Heritage Dictionary of the English Language* (Fourth). Houthton Mifflin Harcourt.
- Raymond, E. S. (2000). *The Cathedral and the Bazaar*. http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/.
- Sherman, A. T., Janvani, F., Zhang, H., & Golaszewski, E. (2018). On the origins and variations of Blockchain technologies. *IEEE Security & Privacy*, *17*(1), 72–77. https://doi.org/10.1109/MSEC.2019.2893730
- Stallman, R. (2002). *Free Software, Free Society: Selected Essays of Richard M. Stallman* (J. Gay, Ed.). GNU Press.
- Voshmgir, S., Zargham, M., & Emmett, J. (2021). Conceptual Models for DAO2DAO Relations'. *Medium*. https://medium.com/primedao/conceptual-models-for-dao2dao-relations-ac2b2d3cc84d.
- W3C. (2021). *W3C Standards*. https://www.w3.org/standards/.
- Web Foundation. (2017). *Web inventor Sir Tim Berners-Lee responds to US net neutrality threat*. Web Foundation. https://webfoundation.org/2017/04/sir-tim-berners-lee-responds-to-us-net-neutrality-threat/.
- Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432–1465. https://doi.org/10.1109/COMST.2020.2969706

PERSONAL INFORMATION MANAGEMENT SYSTEMS_

Heleen Janssen, Institute for Information Law, University of Amsterdam, Netherlands.
Jatinder Singh, Compliant and Accountable Systems Research Group, Computer Science & Technology, University of Cambridge, United Kingdom.

Personal Information Management Systems (PIMS) seek to empower users by equipping them with mechanisms for mediating, monitoring and controlling how their data is accessed, used, or shared.

Context_

There are growing concerns regarding the opacity concerning how data is being processed and (mis)used, where individuals typically lack meaningful transparency, visibility and control over what, how, why and by whom their data are captured, analysed, transferred, stored, or otherwise processed and used (Zuboff, 2015; Lehtiniemi 2017; Berners Lee, 2018). In response, and in line with the growing public discourse regarding data-related issues, PIMS as a concept generally aims to better inform and empower users with regards to the processing of their data (Royal Society, 2019). PIMS are a form of privacy enhancing technology (PET), representing an instance of an approach for *privacy self-management* — whereby users work to manage their own privacy interests (Solove, 2013; Solove, 2020).

Key functionality_

PIMS typically involve an ecosystem, which generally entails a *platform* providing the PIMS infrastructure. The platform provides *users with some* components for handling their personal data. Within this ecosystem, *third parties* seek to process user data (Janssen et al., 2020b). PIMS employ technical, legal and organisational measures that enable users to manage and control their data, and to ensure and validate that the behaviours of third-parties accord with user and platform requirements. Though the specifics of which vary by offering, measures often include (to varying degrees) the ability to determine:

(1) the data collected, captured, stored, or that otherwise available for processing;
(2) that computation, analytics or other processing performed over that data; as well as providing
(3) oversight measures to validate, review and audit what happens to their data.

PIMS often enable *decentralised* data processing, where third-parties that wish to process user data will not directly access a user's data (e.g. where user data are transferred to the third party). Instead, such mechanisms enable the third-party's desired computation, analytics, or other processing to be brought to the user's data (typically residing within a physical or virtual user-centric PIMS *device*), with only the results of that processing returned to the third-party (Janssen et al., 2020a). This (as with other forms of processing) occurs in line with a user's agreement, and only over certain data, as determined by the user.

PIMS may be supported by other novel technologies, such as Distributed Ledgers (Zichichi et al., 2020; see separate entry regarding DLTs).

Origins and coexisting uses/meanings_

The term PIMS is not novel; some older references to the term can be found, for instance, in Barreau, 1995; Jones & Thomas, 1997; Bergman et al., 2008. Nowadays, the term 'PIMS' broadly refers to a class of technology that provides users with means for managing their data *vis-à-vis* those wishing to process it. Note that PIMS is an 'umbrella term', and we see a range of related terms used including: *personal data stores* (World Economic Forum, 2013; De Montjoye et al., 2014; OpenPDS, 2017; Crabtree et al., 2018; Royal Society, 2019; Janssen et al., 2020a); *personal data vaults* (Schluss, n.d.); *personal information management services* (ControlShift, 2014), or *personal data spaces* (European Commission, 2020). The concepts also bear a relationship with some forms of data intermediary (see separate entry regarding "Data intermediary").

PIMS have been proposed by actors in civil society (MyData movement, 2015); academia, where offerings such as OpenPDS or Databox were developed; the private sector (some examples include CozyCloud; Mydex; CitizenMe, or Digi.me), or by actors in research environments with the

PIMS developing into a commercial offering (Dataswift/Hub of All Things, or Solid/Inrupt, the latter being developed by Sir Tim Berners Lee). PIMS are increasingly gaining attention from policymakers, who currently consider mechanisms for regulating and advancing data intermediation services in general, of which PIMS are one example (e.g. European Commission Data Strategy, 2020; European Commission proposal for a Data Governance Act, 2020; German Bundestag bill for Consent Management Services, 2021; Centre for Data Ethics and Innovation (an expert body of UK's government Department for Digital, Culture, Media and Sports, 2021)).

Debate_

PIMS generally adopt an approach that is firmly grounded in the logic of privacy self-management and 'notice and consent', whereby users are charged with managing their own privacy interests (Solove, 2013; Solove, 2020; Janssen et al., 2020b). However, such approaches are the subject of critique, with arguments that they are largely ineffective given the systemic issues inherent in digital ecosystems, such as those regarding power and information asymmetries (Barocas & Nissenbaum, 2009; Sloan & Warner, 2013; Bietti, 2020).

Although some forecasted that PIMS could generate considerable economic benefits for businesses and consumers alike (ControlShift, 2014; Brochot et al., 2015; European Commission, 2020), the business cases for PIMS platforms vary and continue to be developed (Bolychevsky & Worthington, 2018).

Conclusion_

Personal Information Management Systems (PIMS) aim to inform and empower users by equipping them with mechanisms for mediating, monitoring and controlling how their data is accessed, used, or shared. Their purpose is to provide an alternative to the data processing practices common today. PIMS are growing in prominence with many offerings in the pipeline. While gaining attention from developers, researchers, industry and policymakers, questions over the business cases and the ability for PIMS to overcome the systemic issues in digital ecosystems remain.

References_

- Abiteboul, S., André, B., & Kaplan, D. (2015). Managing your digital life. *Communications of the ACM*, *58*(5), 32–35. https://doi.org/10.1145/2670528
- Barocas, S., & Nissenbaum, H. (2009). On notice: The trouble with notice and consent. *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*. https://ssrn.com/abstract=2567409
- Barreau, D. K. (1995). Context as a factor in personal information management systems. *Journal of the American Society for Information Science and Technology*, *46*(5), 327–339.
- Bergman, O., Beyth-Marom, R., & Nachmias, R. (2008). The user-subjective approach to personal information management systems design: Evidence and implementations. *Journal of the American Society for Information Science and Technology*, *59*(2), 235–246. https://doi.org/10.1002/asi.20738
- Berners Lee, T. (2018). *One small step for the Web...* [Open letter]. Inrupt. https://inrupt.com/blog/one-small-step-for-the-web
- Bietti, E. (2020). Consent as a free pass: Platform power and the limits of the informational turn. *Pace Law Review*, *40*, 317–398.
- Bolychevsky, I., & Worthington, S. (2018). Are Personal Data Stores about to become the NEXT BIG THING? [Medium]. *Irina Bolychevsky*.
- Brochot, G., Brunini, J., Eisma, F., Larsen, R., & Lewis, D. J. (2015). *European Commission: Personal Data Store* (MPhil Technology Policy) [Final report]. University of Cambridge. https://www.academia.edu/20193979/European_Commission_Report_on_Personal_Data_Stores
- Centre for Data Ethics and Innovation. (2021). *Unlocking the value of data:Exploring the role of data intermediaries* (Report Commissioned by the UK Government's Department for Digital, Culture, Media and Sport (DCMS)) [Report]. Centre for Data Ethics and Innovation. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf
- ControlShift. (2014). *Personal Information Management Systems – an analysis of an emerging market: Unleashing the power of trust*. ControlShift. https://www.ctrl-shift.co.uk/insights/2014/06/16/personal-information-management-services-an-analysis-of-an-emerging-market/

- Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., Amar, Y., Mortier, R., Li, Q., Moore, J., Wang, L., Yadav, P., Zhao, J., Brown, A., Urquhart, L., & McAuley, D. (2018). Building accountability into the Internet of Things: The IoT Databox model. *Journal of Reliable Intelligent Environments*, *4*(1), 39–55. https://doi.org/10.1007/s40860-018-0054-5
- de Montjoye, Y.-A., Shmueli, E., Wang, S. S., & Pentland, A. S. (2014). openPDS: Protecting the Privacy of Metadata through SafeAnswers. *PLoS ONE*, *9*(7), e98790. https://doi.org/10.1371/journal.pone.0098790
- European Commission. (2020). *A European Strategy for data COM/2020/66 final*. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066
- European Data Protection Supervisor. (2016). *EDPS Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data*. https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
- European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
- *German Bundestag Bill for Consent Management Services: § 26 TTDSG Approved Consent Management Services, End User Preferences*, German Bundestag (2021). https://dsgvo-gesetz.de/ttdsg/26-ttdsg/
- International Association of Privacy Professionals. (2019). Personal information management systems: A new era for individual privacy? *iapp*. https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy/
- Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020a). Decentralised data processing: Personal data stores and the GDPR. *International Data Privacy Law*, *10*(4), 356–384. https://doi.org/10.1093/idpl/ipaa016
- Janssen, H., Cobbe, J., & Singh, J. (2020b). Personal information management systems: A user-centric privacy utopia? *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1536
- Jones, S. R., & Thomas, P. J. (1997). Empirical assessment of individuals' "personal information management systems." *Behaviour & Information Technology*, *16*(3), 158–160. https://doi.org/10.1080/014492997119888

- Lehtiniemi, T. (2017). Personal Data Spaces: An Intervention in Surveillance Capitalism? *Surveillance & Society*, *15*(5), 626–639. https://doi.org/10.24908/ss.v15i5.6424
- Royal Society (Great Britain). (2019). *Protecting privacy in practice: The current use, development and limits of privacy enhancing technologies in data analysis.*
- Schluss. (n.d.). *Schluss*. https://schluss.org
- Sloan, R. H., & Warner, R. (2013). Beyond notice and choice: Privacy, norms, and consent. *Journal of High Technology Law*, *14*, 370.
- Solove, D. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1888–1903.
- Solove, D. J. (2020). The myth of the privacy paradox. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3536265
- World Economic Forum & The Boston Consulting Group. (2013). *Unlocking the value of personal data: From collection to usage*. World Economic Forum. http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf
- Zichichi, M., Ferretti, S., & D'Angelo, G. (2020). On the efficiency of decentralized file storage for personal information management systems. *2020 IEEE Symposium on Computers and Communications (ISCC)*, 1–6.
- Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

PROTOCOL_

Gerd Beuster, University of Applied Sciences Wedel, Hamburg, Germany.
Oliver Leistert, Leuphana Universität Lüneburg, Germany.
Theo Röhle, Department of Journalism, Media and Communication, University of Gothenburg, Sweden.

Protocol describes a cascade of formalised standards or agreements to be implemented as control regimes for flexible material and/or semiotic organisation. It predictably structures in an often layered, sometimes hierarchical way the behaviours of data and objects to participate in infrastructural networks. Protocol is defining all possible operations on its coded objects based on rules, albeit being able to incorporate important differences of inputs. While 'protocol' may refer specifically to internet protocols, it also describes a mode of organisation evident in a variety of technical and non-technical settings.

Origin and evolution of the term_

Protokollon, a middle greek composite (protos / first and kolla / glue), was a protective paper, or flyleaf, that was glued to subsequent files or documents and usually contained a bibliographic record of some sort. It certified the authenticity and validity of the documents, thereby producing the *acta* or legal files (Vismann, 2008). In this sense, it can be considered an early techno-social system of administration that has functional equivalents from Antiquity up until today.

Protocol authorises and validates acts of administration (Crabu, 2014; Niehaus & Schmidt-Hannisa, 2005), a property that makes it performative. The effect is a formally defined authoritatively coded, i.e. written, record of what has happened: Quod non est in actis non est in mundo. Protocol registers and verifies the administration of what is or has been, letting protocol interface with ontopowers (Massumi, 2015). As protocols code e.g. knowledge in their specific ways, a protocological conflict of "translation across the milieu of knowledge" (Rossiter, 2016, pp. 96ff) can occur.

As a text type for the judiciary, protocol makes interrogations admissible, transforming an ephemeral, spoken statement into a fixed, written one. Here, protocol is a precondition for a commonly shared authoritative record of events from the past. Further, a protocol is simultaneous to the events it records, gaining its authority (a) from this presentist, co-emergence with the spoken act, and (b) through formal criteria (Vismann, 2008, pp. 53–55). A major protocological concern is to reach a certified consensus about what happens or has happened, a purpose that historically has been supported by different media technologies.

In diplomacy, protocol encompasses control over the totality of all forms of conduct to eliminate any mishaps potentially causing tensions between governments. In the sciences, a protocol formalises a scientific experiment, prescribing procedures to follow and materials to use in order to support the replication processes for the testing of a hypothesis. Different branches of science vary in their protocological practice, as they vary in their experimental practice. Scientific protocols are rarely as standardised as technical protocols, but need to include all the necessary information for obtaining consistent results. By invoking orderly, rule-based processes, often independent from time and place, protocols can be understood as relational and infra-structuring. In very general terms, all institutions are dependent on protocols and standards to achieve representative comparability of worldly events (Bowker & Star, 2000). However, the processes of protocol construction in relation to scientific practices remain an open research question for STS (Crabu, 2014).

When the *act* of executing a protocol is taken into account, there remains a strong resemblance between the persons manually producing *acta* / files, and computers executing protocols, because both produce formatted, encoded data.

Internet protocols_

Technically speaking, internet protocols "regulate the communication of geographically distributed program objects" (Popovic, 2018, p. 6). When the humanities and social sciences have engaged with the nature of this regulation, they have primarily focused on the relationship between control and decentralisation. A core claim has been that the TCP/IP suite, including simple forwarding rules and the end-to-end principle,

has inherently decentralising qualities, thus representing new distributed forms of power relations (Galloway & Thacker, 2004; Galloway, 2004). On the other hand, it has been pointed out that the "standards war" between TCP/IP and Open Systems Interconnection (OSI) in the late 1980s and early 1990s highlights the role of centralised control for enabling interoperability in large-scale internetworking (Blanchette, 2011; Russell, 2014).

Based on empirical accounts of engineering discourses and their historical developments (e.g. Abbate, 1999; de Nardis, 2009; Gillespie, 2006), recent investigations have broadened the outlook towards different varieties of control mechanisms involved in internet traffic management, such as *Deep Packet Inspection* and *Quality of Service* (McKelvey, 2018). Routing has been singled out as an especially relevant problem when it comes to protocological control, since it relies on shared information about network topology, with different routing strategies involving apparent trade-offs between efficiency and centralisation (Dourish, 2015). For example, the Exterior Gateway Protocol introduced the concept of autonomous networks and enabled communication between them, but also paved the way for the dominance of TCP/IP across these networks. The introduction of the Border Gateway Protocol allowed for a broadening of the Arpanet-dominated routing hierarchy, but it implied a transfer of centralised control rather than its dispersion (Fidler, 2019). The fact that routing decisions at the edges rely on information obtained from centralised databases, such as the Routing Assets Database or Internet Route Registries, means that measures of network topology and routing criteria need to be standardised and coordinated (Mathew, 2016).

Internet security protocols_

In IT generally, security protocols guarantee that information exchanged by two or more parties is received and interpreted correctly by the intended party or parties. These requirements can be described by properties of the protocol. In respect to security, the core properties are the "Security Triad" of (1) confidentiality of information, (2) integrity (the information cannot be altered), and (3) availability (information is available to legitimate parties when needed) (National Institute of Standards and Technology, 2004). While these are the core security properties, they may not be present in all protocols (for example, confidentiality may not be required).

Also, additional properties may be required in certain protocols, for example non-repudiation (a party cannot deny a communication act), anonymity, or authenticity. Cryptographic methods are such an essential element of security protocols that the terms "security protocols" and "cryptographic protocols" are often used synonymously in IT (e.g., Dong & Chen, 2012, p. 1).

Security protocols are employed in communications where at least one of the parties, including external parties, may violate at least one of the principles critical in the communication context. Without a security protocol, these kinds of interactions require trust in the honesty of the parties. Depending on the semantics of the term trust, the goal of security protocols is to reduce the amount of trust required (Ferguson et al., 2010, p. 217) or to establish trust (Anderson, 2020, p. 125). Ideally, a security protocol guarantees the relevant principles even if the attacker(s) can manipulate the communication channel at will, i.e. they can receive, create, drop, and manipulate all messages transmitted (Dolev & Yao, 1983, p. 199).

Ideally, security protocols are formally defined and verified, i.e. the security protocol is defined in mathematical terms, and a formal proof of the maintenance of the security properties is provided. These proofs hold under certain assumptions about the context of the protocol, like the environment and properties of the cryptographic primitives used. Therefore, even verified security protocols may fail (Anderson, 2020, pp. 145-146).

Blockchain protocols_

With open, distributed ledger systems, like bitcoin (Nakamoto, 2008), blockchain protocols are most importantly concerned with the reaching of a consensus among the networking peers for system reliability. To reach consensus, mechanisms of incentivising the partaking peers have shown good enough results for such systems to remain reliable over time (Bano et al., 2017; Tasca & Tessone, 2019). Adversarial assumptions are the baseline of all such protocols.

Without a central routing authority, *gossiping* between connected peers remains a robust but rather slow way of information propagation within

the network (Birman, 2007). In return, a slow propagation poses the problem of only partial synchrony within the network (Dwork et al., 1988), such that a computation has to probabilistically end, when a deterministic ending is not viable (Bracha & Toueg, 1985). What is more, the "Byzantine Generals Problem" formulated in the early 1980s (Lamport et al., 1982) specifies conditions to be fulfilled for a distributed system to reliably communicate among its peers while tolerating some presence of faulty acting nodes (without knowing about it).

Mathematical game theory formalises the behaviour of actors in such a system and can show the parameters in which their behaviour is supportive to the system (Liu et al., 2019). The security of permissionless blockchain protocols depend on a (single or coordinated group of) malicious actor(s) not being able to control more than 50 % of a certain resource. In proof-of-work blockchains like bitcoin, this resource is (spent) computational power; the participants attempt to solve a cryptographic puzzle by brute force, called mining. This drove bitcoin into a hardware arms race and a power consumption amount that can hardly be justified. *Proof-of-stake* systems, such as Cardano (David et al., 2018; Kieran, 2020), abstract the consensus mechanism towards financial powers. The resource here is the system's asset itself (Brünjes et al., 2020). In both cases, the system's own asset is used to incentivize the honest nodes of the system, thus the system's stability depends on a commonly shared valuation of that asset.

No matter which consensus protocol, the processes it governs always include block proposal, block validation, information propagation, block finalisation, and incentive mechanism (Xiao et al., 2020).

Issues currently associated with the term_

In the humanities and social sciences, the focus of the debate has shifted from abstract claims about inherent political properties of internet protocols to contextualised accounts of specific protocols involved in internet governance and operation (de Nardis et al., 2020; ten Oever, 2021). This includes increased consideration of social factors, institutional procedures and material aspects of internet infrastructure. The general thrust of the debate has thus moved towards identifying historically emergent and contingent structures of control triggered by protocol

developments, including more elaborate investigations of decentralising and centralising aspects.

In the blockchain space, much like "decentralisation" (Bodó et al., 2021), "protocol" has become a charged concept in discussion around governance. Since a blockchain protocol organises the production of the chain by way of achieving an indisputable consensus among the block producing nodes, the relation between onchain and offchain governance has become the focal point of an intense debate (Reijers et al., 2021). A first emblematic expression of this dispute was a contested and unplanned Ethereum fork that divided the Ethereum community, following the hack of "The DAO" (DuPont, 2018). One camp resisted upgrades to the protocol that could have mitigated the hack, claiming that what the protocol does is what everyone has agreed upon, and nothing else.

The idea that protocols from distributed computing systems may serve as blueprints for societal issues and problem solving has been criticised and the productivity of a dissensus concerning consensus protocols has been brought to the fore (Brekke et al., 2021). At the same time, a semantic ambivalence on the concept of trust in this context has been highlighted, providing new semantics ("confidence machine") in order to better locate the problematic of trust (DeFilippi et al., 2020; see also Werbach, 2018).

Misconceptions and biases in the discussion around the term_

In the narrower meaning of computer protocols, it is important to differentiate (1) protocols as descriptions of the precise terms by which computers can communicate, (2) an implementation as the creation of software that uses a protocol, and (3) a standard as the definition which protocol should be used for what purposes (Kelty, 2008, p. 166). A further aspect has been termed "embodiment" (Dourish, 2015): the running implementation in a concrete setting that affects a protocol's operations and possible issues, e.g. of scaling. Although these issues can be modelled and simulated to some degree beforehand, a running instance of a protocol provides further analytical insights into the complexity of its materiality.

In abstract terms, protocols are content agnostic to some degree (Galloway & Thacker, 2007, p. 47), qualifying them as quasi-universal (Galloway,

2004). The flip side here is that all non-coded or non-codable life-forms, objects, or data can not exist under protocological control (Mejias, 2013, p. 114).

Conclusion_

From ancient administration to the judiciary to diplomacy to scientific practices to internet engineering, protocols invoke an orderly, rule-based, coding process of certification, producing a truth or state agreed upon, whether between people or machines. Protocols abstract from historical contexts, objectify and exclusively define all possible operational relations among such objectified entities. This naturally causes issues of interoperability between different protocols. Protocols are robust and quasi-universal. Once operationalised in infrastructures, protocols act immanently conservative and upgrades transcending its encoded rules, such as new functionalities, often must be invoked from the outside, by way of non-protocologically defined mechanisms. Technical protocols are usually cascades of formalised standards or agreements.

References_

- Abbate, J. (1999). *Inventing the Internet*. MIT Press.
- Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
- Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2019). SoK: Consensus in the age of blockchains. *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 183–198. https://doi.org/10.1145/3318041.3355458
- Birman, K. (2007). The promise, and limitations, of gossip protocols. *ACM SIGOPS Operating Systems Review*, *41*(5), 8–13. https://doi.org/10.1145/1317379.1317382
- Blanchette, J.-F. (2011). A material history of bits. *Journal of the American Society for Information Science and Technology*, *62*(6), 1042–1057. https://doi.org/10.1002/asi.21542
- Bodó, B., Brekke, J. K., & Hoepman, J.-H. (2021). Decentralisation: A multidisciplinary perspective. *Internet Policy Review*, *10*(2). https://policyreview.info/concepts/decentralisation
- Bowker, G. C., & Star, S. L. (2000). *Sorting Things Out: Classification and Its Consequences*. MIT Press.

- Bracha, G., & Toueg, S. (1985). Asynchronous consensus and broadcast protocols. *Journal of the ACM*, *32*(4), 824–840. https://doi.org/10.1145/4221.214134
- Brekke, J. K., Beecroft, K., & Pick, F. (2021). The dissensus protocol: Governing differences in online peer communities. *Frontiers in Human Dynamics*, *3*, 641731. https://doi.org/10.3389/fhumd.2021.641731
- Brünjes, L., Kiayias, A., Koutsoupias, E., & Stouka, A.-P. (2020). Reward sharing schemes for stake pools. *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, 256–275. https://doi.org/10.1109/EuroSP48549.2020.00024
- Crabu, S. (2014). Give us a protocol and we will rise a lab: The shaping of infra-structuring objects. In A. Mongili, G. Pellegrino, & G. C. Bowker (Eds.), *Information Infrastructure(s): Boundaries, Ecologies, Multiplicity* (pp. 121–143). Cambridge Scholars Publishing.
- David, B., Gaži, P., Kiayias, A., & Russell, A. (2018). Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In J. B. Nielsen & V. Rijmen (Eds.), *Advances in Cryptology – EUROCRYPT 2018* (Vol. 10821, pp. 66–98). Springer International Publishing. https://doi.org/10.1007/978-3-319-78375-8_3
- De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*, 101284. https://doi.org/10.1016/j.techsoc.2020.101284
- DeNardis, L. (2009). *Protocol Politics: The globalization of Internet Governance*. MIT Press.
- DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (Eds.). (2020). *Researching Internet Governance: Methods, Frameworks, Futures*. MIT Press.
- Dolev, D., & Yao, A. C. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208.
- Dong, L., & Chen, K. (2012). *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*. Springer.
- Dourish, P. (2015). Protocols, packets, and proximity. In L. Parks & N. Starosielski (Eds.), *Signal Traffic: Critical Studies of Media Infrastructures* (pp. 183–204). University of Illinois Press.
- DuPont, Q. (2018). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In M. Campbell-Verduyn (Ed.), *Bitcoin and Beyond* (pp. 157–177). Routledge.

- DuPont, Q. (2019). *Cryptocurrencies and Blockchains*. Polity.
- Dwork, C., Lynch, N., & Stockmeyer, L. (1988). Consensus in the presence of partial synchrony. *Journal of the ACM*, *35*(2), 288–323. https://doi.org/10.1145/42282.42283
- Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
- Fidler, B. (2019). The evolution of internet routing: Technical roots of the network society. *Internet Histories*, *3*(3–4), 364–387. https://doi.org/10.1080/24701475.2019.1661583
- Galloway, A. R. (2004). *Protocol: How Control Exists After Decentralization*. MIT Press.
- Galloway, A., & Thacker, E. (2004). Protocol, control, and networks. *Grey Room*, *17*(10).
- Gillespie, T. (2006). Engineering a principle: 'End-to-end' in the design of the Internet. *Social Studies of Science*, *36*(3), 427–457. https://doi.org/10.1177/0306312706056047
- Kelty, C. M. (2008). *Two Bits: The Cultural Significance of Free Software*. Duke University Press.
- Kieran, C. (2020, March 23). From Classic to Hydra: The implementations of Ouroboros explained. *IOHK Blog*. https://iohk.io/en/blog/posts/2020/03/23/from-classic-to-hydra-the-implementations-of-ouroboros-explained/
- Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176
- Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y.-C., & Kim, D. I. (2019). A survey on blockchain: A game theoretical perspective. *IEEE Access*, *7*, 47615–47643. https://doi.org/10.1109/ACCESS.2019.2909924
- Massumi, B. (2015). *Ontopower: War, Powers, and the State of Perception*. Duke University Press.
- Mathew, A. J. (2016). The myth of the decentralised internet. *Internet Policy Review*, *5*(3). https://policyreview.info/articles/analysis/myth-decentralised-internet
- McKelvey, F. (2018). *Internet Daemons: Digital Communications Possessed*. University of Minnesota Press.
- Mejias, U. A. (2013). *Off the Network: Disrupting the Digital World*. University of Minnesota Press.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

https://bitcoin.org/en/bitcoin-paper
- National Institute of Standards and Technology. (2004). *Standards for security categorization of federal information and information systems* (NIST FIPS 199; p. NIST FIPS 199). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.199
- Niehaus, M., & Schmidt-Hannisa, H.-W. (Eds.). (2005). Textsorte Protokoll. Ein Aufriß. In *Das Protokoll: Kulturelle Funktion einer Textsorte* (pp. 7–23). Peter Lang GmbH.
- Popović, M. (2018). *Communication Protocol Engineering* (Second). CRC Press.
- Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Cubillos Vélez, A., & Orgad, L. (2021). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi*, *40*(4), 821–831. https://doi.org/10.1007/s11245-018-9626-5
- Russell, A. L. (2014). *Open Standards and the Digital Age: History, Ideology, and Networks*. Cambridge University Press.
- Tasca, P., & Tessone, C. J. (2019). A taxonomy of blockchain technologies: Principles of identification and classification. *Ledger*, *4*. https://doi.org/10.5195/ledger.2019.140
- ten Oever, N. (2021). "This is not how we imagined it": Technological affordances, economic drivers, and the Internet architecture imaginary. *New Media & Society*, *23*(2), 344–362. https://doi.org/10.1177/1461444820929320
- Vismann, C. (2008). *Files: Law and Media Technology*. Stanford University Press.
- Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.
- Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for Blockchain networks. *ArXiv*. https://arxiv.org/abs/1904.04098v1

REPUTATION_

Primavera De Filippi, CERSA, CNRS, Paris, France. Harvard University's Berkman Klein Center for Internet and Society, United States.
Ori Shimony, Research and Development, dOrg, United States.
Ámbar Tenorio Fornés, GRASIA, Universidad Complutense de Madrid, Spain.

Reputation in a blockchain-based system is a digital representation of an entity's standing or status in a specific domain.

Origin_

Technologies such as the internet, or blockchain, enable large scale interactions among total strangers. Reputation systems (Resnick et al., 2000) appeared as a solution to facilitate these interactions when some level of trust was required, such as in online shopping in peer to peer marketplaces like eBay, or online production communities (Benkler, 2006). Yet, these systems generally relied on a centralised operator, in charge of managing user reputation.

There are several decentralised reputation systems (Hendrikx, 2015), most relying either on maintaining a personal list of trusted and untrusted nodes; aggregating such reputation information from other trusted nodes (with certain degree of transitivity such as in web-of-trust); or using Distributed Hash Tables to manage a global directory of semi-trusted nodes (Chawathe et al., 2003).

Blockchain technology introduces the possibility for a next generation of reputation systems that utilise persistent global state and immutable transaction histories. This allows for transparency and security guarantees that were unavailable in previous distributed systems. Furthermore, the openness and persistence of blockchains makes them a valuable tool to support shared data stores that can be leveraged by multiple services, thereby enhancing reputation portability and interoperability.

Evolution_

Bitcoin (Nakamoro, 2009) relied on blockchain technology to create a distributed payment system operating on top of a peer-to-peer network. The operations of Bitcoin did not rely on trust or reputation. Instead, the influence of every network node is determined by the amount of resources engaged into the network: the greater the amount of resources, the more influence one has in the network. Many of the other blockchain-based networks that followed suit relied on similar protocols, also based on a resource-driven model (i.e. the amount of hashing power in the case of Proof-of-Work or the amount of tokens holding in the case of Proof-of-Stake).

Early reputation systems have been implemented at the infrastructure layer, as trust-based alternatives to the Proof-of-Work or Proof-of-Stake consensus algorithm. For instance, delegated Proof-of-Stake (Larimer, 2014) allows for a more meritocratic system, based on merit or perceived trustworthiness. As a result, anyone holding a particular amount of reputation within a blockchain community will have influence in proportion to the amount of reputation they hold.

At the application layer, the introduction of "reputation" in the blockchain space was also an attempt to move away from the perception of blockchain technology as a purely trustless system, to enable the establishment of more sophisticated systems where some actors *can* be trusted. As argued by Hawlitschek and colleagues (Hawlitschek et al., 2018), the introduction of "reputation" is necessary for the establishment of trustless systems that operationally rely on trust. On the one hand, trustless systems such as Bitcoin are based on the assumption that no one *can* or *shall* be trusted. Hence, these systems are designed to entirely eliminate the need for trust, relying on cryptographic primitives and proofs in order to ensure that people behave according to the rules (Ali et al., 2016). On the other hand, there are many human-sensitive services (e.g., peer-to-peer marketplaces like Uber, Airbnb, or eBay) based on the assumption that some actors can be trusted to behave honestly. These systems rely on "reputation" in order to help users assess the trustworthiness of the other users interacting on these platforms. In order to provide these types of human-sensitive mediation services, blockchain-based applications need to also rely on some kind of reputation system.

Coexisting uses/meanings_

Existing blockchain reputation systems vary widely in how reputation is earned and utilised. In many blockchain-based marketplaces, reputation does not have an explicit or software-defined role, but acts as a signal of trustworthiness. For instance, in service marketplaces (Gitcoin, Bounties Network), users can decide who to hire or work for based on transaction histories and summary statistics. Similarly, in digital goods marketplaces (Rarible, OpenSea), a buyer can review the seller's transaction history to evaluate the quality of goods for sale before making a purchase.

In blockchain-based social media (Steemit, Hive, Sapien, Relevant) and work networks (Colony, Sourcecred), reputation represents a user's evaluation weight on other users' contributions. Reputation can be global in scope or limited to a specific community or domain. Evaluation-weighting alters reputation dynamically, as users continuously influence each other's reputation scores in proportion to their own reputation. Some systems also incorporate time-based mechanisms to decay reputation with inactivity.

In blockchain-based governance frameworks (Aragon, DAOstack, Moloch), reputation often determines a user's voting weight on proposals in a given organisation. Reputation can also entitle the user to a proportional claim of the organisation's assets or ongoing revenues. Reputation is often modified through community voting, where the votes of community members are weighted by their reputation (e.g. a community can vote whether to give 50 reputation points to Alice or remove 100 reputation points from Bob). Just as in social media cases, reputation can also be modified by dynamic criteria stipulated by the community, such as reputation rewards for voting with the majority, creating proposals that pass, or reputation penalties for the reverse.

Issues currently associated with the term_

A. Different types of reputation_

First of all, it is important to distinguish between two different types of reputation systems: "personal" and "global" reputation systems (Hendrikx, 2015).

Personal reputation systems are specific to an individual. They represent the standard mechanism of peer-to-peer reputation assignment. These systems are designed to assign a personal reputation score to each member of a particular network or community, although such a score will ultimately be relevant only to one specific individual. Hence, these systems necessarily rely on direct user input: users are expected to score each of their interactions with other community members, in order to help the system compute their corresponding reputation score. However, these systems often suffer from scalability issues. Indeed, the purpose of a reputation system is to provide information about the qualities of different users in a given domain, so that other users can make informed decisions about who they wish to interact with. Yet, a personal reputation system has limited capacity to do so, because it is not possible (or too costly) for a single user to evaluate the qualities of all the users in the system. In order to overcome this limitations, many of these reputation systems often implement a "web of trust" mechanism, leveraging the information submitted by other people (who are regarded as trustworthy by the user) in order to compute the personal reputation score of those with whom such user did not yet have a sufficient amount of interaction.

Global reputation systems are not specific to any community member, but rather to the community as a whole. These systems assign a single and unique reputation score to the different actors in a particular community or network, which will be regarded by all community members as the sole and legitimate score. These reputation systems are rather easy to implement in a centralised platform; they are much more difficult to implement in a decentralised setting, since they require highly sophisticated mechanisms of reputation transfer that will not fall prey to Sybil attacks, where anyone can create multiple pseudonymous accounts to gain disproportionate influence over the system.

It is important to note that both personal and global reputation systems suffer from specific limitations, although to different degrees. First of all, there is the problem of reputation being reduced to a single measure or score, which might not properly reflect the preferences of individual communities. Such a problem is particularly relevant in the context of global reputation systems, which are designed to average reputation into a particular score, even if values are highly heterogeneous within the community of reference. Yet, it also subsists in the context of personal

reputation systems that rely on a broader web-of-trust mechanism. Second, both global and personal reputation systems might suffer from an excessive lack of granularity, to the extent that they do not differentiate between defined characteristics or properties (e.g., reputation associated with a particular skillest, as opposed to a generic reputation score). Finally — and relatedly — reputation valuations can be based on objectively quantifiable facts, as much as subjective opinions. Mixing the two can lead to misleading aggregate reputation signals.

B. Sybill attacks and identity_

Unlike popular online services, decentralised systems have no central party to verify user identities, ban fake accounts, or patrol spam. While beneficial for privacy, this opens the door to Sybil attacks. While decentralised sybil-proof reputation systems have long been regarded as a theoretical impossibility (Cheng & Friedman, 2005), blockchain-based reputation systems might overcome these challenges (Almasoud et al., 2020).

One approach is to minimise the possibility of users leveraging multiple accounts by relying on centralised or decentralised identity systems — also known as "proof of personhood" (Siddarth et al., 2020). Decentralised identity systems often rely on web-of-trust models, where a small set of users slowly invites more users to be peer-verified over time (Liu et al., 2020), or on credential-based models, where users can prove their uniqueness by collecting attestations about their identity from trusted third parties (Wang & De Filippi, 2020).

Alternatively, reputation systems can be leveraged to avoid the need of identifying users. In that model, users need to accumulate a certain degree of reputation within a particular blockchain-based system in order to influence the operation of that system (in proportion to the reputation they hold), and — potentially — assign reputation to other users of the system (Almasoud et al., 2020). Because of the proportionality between reputation and influence, an individual has to contribute just as much value, regardless of how many accounts they spread the effort over, so there is no added incentive for Sybil attacks (Pazaitis et al., 2017).

C. Privacy_

In light of its attributes of transparency, censor-resistance, and immutability, blockchain technology can be instrumental to the operations of both personal and global reputation systems, enabling anyone to access and retrieve these scores, in order to compute both a personal and a global reputation score.

However, in order to protect the privacy of users, the reputation system should avoid permanently registering in a blockchain the association between real-world identities and the identities of the reputation system. In addition, users should be aware of the risks of linking real-world identities to their blockchain accounts. Maintaining this separation makes it possible for users to protect their privacy while allowing for anyone interacting within their blockchain-based identity to evaluate the risks of each user in that domain.

This is especially relevant in light of the new European General Data Protection Regulation, which provides users with the possibility to request the erasure of specific information deemed inaccurate, inappropriate, or obsolete. Given the immutability of a blockchain, the recording of any type of data that can affect the reputation of a particular persona would potentially violate the provisions of the law, insofar as the persona can be linked back to a real-world identity.

D. Oligarchies and power distribution_

The use of reputation systems also raises concerns about power concentration. The creation and consolidation of oligarchies are common in online communities. However, reputation systems might reinforce inequalities in such communities, as powerful actors are more likely to be trusted and increase their reputation while those with low reputation will have fewer opportunities to increase their reputation. Blockchain systems use reputation as a source of economic or political power: these options are explicitly made available in many governance frameworks (Aragon, DaoStack, Moloch). Thus, the accumulation of reputation in such blockchain systems might result in even stronger power inequalities than in other online communities.

E. Amplification of social inequalities_

It is worth considering the potential biases reputation systems incorporate and reproduce. First, not all activities or contributions are a source of reputation in online communities (Rozas & Gilbert, 2015). Some activities, such as contributing source code in free software projects are explicitly valued in these systems, while others such as community organising, or affective labour, typically carried by women (Iosub et al., 2014) are often invisible to these reputation systems. These types of biases can trigger new forms of inequalities incorporated directly into the algorithms managing a platform, such as higher work time and lower average wage for women in the so-called gig economy (Barzilay, 2016). We have briefly considered the reproduction of gender inequalities by reputation systems. However, other dimensions of social injustice such as race or class, and their interactions, should also be considered when studying how reputation systems reproduce them.

Conclusion_

Reputation in a blockchain-based system is a digital representation of an entity's standing or status in a specific domain. Reputation is usually derived from aggregated peer-evaluation of the entity's past actions. It can be leveraged both explicitly through functions in the code (voting power, economic rights) or implicitly as a means of signalling an entity's trustworthiness.

References_

- Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). Bootstrapping trust in distributed systems with blockchains. *;;Login:*, *41*(3), 52–58. https://www.usenix.org/publications/login/fall2016/bootstrapping-trust-distributed-systems-blockchains
- Almasoud, A. S., Hussain, F. K., & Hussain, O. K. (2020). Smart contracts for blockchain-based reputation systems: A systematic literature review. *Journal of Network and Computer Applications*, *170*. https://doi.org/10.1016/j.jnca.2020.102814
- Barzilay, A. R., & Ben-David, A. (2016). Platform inequality: Gender in the gig-economy. *Seton Hall Law Rev*, *47*(2), 393–431. https://scholarship.shu.edu/shlr/vol47/iss2/2

- Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.
- Chawathe, Y., Ratnasamy, S., Breslau, L., Lanham, N., & Shenker, S. (2003). Making gnutella-like p2p systems scalable. *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 407–418. https://doi.org/10.1145/863955.864000
- Cheng, A., & Friedman, E. (2005). Sybilproof reputation mechanisms. *Proceedings of the 2005 ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, 128–132. https://doi.org/10.1145/1080192.1080202
- Gai, F., Wang, B., Deng, W., & Peng, W. (2018). Proof of reputation: A reputation-based consensus protocol for peer-to-peer network. *International Conference on Database Systems for Advanced Applications*, 666–681. https://doi.org/10.1007/978-3-319-91458-9_41
- Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005
- Hendrikx, F., Bubendorfer, K., & Chard, R. (2015). Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing*, *75*, 184–197. https://doi.org/10.1016/j.jpdc.2014.08.004
- Iosub, D., Laniado, D., Castillo, C., Morell, M. F., & Kaltenbrunner, A. (2014). Emotions under discussion: Gender, status and communication in online collaboration. *PloS one*, *9*(8). https://doi.org/10.1371/journal.pone.0104880
- Larimer, D. (2014). *Delegated proof of stake (dpos). Bitshares Whitepaper* [White Paper].
- Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, *166*. https://doi.org/10.1016/j.jnca.2020.102731
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- Pazaitis, A., De Filippi, P., & Kostakis, V. (2017). Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. *Technological Forecasting and Social Change*, *125*, 105–115. https://doi.org/10.1016/j.techfore.2017.05.025
- Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM*, *43*(12), 45–48. https://doi.org/10.1145/355112.355122

- Rozas, D., & Gilbert, N. (2015). *Talk is silver, code is gold? Contribution beyond source code in Free/Libre Open Source Software communities* (Working Paper 2015:1). Centre for Research in Social Simulation. https://cress.soc.surrey.ac.uk/web/sites/default/files/publications/working-papers/paper_contribution_beyond_source_code.pdf
- Siddarth, D., Ivliev, S., Siri, S., & Berman, P. (2020). Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-resistance in Proof of Personhood Protocols. *ArXiv*. http://arxiv.org/abs/2008.05300
- Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion, frontiers in blockchain. *Frontiers in Blockchain*.[https://doi.org/10.3389/fbloc.2019.00028

SELF-SOVEREIGN IDENTITY_

Alexandra Giannopoulou, Institute for Information Law (IViR), University of Amsterdam, Netherlands.
Fennie Wang, Dionysus Labs, United States.

The concept of self-sovereign identity (SSI)[1] describes an identity management system created to operate independently of third-party public or private actors, based on decentralised technological architectures, and designed to prioritise user security, privacy, individual autonomy and self-empowerment.

Origin_

Bringing Westphalian state-centred sovereignty to the individual level, SSI emerged from the aspiration of self-determination and of direct *self-governance* (Orgad, 2018, p. 253) for each individual, outside state intervention. Identity is considered foundational for promoting social equality, freedom, democracy, and financial independence (Verhulst & Young, 2018). Originally, *self-sovereign authority* — the ideological progenitor to SSI — referred to '*the actual default design parameter of Human identity, prior to the "registration" process used to inaugurate participation in Society. The act of "registration" implies that an administration process controlled by Society is required for "identity" to exist. This approach contrives Society as the owner of "identity", and the Individual as the outcome of socio-economic administration*' (The Moxy Tongue, 2012). Autonomy is viewed as a determining element of self-sovereignty, ideologically aligning with transcendentalism. According to Trotter (2014, p. 245), '*each of us is owned by the state, which grants leeway (…) to govern and dispose of certain aspects of our bodies and lives*'.

In the race towards digital sovereignty, i.e. '*the ability of individuals to take actions and decisions in a conscious, deliberate and independent manner*' (Pohle & Thiel, 2020) aiming to establish control '*over their data, device, software, hardware, and other technologies*' (Couture & Toupin, 2019, p. 12), identity management is key. Identities and their respective technological infrastructure vices begin to merge, while becoming a resource for the global economy: biometrics are turning into governmental infrastructures and are associated with state-issued identifiers and citizen IDs establishing

citizenship (Lyon, 2008). Behavioural identity is derived from consumer personal data, collected and monetised by private actors. Technical identities are formed by local access control IDs. Health identities start to appear as immunity passports. Financial identity escapes financial institutions and generates value in *fintech* (Westermeier, 2020). Situated within broader digital identity development discussions[2] (United Nations, 2015), control over identity becomes instrumental as individuals, state, and private actors compete for power over its physical and digital expressions.

The concept of SSI has been elaborated as an expression of personal digital sovereignty by Christopher Allen (2016). He used it to describe a principle-based framework that would create a decentralised system of user-centric, self-administered, interoperable digital identities. This system is driven by ten foundational principles, following Kim Cameron's Laws of Identity (2005): 1) Existence, 2) Control, 3) Access, 4) Transparency, 5) Persistence, 6) Portability, 7) Interoperability, 8) Consent, 9) Minimalisation, 10) Protection, that would aim to constitute the (missing) "identity layer" on the internet (Preukschat & Reed, 2021). It embodies a specific vision of decentralised digital identity, separated from pre-existing centralised and federated models, which aims to decouple identity issuance by the state in order to bring it to the full control of the citizen (The Moxy Tongue, 2016). At the minimum, SSI '*makes the citizen entirely responsible for the management, exploitation and protection of one's data*' (Herian, 2019, p. 115). While implementations of its principles vary substantially, it can be said that SSI aims to '*enable a model of identity management that puts individuals at the center of their identity-related transactions, allowing them to manage a host of identifiers and personal information without relying upon any traditional kind of centralized authority*' (Renieris, 2020). This does not imply that the actors responsible for issuing elements of one's identity will be stripped from their privilege[3], but rather that an individual in possession of more identifiers can present all claims correlated to those identifiers '*without having to go through an intermediary*' (Wagner et al., 2018, p. 9).

