Benchmarking the Impact of the Next Generation Internet Initiative

FINAL STUDY REPORT

Clémentine Valayer – Gartner Consulting
STUDY 2023-044
April 2024

Gartner

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate E — Future Networds
Unit CNECT.E.3 — Next Generation Internet

Contact: Jean-Luc Dorel

E-mail: Jean-Luc.DOREL@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Benchmarking the Impact of the Next Generation Internet Initiative

FINAL STUDY REPORT

Directorate-General for Communications Networks, Content and Technology
Next Generation Internet

2024 EN

Manuscript completed in April 2024

1st edition (corrected)

Luxembourg: Publications Office of the European Union, 2024

PDF ISBN 978-92-68-14314-8 doi:10.2759/062218 KK-05-24-246-EN-N

Contents

Executive summary

The Next Generation Internet (NGI) is an EU initiative aimed at driving internet technology towards a human-centric internet aligned with European values. The NGI program provides financial support to grassroots open source projects covering various layers of the Internet. The program started operationaly in 2019 mobilising about 140M€ over 5 years and supporting more than 1000 projects.

This benchmark study evaluates the impact of NGI projects based on the following criteria: **alignment with EU Digital rights, enabling EU legislation, impact on standardisation, provision of alternative solutions, and sustainability**. The study aims to provide quantitative and qualitative insights into the NGI portfolio's performance and technological building blocks, as well as recommendations for the future evolution of the initiative. The findings aim to inform policy-making decisions and shape future work programs.

Overall, the NGI program has had a significant impact in shaping an EU tech landscape that is sustainable, sovereign, and aligned with EU policy and values.

The **quantitative** data based on a survey shows that all responding projects exhibit a clear alignment with **European Digital rights and principles**. They prioritise the rights of individuals, promote freedom of choice, enhance safety and security, promote sustainability, and foster active participation in the digital public space. NGI projects demonstrate a strong degree of impact on **enabling different EU legislations**, with a focus on supporting GDPR compliance (39% of respondents), the Digital Services Act (DSA) and Digital Market Act (DMA) (23%), the Cyber Resilience Act (30%), EU digital identity initiatives (15%), ensuring freedom of choice online (47%), and supporting the concept of digital commons (44%).

The survey shows that over half of the NGI projects collaborated with a standardisation organisation such as the W3C, IETF, OASIS, and others. Significant contributions to various **protocols and standards** aim to enhance privacy, security, interoperability, and functionality in the digital landscape. The NGI has actively participated in discussions, issue tracking, and improvement of protocols such as Solid, HTML, CSS, WebAuthn, and DNSSEC, among others. Additionally, NGI funded parties have been involved in the standardisation of software bill of materials (SBOMs) through initiatives like Package URL, OWASP CycloneDX, SPDX, and OASIS CSAF.

57% of responding projects provide **alternatives to existing solutions in the market**. These alternatives cover a wide range of domains and functionalities, including productivity tools, social media platforms, messaging and communication platforms, identity and access management systems, search tools, DevOps tools, operating systems, cybersecurity solutions, hardware

subsystems and tools, streaming platforms, maps, virtual private networks, web analytics services, and cryptography tools.

NGI funded solutions are **widely accessible** through public repositories (84%), distribution platforms and app stores (34%) or both (29%), which **drives their re-use/usage.**

76% of NGI projects have an **active community**, indicating a significant level of reuse, and with an estimated[1] **80,000-strong ecosystem of contributors,** individuals actively contribute to NGI projects through code, testing, and bug reporting, even without direct NGI funding. This collaboration with the Free and Open Source Software (FOSS) community generates a 1:50 multiplier effect; it not only draws in talented individuals but also fosters a collaborative and innovative ecosystem that is expected to persist and continue to contribute to the growth and development of NGI projects.

74% of projects **successfully follow through after the first NGI funding** , which means that 26% of projects have no further activity once the funding ends, demonstrating a 'fail fast' approach to funding of innovation. In 8% of the cases a legal structure was created (company or not-for-profit) to ensure productisation and/or revenue stream.

The survey reveals that 32% of projects received **renewed/additional funding, with public funds being the primary source**, and 68% of this funding being NGI, meaning 1 in 5 NGI projects that got additional funding inside NGI, demonstrating the capacity of the program to enable projects to mature on their way to a self-support level.

The quantitative benchmark data highlighted the positive impact of the funding on EU society, EU policy, standardisation, choice, and sustainability.

The **qualitative analysis** of the impact of NGI projects identifies a set clusters of technology which shape the digital landscape as building blocks of the Next Generation Internet. These technology clusters of digital commons encompass a wide range of areas: network and transport, decentralised social media, Web 3.0 and cryptography, internet tools' evolution, instant messaging, identity and digital signatures, open hardware, collaborative tools, crowdsourced data and AI, virtual worlds/Web 4.0 and the software supply chain. The qualitative analysis describes approximately **100 impactful projects** covering all clusters and how they are drivers for change, mainly in terms of usage and uptake but also how they drive standardisation initiatives. One example is the Fediverse, which has 3.2 M active users, 13M accounts and 19000 instances. NGI has provided the seed funding

[1] The quantitative data in this report is an extrapolation based on a survey with targeted confidence interval of 95% and a 5% error margin

for Mastodon and many other lead projects of the Fediverse, a **decentralised network of interconnected social media.** This qualitative analysis demonstrates the diversity of technology and standards' ecosystems stimulated within each cluster.

The survey was an occasion to collect **feedback from NGI grantees**. It highlights the **positive reception** of the current funding approach, and emphasises the need for **ongoing financial support** to ensure the sustainability and growth of open source initiatives. Suggestions also include diversifying the funding approach, simplifying the monitoring process, and providing clearer guidelines for project impact. Grantees also stress the importance of **focusing on technology topics** that contribute to an open and inclusive digital landscape, while addressing challenges related to scaling, user uptake, and the need for non-coder roles, marketing, technological transfer, and mentoring. **Additionally**, investment in larger education programs, collaboration between open source areas, and an NGI infrastructure offering free hosting services are suggested to enhance community involvement and adoption of NGI project outcomes.

1. Introduction

- Context

The Next Generation Initiative[2] (NGI) initiative aims to put in place the key technological building blocks of tomorrow's Internet and to shape the future Internet as an interoperable platform ecosystem that embodies the values that Europe holds dear: openness, inclusivity, transparency, privacy, cooperation, and protection of data. The goal is to empower users with the freedom of choice among a range of free and open source decentralised digital solutions.

To this end, NGI provides financial support to grass-root projects covering all layers of the Internet: from open hardware, networking and transport technologies, firmware, operating systems and virtualisation, electronic identities and middleware, decentralised ledgers, software productivity tools, traffic supervision tools, up to over-the-top internet and vertical applications.

The NGI initiative primarily operates through the use of financial support to third parties (FSTP), which is a financial instrument authorised by the Financial Regulation of the European Union. This instrument allows projects directly funded by the European Commission to allocate a portion of the grant to third parties in smaller amounts, a practice commonly referred to as sub-granting.

To implement the NGI program, the Commission calls for Research and Innovation Actions (RIA) that are responsible for distributing a significant portion of the allocated budget (typically 80%) through Open Calls to innovators, such as open-source developers, individual researchers, startups, and others.

While some qualitative and quantitative data exist at RIA level there is little evidence on the impact of the third parties' projects funded by NGI.

- Aim of the benchmark study

This benchmark study aims to evaluate the impact of NGI's initial waves of projects by benchmarking the portfolio against various criteria:

  - Impact on society: This criterion assesses the extent to which NGI projects contribute to a society that benefits from increased choice, enhanced privacy, improved transparency, greater inclusion, decentralisation, and better sustainability. These principles are aligned with the European declaration on digital rights and principles.

[2] https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-initiative

- Impact on enabling EU legislation: NGI projects are evaluated based on their ability to support and enable relevant EU legislation, such as the General Data Protection Regulation (GDPR), Digital Services Act (DSA)/Digital Markets Act (DMA), and Cyber Resilience Act (CRA).
- Impact on standardisation: This criterion measures the contribution of NGI projects towards the development and establishment of standards in the industry.
- Impact on alternative solutions: NGI projects are assessed based on their ability to provide viable alternatives and choices to existing solutions in the market.
- Sustainability: This criterion assesses the outcomes including in terms of viability of NGI projects after the conclusion of the funding period.

The results of this study provide a comprehensive overview of the NGI portfolio, analysing its performance against these benchmarking criteria as well as its technological building blocks with regards to the Web 4.0. Additionally, the study offers recommendations on how the NGI initiative can further evolve, both in terms of technology topics and the funding process.

The findings of this study will play a crucial role in informing policy-making decisions and shaping the future work programme, including for considerations for areas such as digital commons and the development of Web 4.0.

- Report

This document presents the overall portfolio impact based on the benchmark data collected in the quantitative[3] and quantitative benchmark phases. It provides the following sections:

1. Introduction
2. NGI portfolio landscape
3. Quantitative impact on EU values, on policy, standardisation, choice and sustainability
4. Qualitative impact description per technology cluster
5. Grantees' feedback

[3] Based on insight collected from the NGI1000 survey. The full methodology of the study is available in annex.

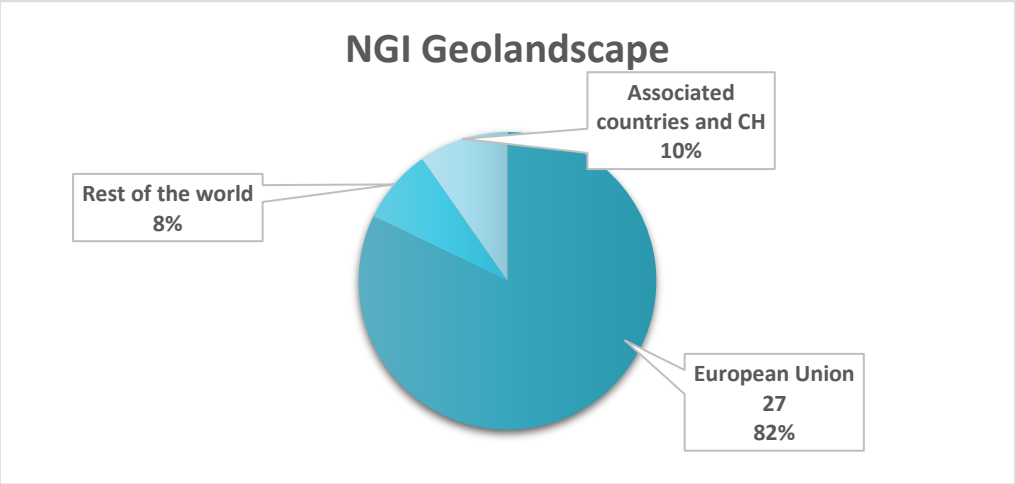
2. NGI Portfolio landscape

This section describes the NGI portfolio landscape[4] in terms of geography and research focus.

2.1. Geolandscape

The NGI funded projects are accessible through an online catalogue, which showcases a wide array of hardware, software, and app solutions. The catalogue has information on the countries associated with the funded projects. As presented in the figure below, the NGI geolandscape primarily focuses on funding projects in countries within the European Union. However, it also extends its reach to associated countries[5] and the rest of the world.

Figure 1 – NGI Geolandscape



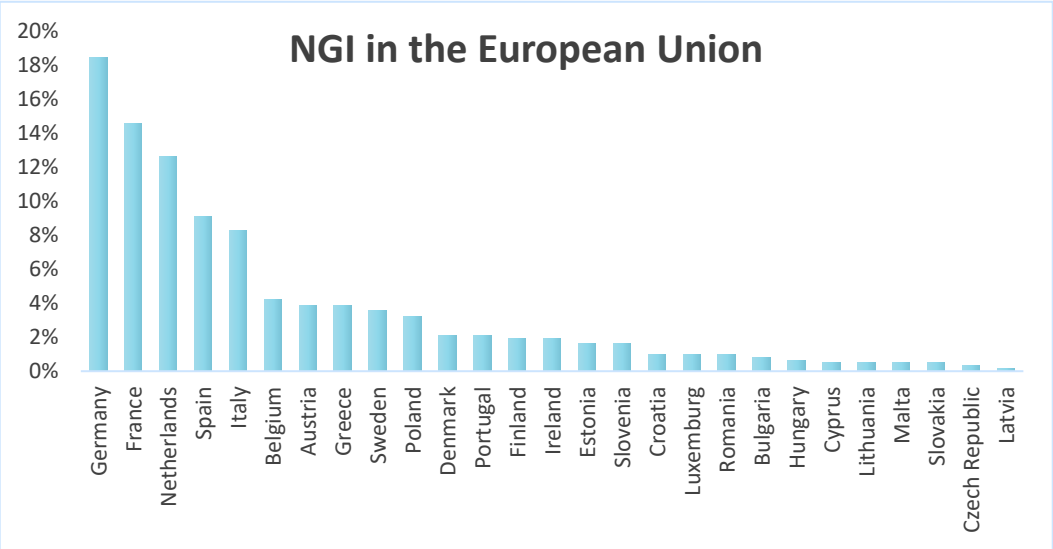
Source: Author's own elaboration

The NGI geolandscape shows a distribution of funded projects across all EU 27 countries. The figure below presentats the distribution of NGI-funded projects across these countries.

[4] The scope of the portfolio is described in detail in annex 2

[5] Third countries associated to Horizon Europe: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_en.pdf

Figure 2 – NGI in the European Union



Source: Author's own elaboration

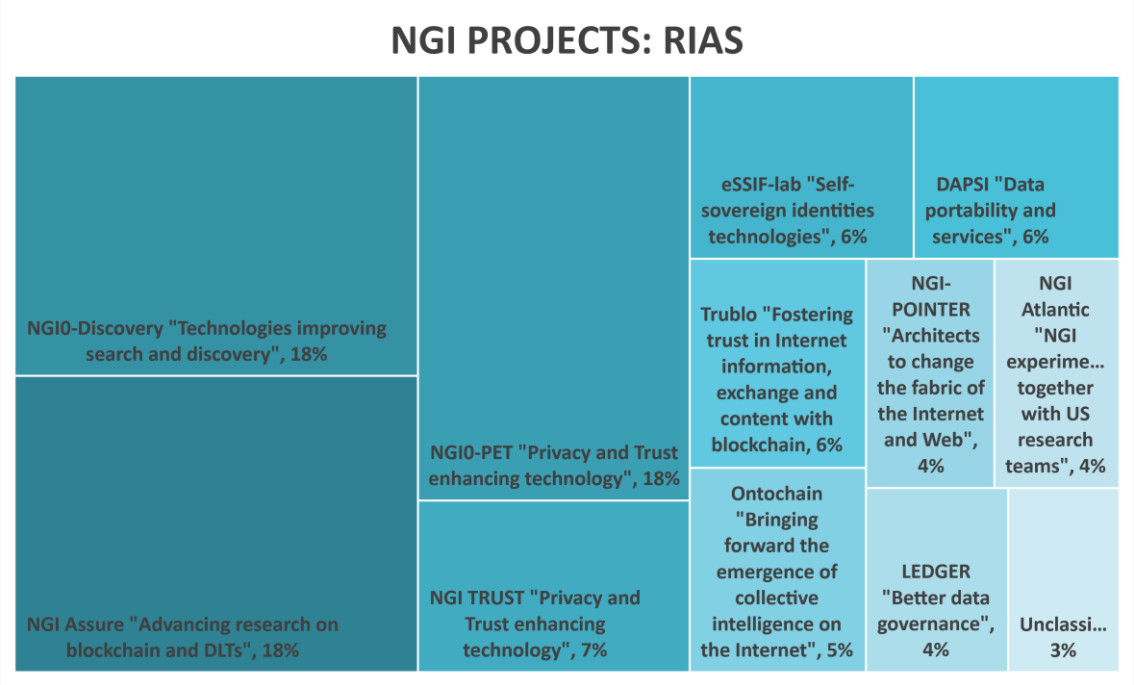
2.2. Research and Innovation Actions (RIAs) and project categories

- RIAs

The NGI initiative is mostly implemented through financial support to third parties. The Commission calls for Research and Innovation Actions (RIA). Their duty is to implement the budget via Open Calls to innovators such as open-source developers, individual researchers, startups, etc.

Based on the data provided in the NGI catalogue, we can analyse the distribution of NGI-funded projects across different NGI calls. The percentages in the figure below indicate the proportion of projects allocated to each call/ RIA.

Figure 3 – NGI projects: RIAs



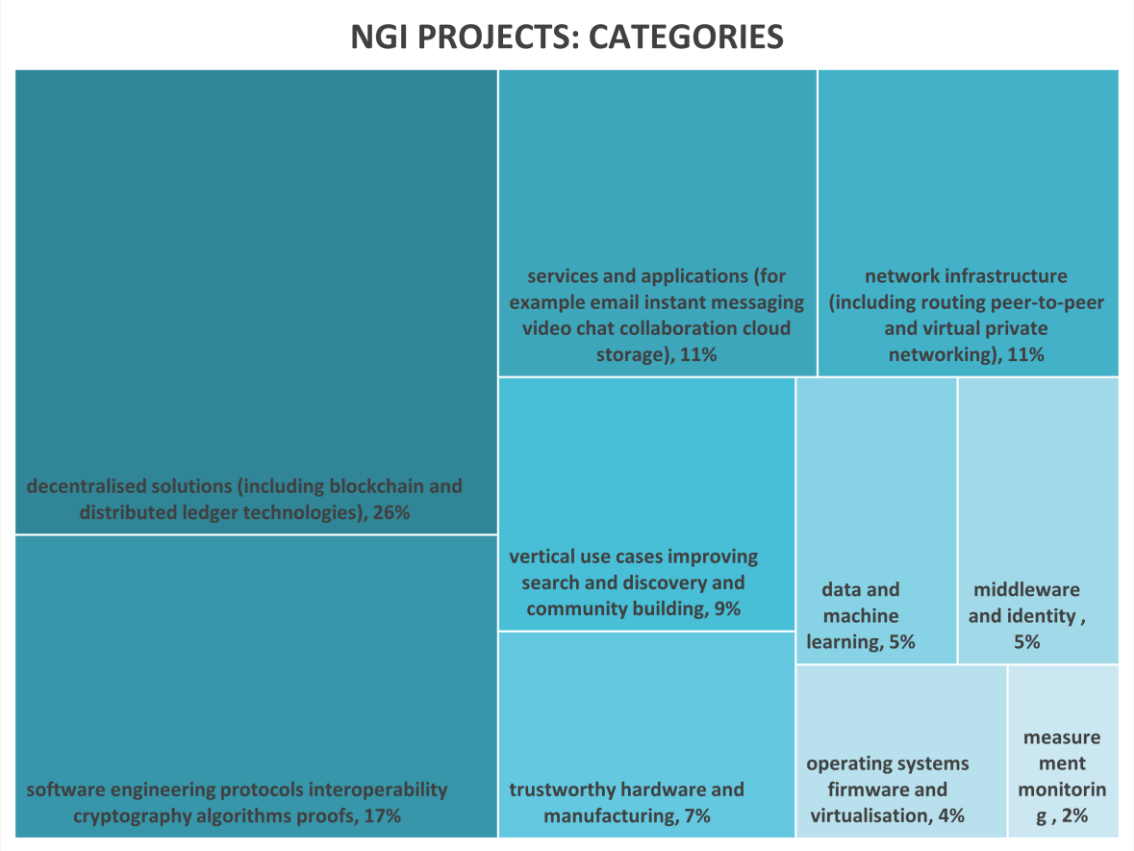
Source: Author's own elaboration

From this analysis, we can observe that the NGI Assure, NGI0-Discovery, and NGI0-PET calls have an equal distribution of projects, each accounting for 18% of the total projects. These calls focus on blockchain, DLTs, search and discovery technologies, privacy, and trust-enhancing technologies. The remaining calls, such as TRUST, eSSIF-lab, DAPSI, Trublo, Ontochain, NGI-POINTER, LEDGER, and NGI Atlantic, each have a smaller allocation ranging from 7% to 3%. These calls cover various aspects of the NGI's goals, including self-sovereign identities, trust-enhancing technologies, data portability, fostering trust, collective intelligence, changing the fabric of the internet and web, better data governance, and international collaborations.

- Categories

The NGI catalogue enables users to explore the diverse range of projects across multiple categories. These areas encompass a wide range of technologies and applications that are driving innovation in the digital landscape. The figure below provides the percentages which represent the relative distribution of NGI-funded projects across these areas.

Figure 4 – NGI projects: categories



Source: Author's own elaboration

Based on the provided data, we can draw several conclusions about the distribution of NGI-funded projects across different areas of focus.

- Firstly, decentralised solutions (including blockchain and distributed ledger technologies), receive the highest percentage of funding at 26%. These solutions aim to enhance security, transparency, and trust while avoiding being a single point of concentration due to their decentralised nature.
- The distribution of funding in NGI-funded projects highlights a significant focus on software engineering, protocols, interoperability, and cryptography algorithms proofs. This category receives a total of 17% of the funding. Software engineering encompasses methodologies, tools, and best practices that improve the efficiency and quality of software development processes. Interoperability refers to the ability of different systems and technologies to seamlessly work together. This area focuses on developing standards, protocols, and technologies that enable interoperability between various digital systems and platforms. Cryptography algorithms and proofs are essential for ensuring data security and privacy. This area involves the development of robust

cryptographic algorithms and mathematical proofs to protect sensitive information and enable secure communication.

- Services and applications, such as email, instant messaging, video chat, collaboration, and cloud storage, receive 11% of the funding. This area focuses on the development of services and applications that enhance communication, collaboration, and data storage. The development of these services and applications aims to improve user experiences and facilitate efficient and secure data management.
- Network infrastructure, including routing, peer-to-peer, and virtual private networking, receives 11% of the funding. Network infrastructure refers to the underlying systems and technologies that enable communication and data transfer. This area involves the development of routing protocols, peer-to-peer networking solutions, and virtual private networking technologies to ensure efficient and secure network operations, crucial for ensuring reliable data transfer.
- Vertical use cases improving search and discovery and community building receive 9% of the funding. This area focuses on developing innovative solutions that improve search and discovery capabilities, as well as community building within digital platforms. It involves the application of technologies like artificial intelligence, data analytics, and social networking to enhance user experiences and interactions. Improving search and discovery capabilities and facilitating community building can lead to more engaging and personalised digital experiences.
- Trustworthy hardware and manufacturing also receive 7% of the funding. This involves the development of secure and reliable hardware components and manufacturing processes, crucial for building trust in digital systems.
- Data and machine learning receive 4% of the funding. This area involves the development of algorithms, models, and tools for data analysis and machine learning applied to internet-related solutions.
- Middleware and identity receive 5% of the funding. Middleware acts as a bridge between different software applications, enabling seamless communication and integration. Identity management systems ensure secure and reliable identification and authentication processes. By investing in this area, there is a commitment to enhancing the efficiency, interoperability, and security of digital systems.
- Operating systems, firmware, and virtualisation receive 4% of the funding. Operating systems serve as the foundation for software applications to run on hardware devices. Firmware refers to the

software embedded in hardware devices, enabling their proper functioning and providing low-level control and functionality. Virtualisation technologies enable the creation of virtual environments, allowing multiple operating systems or applications to run on a single physical machine. By investing in this area, there is a focus on ensuring the smooth operation, security, and scalability of digital systems.

- Measurement, monitoring, analysis, and abuse handling receive 2% of the funding. This area encompasses the development of tools, technologies, and methodologies for measuring, monitoring, analysing, and handling abuse in digital networks. It also includes efforts to identify and apply the potentials of using artificial intelligence techniques to detect and prevent online threats, enhance child safety measures, and promote a secure online environment for children.

In conclusion, the data[6] indicates that the NGI-funded projects are distributed across various areas of focus, reflecting the diverse technological landscape of the Internet industry.

[6] Detailed insight on the number of projects for each category and RIA is available in annex 1

3. Quantitative impact on EU values, on policy, standardisation, choice and sustainability

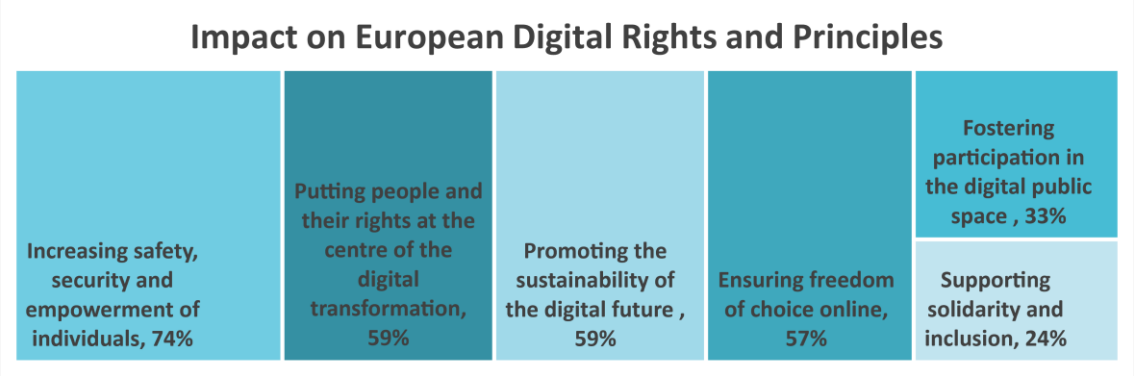
This section provides the assessment of the impact of the NGI projects on EU values, EU policy, standardisation, choice, and sustainability.

3.1. Society and EU Digital Rights

This section examines the impact of NGI's projects on society. It evaluates how these projects contribute to a society that benefits from expanded choices, increased privacy, enhanced transparency, greater inclusivity, decentralised systems, and improved sustainability. These principles align with the European declaration on digital rights and principles.

Based on the data collected, the figure below provides the percentages indicating the proportion of projects that relate to specific aspects of these European Digital rights and principles.

Figure 5 – Impact on European Digital Rights and Principles



Source: Author's own elaboration

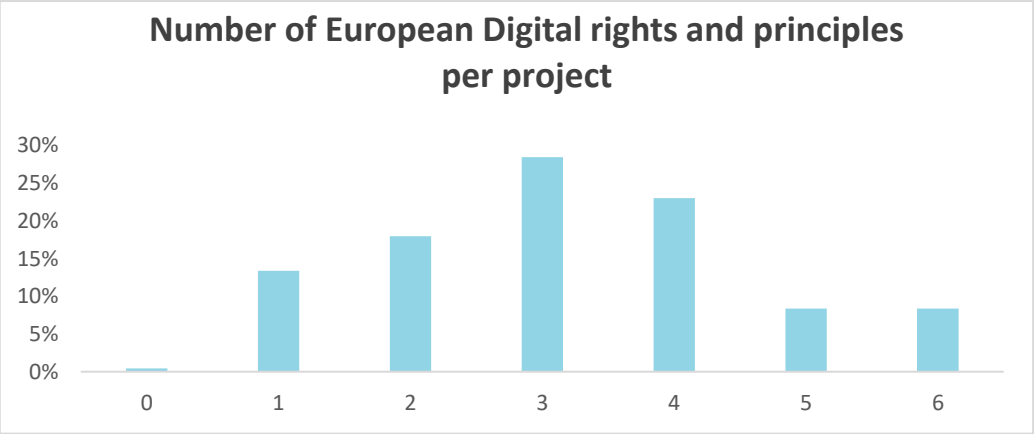
The survey analysis shows:

- 74% of projects are related to increasing safety, security, and empowerment of individuals. This includes initiatives focused on cybersecurity, privacy protection, and empowering individuals to have control over their digital lives.
- 59% of projects are related to putting people and their rights at the centre of the digital transformation. This indicates that a significant number of projects focus on prioritising the rights of individuals.
- 59% of projects are related to promoting the sustainability of the digital future. This includes initiatives that prioritise ethical considerations and responsible use of digital technologies.

- 57% of projects are related to ensuring freedom of choice online. This includes promoting open and accessible digital platforms and services that allow users to exercise their rights and make informed choices.
- 33% of projects are related to fostering participation in the digital public space. This includes initiatives that encourage active involvement, collaboration, and democratic participation in shaping the digital future.
- 24% of projects are related to supporting solidarity and inclusion. This includes initiatives focused on bridging the digital divide, promoting digital inclusion, and ensuring equal access and opportunities for all individuals.

The survey analysis further shows that each NGI project surveyed is connected to at least one European principle, with around 30% of projects implementing three of these values, as the figure below demonstrates. This underscores the free and open source (FOSS) community's ability and readiness to commit to European values.

Figure 6 – Number of European Digital Rights and Principles per Project



Source: Author's own elaboration

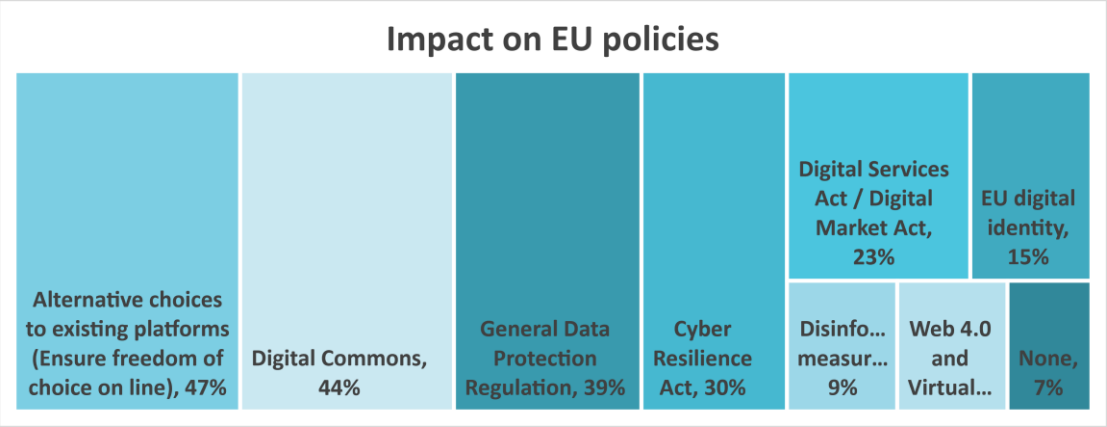
In summary, all projects exhibit a clear alignment with European Digital rights and principles. They prioritise the rights and well-being of individuals, promote freedom of choice, enhance safety and security, promote sustainability, and foster active participation in the digital public space.

3.2. EU legislation and policies

The extent to which NGI projects align with and facilitate compliance with EU legislation and policies is analysed. This evaluation focuses on how these projects contribute to and support relevant EU regulations, including the General Data Protection Regulation (GDPR), Digital Services Act (DSA)/Digital Markets Act (DMA), and Cyber Resilience Act (CRA).

Below is a breakdown of how NGI projects contribute to enabling specific EU legislations, based on the survey analysis.

Figure 7 – Impact on EU Policies



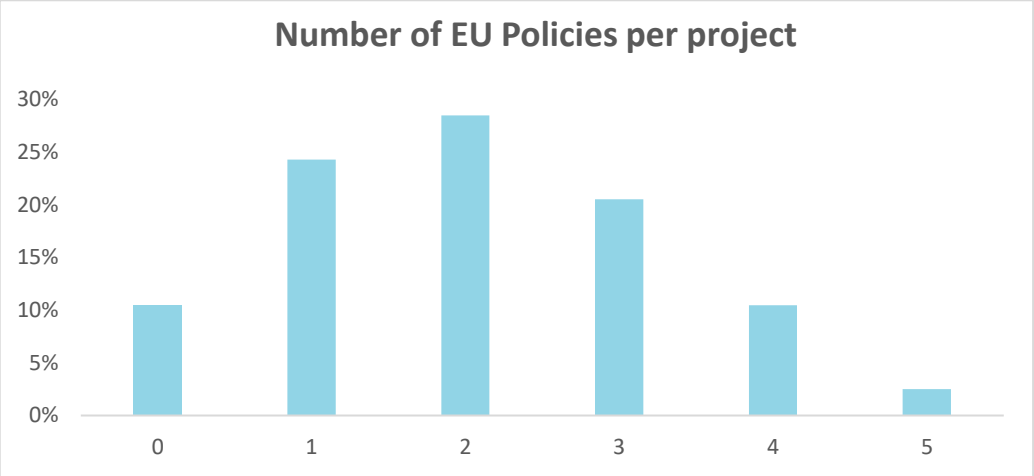
Source: Author's own elaboration

This data highlights that

- Almost half of NGI projects (47%) focus on providing alternative choices to existing platforms, aiming to ensure freedom of choice for users in the online space.
- A high number of NGI projects (44%) contribute to the concept of digital commons, which emphasises the shared ownership and collaborative use of digital resources.
- A significant portion of NGI projects (39%) contribute to enabling the General Data Protection Regulation (GDPR), which focuses on protecting individuals' personal data and privacy.
- Almost a third of NGI projects (30%) contribute to enabling the Cyber Resilience Act, which focuses on enhancing the resilience of digital infrastructure and systems against cyber threats.
- A portion of NGI projects (15%) support and enable EU digital identity initiatives, which aim to provide individuals with secure and interoperable digital identities across different services and platforms.
- A quarter of NGI projects (23%) support and enable the Digital Services Act (DSA) and Digital Market Act (DMA), which aim to regulate online platforms and ensure fair competition in the digital market.
- A small percentage (9%) of NGI projects specifically address measures to combat disinformation and promote information integrity.
- A small percentage (9%) of surveyed NGI projects indicate that they are dedicated to advancing the development and utilisation of Web 4.0 technologies and virtual worlds.

The survey analysis further shows that 90% of NGI projects surveyed are connected to at least one European policy or legislation, with almost 30% of projects implementing two of these, as the figure below demonstrates.

Figure 8 – Number of EU Policies per project



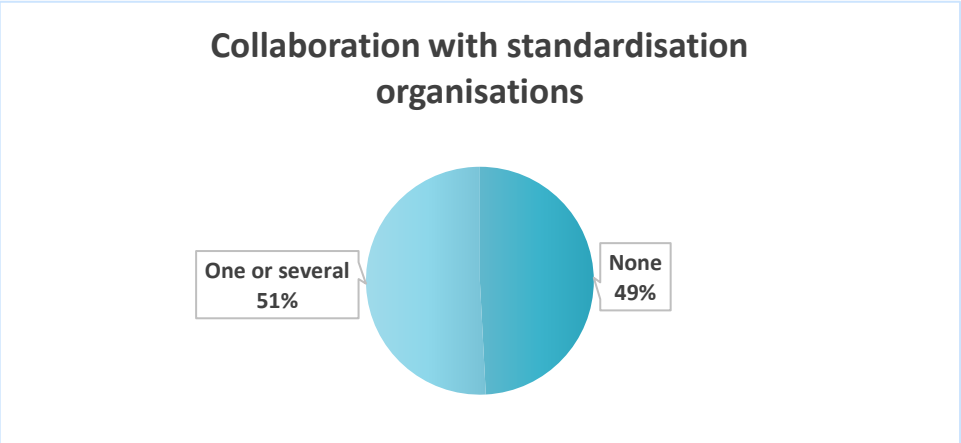
Source: Author's own elaboration

Overall, NGI projects demonstrate a strong degree of impact on enabling different EU legislations, with a significant focus on GDPR compliance, ensuring freedom of choice online, and supporting the concept of digital commons.

3.3. Standardisation

Over half of the NGI projects surveyed mention that they collaborated with a standardisation organisation. Collaborating with standardisation organisations allows NGI projects to align with and develop new protocols, frameworks, and best practices, ensuring interoperability and scalability. This collaboration helps drive innovation, ensures compatibility and interoperability, and fosters a cohesive ecosystem for the NGI. This involvement of NGI projects with standardisation organisations also demonstrates a commitment to creating a sustainable and standardised framework for the future of the internet.

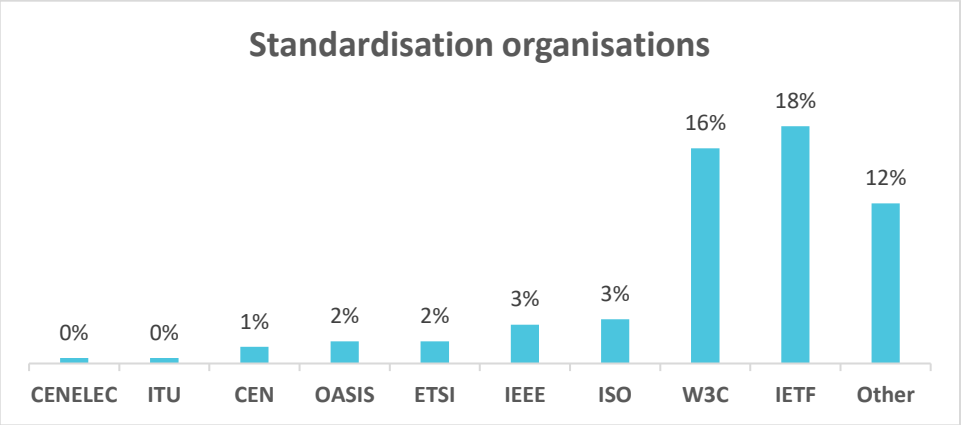
Figure 9 – Collaboration with Standardisation Organisations



Source: Author's own elaboration

The various standardisation organisations cited in the survey are presented in the figure below.

Figure 10 – Standardisation Organisations



Source: Author's own elaboration

The IETF (Internet Engineering Task Force) and W3C (World Wide Web Consortium) being the most cited organisations (respectively 18% and 16%) aligns with their prominent roles in developing internet protocols and web standards.

Protocols cited in the survey for the **W3C** include:

- Discussions and contributions related to the Hypertext Markup Language (HTML), a standard for structuring and presenting content on the web.
- Discussions and contributions related to Cascading Style Sheets, a standard for describing the presentation of a document written in HTML or XML.
- Contributions to the W3C's User Interface Security standardisation activities, aiming to enhance security in web user interfaces.

- FEP (A Fediverse Enhancement Proposal is a document that provides information to the Fediverse community): Involvement in discussions and contributions to the Fediverse Enhancement Proposals, aiming to improve interoperability and functionality in federated social networks. The FEP Process is an initiative of the SocialHub developer community, a liaison of the W3C Social Web Incubator Community Group.
- Contributions to the Solid Protocol aiming to create a decentralised social web platform with data ownership and interoperability.
- Atomic Data standard: Involvement with the Atomic Data standard, which provides a framework for representing and querying structured data on the web. The W3C Atomic Data Community Group is closed since December 2023.
- WebAuthn (issue discussion): Participation in discussions and issue tracking related to the W3C Web Authentication (WebAuthn) standard, which provides a secure and convenient way to authenticate users on the web.

Protocols and standards cited for **IETF** include:

- RFC 8905: An Internet Engineering Task Force (IETF) document that defines the "Requirements for DNS Privacy Service Operators" to enhance privacy and security in DNS operations.
- RFC 9498: An IETF document that specifies the "SIMPLE Made Simple" protocol, providing a framework for session initiation and management in real-time communication applications.
- ROSA (draft-trossen-rtgwg-rosa): A draft document within the IETF Routing Area Working Group (RTGWG) that proposes a framework for routing and orchestration in service-oriented architectures.
- KITTEN working group (IETF): Contributions made within the IETF KITTEN working group, focusing on the development and improvement of Simple Authentication and Security Layer (SASL) mechanisms.
- DNSSEC Bootstrapping (draft-ietf-dnsop-dnssec-bootstrapping): Involvement in the IETF DNS Operations (DNSOP) working group's draft on DNSSEC bootstrapping, aiming to improve the security of the DNS infrastructure.
- RFC 8684: An IETF document that defines the "TCP Extensions for Multipath Operation with Multiple Addresses" to enable multipath transmission in TCP connections.
- RFC 9397: An IETF document that specifies the "Delayed Binding for the Extensible Messaging and Presence Protocol (XMPP)" to optimise resource usage in XMPP communication.

- TCPLS (draft-piraux-tcpls): Involvement in the IETF draft on TCPLS, which proposes a new transport protocol that combines the benefits of TCP and TLS.
- Analytics.txt (draft-ring-analyticstxt-02): Involvement in the IETF draft on Analytics.txt, which aims to provide a standardised way for websites to communicate their analytics practices to users.
- RLED BAT (draft-irtf-iccrg-rledbat-04): Contributions made to the RLED BAT draft within the IRTF ICCRG, focusing on the Rate-Limited Explicit Congestion Control (RLED BAT) algorithm.
- CFRG OPAQUE (draft-irtf-cfrg-opaque): Involvement in discussions and contributions to the Crypto Forum Research Group (CFRG) draft on the OPAQUE password-authenticated key exchange protocol.
- Braid-spec: A specification for the Braid decentralised communication protocol, aiming to provide secure and scalable messaging for applications; currently an IETF draft.
- NTP (Network Time Protocol) draft: Participation in the discussion and contribution to the new draft of the Network Time Protocol, a standard for synchronising time across computer systems.
- JMAP WebPush VAPID (draft-gultsch-jmap-webpush-vapid): Contributions made to the JMAP WebPush VAPID draft, which specifies a mechanism for using VAPID (Voluntary Application Server Identification) in the JMAP protocol.

Standards cited for **OASIS** includes:

- ODF (Open Document Format) TC: Involvement in the OASIS Open Document Format Technical Committee, contributing to the development and improvement of the open standard for office documents.

