NeXt generation Techno-social Legal Encryption Access and Privacy nextleap.eu
Grant No. 688722 Project Started 2016-01-01. Duration 36 months

DELIVERABLE D3.6
Principles of Decentralized Internet Governance

Francesca Musiani (CNRS), Harry Halpin (INRIA), Ksenia Ermoshina (CNRS), Holger Krekel (Merlinux)

Beneficiaries:	CNRS, INRIA
Internal Reviewers:	
Workpackage:	**WP3, D3.6 Principles of Decentralized Internet Governance**
Description:	The principles of internet governance will be explored using the standpoint of science and technology studies, with a focus on how to improve citizen participation and decentralization, as well as “fundamental rights” inspired by Berners-Lee's concept of a “magna carta” for the Web.
Version:	**1.0**
Nature:	**Report (R)**
Dissemination level:	**Public (P)**
Pages:	
Date:	2018-12-31

Project co-funded by the European Commission within the Horizon 2020 Programme

Table of Contents

1. Introduction

This deliverable is the final output of the three-year investigation, with methods coming from the social sciences and, in particular, science and technology studies, of encrypted secure messaging applications and protocols, their developers and users. As a conclusion to this research, it broadens its scope by examining issues of governance, in particular as they relate to dynamics of decentralization, both of the technical architecture and of the “upper layers” of uses/practices and community-building.

The purpose of this deliverable is threefold:

(i) to discuss how principles of internet governance can be explored using the standpoint of science and technology studies,

(ii) to address how this standpoint can be used to explore decentralized technical architectures and their consequences for citizens, their fundamental rights, and civil liberties,

(iii) drawing from case studies examined in previous deliverables, but examining new material (interviews and documents) that particularly address the issue of governance, to provide examples of six models to address the governance of encryption technologies.

2. Internet governance from an STS standpoint

Internet governance (IG) has been shaped by the very real politics and controversies surrounding the “global coordination of Internet domain names and addresses” (van Eeten and Mueller, 2013, p. 724), which are an important, but not the sole factor affecting the internet. Substantively, this research path has focused primarily on institutions including the Internet Corporation for Assigned Names and Numbers (ICANN), on largely UN-dominated processes such as the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF), and on the idea of multistakeholderism as a model for internet-related policy decision-making. Conceptually, the field has been dominated by legal scholarship, and by research based in international relations and institutional economics theory, most of which is focused on the role of the nation state in the management of critical internet resources (also see DeNardis, 2010, 2013).

The mainstream view of IG research is being increasingly challenged for its narrow focus on formal institutions, the role of the state, and for missing the mark on what constitutes governance in a networked environment[1]. Van Eeten and Mueller, for example, suggest that the scope of IG research is much wider than what is being labeled as such. They argue that

1This section draws from joint work with Dmitry Epstein and Christian Katzenbach (2016).

researchers working in areas of telecommunication policy, information security, and cyberlaw all do IG research, even though they are avoiding the label. Conceptually, they suggest rethinking Internet governance label to include “the diversity of governance on the internet” including “environments with low formalization, heterogeneous organizational forms, large number of actors and massively distributed authority and decision-making power” (2013, p. 730). Substantively, they call to study the economics and practices of organisations that are engaged in managing information flows on the internet. We would note that these organizations include technical standards bodies such as the IETF and W3C, as well as open source projects and protocols that do not belong to any organizational body.

In a similar vein, DeNardis (2010, 2013) has criticised mainstream IG research for largely overlooking private arrangements of power when it comes to routing, interoperability, standardization or content filtering online. Raymond and DeNardis have argued for a broader umbrella for IG studies – one that would expose those private arrangements of power in IG. Conceptually, their framework spans six functional areas ranging from “control of critical internet resources” to “architecture-based intellectual property rights enforcement” (2015, pp. 589-594) – all of which focus on the praxis of IG as opposed to discourse about IG, which they view as a weakness of mainstream IG research. Substantively, they identify a series of institutions that host decision-making activities (e.g., policy, standards) as points of control for online information flows. These standards bodies and open project, which are historically transnational, may not consider themselves governance bodies even if their influence *de facto* governs the material protocols that create the Internet.

The traditional focus on Internet governance institutions largely overlooks the mundane practices that make those institutions tick, thus leaving important blind spots in both conceptual and substantive understanding of the practices and power arrangements of IG. The focus on institutions and formal policy instruments makes it harder to empirically analyse the diverse forms of internet-related decision-making and coordination activities that take place outside of formal and well defined boundaries (Musiani, 2015; van Eeten & Mueller, 2013). Treating institutions as given may overlook institutional change and does not account for functional and structural biases embedded in existing institutional arrangements (Hofmann, Katzenbach, & Gollatz, 2016; Ziewitz & Pentzold, 2014). Moreover -- and most importantly given the focus of this deliverable -- the institutional focus obscures the agency of technology designers, policy-makers, and users as those interact, in a distributed fashion, with technologies, rules, and regulations, leading to unintended consequences with systemic effects (Epstein, 2015; Musiani, 2015).

Even though researchers such as van Eeten & Mueller (2013) mention the importance of human agency, IG researchers shy away from empirically analysing or incorporating human agency in conceptualisation of internet governance. This critique gains additional weight when one adopts a broad definition of IG such as “decision making with constitutive (structural) effect whether it takes place within the public or private sectors, and formally or informally” (Braman, 2009, p. 3), or even just recognises that governance “may be just a side

effect of actions with non-governance-related aims" (Hofmann et al., 2016, p. 4).

Tackling the macro questions of politics and power related to IG requires unpacking the micro practices of governance as mechanisms of distributed, semi-formal or reflexive coordination, private ordering, and use of internet resources. Similarly to a scientific lab where "scientific order is constructed out of chaos" (Latour & Woolgar, 1986, p. 33), seemingly stable arrangements of IG arise from the chaos of taken-for-granted, mundane, and often apparently unrelated activities of protocol design, evolution, and use. It is this focus on practices and routines, discourses and design that makes us talk about the doing of internet governance: as an "accomplishment embedded in everyday interaction" (West & Zimmerman, 1987, p. 125). An STS lens can help addressing some of the blind spots left by institutional and state-centric takes on IG, including functional and structural biases, and it can foreground the agency of human actors.

In contrast to classical social theory, which is at the basis of international relations and institutional economics approaches, an STS perspective on Internet governance does not assume the existence of a given social order, that needs to be analytically re-constructed (Wagner, 1994, p. 274-276; Latour, 2005, p. 5-8) – or politically changed by means of regulation. Instead, STS scholars consider the social an "effect generated by heterogeneous means" (Law, 1992, p. 382), thus making continuous processes of ordering – of economic, political, discursive, technical or other nature – the main focus of scientific inquiry. In this context, governance is broadly understood as social ordering, which does not happen exclusively in politically designed institutions, but is also enacted through mundane practices of people engaged in maintaining or challenging the social order (Woolgar & Neyland, 2013).

Conceptually, STS-informed IG research relies on understanding IG as a normative 'system of systems' and it acknowledges the agency, often discrete and pervasive, of both human and non-human actors and infrastructures. Empirically, STS-informed IG research focuses on the dynamics of 'ordering' of assemblages and hybrid arrangements of IG; on the structural and performative effects of controversies and de-stabilisations on norm- and decision-making, or on the construction of authority and trust; and finally, on hybrid forums, private arrangements, users and their practices. Let us say a little bit more about each of those key aspects.

2.1. Key aspects of Internet governance viewed through the lens of STS

IG as a normative 'system of systems'. Technical and political governance are becoming more and more intertwined. The core issue for scholars of IG at the present stage is to acknowledge not only the plurality of these modes of governance, but the fact that they cannot be fully separated. STS approaches plead for an understanding of internet governance as coexistence

of different types of norms, elaborated in a variety of partially juxtaposed forums, enforced, implemented or merely "suggested" via a plurality of normative systems: law, technology, markets, discourses, and practices (Brousseau, Marzouki, & Méadel, 2012) .

Ordering vs regulation (and "back to the institutions"). Acknowledging the diverse origins of norms relevant for the use and design of the internet, most STS-informed IG researchers base their understanding of governance in ordering instead of regulation, management or control. As opposed to these concepts, ordering not only captures the normative effect of mundane practices and daily routines, it is also considered particularly well-suited to the analysis of the organisational forms of global politics as assemblages – hybrid configurations constantly reshaping their purposes and procedures in order to connect and mobilise objects, subjects and other elements, constituted and positioned relationally, around particular issues. In this light, institutions of IG can also be explored with an STS-informed toolbox, by capturing the complexity of global "political" governance arrangements as sets of embedded practices (Flyverbom, 2011).

Agency of non-human actors and infrastructures as loci of mediation. Information intermediaries, critical internet resources, internet exchange points (IXPs), surveillance and security devices play a crucial governance role alongside political, national and supra-national institutions and civil society organisations (Musiani, Cogburn, DeNardis, & Levinson, 2016). IG takes shape through a myriad of infrastructures, devices, data fluxes and technical architectures that are often discreet and invisible, yet nevertheless crucial in subtending building the increasingly public and articulate network of networks. Laura DeNardis (2014, p. 11) defines these entities as infrastructural "control points", around which are entangled matters of technical and economic efficiency, as well as negotiations over human and societal values such as intellectual property rights, privacy, security, transparency. Recent scholarly and policy discussions on "Governing Algorithms" connect with this aspect, and explore not only governance of algorithms, but also the governing power of algorithms themselves (Ziewitz, 2016; Musiani, 2013).

Mundane practices and agency of human actors. Contrary to the institutional approaches to IG, STS-informed scholarship acknowledges the role of invisible, mundane, and taken-for-granted practices in the constitution of design, regulation, and use of technology. It calls the attention to reflexive acts of individuals in articulating internet standards (Braman, 2011), the social aspects of crafting and enacting internet-related policy (Epstein, 2011; Kuerbis, 2010), as well as institutionalisation of non-traditional forms of participation in discourse about IG issues (i.e. multi-stakeholderism), and mechanisms for civic engagement (Epstein, 2013; Nonnecke, 2016). As such it pays the necessary attention to the social - and not just political - aspects of the socio-technical systems of the internet.

Controversies as structuring and performative processes. STS-informed approaches to IG analyse the structuring and performative effects of controversies on governance. Most

prominently, controversies around claims made by different actors or groups about doing IG contribute to the creation of different worlds in which specific notions of governance make sense. Thus, the study of controversies unpacks ‘governance’ as a theoretical and operational concept, by exposing the plurality of notions it refers to, and the consequences of their being in conflict (Cheniti, 2009; Ziewitz & Pentzold, 2014). The very processes by which norms are created, re-negotiated, put to the test, re-aligned, raise conflicts, are as crucial - and perhaps more crucial - in STS perspectives as the “stabilised” norms themselves. The authority of IG institutions should also be analysed as such if we are to avoid an understanding of it as a ‘fait accompli’ (Flyverbom, 2011).

Hybrid forums, privatisation, users… enriching and revisiting ‘multi-stakeholderism’. Several concepts brought in by the STS toolbox, as well as several fieldwork choices, can help unveiling a number of situated practices on, by and for the internet that arguably constitute a vital part of ‘doing internet governance’. In particular, they help enriching and revisiting the concept of multi-stakeholderism (Malcolm, 2008). For example, understanding IG through the lens of Michel Callon et al.’s ‘hybrid forums’ (2009) - entities meant to transform controversies into productive dialogue and bring about democracy - show the importance of actors’ positioning in subsequent decision-making. If the role of the private sector is more and more important in internet governance arrangements, as it is increasingly widely acknowledged, the technology-embedded nature of its intervention can be brought to the foreground by STS methods. Examining the relationship of internet users to content they put online or consume, to their devices and the values they embed, ‘does’ governance inasmuch as it reflects belonging and commitment to a set of norms and to a community in a broad sense, and reveals the interplay of issues of sovereignty, autonomy, and civil liberties (Elkin-Koren, 2012).

3. Decentralized architectures, rights, and liberties

STS approaches to Internet governance are (and have been in this project) of particular interest when it comes to examining the interplay of decentralized and distributed architectures and themes such as human rights, civil liberties, and their protection.

Indeed, beyond the simplified operational definition of decentralized architectures -- a type of network bearing several features: a network made of multiple computing units, seeking to achieve its objectives by sharing resources and tasks, able to tolerate the failure of individual nodes and thus not subjected to single points of failure, and able to scale flexibly -- the choice (see D2.1 for details), by developers and engineers of Internet-based services, to develop these architectures instead of more centralized models has several implications for the daily use of online services and for the rights of Internet users. Our deliverables 3.1, 3.3 and 3.5 have showed how this applies to the field of encrypted secure messaging. This section

attempts to draw some general conclusions on the aspect of decentralization as it relates to governance from an STS standpoint, i.e., addressing issues such as user practices and appropriation, or the reconfigurations of law and rights through choices of architectural design[2].

3.1. Distributed architectures, a repeated and “alternative” choice in Internet history

The choice of decentralized and distributed architectures has been made several times in the past, most of the times in an ‘alternative’ perspective, as an opposition to dominant actors in the ICT economy, or as a ‘counter-cultural’ move. This choice appears to be linked to a very ‘political’ issue: with the increasingly evident centralization of the Internet and the surveillance excesses it appears to foster, what are the place and the role of the (re-)decentralization of networks’ technical architectures? What is the place for user autonomy and empowerment at a time when infringements upon privacy and pervasive surveillance practices are often embedded in network architectures? Are distribution and decentralization of network architectures the ways, as Philippe Aigrain (2010) suggested, to “reclaim” Internet services — instruments of ‘technical governance’ able to reconnect with the original organization of cyberspace?

In the mid-2000s, one could think that the hour of glory of peer-to-peer software was arguably passed, as laws in several countries were targeting it as a technology in order to prevent its uses as a file-sharing infrastructure, and streaming was taking its place as the prime means of consuming content. Furthermore, the client-server logic was increasingly taking hold as the privileged strategy to foster the development of the Web, and to answer the needs of billions of Internet users. And yet, discreetly but creatively, myriad projects aiming at developing Internet services on more decentralized and distributed architectures than the Googles and Facebooks of our times were, in parallel, seeing the light.

These network architectures, all too often reduced to the partial vision one could have via the prism of “pirate practices”, were and are bearers of much more than the piracy vs. sharing opposition. They can be considered as a very interesting “laboratory” where visions and implementations of alternative Internets take place — experiments of “governance by architecture” imbued with different, innovative ways of distributing authority, power, value, sense of community. To our understanding, this is the vision we had of distributed architectures at the beginning of this project is still accurate, and as the NEXTLEAP project comes to an end, we can add a few further remarks to it.

First, the (re-)distribution and the (re-)decentralization of networks are strictly linked — much more so than a few years ago, and in particular after the Snowden revelations — to the discussions of surveillance and privacy issues, and find themselves frequently associated to discussions about encryption. Also thanks to the role that local and distributed technologies, relying on networks such as Tor, have played in rallying and organizing social movements and grassroots resistance tactics, distributed architectures are increasingly seen as

2This section draws from joint work with Cécile Méadel (2016) and Ksenia Ermoshina (forthcoming 2019).

technologies of empowerment and liberation. Yet, they do not escape the powerful double narrative that we have mentioned in 3.1 already, fuelled by previous ones depicting peer-to-peer as an allegedly 'empowering-yet-illegal' technology. If on one hand, the discourse on empowerment and better protection of fundamental civil liberties is very strong, several projects seeking to merge decentralization and encryption to improve protection against surveillance show in parallel a desire, more likely a need, to defend themselves from allegations such as the frequent use of obfuscation technologies by terrorist groups and individuals. This dialectic is taking place in the broader context of discussions about governance by infrastructure and civil liberties (Musiani *et al.*, 2016), some of them particularly related to encryption (or the breaking of it), such as the Apple vs. FBI case and WhatsApp proposing, since April 2016, encryption by default (Ermoshina *et al.*, 2016).

Second, we must cite the extraordinary success of the 'last' — in chronological terms — distributed architecture: blockchain technologies. The success of the blockchain is perhaps still greater in research projects and in anticipations of intermediary-less futures than in fully working applications, and we can recognize, as in previous "expectation cycles" related to distributed architectures and a number of other technologies, both the potential and the hype. Yet, the blockchain and its myriad variants have some specificities that it is, and it will be, very interesting to observe in the coming years; in particular, it seems to be the first decentralized networking technology to be widely accepted — "celebrated" would be more accurate — by national and supra-national institutions, even as its first widespread application, Bitcoin, was born with the explicitly stated goal of making each and every institution obsolete, and its birth, development, functioning are subject to several controversies.

3.2. Governance of/by decentralized and distributed architectures

The research undertaken in recent years, by the authors of this deliverable as well as a number of other colleagues, suggests three directions that an STS-driven reflection on the governance of decentralized/distributed architectures may follow.

We should take into account the "lessons learned" potential of decentralized and distributed architectures, when seen from a historical perspective. The initial Internet model called for a decentralized and symmetrical organization — in terms of bandwidth usage, but also of contacts, user relations, shared knowledge and machine-to-machine communication (Halpin & Monnin, 2016). In the 1990s, the commercial and social explosion of the Internet brings about important changes, exposing the shortcomings — for the network's usability and its very ability to function — of a model presupposing the active cooperation of all network members. The new preeminent model relies on asymmetrical fluxes and numerous barriers preventing the free circulation of data.

Today, in a world of Internet services where fluxes and data converge towards a few giants, experimentations with distributed architectures are seen as a "return to the origins". But is it really about the dominance of an organizational principle at different times in history — or is there a co-existence of different levels of resource centralization, hierarchy of powers, and

cooperation among Internet users over time? Are we indeed witnessing a “war of the worlds” of which the recent tensions around surveillance are the most recent illustration?

Historical approaches also show us the importance of History, with a capital H, for Internet regulation. Architectural choices have profoundly political implications (see DeNardis, 2014): if code is law, and law is code, both are crucially and inextricably transformed by the Internet’s pervasiveness in all aspects of economy, policy and sociability. This Internet includes both distributed, decentralized and centralized models, rather than opposing them. Going back to History allows us to wonder whether we must return to the mythical, original model of a free, open and equal Web, or learn how to articulate the different realities that are currently forming the Internet(-s?). Given the current negative – if not paranoid – views of the centralization of the Web in the hands of Silicon Valley put forward by various academic and populist critics, now more than ever we need to open empowering narratives that do justice to the political vision embedded in the protocols of the real, existing Internet while providing a horizon for future political change in the governance of the Internet.

3.2.1 Centralization and Decentralization

First, it is important to consider the what is at stake in decentralized infrastructures and architectures. Distributed Internet services have transformed and transform today the ways in which actors make sense of their communicative capacities and their responsibilities in information sharing, providing valuable new capabilities – such as file-sharing – to users that were otherwise before unimagined. User empowerment, prompted by several decentralized services — increasingly mobile, self-configurable and flexible — open innovative perspectives for infrastructures of communication, their functions and their mediation capacities among actors (Antoniadis, 2016), which in turn lead to these innovations becoming increasingly mainstream within industry, such as the move from purchasing entire albums of music to per-track purhasing and downloading even in centralized services such as iTunes being inspired by Bittorrent. The issue of user empowerment becomes particularly salient in times when users’ trust (political, economic, technical) in authorities is crucially damaged. Therefore, there is considerable desire by some users to invest in decentralized infrastructure and protocols, as made evident by the enthusiasm over blockchain technologies.

The ways in which distributed architectures reconfigure means and tools of authority and control redefines, at the same time, the very entities — people and organizations — concerned by them. An STS perspective allows to see how the opposition between individual and collective actors is questioned by these architectures. A redefinition and restructuring of communities happens with distributed architectures: what enables the shaping of collectives, what makes them “stick together”, what gathers them and defines the nature of their collective becomes more labile and less formal. Distributed architectures can also co-shape the relationship between specific people: as the example of smart contracts demonstrates (De Filippi and Hassan, 2016), the distribution (or decentralization) reaches the very core of the

architecture and of code, when it enables the personalization of a contract linking two participants and the nature of their relationship. The issue of user empowerment, real or expected, and the assessment of its limits, is at the core of the articulation between decentralization and social organization, between decentralization and governance.