Evolution_

The use of SSI has been tied to the use of a blockchain. However, SSI is blockchain-adjacent, but not blockchain-dependent. As Cheesman points out, '*[s]ome bemoan the conflation of "true SSI" with ill-defined concepts*

such as "user-centric" digital identity, which may not require blockchain technology or use it to its full imagined, decentralised potential.' (2020, p. 6).

The technical dimension of SSI has so far been anchored in *decentralised identifiers* (DID), *verifiable claims* (VC) and other related standards from the World Wide Web Consortium (W3C), the same internet standards organisation behind the common internet protocols we are familiar with today such as HTML and HTTPS. These decentralised identity standards are a set of technical standards for linking and associating data about an identity-subject together in a persistent and universal manner, such that the identity-subject not only has control over how information is linked and used, but is the owner of the profile, rather than a third-party service provider. Thus, the set of linked data, called attestations or claims, may be globally portable. Attestations may include credentials that grant the identity-subject access rights or privileges, or may include verification of information such as a link to identity documents, professional certifications, credit history, or any other data or information. Every attestation that is linked to an identity-subject must be signed digitally by another identity-subject.

SSI systems may be compatible with a blockchain for documenting and attaching the transactions to each identity-subject's profile. The blockchain would record transactions that include the adding or signing of attestations, the granting or revocation of access privileges, and so on. The blockchain documentation creates a record of the data integrity of a set of information linked to an identity-subject.

SSI hinges on the technical efficiency of its core concepts. For instance, no two people should have the same identifier (*unicity*), whereby the identifier cannot reference more than one identity-subject. This condition can be satisfied through the use of cryptography, i.e. mathematically ensuring that only unique identifiers are issued and preventing them from being reissued. In other cases, such as voting or credit checks for cross leverage, no one person should have more than one identifier (*singularity*), whereby the relationship between the identity-subject and identifier is one-to-one only. This condition may be the most challenging in a pseudonymous and decentralised identity system. In a world which requires singularity of identification, technical tools and/or legal requirements that are exogenous to an SSI system appear to be a solution. The singularity

quality of an identifier and identification system has traditionally been solved through centralised databases, wherein all sources of information can be aggregated to one authority that can cross check whether one identity-subject has multiple identities and identifiers (Wang & De Filippi, 2020).

Coexisting uses/meanings_

As described above, SSI is oftentimes used interchangeably with terms such as decentralised identity and digital identity. While the first two terms refer to a rather similar identity management system, one that applies technological architectures such as the ones mentioned above guided by political and ideological agendas, digital identity represents a broader techno-legal societal shift towards incorporating physical identity values in a digital form. It is supported by a network of legal reforms, and facilitated by technological developments (Sullivan & Berger, 2017).

The management of (physical and digital) identity is subject to national regulation, as an expression of digital state sovereignty (Madiega, 2020). On a European level, several initiatives have been launched with a focus on digital identity services. In its recent communication, the European Commission mentions that '*a universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them. Europeans can also benefit from use of data to improve public as well as private decision-making*' (2020a, p. 11). The 'Digital Finance Strategy for the EU' specifies that '*by 2024, the EU should implement a sound legal framework enabling the use of interoperable digital identity solutions*' (2020b, p. 5), which would bring technological standardisation, interoperability, and broader security in customer/user identification and authentication by financial institutions.

According to the Commission, the promotion and regulation of digital identity is essential in maintaining an *'open, democratic, and sustainable society'*, which is one of the main objectives of this data strategy. For this, trusted and secure interactions are essential. The objective would be to ensure appropriate and interoperable identification and authentication frameworks. Current digital identity reforms are often aligned to SSI for their objective to create user-centric data sovereignty. However, and as

pointed out by Sheldrake, '*although SSI has been scoped, architected and built as technology, it is not merely technology. By definition, it is sociotechnology*' (2020, n.p.).

Issues currently associated with the term_

While there have been considerable reforms that have facilitated the proliferation of (private/public) identity solutions, there remain numerous legal compliance shortcomings in the implementation and generalised adoption of decentralised (self-sovereign) identity.

Specifically, the eIDAS Regulation defines different levels of trust services and provides the regulatory environment that enables the creation of numerous interoperable digital identity solutions (Alamillo, 2020; Schroers, 2018). According to Article 3, electronic identification is '*a material and/or immaterial unit containing person identification data and which is used for authentication for an online service*'. Any form of cross-border digital identity (self-sovereign or not) would have to function within a mutually recognised identity framework between EU member states for authentication and access to electronic services.

In addition, identity providers have to conform to data protection regulation such as the GDPR (Renieris, 2020; Giannopoulou, 2020). Compliance appears to be rather challenging, due to constraints related to the governance, architecture, and the technological design of the identity project. For instance, actor liability of decentralised architectures remains uncertain (Finck, 2019). Similarly, the exercise of data subjects' rights within a self-sovereign identity architecture has yet to be tested, especially with the emergence of new types of trust actors.

Many applicable legal norms are sector-specific. In financial regulation, the Payment Services Directive 2 aims to facilitate financial data sharing in order to expand the technological abilities of the existing financial infrastructures (Westermeier, 2020) and to '*promote innovative mobile and internet payment services*'. Identity and the use of strong authentication technological standards are both key in applying and implementing the aspirations of the European legislator within the financial sector. This is also apparent when reviewing *anti money laundering* (AML) and *know your customer* (KYC) obligations, revised by the AML5 Directive, which require a digital identity that facilitates transparency and accountability

of financial intermediaries. The application of these obligations in the broader cryptocurrency network of actors remains unclear.

Public discourse highlights SSI's foundational goal of placing the identity subject in control of their identity data[4] (user-centric identity), and views SSI solutions as a much needed global infrastructure that would provide documentation to large populations that have none, better integrating them in modern digital society (World Bank Group, 2018; World Economic Forum, 2018). However, there are considerable risks related to the expansion of global SSI systems for purposes such as refugee identification. As pointed out by Cheesman (2020, p. 14), '*the emancipatory potential of decentralised, user-owned modes of identification came into tension with the geopolitical reality of the nation-state system in which states' prerogative is to control the legitimate means of movement – or, indeed, identification*'. The persistent integration of an identity layer cannot account for anonymity nor for the contextual, interpersonal nature of most expressions of our identity (Hopman & M'Charek, 2020). Following a tradition of identification technologies, '*intensified regimes of surveillance, securitisation and control*' (Lyon, 2008; Cheesman, 2020) would tend to emerge, further solidifying existing inequalities (Gstrein & Kochenov, 2020).

There is a rapidly flourishing digital identity market, with previously isolated technological infrastructures converging, and enabling the circulation and commodification of identity-data. While often lauded, the commodification of identity by various private identity providers (Birch, 2014) could result in states competing in an open market for (sovereign) citizens. Finally, as reputation (Mac Sıthigh & Siems, 2019) is becoming essential in producing trust within modern platform-mediated digital services (Bodó, 2020), decentralised identity is regarded as an equalising force between power asymmetries. However, lately, new intermediaries have started to emerge in the field of *decentralised reputation systems*, and with them, comes the potential for a new societal order of surveillance (Foucault, 2004), defined by the consequences of assigning persistent identities to control financial, criminal, and human flows.

Conclusion_

Self-sovereign identity (SSI) is rooted in the belief that individuals have the right to an identity independent of reliance on a third-party identity

provider, such as the state or any other central authority. Its implementation requires the development of technical standards, as well as socio-political adaptations rooted in legal amendments in order to be successful. Overall, SSI is implemented as blockchain-adjacent, but not blockchain-dependent identity management systems, which are guided by the fundamental principle of user-centric design, using technical standards that enable user-generated and user-controlled decentralised identifiers, associated credentials, and attestations. This is supplemented by legal and policy requirements to ensure that the objectives for particular use cases are achieved, including balancing competing societal goals between user privacy, security, law enforcement, financial inclusion and risk management.

References_

- Alamillo Domingo, I. (2020). *SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market?* [Report]. European Commission. https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report
- Allen, C. (2016, April 25). The path to self-sovereign identity [Blog post]. *Life With Alacrity*. https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html#dfref-1212
- Birch, D. (2014). *Identity is the new money, london publishing partnership*.
- Bodó, B. (2020). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*. https://doi.org/10.1177/1461444820939922
- Bodó, B., & Giannopoulou, A. (2020). The logics of technology decentralization: The case of distributed ledger technologies. In M. Ragnedda & G. Destefanis (Eds.), *Blockchain and web 3.0: Social, economic, and technological challenges routledge*. https://doi.org/10.4324/9780429029530-8
- Cameron, K. (2005, May). The laws of identity [Blog post]. *Kim Cameron's Identity Weblog*. https://www.identityblog.com/?p=352
- Cheesman, M. (2020). Self-sovereignty for refugees? The contested horizons of digital identity. *Geopolitics*. https://doi.org/10.1080/14650045.2020.1823836
- European Commission. (2020a). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions on shaping Europe's digital future,*

COM(2020) 67 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067
- European Commission. (2020b). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions on a digital finance strategy for the EU. COM/2020/591 final.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591
- Finck, M. (2019). *Blockchain regulation and governance in europe*. Cambridge University Press. https://doi.org/10.1017/9781108609708
- Foucault, M. (2004). *Sécurité, Territoire, Population*. Gallimard.
- Giannopoulou, A. (2020). Data Protection Compliance Challenges for Self-sovereign Identity. In J. Prieto, A. Pinto, A. K. Das, & S. Ferretti (Eds.), *Blockchain and Applications* (pp. 91–100). Springer International Publishing. https://doi.org/10.1007/978-3-030-52535-4_10
- Gstrein, O., & Kochenov, D. (2020). Digital identity and distributed ledger technology: Paving the way to a neo-feudal brave new world? *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2020.00010
- Herian, R. (2019). Regulating Blockchain. Critical perspectives in law and technology. *Routledge*. https://doi.org/10.4324/9780429489815
- Herian, Robert. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, *12*(1), 156–174. https://doi.org/10.1080/17579961.2020.1727094
- Hopman, R., & M'Charek, A. (2020). Facing the unknown suspect: Forensic DNA phenotyping and the oscillation between the individual and the collective. *BioSocieties*, *15*, 438–462. https://doi.org/10.1057/s41292-020-00190-9
- Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, *22*(9), 499–508. https://doi.org/10.1111/j.1467-8519.2008.00697.x
- Mac Sıthigh, D., & Siems, M. (2019). The chinese social credit system: A model for other countries? *Modern Law Review*, *82*(6), 1034–1071. https://doi.org/10.1111/1468-2230.12462
- Madiega, T. (2020). *Digital sovereignty for Europe* (Briefing PE 651.992; EPRS Ideas Papers). European Parliamentary Research Service.
- Manski, S., & Manski, B. (2018). No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World. *Law and Critique*, *29*(2), 151–162. https://doi.org/10.1007/s10978-018-9225-z
- Orgad, L. (2018). Cloud communities: The dawn of global citizenship? In R. Bauböck (Ed.), *Debating transformations of national citizenship.* (pp. 251–260). Springer. https://doi.org/10.1007/978-3-319-92719-0_46

- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532
- Preukschat, A., & Reed, D. (2021). *Self-sovereign identity. Decentralized digital identity and verifiable credentials, MEAP.*
- Renieris, E. (2020). SSI? What we really need is full data portability [Blog post]. *Women in Identity*. https://womeninidentity.org/2020/03/31/data-portability/
- Schroers, J. (2018). The final piece of the eIDAS Regulation [Blog post]. *KU Leuven Centre for IT & IP Law*. https://www.law.kuleuven.be/citip/blog/the-final-piece-of-the-eidas-regulation/
- Sheldrake, P. (2020, October 19). *The dystopia of self-sovereign identity*. Generative Identity. https://generative-identity.org/the-dystopia-of-self-sovereign-identity-ssi
- The Moxy Tongue. (2012, February 15). What is 'sovereign source authority'? [Blog post]. *The Moxy Tongue*. https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html
- The Moxy Tongue. (2016, February 9). Self-sovereign identity [Blog post]. *The Moxy Tongue*. https://www.moxytongue.com/2016/02/self-sovereign-identity.html
- Trotter, G. (2014). Autonomy as self-sovereignty. *HEC Forum*, *26*, 237–255. https://doi.org/10.1007/s10730-014-9248-2
- United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. https://sdgs.un.org/2030agenda
- Verhulst, S. G., & Young, A. (2018). *Field report on the emergent use of distributed ledger technologies for identity management* [Report]. The GovLab. https://blockchan.ge/blockchange-fieldreport.pdf
- Wagner, K., Némethi, B., Renieris, E., Lang, P., Brunet, E., & Holst, E. (2018). *Self-sovereign identity. A position paper on blockchain enabled identity and the road ahead* [Position paper]. Identity Working Group of the German Blockchain Association. https://www.bundesblock.de/wp-content/uploads/2018/10/ssi-paper.pdf
- Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion, frontiers in blockchain. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2019.00028
- Westermeier, C. (2020). Money is data – the platformization of financial transactions. *Information, Communication & Society*, *23*(14), 2047–2063. https://doi.org/10.1080/1369118X.2020.1770833
- World Bank Group. (2018). *Identification for Development Annual Report*

[Report]. https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018_ID4D_Annual_Report.pdf
– World Economic Forum. (2018). *Identity in a digital world — A new chapter in the social contract* [Report]. World Economic Forum. http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Endnotes_

1. We will use the term sovereign identity and SSI interchangeably.
2. According to goal 16.9 of the United Nations 2030 Agenda for Sustainable Development, the objective is to 'provide legal identity for all, including birth registration' by 2030.
3. In that regard, it distances itself from the concept of sovereignty (Manski & Manski, 2018).
4. This objective is perfectly aligned with the ideals of decentralisation that drove the development of blockchain technology in general (Bodó & Giannopoulou, 2020).

SMART CONTRACTS_

Primavera De Filippi, CERSA, CNRS, Paris, France. Harvard University's Berkman Klein Center for Internet and Society, United States.
Chris Wray, Legal Graph Company Limited, United Kingdom.
Giovanni Sileno, Informatics Institute, University of Amsterdam, Netherlands.

A smart contract is code deployed in a blockchain environment, or the source code from which such code was compiled.

Origin and evolution of the term_

Nick Szabo first described *smart contracts* in the late 1990s. He envisioned placing contracts into code that could be both "trustless" and "self-enforcing", enhancing efficiency and removing ambiguity from contractual relationships (Szabo, 1996). The idea was to eliminate the need for trust amongst the parties, by increasing the confidence that the contract will be performed exactly as designed (typically making breaches prohibitively expensive). To illustrate his concept, Szabo compared a smart contract to a vending machine. Individuals insert coins into the machine and — assuming the inserted amount is correct — the machine delivers the goods they requested. This predictable interaction requires little to no trust amongst the contracting parties: the vending machine has no choice but to deliver the goods upon receiving the money. The technological infrastructure of the machine is a guarantee that the contract will be fulfilled as intended.

Later, Szabo envisioned that smart contracts could be embedded into all sorts of property that is valuable and controlled by digital technologies to ensure that the associated contractual provisions are automatically executed by technological means (Szabo, 1997). From a historical perspective, the concept of using machines for the application of normative directives can be dated back to Leibniz, with his famous *Calculemus!* (De Arte Combinatoria, 1666), and returned to more concretely with the advent of legal expert systems in AI and attempts at formalisation of law (e.g. Sergot et al., 1984). Szabo's proposal can thus be seen as a simplification

of the higher-level goal set (with mixed results) by research on normative systems.

Today, the term *smart contract* has been adopted by the blockchain community to refer to code deployed and run in a blockchain environment (Buterin, 2013). In this sense, smart contracts are software programmes executed in a distributed manner by the miners of a blockchain-based network. Smart contracts take parameters (as an input) via incoming blockchain transactions, process these parameters according to some deterministic algorithm, and generate (as an output) either a state change in the smart contract memory or a new blockchain transaction.

Although they can be programmed in any language that can be compiled into a particular blockchain environment or virtual machine, the most prominent platform today for the deployment of smart contract code is *Ethereum*. Indeed, the Ethereum blockchain implements a Turing-complete 1 programming language, called *Solidity*, combined with a shared virtual machine (the Ethereum Virtual Machine or EVM), which has become the *de facto* standard for developing and deploying smart contracts.[2] As a programming language, Solidity is object-oriented, with a strong procedural flavour; its core components are imperative instructions defining "positive" actions, like for instance storing the result of a numeric expression in a variable, or logging certain events on the EVM.

Once deployed, the code of a smart contract is stored — in a compiled form — on the Ethereum blockchain and is assigned an address. In order to interact with the smart contract, parties send a transaction to the relevant address, thereby triggering the execution of the underlying code. As such, Ethereum can be regarded as a global and distributed computing layer, which constitutes the backbone for decentralised systems and applications (Buterin, 2013). While Ethereum was the first of its kind, similar functionalities have since been implemented in other blockchain-based platforms, the most popular of which are *Cardano, EOS, NEO, Tezos*, and *TRON*.[3]

Regardless of the blockchain on which they run, smart contracts fundamentally differ from standard software programmes because they can be executed independently from any centralised operator or trusted third party (De Filippi & Mauro, 2014). Indeed, to the extent that they rely

on a decentralised network that is not controlled by any single operator (Chen & al., 2017), smart contracts are guaranteed to run in a predefined and deterministic manner, free from intervention by any particular third party (Voshmgir, 2017). Hence, just like a vending machine, smart contracts can be said to be *self-executing*, with a *guarantee of execution* (Buterin, 2013).

Smart contracts generally only implement basic functionalities, such as:

- token issuance for the purpose of fund-raising (as in the case of a token sale or Initial Coin Offering (ICO));
- issuance and management of tokens as digital collectibles (e.g. *cryptokitties*);
- decentralised marketplaces for the trading of digital tokens (e.g. OpenSea);
- conditional or recurrent payments based on a set of predefined conditions;
- joint savings accounts, allowing parties to withdraw only a particular amount every day;
- escrow systems programmed to execute a transaction whenever specific conditions are met;
- simple lottery systems[4] collecting funds and redistributing them to the selected winner(s);
- gambling systems (such as *prediction markets*) the operations of which are inherently transparent, permitting users to verify how much money the house has on hand for payouts (e.g. Augur).

Yet, by aggregating multiple smart contracts together, it is possible to create applications with more advanced functionalities. These include decentralised finance applications, such as lending platforms (e.g. MakerDAO) and liquidity pools (e.g. Uniswap, Aave); social media platforms (e.g. Akasha, Karma, Peepeth); or even distributed governance systems for blockchain-based assets, often referred to as *Decentralized Autonomous Organizations* (e.g. TheDAO, MolochDAO, DxDAO, etc.).

Perhaps one of the greatest potentials of smart contracts lies in the extent to which they can be used to complement or supplement existing legal contracts. They could be used, for instance, to increase the security of identification phases, to facilitate the subscription for shares in a company, the management of an insurance policy, or even the execution of an

employment contract (Alhabry & Van Moorsel, 2017). However, most implementations of smart contracts in the legal field are still far from being widely adopted, or even useful. Indeed, for the majority of legal applications (beyond pure financial applications), much of the computation cannot be done by the smart contracts alone, because the smart contract does not have access to information that is not recorded on a blockchain. This is why many smart contracts rely on so-called "oracles": blockchain addresses controlled by some trusted third parties through which the relevant inputs to the contract are provided. Oracles make it possible for smart contracts to react to external data for the implementation of more sophisticated applications — such as a parametric crop insurance service, which receives information from a national weather service and automatically disburses funds based on predefined conditions (Cohn & al., 2017). Relevant extensions enabled by oracles concern *ex-post* enforcement mechanisms and dispute resolution by means of witnesses, juries and other roles (e.g. Kleros), or more advanced *ex-ante* enforcement controls by means of external reasoners (see e.g., Idelberg et al., 2016; Liu et al., 2020).

Misconceptions_

There are many misconceptions in the discussion around *smart contracts*. First, smart contracts are often believed to be script-like programmes executed on a blockchain, though from a technical perspective, the operations of smart contracts are ultimately defined by the set of instructions fed (in the form of "bytecode") into the virtual machine, which will be executed by the underlying blockchain network. This means that the actual performance of a smart contract does not depend on the subjective expectation of the parties, based on their interpretation of the source code, but merely on the operations dictated by the compiled bytecode deployed to the blockchain (De Filippi & Hassan, 2018).

This leads us to a second key misconception about *smart contracts*: they generally act as a technical representation of a legal contract, for at least two fundamental reasons. Firstly, in the *nature* of their expression: smart contracts are inherently more rigid (and therefore more limited) than legal contracts (De Filippi & Wright, 2018). While the clauses of a legal contract (written in natural language) may apply to an indefinite number of situations — because of the inherent flexibility and ambiguity

of natural language — the provisions of a smart contract are expressed in a formalised language that does not have nearly the same degree of flexibility as natural language (Levy, 2017). As a result, many contractual clauses (e.g. *bona fide* obligations) cannot be codified in a blockchain-based infrastructure because they simply cannot be expressed in code (Sklaroff, 2017). Rigidity is also partially due to the closure determined by specific technological choices; for instance, although Solidity considers the use of libraries (i.e. reusable smart contract deployed code), those cannot be updated, and their semantic staticity is reflected in the contracts relying upon them. That being said, such limitations also represent one of the key benefits of a smart contract, as contracting parties may want their contractual performance to rely exclusively on precise and quantifiable outcomes.

Secondly, in the *scope* of their performance: only a very limited class of contractual obligations can be fully embedded into a smart contract (Mik, 2017). At a computational level, smart contracts enjoy the convergence of imperative instructions with positive duties, but this also means that they do not include explicit directives about e.g. prohibitions, nor about institutional power. This would not really be problematic if smart contracts were only concerned with operations under their control. However, most legal contracts refer to rights and obligations outside of the blockchain infrastructure, which cannot therefore be administered via a smart contract. If contractual obligations are triggered by external conditions, a smart contract will depend on a third party-operated programme (i.e. an "oracle") to record all the relevant information about such external conditions onto a blockchain (Egberts, 2017). If the contractual obligation itself requires an external intervention, no blockchain-based infrastructure will ever be able to guarantee the proper performance thereof. In particular, legal title to, or beneficial interest in, any property or asset that exists outside of the blockchain infrastructure (i.e. anything other than a blockchain-based asset) cannot be transferred merely by recording a state change into a blockchain, but only in accordance with applicable law. For instance, transferring land ownership cannot be performed automatically by a smart contract because it requires administrative formalities that cannot be completed on a blockchain. In this case, a smart contract could only record the payment, along with the current owner's intention to transfer ownership to a third party — e.g. via the transfer of an asset-backed token.

Sometimes, the mere act of transacting with a smart contract could give rise to a legal agreement, provided that the minimum legal requirements for contract formation are met in the relevant jurisdiction (Werbach & Cornel, 2017). Conversely, any additional provisions that cannot be fully codified in (and therefore automated by) a blockchain will merely qualify as a promise under an executory contract that may only be enforced through a court order (Herian, 2020). Thus, just as a vending machine can automate the performance of a contract to sell only the physical goods contained within it, so a blockchain-based smart contract can provide automatic performance of a contract relating only to transactions in blockchain-based assets (Hulicki, 2017).

A related problem is the impossibility of technically *nullifying* the execution of a smart contract in case some underlying conditions make its execution invalid from a legal point of view. Even if such a situation could be identified by means of an external oracle, the chain of transactions stemming from an invalid performance cannot be recovered, unless the possibility has been pre-codified within the smart contract itself.

Several other misconceptions about smart contracts are related to trust. First, it is often said that smart contracts are entirely self-executing (Zhou et al., 2019). Yet, as highlighted above, a smart contract will always rely on a certain amount of trust and/or verification, especially when its execution depends on external information recorded onto a blockchain by a third party (Guadamuz, 2019). If the smart contract depends on a given "oracle" for its basic functionality, the failure of such an oracle to provide the necessary information will prevent the execution of the smart contract (Muhlberger et al., 2020). More fundamentally, a smart contract's proper functioning ultimately depends on the network of miners that operate the underlying blockchain network (De Filippi et al., 2020). Were these miners collectively to decide to prevent the execution of a smart contract, they could either censor all transactions addressed towards that particular smart contract's address (a soft fork) or modify the blockchain protocol in order to change the code of the smart contract or its implementation (a hard fork). While such an intervention is unlikely to happen on a recurrent basis, it is not merely theoretical — as shown by the hard fork of the Ethereum blockchain in the aftermath of TheDAO attack 5 (Reijers et al., 2018).

Conclusion_

A *smart contract* is code deployed in a blockchain environment, or the source code from which such code was compiled. It is executed in a distributed manner by the miners of the underlying blockchain network if and when the underlying conditions are met. Execution of a smart contract is triggered via a blockchain transaction and will produce a change in the blockchain state.

References_

- Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *Computer Science & Information Technology*, *7*(10). https://doi.org/10.5121/csit.2017.71011
- Buterin, V. (2013). *Ethereum whitepaper: A next-generation smart contract and decentralized application platform* [White Paper]. https://ethereum.org/en/whitepaper/
- Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). Decentralized execution of smart contracts: Agent model perspective and its implications. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, & M. Jakobsson (Eds.), *International conference on financial cryptography and data security* (pp. 468–477). Springer. https://doi.org/10.1007/978-3-319-70278-0_29
- Cohn, A., West, T., & Parker, C. (2017). Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids. *Georgetown Law Technology Review*, *1*(2), 273–304. https://georgetownlawtechreview.org/smart-after-all-blockchain-smart-contracts-parametric-insurance-and-smart-energy-grids/GLTR-04-2017/
- Corrales, M., Fenwick, M., & Haapio, H. (Eds.). (2019). *Legal Tech, Smart Contracts and Blockchain*. Springer. https://doi.org/10.1007/978-981-13-6086-2
- De Filippi, P., & Hassan, S. (2018). Blockchain technology as a regulatory technology: From code is law to law is code. *arXiv*. https://arxiv.org/abs/1801.02507
- De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of

governance. *Technology in Society*, *62*. https://doi.org/10.1016/j.techsoc.2020.101284

- De Filippi, P., & Mauro, R. (2014, August 25). Ethereum: The decentralised platform that might displace today's institutions. *Internet Policy Review*. https://policyreview.info/articles/news/ethereum-decentralised-platform-might-displace-todays-institutions/318
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
- Egberts, A. (2017). *The oracle problem-an analysis of how blockchain oracles undermine the advantages of decentralized ledger systems*. https://doi.org/10.2139/ssrn.3382343
- Guadamuz, A. (2019). All watched over by machines of loving grace: A critical look at smart contracts. *Computer Law & Security Review*, *35*(6). https://doi.org/10.1016/j.clsr.2019.105338
- Herian, R. (2020). Smart contracts: A remedial analysis. *Information & Communications Technology Law*, *30*(1), 17–34.
- Hulicki, M. (2017). The legal framework and challenges of smart contract applications. *Conference on System Sciences*, 3–4. http://www.cs.bath.ac.uk/smartlaw2017/papers/SmartLaw2017_paper_3.pdf
- Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). Evaluation of logic-based smart contracts for blockchain systems. Rule technologies. In J. J. Alferes, L. Bertossi, G. Governatori, P. Fodor, & D. Roman (Eds.), *Rule Technologies. Research, Tools, and Applications* (pp. 167–183). Springer International Publishing. https://doi.org/10.1007/978-3-319-42019-6_11
- Lauslahti, K., Mattila, J., & Seppala, T. (2017). *Smart contracts–How will blockchain technology affect contractual practices?* (Report No. 68). ETLA. http://hdl.handle.net/10419/201350
- Levy, K. E. (2017). Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society*, *3*, 1–15. https://doi.org/10.17351/ests2017.107
- Liu, L., Sileno, G., & Engers, T. V. (2020). Digital enforceable contracts (DEC): Making smart contracts smarter. In S. Villata, J. Harašta, & P. Kremen (Eds.), *JURIX 2020: The 33rd annual conference on legal knowledge and information systems* (pp. 235–238). https://doi.org/10.3233/FAIA200872
- Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, *9*(2), 269–30. https://doi.org/10.1080/17579961.2017.1378468

- Mühlberger, R., Bachhofner, S., Ferrer, E. C., Di Ciccio, C., Weber, I., Wöhrer, M., & Zdun, U. (2020). Foundational oracle patterns: Connecting blockchain to the off-chain world. *International Conference on Business Process Management*, 35–51. https://doi.org/10.1007/978-3-030-58779-6_3
- Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Vélez, A. C., & Orgad, L. (2018). *Now the code runs itself: On-chain and off-chain governance of blockchain technologies*. 1–11. https://doi.org/10.1007/s11245-018-9626-5
- Savelyev, A. (2017). Contract law 2.0: 'Smart'contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036
- Sergot, M. J., Sadri, F., & Kowalski, R. A. (1986). The British Nationality Act as a logic program. *Communications of the ACM*, *29*(5). https://doi.org/10.1145/5689.5920
- Sklaroff, J. M. (2017). Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, *166*, 263–303. https://scholarship.law.upenn.edu/prize_papers/9/
- Szabo, N. (1996). Smart contracts: Building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, *16*.
- Szabo, N. (1997). *The idea of smart contracts*. Nick Szabo's Papers and Concise Tutorials. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html
- Voshmgir, S. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, *26*(5), 499–509. https://doi.org/10.1002/jsc.2150
- Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, *67*(2), 313–382. https://scholarship.law.duke.edu/dlj/vol67/iss2/2/
- Zou, M., Cheng, G., & Soria Heredia, M. (2019, April). In code we trust? Trustlessness and smart contracts. *Computers and Law*. https://www.scl.org/articles/10493-in-code-we-trust-trustlessness-and-smart-contracts

Endnotes_

1. A programming language is Turing-complete if it is computationally equivalent to a Turing machine. That is, any problem that can be solved on a Turing machine using a finite amount of resources can be solved with that programming language using a finite amount of resources.
2. By contrast, Bitcoin Script is not Turing-complete.
3. Note that, although limited in its capabilities, Bitcoin's simple script language also allows for the creation of custom smart contracts like multisignature accounts, payment channels, escrows, time locks, atomic cross-chain trading, oracles, or multi-party lottery with no operator.
4. Note that because smart contract code is inherently and necessarily deterministic, randomised action — such as selecting a lottery winner — rely on novel sources of pseudo-randomness which are based on the content of previous blocks.
5. TheDAO was a decentralised investment fund deployed as a smart contract on the Ethereum blockchain in 2016, which raised over USD$ 150 million in less than one month. However, a few days before the launch, a vulnerability was found in the code of the smart contract governing TheDAO, which was exploited in order to drain over USD$ 60 million from the fund.

SOCIAL APPROPRIATION OF NEW TECHNOLOGIES_

Francisco Javier Moreno Gálvez, University of Seville, Spain.
Francisco Sierra Caballero, University of Seville, Spain.

The social appropriation of new technologies refers to technological and social processes of mediation in the interaction between social actors and technological devices. As such, the concept transcends relatively straightforward ideas of access and use of technology to focus on: how users develop technological and cognitive competences; the meaningful integration of the technological devices into subjects' everyday lives and behaviour; the active and creative production of meaning; social mediation within communities of users; and the way that the interests of communities of users are represented in public spaces. This text outlines the key concepts and debates in the appropriation of new technologies through a genealogical reconstruction of relevant academic traditions, including, amongst others, cultural studies and the sociology of the uses of new technologies. This interdisciplinary approach takes into account the technical, cognitive, educational and communicative dimensions of new technologies and how they may be useful for understanding contemporary processes of technological change.

Origin and evolution_

To understand the genesis of the concept of social appropriation of new technologies we can start by considering the concept of appropriation in social production and reproduction from two key critical perspectives: Michel de Certeau's social autonomy in everyday life and the materialist psychology of Aleksei N. Leóntiev and Lev Vygotsky (de Certeau, 1980; Leóntiev, 1959).

Firstly, as one of the main influences on the development and popularisation of the concept of appropriation, the work of de Certeau can be situated in the debates on social autonomy that arose in the wake of the May 1968 student revolution in France. Within this line of thought, the conflictive aspect of Marxist debate on appropriation was recovered and translated for use in the analysis of political autonomy in the context

of social relations of reproduction (Jauréguiberry & Proulx, 2011). In The Practice of Everyday Life (Certeau, 1980) de Certeau examined quotidian culture as a process of approbation and showed that people's everyday practices deviated from the framework provided by technocratic and industrial cultures. His work opened up the possibility of conceiving individuals not as mere consumers but actors that constitute themselves autonomously in key domains of everyday culture, through practices related to consumption, habitat and reading.

Secondly, from the field of materialist psychology, Leóntiev and Vygotsky challenged the dominant approach of behavioural psychology by developing a socio-historical perspective that emphasised the social and cultural origins of individual and collective behaviour (Crovi, 2013; Leóntiev, 1959). Building on the work of these two authors, various generations of academics went on to develop a materialist approach to appropriation. In this conceptualisation, appropriation relates to the interaction between individuals and cultural products (including technologies), or can be conceived as a game within which the externalities of the object are combined with the individuals' interiorisation of the semiotic systems, social structures, concepts and techniques inscribed in said object (del Río, 2002; Freire, 1973; Engeström, 2001; Sannino et al., 2009).

Although following different paths, two main lines of work, which eventually converge, can be observed in the evolution of the study of the social appropriation of technologies: media consumption and reception studies, including cultural studies, and the sociology of the uses of new technologies, from the French-speaking tradition.

Media consumption and reception studies have been a central point of communications research since the inception of the discipline in the mid-twentieth century, but it has evolved through various stages. Functionalist perspectives, for example, focused on the persuasive effects of communication on audiences, which were conceived as a homogeneous and passive group (Lasswell, 1948; Lazarsfeld & Merton, 1948; Wright, 1964). In contrast, a turn in reception studies in 1960s saw the gradual introduction of macro-sociological variables and an understanding of media as a socio-cognitive mediation system (Wolf, 1987) that placed the subject at the centre of the analysis of consumption[1]. This turn influenced work in psychology and functionalist theories of sociology

(Katz et al., 1974), as well as new approaches from within the field of cultural studies (During, 1993).

In the evolution of media studies, the work of British and Latin American strands of cultural studies stand out as particularly relevant. On the British side, the so-called founding fathers of cultural studies, Stuart Hall, E.P. Thompson, Raymond Williams and Richard Hoggart (Mattelart & Neveau, 2003), opened the door to an understanding of reception that went beyond access and use by taking into account the capacity of the subject to actively and critically construct meaning in specific social contexts. In Latin America, a theoretical framework was developed that shifted the focus from media to spaces where meaning is produced, in other words: the space of mediation (Beltrán & Zeballos, 2001; García Canclini, 1990; Martín Barbero, 1987). This interdisciplinary approach brought together concepts from cultural studies, educommunication (Kaplún, 1992; Orozco, 2001) and political economy perspectives (Bolaño et al., 2012)[2]. The result was a new model for the study of practices related to the creation and appropriation of culture, the activation of people's competence and creative experience, and the recognition of differences (Martín Barbero, 2002).

Distinct from reception studies, the second line of work developed in the French-speaking tradition of the sociology of the uses of new technologies in the 1980s (Jouët, 2000; Proulx, 2015). Instead of attempting to extend or prolong the analysis of media uses, it centred on sociological approaches to the contextualised use of technological objects such as the television remote control, home computing, the telephone answering machine and, above all, the experience of Minitel. Traditionally, this theoretical approach has favoured a critical frame of analysis. Inscribed in concepts of social autonomy, it was often defined by research on social struggle, such as the fight for information literacy or the social appropriation of technologies as a possible source of autonomy for individuals or social and political emancipation for groups. Not defined as consumers, the idea of appropriation constitutes social actors as agents that deploy active and creative resistances in their everyday interactions with new technologies (at work, during leisure time, in family relations). Within the framework of daily life and practices, users give technical objects subjective meanings (projections, associations), while uses are embedded in a system of social relations (class, gender, interethnic, intergenerational) and a lifeworld that

shapes and is shaped by technological uses (Granjon, 2012; Granjon et al., 2009; Jauréguiberry & Proulx, 2011).

These approaches represented a watershed at various levels. By shifting the focus from the analysis of effects to the study of reception, appropriation is reconfigured as a process of negotiation between the emitter and receiver that is situated in specific sociocultural contexts. And, as an ordinary everyday practice, reception is therefore understood to be a continuous, complex, contradictory and interactive phenomenon. Collectively, this takes the study of appropriation beyond mere reception and a question of simple consumption. Hence, with the evolution of technological change these currents of thinking gradually abandoned the framework of reception studies because, in new digital networks, the relation between subjects transcends the notion of 'active reception' that had been the dominant theoretical idea. Progressively, research shifted its focus to processes of appropriation and digital competence in new technologies that centre on everyday practises in the current social and cultural context (Ang, 1990; Hall & Du Guy, 1996; McRobbie, 1994; Morley 2010, 2007; Morley & Silverstone, 1990; Silverstone, 2016).

Coexisting uses and meanings_

Over time, the theoretical proposals of the different perspectives have hybridised as a result of dialogue between authors and schools of thought. We can therefore identify different ways of defining the social appropriation of new technologies that share common ground, such as a rejection of explanations that are limited to understandings of access and use of technologies in terms of adaptation, integration or assimilation (Crovi, 2013).

One approach uses the concept of 'information capital' as a means of providing a holistic explanation for the process of access, use and appropriation of new technologies. This integrates not just economic barriers of access to digital devices or electronic networks, but "the technical ability to handle network infrastructures, the intellectual capacity to filter and evaluate information [as well as] the motivation to actively search for information and the ability to translate information into social practice" (Hamelink, 2000, p. 91).

Another perspective, proposed by researchers linked to the Latin American Network for Research on the Appropriation of Digital Technologies (RIAT) (Cabello & López, 2017; Lago Martínez et al., 2018; Sandoval, 2019) is to define the process of social appropriation of new technologies as "the set of sociocultural processes that intervene in the use, socialisation and signification of new technologies in diverse sociocultural groups" (Winocur, 2013: p. 62, translation by the authors). Within this perspective, appropriation can be analysed through the interrelationship of various dimensions, such as: availability, access, knowledge, elucidation, reflexivity, competencies, interactivity, use and the development of personal and collective projects (Morales, 2014).

Another way of ordering these dimensions is the ideal-type approach to the social appropriation of new technologies that has been developed by the French sociological tradition. As well as the pre-standing condition of material access to the technological device, this approach uses five levels or conditions (Jauréguiberry & Proulx, 2011, pp. 81-82):

(1) Technical and cognitive mastery of the device.
(2) Meaningful integration of the use of the technology in the actor's everyday practice.
(3) Repetitive use of the technical device that opens up the possibility of creative (new) uses in social practice.
(4) Mediation in a community of practice as a source of exchange (producers of collective intelligence), transmission, and support between learning subjects.
(5) At a truly collective level, appropriation implies that users and their needs are adequately represented in the establishment of public policies and that they are taken into account in processes of change and innovation in companies (industrial production and commercial distribution).

Current issues_

A central debate traverses the evolution of research on the access, use and appropriation of new technologies in terms of the positive or negative impact of technological innovation for social change. Perspectives that advocate for the potentialities of technologies tend to focus on their dissemination — in particular material access to networks and technological equipment — as a means to overcome the inequality that

plagues contemporary societies. This conception of new technologies is linked to post-industrialist theory and authors such as Daniel Bell, Fritz Machlup, Alvin Toffler, Zbigniew Brzezinski, Marc Porat, Nicholas Negroponte and Bill Gates, among others, (Becerra, 2003; Webster, 2004). This group has been highly influential on the technological programmes of various governments and transnational organisations. Examples of projects developed within this ethos include the Informatisation of Society in France (Nora & Minc, 1978), the Information Superhighway in the United States (Gore, 1994), the European Information Society (European Council, 1994), and the World Summit on the Information Society (United Nations, 2005).

In contrast, other research argues that technological development can be damaging as it may exacerbate imbalances in social power and worsen inequality (Robins & Webster, 1999). This line of work ranges from studies that highlight the use of technological innovation for increased surveillance and social control (Lanier, 2011; Mattelart & Vitalis, 2014; Morozov, 2011) to research on the technological determinism of perspectives that focus on material access to technology while neglecting the social aspect of the transformation of information and data into knowledge (Archer, 2017; Mosco, 2009; Servaes & Carpentier, 2006).

Such dichotomies and technological determinism can be avoided by analysing new technologies through the various dimensions of social appropriation and by understanding the process of mediation that takes place between the technical and the social. In this sense, neither can be understood separately: mediation is "technical because the tool used structures practices, and social as the motives, the forms of use, and the meaning given to the practice are drawn from the social body" (Jouët, 2000, p. 497, translation by the authors). Thus, an interesting dialogue is established between the previous lines of thought and those that analyse the conception of technological devices and their technological affordances – the possibilities for action and interaction open to users of specific technologies, but which is always limited by said technology's design (Bardini, 1996; Hutchby, 2001).

Linked to this double mediation is a prolific field of research on the 'digital divide', which focuses on differences in the appropriation of technological objects based on geographic location, socio-economics, gender, and

generation, among others, that can lead to social labelling and, frequently, exclusion (Ragnedda & Muschert, 2013; Van Dijk, 2020). Although there is a notable lack of systematic reviews, a significant body of research has examined topics such as differentiated modes of appropriation of subjects based on a lack of equality in the development of technological infrastructures at a global level, as well as between urban and rural areas; how new technologies can generate income and educational inequality; differences in interests between men and women that result from the historical male domination of digital objects (); and the reconfiguration of intergenerational social relations due to a breach in cultural and social practices between digital natives and older members of society (Cabello & López, 2017; Granjon et al., 2009; Gómez, 2012; Lago Martínez et al., 2018; Livingstone et al., 2017; Pereira, 2015; Sáinz et al., 2008).

Finally, we can identify work, from various scientific disciplines, that uses the concepts of technological appropriation or social appropriation of new technologies to analyse the interaction between subjects and digital devices. Beyond studies in communication and the analysis of the reception of new media and technologies, interdisciplinary studies are focusing on digital inclusion, education and media literacy, rights to communication, community computing, social movements and social change, and public policy in the information society.

Conclusion_

The social appropriation of new technologies refers to technological and social processes of mediation in the interaction between social actors and technological devices. As such, the concept transcends relatively straightforward concepts of access and use of technology to focus on: how users develop technological and cognitive competences; the meaningful integration of the technological device into subjects' everyday lives and behaviour; the active and creative production of meaning; social mediation within communities of users; and the way that the interests of communities of users are represented in public spaces.

References_

- Ang, I. (1990). Culture and Communication: Towards an Ethnographic Critique of Media Consumption in the Transnational Media System. *European Journal of Communication*, *5*(2), 239–260. https://doi.org/10.1177/0267323190005002006
- Archer, M. S. (2017). Theory, culture and post-industrial society. *Sociologia*, *LI*. https://doi.org/10.36165/2411
- Barbas Coslado, A. (2012). Educomunicación: Desarrollo, enfoques y desafíos en un mundo interconectado. *Foro de Educación*, *10*(14), 157–175.
- Bardini, T. (1996). Changement et réseaux socio-techniques: De l'inscription à l'affordance. *Réseaux*, *14*(76), 125–155. https://doi.org/10.3406/reso.1996.3715
- Becerra, M. (2003). *Sociedad de la información: Proyecto, convergencia, divergencia*. Grupo Editorial Norma.
- Beltrán, L. R., & Zeballos, R. (2001). *Estrategias de comunicación y educación para el desarrollo*. Red ERBOL / Universidad Católica Bolivariana.
- Benjamin, W. (1968). *Illuminations*. Schocken Books.
- Blumler, J. G., & Katz, E. (Eds.). (1974). *The Uses of mass communications: Current perspectives on gratifications research*. Sage Publications.
- Bolaño, C., Mastrini, G., & Serra, F. (Eds.). (2012). *Political economy, communication and knowledge: A Latin American perspective*. Hampton Press.
- Brecht, B. (2015). *Brecht On Film & Radio*. Bloomsbury Publishing. http://www.myilibrary.com?id=752371
- Cabello, R., & López, A. (Eds.). (2017). *Contribuciones al estudio de procesos de apropiación de tecnologías*. Ediciones del Gato Gris.
- Certeau, M. de. (1980). *Arts de faire* (Nouv. éd). Gallimard.
- Crovi Druetta, D. (2013). Matrices digitales en la identidad juvenil. In F. Sierra Caballero (Ed.), *Ciudadanía, tecnología y cultura. Nodos conceptuales para pensar la nueva mediación digital* (pp. 211–232). Gedisa.
- del RÌo, P. (2002). The External Brain: Eco-Cultural Roots of Distancing and Mediation. *Culture & Psychology*, *8*(2), 233–265. https://doi.org/10.1177/1354067X02008002440
- During, S. (Ed.). (1993). *The cultural studies reader*. Routledge.
- Engeström, Y. (2001). Expansive Learning at Work: Toward an activity theoretical reconceptualization. *Journal of Education and Work*, *14*(1), 133–156. https://doi.org/10.1080/13639080020028747

- Freire, P. (1973). *Education for critical consciousness*. Bloomsbury Academic.
- García Canclini, N. (1990). *Culturas híbridas: Estrategias para entrar y salir de la modernidad* (nueva edición, 6. reimpresión). Paidós.
- Gomez, R. (Ed.). (2012). *Libraries, Telecentres, Cybercafes and Public Access to ICT: International Comparisons*. IGI Global. https://doi.org/10.4018/978-1-60960-771-5
- Gore, A. (1994). Forging a new Athenian age of democracy. *Intermedia*, *22*(2), 4–7.
- Granjon, F. (2009). *Reconnaissance et usages d'Internet: Une sociologie critique des pratiques de l'informatique connectée*. Presses des Mines. https://doi.org/10.4000/books.pressesmines.252
- Granjon, F. (2012). *Reconnaissance et usages d'Internet: Une sociologie critique des pratiques de l'informatique connectée*. Presses des Mines. https://doi.org/10.4000/books.pressesmines.252
- Hall, S. (1973). *Encoding and decoding in the television discourse* (Hall, S. (1973). Encoding and Decoding in the Television Discourse. Paper for the Council of Europe Colloquy on "Training in the Critical Reading of Television Language. University of Leicester.).
- Hall, S., & Du Gay, P. (Eds.). (1996). *Questions of cultural identity*. Sage.
- Hamelink, C. J. (2000). *The ethics of cyberspace*. Sage Publications.
- Hutchby, I. (2001). Technologies, Texts and Affordances. *Sociology*, *35*(2), 441–456. https://doi.org/10.1177/S0038038501000219
- Jauréguiberry, F., & Proulx, S. (2011). Bibliographie: In *Usages et enjeux des technologies de communication* (pp. 126–141). Érès. https://doi.org/10.3917/eres.jaure.2011.01.0126
- Jouët, J. (2000a). Retour critique sur la sociologie des usages. *Réseaux*, *18*(100), 487–521. https://doi.org/10.3406/reso.2000.2235
- Jouët, J. (2000b). Retour critique sur la sociologie des usages. *Réseaux*, *18*(100), 487–521. https://doi.org/10.3406/reso.2000.2235
- Kamark, E. C., & Nye, J. (Eds.). (2002). *Governance.com. Democracy in the information age*. Brookings Institution Press.
- Kaplún, M. (1992). *A la educación por la comunicación: La práctica de la comunicación educativa*. FLACSO.
- Lago Martínez, S. (Ed.). (2018). *Acerca de la apropiación de tecnologías: Teoría, estudios y debates*. Ediciones del Gato Gris.
- Lanier, J. (2012). *Ten arguments for deleting your social media accounts right now* (First edition). Henry Holt and Company.
- Lasswell, H. D. (1948). Structure and function of communication in society. In L. Bryson (Ed.), *Communication of ideas* (pp. 37–52).