“Other organisations” cited gather a set of standardisation initiatives which include:

- Collaborations with the XMPP Standards Foundation(XMPP Standards Foundation defines protocols on top of IETF’s Extensible Messaging and Presence Protocol (XMPP)), including updates and publication of various XMPP Extension Protocols (XEPs) related to authentication, stream management, and more.
- Contributions made to address errata and specify the use of Cross-Origin Resource Sharing (CORS) in the OpenID Connect protocol, enhancing security and interoperability. OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 framework of specifications (IETF RFC 6749 and 6750).

- Involvement with UniResolver, a decentralised identifier (DID) resolver, specifically related to the "moncon" DID method. The Universal Resolver resolves Decentralised Identifiers (DIDs) across many different DID methods, based on the W3C DID Core 1.0 and DID Resolution specifications. It is a work item of the DIF Identifiers&Discovery Working Group.
- Contributions made to the Resource Mapping Language (RML), a standard for expressing mappings between heterogeneous data sources. RML is defined as a superset of the W3C-recommended mapping language, R2RML, that maps data in relational databases to RDF.
- Contributions made to improve the Web Platform Tests test suite, which provides a comprehensive set of tests to ensure interoperability and conformance of web platform implementations.
- Involvement with the Lib25519 library, which provides cryptographic functions based on the Ed25519 elliptic curve.
- Involvement with the NeoChat project within KDE, including issue tracking, bug reporting, and merge requests for the development of the chat application. NeoChat is a client for Matrix, the decentralised communication protocol for instant messaging.
- Standardisation of Software-bill of materials (SBOMS):
    - Package URL (purl-spec): A standard emerged from NGI-funded work, providing a standardised way to identify packages in SBOMs and related tools and databases.
    - OWASP CycloneDX: An industry-wide standard for exchanging SBOMs, adopted by OWASP (Open Web Application Security Project) for enhancing software supply chain security.
    - ECMA (standardisation of OWASP CycloneDX): The standardisation process of OWASP CycloneDX at ECMA, a standards organisation for information and communication systems.
    - OSSF OSV (at the Linux Foundation): Adoption of the Package URL standard by the Open Source Security Foundation's Open Source Vulnerability Database (OSV) project, hosted by the Linux Foundation.
    - OASIS CSAF: Adoption of the Package URL standard by the OASIS Cyber Threat Intelligence (CTI) Technical Committee's Common Security Advisory Framework (CSAF) project.
    - SPDX: Adoption of the Package URL standard by the Software Package Data Exchange (SPDX) project, providing a standard format for sharing software component information.

- Contributions made to the Open Geospatial Consortium, focusing on geospatial standards and interoperability.
- The Internet of Production (IoP) Alliance (integration of digital technologies and connectivity within industrial production processes): Contributions made to Open Know-How, an open data model for sharing hardware designs and documentation online.

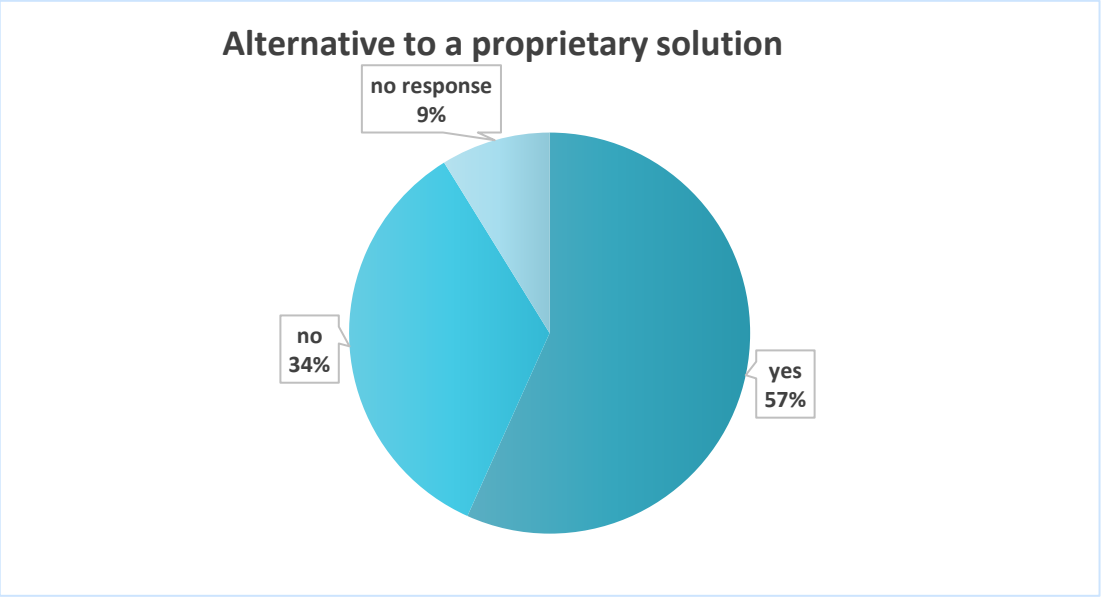
In conclusion, the NGI has made significant contributions to various protocols and standards, working in collaboration with organisations such as the W3C, IETF, OASIS, and others. These contributions aim to enhance privacy, security, interoperability, and functionality in the digital landscape. The NGI has actively participated in discussions, issue tracking, and improvement of protocols such as Solid, HTML, CSS, WebAuthn, and DNSSEC, among others. Additionally, the NGI has been involved in the standardisation of software bill of materials (SBOMs) through initiatives like Package URL, OWASP CycloneDX, SPDX, and OASIS CSAF.

3.4. Alternatives, freedom of choice

In assessing NGI projects, it is important to evaluate their impact on providing viable alternatives and choices to existing solutions in the market. By offering alternatives, NGI projects have the potential to promote competition, innovation, and user empowerment. These projects aim to challenge the status quo and address the limitations or shortcomings of current solutions.

The survey findings indicate that a significant majority, specifically 57% of NGI projects, provide an alternative to proprietary solutions.

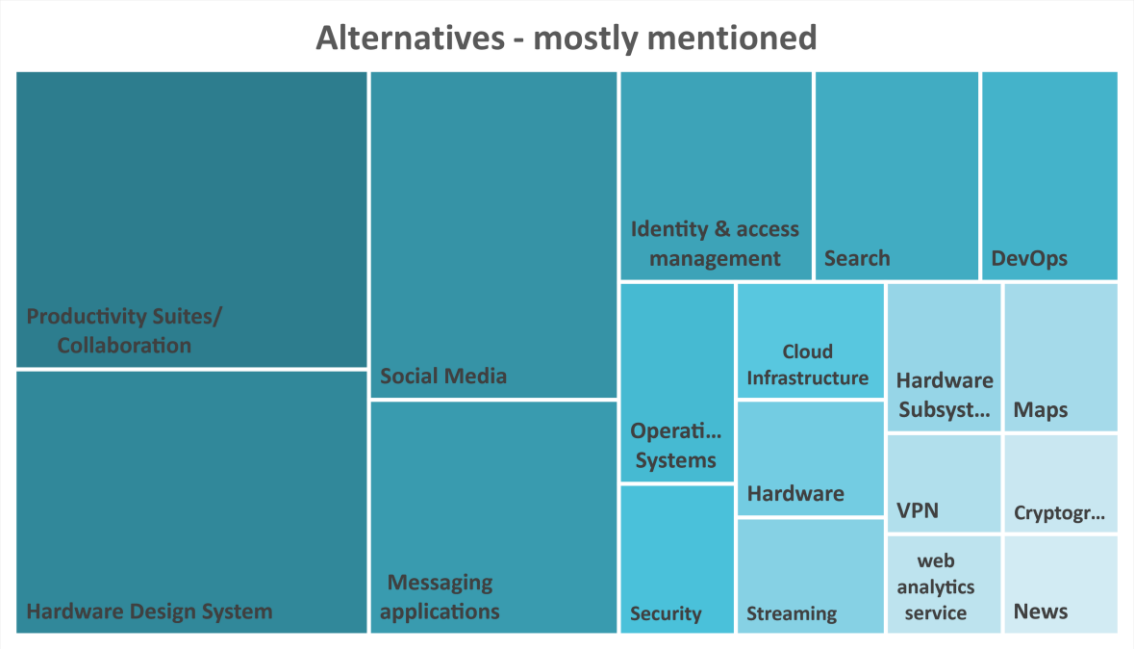
Figure 11 – Alternatives to a Proprietary Solution



Source: Author's own elaboration

These alternatives encompass a broad spectrum of solutions. The figure below highlights those that were mentioned multiple times.

Figure 12 – Alternatives – Mostly Mentioned



Source: Author's own elaboration

These are:

- Software suites or tools that enhance productivity and enable collaboration among users, facilitating document creation and sharing.
- Systems or tools used in electronic product development, aiding in the design and simulation of hardware components.
- Social media platforms that allow users to connect and interact with each other.
- Messaging and communication platforms.
- Systems or services that manage user identities and control access to resources, ensuring security and privacy (Identity & access management)
- Search tools or engines that help users find specific information within a given domain or dataset.
- Tools and practices related to software development and operations (DevOps), promoting collaboration and efficiency.
- Operating systems.
- Services or products that protect against cyber threats and ensure the security of digital systems and data.

- Providers of virtualised computing resources, storage, and networking services, enabling flexible and scalable IT infrastructure (Cloud).
- Hardware and hardware subsystems: examples: hardware that enables devices to connect to wireless networks.
- Solutions related to platforms that provide online video or audio content for users in streaming.
- Maps.
- Virtual private networks, which allow users to create a secure and encrypted connection over a less secure network
- Web analytics service: tools and platforms that provide insights and data about website performance
- Cryptography tools for protecting sensitive data, securing communication channels, and preventing unauthorisd access.
- News: solutions for debunking fake news and for providing detailed agiculture weather forecasts.

Other alternative solutions cited once in the survey cover a wide range of domains and functionalities, including data management, databases, networking, productivity, and more.

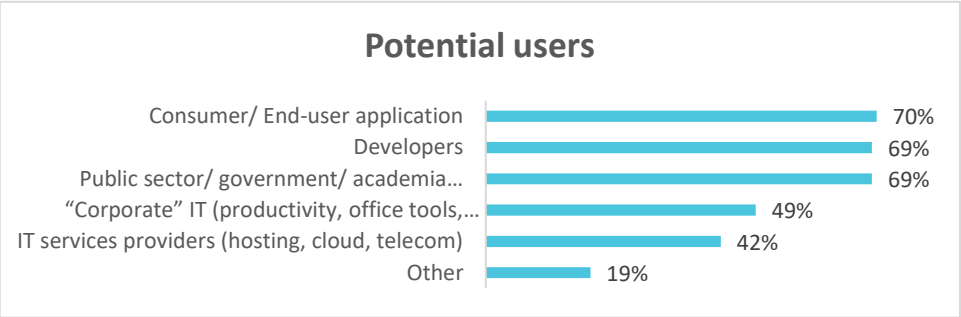
In conclusion, it is important to note that while the solutions presented here offer alternatives to the status quo, some which are very popular already, not all of them are fully deployable or available for use. Some may still be in the research stage or undergoing development. However, they serve as a promising starting point and as they continue to evolve and mature, they may become viable alternatives that challenge and disrupt the current technological landscape.

3.5. Sustainability

3.5.1. Sharing and reuse of the solution

As shown in the figure below, the survey insights indicate that NGI solutions cater to potential **users** across diverse ecosystems, with similar potential levels of interest (70%) from end-user applications, developers, and the public sector. NGI also targets “corporate IT“ such as productivity suites (50% of projects) and IT service providers (42%).

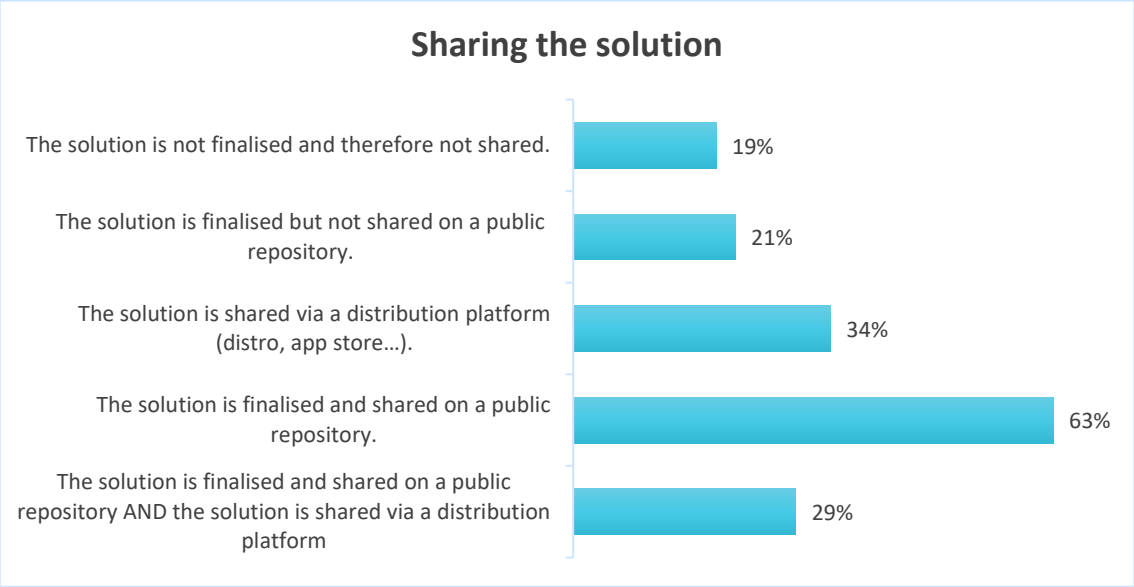
Figure 13 – Potential Users



Source: Author’s own elaboration

Sharing the the solution through a repository, pushing it through distributions, and ensuring it is easily discoverable and reusable through app stores are all important factors in promoting its adoption and reuse. The figure below illustrates the survey results regarding the sharing of the solution.

Figure 14 – Sharing the Solution



Source: Author’s own elaboration

63% of respondents share their solution on a public repositor, such as GitHub, making it easily accessible to the community. Developers can clone, fork, and contribute to the project, fostering collaboration and encouraging reuse. The availability of the solution in a centralised repository also makes it easier for others to find and evaluate its suitability for their own projects.

34% of respondents share it via a distribution platform. Using these platforms, such as such as package managers, simplifies the process of installation and integration. It allows users to easily access and deploy the solution within their own environments, increasing the likelihood of its reuse. Making the solution available through app stores, increases its visibility and accessibility to a wider

audience. Users can easily search for and install the solution on their devices, promoting its adoption and potential for reuse.

It is interesting to note that 29% have their solution both shared on a public repository AND shared via a distribution platform.

These sharing practices contribute to the sustainability of the NGI projects by facilitating collaboration, increasing visibility, and simplifying the process of integrating the solution into different projects and environments.

By examining the extent of **reuse and adoption** of NGI-funded projects, we can evaluate their sustainability.

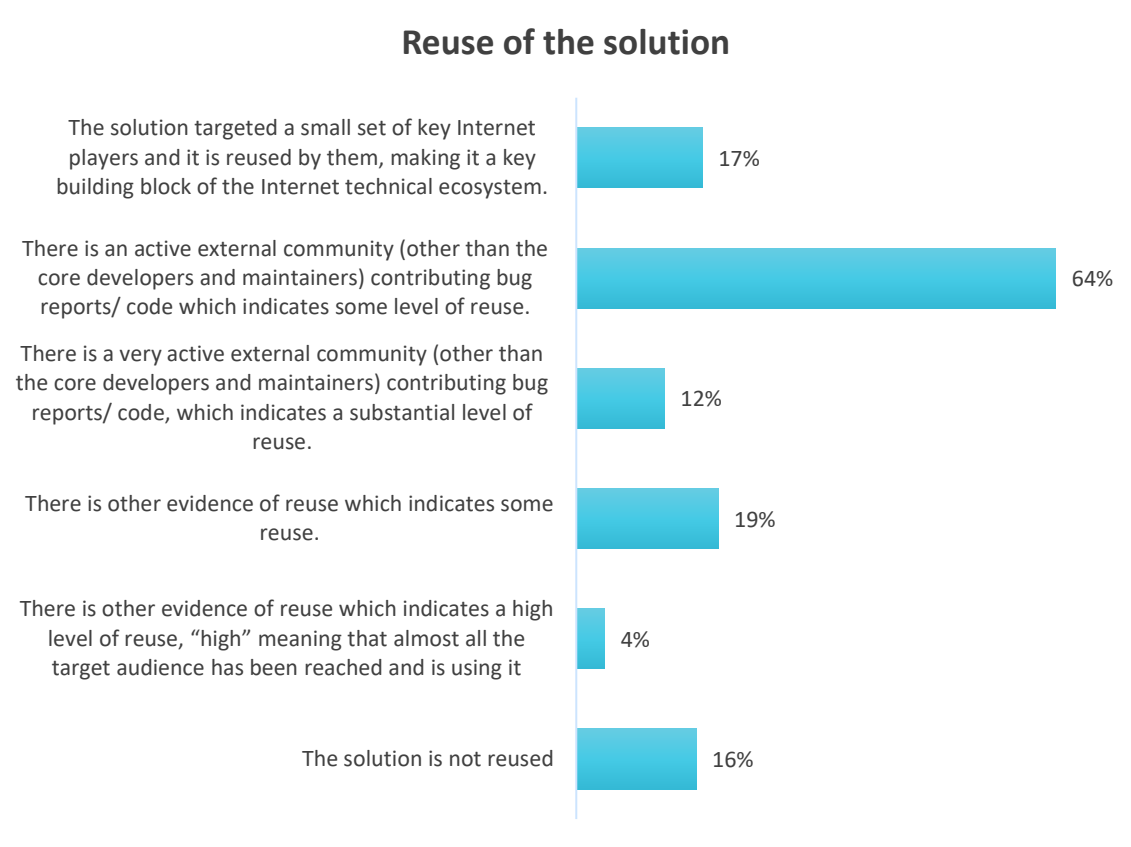
Evaluating the reuse of FOSS solutions through proxy insights on external community (other than the core developpers and maintainers) activity can be a valuable approach. This is important as free and FOSS software is often downloaded without tracking the users over time. A high level of community engagement with active participation in reporting bugs and contributing code suggests a substantial level of reuse because this indicates that the solution is being used by external users who are actively involved in its development and improvement.

The survey outcomes, presented in the figure below, indicate 76% of the NGI projects have an active or very active external community. This suggests that there is a significant level of reuse happening, as the active community members are likely contributing bug reports and code.

In addition, the survey identified alternative methods of assessing reuse.

For 17% of the projects, while there may not be evidence of reuse based on an active community, the adoption of the project by key Internet players which were targeted demonstrates its value within the Internet technical ecosystem.

Figure 15 – Reuse of the Solution



Source: Author's own elaboration

The survey also specifically sought evidence of reuse beyond community activity. Out of the projects surveyed, 23% (19% + 4%) declared belonging to this category and provided examples of other evidence of reuse.

The following is a non-exhaustive list taken from the survey (other examples from the qualitive analysis are presented in section 4) that exemplifies this evidence:

- Evidence of uptake by end users
    - GNU Name System project developed standards that are reused by parties outside the projects' ecosystem, showing uptake visible through a press release[7].
    - Free Software Vulnerability Database, and the subsequently NGI funded projects contributed to solutions which have about 2M downloads per month.
    - The NGI-funded project Peertube aimed to create a decentralised streaming video platform. There is evidence of the reuse of the

[7] https://medium.com/@AraxCorp/arax-holdings-corp-takes-an-important-step-in-fintech-with-revolutionary-payment-protocol-9fb25048d78f

software to create a network of federated platforms, based on the statistics8 of Peertube instances: Over 200.000 users, over 1000 instances, 330 TB of video files and 85M views.

  - Monal is an XMPP instant messaging client for macOS and iOS. The user can use different apps and services, such as Monal, from a single but also multiple accounts. This serves a decentral and sovereign infrastructure and digital communication on the internet. Monal demonstrates 15000 installs through apple's app store in 2023.

- Evidence of re-use within their respective ecosystems
  - The Servo project develops a web rendering engine written in Rust, a programming language, and adaptable to desktop, mobile, and embedded applications. The project has produced popular Rust crates that are widely used within the Rust ecosystem. Rust crates are reusable packages or libraries in the Rust programming language ecosystem. They provide a modular approach to code organisation, encapsulating functionality that can be imported and used in Rust projects.
- Interest from outside the ecosystem
  - The Interpeer Project's purpose is to research and develop novel peer-to-peer technologies for open and distributed software architectures. It has received some interest in technologies from the Consultative Committee for Space Data Systems (CCSDS), but that is early stages yet. CCSDS is a multi-national forum for the development of communications & data systems standards for spaceflight.
- Presentation of projects at high visibility events which may trigger reuse
  - GNU Taler is a free software-based microtransaction and electronic payment system. Unlike most other decentralised payment systems, GNU Taler does not use a blockchain.The project was invited to present their project to central banks outside of Europe.
  - The freenet-routing project was described in an invited talk as one of four speakers in the SUMA e.V. congress 2022[9] to present its progress for privacy preserving communication online.
- Integration into existing systems and tools

[8] https://instances.joinpeertube.org/instances/stats?includeAll=true

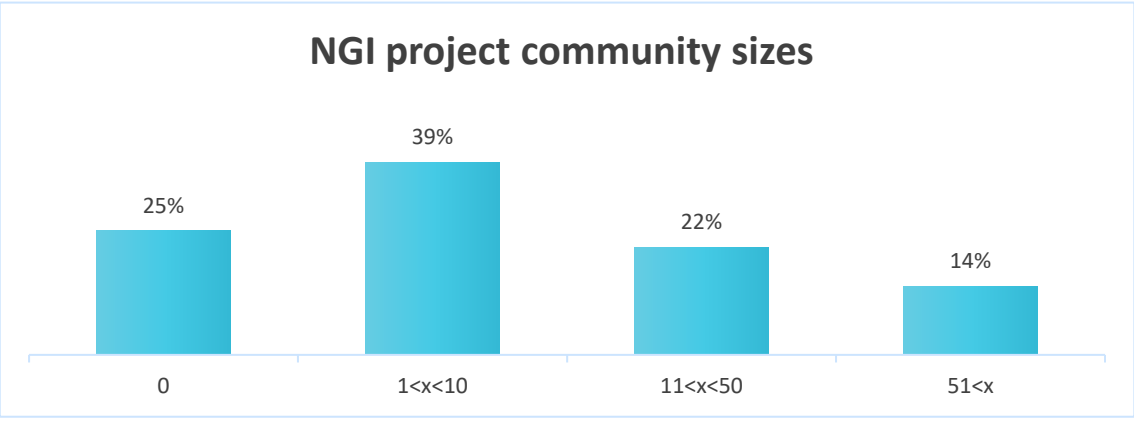
[9] https://suma-ev.de/suma-kongress-2022-videos/

- The URLFrontier project aims to develop a crawler-neutral API that facilitates communication between web crawlers and web frontiers. It seeks to provide a standardised set of operations for web crawlers, including retrieving the next URLs to crawl, updating information about processed URLs, adjusting crawl rates for specific hostnames, obtaining a list of active hosts, and accessing statistics. The URLFrontier is a key component in the Open Web Index, a basis of an open European infrastructure for internet search from the Openwebsearch.eu project.
- NoScript is a popular browser extension that allows users to control and customise the execution of JavaScript, Java, Flash, and other potentially harmful or intrusive web elements. By default, NoScript blocks all scripts on web pages, providing users with granular control over which scripts are allowed to run. The NGI project focused on the ABE-Quantum, the next generation of the Application Boundary Enforcer (ABE), a NoScript module that provided protection against several cross-site and cross-network attacks. NoScript is integrated into the Tor Browser, a web browser that prioritises privacy and anonymity by routing internet traffic through the Tor network. It is based on the Mozilla Firefox browser and includes additional privacy-enhancing features.

3.5.2. Community

The ongoing interactions, bug reports, and feature requests indicate that the projects are being actively used and improved upon, ensuring their continued relevance and usefulness. This sustainability criteria leverages the size of the community. It identifies the number of people in the community, apart from those funded by NGI, as shown in the figure below.

Figure 16 – NGI Project Community Sizes



Source: Author's own elaboration

The results of the survey highlight that

- 75% of projects have a community
- 40% of projects have a small community (<10 people) contributing
- Close to 15% of projects have a large community (over 50 people).

Additional insight from the survey shows that 6 projects are running with a community larger than 1000 people, e.g. Open Street Map or NixOS.

Based on the data points above and the survey response rate, it is estimated[10] that the funding of an NGI contributor impacts a community of 50 open source contributors, and that approximately 80,000 individualsactively contribute to NGI projects in software forges (gitlab, github…) for example through code, testing, and bug reporting, even without direct NGI funding.

This existing community is expected to persist and continue to contribute to the growth and development of NGI projects.

In conclusion, collaborating with the Free and Open Source Software (FOSS) community generates a multiplier effect. It not only draws in talented individuals but also fosters a collaborative and innovative ecosystem.

3.5.3. Project outcomes

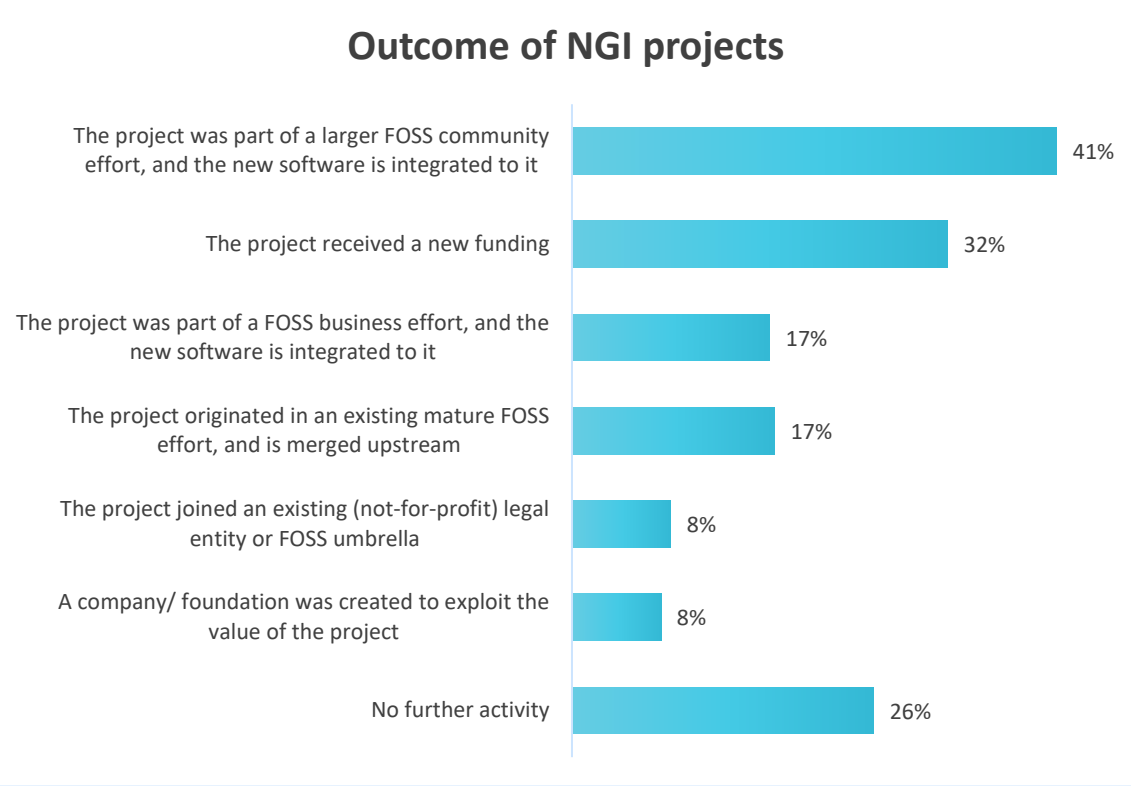
The sustainability criterion assesses the outcomes including in terms of viability of NGI projects after the conclusion of the funding period.

The project outcomes can vary, and according to the survey results depicted in the figure below, 74% of projects successfully follow through. Several key insights can be derived from the different data points:

First, with 26% of projects having no further activity once the funding ends, this shows that NGI funding adopts a 'fail fast' approach to innovation. However, since the projects are Free and Open Source Software (FOSS), the code is made available, enabling potential reuse when opportunities arise.

[10] Extrapolation from survey data: number of community members contributing to an NGI project (22808). See annex 2 for methodology details.

Figure 17 – Outcome of NGI Projects



Source: Author's own elaboration

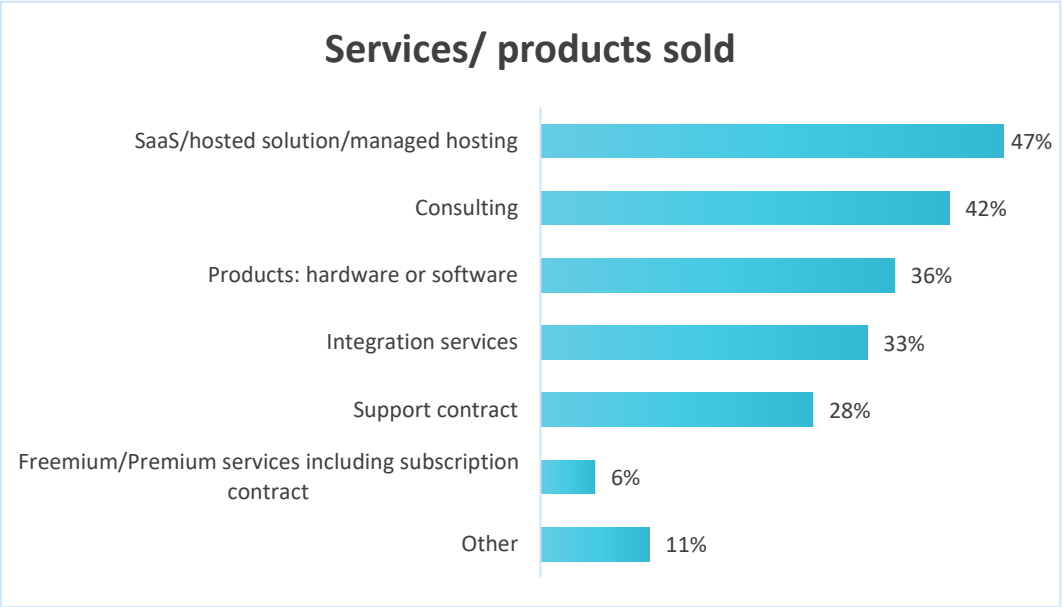
Second, the survey results also indicate that the outcomes of over half (58%) of the projects have been integrated into a wider FOSS business (17%) or community (41%) efforts. In addition, 17% of the projects originated from an existing mature FOSS effort and have been successfully merged upstream. This indicates that for 75% of the projects, the funding is utilised within existing FOSS initiatives, accelerating their development.

Third, the survey results reveal that 16% of the projects have either joined a legal entity or FOSS umbrella (8%) or established a company/foundation to exploit the value of the project (8%).

Considering this last data point and the survey response rate, it can be estimated that the NGI has facilitated the establishment of approximately 80 new sustainable legal structures.

For the companies that were created or existed when the NGI funded, the business models vary. According to the additional data provided in the figure below, it is interesting to note that half adopt a business model that involves providing Software-as-a-Service (SaaS), hosted solutions, or managed hosting.

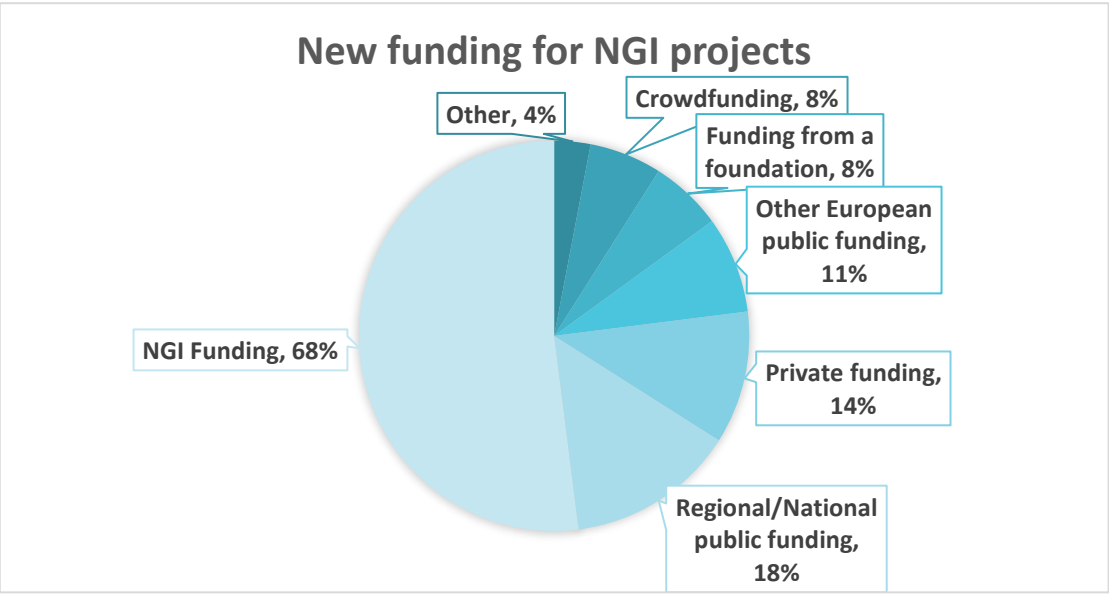
Figure 18 – Services or products Sold



Source: Author's own elaboration

Lastly, the survey results indicated that a third of projects (32%) received new funding, within or outside the NGI. Additional insight, provided in the figure below, shows where this funding comes from.

Figure 19 – New Funding for NGI Projects



Source: Author's own elaboration

Overall, additional funding is mostly fueld my public funds (97%) but projects are funded by multiple sources and private and crowdfunding contribute to 22% of new funding.

With 32% of projects receiving new funding and 68% of new funding being NGI we can estimate that 20% of projects got additional funding inside the NGI, demonstrating a sustainability of funding allowing projects to mature or to evolve before they can reach a self-support level.

3.6. Conclusion

Overall, the survey results on the outcomes of the NGI projects highlight the positive impact of the funding on EU society, EU policy, standardisation, choice, and sustainability. The effect of the NGI is also fostering innovation, interoperability, integration into existing initiatives, and the establishment of sustainable structures, ultimately contributing to the growth and development of the internet FOSS community.

4. Qualitative impact description per technology cluster

The qualitative analysis of the impact of NGI projects identifies a set clusters of technology which shape the digital landscape as building blocks of the Next Generation Internet. These technology clusters of digital commons are: open hardware, network and transport, Web 3.0 and cryptography, virtual worlds/Web 4.0, internet tools' evolution, decentralised social media, instant messaging, identity and digital signatures, collaborative tools, crowdsourced data and AI,and the software supply chain.

The NGI grants often provided in the early stages of the internet's digital commons projects serve as seed money that helps in their roadmap development towards core values such as privacy and inclusion. NGI grants have also funded some of the digital commons in later stages of their life cycle, contributing in various manners to improving the accessibility and adequacy of the solutions and therefore contributing to their reusability.

The qualitative analysis describes in this section approximately 100 impactful projects covering all clusters and how they are drivers for change, mainly in terms of usage and uptake but also how they drive standardisation initiatives. This analysis demonstrates the diversity of technology and standards' ecosystems stimulated within each cluster.

4.1. Open hardware

The open hardware movement is relatively new compared to FOSS but which similarly benefits from community developments that can achieve high level of complexity of hardware design despite relatively small funding. NGI is supporting this movement impacting the internet infrastructure by funding a significant number of open hardware efforts (approx. 10% of NGI projectsin various key areas notably tools for open hardware which are alternative to major proprietary Electronic Design Automation (EDA) providers.

NGI has helped projects collectively build an entirely open tool chain as well as manufacture a new chip entirely based on FOSS and open designs.

Open hardware is also relevant at chip design level: the close collaboration between NGI0 PET-hardware projects resulted in the fabrication of Libre-SOC's 180 nanometer Power ISA test ASI. This is "the world's first Power ISA implementation outside of IBM to go to silicon", paraphrasing the Open Power Foundation.

More specifically, NGI has funded projects at the level of Printed Circuit Boards (PCB) design, open chips and Field-programmable gate array (FPGA).

- PCB design

At the level of PCB design, NGI has funded several new Electronics Design Automation (EDA) solutions as well as improvements to existing FOSS tools.

This includes KiCad, a project that originally grew out of work done at the University of Grenoble. KiCad is a comprehensive open-source electronics design application suite, catering to the needs of professional electronics designers as well as newcomers to the field. This suite encompasses a wide range of essential tools, including schematic capture, printed circuit board (PCB) layout, circuit simulation, 3D viewer, and more. KiCad is compatible with multiple operating systems, including Windows, macOS, and Linux, ensuring accessibility to a broad user base.

> Some PCB factories report very high usage of **KiCad** across their customers, e.g. European PCB factory Aisler reported that 42.25% of designs that went into production in January 2024 were designed by their customers with KiCad, adding: "This shows how FOSS and free to use EDA's like KiCad lower the entry barrier for electrical designers and students".

Ringdove EDA is an advanced Electronics Design Automation (EDA) toolkit designed for the Printed Circuit Board (PCB) design workflow. It offers a modular and portable solution, with two flagship projects: sch-rnd for schematics capture and pcb-rnd for PCB editing. One of the key strengths of Ringdove is its modular code structure and efficient management of dependencies. This allows for high portability across different systems, including older, current, and future platforms. Additionally, Ringdove supports various workflows, including interactive graphical design, interactive command line usage, and headless automated processing. A notable feature of Ringdove is its capability to handle file formats from other EDA software. This includes the ability to load proprietary formats, thereby enhancing accessibility to existing or legacy hardware designs within the Open Source community. The primary focus of Ringdove is on programmability, providing users with extensive options for customisation and automation.

LibrePCB is another alternative PCB solution that provides developers with an alternative to the widely used PCB design suite from the German company Eagle, which was bought and is about to be closed down by its new owner.

- Open Chips

SpinalHDL is an independent Hardware Definition Language (HDL) that has gained recognition for its quality and capabilities. SpinalHDL has found adoption across the world in both commercial and academic settings, for a variety of projects like J1Sc Stack CPU, VexRiscv, NaxRiscv, SaxonSoc, open-rdma and MicroRV32 SoC as well as Network Attached Deep Learning Accelerators, VPN acceleration, and computer architecture research and education.

> SpinalHDL has been positively reviewed by a principal hardware engineer at Nvidia, noting its efficiency and configurability in his analysis of SpinalHDL.

VexRiscV is a high performance RISC-V processor which has become a reference architecture for third party embedded systems platforms like Zephyr

and companies like Antmicro. It is also part of commercial foundry offerings such as eFabless: every chip produced in their rapid prototyping service and the open shuttle service (funded by Google) is created with the Caravel management harness build on VexRiscV. VexRiscv was the first multi-core capable FPGA-optimised CPU on the extensive RISC-V cores list maintained by RISC-V International. Its successor NaxRISCV is gaining traction in , and is also currently used for independent academic research into for instance mitigations of security risks exposed in Intel and AMD chips.

VexRiscv is used in the German research project for "Hardening the value chain through FOSS EDA tools and Processors" (HEP, hep-alliance.org). There were follow up investments from that project into VexRiscv, extending features to the underlying SpinalHDL language and completing the formal proof of the VexRiscv chip design. The fact that VexRiscv technology has been employed in the creation of security chips speaks of the project's technical expertise.

- FPGA

UL3XM and ULX4M offer an affordable and open platform to work with field-programmable gate arrays, essential to embedded systems used for example in routers and mobile phones, but also in telecommunication infrastructure and medical devices.

It is already used in other NGI projects: the open hardware laptop Balthazar and the modular open hardware T&M (Test & Measurement) solution EEZ DIB.

NGI-funded projects include OpenXC7, kintex-nextpnr, and Apicula, which enhance the Yosys logic synthesis tool, benefiting the open-source FPGA ecosystem. Yosys is by now a well established tool and it is the most popular open-source logic synthesis software. Yosys was initially developed for FPGAs and it has become a viable alternative to proprietary toolchains, at least for the FPGAs which are so far supported. The reach of Yosys is growing steadily with NGI which funded projects to enhance Yosys/nextpnr and to support more FPGA types.

Quoting the NGI-funded project Apicula: "Only a few years ago, you could only program FPGAs with the proprietary tools provided by the vendors. But FOSS FPGA tools have been making great strides, and there are now mature FOSS synthesis and PnR tools, namely Yosys and Nextpnr."

Icestudio project provides a graphical interface for creating circuits and it lowers the entry barrier for FPGA/ASIC design. Looking at the popularity on Github we conclude that it already has a good userbase and it shows to be promising for educating the next generation of developers.

The benefits of open hardware include reducing costs and restrictive licensing agreements, thus increasing access to innovation. NGI funded projects aim to commoditise the hardware stack and promote reuse at the component level, enhancing trust and reducing lock-in. However, open hardware has not gained as much prominence as FOSS due to challenges such as scattered designs, difficulties in interconnection and reuse, and complexities in bringing designs to physical artifacts.

Other tools include Mosaic is a tool for designing and simulating analog integrated circuit designs, the first step of chip design. Luna develops a place and route tool, an essential stage in making chips and boards that can make or break their performance, sustainability and usefulness.

4.2. Network and Transport

While the internet is commonly known to rely on the Internet Protocol, its functioning involves a much wider range of technologies that ensure resilient connectivity over many different providers and guarantee a bitstream between two end-points. The evolution of these technologies is key to adapt to changing topologies, traffic behaviors or legal requirements.

The following NGI initiatives collectively contribute to the renovation and improvement of network and transport layers, addressing various aspects such as routing protocols, VPN security, transport efficiency, and network resilience.

- Routing

The selected project covers internet inter-domain routing that is vital to transmit information among providers both by improving existing technology (with 2 projects) and also with a new technology (SCION).

NGI programme funded 7 projects related to SCION, or Scalability, Control, and Isolation on Next-Generation Networks, a clean-slate routing architecture which offers a.o. multi-path and path-awareness capabilities by design. It brings several improvements to inter-domain routing, specifically BGP (Border Gateway Protocol). It enhances route control by organising Autonomous Systems into isolation domains, allowing for more precise control over routing policies. SCION also provides natural failure isolation, containing failures within individual domains to prevent widespread impact. Trust establishment is another benefit, as SCION's architecture enables explicit trust information, addressing trust-related issues like route hijacking. Additionally, SCION enables scalable routing updates with high path freshness, ensuring efficient and timely updates for optimal routing decisions.

The Secure Swiss Finance Network (SSFN) is one of the first communication networks to be built on SCION. SCION is considered so secure that the Swiss National Bank and SIX are building a network on it for the highly sensitive exchange of data between banks. SIX operates, develops and digitalises business and private payments for the Swiss financial center.

SCION is following a standardisation process at IETF.

SCION has established an active community of FOSS implementors with the goal to drive and facilitate the adoption of SCION. It serves as a reference implementation and a common basis for the SCION ecosystem. It is a vendor-

independent, low-barrier entry point to SCION, and can serve as an insurance or fallback for SCION adopters.

The PANAPI (Path Aware Networking Application Programming Interface Design and Implementation) project designs a sophisticated host-based network-path selection engine on top of the SCION network architecture, and provides it as an open-source implementation of the abstract next-generation transport service API currently being drafted in an IETF Working Group.

The outcome of the PANAPI project is as an open-source implementation of the abstract next-generation transport service API currently being drafted in the IETF TAPS Working Group.

The NGI funds the integration of Krill, an open-source RPKI (Resource Public Key Infrastructure) Certificate Authority, with BGP (Border Gateway Protocol). RPKI is a security framework that helps validate the ownership of IP address blocks and prevent the propagation of unauthorised or invalid routing information.

The Rotonda Secure Extensions project funded by NGI aims to implement BGPSec, a security extension for Border Gateway Protocol, in the Rust programming language and integrate it into the Rotonda modular routing project. Rotonda focuses on enhancing BGP observability and simplifying BGP provisioning in networks. Rust aims to significantly improve software reliability through memory safety guarantee.

- Virtual Private Network

Virtual Private Networks (VPNs) are used to extend access to a private network (one that disallows or restricts public access) to users who do not have direct access to it, such as an office network allowing secure access from off-site over the Internet. The benefits of a VPN include security and greater flexibility for remote workers.

WireGuard is a next-generation VPN protocol that simplifies secure tunneling using state-of-the-art cryptography. Unlike complex options like IPsec and OpenVPN, WireGuard focuses on implementation and usability simplicity. It utilises modern cryptography, including a 1-RTT handshake for perfect forward secrecy and identity hiding. WireGuard also employs a novel IP-binding cookie MAC mechanism to prevent common denial-of-service attacks. Key distribution is handled out-of-band with short Curve25519 points. With less than 4,000 lines of code, WireGuard is auditable and implemented within the Linux kernel for high performance. Overall, WireGuard is an open-source VPN utility that is simple, modern, and secure. The 8 NGI-funded projects continued the effort to make WireGuard land within the

Wireguard is originally designed and released for the Linux kernel, and it is now cross-platform (Windows, macOS, BSD, iOS, Android) and widely deployable. As of February 2024, 21 commercial VPN companies offer the WireGuard protocol as a connection option.

Linux kernel, upgrade some parts of the cryptography inside the Linux kernel, and do a comparative analysis of Wireguard protocol implementations on Windows, iOS and Android so quality and reliability can be assured across implementations.

Quantum computers pose a significant threat to modern cryptosystems, potentially breaking them within a few years. This jeopardises the security of all internet systems, including personal messages and banking. Even data transmitted today can be stored by espionage agencies and decrypted in the future. To address this risk, NGI-funded Rosenpass offers a solution that can be used alongside WireGuard. Rosenpass does not alter the encryption of WireGuard but provides an additional key that is resistant to quantum attacks, enhancing the security of the system.

- Mesh networking

NGI-funded Irdest is a networking research project focused on building sustainable and user-controlled communication networks. It utilises a dynamic mesh network where devices connect directly, creating a decentralised infrastructure. The project aims to make decentralised networking technology more accessible, allowing developers to create applications native to the mesh network without relying on central servers or internet access. At the core of the network is Ratman, a router application that enables seamless communication between devices using various connection types.

- Critical network infrastructure

Terrestrial Trunked Radio (TETRA) is a widely adopted European standard for trunked radio systems. It is utilised globally in various sectors, including European police agencies, military operations, emergency services, SCADA telecontrol for oil rigs, pipelines, transportation, as well as electric and water utilities and other critical infrastructure operators. TETRA employs authentication and encryption mechanisms to ensure secure communication. However, these are implemented using proprietary cryptographic cipher-suites known as TAA1 and TEA. These cipher-suites are only accessible to select parties under strict non-disclosure agreements (NDAs), which contradicts the principles of open technologies and Kerckhoffs's principle, which states that the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge. To address this issue, the NGI-funded Retetra project has been initiated with the objective of reverse-engineering and conducting cryptanalysis on the TAA1 and TEA cipher-suites. The ultimate goal is to develop a research-oriented implementation of these cipher-suites as free

and open-source software (FOSS), providing a pathway to transition from unexamined and proprietary security mechanisms to open standards.

The RETETRA project initiated a responsible disclosure procedure after discovering significant vulnerabilities in the TETRA standard, which could greatly impact public and critical infrastructure. In collaboration with the Netherlands National Cyber Security Center, a responsible disclosure trajectory was undertaken. This involved meetings with the international standards committee and representatives of the standards body, including TCCE, SC TSA and ETSI. The RETETRA team also organized meetings with international law enforcement agencies to inform them about the findings. They briefed representatives from over 10 different countries.

- Transport layer

The transport runs above the network layer and ensures a reliable stream of bit between two end-points (e.g. a client and a server).

NGI funded MPTCP (Multipath TCP,) a project for enhancing the performance and reliability of data transmission in 5G networks. MPTCP is an extension of the TCP transport protocol that enables the use of multiple physical paths in parallel. MPTCP allows for faster transfers, seamless transition between different network connections (e.g., WiFi to cellular), and potential prevention of traffic spying.

MPTCP was implemented in the linux kernel in March 2020. The MPTCP protocole is the object of an Internet Standards Track document at IETF.

4.3. Internet technology evolution

One of the areas of focus for the NGI is the evolution of key internet tools, which include the Domain Name System (DNS), web browsers, and email. These tools play a crucial role in the growth and adoption of the internet, and the NGI recognises the need to continue evolving and improving them impacting the user's need for privacy security, interoperability and propose alternative solutions.

- Domain Name System (DNS)

The GNU Name System (GNS) is a decentralised and secure naming system built on top of GNUnet, an alternative network stack for building secure, decentralised and privacy-preserving distributed applications. GNS addresses the limitations and vulnerabilities of the current Domain Name System (DNS), such as traffic amplification attacks, censorship,

GNS offers an alternative naming system that addresses the limitations and vulnerabilities of traditional DNS. It provides enhanced security, privacy, and censorship resistance while maintaining compatibility with the existing infrastructure. GNS has been published as RFC 9498 as an independent track RFC.

mass surveillance, and offensive cyber warfare. GNS enables users to securely resolve names to values, which can represent other users or network services. Users interact with GNS by typing in a hostname that ends in a top-level domain (TLD) that is configured in the “GNS” section, matches an identity of the user or ends in a Base32-encoded public key. Key features of GNS include censorship resistance, query privacy, secure name resolution, and compatibility with DNS. It allows users to register names as TLDs and resolve other namespaces within their TLDs. The NGI-funded project aimed to document the protocol on a bit-level (RFC-style) and create a second independent implementation against the specification. Furthermore, it aimed to simplify the installation by providing proper packages that, when installed, automatically integrate the GNS logic into the operating system.

DNSSEC (Domain Name System Security Extensions) plays a crucial role in ensuring the authenticity and integrity of DNS responses, providing trust in the DNS infrastructure. As DNS is a critical component of Internet communication, safeguarding its security is of paramount importance. DNSSEC not only enhances trust in the DNS but also enables other technologies that improve the security, privacy, and trust of Internet users. The DNSSEC Key Signing Suite project funded by NGI aims to develop a comprehensive set of tools, scripts, and guidelines, referred to as a playbook, to facilitate simplified key signing processes. This suite incorporates standardised ceremonies with automated checks and audits wherever possible. The impact of this initiative is twofold. Firstly, it will establish reliable, predictable, and verifiable key ceremonies, thereby enhancing trust in DNSSEC. Secondly, it will alleviate operational burdens, making validated and trustworthy signing procedures more accessible to a broader range of DNSSEC operators, including smaller or less financially viable top-level domain operators. This initiative will not only bolster trust in the DNS infrastructure but also enable a wider adoption of DNSSEC by making it more feasible and manageable for a diverse range of operators.

- Browser

JShelter, also known as JavaScript Restrictor, is a browser extension that aims to enhance user control over web browsers. It allows users to restrict the APIs provided by the browser, similar to how a firewall controls network traffic. By doing so, JShelter improves user control and privacy while browsing the web. The NGI funded project has several goals, including analysing fingerprinting scripts deployed on the web to enhance anti-fingerprinting techniques in JShelter. It also focuses on improving integration, functional and unit testing, as well as usability and documentation.

Jshelter is available in the Chrome webstore and as a Mozilla add-on.

Servo is a web rendering engine that was originally created by Mozilla Research in 2012. Components of Servo have been adopted by the Firefox web browser. It can be embedded in various applications and aims to be modular and independent. Servo is written in Rust, taking advantage of the language's memory safety and concurrency features. It provides robust support for WebGL and WebGPU, making it suitable for interactive and immersive applications. NGI funding supports integration with Tauri, support for floats and writing modes and tables which will increase the number of web pages and applications rendered properly in Servo. Tauri is a system for distributing cross-platform applications that relies on engines present on a system - effectively those owned by Apple, Google, and Microsoft. Servo is now cross-platform, with support for Windows, macOS, and Linux, and the team is actively working on adding Android support and exploring future ports to other platforms and embedded devices.

In 2020, the stewardship of Servo was transferred from Mozilla Research to the Linux Foundation. Since then, there has been renewed activity in the project led by Igalia, a spanish free and FOSS software SME. By joining the Linux Foundation Europe in September 2023, Servo aims to increase further its visibility within the European community and grow its market penetration. This move is expected to enhance funding opportunities and ensure the long-term sustainability of the project.

.

Wolvic is a web browser designed specifically for virtual reality (VR) and enhanced reality (XR). It aims to incorporate features like VR peripheral awareness and spatial reasoning to enhance the user experience. Wolvic is unique as it is the only open-source browser in the XR field, allowing device manufacturers and third parties to create their own versions and explore the growing XR space. See section on web4.0 and virtual worlds.

- email

Lightmeter aims to simplify the management of email servers, providing visualizations, monitoring, and notifications to improve performance and security. It enables individuals to regain control over sensitive communications by either running their own mail servers or relying on more diverse and trustworthy mail hosting services. By offering these capabilities, Lightmeter contributes to the overall goal of empowering users and enhancing the privacy and security of email communications.

Lightmeter is evaluated today at $3 to 5 million and it received $820k in seed funding in March 2022.

Email is also a very robust and reliable infrastructure that is used for decentralised instant messaging (see deltachat).

4.4. Web 3.0 and cryptography

Web 3.0 incorporates concepts such as decentralisation, tokenisation, transactional internet while cryptography coversa new web ecosystem requiring higher security standards. The NGI funds projects which drive next generation digital payments and usage of cryptography technology within this ecosystem.

The NGI TALER (Taxable Anonymous Libre Electronic Reserves) pilot, which began on December 1, 2023, aims to develop and deploy a free and open-source digital payment system. Based on the GNU TALER project, it focuses on providing an open and privacy-focused framework for electronic payments. A key feature of GNU TALER is that recipients are identified by payment service operators, while spenders can remain anonymous, ensuring privacy while preventing tax evasion, money laundering, and financing of terrorism. NGI TALER will work towards legally operating the GNU TALER payment system in Germany, Hungary, and Switzerland. It will integrate the exchange software with core banking systems, establish operational procedures, and make GNU TALER available through retail banks such as GLS in Germany and MAGNET Bank in Hungary.

The GNU TALER project is part of the GNU project, which was launched in 1983 by the Free Software Foundation (FSF) to develop a free and open-source Unix-like operating system. Since then, TALER has demonstrated the usability and scalability of the approach, with the latest version of the implementation code expected to exceed 50,000 transactions per second on a single system. Furthermore, TALER provides wallets available for Android and iOS, but also as browser plugins (Web Extensions). Some core-banking and e-commerce integrations exist as well, with more being developed under the NGI TALER pilot.

The NGI Taler project has benefited from a progression of funding, starting with small-scale initiatives, followed by upscaling, and ultimately piloting use cases with a substantial budget. The initial funding was small-scale, including NGI0-PET (1st seed), NGI-Assure, and NGI-Entrust, which focused on seed funding and roadmapping activities. This allowed the project to start its development and lay the groundwork. Afterwards, the project received additional funding for upscaling through NGI-Pointer, which provided a larger budget of 150,000 euros. Finally, the Taler project secured a significant budget of over 5 million euros to pilot various use cases. In the context of the pilot, the implementation of the GNU Taler payment system in Switzerland involves collaboration between Taler System (TSYS), a Swiss bank, a Self-Regulatory Organization (SRO), and the FINMA (Swiss regulatory body). TSYS will integrate GNU Taler with the core banking system of the Swiss bank and become a member of an SRO. This collaborative effort aims to facilitate the successful launch and operation of the GNU Taler payment system in Switzerland, ensuring compliance with regulatory requirements and fostering integration with domestic merchants.

In Switzerland, NGI TALER will launch GNU TALER under the "sandbox exception" and integrate it with a Swiss bank's core banking system, complying

with AML and KYC rules. The pilot will also integrate GNU TALER payments into the supply chain of book professionals and deploy additional features for selling or lending books online or in person. It will assess the accessibility, usability, and acceptance of TALER technologies, particularly for marginalized groups in the health sector, including elders, youth, and people with disabilities. Integration with the FLOSS development ecosystem through donations and pledges is also planned. Overall, NGI TALER aims to develop and deploy a privacy-focused digital payment system, integrate it with banking systems, expand its use in various sectors, and assess its accessibility and usability for marginalized groups.

The security of the Web ecosystem is heavily reliant on the Transport Layer Security (TLS) protocol. However, vulnerabilities and bugs in TLS implementations are still discovered regularly. To address this, Bertie is introduced as a high-assurance TLS 1.3 implementation written in a subset of Rust called hacspec. It utilizes the formally verified HACL* cryptographic library and allows for verification of its protocol code using the F* framework. This approach ensures strong guarantees from the cryptographic layer to the protocol API. The NGI funding aims to stabilize Bertie, enhance its documentation and testing, improve performance, maintain its proofs, and establish it as an open-source project adhering to best practices and long-term software support. This support will contribute to the development of a more secure and reliable TLS implementation, addressing the ongoing challenges in the TLS ecosystem.

The emergence of quantum computers poses a threat to the integrity and confidentiality provided by traditional public key cryptography. To address this, a new class of "post-quantum" or quantum-safe cryptographic algorithms (QSC) is being standardised by the National Institute of Standards and Technology. In order to facilitate the easy deployment of QSC, these algorithms need to be integrated into existing security installations. The NGI-funded project **oqs-provider** (open-quantum-safe) is a standalone integration of QSC into the OpenSSL software framework. OpenSSL is an open-source software library that provides cryptographic functions and protocols to secure communication over computer networks. It is widely used for implementing secure sockets layer (SSL) and transport layer security (TLS) protocols, which are essential for establishing secure connections between clients and servers on the internet. By adding the oqs-provider binary, any OpenSSL installation and applications built on top of OpenSSL that permit crypto-providers can automatically utilise any QSC algorithm supported by the liboqs open-source framework. The liboqs framework provides the QSC algorithms that are either finalists or candidates in the NIST Post-Quantum Cryptography standardisation competition.

KEMTLS is an alternative approach to the TLS (Transport Layer Security) handshake that utilises post-quantum

The Open Quantum Safe (OQS) project is part of the Linux Foundation's Post-Quantum Cryptography Alliance (PCQA), launched in February 2024. PCQA is a collaborative initiative to drive the advancement and adoption of post-quantum cryptography, bringing together industry leaders, researchers and developers.

Key Exchange Mechanisms (KEMs) instead of signatures for authentication during the handshake process. By incorporating post-quantum KEMs, KEMTLS aims to enhance the security and resilience of the TLS handshake against quantum attacks. The NGI project's objective is to prepare KEMTLS for standardisation by the Internet Engineering Task Force (IETF). To achieve this, the project implements KEMTLS in various open-source TLS software libraries. These implementations will demonstrate the viability and interoperability of KEMTLS. The software will serve as a reference for future implementers, enabling them to validate their own implementations against the project's reference. Additionally, the project will explore optimisations for using KEMTLS in specialised environments like the Internet of Things (IoT) and investigate certification issues related to KEM keys.

4.5. Web 4.0 and virtual worlds

Web 4.0 is expected to integrate digital and real objects and environments, as well as enhance interactions between humans and machines. The NGI funds projects that focus on preparing the ground for users' experience and privacy.

Wolvic is a web browser specifically designed for virtual reality (VR) and enhanced reality (XR) experiences. It allows users to immerse themselves in a virtual world while browsing the web. The NGI funding aims to enhance the Wolvic browser by adding important features such as VR peripheral awareness and spatial reasoning. VR peripheral awareness involves placing contextual information on the edge of the user's vision, while spatial reasoning provides a 3D representation of navigation-related information. Wolvic is unique in that it is the only open-source browser available in the XR space. This means that device manufacturers or other third parties can create their own versions of Wolvic to explore the growing XR field.

Igalia, a company expert in web engines, multimedia, graphics, and embedded systems had announced the launch of Wolvic in 2022, aiming to continue the work started by Firefox Reality. They aimed to build an ecosystem in the XR space. Wolvic entered stores in a beta phase as it transitioned features previously provided by Mozilla and addresses various issues. To access Wolvic, users can look for it in various app stores such as Huawei AppGallery, Oculus App store, and the Pico Store. Alternatively, users also have the option to download and build Wolvic themselves, allowing for customization and flexibility in its deployment. Users were and are still encouraged to contribute by filing any issues they encounter on the project's GitHub repository, helping shape the browser's development and ensure its success.

SearXR is a search platform designed specifically for virtual reality (VR), augmented reality (AR), and big screens. It aims to provide a more suitable and private search experience for alternative devices like VR headsets and conference presentations. The NGI funded project aims to enhance search interfaces by improving screen layout, privacy, and compatibility with WebXR

technology. It is built upon SearX and W3C's WebXR, allowing users to search or add XR features to their own SearX instance.

Manyfold is a web application project that focuses on managing collections of 3D models, particularly catering to the needs of the 3D printing community. It is designed to be self-hosted and enables users to browse, organise, and analyse their downloaded models. The NGI funded project aims to evolve into a decentralised multiuser platform for hosting and distributing 3D content. By utilising ActivityPub, Manyfold aims to create a decentralised alternative to platforms like Thingiverse, allowing users to run their own instances and subscribe to content on other servers. It also allows collaborators to release designs under their preferred license model and to control their designs. Additionally, the project aims to develop an open format for progressive transmission of 3D mesh data, enabling quick previews of remote models and low-quality previews for commercial content.

XR Fragments provides a small specification to treat 3D models as linkable AR/VR websites, which enables the discovery, referencing, navigation, and querying of 3D online content in an interoperable manner. It allows to address and control any 3D model or object with W3C Media Fragments and URI Templates. The goal is to overcome the limitations of current browsers that exit fullscreen or WebXR mode when switching web addresses, thus disrupting the immersive experience of navigating the 3D web.

4.6. Decentralised social media

The **Fediverse** is a decentralised network of interconnected social media platforms that use the **ActivityPub protocol** for communication and federation and offering interoperable alternatives to all major central social media. It is a federated social network where different instances or servers can communicate with each other, allowing users to interact across different platforms while maintaining control over their data. Trust in the Fediverse is not solely dependent on a centralised authority or single identity verification mechanism. Instead, it is built through a combination of decentralised governance, reputation systems, community moderation, transparency, and user control. In the Fediverse, identity is typically established through user accounts on individual instances or servers. Each user has a unique identifier associated with their account, which is used to authenticate and establish their identity within the network. The Fediverse operates on a federated model, where different instances or servers can communicate with each other. This allows users to follow and

ActivityPub has been added to the large blogging platform Wordpress.

Meta CEO announced testing making Threads posts available on Mastodon and other ActivityPub-supporting services, and explained that making Threads work with the interoperable standard “will give people more choice over how they interact and it will help content reach more people.”

interact with users on other instances. The federation model helps distribute trust across multiple servers and reduces reliance on a central authority. Reputation systems can be implemented within the Fediverse to help establish trust.

The W3C ActivityPub protocol enables the exchange of messages, posts, and other social media activities between different instances in a decentralissed manner. It allows users to follow and interact with users on other instances, similar to how email works - essentially providing a social link mechanism that allows to verify whether indeed some message originated with the person or organisation it is ascribed to.

NGI provided the seed funding for many of the leading projects, such as ActivityPods, Bonfire, Castopod, Flarum, ForgeFed, Funkwhale, GNU social, Hubzilla, Indigenous, Kbin, Keyoxide, Lemmy, Mastodon, Mobilizon, Owncast, PeerTube, PixelDroid, Pixelfed, Pleroma and Xwiki. NGI also funded bridging mechanism for various communication protocols, such as XMPP, Matrix.

Kbin is a decentralised content aggregator and microblogging platform running on the Fediverse network. It can communicate with many other ActivityPub services, including Mastodon, Lemmy, Pleroma, Peertube.

Mastodon is a decentralised social media platform that operates on the principles of the Fediverse. It is an open-source microblogging platform, an alternative to X former Twitter, that allows users to create accounts, post updates, follow other users, and engage in conversations. Mastodon instances are independently operated by individual users, user groups or organisations, and users can choose which instance to join based on their preferences or create their own instance. One of the key features of Mastodon is its federated nature. Instances can communicate with each other using the ActivityPub protocol, enabling users from different instances to interact and follow each other. This decentralised approach gives users more control over their data, privacy, and the ability to choose the community they want to be a part of. The European Commission uses Mastodon.

The fediverse has 3.2 M active users, 13M accounts and 19000 instances.

More specifically, Mastodon has 2.8M active users in the last 6 months, and there are 9500 mastodon instances.

The european Commission Mastodon instance - social.network.europa.eu - is run by the EDPS, and there are close to 30 Accounts . The cumulated number of subscribers (not counting subscription to multiple accounts) is just under 200000.

While it shares similarities with existing projects like Mastodon, **GoToSocial** specialises in catering to small-scale or individual users who operate on low-powered devices such as single-board computers or repurposed old laptops functioning as home servers. It is currently in its alpha software stage.

Lemmy is an alternative to a social media platform like Reddit, which operates as a link aggregation and discussion platform, allowing users to submit links, images, and text posts to various communities.

Pleroma is an extendable ActivityPub communication server that offers flexibility and customisation options for users. It can be lightweight and suitable for running

on a personal homeserver or scaled up for more extensive infrastructure. As part of the Fediverse, Pleroma facilitates interactions with other servers and provides a seamless experience for displaying various types of content, not limited to microblogging.

PeerTube is a decentralised video hosting platform that operates on the ActivityPub protocol. It provides an alternative to centralised video hosting platforms like YouTube, but allows content creators to retain control over their content. Users can host their own instances or join existing ones to create communities and share videos. One of the key features of PeerTube is its federation capability. This means that instances can communicate and share videos with each other, allowing users to discover and watch videos from different instances within the PeerTube network. This decentralisation helps distribute the hosting and bandwidth load, making PeerTube more scalable and resilient. A PeerTube instance (tube.social.europa.eu) piloted by EDPS is available for EU institutions.

The **Fediverse Test Suite** project is an initiative aimed at promoting interoperability within the W3C ActivityPub framework by establishing an automated test framework and developing test cases.

Spritely is a project developing the next generation of Fediverse platforms by adding richer communication and privacy/security features to the network. The NGI project showcases a chat interface that integrates a contact list. This approach helps enhance security by reducing phishing risks, facilitating the discovery of other users, and eliminating the need for a centralised naming authority. NGI funding allowed to document OCapN's (Object Capability Network) functionality as a set of specifications so that OCapN's technology can be incorporated into any programming language environment. OCapN is a new protocol to add support for secure, seamless, and distributed (often peer-to-peer) communication for networked applications. It is currently the focus of a group working on prestandardisation. The Spritely project is now at the core of a newly founded non-profit, the Spritely Institute.

Scuttlebut (SSB) is an edge computing, peer-to-peer communications protocol. It is currently developed by an established global community with a variety of implementations, the most wide-spread implementation currently being the main network of ~20,000 nodes. Its unique network architecture in which data flows opportunistically between nodes and along paths of trust relationships between humans, it is due to this the protocol is called “the gossip protocol”. The organisational structure behind Scuttlebutt is distributed over several projects globally. This approach of social media is complementary and different from Activity Pub.

4.7. Instant messaging

NGI funded a noticeable part of the transition of messaging to End-to-End Encrypted protocols, particularly in the realm of XMPP (Extensible Messaging and Presence Protocol), which is an internet standard for real-time communications. NGI's support has enhanced the implementation of end-to-end encryption in XMPP, with various clients such as Conversations, Dino, Movim and Kaidan incorporating support for modern cryptography, specifically OMEMO (Multi-End Message and Object Encryption), an XMPP Extension Protocol (XEP) for secure multi-client end-to-end encryption. This advancement has brought privacy to end users and positioned XMPP on par with some proprietary messaging offerings.

There is active tracking of interoperability and support for end-to-end encryption across the XMPP ecosystem. The website "Are we OMEMO yet", which monitors the progress of OMEMO implementation in different XMPP clients and servers, refers to these NGI projects as fully compliant.

Meanwhile, in the standards community, there has been a convergence towards group message encryption. Initial support for end-to-end encryption in messaging tools has paved the way for the evolution and development of new standards.

The NGI funded openMLS infrastructure project, which aims to design and implement infrastructure components for the Messaging Layer Security (MLS) protocol, is currently under development by the Internet Engineering Task Force (https://datatracker.ietf.org/doc/draft-ietf-mls-protocol/). While it is possible to run MLS peer-to-peer, many use cases require central components to manage message ordering, queueing, and group state. The goal of the project is to create secure, metadata-minimising, modular components that allow for federation. This will lay the foundation for improving existing and future messaging applications and validating potential future application-layer specifications.

Several messaging tools have embraced these evolving standards to enhance their security features. DeltaChat and DeltaBot are examples of projects that have integrated group message encryption into their platforms. Both use email as the underlying infrastructure which proves to be very reliable even in areas with restriction on internet access. The NGI funded project WebXDC/Deltachat aims to further develop the concept of WebXDC apps, including making data portable with enhanced security controls. WebXDC, an evolving effort, explores the concept of "private apps" that are portable web apps enabling users to interact outside the traditional client-server paradigm, such as over end-to-end encrypted (E2EE) chat. These mini-apps offer interesting interaction patterns without the need for centralised infrastructure or additional logins. WebXDC grew from Delta Chat, an innovative solution that utilises secure email-based communication technology protected with OpenPGP/Autocrypt. The NGI funded DeltaBot project focuses on researching and developing decentralised, E2EE-encrypting, and

socially trustworthy bots for Delta Chat. These bots bridge messaging platforms like IRC and Matrix, provide media archiving, and integrate with ActivityPub and RSS/Atom to enable users to discover new content. The project aims to provide well-tested and documented chat bots in Python, as well as assist others in writing and deploying their own custom bots.

MonalIM and Movim have also implemented these standards to ensure secure communication for their users. Monal IM is an open-source instant messaging client designed for iOS and macOS operating systems. The Monal IM project focuses on enhancing its chat interface by implementing end-to-end encryption. Movim is a web platform that delivers social and IM features on top of the mature XMPP standard. Mellium aims to create an easy to use implementation of the OMEMO encryption standard (XEP-0384: OMEMO Encryption) that is compatible with popular instant messaging clients.

Additionally, Libervia, which offers several interfaces (web, desktop, mobile, command line, text UI), explores the XMPP protocol beyond instant messaging for its offering which includes blogging and file sharing.

4.8. Collaborative tools

CryptPad provides an office suite with a number of collaborative tools for team productivity: a text editor, spreadsheets, slides, shared whiteboard, online forms and task planning/Kanban. Its end-to-end protection of user privacy - by design the server is unable to read anything users write - is key to its use by many organisations for privacy preserving purposes. CryptPad Blueprints is NGI funded and aims to provide a guide for users on how to use CryptPad in the most secure way; provide experimental prototypes and/or mockups for future features such as Offline first editing with Conflict Free Replicated Data Types (CRDTs), perfect forward secrecy for a more fine-grained degree of access control e.g., to the document history and account-recovery mechanism making use of social secret sharing. A conflict-free replicated data type (CRDT) is a data structure that allows for independent and concurrent updates to replicas in a network without coordination. CRDTs include algorithms that automatically resolve inconsistencies, ensuring eventual convergence.

openDesk (ex-Sovereign Workplace) is the German governmental project that works towards a digital sovereignty future. It's led by the Federal Ministry of the Interior, Building and Community and is commissioned by the IT Council. The funding from this project was used to deliver a new Diagram application based on draw.io, a NextCloud integration, and the team also did a lot of work on security and accessibility issues. OpenDesk reuses components from communities that received NGI funds e.g. Xwiki, NextCloud, Matrix or Collabora.

CryptPad AUTH is an NGI funded project aiming to bring more security to CryptPad through support for external authentication methods. Thus, the CryptPad team worked and delivered 2-Factor Authentication (2FA), available since the 5.4.0 release, and Single-Sign-On Authentication (SSO), available as a plugin.

Interpeer Project, funded by NGI, focuses on CRDTs like Wyrd as part of their work on novel peer-to-peer technologies for open and distributed software architectures. Their goal is to enable serverless modes of operation for collaborative software with rich feature sets comparable to centralised client-server architectures. The project aims to facilitate low-latency and high-bandwidth use cases, such as peer-to-peer video communications with high-quality resolutions like 4k. By leveraging CRDTs, the Interpeer Project aims to advance the capabilities of decentralised and collaborative software.

The Interpeer project received significant follow up funding (120 kEUR) from Internet Society Foundation as part of their mission to enable new research on the future of the Internet.

4.9. Crowdsourced data and AI

The NGI funds projects that support the crowdsourcing of data and AI infrastructures which are key in adhering to EU values.

- Location data

Location awareness plays a crucial role in delivering relevant services and empowering communities by providing information on what is nearby and accessible. However, location data is not only privacy-sensitive but also culturally specific. To address these challenges, **OpenStreetMap**, a collaborative public geographic open data set, serves as an important data commons that enables users to reuse geographic knowledge and contribute to it. The funding capabilities of NGI supported many initiatives in this space which not only helped to expand and improve OpenStreetMap itself, but also funded applications and tools to consume such data either directly through user-friendly applications (organic maps) or through a library (nominatim-lib) , perform quality assurance (streetcomplete together) , to create custom data sets (umap), improve resilience

and privacy by allow self-host the data sets (protomaps), query (nominatim) the data set, and making the map usable in different environments and for every use case (map complete). The funding from NGI helped improve security and robustness of key parts of the infrastructure, including finding and fixing a security flaw within the main address search algorithm of openstreetmap.org (Nominatim) but also significantly improving coverage benchmarking of address queries. A key differentiator is also the ability for anyone to produce maps in local (minority) languages, marking cultural and historical landmarks important to for instances specific communities. This makes OpenStreetMap also a key part of any policy aimed at promoting diversity, historical awareness and cultural richness.

From a resilience perspective, the OpenStreetMap ecosystem stands out as a user-powered, self-hostable maps (digital sovereign) which can be used offline and synchronised peer-to-peer, tailored to every use case (including temporal maps, historical maps, etc), and as a result can be used without privacy or confidentiality leakage. This is important because known users of this data include the International Federation of Red Cross and Red Crescent Societies (IFRC), Médecins Sans Frontières/Doctors Without Borders, Pan American Development Foundation, United Nations and the World Bank. Note that OpenStreetMap data is also actively used by many of the largest consumers of map data, including hyperscalers like Meta, Baidu and Apple, as well as public sector and government agencies from around the world.

The NGI funded Organic Maps is one of the largest and fastest growing FOSS applications in app stores, breaching the one million users in 2023. This achievement is noteworthy considering that it requires active installation and replaces a pre-installed alternative from a large market player like Google Maps.

In addition to OpenStreetMap there are additional geographic information efforts supported by NGI Zero such as Geolexica which is a product of ISO/TC 211 Geographic information/Geomatics, working on standardisation in the field of digital geographic information. The official portal of ISO/TC 211 features the semantic search funded through NGI Zero, allowing people to find terms in the Multi-Lingual Glossary of Terms by using natural language.

- Artificial intelligence

One of the big challenges with Generative AI is the amount of resources required to run even simple models. The NGI Zero-funded AI Horde addresses this by providing access to AI models and resources to a wider audience. It operates as a crowdsourced virtual cluster, utilising a dynamic set of AI models to generate images and text. By contributing their hardware resources, individuals collectively form a public service, enabling people without expensive hardware to use modern AI models on a best-effort basis.

One of the key advantages of AI Horde as a crowdsourced infrastructure is its role as a hub for discovering new AI models and styles. This allows new entrants to easily reach a broader audience without much effort, while users can interact

with various open-source AI models through a single unified interface. Moreover, AI Horde has convenient integrations with ActivityPub tools like Mastodon and Lemmy, enabling automatic generation of images by inviting the AI Horde to contribute via a remote prompt. This makes AI Horde a comprehensive platform for accessing new algorithms and services in the field of Generative AI.

After the emergence of Chat GPT, the NGI programme has decided to open the calls to generative AI resulting in projects such as AI Horde within a few months, demonstrating the flexibility and reactiveness of the NGI programme.

- Data sets

In 2023, the European Commission introduced the Digital Services Terms and Conditions Database, a consumer-facing portal. This database is built upon the code and data of the NGI Zero-funded project called Open Terms Archive, a digital common that produces (since 2020) datasets of the evolution of contractual documents (Terms of Service, Privacy Policy…) over time, enabling analysis and comparison. Open Terms Archive is a decentralised and federated ecosystem, meaning that anyone can start tracking documents on their own and make them available to others, no matter the target domain. All public collections and tracked documents that match federation quality criteria are counted in the ecosystem size. Data in this repository is distributed under an ODC-BY 1.0 license. That means you are free to share (to copy, distribute and use the database), to create (to produce works from the database), to adapt (to modify, transform and build upon the database) as long as you attribute the resulting works to Open Terms Archive contributors.

By automatically indexing the contracts, the database offers insights into the digital agreements. The database now encompasses 790 terms and conditions from more than 400 services provided by over 290 distinct service providers. By adopting this FOSS tool, the EC was able to reach its own legislative goals in a short period of time.This is an example of the effectiveness of utilising NGI-funded projects to meet policy goals.

The database leverages obligations for digital services to make their contracts available in an easily accessible and machine-readable format (cf. Article 14 of Regulation 2022/2065) and obligations of online platforms, including social media, app stores and market places, to publish clear and complete contracts both for professional users (cf. Article 3 of Regulation 2019/1150) as well as for end users (cf. Article 14 Regulation 2022/2065).

4.10. Digital identity and signatures

Digital identity and digital signatures are a large focus of the NGI Funding, for example:

- TRUSTCHAIN started in January 2023 and will end in December 2025. The 10M project will distribute to sub-grantees around 8,8 M within five Open Calls on topics pertaining decentralised digital identity solutions, user privacy and data governance, and green scalable and sustainable DLTs (Distributed Ledger Technologies).
- As regards the NGI eSSIF-Lab, the 36-month project of almost 7M budget started in November 2019 and ended in December 2022. The project delivered 58 implementations of digital identity components, products, and services.

In the context of eSSIF-Lab, a number of contributions were made to standards, specifications and associated interoperability testing on verifiable credentials and decentralised identifiers like the W3C, the Decentralised Identity Foundation and the European Blockchain Services Infrastructure (EBSI), a network of distributed blockchain nodes across Europe. By the end of the project, more than 7 EBSI compliant digital wallets were delivered, while several of the eSSIf-Lab subgrantees participated in the early adopter's programme or other EBSI-related actions (for example Gataca, Danube tech, WaltID, iGrant.io, Validated ID). Gataca is part of the EUDI Wallet Large Scale Pilots. iGrant io, Validated ID and SICPA are also partners of the EUDI pilots.

Transatlantic SSI Interop demonstrated the interoperability of experimental decentralised identity infrastructures in the US and EU. On the US side, partner Digital Bazaar set up the infrastructure for issuing digital Permanent Resident Cards, as envisioned by the US Department of Homeland Security's (DHS) Silicon Valley Innovation Program (SVIP). In the EU, Danube Tech issued digital diplomas using the pre-production European Blockchain Service Infrastructure (EBSI). In terms of impact, the project demonstrated how the US- and EU-issued digital identity credentials can be exchanged between the two sides.

NGI and Innovation, Science and Economic Development Canada (ISED) jointly led this series of workshops held from spring to summer 2021 to discuss interoperability and mutual support of digital credentials. One of the key findings of the workshops was that Canada and the EU already use a variety of Self-Sovereign Identity (SSI) and digital credential technologies, many of which are not interoperable with each other. In addition, different technologies and approaches to SSI and digital credentials are emerging in different economic sectors and at different levels of government, creating a risk of economic and jurisdictional technological silos.

Specific contributions of NGI-funded projects related to a diverse range of standards and technology ecosystems are highlighted below.

- FIDO[11]2 and W3C

[11] Fast Identity Online (FIDO)

The FIDO2 Project is a joint effort between the FIDO Alliance and the World Wide Web Consortium (W3C) whose goal is to create strong authentication for the web. At its core, FIDO2 consists of the W3C Web Authentication (WebAuthn) standard and the FIDO Client to Authenticator Protocol 2 (CTAP2).

Nitrokey is a USB key that provides data encryption and two-factor authentication with Fast Identity Online (FIDO) protocol, a technical specification for online user identity authentication. The free software and open hardware enables independent parties to verify the security of the device. While email encryption in webmail is not possible with Nitrokey, the NGI funded project aims to enable its use with web applications by leveraging the FIDO protocol. This eliminates the need for device drivers, browser add-ons, or separate software, making it compatible with any modern browser that supports WebAuthn. NGI-funded projects also focused on enhancing Nitrokey's capabilities by expanding its firmware to support additional secure elements in Trussed and developing PIV support for Nitrokey 3. This will enhance security and convenience for users, making Nitrokey a comprehensive open hardware security key.

Several major FOSS projects allow their developers to use Nitrokey devices to secure their software supply chain. For example, the Linux Foundation provides free Nitrokeys to developers of the official Linux kernel. Likewise, the Linux distributions Gentoo and Arch provide their developers with free Nitrokeys. Nitrokeys are used in particular for SSH access to git and package servers, for the signature of the source code and for the software signature. By preventing malicious code from being injected into the software, they effectively protect against software supply chain attacks.

- OpenPGP

Several Nitrokey models exist which each support different standards. **OpenPGP** can be used to encrypt emails and also certificates used to login to servers with OpenVPN or OpenSSH.
OpenPGP is a widely used email encryption standard (defined by the Internet Engineering Task Force in RFC 4880). Implementations of OpenPGP are used for a wide range of purposes, to sign, encrypt and decrypt texts, emails, files, directories and disks. OpenPGP-compatible systems also allow users to create their own 'web of trust', where people accumulate and sign each others' keys for trusted communication without a central point of authority. NGI has funded thirteen projects related to PGP.

Gpg4win (GNU Privacy Guard for Windows) is a cryptography tool package originally commissioned by the German Federal Office for Information Security (BSI) for encrypting and signing in Windows, including in MS Outlook and Windows Explorer and reuses OpenPGP.

- Decentralised identifiers (DIDs)

Decentralised identifiers (DIDs) are a type of identifier that enables verifiable, decentralised digital identity. A DID refers to any subject (e.g., a person, organisation, thing, data model, abstract entity, etc.) as determined by the

controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralised registries, identity providers, and certificate authorities. NGI has funded the Universal DID Resolver and Registrar projects which are open-source software components that implement DIDs and that are developed and maintained in collaboration with relevant community and industry stakeholders, including the Decentralized Identity Foundation, uPort, Jolocom, Sovrin, Civic, Veres One, Blockstack, ERC725 Alliance, and more. They are aligned with the corresponding W3C community group specification efforts, ensuring compatibility and interoperability. DidRoom is an open-source multiplatform and multifunctional Identity DID/SSI wallet, based on the NGI-funded work in Signroom, which is compliant with the **W3C-DID**, **W3C-VC** standards and **eIDAS 2.0** (based on the EUDI-Architecture Reference Framework specifications). The software allows to embed valid signing code into every web application, and it is easy programmable (even for non-experts) through a no-code English-like language.

- Attribute Based Credentials (ABC)

Attribute Based Credentials (ABC) are a form of authentication mechanism that allows to flexibly and selectively authenticate different attributes about an entity without revealing additional information about the entity (zero-knowledge property). The identity management solution funded by NGI Yivi/IRMA provides a privacy-preserving alternative to identity management that works with selective disclosure. The attribute based system can be used to provide strong proof of the authenticy of certain data or meeting certain eligibility criteria (e.g. place of birth, age, business registration, biometric details), without having to reveal any other data. It can also be used for identity based encryption, to send end-to-end encrypted messages to people that have not previously set up a secure encrypted channel. The NGI project focused on making IRMA easy to use for everyone, conducting a formal large-scale evaluation of IRMA that focuses on usability in general as well as on accessibility (i.e. for users with disabilities) in particular.

The Dutch parliament has recently passed the Digital Government Act, laying down general rules to make sure that people can securely access electronic public and semi-public services, and share personal data with confidence. Read more about the Digital Government Act and Yivi, and IRMA as precursor EU-wallet-ID. Yivi FOSS solution is used in production by the Dutch public sector, the national Chamber of Commerce, various commercial identity providers, various health care providers and insurance companies.

The European Commission is currently running several pilots with identity wallets, involving Yivi/Irma.

- Password protection

Passwords are commonly used for remote access to private services, but they pose a significant security risk as humans struggle to remember strong passwords. There are evolving tools to work with passwords more securely. The SPHINX approach provides information-theoretically secure password storage, eliminating the need for users to trust the server. The OPAQUE protocol

(proposed to IETF standardisation) helps eliminate phishing attacks during server authentication. Combining SPHINX and OPAQUE offers strong guarantees while allowing users to remember only one or a few passwords. The NGI project aims to develop a secure SPHINX server and refine a protocol for data management. It also plans to integrate the OPAQUE protocol into various free software ecosystems and popular webservers.

4.11. Software supply chain

- Reproducible builds and bootstrappability

NGI funds projects focusing on securing the software supply chain through two key advancements: reproducible builds and bootstrappability. Reproducibility ensures that the output of the supply chain remains consistent when given the same inputs, providing developers with confidence in the reliability of the software. Bootstrappability focuses on making the inputs from the supply chain transparent and human-readable, eliminating black boxes that could introduce vulnerabilities.

NGI funds the 3 million euro programme Fediversity, a hosting provider/cloud platform in-a-box based on NixOS. Because NixOS is reproducible, it is suited for complex deployment scenarios where consistent behaviour, stability and configurability matter, such as running state-of-the-art services for the Fediverse.

NGI has provided support to cross-platform package managers like Nix and Guix. The GNU Mes project, with NGI's support, became the first publicly available software project to achieve a near full source bootstrap, reducing the size of binary code from 130 MB to just 357 bytes of assembly. Achieving a full source bootstrap allows code portability across different computer architectures. These efforts in porting GNU Mes and Guix to various CPU architectures have played a significant role in making alternative architectures like RISC-V and OpenPower market-ready. Additionally, NGI's support for Nix's embedded implementations, Mobile NixOS and Liminix, has enabled declarative packaging on mobile phones and MIPS systems commonly found in home routers and other Customer Premise Equipment.

- Auditability, predictability, and resilience

NGI has also focused on improving the auditability, predictability, and resilience of the software supply chain. Efforts have been made to automatically generate a Software Bill of Materials from Nix packages (Genealogos), automatically packaging entire language ecosystems (Dream2nix), and creating a memory safe re-implementation of Nix (Tvix). NixOS-UEFI combines the power of the reproducible package manager Nix with the cryptographic protections of UEFI Secure Boot to provide concrete assurances about the authenticity of the software being booted into.

NGI has also ensured the long-term availability of source code by supporting the ingestion of software ecosystems into the UNESCO-sanctioned Software Heritage and establishing a direct pipeline between Nix and Guix packaged software into Software Heritage.

Software forges are essential components of the software supply chain as they provide the necessary infrastructure for publishing code and enabling collaboration among developers. In many cases, teams rely solely on these forges and lack other infrastructure, including identity management solutions beyond the login to third-party platforms. This heavy reliance on external platforms poses security and privacy risks. Therefore, it is crucial to have fallback options in case these dependencies fail, ensuring resilience in the software development process. NGI has supported the development of free and open-source alternatives to providers like GitHub. Tools such as Sourcehut, Pagure, and Forgejo offer lightweight self-hostable options for publishing code and collaborating on software projects. NGI has also funded the ForgeFed project, which enables collaboration between software developers across different platforms through the use of the ForgeFed protocol based on ActivityPub. Tools like Forgejo and Pagure are using ForgeFed to enable software forges to federate, allowing members of any such forge to seamlessly contribute to projects hosted on other web locations.

- Software Composition Analysis

NGI funds projects in the area of software composition analysis, including VulnerableCode, ScanCode, and Package-URL, that build FOSS used for ensuring software supply chain integrity and security.

  - Free and open database of FOSS package vulnerabilities

Discovering and remediating vulnerabilities is a critical aspect of software supply chain security, especially with the widespread usage of Free and Open Source Software (FOSS). However, organisations face challenges in efficiently identifying vulnerabilities in FOSS components that form the foundation of their software systems. These challenges arise from proprietary data structures and tools primarily designed for proprietary software, over-reliance on single sources like the US National Vulnerability Database, and low-quality data with numerous false positives.

To address these challenges, NGI has provided funding for the development of **VulnerableCode**, a free and open database of FOSS package vulnerabilities. NGI has also supported the expansion of VulnerableCode's functionality through the development of related utilities and integrations. VulnerableCode aggregates, correlates, and curates vulnerability data from multiple sources, automating the search for security vulnerabilities in FOSS components.

The NGI-funded FederatedCode software metadata project is a decentralised system for FOSS metadata to generate data of FOSS packages' origin, license,

and vulnerabilities to support software supply chain integrity that extends the reach and ease of access for VulnerableCode data and PURL data (see below).

- Standardised software package identification

Package-URL, or PURL (Package Uniform Resource Locators) standardises existing approaches to reliably identify and locate software packages in a mostly universal and uniform way across programming languages, package managers, packaging conventions, tools, APIs and databases. PURL was originally developed for use in NGI-funded open source Software Composition Analysis (SCA) tools ScanCode and VulnerableCode, and additional support from NGI extended PURL's functionality and interoperability.

PURL is the de-facto standard for vulnerability management with package references by software bill of material (SBOM) and Vulnerability Exploitability eXchange (VEX) specifications like CycloneDX, SPDX, OpenVEX, and Linux Foundation OSSF OSV Schema (open source vulnerabilities), which in turn are actively used by most open source projects and commercial products that need to identify software packages and vulnerabilities. CASF, the Common Security Advisory Framework, is a standard co-developed by the German Federal Office for Information Security which also references PURL.

”39% of organizations would like to see support for globally unique identifiers. Globally unique identifiers is a work in process supported by the leading data formats for package URLs (PURLs)”. The State of Software Bill of Materials (SBOM) and Cybersecurity Readiness The Linux Foundation report.

“Package URLs (purl) is a promising Defined Identifier.” The Minimum Elements For a Software Bill of Materials (SBOM) Pursuant to Executive Order 14028 on Improving the Nation’s Cybersecurity

“New recommendations drafted by members of OWASP, The Linux Foundation, Oracle, and others, aim to improve the accuracy of the National Vulnerability Database (NVD) with a focus on modern, automated use cases. Their first paper titled A Proposal to Operationalize Component Identification for Vulnerability Management. recommends that MITRE and the NVD adopt Package URL for the identification of open source and commercial software along with multiple GS1 standards for hardware. In doing so, the accuracy of vulnerability management can be dramatically improved while increasing the efficiency and effectiveness of the teams doing it. New Recommendations to Improve The National Vulnerability Database OWAPS The Open Worldwide Application Security Project

- Code scanning engine

ScanCode is a code scanning engine, used worldwide to identify any open source components, their dependencies and their license compliance data in an application codebase. Support from NGI extended the functionality of ScanCode to include support for Package-URL (PURL)-driven services and databases such as collecting extended software package metadata, performing on-demand dependency resolution, and integrating with VulnerableCode. ScanCode also identifies and verifies the integrity of deployed code packages and validates their origin to mitigate attacks through software dependencies and code injection in binary builds.

The NGI-Funded back2source ScanCode and PURL projects use a "trust but verify" approach to ensure that binaries of a FOSS package match its source code - any discrepancy could be malware or a vector for unknown software vulnerabilities.

P.Ombredanne, AboutCode Europe president and lead maintainer of ScanCode and AboutCode open source projects reported:

"NGI-Funded AboutCode open source tools are now used throughout the industry to support open source program offices, and software supply chain security worldwide. In particular, the tools are known to be used throughout European organisations including in automotive with four of the top German and French car manufacturers, a German leading automotive parts manufacturer, two of the top French and German telecommunication companies, two leading German industrial companies, two of the top nordic electronics and communication equipments company, four of the world digital economy leaders, two of the top US chips manufacturers, a leading US software database vendor, and many software teams of all size everywhere.

These tools are downloaded collectively about 2 million times each month.

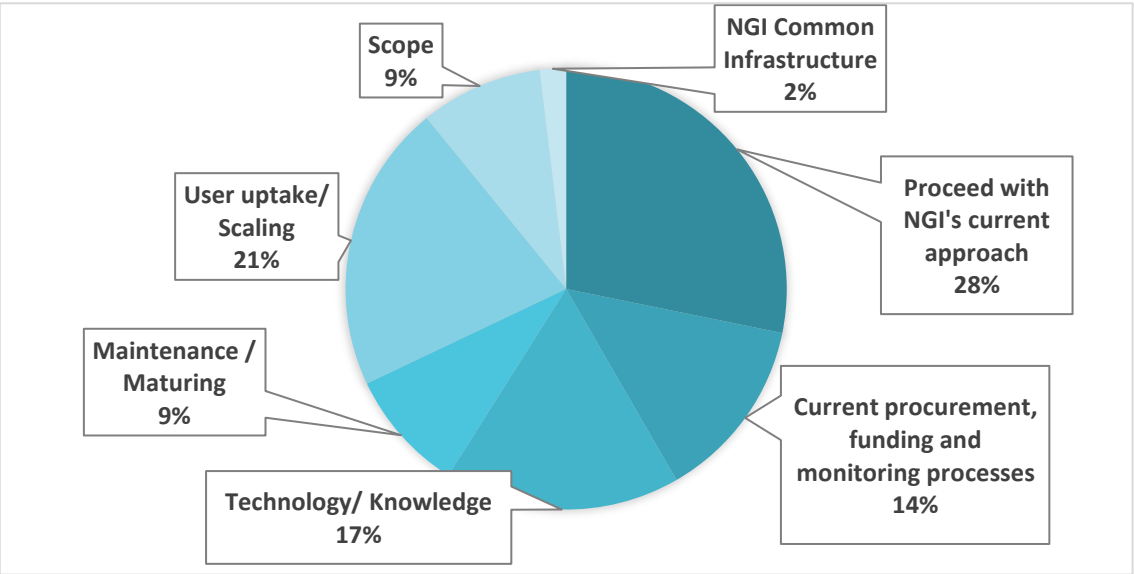
NGI support has been key to help AboutCode develop and sustain new features for supply chain security that will prove important for European organisations to comply with the Cyber Resilience Act with less efforts and costs."

5. Grantees' Feedback

- Introduction

The feedback received from NGI grantees regarding how NGI funding can improve the uptake and success of the Next Generation Internet can be categorised into seven types of responses. These responses, as depicted in the figure below, include suggestions to maintain the current successful funding approach, recommendations for adapting procurement, funding, and monitoring processes, expanding technology topics, addressing challenges related to maintenance, maturing, and user uptake of open-source projects, and ways in which an NGI Common infrastructure can support the community and early adopters. The feedback also touches on the scope of the projects.

Figure 20 – Feedback from the Survey Respondents



Source: Author's own elaboration

- Proceed with NGI's current approach

Close to one third of the feedback received through the survey highlights the positive aspects of the current approach and the main message is "continue".

Firstly, participants express their appreciation for the funding opportunities provided, stating that it has had a significant impact on their projects and allowed them to pursue innovative ideas.

Participants appreciate that the application process is straightforward and does not involve excessive administrative burdens, allowing them to focus on their technical objectives and project development. This streamlined approach is seen as a progress from traditional funding models that often involve complex consortium setups and extensive reporting requirements.

Participants acknowledge RIAs' effective interface between the communities and the European Commission, facilitating rapid progress while ensuring compliance with funding requirements.

Feedback also insisted that the NGI funding should continue to support community open source projects. FOSS is considered essential for promoting digital sovereignty, privacy, and security. The funding enables developers to create alternatives to proprietary software and contribute to the development of a competitive European digital ecosystem. Participants emphasise the need for ongoing financial support to ensure the sustainability and growth of open source initiatives.

Furthermore, survey participants highlight the importance of public awareness and education about NGI funding opportunities. They suggest that more efforts should be made to spread the word and make potential applicants aware of the funding options available. This would help attract a broader range of talent to submit innovative proposals.

> *"The NGI initiative has been *brilliant* on so many levels[…]. As a civil society organisation, we have won many competitive grants from different funders and programs over the years. But as an example, NLNet's NGI grant scheme is by far one of the leanest, lightest weight application processes we've seen. It combines this process with high expectations as to the creative and technical content, and friendly check ins along the way. As recipients, we can see they've been refining their processes very diligently, carefully paring away time-wasting forms and hurdles, but retaining meaningful questions.*
>
> *The result is that smaller organisations can actually compete. For so many grants, an organisation literally has to have a full time staff member grant-writer - or a team - just to do compliance and file grant applications. That stifles innovation, and makes people at smaller orgs - technologists and decision-makers - afraid to try new or brave ideas. The light-weight demands of this NGI funding application process wipe those problems away. The funds are not huge, but the program shows if there is good progress in thinking, coding and innovation, there is an open door to apply for funding the next step on the path. Process matters a lot if you want good applicants, and thus quality impact. It's a very smart structure."*
>
> Survey feedback

- Adaptations to the current procurement, funding and monitoring process

Some feedback (15%) received targets the efficiency, accessibility, and impact of the NGI funding program with recommendations for adapting the current procurement, funding and monitoring processes, as highlighted in the points below.

The NGI funding approach could be diversified to include small-scale funding (€10k up to €100k) for new ideas and projects, medium and large-scale funding (€100k-€5M) for scaling up existing projects in the EU NGI space that have

proven sustainability, and strategic funding for areas of priority to European digital sovereignty.

To **support the follow-up funding** of existing projects, the recommended new approaches for NGI funding are:

a) increasing the number of open calls for additional funding to encourage innovation and expand existing projects,
b) streamlining the process of obtaining follow-up funding,
c) providing funding for coaches who can assist previous NGI grantees in applying for other funding programs, and
d) designing improved support programs that offer better visibility and guidance towards second-stage and further funding opportunities.

These measures aim to ensure continued support and growth for successful NGI projects.

To address **the challenge of finding contributors** to work under grants, it is suggested to fund foundations that have direct access to open source/free software developers. While there are existing initiatives aimed at connecting contributors with funded projects, further efforts in this direction are recommended.

The RIA plays a crucial role in **bridging the gap** and facilitating effective communication between the technical aspects of the project and the EC. To enhance the translation between technical products/projects and the European Commission, it is proposed to allocate larger amounts of funding to the RIA.

In order to accommodate **the needs of non-profit organisations and alternative governance structures**, it is recommended to consider their specific requirements in the application process (see box).

To support FOSS developers, it is suggested to provide upfront payments. This involves reducing milestones and micromanagement, allowing for more flexibility in milestone structures and funding. This approach would recognises the evolving nature of projects and the need to adapt to market demands quickly.

To **streamline the monitoring process and alleviate the burden** on projects, it is recommended to simplify the process and reduce the number of deliverables required. Instead of focusing solely on deliverables, the emphasis should be placed on assessing the actual value delivered by the projects.

In line with the previous point, it is suggested to provide **clearer guidelines that highlight key aspects related to impact**, such as standardisation. By offering more explicit guidance, developers can better understand the specific requirements and expectations for their projects, particularly in areas that have a significant impact.

- Technology topics and knowledge sharing

Approximately 17% of the feedback provided relates to technology topics and knowledge sharing.

When polled about which technology topics to fund in the fututure, respondents recommended to continue to focus on contributing to a more open and inclusive digital landscape, with projects that are open source, decentralised, and promote user freedom, providing alternative choices to existing platforms to ensure freedom of choice online, addressing hardware vendor lock-in and promoting ownership and interoperability standards.

Additionally, the NGI should continue to contribute to the development of a more robust and secure digital ecosystem with projects that enhance service portability, improve basic internet technologies (DNS, email, IPFS[12], Fediverse …), and advance network infrastructure.

Thirdly, the NGI should continue funding projects that contribute to a more inclusive and user-centric internet. Examples include user-friendly and accessible communication tools that prioritise privacy and decentralisation, solutions that ensure digital content and platforms are accessible to individuals with disabilities. By funding user-centered design and usability efforts such as the implementation of WCAG (Web Content Accessibility Guidelines) compliance in projects, the NGI would also promote inclusivity and equal access to information and services, enhance the overall usability and adoption of digital technologies. Localisation efforts can also play a crucial role in making digital solutions more accessible and relevant to local communities and diverse cultural contexts.

Several new areas of focus were suggested, which cover areas related to legislation, AI and strategic investments.

In the public sector, there are legal issues related to data confidentiality that require authentication without disclosing the actual data. This is crucial due to factors such as corporate trade secrets, legal regulations, and privacy concerns. Zero-knowledge proofs can play a significant role in addressing these challenges. By investing in technologies that enable secure data verification without exposure, NGI funding can facilitate the implementation of legal requirements. Similarly, in the light of the Cyber Resilience Act, NGI should fund bug fixing and the strengthening of cybersecurity measures in general, ensuring relisience and security of the Internet ecosystem.

In addition, by investing in projects that develop technologies to detect and mitigate the spread of AI-generated random content, the NGI can contribute to a safer and more reliable digital environment.

[12] InterPlanetary File System is a protocol, hypermedia and file sharing peer-to-peer network for storing and sharing data in a distributed file system.

Several feedback areas focus more on the strategic level. First, NGI should invest in the maintenance of key FOSS infrastructure projects. Second, by supporting the development of seamless integrations between FOSS solutions, the NGI can level the playing fields for competing of FOSS projects with strongly integrated proprietary offerings. Third, there was a request to ensure representation in the IETF leadership which is key for decision-making in the Internet standards ecosystem.

Lastly, feedback also targeted knowledge exchange and channeling of expertise, such as to organise a browser-dev conference or similar dissemination events where projects can meet and share knowledge. It was also recommended to convene "citizen assemblies" of randomly selected FOSS community members to consider and weigh potential NGI solutions.

- Maintenance / maturing of NGI projects

Approximately 10% of responses addressed topics related to the need for long-term sustainable funding to support the maintenance and ongoing development of projects. While NGI funding is effective in kickstarting projects, it lacks continued maintenance funds, and this could be addressed by providing additional support to developers (or making them more aware of it) in creating sustainable funding models for the future of their work. Funding should not only focus on new projects but also on bug fixing, documentation, and other unsexy work that is necessary for the maturity and impact of open-source projects. It argues that while funding often focuses on new development and shiny features, the majority of work required for NGI technologies to make a real-world difference lies in maintaining, polishing, documenting, maturing, and publicizing existing projects.

Feedback also suggests that the NGI should identify existing open-source projects with market traction and provide funding for lead developers to continue their work within universities. This recommendation aims to provide a stable environment for FOSS developers to continue their work without financial constraints. By introducing their projects and FOSS development processes to the student body, it would foster innovation and ensure the future sustainability of these projects.