However, there has been concerns in protocol development that are trending away from decentralization in order to satisfy the purported needs of users for ever-increasing features, higher availability, and lower latency. As noticed by Marlinspike, decentralization makes it increasingly difficult, if not impossible, to add new features, as every user's software must agree to adopt the new feature. If a user cannot be reasonably assured new features will be supported by other participants in a decentralized protocol, the new features cannot be relied on and should not exist. Marlinspike believes that this leads decentralized protocols such as XMPP to eventually stop evolving, and so be overcome by proprietary protocols with centralized governance. In terms of operational reliability to even have participants in a system communicate, decentralized systems by design may lead to lower availability as users that host operations for other users may drop in and out of the system. Yet these users will not blame the other users, but the system as a whole and so switch to centralized systems as, in contrast, centralized systems with cloud-backed infastructure can provide more stable availability under normal operating conditions, even if decentralized systems are more resistant to catastrophe. Users may be empowered by decentralized systems, but users also ultimately want reliable and available services.

There is also a spectrum of decentralization, not a simple opposition between centralization and decentralization. To return to D2.1, we have systems that are fully ***decentralized***, where the users themselves provision infrastructure as part of the protocol, such as in P2P systems like Bittorrent and Bitcoin. Each user would either run the same software codebase or a codebase that fit a standard on their own machines. In contrast, systems modelled on the original Internet, such as the e-mail standard SMTP and web-browsers using HTTP (as well as newer standards like XMPP), were designed as ***federated*** architectures where a central server would serve numerous users who could use the client software of their choice, but that software would operate in accordance with a common standard. While a user could always run their own server, such as their own custom of e-mail server or web server hosted "in their closet," most users are expected to simply chose a server they trust. The open standards allow multiple central servers that host different users to communicate, so that any user on one server can communicate to any other user on another server – thus creating a federation. On the other extreme, a ***centralized*** system allows users to only communicate to other users using the same server. This allows for easy deployment of new features and high availability via using the Cloud, but it comes at the cost that users have to fully trust the central server (for example, not to block or alter their communication) and can only communicate to other users on the same central sever. While the exact interplay between user empowerment and the degree of centralization is complex and situational, it is worthwhile investigating each step along the way from Google-based cloud services to full-blooded P2P decentralization.

3.2.3. Financial sustainability

Second, the issue of whether or not decentralization may provide a sustainable alternative for the Internet 'ecology' is still very contentious within the circles of protocol development. The technical features of distributed architectures (direct connections, resistance to failure) and their ability to support the emergence of organizational, social and legal principles (privacy, security, recognition of rights) offer new paths of exploration and preservation of the Internet's balance. At the same time, the road towards decentralization is far from linear, and distributed organizations do not take shape according to a single plan. The users behind nodes of distributed architectures can assemble in collectives that are very varied in nature, complexity and underlying motivations. This variety may be dependent upon modes of aggregation, visibility devices, types of communication tools and envisaged business models (as well as the difficulty of identifying sustainable ones). The different models enabling the shaping of "collectives" are especially varied (Chrysos, 2016). Nonetheless, these collectives and their decentralized infrastructure often are expected to have difficulties financing both the continuing development of their protocol as well as the participation of users in their decentralized system.

The heterogeneity of distributed architectures raises issues that are especially important when it comes to the interplay of law and economy in these ecosystems. Network access providers historically have raised economic objections to decentralized models, having programmed and organized their own networking infrastructure with the idea that the most part of users' online activities were going to consist in downloading data and information from clusters of servers – and so leading to download latency being lower than upload latency for their own users, providing a technical barrier for user participation in decentralized systems. Likewise, there are concerns over users new capabilities rendering existing laws difficult to enforce, such as the spread of copyright media via P2P file-sharing networks or the breaking of economic sanctions via privacy-preserving Bitcoin variants. Finally, developers-turned-entrepreneurs themselves often need to revisit the choice of decentralization, because of unexpected user practices, the impossibility of making distributed technology "easy" for the public to users, or the seductive simplicity of centralized infrastructures and economic models (see Musiani, 2018).

Therefore, we can categorize protocol architectures and systems in different ways according to their plans for financial sustainability. On one hand, there are systems that are purely ***non-profit***, either because the developers themselves, those that run operations, or the users themselves are not expected to have a financial incentive for running the service. One example of this is the Tor project. The developers of the Tor protocol themselves are paid via a centralized non-profit foundation that receives grants from primarily government agencies, with Tor itself being co-founded by Paul Syverson from the Office of Naval Research;this being perhaps an ironic situation for the most popular anonymous overlay network meant to defeat mass surveillance that served as the foundation for both Wikileaks, but even CIA agents are meant to use Tor to gain higher anonymity while operating overseas. Those

running the (mostly) decentralized operations such as Tor relays and entry/exit nodes themselves are not rewarded in a monetary fashion, but rewarded purely by increased reputation in the community that supports human rights and privacy, despite the very real costs associated with police raids on Tor servers. Lastly, the users are expected to access Tor for free.

On the other side of the spectrum are ***for profit*** companies that provide some kind of service where users pay to access the service. This model easily fits centralized service providers such as the traditional provisioning of VPN (Virtual Private Networks) for a monthly fee or the per-download payment model of Apple iTunes. Users may access the service for free, such as in Google, but may also be monetized indirectly via advertisements, a development known as surveillance capitalism. More interesting are the attempts to monetize decentralized systems. The first attempt to do so was the P2P file-sharing service MojoNation, whose runaway inflation eventually led the system to collapse. Bittorrent, despite being ran by a single for-profit company, thus let users join their P2P service for free. With the advent of Bitcoin and the purchase of Bittorrent by the Chinese blockchain company Tron, there will be another attempt to pay for Bittorrent hosting of files via BTT (Bitocin Torrent Token). Another similar attempt is being made to create a web browser without advertising via the Brave Browser, which instead of letting service providers surveil users, attempts to fund further Brave software development by having advertisers pay in BAT (Basic Attention Token) for access to Brave's privacy-enhanced, if centralized, advertising network.

3.2.4. Standards: Law, responsibility, authority and governance

Finally, distributed and decentralized architectures may be considered as a prism to observe the reconfigurations of law, of authority and, more generally, of democracy, as per the emergence of technical norms: These norms can be given explicit shape as technical standards or simply given implicitly as the code itself. Note that decentralized systems do not require traditional laws per se for their operations; in fact traditional legal systems are deeply questioned and challenged by the fragmentation of entities caused by distributed architectures. However, at the same time, the possibility for citizen-centric technical norms embedded in every citizen by decentralized systems could be a "reshaping element for the law", enabling the re-conceptualization of fundamental notions such as liability, participation, property and privacy (Dulong de Rosnay, 2016). In fact, one of the fundamental hypotheses put forward by advocates of decentralization is that these architectures can provide a new basis in code to preserve fundamental rights.

The question is: Where is the authority from which these technical norms emerge, and who is responsible for shaping these norms? These technical norms arise first and foremost from the "running code" of the technical system itself, while the responsibility for the norms lies in the very real social power of one or more individuals. In centralized systems, the code can be easily maintained and put behind a single server. There is indeed "a single source of truth" in the running code of the server, and in terms of social power, the sole responsibility for this

code lies with the programmers – or even single programmer – who controls the code and the server. In the case of centralized systems, the source code may be open source, but the end-users must simply trust that the server is running the same code as that end-users and developers are given. In decentralized and systems, this code has to be distributed to users so they can run the software themselves on either their own server (in the case of federation) or their own peer (in the case of more fully decentralized P2P systems). There is often a original, perhaps legendary or even mythic, programmer that in the popular imagination of the developer and user community created the original protocol and code (as is the with Richard Stallman and Satoshi Nakamoto). However, in decentralized systems there is usually the necessity to require the code itself to be open source so that it can both run across as many types of machines as possible and so that it can be easily found and downloaded by users. Historically, this leads to a less corporate, more community-driven culture around decentralized systems as they tend to dovetail with the open source and free software movements.

Nonetheless, the technical norms embedded in code do not simply escape the social process of governance, and both centralized and decentralized architectures develop over time social processes of governance, where the maintenance and evolution of the technical norms given by the code evolves. In all systems, in terms of code this tends to be the social process over who gets to "commit" code to the production system that users actually engage with. In centralized systems that are closed source, the process is usually cloaked in mystery to end-users and other developers, done within the restrictions of an opaque corporate governance structure. In open-source models, the process is often still the "benevolent dictator for life" where a single programmer controls the evolution of the codebase, as he or she is given authority to determine which modifications to the original source code are "committed" to the final release. More common than a single programmer is often a group of programmers, who using informal consensus maintain control over the source code. If there are disagreements over modifications to the original code, then factions of the programmers who control the code, or even an entirely outside coder or group of coders, may "fork" the codebase and create their own parallel version. Users can give feedback and demand new features via discussion forums and comments on the codebase, but in the end have very little power. Forks can also lead to incompatible if similar versions of the codebase, which in a decentralized system may split the codebase and so tear a decentralized system apart, reducing the availability and destroying what network effects the decentralized system provided before the fork.

In order to create a more structured social governance of technical norms, the goverance of important protocols tends to move towards standards bodies, where standards in a broad sense are written documentation that makes the operation of the protocol *explicit*. The primary reason for the emergence of standards is typically very pragmatic: Multiple running code-bases that implement the same protocol need a single written specification in order to co-ordinate development. In this vein, the first documentation of the features and capabilities of a protocol, along often with the design rationale of the original programmers, is given by a ***informal specification.*** This kind of document, such as the original RFCs of the IETF, is

often kept in a publicly accessible manner so programmers can write different implementations in programming languages of their choice, while still maintaining compatibility with the original codebase. They also may simply be maintained, such as done by Tor, in order to maintain the coherency of a single codebase – which gives a decentralized system like Tor the ability to have their coders move the code from one language to another over time, i.e. from C to Rust in the case of Tor. Interestingly enough, these specifications allow abstract protocols bridge the divide between open and closed source to be implemented, allowing the same protocol to be implemented by both open source and closed source developer teams, including developer teams that do not even know each other or co-ordinate. Over time, the informal specification may become more and more detailed, with increasing number of test-cases to test for compliance with the code. However, an informal specification still ultimately may not have a well-defined governance body, with the specification controlled by a single developer or group, and no representation of users or other interests.

As certain protocols become increasingly critical, there emerges full-fledged social governance bodies with formal and well-defined social governance processes around the evolution of the specifications, and so these specifications are known as ***standards***. As standards, these specifications often go beyond the code themselves and develop various interfaces to the traditional legal system, such as processes to determine patents (and so licensing) of patents in the standards: These may vary from the informal “Note Well” process of the IETF that demands patent disclosures to the strict royalty-free licensing of the W3C. Also, these standards bodies often attempt to bring in various stakeholders even if they are not directly working on a standard in order to maintain the technical norms, such as liaisons with governments as done by the ITU (International Telecommunications Union). The formal process may even begin to resemble a government. However, standards are not a panacea: Take for example the World Wide Web Consortium (W3C). Founded by the “lone programmer” responsible for the Web and the first Web browser, Tim Berners-Lee, this standard body broke with the slower and more informal IETF to form a rigorous voting-based process for adding features to important standards such as HTML (although Berners-Lee, as Director “for life,” managed to maintain a veto power. While civil society groups representing users such as the Electronic Freedom Frontier (EFF) were allowed to join and vote, when a small group of large Silicon Valley companies led by Netflix, Google, and Microsoft decided to add controversial digital rights management (DRM) to HTML, there was considerable pushback by civil society group, open-source projects, and universities due to the security concerns and lack of freedom DRM would inflict on end-users. However, the more corporate members won the vote and Tim Berners-Lee approved of adding DRM to W3C, the question of voting and democracy at the heart of W3C’s formal standards process became transparent: Did smaller civil society groups like EFF who self-proclaimed to represent the best interests of users represent ordinary people? Or were users actually represented by services like Netflix and Facebook that wished to give them easier-to-use streaming video? The core lacuna of the democratic governance of standards bodies is how to represent the users themselves.

4. Six models for governance of encryption technologies

The final section of this deliverable draws from case studies partly examined in previous deliverables (3.1, 3.3, 3.5), partly new, and examining new material (interviews and documents) that particularly address the issue of governance in light of NEXTLEAP's focus on secure messaging and e-mail platforms. Also, we expand these issues of governance to take into account examples from the blockchain space, where the focus is on cryptocurrency. In doing so, this study seeks to provide one example for each of six models to address the governance of cryptography-based projects and technologies. The models are established according to the following criteria: 1) centralized vs. decentralized, 2) non-profit vs. for-profit, and 3) the presence or absence of a standard (either a full-fledged standard or informal). These projects were chosen to cover the space of options facing software projects, allowing centralized projects to be compared to decentralized projects in particular.

Drawing from the approaches described above, this section shows how the definition of governance of encryption and decentralization is very much "situated" in the strategies and the practices of the different projects and companies -- their development process, their business models, their relationship to users and to standardization bodies, etc. All these aspects are imbued with "political" value to the extent that choices made on each of them influence users' prerogatives, duties and possibilities to exert agency -- ultimately, their rights and liberties on encrypted messaging platforms.

	(De-)Centralized	For-/No-Profit	(No/)Standards
Signal	Centralized	Non-profit	No standards
Autocrypt	Federated	Non-profit	Informal Standards
IETF MLS	Federated	For-profit	Standards
Bitcoin	Decentralized	For-profit	No standards
Ethereum	Decentralized	Non-profit	Informal Standards
Tezos	Decentralized	Non-profit	No standards

4.1. Non-profit, centralized, no standards: Signal

Signal was the first modern secure messaging application to offer ground-breaking end-to-end encryption for free, and it currently has approximately 35 million users. While Signal itself is not the most popular messaging application (in comparison to the more than billion users on WhatsApp), the Signal Protocol has deeply transformed the whole field of secure messaging. The Signal Protocol, first known as Axolotl, introduced a solution to the known limits of both PGP and OTR (Off-the-Record Messaging). Like OTR, Signal maintains forward secrecy by virtue of a Diffie-Hellman key ratchet, but by using a double ratchet rather than a single ratchet. Unlike PGP-based solutions, forward secrecy means that a key compromise at a given moment only allows messages in the future to be compromised, so past messages cannot be read. Going beyond OTR, the Signal Protocol introduces another property, that of "future secrecy" (more accurately entitled "post-compromise security") so that messages indefinitely in the future cannot be read at any point in the future in the case of a key material compromise (Cohn-Gordon et al., 2016). In the context of Snowden revelations, Signal's solution seemed to be the perfect fit for most messaging application, and so provoked a general "turn to encryption" among secure messaging applications, where one after another important private sector players adopted the Signal Protocol, bringing encryption-by-default in messaging to billions of users: WhatsApp, Google, Facebook, and Skype all implement the Signal Protocol.

Signal was founded originally as TextSecure in 2011 as a project ran by Moxie Marlinspike for encrypting text messages. In 2011, he re-branded TextSecure as Signal and dropped the support of text messages, inventing the Signal Protocol with the help of the cryptographer Trevor Perrin. In 2013, Signal's founder and lead developer Moxie Marlinspike created Open Whisper Systems described as a "nonprofit software group," to manage the development and maintenance of Signal protocol and application, although Open Whisper Systems was founded as a single-owner limited liability company ran by Marlinspike, with all other workers being contractors.

In terms of the technical code itself, Signal is centralized. There is a single Signal server that all messages go in and out of, and Signal users can only communicate to other users on the Signal server. Signal users must register using a single application and a phone number that is stored in an secure enclave on the Signal server. Signal was criticized as this allegedly creates a "single point of failure" and an easy target for police requests and attacks. However, Signal's decision to not store metadata on its server beyond the very short delays necessary to deliver a message[3], coupled with modern cryptography seem to minimize risks related to the entire secure messaging solution being run on a centralized server.

In terms of funding, Signal follows a non-profit model: Signal claims to have never received any venture capital funding but relied on grants from organizations such as Freedom of Press Foundation, Open Technology Fund, Knight Foundation and others. However, these grants

3According to Signal's Privacy Policy https://signal.org/legal/#privacy-policy

are said by Marlinspike not create resources to maintain all three client platforms of Signal and the related server-side infrastructure. Signal has been investigating attempts to monetize via payments over Signal, resulting in the Mobilecoin initiative in mid-2018. However, Mobilecoin is being ran as a separate for-profit company by Josh Goldbard with Moxie Marlinspike as an advisor, and although it has raised 50 million for development in its Initial Coin Offering (ICO) from private investors, it has yet to deploy and Signal may or may not be its deployment platform of choice. In 2018, Signal received a $50 million donation from the co-founder of WhatsApp, Brian Action. This led to the creation of the non-profit Signal Foundation, with the goal to make Signal sustainable and to be able to extend Signal's team, that has so far never been more than 7 people.[4] The Signal Foundation was founded with Moxie Marlinspike as the CEO, and WhatsApp's co-founder Brian Acton as Executive Chairman. The larger mission of Signal Foundation was described as "to pioneer a new model of technology nonprofit focused on privacy and data protection for everyone, everywhere."[5]

Signal is commonly associated with the figure of its lead developer Moxie Marlinspike, who has become known as the original and charismatic, given his anti-authoritarian views and nomadic lifestyle, champion of the application. For many users that we have interviewed, this charismatic dimension of an app's creator is one of the crucial reasons to choose a certain messaging app. The trust in a tool is often based on trust in the person behind. As interviews have shown, Signal's development and maintenance is guided by Marlinspike's normative vision of Signal's technical and socio-political mission. Thus, such important choices as to standardize or not the protocol, accept or reject decentralized forks of the protocol, collaborate or not with free software communities, and so on have so far largely depended on Marlinspike's decisions. Moxie Marlinspike personally built the Android application, the first implementation of Signal, and maintains the iOS version, so any change to the code must be personally approved by himself. For example, currently Signal requires identification of users via a unique phone number that receives a registration text. While many users have argued against this on privacy grounds. Yet Moxie has decided that Signal still requires a phone number, as identification using a phone number and access to phone contact book is the only way to discover contacts automatically without importing the entire contact book to the server which would create a much larger privacy problem for all users if the centralized Signal server was seized or compromised. Also, as the normative goal is to allow access to encryption to as many people as possible, just as in WhatsApp, access to the phone book creates a network effect and opens the possibility of viral growth of Signal, as they see other contacts already using it. In this way, Moxie Marlinspike is a typical "benevolent dictator for life" of Signal, guiding further development of the application purely by his personal norms.

However, funding organizations, such as Open Technology Fund, and the broader Internet Freedom community,[6] have played an important role in some of the technical and social

4https://signal.org/blog/signal-foundation/
5Ibid.
6Network of NGO activists, technologists, lawyers, journalists and funders working on privacy and security-related issues and gathering at several events such as RightsCon or

decisions recently taken by Moxie Marlinspike. In order to enable push notifications on mobile phones, Marlinspike took the controversial decision to work with Google Push notifications. Furthermore, he makes Signal available as an application on both Google Play and Apple Store, in order to reach the largest audience, but he has refused to make it available on the free software "app store" F-droid for Android users trying to avoid installing Google Apps. He did this on grounds that he did not want his signing key that verifies the application to be controlled by the Free Software Foundation. While Signal is still absent on F-Droid, Marlinspike did make the decision in 2017 to make available a certified APK file (verified and signed by Marlinspike) on their website that lets users install Signal without Google Play[7] This was partly due to pressure and requests from digital security trainers, power-users and privacy advocates, based on research on high-risk users in the countries like Syria where Google Play is inaccessible due to international sanctions or censorship.

Currently Signal protocol has become a "de-facto standard" of end-to-end encrypted messaging applications, and has been adopted by popular proprietary apps, such as WhatsApp, Allo and Facebook Messenger, and forked by many smaller open-source alternatives, such as the OMEMO extension of Conversations or Matrix.org. In this process a "de facto standard" is defined as "something that works" and that's been "iterated" and redeployed by others. In this sense, all of the various Signal protocol deployments work as 'crash-tests' for the protocol, where the protocol gets "forged" by usage. As the features of the Signal protocol are clearly superior to other protocols like OTR and PGP in terms of privacy and security features, developers – including those working in federated (Conversations) or peer-to-peer (Briar) projects – see the Signal protocol as one of the best designs available, even if it is not fully standardized.

However, the adoption of Signal Protocol has not happened in the same ways for free software and proprietary projects. First, Marlinspike has released his code under the GPL license, which due to the virality of the GPL clause (i.e. any other software that GPL licensed software is integrated against inherits the GPL) makes it impossible to integrate Signal against non-open source commercial software. Therefore, when commercial companies like WhatsApp decided to integrate the Signal Protocol, they asked for the code itself, called *libsignal*, to be released under a "dual license", i.e. another non-GPL license. Marlinspike would then charge the company a large amount of funds to release his code under a less restrictive license as well as for engineering time spent on the integration. The decision of Signal's lead developer, Moxie Marlinspike, to sell the protocol to WhatsApp, and later to Facebook, was controversial in open-source circles. The controversial deal was legitimized by a mission to "bring encryption to the masses" via implementing end-to-end encryption in already popular, not activist-centric, messaging applications.

However, open source projects could not easily also integrate against the Signal Protocol. One concern was branding confusion. For example, when Signal dropped support for encrypted text messages, other developers forked the code to preserve this functionality but

Internet Freedom Festival.
7https://signal.org/android/apk/

called it “SecureText.” Moxie objected, concerned that it would cause confusion in users with “TextSecure.” Moxie has also been very concerned over the quality of other open-source secure messaging applications, pointing out numerous errors in the ChatSecure XMPP OTR application. In general, Moxie prefers there to be one high-quality codebase, *libsignal*, and has viewed even informal specifications as dangerous as it could lead a developer to miss an important, if undocumented, aspect of the security of the entire protocol, and so he has been openly critical of attempts by developers such those involved in OMEMO to reimplement Signal in a federated environment.

When commercial companies such as Wire, which at the time maintained a single centralized closed-source server and open-source clients, tried to reimplement Signal, they claim that Moxie demanded a substantial financial payment. ChatSecure’s lead developer explains this conflict as a consequence of a specific licensing politics (Signal being under GPL), that lead to tampering and modifications in the legal terms and agreements between Signal team and other implementers: “So part of his [Moxie’s] arguments with Wire was that they [Signal] hadn’t documented Signal protocol, so there was no open specification, so if you wanted to write a compatible reimplementation, you would have to read the source code which would create a derivative work, which would not allow you to use it commercially because he would argue he still has copyright of the majority of the work.” Consequently, Wire had to rewrite Signal protocol using Rust, in absence of a good documentation. Indeed, for a long time Signal protocol was not well-documented, and the specifications[8] came out only around mid-2016, “under community pressure”, as Matrix.org lead developer puts it, describing non-standardization of Signal protocol as a “business-model.” Although this has led the Signal application to being viewed as a “de facto” standard of highest quality, there is no official standard and no support for decentralization planned by Signal.

4.2 Non-profit, decentralized, informal specification: Autocrypt

The Autocrypt specification is a set of guidelines that “describe ways to how e-mail programs negotiate encryption capabilities using regular emails.”[9] Autocrypt proposes a solution to key exchange problem, one of the largest problems for user adoption of the standard IETF PGP encryption. Typically, PGP usage requires the discovery of the key material via key-servers or some other kind of “in person” key exchange in order to enable encryption and a possible type of authentication. The Signal Protocol solves this issue by having the central Signal server associate “pre-keys” with the phone numbers, and in older decentralized chat protocols like OTR the problem was solved by shared secrets. In contrast, Autocrypt has a specification for putting public key material in headers of the email. By virtue of “going back to the past” to e-mail, Autocrypt inherits the federated model of e-mail but attempts, building on OpenPGP, to layer encryption on top of SMTP. Autocrypt makes this key exchange e-mail interoperable such as K9 and Enigmail. The Autocrypt effort has been co-founded by several NEXTLEAP researchers end 2016 in Berlin and has had several

8https://signal.org/docs/
9https://autocrypt.org/

3-5 day open gatherings over the course of 2017 and 2018. These various aspects of e-mail encryption and culminated end 2017 in the publication of the Level 1 specification for usable e-mail end-to-end encryption. One particular practise was to arrange the gatherings less around “time schedules” and more like a permanent un-conference: participants can go for new sessions on an ad-hoc basis and can also leave and join sessions at will, or just take a walk for a coffee break, with meetings taking place around conferences, mainly the Internet Freedom Festival 2017 and 2018 as well as the Chaos Communication Congress (33c3 and 34c3). User testing and experiences in the field of multiple messengers now drive the discussions and decisions about the next versions of the Autocrypt specification. Although the OpenPGP standards have not been updated for more than a decade and face the problem of a declining usability in face of the success of the Signal application, Autocrypt is gaining traction among mail application developers and in the general OpenPGP community.

One particular attempt by Autocrypt to compete directly with Signal in the space of secure-messaging is the Delta.Chat secure messaging application. Delta.chat is the pioneer of what is now called “messaging-over-email” effort, suggesting an original take on federation by using SMTP, normally used for email transmission, for delivery of instant messages. Behind this project - a larger push for “social decentralization”, that aims to unbind users from “messenger silos”. While centralized messengers like Signal lack interoperability, Delta.Chat relies on the pre-existing email infrastructure and is potentially scalable to billions of email users, although the current user base is at most a few hundreds. The general effort of reusing user interfaces of existing popular messaging apps (first version was inspired by Telegram user interface, while the new dev-version is using Signal user interface), is also falling in the same attitude: instead of creating yet another silo, to propose users something they already know and are familiar with, in order to minimize migration efforts. While it has originally started as a “lone wolf” project, German developer Bjoern Petersen being the “man behind the idea,” Delta.Chat has soon joined other projects and progressively have become a collaborative effort with network of small open-source communities, continuously contributing to it.

Several key contributors in DeltaChat have also been active in the Autocrypt community and both share a set of practises. Both have been quite “loosely coordinated” with around a dozen active contributors from developers and crypto library designers, to UX/usability experts. These contributors, working on a voluntary basis, are mostly decentralization or crypto enthusiasts, who have known each other from various offline hacker gatherings, or online discussions and collaborations around email, decentralization and certain politically engaged hacker circles, including “activist tech collectives”. Both efforts also have many people use Internet-Relay-Chat (IRC) on freenode, a major gathering point for open source developments. The #autocrypt and #deltachat rooms each have 60-70 participants and DeltaChat counted for September 2018 around 5500 posted chat lines. Similar to Signal, both efforts also use the github.com site and the “git” versioning tool to discuss, collaborate and review each other’s changes. Although it may sound very positive, in terms of governance, this has led to an informal set of developers that control access to the code and the specification, even if they are quite open about accepting changes and modifications.

The Autocrypt effort and most encrypted e-mail applications are primarily non-profit and funded via grants. In fact, the Autocrypt effort has currently being funded by the NEXTLEAP effort itself. Further funding for Delta.Chat has been provided by the Open Technology Fund since July 2018, and so has concreticized in a way the “core” team working with Delta.Chat, many regular and active contributors, for example for Delta.Chat desktop effort, continue working without any “official” affiliation. Nonetheless, Autocrypt and its implementation such as Delta.chat seem to share a tacit agreement on certain modes of collaboration and informal governance that avoid reproducing what is understood as the “startup way”, that attributes fixed roles to team members, and establishes hierarchies within teams. Instead, the work is organized more or less around a set of main components of Delta.Chat, such as Delta.Chat core, Delta.Chat Android (and recently iOS), Delta.Chat Desktop, Legal and Licensing effort, as well as Usability and Needfinding. Currently Delta.Chat evolves more as an “ecosystem” than as a “messaging app”: instead of proposing “one solution to all problems”, it develops thinking towards bridging various solutions with the aforementioned components of Delta.Chat. The priorities for development and collaborations are partly informed by fieldwork and constant informal communication with targeted user communities, mainly high-risk journalists and human rights activists and NGOs. For example, one of the current efforts is focused on making Delta.Chat “pluggable” with the DAT peer-to-peer file sharing protocol. While some of these decisions for Delta.Chat development and collaboration are “naturally” pushed forward by various Delta.Chat team members out of their personal technical or political preferences, others are also driven by the design of the current funding proposal, supported by the Open Technology Fund.

Nonetheless, not having a standard and none of the contributors actually being cryptographers have led to concrete problem with the protocol that have very real-world ramificatios for users. Autocrypt does not improve the security properties of PGP, but instead makes it more usable. However, the security problems of Autocrypt -- as detailed in D2.3 – are quite considerable in comparison, as PGP does not provide authentication in a standardized fashion and does not use modern cryptographic primitives or best practices. In comparison with the Signal Protocol, PGP e-mail is strictly less secure and privacy-preserving, as a single key compromise can lead to the decryption of all previous and future e-mails, and the lack of authentication allows forwarding attacks. Therefore, while Delta.Chat is a useful experimental exercise, currently Delta.Chat is collaborating with activist-oriented email providers to provide new features such as automatic account creation, tailored for specific use-cases involving field missions for journalists and activists with self-destroying temporary accounts. This would imply that Delta.Chat is somehow safer to use than Signal for at-risk users, when in fact the reverse is true: As a secure messaging application based on PGP, Delta.chat lacks forward secrecy and post-compromise security, and so is strictly much more dangerous than Signal to use, with private information such as sender and receiver also being revealed in non-encrypted “plaintext” by the headers. Therefore, the more open-source, yet amateur, approach of Delta.Chat may actually end up endangering the community it intends to help.

While being essentially non-for-profit and activist-inspired project, Autocrypt and its implementations like Delta.Chat aims to be usable by larger user communities. In terms of licensing, Delta.Chat did the opposite of Signal: Recently the team has made a choice for Mozilla Public Licence in order to open up collaborations with for-profit actors: “The move from GPL to MPL is meant to be more inviting for also commercial collaborators as it is now easier to incorporate DeltaChat’s core chat/contact and IMAP/SMTP/Autocrypt implementations in all kinds of offerings.”[10] One of these potential commercial collaborators is Open Xchange, now working on “messaging over IMAP” solution. However, Autocrypt does not currently plan to join the IETF for standardization, preferring its loose and non-rigid working-style. While this may be advantageous for the open-source community, it’s unclear how the effort will spread to large e-mail providers, such as Gmail (who have previously expressed interest in encrypted e-mail) without the standardization necessary to ensure interoperability. So despite the success in bringing together the previously moribund PGP standardization effort, without committing to the IETF standardization needed to deal with the rest of e-mail ecosystem, Autocrypt headers even being marked as ‘spam’ by providers

4.3 For-profit, centralized, with standards: IETF MLS[11]

In contrast to Signal and Autocrypt, the new IETF Working Group on Messaging Layer Security (MLS) specificially brings together for-profit companies and the open-source community to work on a fully-fledged standard via a formal governance process. MLS was provoked in part by research and studies, such as those done by NEXTLEAP, that showed that one of the most important failings of Signal was its inability to do large group management. This problem was a problem originally from the cryptographic protocol, which like OTR, had a cryptographic ratchet that assumed the classical set-up between two participants. Thus, when faced with groups, Signal had to either have to revert to the slow and unscalable approach where each message had to be “repeated” to each member of the group, repeating the ratchet, or revert to a shared symmetric for the group that lost the forward and post-compromise security properties of the Signal Protocol. As many applications have to deal with large groups, such as WhatsApp and Facebook Chat, there was considerable desire from industry to build a messaging protocol with the same security properties of the Signal Protocol that could scale to large groups. Inspired by the work of researchers at Oxford that used a Merkle Tree of Diffie Hellman ratchets to scale a variant o the Signal Protocol to large groups, industry representatives in Silicon Valley from Cisco, Google, and Facebook all met together to decide whether or not a new standardization effort could be launched. Inria, due to their excellent work on formally verifying TLS 1.3 in the IETF and their research into formally verifying the Signal Protocol as part of NEXTLEAP, joined the group.

The time seemed to be right. As put by Richard Barnes of Cisco, one of the editors of the

10https://delta.chat/en/2018-11-17-deltaxi

11Data on Mozilla are derived from an interview with Richard Barnes of Cisco, editor of the MLS specifications, as well as Nick Sullivan of Cloudflare, the co-chair of the MLS Working Group.

MLS working drafts, “In the evolution of the messaging security industry, Signal has reached a phase 1 complete level of maturity, we have several products fielded based on an initial technology set (...) It's ripe for a second wave of technology development.” The idea for a standard was also naturally attractive to companies that realized the historic weaknesses in PGP (weaknesses in terms of security that have not been fully addressed yet by Autocrypt, as poined out in D2.2) and so that needed a modern messaging protocol. However, while the Signal Protocol had been embraced by industry initially, the problems of the large licensing fees and the lack of flexibility in changing the initial design by Moxie Marlinspike (to the worse, as Marlinspike would point out) led to the desire of industry for a standard that could be easily implemented in both open and closed-source across industry, with a clear governance process.

The choice of standardization brought together these for-profit companies from Silicon Valley with researchers, and now slowly with open source communities around OTR and Matrix.org, due to the fact that secure messaging was now considered a required feature in messaging application across industry and that it was each company’s best interest to not attempt to design their own, but to work together for the common good as these companies were not directly competing on the basis of secure messaging, unlike for-profit companies like Telegram that have not joined the standardization effort. Each company would maintain their own for-profit models. For example, Nick Sullivan of Cloudflare, co-chair of the MLS Working Group, stated that “Cloudflare sits in front of traffic and does various things for security or reliability concerns on the company’s site. The origin of our company is a service that takes technology around spam and attack prevention and applies it on a wide scale to anyone who wanted to sign up in a low-cost and low-friction manner….MLS and my specific involvement is not tied to Cloudflare's products or product lines and more tied to general philosophy, a slogan, "to help build a better internet, more private, more trustworthy, more reliable, more cost-effective" and MLS fits into this pretty nicely and a lot of what internet is used for.” Other companies had particular applications, such as Facebook Messenger, Cisco WebEx, or Google Chat, that needed to support large-group messaging. These companies faced a crisis of legitimacy, as end users would trust Moxie Marlinspike and Signal more than a protocol developed by Facebook that was even technically better. By working with academic researchers that had deeply studied the Signal Protocol and by using the IETF as a trusted brandname, these companies could eliminate their dependency on the norms and demands of Moxie Marlinspike.

4.5 For-profit, decentralized, no standards: Bitcoin

To explore the for-profit, decentralized and un-standardized model, we were able to interview developer and activist Amir Taaki, who was heavily involved in Bitcoin from its early days. Amir had been a free software developer for 15 years, when he got into Bitcoin. He was interested to find a monetary payment system on the internet for a project he was involved in, and Bitcoin was suggested to him. He subsequently became extremely involved in Bitcoin,

eventually deciding that he needed to secure his stock of digital currency, which led to the development of Darkwallet. He put together a team, Patrick and Donald Norman, and they were one of the biggest actors on the market in terms of volume. They obtained 100K in Bitcoin donations; the team (6-7 people) shared a house and paid themselves as little as possible in order to finish the code. The project was entirely free software and made of volunteers (friends among each other), even though the core team was self-paid during the time it worked on the project.

In the view of Amir Taaki, the early vision of Bitcoin was badly engineered and suffered from controversies among different teams of developers. The creation of the Bitcoin Foundation happened, in this light, when a particular group of developers tried to exclusively manage media representations around Bitcoin. However, two visions of Bitcoin kept existing: one seeing it as a payments innovation, and the other as uncensorable money. The creation of DarkWallet was a way to show that these two sides existed.

DarkWallet project leads do not know how many people use their software, as it is freely available on GitHub. As showed by debates such as the Segwit one[12], the power in Bitcoin ultimately lies in the hands of the core developers. People that own the currency are the shareholders, and a lot of those people were disappointed and split off; this led to a lot of lost talent in the community. The same thing is happening with Ethereum Wizards, who are not skilled developers, but rather economic actors, while every project needs a "skilled hardcore elite." Amir's wish was to prevent the corporate dynamic from capturing Bitcoin, and he wished to solidify Bitcoin, but he feels that things have gone in the opposite direction. He feels that it is the case for several "idealistic" that end up being co-opted by states, governments and major companies, and undermining the promise of the technology. The hacker vision needs to be reinvigorated.

Standardization, in Amir's view, is appropriate when the technology has reached a mature level. A charismatic leader eventually is no longer able to run a project on his or her own; instead an organization is needed to hold together the vision. The current state of Bitcoin is that the vision has been replaced by software, as it is run by an engineering elite that makes exclusively technical decisions in order to make software: choose from different repos, establish a system of bounties… The main question should be social, not technological: to have an effective way for the technical frame, the team of developers and the community to interact.

To Amir, academics are very important, although the blockchain space has a bit of disdain for academics, so they are not being used effectively. This is a more general problem with the field of blockchain and cryptocurrency: very fragmented, with arcane academic techniques, which leads the for-profit world to be a bit disconnected from the academic world.

In terms of privacy and its relative importance in Bitcoin, in the beginning, users did think

12 https://medium.com/@brenmcma/understanding-segwit-and-the-bitcoin-scaling-debate-c9f7170e9e79

Bitcoin was anonymous and private; at a later stage, it became clearer that it could be tracked, and better privacy-protecting techniques had to be developed. When Bitcoin first came out, there was no knowledge base on this, and the Bitcoin Foundation was working with regulators who wanted better tracing. However, in the view of Amir, anonymity is important as a constraint on power, a means of self-defence.

One of the main causes of Bitcoin's problems was, in Amir's opinion, that the mythical 'Satoshi Nakamoto' left the project at its outset, and Bitcoin has been looking for a competent leader since then. For the development of Bitcoin, the introduction of financial incentives to work on software took it to the next level as it was able to spearhead a wider movement.

Three possible scenarios could play out for Bitcoin governance in the coming years: One is a government/state-led enclosure that brings it back into the dominant financial paradigm. The second one is a ruthless corporate entity 'draining' the potential of cryptocurrency. The third one would be able to bring forward the liberatory aspects of this technology. Most likely, the future will be a mix of these three scenarios.

4.6 For-profit, decentralized, open source: Tezos[13]

Tezos presents itself as "a blockchain that can evolve by upgrading itself", and according to its website, places a special importance to "formalizing blockchain governance"[14]. Stakeholders vote on amendments to the protocol, including amendments to the voting procedure itself, to reach social consensus on proposals. Tezos supports smart contracts and offers a platform to build decentralized applications.

It is important to affirm that despite its manifesto, Bitcoin has indeed governance, even though it does not like having it. So at the present stage, it is important to take this as a given, and to try to control it, to "grab the governance bull by the horn and constrain it". The original point of view of Tezos is to decentralize further than Bitcoin, as they have incentives to participate in the network as a developer, and not just a miner.

Tezos does not describe itself as having a business model, but rather an incentive structure. The system provides a way for contributions to be rewarded, so the participants reward contributors The Tezos Foundation gives grants: a long-term way for financing is that when somebody proposes changes to the protocol, a reward can be proposed for the change, so a user can finance his or her own reward for improvement, and can ask the network to inflate a little bit to compensate him or her for work.

13This section is based on an interview with Tezos

14https://tezos.com/learn-about-tezos/; Wired featured a story about Tezos in June 2018: https://www.wired.com/story/tezos-blockchain-love-story-horror-story/

What Tezos finds most interesting in governance is agreeing on a technical roadmap for the project. It's a constitutional process that is both formal and incentive-based. As such, to sum it up, “Tezos has a process for making a new Tezos,” and “is good at standardizing itself.” A precondition for governance is that all need to agree on exactly what is going on, and everything is kept open source.

Privacy is an important factor. Tezos would prefer there to be non-private data on the blockchain. In terms of its relationship with GDPR, EU enforcement has not regulated the technology itself, but the uses of the technologies. So, the burden is on the manager of the blockchain, as if it puts its customers’ data on the blockchain, it's its fault,and not the responsibility of the blockchain itself as a technical mechanism. However, “what would be scarier, would be if customer data was on the blockchain, and they can't do it, then a court would order to remove the data, then they ordered all the copies. I am worried over court orders to shut down a chain because it has a phone number, it is dangerous and makes people liable.”

It is widely thought that governance of the blockchain means that some large entity or corporation will hold a large amount, however, cryptocurrencies work when lots of people hold a small amount. Tezos does not really worry about corporate capture via owning a large amount of tokens, as it still have forking as an escape hatch. Their biggest concern is a large corporation influencing things that do not (yet) have a well-defined governance structure.

Decentralization, in Tezos’ view, will be a matter of economics: there are economic forces that push towards centralization, so it is really hard to design a system that doesn't collapse into centralization, because centralization gives you efficiency and defends against free riders. There is a need to find economies of scale; proof of stake helps more than proof of work, as having a large amount of tokens does not seem as helpful as putting as much friction as possible between tokens.

It is hard to say what the future of blockchain governance holds. For example, Ethereum didn't have a standard for including addresses and people started using Ethereum addresses without checksum protection, lots of ether were lost. That is why it is important to reach a standard early, have a good ‘by default’ option, and Tezos is aiming at doing that.

4.6. Non-profit, decentralized, standards: Ethereum (Foundation)[15]

Ethereum is an open source computing platform and operating system, based on a blockchain principle and sporting a smart contract functionality. The platform generates the blockchain supporting the Ether cryptocurrency.

15This section is based on an interview with Vlad Zamfir, Ethereum Foundation

The origins of Ethereum lie in broader tendencies of the blockchain space, which exists as a response to governance issues. However, Bitcoin exists due to governance issues around monetary police and control of financial system, and Ethereum is about the control and governance of much larger issues, motivated by the same culture but applied to a much broader scope. Formal development of Ethereum began in early 2014 through a Swiss company, *EthSuisse*. A Swiss non-profit foundation, the Ethereum Foundation (*Stiftung Ethereum*), was subsequently created as well. Development was funded by an online public crowdsale (summer of 2014, called ICO for initial coin offering); participants bought the Ethereum value token (ether) in bitcoins.

Ethereum comprises about 100 people directly involved in its development, but has a much larger community (about 100,000). The Ethereum Foundation does not have a business model, drawing its revenue primarily from the DevCon conference cycles. The foundation has funding as it holds Ether and manages the ICO.

The technical decision making is relatively decentralized, while the political and non-technical decision-making is, according to Vlad Zamfir, very dysfunctional, as there are no legitimate norms and opinions by so many people need to be managed. In Vlad's intentions, the Ethereum system would do two things: one would be to provide a system that isn't capturable, and the other would be to provide a system that represents the needs of people's communications.

Vlad Zamfir has a very broad view of what constitutes a stakeholder in Ethereum, as many people are potentially impacted. Stakeholders in the Ethereum system are not necessarily the holders of Ether, but people who are affected by governance decisions. This includes fundamental participants, trademark users, miners, node operators, infrastructure providers, payment providers, policy bodies and in particular, the United States government… and the global public. The broader Ethereum community is made of people who take part in the shared narrative for stakeholder interest to be public. There is a risk of capture of metadata during a number of operations involving governance, including the identification of stakeholder interest, the representation of people, and the levers for decision-making.

In Vlad's view, Bitcoiners have a view of ruthless minimization, and they have implemented a number of norms to "castrate" governance as a way of reducing risk of capture, but at expense of many stakeholders. Ethereum developers have made a tradeoff of a more difficult design, and having the ability to make decision of what happens on the chain, but at the same time this makes it harder for the system to be captured by special interest groups.

In terms of standardization, an Ethereum Improvement Proposal (EIP) process exists to "describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards"[16]: for the most part, deeply technical people identify issues that do not exist yet and forecast possible solutions. The interface to the blockchain protocols

16https://eips.ethereum.org

cannot really be standardized, although there are attempts, but most fail due to a poor implementation of consensus mechanisms.

Vlad participates in two main ways in other standards processes outside of EIPs: the first is a road map, a shared understanding of where the blockchain community is going as a community in the long-term, in particular for technical upgrades; the second is research, both in terms of philosophy and of 'real' protocol research. There are also attempts of funding public infrastructure that makes Ethereum more valuable, primarily to bring together the ecosystem which determines the price of Ether. In particular, there is lots of infrastructure provided at a loss by Consensys, and the positive impact can be internalized enough by Joe [Lubin, one of Ethereum's core developers] to outweigh the cost.

Although Vlad would love Ethereum to have security proofs, he does not like academia that may be ready to put the necessary resources into it, and most of Ethereum's practitioner community does not care about proofs but about running code. And according to him, auditing running code is nightmarish, as it involves level of sophistication most people do not have, verifying software is way harder to checking theorems. Proofs are however required for core infrastructure, specifications need to be formally verified, and it is complicated to get implementations formally verified.

The main question of governance in the blockchain space according to Vlad is to further flesh out and detail its future legal status in various jurisdictions, and across the spectrum of blockchain-based applications.

5. Conclusion

In 2010, Philippe Aigrain suggested that it was time to "reclaim" Internet services, as instruments of "technical governance" perhaps better connected with the way the Internet once was. This deliverable has provided a theoretical and empirical overview of the variety of ways in which this "reclaiming" takes shape, and suggests ways in which social, economic and legal sciences research can approach it as a subject of inquiry.

As Philip Agre once stated, architecture is politics, but it is not a substitute for politics (Agre, 2003), an insight whose relevance is more evident by the day. Indeed, questions of intermediation and dis-intermediation, distribution of power, privatization of governance, privacy by design and by architecture, have hardly been more important in recent history than they are in our post-Snowden era, and reach out to the very ways in which Internet governance unfolds in our present times.

The inscription and embeddedness of the norms within the code and standards of the architecture itself can complement traditional laws, and we need to investigate this complementarity. This opens up a number of questions: How do distributed architectures redefine user skills, rights, capacities to control? How can law support user practices and their diversity, instead of countering them? What are the differences when compared to centralized architectures, non-modifiable by users, where data are stored on clusters of servers exclusively controlled by service providers? In terms of authority and control, what are the consequences of introducing encryption, file fragmentation, sharing of disk space in the technical architecture? While “first-generation” P2P networks have affected copyright first and foremost, decentralized Internet-based services prompt us to investigate issues like the redefinition of notions such as creator and distributor, the transformed status of personal data, the responsibility of technical intermediaries, the ‘embeddedness’ of law into technical devices, the kinds of entities needed to empower people with knowledge.

Ultimately, distributed architectures show the extent to which the articulation of normative systems and networked technologies is very much a “construction site” — collective, often informal norms have a central role, and they have a very ambiguous (but very much present) articulation to legal regulation. As showed by specific points of tension (shown, e.g., the blockchain subtending Bitcoin, its re-intermediations and re-concentrations; see Musiani, Mallard and Méadel, 2017), the making of distributed architectures is not the exclusive purview of so-called “democratic” arrangements. However, the awareness of the articulation between informal/collective norms and legal regulation seem to be particularly present in those contexts where distributed architectures start to be identified, not only by user communities but by institutions as well, as legitimate and empowering alternatives.

At present, as the last part of this deliverable has shown, the path towards non-profit, decentralized standards appears far from linear, but it does seem to constitute the way ahead. As we have seen throughout the case studies in previous deliverables and the present one, ecosystems have different levels of decentralization and centralization at different layers; while centralization delivers faster results with a for-profit structure, decentralization is in theory more resilient and builds more long-term value, as the Internet and the Web themselves have taught us over the years. The question for the immediate future appears to be whether the blockchain community, with experiments such as Ethereum, will be able to learn from the failures and successes of standardization in the Internet/Web space around messaging.

