



Open Source Congress 2024

Shaping the Future of
Collaboration in AI, Security,
and Digital Public Goods

December 2024

Anthony Williams, President and Co-founder, *DEEP Centre*

Foreword by Chris Xie and Yue Chen, *Futurewei Technologies, Inc.*

Open Source Congress 2024

The Open Source Congress is an annual gathering bringing thought leaders, practitioners and community leaders together to help **shape the future of open source technology.**



China's contributions to open source, exemplified by OpenHarmony and OpenEuler, underscore its commitment to **bolstering global collaboration and digital sovereignty.**



Regulatory pressures from governments worldwide have underscored the need for **proactive, community-driven policy advocacy.**



Open source AI has democratized access to powerful AI tools, enabling developers, researchers, and companies worldwide to experiment, share, and improve upon existing models.



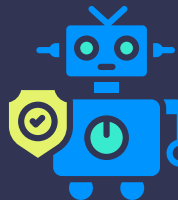
Responsible AI includes training AI systems on diverse datasets and baking **ethics, safety, and transparency into AI models** from the outset, not as an afterthought.



The growing ubiquity of open source software makes **cybersecurity increasingly critical to ensuring the safety, trust, and reliability** of the world's global digital infrastructure.



The Congress highlighted the need for **AI-specific security frameworks,** including adequate guardrails, provenance tracking, and shared repositories of high-quality training data.



Open source is a driving force behind **decentralized technologies** like blockchain that offer users control over their data, assets, identities, and digital interactions.



Digital public goods like open source software and open data have become vital tools for achieving global progress in education, healthcare and climate change.



Congress participants agreed that **continuous dialogue and cooperation** are critical for addressing ecosystem challenges like cybersecurity, sustainability, and regulatory compliance.



Proposals for **strengthening open source collaboration** included continuing the annual Congress, forming a peer-to-peer network, and establishing a global secretariat.



The Open Source Congress is evolving into a **year-round platform for collaboration,** with plans for position papers, expanded participation, and a 2025 event in Brussels.

Contents

- Foreword 4
- The 2024 Open Source Congress: Continuing the Collaboration 5
- Setting the Context: The Evolving Role and Impact of Open Source Software 7
- Open Source Artificial Intelligence: Balancing Innovation and Responsibility 9
- Open Source Cybersecurity: Enhancing Security Through Collaboration 14
- Broader Horizons: From Decentralized Infrastructure to Digital Public Goods 19
- Collaboration Between Open Source Organizations: Building a Sustainable Future 23
- Conclusion: Charting a Path Forward 27
- Acknowledgments 29
- About the Author 29
- Appendix: List of Open Source Congress 2025 Participating Organizations 30

Foreword

Open Source Congress (OSC) 2024 marked a milestone in the evolution of the global open source ecosystem, showcasing remarkable progress in participation and organizational excellence. Hosted in Beijing, China, under the professional stewardship of OpenAtom Foundation, the conference attracted a diverse array of voices from across the globe, enriching the discussions and solidifying the event's reputation as a cornerstone for open source collaboration. OpenAtom Foundation's unwavering support and meticulous organization elevated the conference to new heights, setting a benchmark for future events.

At its core, OSC 2024 exemplified the community's growing awareness of the critical issues facing the global open source movement. From fostering collaboration to addressing emerging challenges, the participants engaged in thoughtful dialogue and began taking actionable steps to safeguard and promote the values of open source. One significant development is the Eclipse Foundation's commitment to organize and host OSC 2025, a testament to the expanding network of organizations dedicated to OSC's mission.

However, the challenges ahead remain formidable, particularly in defining the future of OSC itself. A central question persists: Is there sufficient will within the OSC community to formalize a global, inter-foundation, and multi-stakeholder organization? Such a unified initiative could amplify the collective impact of OSC, aligning efforts with other important initiatives, such as the United Nations' OSPO for Good and the OpenForum Europe's advocacy in Europe. While these efforts share common goals, they often operate with varying priorities, underscoring the need for a cohesive, global strategy.

We hope that like-minded organizations with shared visions will join forces to create a truly global initiative. Such an effort would not only protect the principles of open source but also elevate it as a universal knowledge base, benefiting all of humanity. Let this be the beginning of a unified and impactful movement.

Chris Xie and Yue Chen

Futurewei Technologies, Inc.

The 2024 Open Source Congress: Continuing the Collaboration

The [Open Source Congress \(OSC\) 2024](#) in Beijing brought some of the community's brightest minds together to help shape the future of open source technology. Hosted by the OpenAtom Foundation, this second edition of the Congress fostered an intimate setting for candid conversations underscoring both vital challenges facing the ecosystem and the growing influence of open source solutions across regions and industries. With a focus on open source artificial intelligence (AI), cybersecurity, decentralized infrastructure, and global collaboration, the vibrant exchange of critical ideas in Beijing broadened and deepened a community dialogue that commenced at the inaugural 2023 event held in Geneva, Switzerland.

The Legacy of Geneva

The 2023 Open Source Congress in Geneva was a seminal event at a critical moment in time. The growing ubiquity of open source software (OSS) intensified regulatory scrutiny and increased the urgency of securing open source infrastructure. At the same time, community leaders worried that geopolitical rivalries and the growing threat of techno-nationalism could slow technological progress and undermine the international collaboration on which the OSS community depends.

In the two years preceding the 2023 Congress, the United States introduced the CISA Open Source Security Roadmap, and the European Union launched its Product Liability Directive and Cyber Resilience Act (CRA). These regulatory initiatives introduced measures to increase liability for product safety and required more timely disclosure and patching of security vulnerabilities. Unfortunately, some of these otherwise well-intentioned regulatory initiatives lack a nuanced understanding of the implications for the OSS community's unique development, commercialization, and licensing models. As a result, they pose significant compliance challenges and demand an urgent response from the community.

Meanwhile, global trade tensions, geopolitical conflicts, and a heightened emphasis on digital sovereignty had recently emerged as genuine impediments to international collaboration on digital technologies. For example, In 2022, the United States and China introduced strict export controls on semiconductors and other strategic assets to limit the flow of critical technologies across borders. Many in the open source community worried that curtailing trade in technology could lead to the fragmentation of OSS development into regional enclaves, thwarting efforts to promote inclusivity and cultivate a more diverse talent pool within the community.

Finally, high-profile cybersecurity incidents like Log4Shell and XZutils had made efforts to secure and safeguard critical open source infrastructure a focal point for community leaders. Just as bad actors can compromise

proprietary software products, cyber criminals exploit open source's openness to introduce vulnerabilities and backdoors into open source projects. Sophisticated OSS supply chain attacks were increasing, alerting the OSS community to the urgent need to bolster its cybersecurity posture.

In short, regulation, techno-nationalism, and cybersecurity challenges had profoundly transformed the open source landscape and created an imperative for collective action. Stakeholders across the community recognized that greater collaboration among OSS projects and the foundations that support them was urgently needed to enable community members to stand together on these common challenges. The call to action for open source leaders was to forge a mutual commitment and action plan for ensuring fidelity to the community's essential principles of openness, inclusivity, cooperation, and community-driven development.

Continuing the Collaboration in Beijing

The discussions in Geneva concluded with a consensus that there is significant value in regularly convening leaders of OSS foundations and working collectively to steward the global open source ecosystem. There was also broad support for rotating this annual gathering through traditionally under-represented regions of the world. Thus, to continue this collaboration, the OpenAtom Foundation graciously agreed to host the 2024 edition of the Open Source Congress in Beijing. The remainder of this report documents the 2024 Open Source Congress proceedings and highlights key discussion points and conclusions from this momentous event.

