INTERNET POLICY REVIEW
Journal on internet regulation

Volume 11 **Issue** 1

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Protocol

Gerd Beuster *University of Applied Sciences Wedel*
Oliver Leistert *Leuphana Universität Lüneburg*
Theo Röhle *University of Gothenburg*

DOI: https://doi.org/10.14763/2022.1.1651

Published: 31 March 2022
Received: 17 September 2021 **Accepted:** 6 March 2022

Funding: Oliver Leistert received funding from Deutsche Forschungsgemeinschaft (DFG) under grant agreement 440949657.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Beuster, G. & Leistert, O. & Röhle, T. (2022). Protocol. *Internet Policy Review*, *11*(1). https://doi.org/10.14763/2022.1.1651

Keywords: Protocols, Internet protocol (IP), Blockchain

Abstract: 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. 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.

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

Definition

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

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with

CREATe

UOC
R&I
IN3
Internet
interdisciplinary
Institute
Universitat Oberta de Catalunya

cnrs
centre
internet
et societe

UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies