Decentralisation in the blockchain space

Bodó, B.; Brekke, J.K.; Hoepman, J.-H.

DOI
10.14763/2021.2.1560

Publication date
2021

Document Version
Final published version

Published in
Internet Policy Review

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Decentralisation in the blockchain space

Balázs Bodó *University of Amsterdam* bodo@uva.nl
Jaya Klara Brekke *Durham University* j.k.brekke@durham.ac.uk
Jaap-Henk Hoepman *Radboud University* jhh@cs.ru.nl

DOI: https://doi.org/10.14763/2021.2.1560

Published: 19 May 2021
Received: 25 November 2020 **Accepted:** 10 May 2021

Funding: Dr. Bodó received funding from the European Research Council under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Bodó, B. & Brekke, J. K. & Hoepman, J.-H. (2021). Decentralisation in the blockchain space. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1560

Keywords: Blockchain, Decentralisation

A draft of this article underwent open peer-review as an **Open Abstract**

Abstract: 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.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

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).

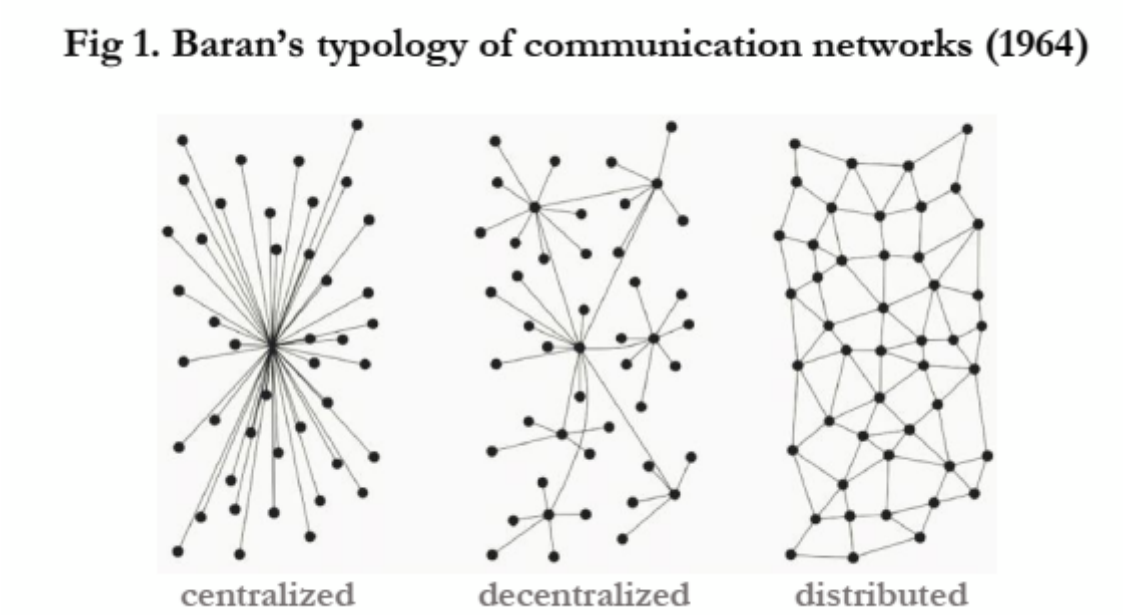

FIGURE 1: Various network topologies (Baran, 1964).

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).

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.

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

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

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].

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. A DDoS 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

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

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.

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 au-

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

thoritarian, 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.

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with

centre
– internet
et société