Institute for Religious and Social Studies.
- Lazarsfeld, P. F., & Merton, R. K. (2007). Mass communication, popular taste and organized social action. *Communication of ideas*, 229–250.
- Leóntiev, A. N. (1959). *Problems of the development of the mind*. Progress Publishers.
- Livingstone, S., Nandi, A., Banaji, S., & Stoilova, M. (2017). *Young adolescents and digital media: Uses, risks and opportunities in low- and middle-income countries: A rapid evidence review*. London School of Economics Report. http://eprints.lse.ac.uk/83753/1/Livingstone_Young_Adolescents_Digital_Media.pdf
- Martín Barbero, J. (1987). *Communication, culture and hegemony: From the media to mediations*. SAGE Publications.
- Martín Barbero, J. (2002). Oficio de cartógrafo. Travesías latinoamericanas de la comunicación en la cultura. *Oficios Terrestres*, *14*, 157–158.
- Mattelart, A., & Neveu, É. (2003). *Introduction aux cultural studies* (Nouvelle éd). la Découverte.
- Mattelart, A., & Vitalis, A. (2014). *Le profilage des populations: Du livret ouvrier au cybercontrôle*. Découverte.
- McRobbie, A. (1994). *Postmodernism and Popular Culture*. Routledge.
- Morales, S. (2014). La apropiación de medios y TIC. Una propuesta teórico-metodológica. In V. Mayora Ronsini (Ed.), *Estudos de recepção Latino-Americanos: Métodos e práticas* (pp. 44–59). Institut de la Comunicació, Universitat Autónoma de Barcelona.
- Morley, D. (2007). *Media, modernity and technology: The geography of the new*. Routledge.
- Morley, D. (2010). Domesticating dislocation in a world of 'new' technology. In C. Berry (Ed.), *Electronic Elsewheres. Media, Technology, and the Experience of Social Space* (pp. 3–16). University Minnesota Press.
- Morozov, E. (2011). *The net delusion. The Dark Side of Internet Freedom*. PublicAffairs.
- Mosco, V. (2009). *The political economy of communication* (2nd ed). SAGE.
- Nora, A., & Minc, S. (1978). *L'informatisation de la société*. La Documentation Française.
- Orozco, G. (2001). *Televisión, audiencia y educación*. Grupo Editorial Norma.
- Pereira, S. (Ed.). (2015). *Digital literacy, technology and social inclusion. Making sense of one-to-one computer programmes around the world*. Edições

Húmus.
- Proulx, S. (2015). La sociologie des usages, et après ? *Revue Française Des Sciences de l'information et de La Communication*, *6*. https://doi.org/10.4000/rfsic.1230
- Ragnedda, M., & Muschert, G. W. (Eds.). (2013). *The digital divide. The internet and social inequality in international perspective*. Routledge.
- Robins, K., & Webster, F. (1999). *Times of the Technoculture. From the information society to the virtual life*. Routledge.
- Sainz, M. (2008). *Review of the concept digital literacy and its implications in the study of the gender digital divide. UOC*. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/1283/3/sainz_castano_artal.pdf
- Sandoval, L. (2019). La apropiación de tecnologías en América Latina: Una genealogía conceptual. *Virtualis*, *10*(19), 1–19.
- Sannino, A. (Ed.). (2009). *Learning and expanding with activity theory*. Cambridge University Press.
- Servaes, J., & Carpentier, N. (Eds.). (2006). *Towards a Sustainable Information Society*. ECCR.
- Shirky, C. (2009). *Here comes everybody: The power of organizing without organizations*. Penguin Books.
- Silverstone, R. (Ed.). (2017). *Media, Technology and Everyday Life in Europe* (0 ed.). Routledge. https://doi.org/10.4324/9781315249384
- United Nations General Assembly. (2005). *Resolution adopted by the General Assembly on 16 September 2005*. United Nations. https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_60_1.pdf
- van Dijk, J. (2020). *The digital divide*. Polity.
- Webster, F. (Ed.). (2004). *The information society reader*. Routledge.
- Winocur, R. (2013). Una revisión crítica de la apropiación en la evaluación de los programas de inclusión digital. In S. Morales & M. I. Loyola (Eds.), *Nuevas perspectivas en los estudios en comunicación. La apropiación tecno-mediática* (pp. 53–64).
- Wolf, M. (1987). *La investigaci??n de la comunicaci??n de masas: Cr??tica y perspectivas*. Paidós.
- Wright, C. R. (1964). Functional analysis and mass communication. In L. A. Dexter & D. M. White (Eds.), *People, society and mass communication* (pp. 91–109). The Free Press.

Endnotes_

1. Although some authors had highlighted the active nature of audiences before this point in time (Brecht, 2015; Benjamin, 1968), their influence came, fundamentally, through a reassessment of their work in the 1960s.
2. Educommunication, also known as media literacy or media education in English-speaking contexts, refers to an interdisciplinary and transdisciplinary field of study on the theoretical and practical dimensions of two disciplines: education and communication. This concept was popularised by UNESCO in the 1970s and was primarily based on the work of authors like Mario Kaplún who adapted the pedagogic work of Paulo Freire to the field of communication (Barbas, 2012, pp. 159-161). On the other hand, the political economy perspective was also influential due to its concern with the cultural processes of production and reproduction of capital, class relations, contradiction, conflict, and struggles of opposition and resistance that traverse the media landscape (Mosco, 2009).

THE WEB OF VALUE_

Indrek Ibrus, Baltic Film, Media and Arts School (BFM), Tallinn University, Tallinn, Estonia.
Ulrike Rohn, Baltic Film, Media and Arts School (BFM), Tallinn University, Tallinn, Estonia.

The future iteration of the internet is often branded as Web3, claimed to be a decentralising phase of its evolution, a reaction to the centralisation in the Web 2.0 era. This upcoming version of the internet, afforded by distributed ledgers and blockchain technologies, is sometimes also called the "Web of Value". It highlights the expectation that as much of the content and services on the internet get "tokenised", which enables their trade and related operations of 'value creation'. It is claimed that as the value of everything on the internet becomes more salient, conditioning new kinds of economic activities, relationships and forms of organising. In this article we discuss these expectations as imaginaries, the implications of which vary based on how they are framed or interpreted by different economic theories.

Introduction_

The Web of Value (or the 'Internet of Value') is a term that is often employed synonymously with 'Web3',[1] or the 'Internet of blockchains', and is mostly used in industry discourse. It refers to an internet where users can publish, distribute, and trade information, services, and products of 'value' without the interference of intermediaries (see Floros, 2019; Skinner, 2016; Tapscott & Tapscott, 2016; Upadhyay, 2019; Vadgama et al., 2022). Its second main denotation is the condition where many internet content items or relationships (for instance memberships to communities) have value perceivably attached to them. This means that they are turned into tokens and their price in other kinds of tokens is easily accessible. For instance, a digital book can exist in the form of an non-fungible token (NFT)[2] and all transactions with it in various cryptocurrencies, including details such as prices, are observable on a public blockchain. In this way, the relative value of all content units or services is understood as salient, calculable, transferable and tradable.

The implications of these denotations, however, depend on varying conceptualisations of 'value'. We will discuss these conceptualisations below, comparing classical, neoclassical and heterodox approaches to value creation, as well as the implications of the concept of public value. The classical approach is understood to be constituted by the works of seminal authors before the 20th century – such as Adam Smith, David Ricardo and Karl Marx – that saw labour as central to value creation. The neoclassical approach that dominates current mainstream economics emerged in opposition to the classical approach, establishing the rational perception of utility by buyers as central to the definition of value. Heterodox approaches such as evolutionary and institutionalist economics challenge the neoclassical approach by arguing that value creation processes and value perceptions are path dependent and rely on interactions between different institutions that may, however, have rather different rationales and understandings regarding what is of value.

We limit our analysis to these broad approaches (which all have their inherent differences) as they provide the most distinctive alternatives to interpreting the implications of the emergent new iteration of the internet. The analysis demonstrates how these value theories lead to different social imaginaries on the future of the internet. The conceptualisation of the 'social imaginary' builds on work by Robin Mansell (2012) who used it to describe the differences in the way societal actors understand and make sense of the dynamics of technological innovation. As such the concept of an imaginary constitutes a basis for a critical analysis of their interests and actions in information society evolution.

Neoclassical interpretation_

When the Web of Value is understood to mean trading between individuals, and the value of an asset is expressed in price. Price is mainly determined by the asset's scarcity (as in the case of non-fungible tokens) and by its utility to buyers; this could be understood as a neoclassical approach to value. Neoclassical economics has dominated micro-economics since the 1950s and together with, first, Keynesian and, later, New Keynesian economics has formed the 'neoclassical synthesis', constituting what is understood as contemporary mainstream economics. Its view of value creation makes a few specific assumptions: firstly, that all buyers are universally capable utility calculators who know what is best for them

and what price to pay for a given asset, given its utility and scarcity; and, secondly, that monopolies are not able to interfere in the market by price-setting. Such assumptions have been questioned by scholars within heterodox economics, especially those working within evolutionary and institutional economics.[3] Their critique of monopolies has been relevant in the context of both contemporary finance (dominated by banks) and the internet economy of information goods (dominated by platforms). Banks and platforms are seen as centralised institutions whose semi-monopoly position is enabled either by state regulations (licences to banks) or the specific features of internet economies (network effects, multi-sided markets). Their dominance is seen as a distortion of markets and is understood to have motivated various kinds of blockchain-enabled decentralisation efforts.

While the ethos of Web3 is about decentralisation, it has been suggested that defining value through price and scarcity encourages speculative activities that are not processes of value creation, but mere value extraction. Mazzucato (2018b, p. 221) has critiqued that Web 2.0 platforms typically have not created value themselves, but have been able to extract value from the contributions of others on their platforms. This has been possible due to the network effects of these platforms and their control over the multi-sided markets they have facilitated. That is, they have been in the position to extract value from the data-resources at their disposal. In the case of Web3, a risk could emerge again when internet content or services (e.g. books, videos, videogame accessories, licences, tickets, etc.) are turned into financial assets. The focus remains on value extraction in the form of resulting operations with those assets, and the development of various financial instruments (derivatives such as futures, swaps, etc.), which could be compared to the 'financialisation' of the real economy and its known risks. These include: a focus on short-term profits instead of long-term investment; a gradual transfer of assets into the hands of the few; non-productive rent becoming a dominant activity; and the emergence of monopolies. All this, in effect centralisation of resources (tokens of various kinds) instead of decentralisation, could limit wider access to cultural/information services and to participation in value creation (Lotti, 2018).

The emergence of monopolies is typically seen as undermining productivity and wider value creation since monopolies exploit their position to seek rent.

Ricardo (1817) was the first to define rent as a reward for the ownership of a resource, but not as a contribution to societal wealth creation. In the context of Web 2.0 it has been the ownership of dominant platforms, typically following early entry into a specific digital services market and the resulting network effects and the eventual (semi-)monopoly status of the platforms, that has enabled similar rewards to be sought (Christophers, 2020, p. 182; Mansell & Steinmuller, 2020, p. 38; Sadowski, 2019; 2020). The potential wider financialisation in Web3 could bring about similar dynamics, as early elite investors could gain control over majority stakes in available assets (Zook & Grote, 2020).

Yet, blockchain-based financial ecosystems were created in opposition to centralisation in financial markets and value extraction via rent, that is, in opposition to banks 'creating money' (issuing debt without necessary reserves). This opposition to monopolies, especially content mediation platforms and their value extraction practices, could still be seen as the driving ethos of the Web3 industries (Jin et al., 2022). Nakamoto's (2008) proposition for the transparent and collective appropriation (block production and network governance) of the means of monetary production has been seen by some as echoing, paradoxically, Marx's call for the collective appropriation of the means of production (Alizart, 2020). This suggests that the neoclassical interpretation of how value ought to be created in the Web of Value is neither prevalent nor without alternatives.

To summarise: the neoclassical approach to value emphasises how value equals price, and how price depends on perceptions of scarcity and utility. From this perspective, the Web of Value refers to the technological apparatus where the scarcity of an asset is always clear, as is its resulting price – when all assets and transactions can be accessed on public blockchains they become a matter of public record, together with their history (which communicates the evolution of their perceived value and utility). The risk in this particular perception of value is that it focuses on market speculation and value extraction, which may lead to excessive financialisation of the internet economy.

Heterodox interpretations_

Institutional and evolutionary economic approaches emerged in the course of the early 20th century and today form the leading approaches

within heterodox economics. They present an alternative to mainstream economics while focusing mainly on the phenomena of change and innovation. One of the central contributions from these approaches has been the linking of communicative action (meaning systems), community evolution and the values that emerge in such communities with the concept of economic value. When neoclassical economics understands the purpose of economics as studying the production and distribution of scarce resources then institutional economics understands the economy as being made of rules set by all kinds of institutions and communities. Building on Veblen, Commons and Dewey, the neo-institutionalist Marc R. Tool (1979), for instance, argued that economic value is expressed in 'the continuity of human life and the noninvidious recreation of community through the instrumental use of knowledge'. In this view, values or related perceptions of utility are never individual, but are constituted by the communities via communicative means. Both digital ledgers and money are important media for coordinating such communication.

That money is another medium (of value) has been highlighted since Aristotle. But it can only function as a medium of value communication when it is used for payments. Swartz (2020, p. 16) argues that communication through payments knits humans together in a shared economic world: transactional communities. Members of such communities might share imbricated senses of identity, geography, temporality, discourses, politics and practices, but they must all share a belief in the particular money as a medium of value. What, how and when is typically bought and sold for this money distinguishes transactional value communities. 'When we exchange money, we agree not just on its quantity but on its meaning. The technologies of money – which make it transactable and valuable – are mechanisms of maintaining these shared understandings' (Swartz, 2020, p. 18). Swartz posits that in the contemporary technological environment we should talk about money and payments not just as media but as 'social media' – referring to the participatory and communal nature of many of the contemporary payment technologies and platforms. These technologies have 'memory': transactions are recorded, often publicly, and this makes transactional communities visible and purchases explicit, in order to communicate the sociality and values attached to the transactions. Such public communications start functioning self-referentially; the community 'auto-communicates' (Hartley et al., 2021, pp. 79-82) and it becomes aware of itself. Yet, the firms that run the payment systems of

Web 2.0 type platforms (Venmo, WeChat, AliPay) have control over such community auto-communications and their communal memory-making and, therefore, self-creation. It is in this context that distributed ledgers have emerged as an alternative governance apparatus, as they facilitate a distributed transactional memory that could enable transactional communities to become autonomous and self-coordinating.

The evolution of transactional communities with their own distinctive memories and value systems could also be understood in the growth of blockchains, their coins, other tokenised assets and in the emergence and multiplication of decentralised autonomous organisations (DAOs; see Hassan & De Filippi, 2021). Blockchains and DAOs (especially when the latter issue their own tokens) become distinct transactional communities because they are linked by a shared medium of value. As participation in such networks is typically rewarded by the network's money or other assets, loyalty to the network is architecturally enforced. Alizart (2020, p. 37) emphasises that as blockchain participants all have roles (as block creators, validators, etc.) they are not merely utility receivers; rather, they are network owners and in the same way its 'civil servants'. In this way, what is private and what is public converges in effect. DAOs could be seen as providing new technological affordances to the operations of economic co-operatives, but may also present the risk of financialising all their operations (Schneider, 2022). Nevertheless, this perspective suggests that Web3 could emerge as a constellation of novel institutional forms (Berg et al., 2019), tied by distributed ledgers as new value media with the potential to improve wider participation in value production, especially with regard to information goods, such as media content and cultural services. The multiplication of such communities could lead to further diversification of value systems.

To summarise: there is a view, based on versions of institutional and evolutionary economics, that value is collectively produced and value systems are specific to communities, and that blockchains are not only making this explicit but enforcing the multiplication of such systems in the economy. The Web of Value could henceforth refer to the Internet era when such multiplication takes place through the broad implementation of monetary self-governance and decentralisation technologies.

Classical approaches to labour as value_

Decentralisation technologies could also once again make relevant what are known as classical approaches to value creation. The classical economists Adam Smith, David Ricardo and Karl Marx highlighted that value is initially created by labourers – those who produce something that could have exchange value in the market. They all criticised, in various ways, forms of rent-based value extraction. Their critiques evolved at different stages of early industrialisation, when the role of individual labour in value creation became gradually less clear. This process has culminated in the digital economy, where value is created in collaborative processes by multitudes of diverse actors, but where individual contributions are often difficult to trace. As a result, labour has become immaterial, untransparent and immeasurable (Hardt & Negri, 2005), thus strengthening the neoclassical, demand-based view of value creation. The difficulties in identifying and measuring cultural content creation labour have arguably led to exploitation, insecure and uneven rewards to labourers (Dal Jong & Feenberg, 2015; Duffy, 2015; Terranova, 2000) and has empowered the positions of centralised intermediaries, such as large platforms, broadcasters and publishers.

In this context, one of the imaginaries related to the Internet of blockchains is the ability to record labour by means of smart contracts. It builds on Locke's (1690) concept of 'just deserts'; that is, in an economic system in which individual labour is important, it is possible to identify and then condition just rewards. While much of the technological innovation, especially recently, has focused on surveilling labourers (Böhm & Land, 2012; Moore, 2019), the situation could be understood as potentially different with public blockchains. With smart contracts, digital labour could be traced across a supply chain, and who produced or repurposed what would be on the public record – in effect open data. It could become evident how value is built when each of its components is contributed by, for instance, independent labourers and small firms. To bring this about, governments have started to set up blockchain-based digital infrastructures of registries that would underpin cultural production ecosystems (for instance, copyrights registries). These could enable identity management, data security, asset provenance, contracting and value transfer (Potts & Rennie, 2018; Norta et al., 2018). There are several such projects currently in development in the EU, Australia, etc. These are typically

understood as base-layer infrastructures enabling the further operations of Web3-type cultural industries.

To summarise: there is an expectation that decentralisation technologies could highlight the role of individual productive labour in value creation and, in doing so, undermine the dominant methods of unproductive value extraction in digital markets.

Public value_

Studies of economic value have always featured discussions on the distinction between public and private value. Aristotle, for instance, distinguished between exchange value and use value (potentially by all members of the public). As suggested above, these distinctions could become blurred in blockchain governance and in how blockchain networks create value. Contemporary studies of public value creation first emerged in response to *New Public Management Theory*, which was driven by the aim to make the public service more 'businesslike' and to improve its efficiency by using private sector management models – in line with ideas within neoclassical micro-economics. The proponents of the public value theory (Moore, 1995; Benington & Moore, 2011; Mazzucato, 2018a; 2018b; McBride et al., 2019) have instead focused on the role of governments or public agencies as dynamic innovators and co-creators of value in the interest of the wider public. While Moore and Benington (2011) have emphasised that governments ought to secure a functional public sphere where shared values are agreed upon and then pursued collaboratively by multiple agencies, Mazzucato, based on the ideas within evolutionary economics, has highlighted the public sector as a risk-taker and innovator in the interest of the wider society, including private sector innovators.

Such focus on the public sector could be seen as being in contrast with the ethos of the decentralisation technologies that have been about avoiding dependence on the centralised authority of government. Yet, we propose that the public value concept is relevant in interpreting the Web of Value promise from another angle. This is, firstly, because all public blockchains could be understood as being providers of public value: as technological infrastructures, they provide non-discriminatory use value to all parties. Secondly, as peer-to-peer technologies, they presume the pooling or sharing of resources, a commitment to a common purpose

and contributions to their governance. This brings about the blurring of private and public, as discussed above.

Also, as discussed in the previous section, rationales exist for governments either to use blockchain technologies or to contribute to autonomous initiatives when they see that a particular network or infrastructure could create broader public value to society. One example of this is the European Commission's blockchain strategy, which foresees the development of the European Union's own public services blockchain, which would be interoperable with private sector (public) blockchains. Such potential interoperability follows the understanding of Benington and Moore (2011, p. 15) that, in complex digital economies, public value emerges from the interconnections and interactions between heterogeneous sets of parties, sites and networks. The role of government therein is not one only that of a rule-setter or service provider for various value creators, but of a proactive shaper of the public sphere, interlinking parties and directly creating (public) value. In the context of Web3 development this could mean that government-provided ledgers (with regard to securing data on identities, asset provenance, rights, legal statuses and other contextual aspects) provide use value to all network participants, but in the process it could also limit the potential financialisation of interactions within the Web3 space.

To summarise: when interpreting the meaning of the Web of Value, it is important to distinguish the concept and functions of 'public value' and the role of public agencies in the broader 'value ecosystems' of Web3.

