

Software

Transparency Foundation Charter

Fundación para la Transparencia del Software

Madrid, October 1st, 2021

“The vision of the Software Transparency Foundation is a frictionless exchange of validated and related Software Bills of Materials (SBOM) throughout the software supply chain”

Mission

Our mission is to “bring transparency to the software supply-chain” with a goal of harmonizing how information is shared about the software that we build, acquire, and operate.

Our focus will be on operationalizing existing and emerging standards like SPDX and ISO/IEC 5230 using open source tooling and data, and technologies to facilitate generating, notarizing, relating and validating Software Bills of Materials (SBOM).

Driving adoption of SBOM

By providing Open Source tools for generating, notarizing, relating and validating Software Bills of Materials (SBOM), we will facilitate broad adoption. This will ease Software Supply Chain traceability, drastically reducing open source-related cybersecurity and license compliance effort.

The Software Transparency Foundation will provide a complete set of open source Software Composition Analysis (SCA) and other tools, which otherwise are out of reach for small and mid-sized organizations.



Enabling a decentralized validating entity

The Software Transparency Foundation proposes to enable a decentralized SBOM Ledger to allow public validation of SBOMs by comparing their cryptographic checksums published in a blockchain, along with their date stamps and relationships to preceding SBOMs.

A decentralized, immutable SBOM Ledger will contribute to completeness of visibility in the supply chain.

Facilitating SBOM interoperability

The Software Transparency Foundation aims at solving the traceability issue of software components across the supply chain tree, without any depth limitation.

It proposes, amongst others, a decentralized SBOM ledger that will offer a format-agnostic registry of Software Bills of Materials and their relation to their parents. This allows easily tracing and validating software components across the supply chain, regardless of the format in which the SBOM document is generated.

Membership & Sponsorship Programs

The Software Transparency Foundation offers five sponsorship programs: Diamond, Gold, Silver, Bronze and Community

Diamond and Gold sponsors are members of the Governing Board .

In exceptional cases, the Governing Board will consider offers of relevant intellectual property, labor, and other resources as ‘payment in kind’ towards an annual sponsorship.

All sponsors are entitled to participate in project meetings, and to identify their company/community as sponsors of the Software Transparency Foundation.



The Community Member category of membership is limited to non-profits, open source projects and individuals, and requires approval by the Governing Board, or, if the Governing Board sets criteria for joining as an Community member, the meeting of such criteria.

Non-Community sponsors have access to the SBOM Ledger application with a number of prepaid transactions defined for every type of Sponsorship Program.

The Governing Board shall amend/adopt the Sponsorship Program and publish it on the Software Transparency Foundation website.

Open Governing Board

The Governing Board voting members shall consist of one representative appointed from each Platinum or Gold Member and the Steering Committee Chair.

The Governing Board responsibilities consist of:

- Approving the budget to direct the use of funds raised from all sources of revenue
- Electing a Chair of the Project to preside over meetings, authorize expenditures approved by the budget and oversee operations
- Voting on decisions or matters before the Governing Board
- Overseeing all Project business and marketing matters
- Adopt and maintain policies or rules and procedures for the Project as appropriate, such as a Code of Conduct, a trademark policy and any compliance or certification policies.

Governing Board meetings shall be limited to the Governing Board representatives, the Director (if any), and invited guests and follow the requirements for quorum and voting outlined in this Charter. The Governing Board may decide whether to allow one named representative to attend as an alternate.

The Governing Board meetings shall be confidential unless approved by the Governing Board. The Governing Board may invite guests to participate in consideration of specific Governing Board topics (but such guests may not participate in any vote on any matter before the Governing Board). The Governing Board should encourage transparency, including the public



publication of public minutes within a reasonable time following their approval by the Governing Board.

Steering Committee

It is anticipated that the Steering Committee will meet monthly and will include work teams, as may be created by the Steering Committee, reporting up to the Steering Committee.

Participation on the Steering Committee and its work teams is open to all interested parties.

The Director, if any, shall be entitled to observe all meetings of the Steering Committee and any work team meetings on a non-voting basis.

The voting members of the Steering Committee shall consist of:

- One appointed representative from each Platinum Member
- Each work team lead, as such may be determined pursuant to procedures decided upon by the Steering Committee with approval of the Governing Board
- One elected representative from the Community Members

The Steering Committee shall be responsible for:

- Development, management and updating of the Software Transparency Foundation SBOM Ledger
- Appointment of a Chair to preside over meetings and to serve on the Governing Board
- Such other activities as the Governing Board may assign to the Steering Committee

Outreach Committee

The voting members of the Outreach Committee shall consist of one appointed representative from each Platinum Member.

The Outreach Committee shall be responsible for designing, developing and executing efforts to build a Software Transparency Foundation ecosystem throughout relevant supply chains on behalf of the Governing Board and in collaboration with the Governing Board, and shall appoint a chair to preside over meetings of the Outreach Committee.



The Director, if any, shall be entitled to observe all meetings of the Outreach Committee on a non-voting basis.

Voting

While it is the goal of the project to operate as a consensus based community, if any decision requires a vote to move forward, the representatives of the Governing Board, Steering Committee, or Outreach Committee, as applicable, shall vote on a one vote per voting representative basis.

Decisions by vote shall be based on a majority vote, provided that at least sixty percent (60%) of the Governing Board, Steering Committee, Outreach Committee or other committee representatives, as applicable, must be either present or participating electronically or by written action in order to conduct a valid vote.

In the event of a tied vote with respect to an action by the Governing Board, Steering Committee, Outreach Committee or other committee created by the Governing Board, the chair of such board or committee shall be entitled to submit a tie-breaking vote.

Any matter that is not resolved in either the Steering Committee or Outreach Committee may be submitted by the respective Chair of that Committee to the Governing Board for resolution.

Any matter that is not resolved in a work team may be submitted by a work team member to the respective Committee under which that work team was formed.

The Governing Board may designate officer positions within the Project and set procedures for the conducting of the election of the Community Member representative to the Steering Committee and the election of any officer or other position within the Project.

Code of Conduct

The Governing Board shall define and adopt a code of conduct.



Budget

The Governing Board shall approve an annual budget and commit to never spend in excess of funds raised.

The annual budgeted spend shall be shaped substantially according to the following framework:

- Research and development 50%
- Outreach (mostly marketing) 30%
- Other 20%

The Governing Board shall adjust the framework from time to time based on the needs of the project.

The Governing Board shall provide quarterly reports of spend levels against the budget.

Intellectual Property Policy

All documentation will be received and made available by the Project under the Creative Commons Zero License version 1.0 Universal (CC0 1.0)

Amendments

This charter may be amended by a super majority vote of all Governing Board members.