Funding should also support the nurturing, development and management of the community and digital commons, with funding allocated to support the maintenance of infrastructure, timely response to support requests, and the growth of the community. Feedback mentioned that digital commons are crucial for fostering innovation and equitable access, and nurturing and preserving them is essential for a more connected and just society.

- Scaling and user uptake

Approximately 20% of feedback highlighted the challenges of scaling and user uptake of FOSS projects. Suggestions included the funding of more non-coder

roles to work on user adoption of digital commons, of marketing and public relations to showcase open-source products and educate the public about their benefits.

The challenge of competing with well-funded proprietary solutions was also mentioned, together with the the need for public education on privacy and security to highlight the advantages of alternative solutions.

Moreover, feedback emphasises the importance of creating high-quality software and the need for technological transfer and integration with established companies. Lastly, feedback highlights the importance of mentoring projects to become self-sufficient.

- Scope

Close to 10% of feedback addressed the scope of the NGI. It emphasises the need for grants to cover short-term operational and growth costs, including infrastructure, legal paperwork, certifications, compliance, and marketing. These costs are necessary to convert a technical solution into a marketable product.

Feedback also suggests investing in larger education programs and funding, particularly in digital skills and open source, for children, students, and basic education on digital rights. It also emphasises the importance of connecting different but complementary open-source areas to foster growth. It advocates for launching larger software initiatives to enable the formation of teams capable of building complex software that can compete with proprietary solutions. It highlights that while fragmentation is necessary for innovation, convergence into larger projects may be required to have a significant impact, calling for more collaboration with projects working in the same area.

- NGI project infrastructure

Feedback presents some ideas for supporting open-source projects in their early phases, such as motivating the community to contribute and providing computational infrastructure. It suggests offering free hosting services to demo the software 24/7, allowing users to directly experience it instead of relying on repositories with source code that requires installation expertise. Free hosting services could also allow projects to offer free services to early adopters. This enables the gathering of real usage data and error tracking without burdening early adopters with payment for hosted services. In addition, feedback proposes providing high-performance continuous integration and other computing resources to support the development and testing of the NGI open-source projects.

- Conclusion

The feedback that was requested to the NGI grantees is important because it can show if there is an alignment between the fund and the targeted community of innovators. The current approach of the NGI funding initiative is highly regarded,

with participants appreciating the funding opportunities provided and the streamlined application process. However, because of the nature of a common digital infrastructure which must be seen as an investment, there is a need for ongoing financial support to ensure the sustainability and growth of these open-source initiatives. Recommendations for adaptations to the current procurement, funding, and monitoring process include diversifying the funding approach in that sense, simplifying the monitoring process, and providing clearer guidelines for project impact.

The grantees recommend to continue focusing on technology topics that contribute to a more open and inclusive digital landscape, a robust and secure digital ecosystem, and a more inclusive and user-centric internet. However, they highlight that long-term sustainable funding is needed to support the maintenance and ongoing development of projects, and funding should also support the nurturing and management of the community of these digital commons. Challenges of scaling and user uptake of NGI projects include the need for non-coder roles, marketing and public relations, technological transfer and integration, and mentoring projects to become self-sufficient.

More generally, the grantees mention that there should be funding for digital skills and open source. Collaboration and connection between different open-source areas are also important. Lastly, an investment in an NGI infrastructure providing high-performance continuous integration and offering free hosting services would lower barriers of involvement by the community and uptake by early adopters of NGI project outcomes.

6. Conclusion

In conclusion, the Next Generation Internet (NGI) program, with its funding of over 100 million euros, has had a significant impact on shaping a sustainable, sovereign, and EU-aligned tech landscape. The program supports grassroots projects that prioritise European digital rights and principles, enabling compliance with EU legislation and promoting the concept of digital commons. NGI projects have made substantial contributions to protocols and standards, enhancing privacy, security, interoperability, and functionality in the digital realm. These projects also provide alternative solutions in various domains, challenging the current technological landscape. The survey results indicate that NGI solutions cater to diverse ecosystems and have an active external community, fostering collaboration and innovation within the Free and Open Source Software (FOSS) community. The funding has had a positive impact on EU society, policy, standardisation, choice, and sustainability, fostering innovation and integration into existing initiatives. The qualitative analysis identifies technology clusters that shape the digital landscape and drive change in the Internet ecosystem, demonstrating the diversity and impact of NGI projects within each cluster. The feedback from NGI grantees emphasises the need for ongoing financial support, diversification of funding approaches, simplification of monitoring processes, and clearer guidelines for project impact. Recommendations include collaboration between open-source areas, and the provision of an NGI infrastructure offering free hosting services to enhance community involvement and adoption of NGI project outcomes. These insights and recommendations aim to inform policy-making decisions and shape the future work program of the NGI initiative.

7. Annexes

7.1. Annex 1: Project categories within RIAs

The table below provides the number of projects within each RIA and project category.

Call / Technology category	decentralised solutions	software engineering protocols, interoperability cryptography algorithms proofs	services and applications	network infrastructure	vertical use cases improving search and discovery and community building	trustworthy hardware and manufacturing	data and machine learning	middleware and identity	operating systems firmware and virtualisation	measurement monitoring
	26%	17%	11%	11%	9%	7%	5%	5%	4%	2%
NGI Assure "Advancing research on blockchain and DLTs"	11	57	5	28		13	8	11	12	
NGI0-Discovery "Technologies improving search and discovery"	10	5	21	6	63	3	14	12	6	2
NGI0-PET "Privacy and Trust enhancing technology"	7	28	14	17	1	34	2	11	15	7
NGI TRUST "Privacy and Trust enhancing technology"		14	19	2	2	4	11	1		3
eSSIF-lab "Self-sovereign identities technologies"	50									
DAPSI "Data portability and services"	10	17	13		1		1	4		

Call / Technology category	decentralised solutions	software engineering protocols, interoperability cryptography algorithms proofs	services and applications	network infrastructure	vertical use cases improving search and discovery and community building	trustworthy hardware and manufacturing	data and machine learning	middleware and identity	operating systems firmware and virtualisation	measurement monitoring
Trublo "Fostering trust in Internet information, exchange and content with blockchain	45									
Ontochain "Bringing forward the emergence of collective intelligence on the Internet"	22	5	5	5	1		1	2		3
NGI-POINTER "Architects to change the fabric of the Internet and Web"	2		9	18	1	3		2	1	
LEDGER "Better data governance"	33									
NGI Atlantic "NGI experiments together with US research teams"	5	1	5	10	1		6			3

Among the NGI calls, there are five calls that have a concentration of projects in specific categories.

Firstly, the call "LEDGER: Better data governance" exclusively funds projects in the ledger category of decentralised solutions. This indicates a strong focus on developing decentralised ledger technologies to improve data governance and security.

Additionally, four calls have over 40 projects in specific categories:

NGI Assure: This call focuses on advancing research on blockchain and DLTs. It has a significant concentration of projects in the category of cryptography algorithms proofs. This highlights the importance of developing and validating cryptographic algorithms to ensure the security and trustworthiness of blockchain and DLT systems.

NGI0-Discovery: This call aims to improve search and discovery technologies. It has a concentration of projects in two categories: vertical use cases and community building. Vertical use cases refer to specific industry or domain-specific applications of technology, while community building focuses on fostering collaboration and engagement within the NGI community. This indicates a focus on practical applications and community-driven development in the search and discovery domain.

eSSIF-lab: This call focuses on self-sovereign identities technologies. It has a concentration of projects in the category of decentralised solutions. This aligns with the goal of developing technologies that empower individuals to have control over their digital identities in a decentralised manner.

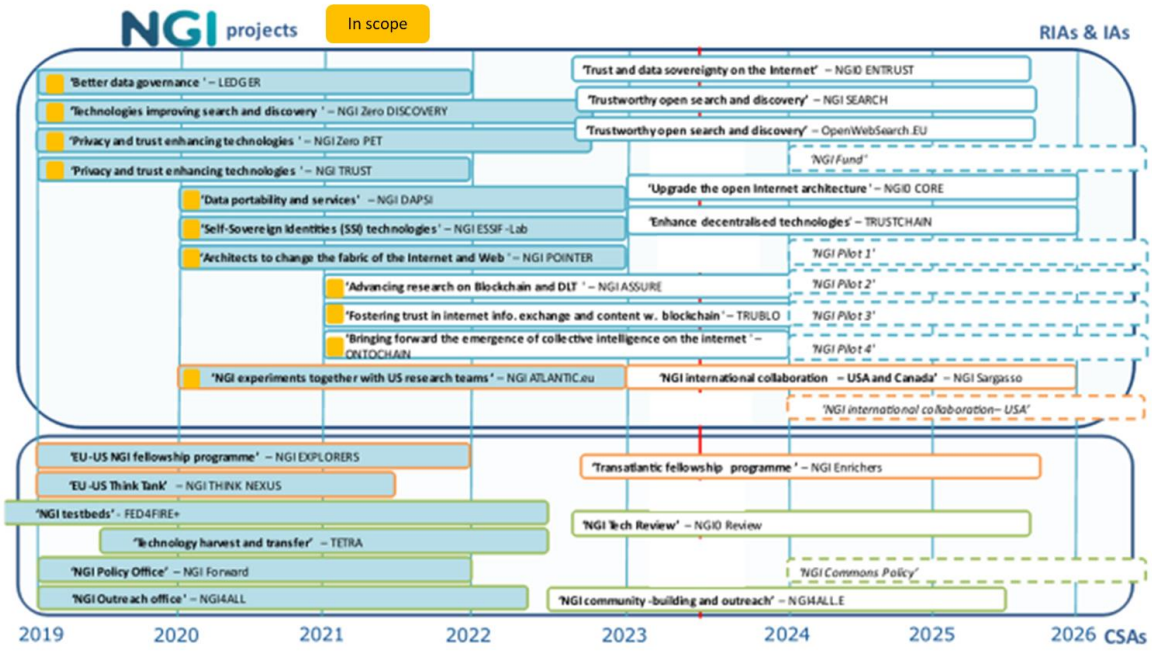
Trublo: This call aims to foster trust in Internet information, exchange, and content with blockchain. It also has a concentration of projects in the category of decentralised solutions. This further emphasises the importance of blockchain technology in building trust and transparency in the digital landscape.ive calls have a concentration of projects in specific categories. One call exclusively funds projects in the ledger category of decentralised solutions. Four calls have over 40 projects in specific categories, including software engineering, protocols, interoperability, cryptography, algorithms, proofs (NGI Assure), vertical use cases improving search and discovery, and community building (NGI Discovery), decentralised solutions (eSSIF-Lab and Trublo).

This concentration shows that these calls are targeted towards specific categories and have been successful.

These initial RIAs were specialised, but the calls became less specialised, addressing the entire technology stack through NGI Commons.NGI Discovery and NGI PET are the two calls that have projects spanning across all technologies.

7.2. Annex 2: Methodology

7.2.1. Scope



Source: DG CONNECT

The first wave of NGI projects funded from the 2018, 2019 & 2020 work-programmes are now over. This concerns the following RIAs:

- NGI TRUST
- NGI0-PET
- NGI0-Discovery
- LEDGER
- DAPSI
- NGI-POINTER
- eSSIF-lab
- NGI Atlantic
- Ontochain
- NGI Assure (extended until 31/08/2024)
- Trublo

The above RIAs have funded a large portfolio of projects which are available in the NGI catalogue. The following list of the related 784 projects is provided by DG CONNECT. This is the initial scope of the study. Section 2 “Portfolio analysis” covers this scope.

DG CONNECT and Gartner decided to include in the survey and its subsequent analysis two RIAs, namely: NGI0-Entrust and NGI0-Core. This expands the list

of targeted projects[13] to 1014 as counted at the end of the survey period. Sections 3 and 4 are based on this widened scope.

The NGI grants often provided in the early stages of the internet's digital commons projects serve as seed money that helps in their roadmap development towards core values such as privacy and inclusion. NGI grants have also funded some of the digital commons in later stages of their life cycle, contributing in various manners to improving the accessibility and adequacy of the solutions and therefore contributing to their reusability. In this report, an NGI project is a digital commons project which has received an NGI grant.

7.2.2. Overall approach

Gartner proposed a methodology that will ensure that data are collected in an efficient way to infuse in each of the required benchmarks.

The methodology consists of two steps. The first step focuses on the whole portfolio of NGI third party projects (called NGI 1000 for simplicity) which delivers a quantitative analysis. The second step focuses on a subset of projects (NGI 50) which are identified as most impactful and aims to develop a qualitative analysis based on their impact in relation to Web 4.0 technology.

7.2.3. Step 1: NGI 1000 – Quantitative Benchmark

The quantitative benchmark is composed of 2 dimensions:

a) The catalogue analysis, which provides insight in the geolandscape of the NGI projects and on their distribution among the different RIAs and categories.
b) The benchmark of the NGI's impact on EU society and values, on policy, standardisation, choice and sustainability.

The catalogue analysis (a) is based on the data set (CSV file) downloadable from the NGI catalogue list.

In order to assess the impact of the projects (b), a questionnaire and subsequent survey are developed with DG CONNECT. The questionnaire is presented below.

[13] https://www.ngi.eu/discover-ngi-innovations/?&NGI_project=2726,2733,2735,2909,2737,2731,2732,4167,2728,4155,2729,2734,4082

NGI 1000 data point	Response
1. Please identify your project (s) (project name if possible as in NGI catalogue, short description).	Open field
2. What was/is the contracting channel for the first grant received? (please select)	Drop down RIA/organisation list
3. How would you qualify the impact of your project in relation to the European Digital rights and values?	List (multiple choice) • None • Putting people and their rights at the centre of the digital transformation • Supporting solidarity and inclusion • Ensuring freedom of choice online • Fostering participation in the digital public space • Increasing safety, security and empowerment of individuals • Promoting the sustainability of the digital future
4. Which situation best qualifies the way your solution is shared?	Multiple choice • The solution is not finalised and therefore not shared. • The solution is finalised but not shared on a public repository. • The solution is finalised and shared on a public repository. • The solution is shared via a distribution platform (distro, app store…).
5. Who are the potential target users of your solution?	List (multiple choice) • IT services providers (hosting, cloud, telecom) • Consumer/ End-user application • “Corporate” IT (productivity, office tools, security...) • Public sector/ government/ academia… • Developers • Other

NGI 1000 data point	Response
6. Which situation (s) best qualifies(y) the actual reuse/impact of your project?	Multiple choice • There is an active external community (other than the core developers and maintainers) contributing bug reports/ code which indicates some level of reuse. • There is a very active external community (other than the core developers and maintainers) contributing bug reports/ code, which indicates a substantial level of reuse. • The solution targeted a small set of key Internet players and it is reused by them, making it a key building block of the Internet technical ecosystem. • There is other evidence of reuse which indicates some reuse. • There is other evidence of reuse which indicates a high level of reuse, “high” meaning that almost all the target audience has been reached and is using it. • The solution is not reused
7. Please indicate the evidence of reuse	Open question
8. Which of these EU legislations and/or policies does your project relate to?	List (multiple choice) • None • General Data Protection Regulation • EU digital identity • Cyber Resilience Act • Digital Services Act / Digital Market Act • Alternative choices to existing platforms (Ensure freedom of choice on line) • Disinformation measures • Web 4.0 and Virtual Worlds • Digital Commons
9. Which Standards Developing Organisation did you collaborate with in the context of your project?	List (multiple choice) • None • W3C • IETF • OASIS • IEEE • ISO • ITU • ETSI • CEN • CENELEC • Other
10. If your project contributed to standards, please provide a link to the contribution	Open question

NGI 1000 data point	Response
11. Is your solution open source?	No Yes
12. Does your open-source solution provide a viable alternative to a proprietary solution?	No Yes
13. Which proprietary solution does your project provide an alternative for?	Open question
14. What is the outcome of your project?	List (multiple choice) • No further activity • The project received a new funding • The project was part of a larger open source community effort, and the new software is integrated to it • The project was part of an open-source business effort, and the new software is integrated to it • The project joined an existing (not-for-profit) legal entity or FOSS umbrella • The project originated in an existing mature FOSS effort, and is merged upstream • A company/ foundation was created to exploit the value of the project – including for example a steward ownership company
15. If your solution is open source, which license have you selected?	Apache CECILL CDDL Common Development and Distribution License Eclipse Public License European Union Public License GNU General Public License GNU Lesser General Public License Mozilla Public License The 2-Clause BSD License The 3-Clause BSD License The MIT License Other
16. If the project received a new (non-NGI) funding, was it:	List (multiple choice) • Regional/National public funding? • European public funding? • private funding? (VC, global charity) • crowdfunding? funding from a foundation?
17. If the project received a new NGI funding, which is the contracting party?	Closed list of RIAs

NGI 1000 data point	Response
18. If a company was existing or was created, what is the business model?	List (multiple choice) • Integration services • Consulting • SaaS/hosted solution/ managed hosting • Freemium/Premium services including subscription contract • Support contract • Products: hardware or software • Other
19. If a company was created, how many full time employees does it have?	open numerical question
20. What is the size of your community contributing to your solution (number of people, apart from those funded by NGI)?	Open numerical question
21. What can the NGI funding do to improve the uptake and success of the Next Generation Internet (e.g.: Digital Commons, Web 4.0, Virtual Worlds)?	open question

The survey is anonymous: it does not track IP addresses and does not request the respondent's email. The European Commission aims to publish the results. However, there is a possibility to opt out individual contributions. In the case where the respondent received funding from multiple channels, the respondent is requested to mention the first funding channel received in the 2nd question and there is an option to select additional fundings later in the survey.

The invitation to complete the survey and the link is sent to third parties by DG CONNECT via RIA coordinators.

The tool used for the survey / the data collection is EU Survey. DG CONNECT is owner of the NGI1000 survey[14]. The results of EU Survey are downloadable in .cvs format, which served as data set used for the analysis of the impact.

The number of responses to the survey was high, with 247 responses as of the timeline provided within the context of this study[15]. The quality check of the responses identified some invalid responses (for example, which provided insight on an RIA instead of a specific project.) The final dataset for this study is based on 239 responses. For each survey entry, one or several NGI projects were

[14] https://ec.europa.eu/eusurvey/runner/NGI1000BenchmarkingSurvey

[15] DG CONNECT has decided to keep the survey open for continuously tracking the impact of the NGI.

described, leading to a total of 291 projects[16] referenced in the survey responses, indicating a response rate of 28.7%. The extrapolation of data points takes into account the total number of projects[17]. The multiplier effect regarding the community takes into account an estimation provided by DG CONNECT of the number of grantees per project: 1,5. The quantitative analysis file is not published, as the survey provided the option to opt out from publication, which 62 respondees chose.

The derived quantitative analysis of the impact of the NGI is described in **section 3** of this report. Some of the survey questions are open, and some of the results are used to explain the quantitative results in section 3.

The results of this analysis were presented at the following conferences:

- Open Source Policy Summit 2024
- FOSDEM 2024

Section 5 provdes an analysis of the survey responses on the feedback about the NGI initiative.

With a high success rate and a high quality of responses for the survey, the next step focused on gathering additional qualitative insight on the very impactful projects and their technology landscape within Web 4.0.

7.2.4. Step 2: NGI 50 – Qualitative Benchmark

The aim of the qualitative analysis is to develop insight in the projects within the various technology clusters funded by the NGI. Data that contributed to this qualitative data collection aimed at understanding how these solutions relate to the various benchmarking pillars, i.e.: how do they provide an alternative, how do they relate to the EU Digital rights of decentralisation, user centricity, …, how do they adhere and/or contribute to standardisation and interoperability between various solution, and how wide is their user base. An initial scoring of the survey responses was done to provide an overview of how impactful these projects were. An interview with RIAs was organised in order to refine the insight on the various benchmarking pilars and potentially identify additional impactful projects which were not in the survey results; the outcome of the qualitative data collection aimed

[16] For a population of 1014 targeted projects, a margin of error of 5% and a confidence level of 95%, a representative sample would be 279 responses, which is lower than the results obtained.

[17] For example, the survey data indicates a number of 99 FTEs for the companies created, which extrapolated results in 99*1014/291 = 345 FTEs estimated.

also at shaping the technology landscape of projects within clusters supporting the Web 4.0. This final list of projects is the basis of the narrative of section 4.

Further evidence from desk research and documentation provided by RIAs are then analysed within the Web 4.0 technology cluster landscape, highlighting how these projects impact the different benchmarked areas (standardisation, EU digital rights, Sustainability, …). The analysis is shared with the RIAs who can further contribute if needed, using a cryptpad solution from the European Commission.

The outcome of the qualitative analysis is provided in **section 4** which described the technology clusters, and in **section 5** which provides feedback from the grantees for the next steps of the NGI.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

KK-05-24-246-EN-C

Publications Office
of the European Union

doi: 10.2759/062218
ISBN: 978-92-68-14314-8