Conclusion_

The term Web of Value typically refers to a forthcoming era where most internet content and services are tokenised and turned into assets to be traded. This implies that the value of those assets emerges during trading, at equilibrium points determined by both the scarcity of assets and their demand by and utility to buyers. This interpretation should be recognised as a neoclassical approach to value, which could drive the financialisation of the internet economy. Building on classical political economy and heterodox economics, it is possible to demonstrate alternative ways to interpret value creation in the Web of Value. Based on these, distributed ledgers could be used to highlight the role of labour in value

creation and to empower workers. Decentralisation technologies could also be used to highlight how value is produced communally, facilitating the multiplication of value systems. Lastly, novel forms of decentralised governance could facilitate a partial convergence of public and private value creation and lead to new ways for public agencies to provide public value on the internet. However, all the various interpretations of the Web of Value promise competing imaginaries for the design of the future internet, central to which is the concept of value. As Mansell (2012) has shown, all the competing imaginaries, even if in conflict, end up in (interdisciplinary) dialogue and contribute to the shaping of the future internet.

References_

- Alizart, M. (2020). *Cryptocommunism*. Polity.
- Benington, J., & Moore, M. H. (Eds.). (2011). *Public value: Theory and practice*. Palgrave Macmillan.
- Berg, C., Davidson, S., & Potts, J. (2019). *Understanding the blockchain economy: An introduction to institutional cryptoeconomics*. Edward Elgar.
- Böhm, S., & Land, C. (2012). The new 'hidden abode': Reflections on value and labour in the new economy. *The Sociological Review*, *60*(2), 217–240. https://doi.org/10.1111/j.1467-954X.2012.02071.x
- Christophers, B. (2020). *Rentier capitalism: Who owns the economy, and who pays for it?* Verso.
- Duffy, B. E. (2016). The romance of work: Gender and aspirational labour in the digital culture industries. *International Journal of Cultural Studies*, *19*(4), 441–457. https://doi.org/10.1177/1367877915572186
- Floros, E. J. (2019). Web 3.0 – The internet of value. In S. Chishti, T. Craddock, & R. Courtneidge (Eds.), *The paytech book: The payment technology handbook for investors, entrepreneurs and fintech visionaries* (1st ed., pp. 127–128). Wiley. https://doi.org/10.1002/9781119551973.ch38
- Hardt, M., & Negri, A. (2005). *Multitude: War and democracy in the age of empire*. Penguin.
- Hartley, J., Ibrus, I., & Ojamaa, M. (2021). *On the digital semiosphere: Culture, media and science for the Anthropocene*. Bloomsbury.
- Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1556
- Jin, D. Y., & Feenberg, A. (2015). Commodity and community in social networking: Marx and the monetization of user-generated

content. *The Information Society*, *31*(1), 52–60. https://doi.org/10.1080/01972243.2015.977635

- Jin, L., Hamilton, G., Walden, J., Noon, S., Walkush, D., & Kothari, M. (2022, May 24). The ownership economy 2022 [Blog]. *Variant Fund*. https://variant.mirror.xyz/WwHDcojWvXU8mwYbcsvnN1kx6uLS4wV6fuS-ghkw3X4
- Locke, J. (1982[1690]). *Second treatise on government* (R. H. Cox, Ed.). Harlan Davidson.
- Lotti, L. (2018). Financialization as a medium: Speculative notes on post-blockchain art. In I. Gloerich, G. Lovink, & P. de Vries (Eds.), *MoneyLab reader 2: Overcoming the hype*. Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2018/01/MONEYLABREADER2OVERCOMINGTHEHYPE.pdf
- Mansell, R. (2012). *Imagining the internet: Communication, innovation, and governance*. Oxford University Press.
- Mansell, R., & Steinmueller, E. W. (2020). *Advanced introduction to platform economics*. Edward Elgar.
- Mazzucato, M. (2018a). *The entrepreneurial state: Debunking public vs private sector myths*. Penguin Books.
- Mazzucato, M. (2018b). *The value of everything: Making and taking in the global economy*. Allen Lane.
- McBride, K., Toots, M., Kalvet, T., & Krimmer, R. (2019). Turning open government data into public value: Testing the COPS Framework for the co-creation of OGD-driven public services. In M. P. Rodríguez Bolívar, K. J. Bwalya, & C. G. Reddick (Eds.), *Governance models for creating public value in open data initiatives* (Vol. 31, pp. 3–31). Springer International Publishing. https://doi.org/10.1007/978-3-030-14446-3_1
- Moore, M. H. (1995). *Creating public value: Strategic management in government*. Harvard University Press.
- Moore, P. V. (2019). E(a)ffective precarity, control and resistance in the digitalised workplace. In D. Chandler & C. Fuchs (Eds.), *Digital objects, digital subjects: Interdisciplinary perspectives on capitalism, labour and politics in the age of big data* (pp. 125–144). University of Westminster Press.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- Norta, A., Hawthorne, D., & Engel, S. L. (2018). A privacy-protecting data-exchange wallet with ownership- and monetization capabilities. *2018 International Joint Conference on Neural Networks (IJCNN)*, 1–8.

https://doi.org/10.1109/IJCNN.2018.8489551
- Potts, J., Cunningham, S., Hartley, J., & Ormerod, P. (2008). Social network markets: A new definition of the creative industries. *Journal of Cultural Economics*, *32*(3), 167–185. https://doi.org/10.1007/s10824-008-9066-y
- Potts, J., & Rennie, E. (2018). Web3 and the creative industries: How blockchain is reshaping business models. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3270663
- Ricardo, D. (1817). *Chapter III: On the principles of political economy and taxation*. John Murray.
- Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, *6*(1). https://doi.org/10.1177/2053951718820549
- Sadowski, J. (2020). The internet of landlords: Digital platforms and new mechanisms of rentier capitalism. *Antipode*, *52*(2), 562–580. https://doi.org/10.1111/anti.12595
- Schneider, N. (2022, August 11). *Cryptoeconomics as a limitation on governance*. https://mirror.xyz/ntnsndr.eth/zO27EOn9P_62jVlautpZD5hHB7ycf3Cfc2N6byz6DOk
- Skinner, C. (2016). *ValueWeb: How fintech firms are using Bitcoin blockchain and mobile technologies to create the Internet of Value*. Marshall Cavendish International.
- Swartz, L. (2020). *New money: How payment became social media*. Yale University Press.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin and other cryptocurrencies is changing the world*. Penguin Business.
- Terranova, T. (2000). Free labor: Producing culture for the digital economy. *Social Text*, *18*(2), 33–58. https://doi.org/10.1215/01642472-18-2_63-33
- Tool, M. R. (1979). *The discretionary economy: A normative theory of political economy*. Routledge.
- Upadhyay, N. (2019). *Unblock the blockchain*. Springer.
- Vadgama, N., Xu, J., & Tasca, P. (2022). *Enabling the Internet of Value: How blockchain connects global businesses*. Springer.
- Zook, M., & Grote, M. H. (2020). Initial coin offerings: Linking technology and financialization. *Environment and Planning A: Economy and Space*, *52*(8), 1560–1582. https://doi.org/10.1177/0308518X20954440

Endnotes_

1. Blockchain industries have coined the term Web3 to denote a new version of the internet that is expected to arrive after the era of Web 2.0. The latter is therein understood as dominated by platforms that typically provide services in exchange for users' personal data. Web3 is understood to rely on decentralised apps that run on blockchains, and is expected to allow users to autonomously control their various digital assets, including their personal data.
2. An example of this could be a solution provided by Book.io.
3. Evolutionary and institutional economics argue that any buyer rationality is contextual, depending on institutionally or culturally framed value systems, as well as on interactions with others representing those differing value systems or interpretations of utility. It has been demonstrated to apply especially in the case of information or cultural goods, where value perceptions depend on networked communicative activities with others (Potts et al., 2008). Both approaches have been addressing how the evolution of monopolies and other institutional continuities could limit degrees of freedom to price action.

TRACEABILITY_

Nanna Bonde Thylstrup, Department of management, society and communication, Copenhagen Business School, Denmark.
Matthew Archer, Graduate Institute for International and Development Studies, Geneva, Switzerland.
Louis Ravn, Copenhagen Business School, Denmark.

Traceability is the ability to identify and trace something or someone. Traceability is an increasingly prominent research topic in decentralised technosocial systems in fields as diverse as health, sustainability, finance, and supply chain management. At the same time, traceability connotes different meanings and potentialities within each of these fields. This Glossary article homes in on "traceability" as a concept that is deceptively simple but fundamentally crucial in blockchain technologies. First, the entry provides an overview of the historical background of traceability within digital technologies. The entry then outlines the most critical dimensions of the concept by relating the term to questions about accountability, explainability, and speculation. Finally, emergent methodological and theoretical insights concerning traceability as a paradoxical concept in distributed technologies are highlighted.

Introduction_

The Oxford English Dictionary (OED) defines "traceable" as something that is "capable of being traced". In the analogue world, various methods have been devised to ensure that objects and subjects are capable of being traced — things like seals and censuses and certificates and spreadsheets. Over the past few decades, digitalisation has allowed traceability efforts to intensify, expanding the scale and scope of things that are not only capable of being traced, but also leave traces seemingly everywhere, often inadvertently (Thylstrup, 2019, 2022). As Philip Agre outlines in his classic text "Surveillance and capture: two models of privacy", the development of technologies of traceability were in particular intensified by the emergence of standardised and globalised supply chain systems in the mid to late 20th century (Agre,

1994). Today, the growing ease of tracking and growing volumes of left-behind traces make the promise of perfect traceability seem increasingly achievable.

Blockchain technologies, in particular, have come to signify this possibility as a means of clarity within otherwise black-boxed infrastructures (Bertino et al., 2019; Kritikos, 2020). They have also, however, given rise to a new politics of traceability that is both imbricated in deeper power structures but also shaped by the new technological affordances of digital distributed ledger systems.

Histories of traceability_

The contemporary definition of traceability, according to the *Oxford English Dictionary*, has been shaped by diverse contexts, ranging from geography (1793) and natural theology (1802) to archaeology (1854) and physiology (1874). In addition, the OED cites a late 19th-century law journal, which argued that "The doctrine of following trust money depends on traceability," a meaning that is echoed in the common law definition of traceability (tracing) as the right to assert claims against one's property (Scott, 1965).

It is no coincidence that traceability occurs within the context of capital and control. Control derives etymologically from the French *contre-roule*, a duplicate of another document kept to crosscheck. The origins of the word control thus link to verification, later branching into broader meanings of management and surveillance in the 17th century (Chamayou, 2015). Therefore, traceability has historically been a critical factor in economies of scarcity and colonialism. It enables verification of ancestry and origins (Fourcade, 2012), as well as management techniques that create new information flows and control.

Ledgers are central traceability technologies, functioning as *contre-roules* designed to enable *verification* and *management*. The rendering of enslaved Africans as ledger entries, for instance, not only ensured control in the form of rights to locate and reclaim them in the case of escape but also gave rise to modern management practices (Browne, 2015; Rosenthal, 2018). Moreover, and sometimes relatedly, it gave rise to value speculation, for instance, in insurance claims (Baucom, 2005; Keeling, 2019).

Traceability in the age of blockchain_

In his work on the infrastructures of traceability in the digital age Professor of accounting Michael Power foregrounds three different "faces or ontologies" of traceability: ideational (traceability as regulatory ideal), material (traceability as technological infrastructure), and processual (traceability as organisational connectedness and distributed agency) (Power, 2019). *Ideationally*, traceability is a programmatic value related to the facilitation of regulation and accountability. In this regard, traceability means the ideal of accurately tracing people and things. *Materially*, traceability takes the form of diverse technologies (analogue and digital), including ledgers, passports, and blockchains. And *processually*, traceability is the continual establishment of connectedness across a multitude of organisations. Each of these ontologies, a word Power uses almost synonymously with "characteristics", is exceedingly relevant in the context of blockchain technologies: the growing interest in blockchains is connected, at least in part, to the radical promises of democratisation and decentralisation that blockchain proponents constantly expound; for several emerging traceability schemes, blockchain is the traceability infrastructure; finally, these schemes connect actors across organisational forms (producers, regulators, etc.) and levels (from individuals to institutions). Furthermore, each of these three ontologies further highlights the inherently political nature of traceability technologies, which, as Calvão and Archer (2021) show in the context of mineral supply chains, have "the potential to actively reshape socio-spatial scales and create new digital territorialities with impacts on livelihoods, control and intermediation, and social inclusion."

The *ideational* dimension of traceability in blockchain technologies embody the possibility of regulation and accountability through the affordances of their technological apparatus. In light of an ever-more globalised and complex world, distributed ledgers embody a regulatory ideal of knowing the origins and paths of people and things insofar as they promise accuracy and immutability. That is, distributed ledgers are claimed to capture in an accurate and tamper-proof way historical records of transactions, which then allow regulation and accountability through inquiries into them. This programmatic ideal of accurately tracing people and things is mirrored in various contexts of blockchain technology application from supply chain provenance (Kim & Laskowski, 2018) through accountability in governmental affairs (Aztori, 2017) to secure data sharing (Shrestha

et al., 2020). There is also, however, a tension between blockchain-enabled traceability as a regulatory ideal and demands for data justice, privacy and anonymity. In this context, for instance, groups such as the Center for Democracy and Technology (Kamara et al., 2021) and scholars at the Stanford Internet Observatory (Pfefferkorn, 2021) have expressed concerns about the implications of traceability for the future of privacy and anonymity. Scholars have in this context also pointed to the ambivalence haunting decentralised systems, because they are now both understood in terms of their evasion of regulation (Walker, 2021) and achievement of privacy (Bodó et al., 2021) as well as facilitating the very same through traceability. Thus, the ideational ontology of traceability in distributed ledger technologies is paradoxically implicated in a tension between the potential for regulation and accountability, and a commitment to their evasion.

Materially, the technological architecture of blockchain is emblematic of the material face of traceability. This stems mainly from the material affordances of digital distributed ledgers which constitute a specific type of database maintained on a distributed network, whose participants, therefore, have a shared, identical, and ideally tamper-proof record of transactions (Davidson et al., 2016). Most crucially, and because of this, they differ from traditional ledgers in that they prevent the need for a central trusted third party (Maurer, 2016). On a fundamental level, the word "blockchain" itself encapsulates the particular materiality of traceability: "blocks" capture detailed data that is then linked to each other in a historically linear and traceable "chain". In this vein, Power (2019) stipulates: "Blockchain is, therefore, the dream of, the metaphor for, a perfect, uniquely referential, precise traceability infrastructure" Scholars have also, however, pointed out that this imaginary of blockchain is sometimes far removed from the reality of blockchain technology in use (Power, 2019; Calvão & Archer, 2021). While blockchain technologies may reify the computational imaginaries of linear time, now down to the "femtosecond" as Geoffrey Bowker observes (Bowker, 2021), they also operate as a chain of translation. As Marieke de Goede (2018) notes, such chains always involve a "dynamic process of continuous circulation, referral, and contestation" producing not only a politics of logistics but also of modification. Thus the imaginary of blockchains as producing a neatly iterated trace that can be followed from one point in time to another point in time obscures the self-referential relationships

and feedback loops that such traceability initiatives invariably generate and the iterative information ecologies they are part of (Amoore, 2019).

Moreover, blockchain technologies, which rely on inordinate inputs of physical resources (energy and water, in particular) and produce increasingly vast amounts of (Cooper 2021), exemplify the material contradictions of traceability. Nevertheless, the promise of traceability in the context of blockchain technologies is premised on specific technical characteristics of distributed ledgers, even if claims about those characteristics do not match the reality of actually-existing blockchains. Importantly, distributed ledgers differ from traditional ledgers in that they prevent the need for a central trusted third party (Maurer, 2016). In doing so, distributed ledger technology allows the consensus-building process in socio-economic matters to be shifted away from governments and big corporations, with whom these competencies traditionally rested, leading Davidson et al. (2016) to theorise blockchains as a kind of institutional innovation. Moreover, the purportedly "trust-free" nature of distributed systems facilitated the emergence of self-executing *smart contracts*, enabling the verification of transactions without human interference (Maurer, 2016). Although a growing body of critical scholarship has rejected many of these claims about the immutable, decentralised, and trust-free nature of blockchains, these narratives persist in popular discourse and are fundamental to the promise of blockchain-enabled traceability schemes.

Distributed ledger technologies also bear the imprint of traceability's processual trait. Crucially, the processual establishment of connectedness links discrete organisational entities into an interconnected, dynamic infrastructure. This is a prerequisite for inquiries into the traces of objects moving through time and space (Power, 2019). For instance, this is a relevant undertaking in supply chains that span organisational boundaries, where blockchain-based traceability platforms have been proposed as a solution (Da Cruz & Cruz, 2020). The highly scattered and crime-ridden fisheries industry, for example, whose stakeholders include businesses, governments, and NGOs, is made governable through distributed ledgers by means of continual processes interlinking these stakeholders (WWF, 2018; Cruz & Da Cruz, 2020). Similarly, blockchain technologies are deemed suitable for the promotion of international cooperation (Reinsberg, 2021), and as fitting platforms for a well-functioning Internet of Things (Reyna et al., 2018). In doing so, distributed ledger technologies foster distributed modes

of agency and shared responsibility among the implicated organisations. Such modes of governance through processual traceability, however, are themselves generative of novel demands and expectations whose fulfilment, failure, and surpassing imply a politics of traceability. Distributed ledger technologies emerged amid growing societal demands for traceability, providing a technical solution to a particular problem, even as their rapid adoption across different contexts and in different industries has generated new problems of untraceability. Processual traceability through distributed ledger technologies is thus a dynamic practice that links discrete organisational entities into interconnected structures, thereby enacting distributed modes of agency and shared responsibility, and indexing an evolving politics of traceability.

Traceability as accountability, explainability, and speculation_

Having outlined some of the distinct but interconnected facets of traceability, we now turn to three recurring issues cutting across discourses on distributed ledger technologies: traceability as accountability, explainability, and speculation. Firstly, traceability is linked to concerns about accountability, the attainment of which through distributed ledgers is at once promised and questioned by emergent scholarly literature. Secondly, traceability through distributed ledgers relates to explainability insofar as the traces captured on them spark debates about the possibility of accurately explaining diverse spatio-temporal trails. Finally, traceability is also embroiled in speculative matters in the sense of giving rise to new forms of speculations of value.

Accountability_

While traditional ledgers and audit regimes have historically offered traceability techniques of accountability to privileged groups in society (e.g., Baucom, 2005), blockchain-enabled traceability initiatives were and are often praised for their democratising and empowering potential by, for instance, enabling citizens of the developing countries to hold their governments accountable (Kshetri, 2017; Pilkington et al., 2017) or giving consumers access to accurate information about the origins of the products they buy. On a more general level, these hopes are linked to the projected empowering character of blockchain technologies (Tapscott

& Tapscott, 2016). However, a growing critical literature has exposed the illusory nature of these optimistic claims (Roubini, 2018; De Filippi, 2019).

Emergent empirical and theoretical insights in the domain of supply chains serve to demonstrate this. For example, Calvão & Archer (2021) expose that the reality of blockchain use in mineral supply chains is characterised by a growing pervasiveness of private blockchains run by powerful corporate actors, which serves to further marginalise – rather than empower – artisanal miners and other communities at the so-called bottom of the pyramid. Similarly, Kshetri (2021) highlights that while blockchain-enabled traceability under the pretext of accountability has a promising outlook, it is at odds with reality. Because multinationals often design blockchains according to their preferences, they also reinforce existing power imbalances. Thus, blockchain-enabled traceability initiatives for accountability seem to primarily operate in the interests of powerful corporate actors. On one hand, this makes sense: blockchains store information about people and things, and as philosophers from Bacon to Foucault have shown, those who have access to information about people and things tend to have some degree of power over them. Like any other tool or technology, blockchains are inseparable from the social context in which they are used. What is new is the extent to which an overarching concern with traceability has motivated the adoption of blockchain technologies, and the extent to which other desirable outcomes (such as accountability, but also sustainability, democracy, human rights, and so on) increasingly presuppose an embrace of technologically-mediated traceability. This is distinct from the motivation behind other forms of record keeping, such as national or imperial censuses, which were primarily motivated by a desire to collect the accurate amount of taxes from an accountable population. Even if traceability was also an aspect of censusing, which helps governments track migration both internally and externally, traceability seems to have only recently become a dominant ideation.

Explainability_

A second issue associated with traceability in blockchain technologies revolves around questions of explainability. This is particularly true to the extent that decisions based on the analysis of data stored on blockchains have to be explained to affected stakeholders. Through

an analysis of sustainability standards in the tea supply chain, Archer (2021) shows how the purported immutability of 'Big Data' stored on blockchains can be invoked to explain and therefore justify decisions that might otherwise seem unjust. Some sustainability standards stipulate that even household crops cannot be planted within a certain distance of rivers, a space known as a riparian zone, even though many smallholder farmers rely on this land for subsistence agriculture. When audits were paper-based, auditors could overlook these kinds of minor violations, but as audits become more frequent and even automated, and as the records these audits produce become digitised, that flexibility becomes nearly impossible, causing smallholder farmers to potentially lose their valuable sustainability certifications. In attempting to explain this harsh decision, standards developers and multinational companies both point to the objectivity of data and rules, obscuring the human aspects of certification (or, in this case, decertification) behind a rigid veneer of quasi-algorithmic governance. Underlying all this is a fairly straightforward explanation: in order for sustainability certifications to be of value, the products to which those certifications are affixed need to be traceable all the way back to a farm that complies with the standard in question. While blockchain enthusiasts typically foreground the immutability of data stored on blockchains (Tapscott & Tapscott, 2015), it is crucial to keep in mind that entities rendered as data in a blockchain are, like all data, never "raw" or neutral (Gitelman, 2013). Power (2019) reminds us that "technologies of trace creation like blockchain are always imperfect and incomplete realizations of the ideals that motivate them.".

Speculation_

Thirdly, traceability through blockchain technology seems to have engendered new forms of speculations of value. Even the most prominent blockchain-undergirded cryptocurrency, Bitcoin, is used by most not as a medium of exchange but as a speculative asset (Baur et al., 2018). More recently, NFTs, which afford to uniquely identify the owner of a digital artefact, have attracted public attention and monopolised the discourse around blockchains. The staggering sums demanded for NFTs have led many to predict a speculative bubble (Ball, 2021).

The fact that a substantial share of both Bitcoin's and NFTs' utility seems to stem from their speculative potential further demonstrates

that distributed ledgers constitute yet another, but not novel, form of traceability to govern economic relations in well-known ways. Bitcoin, in particular, despite its advertisement by figures like Elon Musk as a radically decentralised and democratic currency, has generated vast amounts of greenhouse gas emissions and has engendered resource conflicts between bitcoin miners and Indigenous communities, and is only valuable insofar as it is easily exchanged with the currencies like the US dollar and euro that Bitcoin advocates so callously deride. As Caliskan (2020) astutely observes, blockchain never truly disintermediates, but simply reintermediates, (re)inscribing unequal power relations even as it gives rise to newly empowered intermediary organisations.

Conclusion_

Traceability is the ability to identify and trace something or someone. Optimistic narratives about the promise of blockchain-enabled traceability tend to be unfounded, obscuring a reality wherein traceability schemes are designed in a way that empowers those who collect, store, and control access to the increasingly vast quantities of data that constitute the digital traces of both people and products. From modern slavery (Nolan & Boersma, 2019) and unaccounted-for emissions to harmful AI systems (Kritikos, 2020) and online privacy, the framing of diverse social and environmental problems as a purely technical challenge of either too much or too little traceability presupposes purely technical solutions that are divorced, discursively at least, from the social contexts in which technologies like blockchains are developed and deployed. But technology never exists in a vacuum, and the politics of traceability are intimately and inextricably linked to the politics of technology.

