Hyperledger Ursa (EOL)

Hyperledger Ursa was moved to end of life status at the request of the maintainers on 27 APR 2023. You are welcome to use and contribute to this code, although the maintainers may or may not be responsive to any questions you have. You would also be welcome to help reactivate this project if you are interested in continuing development of this code.

<table>
<thead>
<tr>
<th>Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>HYPERLEDGER URSA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>END OF LIFE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CII Badge</td>
<td>blocked URL</td>
</tr>
<tr>
<td>Description</td>
<td>A shared cryptographic library that enables people (and projects) to avoid duplicating cryptographic work across projects, increasing security in the process.</td>
</tr>
</tbody>
</table>

Hyperledger Ursa is a shared cryptographic library that would enable people (and projects) to avoid duplicating other cryptographic work and hopefully increase security in the process. The library would be an opt-in repository for projects (and, potentially others) to place and use crypto.

Key Characteristics

As Hyperledger has matured, the individual projects within Hyperledger have started to find a need for sophisticated cryptographic implementations. Rather than have each project implement its own cryptographic protocols, we think it would be more desirable to collaborate on a shared library. There are many reasons to do this:

- **Avoiding duplication:** crypto implementations are notoriously difficult to get correct (particularly when side channels are taken into account) and often require a lot of work in order to complete with a high level of security. The library would potentially allow projects to share crypto implementations, avoiding unnecessary duplication and extra work.
- **Security:** having most (or all) of the crypto code in a single location would substantially simplify doing a security analysis of the crypto portion of Hyperledger. In addition, the lack of duplication would mean that maintenance would be easier (and thus, hopefully, security bugs would be less numerous). People might also be less likely to "roll their own crypto" if there are easily accessible implementations.
- **Expert Review:** in addition, the ability to enforce expert review of all cryptographic code should increase security as well. There has already been at least one substantial bug in a Hyperledger DLT platform at a cryptographic algorithm level. We think that having a concentration of cryptographic experts in Hyperledger will help us minimize the risk of this in the future.
- **Cross-platform interoperability:** if two projects use the same crypto libraries, it will simplify (substantially in some cases) cross-platform interoperability, since cryptographic verification will involve the same protocols on both sides.
- **Modularity:** this could be the first common component/module and a step towards modular DLT platforms, which share common components. While we have already outlined most of the advantages this modularity would bring in terms of actual functionality, a successful crypto library could encourage and push forward more modular activities.
- **New Projects:** it would be easier for new projects to get off the ground if they had easy access to well-implemented, modular cryptographic abstractions.

Documentation

- Motivation

Project Management

- Ursa JIRA

Repositories
Communication

Mailing List

- ursa

Chat (for questions and ephemeral discussions)

Questions are welcome and best asked in Hyperledger Discord. Learn more about Hyperledger Discord here, get the invite and check out one of the many Ursa project channels.

Meeting

- Meetings happen every other week on Wednesdays at 7:00 AM Pacific Time.
  - The most recent meeting was on January 9th, 2019.
  - The next meeting will be on January 23rd, 2019.
- Meeting recordings can be found in the "Meeting Agendas and Notes" tab. Some (very old) previous meeting recordings can be found here.

Agendas

- 2022 Agendas
- 2021 Agendas
- 2020 Agendas
- 2019 Agendas

Notes

- 2022 notes
- 2021 notes
- 2020 notes
- 2019 notes

History

- Proposed by
  - Hart Montgomery, Fujitsu
  - Dave Huseby, The Linux Foundation
  - Nathan George, Sovrin Foundation
  - Dan Middleton, Intel
  - Mic Bowman, Intel
  - Manu Drijvers, DFINITY
  - Jan Camenisch, DFINITY
  - Binh Nguyen, State Street
  - Angelo De Caro, IBM
  - Amit Kumar Gupta, Sai Infratel
  - Vipin Bharathan
  - Shawn Amundson, Bitwise.io
- Approved by the TSC on 2018-11-01

TODO

- Nathan George Document the road mapping process using JIRA and Confluence and what needs to be done.
- Create a rough draft of the RFC process for Ursa.
- Create a rough draft of the selection criteria and checklist for adding new dependencies to Ursa
Recent space activity

Ry Jones
Hyperledger Ursa (EOL) updated Aug 10, 2023 view change

David Boswell
Hyperledger Ursa (EOL) updated Apr 27, 2023 view change

2022 Agendas created Apr 24, 2023
2021 Agendas created Apr 24, 2023
2020 Agendas created Apr 24, 2023

Space contributors

- Ry Jones (360 days ago)
- David Boswell (465 days ago)
- Bruno Hivert (737 days ago)
- Sean W. Bohan (758 days ago)
- Cam Parra (844 days ago)
- ...