Setting the Context:

The Evolving Role and Impact of Open Source Software

Open source software has become a cornerstone of modern technology, driving innovation, collaboration, and inclusivity in business and society. Over the past few decades, OSS has transformed how we develop and share software, enabling anyone—from individual developers to global enterprises—to contribute to and benefit from shared digital infrastructures. By making source code publicly accessible and allowing developers to modify and distribute it, OSS fosters a culture of innovation, transparency, freedom, and continuous improvement.

Open source has revolutionized industries, powering critical systems like cloud computing, mobile applications, and the Internet itself. It has democratized access to cutting-edge technologies, allowing smaller companies and startups to compete on a level playing field with established tech giants. Major companies, foundations and non-profit organizations have adopted open source platforms to build scalable solutions. At the same time, governments and educational institutions use OSS for everything from public administration to scientific research. The flexibility and cost-efficiency of open source have also paved the way for the growth of startup businesses, freelance developers, and tech entrepreneurs, offering new avenues for innovation and business models built on open infrastructures.

Vital Challenges and New Imperatives for Collaboration

Despite its immense success, the OSS community faces several challenges. Sustainability and funding remain significant concerns, as many open source projects rely on volunteer contributions and need more financial support to maintain and scale their systems. Security is another pressing issue; while open source transparency

allows for rigorous code review, it also exposes vulnerabilities that malicious actors can exploit if not adequately managed. Additionally, the governance of open source communities can be complex, and while it has many benefits, decentralized leadership models sometimes lead to fragmentation, project management difficulties, or delayed responses to critical issues.

Given these challenges, collaboration among open source organizations is paramount. Organizations can pool resources, share best practices, and create a more sustainable ecosystem by working together. Collaboration also allows for faster innovation, as communities can build on each other's successes and avoid duplication of effort. Moreover, regulatory pressures from governments worldwide make it essential for open source organizations to have a unified voice in policy discussions. Through collective action, the OSS community can better address shared challenges like security, sustainability, and policy, ensuring that open source technology continues to thrive as a driving force for social and economic progress.

The Global Reach of Open Source Software

The Open Source Congress in Beijing highlights the degree to which OSS is truly a global phenomenon, with its influence now extending far beyond its early roots in North America. As digital infrastructure becomes increasingly central to economic development, governments and organizations worldwide increasingly harness OSS for its transparency, flexibility, and cost efficiency. In regions such as Europe, Asia, and Africa, open source solutions underpin significant innovations in healthcare, education, and public administration. These regions are adopting OSS and becoming substantial contributors to the ecosystem, advancing critical

projects and developing tools to address local needs. For example, several European countries are integrating open source technologies into public policy frameworks and digital sovereignty initiatives, ensuring that digital infrastructure remains secure and accessible.

The international impact of OSS is evident for people in the Global Majority, where open source solutions provide a path toward digital inclusivity. In many emerging economies, OSS is being used to bridge the digital divide, enabling local developers to build scalable technologies without the financial burdens associated with proprietary software. Open source tools also empower local entrepreneurs and startups, allowing them to innovate and compete globally. From smart agriculture in Sub-Saharan Africa to digital government platforms in Southeast Asia, open source projects address region-specific challenges while fostering economic development.

China's Role in Driving Open Source Progress

The OpenAtom Foundation's leadership in hosting the 2024 Open Source Congress underscores another vital dimension in evolving international collaboration on emerging technologies. China has emerged as a powerful force in the global open source community, playing a pivotal role in advancing OSS innovation and adoption.

As the country moves toward becoming a leader in digital infrastructure, its government and private sector have made significant investments in open source technologies. China is increasingly contributing to major international projects, with its developers actively participating in global open source communities. Domestic platforms like OpenHarmony and OpenEuler have gained traction, offering homegrown open source alternatives to proprietary systems. These initiatives reflect China's broader strategy to increase its digital sovereignty.

China's influence on the global OSS landscape extends beyond software development. The country also participates in vital international conversations on open source governance, cybersecurity, and digital public goods, ranging from its engagement with ICANN and various United Nations working groups to its Digital Silk Road initiative and digital infrastructure investments across Africa and the Middle East.¹ In hosting the Open Source Congress, the OpenAtom Foundation demonstrated its dedication to promoting collaboration and setting standards for global open source ecosystems. As the country continues to scale its open source initiatives, China's contributions will accelerate global open source adoption and bolster the impact of OSS across industries.

¹ <https://usali.org/usali-perspectives-blog/understanding-chinas-growing-influence-in-global-data-governance>

Open Source Artificial Intelligence: Balancing Innovation and Responsibility

Over the past decade, artificial intelligence (AI) has undergone significant advancements, transforming industries and reshaping the digital landscape. One of the most impactful developments has been the rise of deep learning, powered by neural networks that can analyze vast amounts of data to identify patterns and make predictions. Deep learning has led to breakthroughs in computer vision, natural language processing (NLP), and speech recognition, enabling technologies like autonomous vehicles, virtual assistants, and real-time language translation. The development of transformer models, particularly GPT and BERT, has revolutionized NLP by making it possible for machines to understand and generate human-like text, fueling applications in chatbots, content generation, and, more recently, large language models (LLMs) like GPT-4.

These advances have solidified AI's role as a transformative force across sectors and paved the way for the next generation of intelligent systems. In healthcare, machine learning algorithms are improving diagnostics, personalizing treatment plans, and accelerating drug discovery, with Google's AlphaFold recently achieving groundbreaking results in protein structure prediction. In finance, AI algorithms automate trading systems, improve fraud detection, and enhance customer service through personalized financial planning and robo-advisors. In transportation, AI is the backbone of autonomous vehicles, enabling cars to navigate complex environments, make real-time decisions, and reduce accidents. AI has also revolutionized manufacturing, where predictive maintenance and intelligent automation systems have optimized production lines, minimized downtime, and increased overall operational efficiency. In retail, AI is improving customer experiences through recommendation systems, dynamic pricing, and demand forecasting, while agriculture is leveraging AI for precision farming, crop monitoring, and optimizing resource use to increase yields.

AI has been a game-changer across industries, and the open source community plays a significant role in its development. Open source platforms like TensorFlow and PyTorch have democratized access to powerful AI tools, enabling developers, researchers, and companies worldwide to experiment, share, and improve upon existing models. This collective effort has accelerated the progress of AI research, with developers achieving significant breakthroughs like transformer models and deep learning architectures using open source methods.

Of course, with AI's groundbreaking potential comes significant responsibility. At OSC 2024, a key theme was open source AI and the efforts to drive innovation while addressing various risks and ethical considerations. Many of the largest developers of AI systems are keeping their AI models closed. However, Congress participants argued that developing AI models in the open has advantages. Open source allows for greater scrutiny and trust, as developers can audit and refine AI algorithms to address security, fairness, and ethical concerns. By lowering barriers to entry and encouraging a global community of contributors, open source AI can also fuel widespread adoption across industries, leading to more diverse and robust AI systems.

Openness and the Imperative for AI Safety and Explainability

Discussions about the nature and meaning of openness in AI became a focal point as Congress participants wrestled with a series of associated questions. What are our expectations for responsible AI? Does having access to the source code qualify as being open? What degree of transparency is reasonable for developers of AI models and tools? Given the market leader's

massive investments in talent, infrastructure, and data, can open source AI stacks compete with proprietary solutions?

Regarding their expectations of responsible AI, open source leaders insisted that the AI community commit to a higher standard of responsible development. Responsible development includes training AI systems on diverse datasets and baking ethics, safety, and algorithmic transparency into AI models from the outset, not as an afterthought. Additional measures could include guidelines for data collection, rigorous testing protocols, and auditing practices to mitigate bias and discrimination.

Congress participants also emphasized the importance of increasing the explainability of AI systems. Explainability improves the ability to express why an AI system has certain weights, or made a particular decision, recommendation, or prediction. Explainability is essential because it increases the trustworthiness, safety, and accountability of the systems that increasingly shape life-changing decisions, such as diagnosing disease or deciding who gets access to credit.

Developing the capability for AI safety, explainability, and fairness requires greater openness, including the factors most AI companies keep hidden, like the model architectures and the data they use to train the models. Take the data supply chain. Bias and discrimination in algorithmic decision-making are unintended consequences of training AI systems on data that reflect society's prejudices and power structures, including biased or discriminatory patterns in hiring, lending, or criminal justice. For example, artificial intelligence systems trained on historical loan data could perpetuate discriminatory lending practices, resulting in unequal access to credit or loans for marginalized groups. Likewise, social justice advocates have criticized predictive policing systems that use AI algorithms to identify crime hotspots and allocate police resources for disproportionately targeting minority communities.

A transparent data supply chain would significantly reduce the risk of biased outcomes in algorithmic decision-making. Transparency would ensure that the sources, quality, and handling of training data are well-documented and traceable. Traceability, in turn, would enable more robust oversight, including the capacity to audit data for discriminatory patterns or unfair representation. The capacity to identify and mitigate biases early in the data collection and preparation stages would also encourage model developers to seek out and deploy diverse and representative datasets.

Concerning model architectures, most LLMs in use today have been described as black boxes. Neural networks make predictions based on statistical probabilities inferred from trillions of data points and, as such, are beyond the scope of human comprehension. Merely looking at the source code in AI does not necessarily explain or shed light on why AI systems generate the outputs they do. Even AI developers concede that they cannot readily explain the outputs of AI systems they are developing.²

Opening the source code alone is insufficient because a given model's behavior depends on its training data and the layers of transformations it applies to that data. These factors are far more complex than what can be inferred just from the code itself. Indeed, the more sophisticated AI systems become, the harder it is to pinpoint exactly how they derive their insights because their internal decision-making processes (e.g., deep neural networks) become opaque and challenging to interpret.

Ultimately, AI explainability and the interpretability of model outputs are ongoing research problems that open source methods could help address. Open source methods would allow researchers and developers worldwide to collaborate on explainability techniques, share insights, and build on each other's progress. For example, open access to AI models and algorithms would enable the community to scrutinize the systems' internal workings, revealing patterns or flaws contributing to a lack of explainability. By developing

² <https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works>

and sharing explainability tools (e.g., SHAP, LIME, or saliency maps), the open source community could also contribute to a more standardized and accessible approach to explaining AI outputs.

Defining Open AI

The discussion on AI safety and explainability highlighted the importance of clearly defining what qualifies as open source AI. Congress participants discussed two prominent initiatives to tackle this challenge: the Linux Foundation's Model Openness Framework (MOF) and the Open Source Initiative's Open Source AI Definition (OSAIID).

The Model Openness Framework is the Linux Foundation's comprehensive framework for objectively evaluating and classifying the completeness and openness of machine learning models. As described by the LF's AI and Data team, the MOF identifies 16 critical components constituting a complete model release and, using these building blocks, defines three progressively broader classes of model openness.³

- **Class III – Open Model:** requires the public release of the core model (architecture, parameters, essential documentation) under open licenses.
- **Class II – Open Tooling:** includes the full suite of code used to train, evaluate, and run the model, plus key datasets.
- **Class I – Open Science:** entails releasing all artifacts in the end-to-end development pipeline, including raw training datasets, research papers detailing the model development process, log files, and more.

Model producers and consumers can use the framework to assess whether the various components of an AI system comply with

broadly accepted open source licenses. In doing so, the framework provides a north star for open AI and a practical roadmap for realizing the benefits of open collaboration in developing AI systems that are open, trustworthy, and beneficial to all.

In addition to the LF's work on the Model Openness Framework, the Open Source Initiative demonstrated significant progress in its effort to define open AI. After two years of consultations, the settled Open Source AI Definition in version 1.0 emphasizes four fundamental freedoms, including the freedom to:⁴

- **Use** the system for any purpose and without having to ask for permission.
- **Study** how the system works and inspect its components.
- **Modify** the system for any purpose, including to change its output.
- **Share** the system for others to use, with or without modifications, for any purpose.

The Open Source AI Definition also outlines the necessary components of an open AI system, including:

- **Open Code:** All code used to train and run the system.
- **Open Weights:** Model parameters and weights made available under open source licenses.
- **Open Data Information:** Detailed information about the datasets used for training, allowing others to recreate similar systems.

Together, the MOF and Open Source AI Definition provide robust frameworks for evaluating the degree to which today's AI systems are consistent with open source principles. Several participants warned the OSS community to set reasonable expectations for

³ <https://faidata.foundation/blog/2024/04/17/introducing-the-model-openness-framework-promoting-completeness-and-openness-for-reproducibility-transparency-and-usability-in-ai/>

⁴ <https://opensource.org/ai>

achieving what they described as practical openness, noting that frontier model developers have considerable power and latitude to pursue proprietary approaches to AI development and commercialization. As one speaker explained, “We may not get access to all of the data, but we may get some valuable components out in the open.”

Most importantly, the frameworks provide a roadmap for ongoing development and addressing societal challenges. By promoting the benefits of open AI and establishing clear criteria, these frameworks will encourage AI developers to build models and data sources that are accessible, modifiable, and auditable. Fostering greater transparency and open collaboration, in turn, will empower stakeholders to address the ethical and social implications of AI adoption, ensuring that we develop and deploy AI technologies in a way that aligns with ethical standards and promotes social good.

Scaling Community-Driven AI

The conversation on open AI naturally turned to the challenges of scaling open source approaches to compete with proprietary solutions. A primary challenge is cost. Developing and running generative AI models is an expensive endeavor that requires vast computational power and infrastructure. Training these models involves processing immense datasets, often with billions or trillions of parameters, using powerful GPUs or specialized hardware. Developers require significant cloud infrastructure and storage to manage the models and the data. The energy consumption for training and running large AI models is also extremely high, adding to operational expenses.

Another significant factor is the specialized expertise to develop and maintain these complex systems. Top AI researchers and engineers, whose skills are in high demand, command high salaries. In this fast-moving field, developers must constantly fine-tune the models, data sources, and infrastructure to handle different applications of AI in finance, healthcare, logistics, and other domains. Combined with the intensive computational needs and

large-scale data processing, securing the necessary talent to drive these advances makes generative AI a resource-heavy and costly field to advance.

The high barriers to entry pose a critical question: How can the OSS community differentiate its value proposition and keep pace with the world’s best-financed AI companies? Congress participants offered several suggestions.

One suggestion was to focus on smaller, specialized models to address niche use cases that may not require the massive scale and resources needed for large language models or other complex systems. Smaller models, by their very nature, require less computational power and fewer resources to train and run, making them more accessible for developers and organizations with limited budgets. In many circumstances, smaller, domain-specific models reduce the need for vast amounts of generalized data, which is often expensive and time-consuming to collect and process. The OSS community can also fine-tune specialized models to perform exceptionally well in specific domains, such as healthcare diagnostics, legal document processing, or financial analytics. By narrowing their focus, these models can outperform generalized AI systems in their respective fields, offering higher accuracy and more relevant outputs.

Another suggestion was to build an open data commons to make high-quality, standardized data more accessible and reduce the costs associated with training models. For example, a data commons could solicit contributions from a global network of academic institutions and research organizations to build domain-specific repositories in critical areas such as healthcare, environmental sustainability, agriculture, or natural language processing. Developers could tailor specialized datasets to address specific problems or industries, making training and developing targeted AI solutions easier. While the data commons proposition is attractive in principle, several speakers warned that open source communities will be challenged to compete with the massive data-ingesting

platforms that continuously feed new data to AI giants like Meta, Google, and Microsoft.

Finally, open source initiatives often receive support from universities, research institutions, philanthropic foundations, and government programs. Congress participants suggested that public funding and partnerships can offset development costs and enable open AI projects to access the computing infrastructure necessary to compete with more prominent proprietary players. These partnerships provide financial support and bring diverse

perspectives and expertise, fostering a collaborative environment for open AI innovation.

Specialized models, curated data commons, and public partnerships offer complementary tactics for increasing the OSS community's capacity to build cutting-edge open source AI applications. By capitalizing on these advantages, open source AI efforts can remain competitive, offering flexible, transparent, and community-driven alternatives to proprietary AI solutions.

Open Source Cybersecurity: Enhancing Security Through Collaboration

Cybersecurity remains a crucial concern in the open source community, and OSC 2024 highlighted the increasing need for cybersecurity frameworks. Discussions emphasized how the rise of AI has heightened the need for AI-specific security protocols, given the unique vulnerabilities that come with AI applications. As AI grows in sophistication, so too do the risks—particularly when it comes to ensuring that AI outputs are secure, reliable, and free from malicious influence.

At the same time, open source software continues to form the backbone of modern digital infrastructure, making security a critical concern. Open source projects underpin some of the world's most vital systems, from powering cloud services to enabling essential tools in healthcare, finance, and government. However, the very openness that fuels innovation in OSS also introduces unique vulnerabilities, such as the risk of supply chain attacks, outdated dependencies, and insufficient oversight of code contributions. Congress participants warned that more frequent and sophisticated cyberattacks are making the security of open source infrastructure essential in safeguarding the integrity and reliability of the global digital ecosystem.

Safety and Cybersecurity in AI

On day one of OSC 2024, panelists assembled to explore emerging security challenges as more and more businesses and organizations integrate AI into critical systems. Discussions focused on best practices for securing OSS against AI-enabled attacks and the role of open-source communities in enhancing AI safety. The panel also highlighted the need for AI-specific security frameworks, including adequate guardrails for AI models, tools for provenance tracking, and shared repositories of high-quality

training data for building open source AI applications free from bias and other flaws.

To set the context for the discussions, the panelists highlighted four significant risks:

1. **Malicious actors deploying AI for harmful ends.** With increasingly powerful AI models come the risk that these bad actors will weaponize these systems to manipulate information, disrupt economies, and undermine social stability. For instance, almost anyone today can use AI-powered systems to create deepfakes or misleading content, influencing public opinion and eroding trust in media and democratic processes. Economically, AI models can enable sophisticated fraud schemes or manipulate markets, potentially causing large-scale financial losses. These models can also exacerbate inequality, as companies may use them to automate jobs and displace workers without putting adequate support systems in place. Biased AI systems can also amplify existing social inequities, leading to discriminatory hiring, lending, and law enforcement outcomes. Speakers warned that AI's growing capabilities have heightened the need for robust ethical guidelines, governance, and security measures to prevent their misuse for harmful purposes.
2. **The acceleration of AI-powered cybersecurity risks.** The rapid acceleration of AI capabilities significantly expands the scope of potential security threats as developers integrate more sophisticated AI systems into critical infrastructure, financial systems, and consumer technologies. As AI becomes more powerful and autonomous, its potential for misuse grows—whether through malicious deep fakes,

the development of autonomous hacking tools, or the exploitation of vulnerabilities in AI-powered systems.

AI's ability to process vast amounts of data and automate tasks also opens up new attack vectors for cybercriminals, including data manipulation and AI-driven malware. To compound matters, the complexity of modern AI models often makes it difficult to detect and mitigate these threats, especially as they evolve faster than traditional security measures. Congress participants called on the OSS community to urgently investigate how to harden infrastructure against those who might use AI as an attack vector. More specifically, speakers noted an urgent need for stronger safeguards, including more robust AI governance frameworks and improved AI-specific cybersecurity protocols to protect against the growing risks.

3. **The proliferation of bad code.** While powerful tools for automating programming tasks, AI code generators could inadvertently lead to a proliferation of harmful code due to several factors. First, these systems often rely on vast datasets of existing code, which may include outdated, insecure, or poorly written examples. When AI models generate code based on these flawed patterns, they can propagate errors, vulnerabilities, or inefficiencies without proper oversight. AI code generators also lack the contextual understanding that human developers have, which can result in code that meets surface-level functionality but fails to adhere to best practices for performance, security, or scalability.

As more developers, including those with limited experience, use AI-generated code, there's a danger that this lousy code could spread across open source projects and commercial software alike, increasing the risk of software bugs and security

breaches. Speakers warned that AI-generated code can exacerbate these issues without thorough review and testing. They also emphasized the need for robust code validation processes and human oversight in AI-assisted development.

4. **The non-deterministic behavior of AI.** Speakers pointed to the non-deterministic behavior of AI as a problem because it introduces unpredictability and a lack of transparency in how AI systems make decisions. Non-deterministic AI models can produce different outputs even when given the same input, making it difficult to understand or trust the system's decision-making process fully. This lack of consistency can be problematic in critical applications, such as healthcare, finance, and legal systems, where predictable and explainable decisions are crucial for accuracy, accountability, and fairness. Non-deterministic behavior also poses challenges for debugging and auditing AI systems, as it becomes harder to trace the steps that led to a particular output.

To counter these AI safety and security risks, Congress participants emphasized the need for an AI-specific security framework that includes guardrails, provenance tracking, rigorous testing, and other measures.

- **Establishing AI-specific governance frameworks** would provide guidelines for secure development, deployment, and monitoring of AI systems. These frameworks could include standards for data provenance, model accountability, and transparency, ensuring that AI systems are auditable and traceable throughout their lifecycle. Legal developments, such as the EU's AI Act, have also stressed the need for developers to take responsibility for their models' use, further highlighting the importance of security and transparency in AI development.⁵

⁵ <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

- **Implementing guardrails.** AI guardrails can play a crucial role in preventing the use of AI for malicious purposes by establishing controls and safeguards that limit the model's ability to engage in harmful activities. These guardrails can include ethical guidelines, built-in constraints, and monitoring systems that govern how AI models are developed, deployed, and utilized. For example, guardrails can restrict AI from generating inappropriate, harmful, or misleading content, such as disinformation or deepfakes, by setting boundaries on the types of inputs the model can process and outputs it can produce.
- **Building provenance tracking into AI systems.** Provenance tracking, or verifying the origin of AI-generated content, enhances transparency and trust in AI systems by revealing how data is processed, what models they use, and how they generate outputs. This process enables users, regulators, and developers to trace the journey of AI-generated content, ensuring it was created ethically and without manipulation. By maintaining a verifiable record of the data sources and algorithms involved in producing content, provenance tracking helps mitigate the risk of misinformation, biased outputs, and malicious alterations.
- **Training AI models on high-quality, vetted data.** High-quality training data is fundamental to eliminating bias and other flaws, as an AI model's accuracy, fairness, and reliability depend primarily on the data developers use to train them. When training data is diverse, representative, and well-curated, it helps ensure that AI systems produce equitable and accurate results across different demographics, use cases, and environments. Speakers argued that carefully selecting and cleaning training datasets will allow AI developers to mitigate algorithmic bias and produce more robust and reliable AI applications.
- **Insisting on rigorous testing and validation of AI-generated code.** Thorough testing is essential to ensure

that AI-generated code meets high standards for security, performance, and functionality. Developers should use automated security scanners and code review processes to detect potential vulnerabilities or inefficiencies in AI-generated code before they deploy it. Training code generators on high-quality code libraries can also prevent the propagation of insecure or flawed coding patterns that AI models might otherwise replicate.

- **Ensuring human oversight remains a critical component of AI safety and AI security.** Regular auditing and human oversight are critical guardrails that help continuously assess AI behavior and intervene when AI models operate outside ethical or legal boundaries. Similarly, experienced developers should review AI-generated code to spot flaws and apply contextual judgment to ensure it adheres to best practices.

Finally, the 2024 Congress emphasized the need for collaborative efforts to share knowledge and tools and enact a more unified and proactive approach to AI security, particularly in hardening defenses and identifying and addressing emerging threats. By working together, the community can develop and implement AI-specific governance frameworks for developing, deploying, and monitoring secure AI systems. These frameworks would include standards for data provenance, transparency, and accountability, helping to mitigate risks like bias, misinformation, and malicious use of AI. Guardrails and provenance tracking—including ethical guidelines and security controls—will also benefit from shared knowledge and resources, enabling open source projects to set boundaries that prevent bad actors from misusing AI models.

Collaboration is especially critical in building repositories of high-quality training data to fuel the development of open source AI applications. Well-curated datasets will ensure that AI systems are trained on diverse, representative, and accurate information, improving their accuracy, reliability, and fairness. By making these datasets openly available, the open source community can also lower barriers to entry, allowing more developers and

organizations to create robust AI solutions without enduring high data collection and preparation costs.

Looking ahead, the open source community must continue to work together to share knowledge on emerging threats and solutions. Only through collective action can the community maintain a proactive and unified approach to safeguarding AI systems and ensuring that AI is developed and deployed responsibly for the benefit of all.

Securing Open Source Infrastructure

Like other categories of software, OSS is not immune to security vulnerabilities. Flaws can exist in the code, and malicious actors can exploit them when discovered. These vulnerabilities may result from coding errors, lack of updates, or insufficient security reviews. On the other hand, open source also offers advantages for security, such as transparency (allowing anyone to review the code), rapid responses from the community when someone discovers a vulnerability, and the ability to customize and harden software for specific security needs.

During day two of OSC 2024, discussions emphasized the growing attack surface for potential security breaches that come with the widespread adoption of open source software across industries. Speakers noted that attackers have recently targeted the software supply chain, injecting malicious code into widely used open source libraries and components. These attacks can compromise numerous downstream applications that rely on these libraries, triggering potentially catastrophic failures and breaches for organizations that depend on OSS.

An analysis by the Cybersecurity Research Center at Synopsys found that 84% of OSS repositories contain at least one vulnerability, with high-risk vulnerabilities particularly prevalent in critical sectors like the Internet of Things (IoT) and automotive industries.⁶ This alarming

trend underscores the gravity of the situation and the urgent need for enhanced security measures. The analysis also noted that using multiple, outdated OSS versions in projects further complicates security, as many companies continue to use open source software without regularly updating or patching vulnerabilities.

To combat these risks, the Congress called for:

- **Enhanced OSS security monitoring.** With hundreds of thousands of OSS packages in production applications throughout the supply chain, OSS developers and users need more robust mechanisms to disclose potential vulnerabilities and assign responsibility for correcting the problems. Congress participants welcomed the efforts of the Open Source Security Foundation (OpenSSF), which plays a vital role in coordinating efforts to secure OSS and directs resources to unsupported or under-resourced areas.
- **Increased adoption of Software Bill of Materials (SBOM).** The widespread adoption of SBOM would increase transparency and traceability in software development, making tracking and securing open source components easier.
- **Improved security governance in OSS projects.** Congress participants noted that, in many cases, there are no official resource allocations and few formal requirements or standards for maintaining the security of critical open source code. Best practices to mitigate vulnerabilities in software supply chains include defining security requirements early in the software design phase, performing regular security reviews in the production phase, and automating security testing, patching, and compliance auditing once end users deploy the software.
- **Increased funding and participation in collaborative security efforts.** Maintaining the disparate OSS components in use today also requires a more significant deployment of funding and resources from the principal beneficiaries of open

⁶ <https://www.csoonline.com/article/574607/at-least-one-open-source-vulnerability-found-in-84-of-code-bases-report.html>

source infrastructure, especially the world's largest technology companies. Congress participants called for shared responsibility within the OSS and broader technology community to maintain critical OSS infrastructure and address known vulnerabilities.

Securing the Digital Future

Discussions at OSC 2024 emphasized the critical role of cybersecurity in ensuring the safety, trust, and reliability of AI systems and the broader OSS ecosystem. As OSS continues to power critical sectors—from healthcare and finance to transportation and public sector administration—it has become an essential component of global digital infrastructure. However, with this widespread adoption comes the growing responsibility to ensure that OSS remains secure and resilient against evolving threats.

Robust security governance is critical to safeguarding the digital future, as it ensures that OSS foundations and other stakeholders adopt a clear and transparent structure for addressing vulnerabilities that arise in open source projects. Without well-defined governance, the sheer scale and decentralized nature of many open source projects can make it challenging to maintain critical OSS components, leading to neglected security flaws and vulnerable software supply chains. Proactive risk management is equally crucial, allowing organizations to anticipate potential security risks, respond swiftly to emerging threats, and secure their software supply chains from malicious actors. By investing in governance and risk management, the open source community can protect its critical role in global infrastructure, ensuring the continued trust and safety of the digital tools that power our world.

Broader Horizons: From Decentralized Infrastructure to Digital Public Goods

One benefit of the expanded two-day format for the Open Source Congress was the ability to broaden the agenda, highlighting new trends and phenomena critical to the open source community. Two prime examples include the session on digital public goods and the presentation and panel discussion on decentralized infrastructure.

- **Decentralized infrastructure.** The rise of decentralized infrastructure reflects the shift away from centralized control in digital ecosystems, where decentralized technologies like blockchain and Web3 enable more secure, transparent, and user-controlled systems. The Congress provided a platform to explore how decentralized infrastructure can drive innovation, enhance privacy, and reduce reliance on large, centralized tech platforms, which aligns with the values of openness and collaboration at the heart of the open source movement.
- **Digital public goods** are freely available open source technologies and data that promote social and economic development globally. By highlighting digital public goods, the Congress emphasized the role of open source solutions in addressing global challenges such as inequality, climate change, and access to essential services.

Both sessions demonstrate how the Open Source Congress promotes forward-looking ideas and helps ensure the ecosystem remains at the forefront in fusing social and technological innovation.

Digital Public Goods: Open Source for Environmental Sustainability and Social Good

As the world grapples with increasingly complex challenges like climate change, poverty, and inequality, digital public goods have

become vital tools for global progress. Whether open source software, data, or digital infrastructure, these freely available tools invite broader participation and more significant innovation in how the world tackles global challenges. From open source platforms that power climate monitoring systems to tools that improve access to education and healthcare in underserved regions, many consider these digital resources as vital to achieving the United Nations Sustainable Development Goals (SDGs).

Open Source and Environmental Sustainability

Take the critical battle to fight climate change and other environmental challenges. Open source software plays a significant role in promoting environmental sustainability by offering solutions that help reduce resource consumption, enhance energy efficiency, and improve environmental monitoring. For example, open source energy management systems optimize power usage in data centers, smart grids, and homes, significantly reducing energy waste. In agriculture, open source platforms enable precision farming to minimize chemical use, conserve water and increase crop yields.

Open source solutions also power real-time environmental monitoring systems that track pollution, deforestation, and climate change impacts. Governments and environmental organizations harness these data-driven insights to inform investment decisions and policies to accelerate their sustainability efforts. The essential point across each example is that open source makes powerful technologies widely accessible, democratizing access to digital public goods that support sustainability and environmental protection.

Open Source for Social Good

Beyond environmental concerns, affordable and accessible OSS technologies have empowered marginalized communities to participate in the digital economy, access critical services, and enhance education. For example, open source platforms have brought high-quality educational tools to underserved regions, providing access to interactive learning materials and resources previously out of reach.

Digital public goods in the healthcare sector have transformed how researchers and public health officials harness medical data to improve healthcare access and outcomes globally. For example, open source health information systems like District Health Information Software 2 (DHIS2) allow governments and organizations to track and manage public health data in low-resource settings.⁷ Open source solutions and telemedicine platforms have also expanded access to modern healthcare services in remote areas.

Harnessing Global Collaboration to Expand Access to Digital Public Goods

The ultimate takeaway from the OSC 2024 discussion on digital public goods is that open source ethos makes it an ideal vehicle for global cooperation in solving social and environmental challenges. Open source projects thrive on collective problem-solving, with developers, organizations, and communities worldwide contributing to and benefiting from innovative solutions. This collaborative spirit aligns perfectly with the need for a unified global response to climate change, poverty, and inequality, where no single entity has the ingenuity and resources to solve these problems alone.

The next step for digital public goods is building a robust talent and funding pool to scale open source innovations across jurisdictions in need. Indeed, to fully realize their potential, the OSS community needs to cultivate a talent pipeline of developers, researchers, and

policy-makers skilled in open source methods and applying advanced technologies to solving global challenges. The ecosystem will also need funding mechanisms, including public, private, and philanthropic sources, to support developing, deploying, and maintaining new solutions. By building the necessary infrastructure—including human capital and financial resources—the global community can ensure that we maximize the reach and impact of digital public goods. Fortunately, the Open Source Congress raised awareness of how the open source community can contribute to a more equitable and sustainable future for all.

Decentralized Infrastructure: Paving the Way for Digital Autonomy

The Open Source Congress in Beijing provided a unique forum to discuss how open source is central to a significant transformation in the digital landscape, marked by a shift from traditional centralized systems that concentrate control in the hands of a few large corporations or institutions to decentralized infrastructure that empowers individuals and communities. In a compelling keynote and panel discussion, the Congress heard how decentralized systems are changing the fundamental architecture of the digital experience and giving rise to decentralized technologies like blockchain, cryptocurrencies, and peer-to-peer networks that give users more control over their data, assets, identities, and digital interactions.

The Congress also heard how open source has been a driving force behind the decentralized technologies central to the Web3 vision. For example, open source developers worldwide are building and experimenting with decentralized applications (dApps) and protocols to foster innovation in smart contracts, distributed ledgers, and decentralized finance (DeFi), all of which underpin the Web3 movement. More broadly, the Web3 ethos of transparency, autonomy, and distributed ownership resonates with the open source commitment to pursuing more equitable and secure digital ecosystems.

⁷ <https://dhis2.org/>

Has the Internet Taken a Wrong Turn?

The OSC 2024 discussion highlighted how several systemic problems with today's digital experience undermine user trust and contribute to societal issues. One primary concern is the use of addictive algorithms, which maximize user engagement by prioritizing sensational, emotionally charged content. These algorithms keep users hooked but can also foster unhealthy habits, increase polarization, and promote extreme viewpoints. Additionally, the proliferation of bots, which account for nearly 46% of Internet traffic, exacerbates this problem by amplifying misinformation, manipulating discussions, and creating the illusion of consensus on controversial topics.

Mass harvesting of personal data represents another problem where platforms collect vast amounts of user information to target ads and influence behavior. This data collection raises serious privacy concerns and leaves users vulnerable to data breaches and manipulation. Social media is also prone to creating filter bubbles, where platforms serve users content that aligns with their existing beliefs, distorting their perception of reality, reinforcing biases, and deepening social divisions. The spread of misinformation and fake news within these environments further distorts public understanding, making distinguishing between credible information and false narratives difficult. These issues contribute to a digital landscape that skews reality, erodes trust, and fragments public discourse.

Moving Forward with Web3

Web3 may not fully resolve the deep sociological issues present in today's social media platforms, such as addictive behavior, polarization, or the spread of misinformation. Still, it does offer the potential to harness open source technologies to create a better digital experience for users. One such example is LF Decentralized Trust, a new umbrella organization that fosters collaboration and innovation across a growing ecosystem of blockchain, ledger,

identity, interoperability, cryptographic, and related technologies. Launched in September 2024, the initiative is home to hundreds of projects ranging from decentralized identity solutions to data tokenization platforms that will enable a more transparent, secure, and inclusive digital future.⁸

By decentralizing control and giving users ownership over their data and digital identities, LF Decentralized Trust and other Web3 initiatives promise greater privacy, security, and autonomy. Users can choose how their data is shared and used, reducing the mass harvesting of personal information and allowing for more ethical data practices. Decentralized platforms could also weaken the power of centralized algorithms that manipulate content for profit, creating the foundation for a safer, more transparent, and user-centric Internet that prioritizes ethical standards over manipulation and exploitation.

To bring the Web3 vision to life, the OSC 2024 also featured an overview of the Tor project (The Onion Router), a powerful digital privacy solution that embodies the principles of decentralization and user control. Tor allows users to browse the internet anonymously by routing their traffic through a network of volunteer-operated servers, known as nodes, which obscure the user's IP address and location. This system provides radical privacy and security by preventing third parties, including governments, internet service providers, and hackers, from tracking users' online activities or identifying their physical locations.

As a decentralized network, Tor operates without a central authority, meaning no single entity controls the flow of traffic or user data. This configuration makes it highly resistant to censorship and surveillance, which is critical in regions with repressive regimes or for users who require protection from tracking and monitoring. Tor also features onion routing, where traffic is encrypted multiple times and sent through a series of random nodes, ensuring that no intermediary has complete visibility of the user's activity.

⁸ <https://www.prnewswire.com/news-releases/linux-foundation-decentralized-trust-launches-with-17-projects-100-founding-members-302248504.html>

Tor established itself as a cornerstone of the Web3 vision by protecting privacy and enabling secure communications. Its use cases range from safeguarding personal privacy to enabling journalists, activists, and whistleblowers to communicate freely and securely in environments where their safety may be at risk. In essence, Tor demonstrates how Web3 technologies can empower users to take control of their digital lives while promoting a more open, secure, and censorship-resistant Internet.

The Next Evolution of Web3

The next evolution of Web3 will see the rise of decentralized applications that empower users to take control of their digital identities and assets. Decentralized digital wallets are emerging as critical tools that allow individuals to securely store and manage

a range of digital assets, including cryptocurrencies, NFTs, and tokens, without relying on centralized intermediaries. These wallets will also enable self-sovereign digital identities, where users control access to their personal information, such as health records or financial data, and decide how and with whom it is shared.

In healthcare, decentralized platforms will give patients control over their health data, allowing them to share their records with medical providers while maintaining privacy and security. In finance, decentralized asset management platforms will empower users to manage investments, loans, and other financial activities without needing banks or brokers, offering enhanced transparency, security, and autonomy over their financial futures. These emerging applications signal a shift toward a more user-centric digital ecosystem driven by Web3's decentralized infrastructure.

Collaboration Between Open Source Organizations: Building a Sustainable Future

The closing sessions of the 2024 Congress reiterated the critical role of collaboration in building a sustainable open source ecosystem. A significant takeaway was the need for continuous dialogue and cooperation between open source organizations to ensure the community's longevity and resilience. While past efforts to orchestrate ecosystem-wide collaboration have been somewhat ad hoc, there was a strong push for structured, proactive collaboration, particularly in response to emerging regulations.

job of rallying the OSS community to work with the European Commission to modify the proposed regulations in response to the community's concerns. However, as one speaker observed, "We had to scramble. We got it done, but we were on the back foot. We don't want to replicate that experience. We need to be more proactive as a community." The critical point is that it shouldn't take a crisis to unite the community.

Leaders from various organizations discussed the importance of institutionalizing collaboration to address regulatory issues, noting that the CRA will hardly be the last instance of a new regulatory initiative that impacts the OSS community. There were also calls for collaboration on other common challenges, such as fiscal sustainability, workforce shortages, and project governance. For example, participants expressed the need for global cooperation to develop shared infrastructures and promulgate best practices.

Continuing a theme from the 2023 discussions on collaboration, the OSS community called for improvements in addressing its weak points, particularly in project management for complex initiatives. With organizations holding vast experience, it's crucial to build the ecosystem's capacity by sharing talent and best practices.

Companies with their skilled workforces can also pitch in to increase the amount of time their staff developers can spend contributing to open source projects. By identifying common priorities and focusing on collaboration, the OSS community will be better equipped to drive innovation. In this regard, several open source actors, also present during the Congress, joined the Open Regulatory Compliance Working Group, to identify best practices and contribute to standards. As one speaker put it, the community is part of a new model for producing technology, and its collective effort has the potential to revolutionize how we build systems and software, making significant contributions to society.



FIGURE 1: SELECT PRIORITIES FOR INTER-FOUNDATION COLLABORATION

The open source community's response to the European Union's proposed Cyber Resilience Act (CRA) is a case in point. Several participants noted that Open Forum Europe did a commendable

Models of Collaboration

Despite the universal agreement that more collaboration would be beneficial, there was little consensus on the best way to promote cooperation across the ecosystem. The discussions were reminiscent of the dialogue in Geneva, where participants debated three central propositions: an annual Congress, a lightweight peer-to-peer network, and a global secretariat.

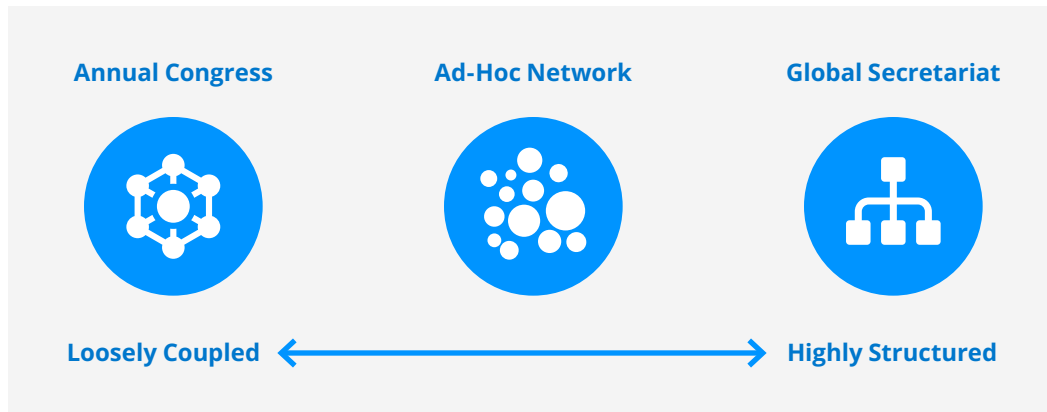


FIGURE 2: A SPECTRUM OF COLLABORATION MODELS.

An annual Congress. For some leaders in the OSS community, a yearly Congress fulfills the primary collaboration needs of the ecosystem by providing a dedicated platform for foundation leaders to share knowledge and plan strategic initiatives. The events in Geneva and Beijing featured lively discussions on critical issues such as sustainability, cybersecurity, technology policy, and the future of open source AI. The annual Congress has demonstrably contributed to building a sense of unity and collective purpose and helped to align diverse organizations around shared goals. The Congress also facilitates networking and peer support, creating partnership opportunities and fostering a more robust and resilient ecosystem.

These benefits notwithstanding, most participants agreed that a once-annual event has limitations when addressing the community's

shared goals and challenges. Critical issues, such as project management, cybersecurity, and policy engagement, often require ongoing attention and timely responses, which a single annual event cannot provide. The gaps between meetings may hinder the ability to maintain momentum on key initiatives, leading to delays in decision-making and substantive progress in critical deliverables. Additionally, the fast-paced nature of open source development means that new challenges and opportunities arise frequently, requiring more continuous dialogue and coordination. Without regular engagement, the community may struggle to address emergent issues, share evolving best practices, or capitalize on collaborative innovations. To sustain effective collaboration, many Congress participants called for more frequent touchpoints and continuous processes to keep the community aligned and on track to address critical challenges.

A lightweight, peer-to-peer network. Congress participants expressed a strong desire to sustain momentum between Congresses, and some felt that a network of OSS foundation executive directors—or, in some instances, a peer group of policy leads—would be sufficient to enhance collaboration and facilitate more frequent touchpoints. OSS leaders favoring a lightweight approach to ecosystem collaboration were skeptical of the benefits of establishing a new global entity requiring a significant investment in people and infrastructure. They noted that there are already several meta-organizations in the ecosystem. Moreover, they placed faith in the capacity of existing OSS foundation leaders to come together at regular intervals, identify shared priorities, and establish working groups to distribute responsibility for managing collaborative efforts.

Those who doubt the peer-to-peer model warned that the day-to-day grind to deliver on existing mandates could sideline inter-foundation cooperation. While there is no shortage of good intentions regarding the need to deepen collaboration, they noted that a lack of funding and executive bandwidth for collaborative efforts could delay or inhibit progress in addressing collective, ecosystem-wide challenges.

A global secretariat for open source. As in Geneva, several Congress participants made a case for a new global secretariat for the open source community. Proponents for a new global entity noted that most industries have international associations that produce collective goods and advocate on behalf of their membership. The open source community, on the other hand, has a large and diverse collection of regional, sector-based, and project-based foundations that cater to the needs of their unique constituents. As a result, participants argued the ecosystem needs an overarching structure or organization to advance the community's shared interests. One participant suggested that today's ad hoc approach leaves many practical matters and questions unsettled, such as which organization will take responsibility for advancing work on common objectives. Who will find and deploy the resources required to execute shared projects successfully? Which organization should serve as a point of contact for policymakers when it comes time to provide input into new regulatory initiatives?

In 2023, Congress participants debated whether it would be possible to thrust an existing organization into a global stewardship role on behalf of the community. However, established OSS foundations have well-defined mandates and resources to deliver against the priorities identified by their member organizations. As such, participants concluded that existing OSS organizations have not been equipped, funded, or mandated by their governing bodies, to play a larger global coordinating and advocacy role for the ecosystem as a whole.

In 2024, several speakers floated an alternative proposal to create a new international secretariat with a mandate to serve the entire ecosystem. They depicted an organization that is genuinely global and representative with deep policy expertise and a neutral positioning. Just as international bodies like the ITU, GSMA, and IEEE do not replace or absorb their national constituent members, they argued that a new global secretariat for the OSS community would not usurp the funding or diminish the relevance of existing organizations. "We need a growth mindset," said one speaker. "Just

because we create a new organization does not mean we reduce the resources available to existing organizations."

Among the dissenters were those who observed that inter-foundation collaboration comes with challenges including significant costs in staff time and other resources that foundations must absorb at the expense of other vital priorities. Several participants also argued that collaboration and consensus-building are only sometimes the best ways to address the ecosystem's challenges. As one speaker observed, "We need to be more specific about where cooperation is mission critical and where we should encourage a diversity of approaches and even competition. Collaboration or cooperation does not mean we give up our independence. We don't have to agree on everything. We can benefit from our diversity."

It was evident by the conclusion of the discussions in Beijing that participants needed further conversations to define the best path for structuring ecosystem-wide collaboration. In the short term, Congress participants said that sustaining momentum was critical. Several suggested that a series of inter-foundation working groups equipped with simple tools for collaboration could make progress on issues such as cybersecurity, regulation, and open source AI.

The Future of the Open Source Congress

Another central theme in the closing stages of OSC 2024 was the future of the Congress itself. Panelists and attendees agreed that the OSC must evolve from an annual event into a continuous, process-driven initiative that fosters global collaboration year-round. Some Congress participants proposed using the Congress to develop and endorse position papers to present policymakers and regulators. Others said the Congress provides an invaluable opportunity for unstructured conversations, informal networking, peer-to-peer engagement, and the airing of diverse perspectives in a safe environment.

The OSC also explored potential focus areas for future editions, including environmental sustainability, open source AI,

organizational governance, and the need for structured leadership, collaboration, and financing to sustain OSS projects and organizations. Congress participants want to maintain Chatham House rules to encourage candid conversations. There was also support for inviting new voices and broadening participation in future editions of the Open Source Congress.

Proposals to bolster the Congress's sustainability included creating a neutral, transparent body to run an annual event and ensure that discussions and initiatives maintain momentum between gatherings. In the meantime, the Eclipse Foundation offered to host the 2025 Congress in Brussels, further solidifying the event as a pivotal platform for the open source community.

Conclusion: Charting a Path Forward

The Open Source Congress 2024 was a landmark event that addressed critical challenges and opportunities in the open source ecosystem. From the rapid rise of AI to the need for better security frameworks and the promise of digital public goods and decentralized infrastructure, the Congress provided a unique platform for fostering collaboration, innovation, and global inclusion. The key takeaways are as follows:

- **OSC 2024 demonstrated how open source AI can help balance innovation and responsibility in deploying AI solutions.** Open source platforms have democratized access to AI tools, driving innovation across sectors like healthcare, finance, and transportation. However, Congress participants emphasized the need for responsible AI development, focusing on transparency, fairness, and explainability to ensure ethical practices and reduce the risk of bias in AI systems. Open AI frameworks, such as the Linux Foundation's Model Openness Framework (MOF) and the Open Source Initiative's Open Source AI Definition, are crucial in defining and promoting responsible AI practices.
- **OSC 2024 surfaced vital challenges and opportunities for scaling open source AI.** Open source AI projects face significant challenges competing with proprietary models, particularly considering the high costs and specialized expertise required. Suggestions for overcoming these barriers include focusing on smaller, specialized models that address niche use cases, building an open data commons to provide accessible, high-quality data, and leveraging public funding and partnerships to support open AI projects. These strategies can help the open source community remain competitive and foster community-driven AI innovation.
- **OSC 2024 stressed the urgent need for enhanced OSS security measures.** Vulnerabilities in open source repositories

and software supply chains can lead to catastrophic breaches, emphasizing the need for better security governance, ongoing maintenance, and vulnerability monitoring. To address these risks, the Congress called for enhanced security measures, including improved monitoring, the adoption of Software Bill of Materials (SBOM) for transparency, more robust security governance in OSS projects, and increased funding and collaboration from major tech companies as well as end user organizations to secure OSS infrastructure. These efforts are crucial to safeguarding the global digital infrastructure powered by OSS.

- **OSC 2024 showcased why decentralized infrastructure and digital public goods represent high-value opportunities for scaling open source innovation.** Decentralized infrastructure and Web3 technologies are reshaping the digital landscape by harnessing open source solutions to reduce reliance on centralized platforms and empower users with more control over their data, privacy, and digital interactions. Open source is also integral to digital public goods that improve access to healthcare and education in underserved regions and address global challenges such as climate change and financial inclusion. OSC 2024 concluded that decentralized technologies and digital public goods hold significant potential to scale the impact of open source solutions and accelerate progress towards a more equitable and sustainable future. Critical next steps for maximizing this potential include building a talent pipeline, securing funding, and fostering collaboration across OSS organizations.
- **OSC 2024 crystallized the community's consensus on the need for institutionalized collaboration.** The open source community recognizes the importance of pooling the ecosystem's knowledge and resources to address shared challenges like regulatory compliance, cybersecurity, and

fiscal sustainability. The ad hoc cooperation that characterized the community's response to the European Union's Cyber Resilience Act, while ultimately effective, highlighted the need for a more structured approach to ensuring the ecosystem's resilience and longevity.

- **OSC 2024 highlighted the need for ongoing discussions on the appropriate community-wide collaboration models.**

There is ongoing debate within the open source community about how best to formalize collaboration. Suggestions include continuing the annual Congress, establishing peer-to-peer

networks, and creating a permanent global secretariat. Each model has its proponents and challenges. However, the inability to achieve consensus on the best way forward at OSC 2024 underlined the need for further dialogue among community leaders.

As the open source community grows and diversifies, the take-aways from OSC 2024 will shape future efforts to ensure that open source technology remains an inclusive, secure, and sustainable force for innovation in the digital world.

Acknowledgments

The author would like to acknowledge the contributions of the open source community leaders who gathered in Beijing and whose insights and commentary inspired this report. I am grateful to Chris Xie at Futurewei, whose leadership and contributions made the Open Source Congress possible, to the Open Atom team for hosting an inspiring event, and to the Linux Foundation for publishing this report. I would also like to offer special thanks to those who took the time to review early drafts and provided valuable advice and insights, including Gael Blondelle, Deborah Bryant, Hilary Carter, Stefano Maffulli, and Enzo Ribagnac.

About the Author

Anthony is the founder and president of the DEEP Centre and an internationally recognized authority on the digital revolution, innovation, and creativity in business and society. He is co-author (with Don Tapscott) of the groundbreaking bestseller *Wikinomics* and its follow-up *Macrowikinomics: New Solutions for a Connected Planet*.

Among other appointments, Anthony serves as a research director with the [Blockchain Research Institute](#), an expert advisor to the [Markle Foundation](#)'s Initiative for America's Economic Future, and a senior fellow with the [Lisbon Council](#) in Brussels. Anthony was recently a committee member of the National Research Council's Committee on [Science for the EPA's Future](#), a visiting fellow with the [Munk School of Global Affairs](#) at the University of Toronto, and chief advisor to Brazil's Free Education Project. His work on technology and innovation has been featured in publications such as the Harvard Business Review, the Huffington Post, and The Globe and Mail.

Appendix: List of Open Source Congress 2025 Participating Organizations

CCF ODC

China Academy of Information and Communications Technology
(CAICT)

DEEP Centre

Digital Asia Hub

Digital Public Goods Alliance

Eclipse Foundation

KAIYUANSHE

Linaro Limited

Linux Foundation

Linux Foundation AI & Data

Linux Foundation Research

Open Infrastructure Foundation

Open Invention Network

Open Source Initiative

OpenAtom Foundation

OpenChain

OpenDigger Community

OpenWallet Foundation

OWASP

Rust Foundation

Shanghai Opensource Information Technology Association

Software Heritage Foundation

The Tor Project

Web3Infra Foundation



Futurewei maintains ongoing, in-depth collaboration with forward-thinking companies worldwide. We pursue openness in research and development by embracing an open innovation model and striving to share ideas and knowledge with technology communities to create new business opportunities.

Our vision is Shaping the Future Toward a Fully Connected, Intelligent World. Our mission is Developing Innovations to Benefit an Intelligent and Digital Society via Open Source, Standardization, and Collaboration within Ecosystems.

Our experts have actively engaged in standards programs for the past two decades. Through this work, we participate in developing next-generation wireless technologies and networks and building open ecosystems through open application platforms for ICT systems.

www.futurewei.com



Founded in 2021, [Linux Foundation Research](#) explores the growing scale of open source collaboration, providing insight into emerging technology trends, best practices, and the global impact of open source projects. Through leveraging project databases and networks, and a commitment to best practices in quantitative and qualitative methodologies, Linux Foundation Research is creating the go-to library for open source insights for the benefit of organizations the world over.



Copyright © 2024 The Linux Foundation


This report is licensed under the [Creative Commons Attribution-NonCommercial 4.0 International Public License](#).

To reference this work, please cite as follows: Anthony Williams, "Open Source Congress 2024: Shaping the Future of Collaboration in AI, Security, and Digital Public Goods," foreword by Chris Xie and Yue Chen, The Linux Foundation, December 2024.

 twitter.com/linuxfoundation

 facebook.com/TheLinuxFoundation

 linkedin.com/company/the-linux-foundation

 youtube.com/user/TheLinuxFoundation

 github.com/LF-Engineering