Things leave traces as they move along a path through space and time from an origin to a destination. The extent to which these traces are interpretable as discrete objects and the extent to which those interpreted objects can be used to map the specific path of a specific thing from a specific origin to a specific destination is the traceability of that thing. From stone blocks to blockchains, from individuals to dividuals, from oral histories to smart contracts, technologies of traceability are certainly not a recent phenomenon. What is new, and what demands much more critical attention, is the increasing prominence of digitally-mediated traceability schemes as a proposed solution to problems ranging from financial

wellbeing to climate change mitigation to food safety to border security. The ideational foundation of these schemes, the materiality of traceability technologies, and the processes involved in their development, adoption, and resistance are always already technopolitical; thus, whether one is interested in traceability as accountability, as a mode of explainability, or as speculation about value(s), the politics of traceability technologies like blockchain must remain front and centre.

References_

- Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, *10*(2), 101–127. https://doi.org/10.1080/01972243.1994.9960162
- Amoore, L. (2020). *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Duke University Press. https://doi.org/10.1215/9781478009276
- Archer, M. (2021). Imagining impact in global supply chains: Data-driven sustainability and the production of surveillable space. *Surveillance & Society*, *19*(3), 282–298. https://doi.org/10.24908/ss.v19i3.14256
- Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5
- Ball, J. (2021, March 13). How non-fungible tokens became the latest tech speculation bubble. *The Guardian*. https://www.theguardian.com/technology/2021/mar/13/how-non-fungible-tokens-became-the-latest-tech-speculation-bubble
- Baucom, I. (2005). *Specters of the Atlantic: Finance Capital, Slavery, and the Philosophy of History*. Duke University Press. https://doi.org/10.1215/9780822387022
- Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, *54*, 177–189. https://doi.org/10.1016/j.intfin.2017.12.004
- Bertino, E., Kundu, A., & Sura, Z. (2019). Data transparency with blockchain and AI ethics. *Journal of Data and Information Quality*, *11*(4), 1–8. https://doi.org/10.1145/3312750
- Bodó, B., Brekke, J. K., & Hoepman, J.-H. (2021). Decentralisation:

A multidisciplinary perspective. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1563

- Bowker, G. C. (2021). Life at the femtosecond. In A. Volmar & K. Stine (Eds.), *Media Infrastructures and the Politics of Digital Time* (pp. 125–142). Amsterdam University Press. https://doi.org/10.1515/9789048550753-008
- Browne, S. (2015). *Dark matters: On the Surveillance of Blackness*. Duke University Press.
- Caliskan, K. (2020). Data money: The socio-technical infrastructure of cryptocurrency blockchains. *Economy and Society*, *49*(4), 540–561. https://doi.org/10.1080/03085147.2020.1774258
- Calvão, F., & Archer, M. (2021). Digital extraction: Blockchain traceability in mineral supply chains. *Political Geography*, *87*, 102381. https://doi.org/10.1016/j.polgeo.2021.102381
- Chamayou, G., & Lloyd, J. (2015). *A theory of the drone*. The New Press.
- Cooper, Z. G. T. (2021). The deep time of Bitcoin: Excavating the "work" in proof-of-work cryptocurrency systems. *AoIR Selected Papers of Internet Research*. https://doi.org/1631738507
- Cruz, E. F., & Da Cruz, A. M. R. (2020). Using Blockchain to Implement Traceability on Fishery Value Chain. *Proceedings of the 15th International Conference on Software Technologies (ICSOFT*, 501–508. https://doi.org/10.5220/0009889705010508
- Da Cruz, A. M. R., & Cruz, E. F. (2020). Blockchain-based Traceability Platforms as a Tool for Sustainability. *Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020*, *2*, 330–337. https://doi.org/10.5220/0009463803300337
- Davidson, S., De Filippi, P., & Potts, J. (2016). Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2811995
- De Filippi, P. (2019). Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream. *Decentralized Thriving: Governance and Community on the Web 3.0*. https://hal.archives-ouvertes.fr/hal-02445179/document
- De Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*. https://doi.org/1583850246
- de Goede, M. (2018). The chain of security. *Review of International Studies*, *44*(1), 24–42. https://doi.org/10.1017/S0260210517000353
- Fourcade, M. (2012). The Vile and the Noble: On the Relation

between Natural and Social Classifications in the French Wine World. *The Sociological Quarterly*, *53*(4), 524–545. https://doi.org/10.1111/j.1533-8525.2012.01248.x

- Gitelman, L. (Ed.). (2013). *"Raw Data" is an Oxymoron*. The MIT Press.
- Kamara, S., Knodel, M., Llansó, E., Nojeim, G., Qin, L., Thakur, D., & Vogus, C. (2021). *Outside looking in: Approaches to content moderation in end-to-end encrypted systems* [Report]. Center for Democracy and Technology. https://cdt.org/insights/report-outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/
- Keeling, K. (2019). *Queer times, Black futures*. New York University Press.
- Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*, *25*(1), 18–27. https://doi.org/10.1002/isaf.1424
- Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly*, *38*(8), 1710–1732. https://doi.org/10.1080/01436597.2017.1298438
- Kritikos, M. (2020). *What if blockchain could guarantee ethical AI?* Think Tank European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2020)656334
- Kshetri, N. (2021). Blockchain and sustainable supply chain management in developing countries. *International Journal of Information Management*, *60*, 102376. https://doi.org/10.1016/j.ijinfomgt.2021.102376
- Maurer, B. (2016). *Re-risking in Realtime. On Possible Futures for Finance after the Blockchain*. https://doi.org/10.6094/BEHEMOTH.2016.9.2.917
- Nolan, J., & Boersma, M. (2019). *Addressing Modern Slavery*. University of New South Wales Press.
- Pfefferkorn, R. (2021, March 3). New Intermediary Rules Jeopardize the Security of Indian Internet Users [Brookings Institute]. *Tech Stream*. https://cyber.fsi.stanford.edu/io/news/new-intermediary-rules-jeopardize-security-indian-internet-users
- Pilkington, M., Cordu, R., & Grant, L. G. (2017). Blockchain and bitcoin as a way to lift a country out of poverty — Tourism 2.0 and e-governance in the Republic of Moldova. *International Journal of Internet Technology and Secured Transactions*, *7*(2), 115–143. https://doi.org/10.1504/IJITST.2017.087132
- Power, M. (1997). *The audit society: Rituals of Verification*. Oxford University Press.

- Power, M. (2019). Infrastructures of traceability. In M. Kornberger, G. C. Bowker, J. Elyachar, A. Mennicken, P. Miller, J. R. Nucho, & N. Pollock (Eds.), *Research in the Sociology of Organizations* (pp. 115–130). Emerald Publishing Limited. https://doi.org/10.1108/S0733-558X20190000062007
- Reinsberg, B. (2021). Fully-automated liberalism? Blockchain technology and international cooperation in an anarchic world. *International Theory*, *13*(2), 287–313. https://doi.org/10.1017/S1752971920000305
- Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046
- Rosenthal, C. (2018). *Accounting for Slavery: Masters and Management*. Harvard University Press.
- Roubini, N. (2018, October 15). Blockchain isn't about democracy and decentralisation — It's about greed. *The Guardian*. https://www.theguardian.com/technology/2018/oct/15/blockchain-democracy-decentralisation-bitcoin-price-cryptocurrencies
- Scott, M. (1965). The right to "trace" at Common Law. *Australian Law Review*, *7*(4), 463–489.
- Shrestha, A. K., Vassileva, J., & Deters, R. (2020). A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives. *Frontiers in Blockchain*, *3*, 497985. https://doi.org/10.3389/fbloc.2020.497985
- Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*.
- Thylstrup, N. B. (2019). Data out of place: Toxic traces and the politics of recycling. *Big Data & Society*, *6*(2), 2053951719875479. https://doi.org/10.1177/2053951719875479
- Thylstrup, N. B. (2022). The ethics and politics of data sets: deleting traces and encountering remains. *Media, Culture & Society* (forthcoming).
- Walker, M. C. W. (2021, September 28). Designed to avoid regulation – the real roots of bitcoin. *LSE Business Review*. https://blogs.lse.ac.uk/businessreview/2021/09/28/designed-to-avoid-regulation-the-real-roots-of-bitcoin/
- WWF. (2018). *New Blockchain Project has Potential to Revolutionise Seafood Industry*. WWF New Zealand. https://www.wwf.org.nz/what_we_do/marine/blockchain_tuna_project/

TRUST IN DISTRIBUTED TECHNOLOGIES_

Moritz Becker, Weizenbaum Institute for the Networked Society, Berlin, Germany.
Balázs Bodó, Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands.

Trust can best be understood as a relational attribute between (1) a social actor and other actor(s) (interpersonal trust) and / or (2) actors and institutions (institutional or systemic trust) and (3) institutions and (trusting) actors (trust as shared expectations), where institutional frameworks define the nature and strength of trust relationships between different actors.

Conceptual background_

The notion of *trust* is of key significance, with a broad literature spanning from social sciences via law to computer science (Blöbaum, 2016; Bodó, 2020; Botsman, 2017; (Clarke et al., 2006), 2006; Fukuyama, 1995; Gambetta, 1988; Giddens, 1990; Hardin, 2002; Luhmann, 2017; McKnight et al., 2011; Putnam, 2001; Schneier, 2012; Sztompka, 1999). This leads to substantial confusions when it comes to discussing trust in the context of digital technologies in general, and in the case of distributed technologies in particular (Baldwin, 2018; Bellini et al., 2020; Dingle, 2018; Jacobs, 2020; Werbach, 2018a). We do not try to represent all aspects of these different disciplinary discussions, instead, we used a simplified model of trust adapted from the work of McKnight et al. (2011) to give a basic overview, point out the most relevant issues, and provide a working definition of trust in the context of blockchain and other distributed techno-social systems.

Trust relationships always involve a number of actors: (1) a trustor, with his or her individual attitudes, trusting beliefs, stands towards trusting, and "generalized faith in humanity", (2) a trustee, that can be an individual, in which case we talk about interpersonal trust (Hardin, 2002), or an institution, the government, or a profession, in which case we talk about institutional, or systemic trust (Giddens, 1990). Trust is the instrument with which the trustor manages the contingencies that relate to trusting the trustee to act competently, in the interest of the trustor in concrete given contexts.

The emergence of trust has three prerequisites. First, it depends on the attitudes, beliefs of the trustor. Second, it is a factor of the (perceived) trustworthiness of the trustee: its past actions, reputation, objectively verifiable, or faith based qualities to be competent, benevolent, and maintain integrity (Mayer et al., 1995). Third, both sides are embedded in wider, institutional environments, which create shared knowledge, a shared understanding of general, and context specific rules of the game (Shapiro, 1987; Zucker, 1985), and which can provide structural assurances on the behaviour of the trustee for the trustor. These latter include legal instruments, such as laws (Balkin, 2016; Hall, 2002), contracts (Foorman, 1997), government regulatory and oversight bodies, professional codes of conduct, governance and quality assurance, or market-based functions, such as insurance against risk.

Trust and distributed technologies_

Within the context of trust and distributed technologies, therefore, the question of trust can have many dimensions. If the role of the distributed techno-social system is to connect people, if it allows, or relies on the collaboration of individuals, in the interpersonal trust dimension, the question is how can we (or: do we need to) trust the (often anonymous) stranger with whom we use the same distributed system. On the other hand, we also need to have some level of confidence in the system itself, and in that case we need to look at the institutional aspects of trust. Here, the main question is whether the technologies we rely on are trustworthy (Bodó, 2020). We can define technology in a narrow way, and thus the questions of trust in and trustworthiness of technical systems, and artefacts is simplified into the question of technical reliability: the security of computer systems, them being free of errors, and bugs, working as intended and advertised (Clarke, 2006). A broader definition would also consider the human and institutional elements which develop and operate those technical systems, and therefore give them agency. In such an approach, the question of trust becomes more akin to more traditional forms of institutional trust. The governance of technology covers these human and institutional elements, and the impact of the governance on the trustworthiness of technical systems turned this issue into a rapidly developing research field (Campbell-Verduyn, 2018; Elkin-Koren & Perel, 2019; Katzenbach & Ulbricht, 2019; Mattila & Seppälä, 2018). Finally, some technical systems mediate and produce trust relationships

themselves (Bodó, 2020). For example, online reputation systems are designed to facilitate interactions that require trust. In these cases, the trustworthiness of these "trust producing systems" becomes an important issue in itself. The following remarks use blockchain as a case study to take a closer look at the controversies and questions associated with it from the perspective of trust.

The academic discussion on blockchain and trust_

Blockchain technology — which was first introduced in 2008 in the context of the digital currency Bitcoin — is often seen as a trust producing technology that might make trustworthy intermediaries such as banks obsolete. Instead, it is often said to replace human-based intermediaries by a "system based on cryptographic proof instead of trust" (Nakamoto, 2008, p. 1) i.e., a network in which all interactions between network participants are coordinated by mathematical and cryptographic code instead of human actors (Dodd, 2018, p. 37; Swartz, 2016). As a consequence, the technology takes a major role in the current public and academic discussion on trust and distributed technologies: some see it as a "machine for creating trust" (Berkeley, 2015), as reducing the cost of trust (Shahaab et al., 2020) or as an enabler of new technology-based modes of trust — "trustless trust" (e.g., Werbach, 2018a, 2018b; Hoffmann, 2015) or "distributed trust" (Botsman, 2017) — that might have a revolutionary impact on social coordination even outside the realm of distributed systems.

These academic discussions on blockchains and trust span across multiple disciplines such as computer science, economics, law and social sciences. Within these discussions, two key controversies can be identified: the first refers to the *conceptual* question of what is actually meant when referring to the term *trust*. The second controversy refers to the *substantive* question of how blockchain technology and trust are related: does blockchain increase trust, decrease trust, make trust obsolete, or represent a shift in the nature of trust?

Regarding the *conceptual* controversy, different understandings of trust can be identified. While some works understand trust as an attribute of the technological system itself (as e.g. suggested by 'trust models' rooted in computer sciences, see Harz & Boman, 2019), others rather understand trust as a system of intersubjective expectations between individuals that

is not necessarily determined by technology (more often so in the social sciences, e.g. Vidan & Lehdonvirta, 2018). From the perspective of trust research, it is vital to recognise these conceptual differences, as these might have a significant impact on the substantive conclusions taken in respect to the nature of trust. Moreover, many academic works provide no precise and theoretically-informed definition of trust (e.g., Davidson et al., 2018; Flood & Robb, 2017; Beck et al., 2016), leaving its meaning vague and ambiguous.

In addition to these conceptual differences, academic works also exhibit *substantial* differences regarding how blockchain and trust are related. Two dominant views can be identified. Proponents of the first view stress the "trust-free" (Beck et al., 2016) or "trustless" (Harz & Boman, 2019; De Filippi & Hassan, 2016; Davidson et al., 2018) capabilities of blockchain technology, assuming it to enable coordination without requiring interpersonal trust between network participants (Maurer et al., 2013, p. 261). In contrast to this view, the second line of academic works emphasises that blockchain networks are — in fact — not completely trustless and that trust enters the network at many levels and contexts (e.g. Corradi & Höfner, 2018, p. 203; Dodd, 2018; Vidan & Lehdonvirta, 2018). Rather than assuming it to abolish (interpersonal) trust, this line of studies rather argues for a *shift* of the nature of trust by blockchain, replacing interpersonal trust with trust (or: confidence, see De Filippi et al., 2020) in the distributed ledger itself (miners, consensus mechanisms, nodes), software developers (Walch, 2019) or new intermediaries (e.g. crypto-currency exchanges in Brekke, 2019, pp. 83-84).[1]

A similar conclusion of a shift in the nature of trust has been drawn in the academic discussion on "smart contracts" and their application in a legal context (Yeung, 2019; Finck, 2019; De Filippi & Wright, 2018). While, at first glance, smart contracts might offer new potentials of making trust obsolete due to the guaranteed execution of encoded legal obligations (Finck, 2019, pp. 72 ff), their real-life-application always requires trusted third parties (O' Hara 2017, p. 99), e.g. in the form of an "oracle" that supplies the smart contract with information from the outside world (De Filippi & Wright 2018, p. 75).

Takeaways for future research_

Against the background of these controversies, two things can be learned for the study of trust in distributed systems: firstly, they corroborate the insight that finding a common theoretical language of the technological aspects of trust among multiple academic disciplines is of utmost importance. Secondly, the oft-quoted finding that blockchain resulting in a shift of trust rather than its abolishment leads to new empirical follow-up questions:

For instance, do network users put trust in the technology itself or in the humans behind it (Walch, 2019, p. 59)?[2] What are sources of trustworthiness of distributed (blockchain) systems, particularly in the case of legal (un-) certainty? How do users behave *vis-à-vis* a system which may or may not be trustworthy, e.g. in the case of the blockchain-based venture capital fund "The DAO" (DuPont, 2018)? Are the technical aspects of a blockchain system enough to establish their trustworthiness (e.g. in the case of crypto-investors against questionable financial products)? How do past accounts of the trustworthiness of institutions (e.g. Sztompka, 1999) compare in relation to blockchain technology?

Addressing these questions should be an important objective for future academic research which might foster our understanding of blockchain technology and trust as well as the role of trust in distributed systems more generally. Important steps into this direction are for instance empirical studies on specific networks using blockchain technology (e.g., Woodall & Ringel, 2019; Meijer & Ubacht, 2018; Vidan & Lehdonvirta, 2018; Lustig & Nardi, 2015) as well as theoretical works that situate the case of blockchain within the broader discourse on trust and technology (e.g., Bodó, 2020; Jacobs, 2020). Moreover, as most empirical studies on trust and blockchain technology concentrate on the Bitcoin blockchain (e.g., Vidan & Lehdonvirta, 2018; Lustig & Nardi, 2015), it would be particularly interesting to see how this case compares to other blockchain applications.

Conclusion and working definition_

In conclusion, we face the following fundamental question: How can we (or: do we need to) trust the (often anonymous) stranger on the other side of a screen? The case of blockchain illustrates that the answer to this question is subject to the changes in our techno-social environment.

Blockchain technology can be viewed as exemplifying a change in mediation structures of trust from interpersonal trust mediated by human-based intermediaries to technological intermediaries. Developing new terms of trust that can account for this institutional change by blockchain technology and conducting empirical studies on this topic are therefore essential for further research on trust and distributed technologies. Based on our theoretical reflections above, we propose the following working definition of trust that might serve as a reference point for future studies on trust in the context of distributed technologies:

Trust is a complex social phenomenon with interrelated individual (psychological, attitudinal, informational), and systemic (economic, legal, technological, social) aspects. It is best understood as a relational attribute between (1) a social actor and other actor(s) (*interpersonal trust*) and / or (2) actors and institutions (*institutional* or *systemic trust*) and (3) institutions and (trusting) actors (*trust as shared expectations*), where institutional frameworks define the nature and strength of trust relationships between different actors. In essence, trust refers to expectations of the trustor made towards the trustee about the occurrence of future actions and / or events (under specific external / environmental conditions) which are often connected to a risk for the trustor. *Trust* denotes the reliance on the trustee despite this risk and can thus be understood as a way of managing contingencies of modern life. It involves both emotional and cognitive elements and is thus to be distinguished from (blind) faith and confidence (Lewis & Weigert, 1985). In the face of recent technological change, we claim that the technological environment has played an increasingly important role in setting the conditions of trust relationships, as evident in the case of blockchain. Future research is needed to not only address the technical aspects of these technologies, but also study their broader social and cultural contexts shaping their emergence and production.