6. References

Agre, P. (2003). “P2P and the promise of Internet equality,” Communications of the ACM, volume 46, number 2, pp. 39–42. doi: http://dx.doi.org/10.1145/606272.606298, accessed 10 November 2016.
Aigrain, P. (2010). “Declouding freedom: Reclaiming servers, services and data,” In: 2020 FLOSS

roadmap (https://flossroadmap.co-ment.com). Third edition, at https://flossroadmap.co-ment.com/text/NUFVxf6wwK2/view/, accessed 10 November 2016
Antoniadis, P. (2016). Local networks for local interactions: Four reasons why and a way forward, First Monday, Volume 21, Number 12, https://firstmonday.org/ojs/index.php/fm/article/view/7123/5661
Braman, S. (2009). Change of state: Information, policy, and power. Cambridge, MA: MIT Press.
Braman, S. (2011). The framing years: Policy fundamentals in the Internet design process, 1969–1979. The Information Society, 27(5), 295–310. doi: 10.1080/01972243.2011.607027
Brousseau, E., Marzouki, M. & Méadel, C. (eds., 2012). Governance, Regulation and Powers on the Internet. Cambridge : Cambridge University Press.
Callon, M., Lascoumes, P. & Barthe, Y. (2001). Agir dans un monde incertain. Essai sur la démocratie technique, Paris: Seuil.
Cheniti, T. (2009). Global Internet Governance in Practice. Mundane Encounters and Multiple Enactments. Unpublished DPhil Thesis, University of Oxford.
Chrysos, P. (2016). Monuments of cyberspace: Designing the Internet beyond the network framework, First Monday, Volume 21, Number 12 https://firstmonday.org/ojs/index.php/fm/article/view/7112/5656
De Filippi, P. & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code, First Monday, Volume 21, Number 12, https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657
Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. Global Governance: A Review of Multilateralism and International Organizations, 18(3), 339-361.
DeNardis, L. (2010). The privatization of internet governance. Presented at the Fifth Annual GigaNet Symposium, Vilnius, Lithuania.
DeNardis, L. (2012). Hidden levers of internet control. An infrastructure-based theory of internet governance. Information, Communication & Society, 15(5), 720-738.
DeNardis, L. (2013). The emerging field of internet governance. In W. H. Dutton (Ed.), The Oxford handbook of Internet studies(pp. 555–576). Oxford, UK: Oxford University Press. doi: 10.1093/oxfordhb/9780199589074.013.0026
DeNardis, L. (2014). The Global War for Internet Governance. New Haven, CT and London: Yale University Press.
DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. Telecommunications Policy. doi:10.1016/j.telpol.2015.04.003
Dulong de Rosnay, M. (2016). Peer to party: Occupy the law, First Monday, Volume 21, Number 12, https://firstmonday.org/ojs/index.php/fm/article/view/7117/5658
Elkin-Koren, N. (2012). Governing Access to User-Generated Content : The Changing Nature of Private Ordering in Digital Networks. In Brousseau, E., Marzouki, M., Méadel, C. (eds.), Governance, Regulations and Powers on the Internet (pp. 318-343). Cambridge : Cambridge University Press.
Epstein, D. (2011, September). Manufacturing Internet policy language: The inner workings of the discourse construction at the Internet Governance Forum. In 39th Annual Telecommunication Policy Research Conference. Arlington, VA.
Epstein, D. (2013). The making of institutions of information governance: The case of the Internet Governance Forum. Journal of Information Technology, 28(2), 137–149.
Epstein, D. (2015). Duality squared: On structuration of Internet governance. In R. A. Lind (Ed.), Producing Theory in a Digital World 2.0 (pp. 41–56). New York, NY: Peter Lang Publishing.
Ermoshina, K., Francesca Musiani and Harry Halpin (2016). “End-to-end encrypted messaging protocols: An overview,” In: Franco Bagnoli, Anna Satsiou, Ioannis Stavrakakis, Paolo Nesi,

Giovanna Pacini, Yanina Welp, Thanassis Tiropanis and Dominic DiFranzo (editors). Internet science: Third international conference, INSCI 2016, Florence, Italy, September 12–14, 2016, proceedings. Lecture Notes in Computer Science, volume 9934. Berlin: Springer-Verlag, pp. 244–254. doi: http://dx.doi.org/10.1007/978-3-319-45982-0_22, accessed 10 November 2016.
Flyverbom, M. (2011). The Power of Networks: Organizing the Global Politics of the Internet. Cheltenham, UK : Edward Elgar Publishing.
Flyverbom, M. (2010). Hybrid networks and the global politics of the digital revolution – a practice-oriented, relational and agnostic approach. Global Networks, 10(3), 424–442. doi:10.1111/j.1471-0374.2010.00296.x
Giovanella, F. (2016). Alternative rules for alternative networks? Tort law meets wireless community networks, First Monday, Volume 21, Number 12
Halpin, H. & Monnin, A. (2016). The decentralization of knowledge: How Carnap and Heidegger influenced the Web, First Monday, Volume 21, Number 12
https://firstmonday.org/ojs/index.php/fm/article/view/7109/5655
Hofmann, J., Katzenbach, C., & Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. New Media & Society.
doi:http://doi.org/10.1177/1461444816639975
Latour, B. (2005). Reassembling the social: An introduction to actor-network-theory. Oxford: Oxford Univ. Press.
Latour, B., & Woolgar, S. (1986). Laboratory life: The construction of scientific facts (2nd edition). Princeton, N.J: Princeton University Press.
Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. Systems Practice, 5(4), 379-393.
Law, J. (2008). On sociology and STS. The Sociological Review, 56(4), 623-649.
Law, J., & Singleton, V. (2014). ANT, multiplicity and policy. Taylor & Francis.
doi:10.1080/19460171.2014.957056
Karanasiou, A. P. (2016). Law encoded: Towards a free speech policy model based on decentralized architectures, First Monday, Volume 21, Number 12,
https://firstmonday.org/ojs/index.php/fm/article/view/7118/5659
Kuerbis, B. (2010, August). Influencing internet governance through social networks and delegation: The case of secure routing. In 38th Annual Telecommunication Policy Research Conference. Arlington, VA.
MacLean, D. (2004). Herding Schrödinger's cats: Some conceptual tools for thinking about internet governance. In Don MacLean (Ed.), Internet Governance: A Grand Collaboration (pp. 73-99) (ICT Task Force Series 5), New York, NY.
Malcolm, J. (2008). Multi-Stakeholder Governance and the Internet Governance Forum. Wembley, WA : Terminus Press.
Marsden, C. (2010). Net Neutrality: Towards a Co-Regulatory Solution. Bloomsbury USA.
Méadel, C. and Francesca Musiani (2015). Abécédaire des architectures distribuées. Paris: Presses des Mines.
Meier-Hahn, Uta (2015, February 5). Internet Interconnection: Networking in Uncertain Terrain [Blog post]. RIPE Labs. Retrieved from https://labs.ripe.net/Members/uta_meier_hahn/internet-interconnection-networking-in-uncertain-terrain.
Mueller, M. L., Kuehn, A., & Santoso, S. M. (2012). Policing the network: Using DPI for copyright enforcement. Surveillance & Society, 9(4), 348–364.
Musiani, F. (2013). Governance by algorithms. Internet Policy Review, 2(3). doi:10.14763/2013.3.188
Musiani, F. (2015). Practice, Plurality, Performativity and Plumbing : Internet Governance Research Meets Science and Technology Studies. Science, Technology and Human Values, 40(2): 272-286.

Musiani, F. (2018). “Quando il peer-to-peer si ‘ricentralizza’: Vincolo sociotecnico, spinta di mercato o fallimento?” In: Gabriele Balbi and Paolo Magaudda (editors). Fallimenti digitali: Un’archeologia dei nuovi media. Bologna: Unicopli.
Musiani, F., Cogburn, D. L., DeNardis, L. & Levinson, N. S. (2016, eds.). The Turn to Infrastructure in Internet Governance. New York: Palgrave/Macmillan.
Musiani, F. and Méadel, C. (2016). “Reclaiming the Internet” with distributed architectures: An introduction, First Monday, Volume 21, Number 12, https://firstmonday.org/ojs/index.php/fm/article/view/7101/5654
Nonnecke, B. M. (2016). The transformative effects of multistakeholderism in Internet governance: A case study of the East Africa Internet Governance Forum. Telecommunications Policy, 40(4), 343–352. doi:10.1016/j.telpol.2015.12.005
Pinch, T., & Leuenberger, C. (2006). Studying scientific controversy from the STS perspective. Presented at the Science Controversy and Democracy, Taipei, Taiwan.
Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. International Theory, 7(3), 572–616. doi:10.1017/S1752971915000081
Van Eeten, M. J., & Mueller, M. (2013). Where is the governance in Internet governance?. New Media & Society, 15(5), 720-736
Wagner, P. (1994). Dispute, uncertainty and institution in recent French debates. Journal of Political Philosophy, 2(3), 270-289. doi:10.1111/j.1467-9760.1994.tb00025.x
West, C. and Zimmerman, D. H. (1987). Doing gender. Gender & Society, 1(2), 125-151.
Woolgar, S., & Neyland, D. (2013). Mundane governance: Ontology and accountability. Oxford University Press.
Ziewitz, M. (2016). Governing Algorithms: Myth, Mess, and Methods. Science, Technology and Human Values, 41(1): 3-16.
Ziewitz, M. and Pentzold, C. (2014). In Search of Internet Governance: Performing Order in Digitally Networked Environments. New Media & Society, 16(2): 306-322

Annex 1. Interview guide for this deliverable

How big is your organization?

Does your organization have volunteers? Does it keep its software open-source?

Please describe how your project/company is run in terms of

- Human resources (who are they? How were they enrolled/hired? etc.)
- Business model (if any)
- Degree of centralization/decentralization of decision making

Are these different aspects the result of initial choices, or choices over time, or evolutions of the project not envisaged at the beginning (e.g. users’ input)?

Do you know how many people use your product(s)?

How do you get user input?

Are there other concerned parties (miners in Bitcoin, for example) that have a stake in your product or standards?

Have any of these aspects change overtime? If yes, can you point to specific episodes/events that changed the course of events?

Do you aim to produce/participate in the production of a standard? What way(s) do you think are best to standardize in your field? (institutional vs. “running code”, others…)

How is your project/company being impacted by the entry into force of GDPR? Any other laws?

What's your opinion of standardization?

Does your company require standards for any parts of their products? If so, which ones and why?

How do (or are thought to) standards help your organization accomplish their goals?

Do you go through standards bodies (IETF/W3C/etc.) in your field? If there is no standards body for your field, do you want one? Why would you chose on standards body over another?

What is your company's take on organization? Do standards help or hurt the intellectual property of your organization?

What is your opinion of difference between disclosure, RAND, RFF in terms of patents?

What is your opinion of licensing? Does your company let you use GPL/MIT/BSD, etc.?

What standards did you not participate in that you use?

What is your opinion on academic research and interacting with academics? Does that happen informally or via standards bodies?

What is your opinion of the use of cryptography in security?

Are you worried about government or corporate influence or subterfuge in standards?

Do you want security proofs? Do you have any opinion of security properties?

Do you think standards bodies pay attention to, and even improve, privacy properties of the standard?

Do you think standards bodies pay attention to, and even improve, decentralization properties of the standard?

Should decentralized protocols be made by running code first, and then standardized, or the other way around? What are your success stories? Stories of failure? What were the origins of your project/company?

What do you think are the future of standards?