References_

- Baldwin, J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications*, *4*, Article 1. https://doi.org/10.1057/s41599-018-0065-0
- Balkin, J. (2016). Information fiduciaries and the first amendment. *UC Davis Law Review*, *49*(4), 1183–1234. https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf

- Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain — The Gateway to Trust-free Cryptographic Transactions. *ECIS 2016 Proceedings Research Papers*. Twenty-Fourth European Conference on Information Systems, İstanbul. https://aisel.aisnet.org/ecis2016_rp/153/
- Bellini, E., Iraqi, Y., & Damiani, E. (2020). Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey. *IEEE Access*, *8*, 21127–21151. https://doi.org/10.1109/ACCESS.2020.2969820
- Berkeley, J. (2015). The trust machine — The technology behind Bitcoin could transform how the economy works. *The Economist*. https://www.economist.com/leaders/2015/10/31/the-trust-machine
- Blöbaum, B. (Ed.). (2016). *Trust and Communication in a Digitized World*. Springer International Publishing. https://doi.org/10.1007/978-3-319-28059-2
- Bodó, B. (2020). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*. https://doi.org/10.1177/1461444820939922
- Botsman, R. (2017). *Who can you trust? How technology brought us together and why it might drive us apart* (1st ed.). Public Affairs.
- Brekke, J. K. (2019). *Disassembling the Trust Machine — Three cuts on the political matter of blockchain*. Durham University.
- Campbell-Verduyn, M. (Ed.). (2018). *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (1st ed.). Routledge. https://doi.org/10.4324/9781315211909
- Clarke, K., Hardstone, G., Rouncefield, M., & Sommerville, I. (Eds.). (2006). *Trust in Technology: A Socio-Technical Perspective*. Springer Netherlands. https://doi.org/10.1007/1-4020-4258-2
- Corradi, F., & Höfner, P. (2018). The disenchantment of Bitcoin: Unveiling the myth of a digital currency. *International Review of Sociology*, *28*(1), 193–207. https://doi.org/10.1080/03906701.2018.1430067
- Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, *14*(4), 639–658. https://doi.org/10.1017/S1744137417000200
- De Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, *21*(12). https://doi.org/10.5210/fm.v21i12.7113
- De Filippi, P., & Loveluck, B. (2016). The invisible politics of Bitcoin: Governance crisis of a decentralised infrastructure. *Internet Policy*

Review, *5*(3). https://doi.org/10.14763/2016.3.427
- De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*. https://doi.org/10.1016/j.techsoc.2020.101284
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
- Dingle, S. (2018). *In Math We Trust: Bitcoin, Cryptocurrency and the Journey To Being Your Own Bank*. Tracey McDonald Publishers.
- Dodd, N. (2018). The Social Life of Bitcoin. *Theory, Culture & Society*, *35*(3), 35–56. https://doi.org/10.1177/0263276417746464
- DuPont, Q. (2018). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In M. Campbell-Verduyn (Ed.), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (pp. 157–177). Routledge. https://doi.org/10.4324/9781315211909-8
- Elkin-Koren, N., & Perel, M. (2019). Algorithmic Governance by Online Intermediaries. In E. Brousseau, J.-M. Glachant, & J. Sgard (Eds.), *The Oxford Handbook of Institutions of International Economic Governance and Market Regulation*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190900571.013.9
- Finck, M. (2019). *Blockchain regulation and governance in europe*. Cambridge University Press. https://doi.org/10.1017/9781108609708
- Flood, J., & Robb, L. (2017). *Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings* (Research Paper No. 17–23). Griffith University Law School. https://doi.org/10.2139/ssrn.3074263
- Foorman, J. L. (1997). Trust and Contracts: Are They Mutually Exclusive? *Business & Professional Ethics Journal*, *16*(1/2/3), 195–203. https://doi.org/10.5840/bpej1997161/2/32
- Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. Free Press.
- Gambetta, D. (1988). Can we trust trust. In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 213–237). Basil Blackwell.
- Giddens, A. (1990). *The consequences of modernity*. Polity Press.
- Hall, M. A. (2002). Law, Medicine, and Trust. *Stanford Law Review*, *55*(2), 463–527. https://doi.org/10.2307/1229596
- Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.
- Harz, D., & Boman, M. (2019). The Scalability of Trustless Trust. In A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, &

M. Sala (Eds.), *Financial Cryptography and Data Security* (pp. 279–293). Springer. https://doi.org/10.1007/978-3-662-58820-8_19
- Hoffmann, R. (2015, May 15). Why the blockchain matters. *WIRED*. https://www.wired.co.uk/article/bitcoin-reid-hoffman
- Jacobs, M. (2020). How Implicit Assumptions on the Nature of Trust Shape the Understanding of the Blockchain Technology. *Philosophy & Technology*. https://doi.org/10.1007/s13347-020-00410-x
- Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1424
- Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, *63*(4), 967. https://doi.org/10.2307/2578601
- Luhmann, N. (2017). *Trust and power*. Polity.
- Lustig, C., & Nardi, B. (2015). Algorithmic Authority: The Case of Bitcoin. *2015 48th Hawaii International Conference on System Sciences*, 743–752. https://doi.org/10.1109/HICSS.2015.95
- Mattila, J., & Seppälä, T. (2018). Distributed Governance in Multi-sided Platforms: A Conceptual Framework from Case: Bitcoin. In A. Smedlund, A. Lindblom, & L. Mitronen (Eds.), *Collaborative Value Co-creation in the Platform Economy* (pp. 183–205). Springer. https://doi.org/10.1007/978-981-10-8956-5_10
- Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": The practical materiality of Bitcoin. *Social Semiotics*, *23*(2), 261–277. https://doi.org/10.1080/10350330.2013.777594
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.2307/258792
- McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, *2*(2). https://doi.org/10.1145/1985347.1985353
- Meijer, D., & Ubacht, J. (2018). The governance of blockchain systems from an institutional perspective, a matter of trust or control? *Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age*, *18*, 1–9. https://doi.org/10.1145/3209281.3209321
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf
- O'Hara, K. (2017). Smart Contracts — Dumb Idea. *IEEE Internet*

Computing, *21*(2), 97–101. https://doi.org/10.1109/mic.2017.48
- Putnam, R. D. (2001). *Bowling alone: The collapse and revival of American community*. Simon and Schuster.
- Schneier, B. (2012). *Liars and outliers: Enabling the trust that society needs to thrive*. Wiley.
- Shahaab, A., Maude, R., Hewage, C., & Khan, I. (2020). Blockchain: A Panacea for Trust Challenges in Public Services? A Socio-technical Perspective. *The Journal of the British Blockchain Association*, *3*(2), 6. https://doi.org/10.31585/jbba-3-2-(6)-2020
- Shapiro, S. P. (1987). The Social Control of Impersonal Trust. *American Journal of Sociology*, *93*(3), 623–658. https://doi.org/10.1086/228791
- Swartz, L. (2016). Blockchain dreams: Imagining techno-economic alternatives after Bitcoin. In M. Castells (Ed.), *Another economy is possible* (pp. 82–105). Cambridge Polity Press.
- Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge University Press.
- Vidan, G., & Lehdonvirta, V. (2019). Mine the gap: Bitcoin and the maintenance of trustlessness. *New Media & Society*, *21*(1), 42–59. https://doi.org/10.1177/1461444818786220
- Walch, A. (2019). In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains. In P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich (Eds.), *Regulating Blockchain: Techno-Social and Legal Challenges* (pp. 58–82). Oxford University Press. https://doi.org/10.1093/oso/9780198842187.003.0004
- Werbach, K. (2018a). *Summary: Blockchain, The Rise of Trustless Trust?* (No. 3; Wharton PPI B-School for Public Policy Seminar Summaries). University of Pennsylvania.
- Werbach, K. (2018b). *The Blockchain and the New Architecture of Trust*. MIT Press.
- Woodall, A., & Ringel, S. (2019). Blockchain archival discourse: Trust and the imaginaries of digital preservation. *New Media & Society*, *22*(12). https://doi.org/10.1177/1461444819888756
- Yeung, K. (2019). Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law. *The Modern Law Review*, *82*(2), 207–239. https://doi.org/10.1111/1468-2230.12399
- Zucker, L. G. (1985). Production of Trust: Institutional Sources of Economic Structure, 1840 to 1920. In L. L. Cummings & B. Staw (Eds.), *Research in Organizational Behavior*. JAI Press.
-

Endnotes_

1. Which components of a blockchain system require trust is largely dependent on its technological architecture. Major differences lie between public / permissionless and private / permissioned blockchain-systems, whereby the latter are usually not considered "trustless", as they afford one or more organisations in a maintaining role that need to be trusted (De Filippi et al., 2020, p. 2).
2. The importance of human actors for the perceived trustworthiness of a system has e.g. been recognised by academic works dealing with the interrelationship of trust and governance (e.g. De Filippi and Loveluck 2016).

WEB MONETISATION_

Catalina Goanta, Utrecht University, Netherlands.
Alfa Yohanis, Department of Computer Science, University of York, United Kingdom.
Vikas Jaiman, Maastricht University, Netherlands.
Visara Urovi, Institute of Data Science, Maastricht University, Netherlands.

Web monetisation is the conversion of user traffic into revenue. Initially referring to websites, in more recent years, the meaning of the term has been expanded to refer to non-website traffic, such as social media applications, which this glossary entry gives more attention to. Within social media, the concept of content monetisation has developed as a way to denote the various approaches content creators have in creating online revenue out of the content they produce. This glossary entry provides an overview of the concepts of web and content monetisation, discusses aspects arising out of their interaction, and addresses three main issues currently associated with the term: the interoperability of social media infrastructures, the interoperability of content and web monetisation, and the moderation of content monetised decentrally.

Origin and evolution of the term_

Since its early days, the internet completely changed the way in which people interacted with information. As personal computing became more pervasive in society across the past decades, so did the online presence of households, which has been steadily on the rise. This was facilitated, among others, by factors such as Tim Berners-Lee contributions of hypertext database architectures (Tim Berners-Lee, 1990), and the development of the internet protocol suite (TCP/IP) reflecting data communication protocols used on the internet (Leiner et al. 1997; Cerf & Kahn, 1974). This is now known as the 'web'.

Globally, the increasing number of people browsing the internet (Statista, 2019) would initially visit websites with static information which had no native payment infrastructures and also no default commercial purpose. By 1994, there were around 3,000 websites on the internet (Statista,

2021). Also called the 'old Web', or Web 1.0 (approximately 1990-2004), this initial period of Internet presence was defined by an inherent asymmetry between content creators and content consumers, with the latter category reflecting the vast majority of Internet users (Cormode & Krishnamurthy, 2008). As companies started building their own online presence, incentives for the commodification of Internet traffic added a commercial layer to the Internet. Companies like eBay triggered the rise of e-commerce by offering new affordances such as information retrieval via search and filters, as well as easy to manage transaction workflows (Fingar et al., 1999). By using such a platform, any entrepreneur could, as a peer, make money on the Internet by selling things. However, not the same could be said for content. With the advent of free information available around the clock via an Internet connection (John, 1996), paying for content with attention became the norm (ZDNet, 2002; Aigrain, 1997). This led to the development of a complex advertising industry and business models which in essence were fighting for pixels and clicks on and from Internet websites (Bambury, 1998; McLeod, 2013). Yet (digital) advertising — especially the intrusive type, featuring pop-ups and mid-stream video interruptions — has never been popular with consumers, and the preference of not having to deal with advertising when consuming content online led to the creation of subscription-based (paywalled) business models (Bambury, 1998; Fishburn et al., 1997) or the use of ad-blockers (Mendelez, 2019).

Web 2.0, a term coined around 2004 to reflect the rise of social media and the interactive Web, brought with it a 'portalization' of Internet content, namely locking users into websites by trying 'to build every possible feature into the site' (Cormode & Krishnamurthy, 2008). Another metaphor used to describe this iteration of the Internet is 'Web as a platform', meaning that software would be built on the Internet instead of as desktop applications (Cabage & Zhang, 2013). In turn, this development attracted the collection and sharing of personal data at unprecedented scales (Goanta & Mulders, 2019). The consolidation of advertising by big tech companies, as well as the secondary markets operating around data brokerage have centralised platform power, in spite of the fact that the Internet as such has never been bigger. In 2021, the Internet consists of a whooping 1.88 billion websites (Statista, 2021). On the one hand, this brings with it certain benefits. In an ever-growing informational landscape, the automation and optimisation of information retrieval

services (e.g. price, offer or availability comparisons) can help consumers with informed choice. On the other hand, if user profiling skews choice based on commercial interests, that can lead to new types of online harms affecting informed consent (Staben, 2012), as well data governance as a whole (Viljoen, 2021). The resulting power centralisation by private actors has led to the so-called 'privatization of Internet governance' (Musiani, 2013), a narrative often used to call into question the legitimacy of advertising-based Internet business models (Wagner, 2019).

Legitimacy issues arising out of governance structure, and user harms characteristic to Web 2.0 have motivated calls for yet a new iteration of the Internet (Web 3.0): the decentralised Internet – verifiable, trustless and self-governing (Dabit, 2021; Harbinja & Karagiannopoulos, 2019). In some ways, the projection of such a new Internet era is considered to be a return to the decentralised architecture initially proposed by Tim Berners-Lee himself (Silver and Forbes Technology Council, 2020): 'No permission is needed from a central authority to post anything on the web, there is no central controlling node, and so no single point of failure … and no "kill switch"! This also implies freedom from indiscriminate censorship and surveillance' (World Wide Web Foundation, 2021). Among the normative narratives relating to the goal of achieving decentralised web governance that embraces new models of monetisation, native payment solutions reflect an important necessary infrastructure. This is what has driven initiatives such as the Web Monetization Protocol (W3C, 2021), proposing an architecture for micropayments which can empower content creators to earn revenue independently from the business models offered by big tech companies. Web Monetization is an API that allows websites to request micropayments from users through their browsers, and that focuses on continuous, rather than discrete payments. An earlier example is the Brave browser, which is supposed to offer users more control over the way in which they deal with their own data on the Internet (Brave, 2021), in a similar vein to Tim Berners-Lee's renewed support for data sovereignty (Verdegem, 2021; Verborgh, 2019).

Issues currently associated with the term_

As an umbrella term, web monetisation includes a very wide variety of business models, including advertising, subscription and crowdfunding-based models supported or facilitated through Internet websites. Web

monetisation is also used generally used in a broader sense than content monetisation: while the first refers to the process of creating revenue out of content available on the web (e.g. blog posts monetised via advertising), the latter is often used in the context of social media monetisation and linked to revenue earned by content creators.

Monetisation business models have become increasingly complex during the past decades. Particularly in the context of content monetisation, the amount of attention Internet users spend on social media has been heavily on the rise, particularly during the recent pandemic (Auxier and Anderson, 2021). In itself, this has led to more granular approaches to monetisation through advertising. A telling example in this respect is the ubiquitous phenomenon of influencer marketing (Goanta & Ranchordas, 2020). Yet all notable social media platforms are developing monetisation policies to create new opportunities for content creators to monetise user traffic on these platforms (e.g. partner programmes where creators receive money from social media companies; Tiktok, 2021).

Monetisation options are becoming increasingly diverse, and also increasingly intertwined. For instance, creators can receive money from platforms (ad revenue), or from sponsors (influencer/affiliate marketing); they can sell their own goods and services through new 'platformised' business models such as drop-shipping, or platform affordances brought about by trends such as social commerce (e.g. Instagram Checkout); they can ask for subscriptions or donations from their audiences, etc. All these monetisation models entail cross-platform activities reflecting that oftentimes, the volatility of monetisation makes it necessary for more sources of revenue to be combined at the same time. Current trends raise three main issues relating to the future of web and content monetisation.

Firstly, given that commercial activity is cross-platform, as well as across applications and websites, there is a question of interoperability: are content creators supported or deterred from relying on more or less sources of monetisation across the Internet? Platforms such as Youtube and TikTok have their own internal tokenisation/donation/ad affordances, often linked to the activities performed on a given platform by a content creator. It therefore seems unlikely that commercial incentives will be developed by these platforms in the following years to facilitate activities (e.g. payment) which take place on other platforms. The flexibility of business cases (or

current general lack thereof) is directly linked to the technical challenges that arise in this space. For instance, current implementations of the Web Monetisation payment are limited, as they depend on the use of specific services such as those offered by the Brave browser, Coil, and Interledger. However, given the tremendously fast pace of developments in this field, and the nature of the competition between platforms, it remains to be seen how this ecosystem will evolve, and how scalability will look like in the next decade.

Secondly, big platforms protect their commercial activities through terms of service, which have been in the past used to deny access to users who were engaging with their affordances externally (e.g. by using browser extensions; Kayser-Bril, 2021). Without clear interoperability incentives, platform terms can create legal shields against potential bridges which can be made between web monetisation and content monetisation currently native to social media.

Lastly, while decentralised solutions such as web monetisation promise the return to a free internet, a fundamental problem of content moderation emerges. If illegal content becomes decentralised (and easier to monetise), the digital monitoring efforts required from public authorities tasked with the enforcement of the law on digital markets would become disproportionately large. Recent regulatory reforms such as the Digital Services Act package (European Commission, 2020) show a tendency of regional regulators to attempt to hone in centralisation in order to achieve the enforcement of state-made content regulation. In the absence of infrastructures to facilitate content moderation (whether public or private), a return to the earlier focus on the Internet's libertarian freedoms is currently incompatible with the complex web of global, regional and national legal standards which online content needs to fulfill.

Conclusion_

In general, web monetisation is the conversion of user traffic into revenue. Initially referring to websites, in more recent years, the meaning of the term has been expanded to refer to non-website traffic, such as social media applications, which this glossary entry gives more attention to. Particularly for social media, the concept of content monetisation has developed as a way to denote the various approaches content creators

have in creating online revenue out of the content they produce. In a more narrow understanding, Web Monetization is a proposed W3C standard for generating website content revenue through micropayments. Three main issues were discussed, most specifically from the perspective of the infrastructures web and content monetisation need to function. Firstly, there is a problem with interoperability within content monetisation, as more and more creators operate across platforms with specific governance and technical infrastructures. Secondly, there is also an interoperability problem between content and web monetisation showing how difficult it may be to link revenue and business models not only from one social media platform to another, but also from social media platforms to other providers of content publication services (e.g. Wordpress). Thirdly, focusing on web monetisation in Web 3.0, a general issue of content moderation emerges, in the absence of centralised entities which can provide filters for illegal or otherwise potentially harmful content.

References_

- Aigrain, P. (1997). Attention, media, value and economics. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.549
- Auxier, B., & Anderson, M. (2021). *Social Media Use in 2021* [Report]. Pew Research. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/
- Bambury, P. (1998). A taxonomy of internet commerce. *First Monday*, *3*(10). https://doi.org/10.5210/fm.v3i10.624
- Berners-Lee, T. (1990). *Information management: A proposal*. CERN. https://www.w3.org/History/1989/proposal.html
- Brave. (2021). *Brave browser*. Brave. https://brave.com.
- Cabage, N., & Zhang, S. (2013). Web 3.0 has begun. *ACM Interactions*, *5*, 26.
- Cerf, V. G., & Kahn, R. E. (1974). A protocol for packet network interconnection. *IEEE Transactions on Communication Technology*, *22*(5), 627–641. https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf.
- Cormode, G., & Krishnamurthy, B. (2008). Key differences between Web 1.0 and Web 2.0. *First Monday*. https://doi.org/10.5210/fm.v13i6.2125
- Dabit, N. (2021). *What is Web3? The Decentralised Internet of the Future Explained*. FreeCodeCamp. https://www.freecodecamp.org/news/

what-is-web3/.
- European Commission. (2020). *The Digital Services Act Package*. European Commission. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
- Fingar, P., Kumar, H., & Sharma, T. (1999). 21st century markets: From places to spaces. *First Monday*, *4*(12). https://doi.org/10.5210/fm.v4i12.707
- Fishburn, P. C., Odlyzko, A. M., & Siders, R. C. (1997). Fixed fee versus unit pricing for information goods; competition, equilibria, and price wars. *First Monday*. https://doi.org/10.5210/fm.v2i7.535
- Goanta, C., & Mulders, S. (2019). Move fast and break things': Unfair commercial practices and consent on Social Media. *Journal of European Consumer and Market Law*, *8*(4), 136–146.
- Goanta, C., & Ranchordas, S. (2020). *The Regulation of Social Media Influencers*. Edward Elgar.
- Harbinja, E., & Karagiannopoulos, V. (2019). Web 3.0: The decentralised web promises to make the internet free again. *The Conversation*. https://theconversation.com/web-3-0-the-decentralised-web-promises-to-make-the-internet-free-again-113139
- John, N. R. (1996). Putting content onto the Internet. *First Monday*. https://doi.org/10.5210/fm.v1i2.477
- Kayser-Bril, N. (2021). *AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook'*. Algorithm Watch. https://algorithmwatch.org/en/instagram-research-shut-down-by-facebook/.
- Leiner, B. M., Cerf, V. G., Clark, D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2017). *Brief History of the Internet 1997* [Report]. Internet Society. https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf
- McLeod, A. M. (2013). *Magazines monetizing their digital presence: Three strategies, some success* [Simon Fraser University]. https://summit.sfu.ca/item/12608.
- Mendelez, K. (2019). The state of web monetization. *State of Web Monetization*. https://write.as/kenmelendez/the-state-of-web-monetization
- Musiani, F. (2013). Dangerous liaisons? Governments, companies and Internet governance. *Internet Policy Review*, *2*(1). https://doi.org/10.14763/2013.1.108
- Pfeiffer, A. (2002). *Why won't you pay for Net content?'*. ZDNet. https://

www.zdnet.com/article/why-wont-you-pay-for-net-content/
- Silver, C. & Forbes Technology Council. (2020). *What Is Web 3.0?* Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/06/what-is-web-3-0/?sh=13cb040258df
- Staben, J. (2012). Consent under pressure and the Right to Informational Self-Determination. *Internet Policy Review*, *1*(4). https://doi.org/10.14763/2012.4.265
- Statista. (2019). *Share of households with a computer at home worldwide from 2005 to 2019'*. Statista. https://www.statista.com/statistics/748551/worldwide-households-with-computer/.
- Statista. (2021). *How many websites are there?* Statista. https://www.statista.com/chart/19058/number-of-websites-online/
- TikTok. (2021). *Business and creator monetization*. TikTok. https://support.tiktok.com/en/business-and-creator.
- Verborgh, R. (2019). Re-decentralizing the Web, for good this time'. *Ruben Verborgh*. https://ruben.verborgh.org/articles/redecentralizing-the-web/.
- Verdegem, P. (2021, February 5). Tim Berners-Lee's plan to save the internet: Give us back control of our data'. *The Conversation*. https://theconversation.com/tim-berners-lees-plan-to-save-the-internet-give-us-back-control-of-our-data-154130
- Viljoen, S. (2021). A Relational Theory of Data Governance. November 2021. *The Yale Law Journal*, *131*(2). https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance
- Wagner, K. (2019). *Mark Zuckerberg explains why an ad-free Facebook isn't as simple as it sounds*. Vox. https://www.vox.com/2019/2/20/18233640/mark-zuckerberg-explains-ad-free-facebook.
- World Wide Web Foundation. (2021). *History of the Web*. World Wide Web Foundation. https://webfoundation.org/about/vision/history-of-the-web/.

ACKNOWLEDGEMENTS_

This book is the result of a collective effort. It all started during a workshop on decentralized technologies held at the Institute for Information Law, at the University of Amsterdam, in 2018. Since then, this editorial project has been, above all, a prolonged occasion for the coming together of passionate and curious minds, willing to create something collaboratively. The excellent editors Florian Idelberger, Andrea Leiter, Morshed Mannan and María-Cruz Valiente, have lent their time, patience, valuable expertise and brain energies to read, review and edit the texts included in this collection. Balázs Bodó, Primavera De Filippi, Aron Fischer, Samer Hassan, Björn Scheuermann and Monica Palmirani – the editorial board - supported the idea of this Glossary from its inception; the shared interest of these academics in developing this project allowed its materialization, and still encourages its continuation. Nothing would have been possible without the invaluable support of Frédéric Dubois, always mediating and motivating everybody else around the project. Thanks, also, to the entire staff of the Internet Policy Review, the Blockchain and Society Policy and Research Lab, and the Institute of Network Cultures for supporting the project at its various steps. Finally, best wishes to Julian Morgan, who must be thanked for taking over the task of keeping the Glossary alive, leading the editorial team throughout future entries submissions.

Valeria Ferrari
Amsterdam
May 2023

AUTHORS_

Valeria Ferrari, Kelsie Nabben, Ellie Rennie, Aron Fischer, María-Cruz Valiente, Florian Tschorsch, Ingolf G. A. Pernice, Brett Scott, Jaya Klara Brekke, Wassim Zuhair Alsindi, André Ramiro, Ruy de Queiroz, Heleen Janssen, Jatinder Singh, Balázs Bodó, Roel Roscam Abbing, Cade Diehm, Shahed Warreth, Samer Hassan, Primavera De Filippi, Isabelle A. Zaugg, Anushah Hossain, Brendan Molloy, Daniel Villar-Onrubia, Victoria I. Marín, Laura Lotti, Florian Idelberger, Péter Mezei, Selwa Sweidan, Karlynne Ejercito, Tyng-Ruey Chuang, Rebecca C. Fan, Ming-Syuan Ho, Kalpana Tyagi, Kelsie Nabben, Michael Zargham, Gerd Beuster, Oliver Leistert, Theo Röhle, Ori Shimony, Ámbar Tenorio-Fornés, Alexandra Giannopoulou, Fennie Wang, Chris Wray, Giovanni Sileno, Francisco Javier Moreno Gálvez, Francisco Sierra Caballero, Indrek Ibrus, Ulrike Rohn, Nanna Bonde Thylstrup, Matthew Archer, Louis Ravn, Moritz Becker, Catalina Goanta, Alfa Yohanis, Vikas Jaiman, Visara Urovi_

institute of network cultures

INTERNET POLICY REVIEW

Blockchain & Society Policy Research Lab