Hyperledger Ursa

Project	
Status	INCUBATION
CII Badge	
Description	A shared cryptographic library that would enable people (and projects) to avoid duplicating other cryptographic work and hopefully increase security in the process.

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

- ursa

- ursa-rfc
- ursa-docs

Communication

Mailing List

- ursa

Chat (for questions and ephemeral discussions)

- #ursa

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

- 2019-01-23 Agenda
- 2019-02-05 Meeting Agenda:
- 2019-02-20 Meeting Agenda
- 2019-03-06 Meeting Agenda
- 2019-03-20 Meeting Agenda
- 2019-04-03 Meeting Agenda
- 2019-04-17 Meeting Agenda
- 2019-05-01 Meeting Agenda
- 2019-05-14 Meeting Agenda
- 2019-05-29 Meeting Agenda
- 2019-07-09 Meeting Agenda
- 2019-07-24 Meeting Agenda
- 2019-08-07 Meeting Agenda
- 2019-08-21 Meeting Agenda
- 2019-09-04 Meeting Agenda
- 2019-09-18 Meeting Agenda
- 2019-10-02 Meeting Agenda
- 2019-10-16 Meeting Agenda
- 2019-10-30 Meeting Agenda
- 2019-11-13 Meeting Agenda
- 2019-12-10 Meeting Agenda

Notes

- 2019-03-20 Meeting Notes
- 2019-04-03 Meeting Notes
- 2019-04-20 Meeting Notes
- 2019-05-01 Meeting Notes
- 2019-05-14 Meeting Notes
- 2019-05-29 Meeting Notes
- 2019-07-10 Meeting Notes
- 2019-07-24 Meeting Notes
- 2019-08-07 Meeting Notes
- 2019-08-21 Meeting Notes
- 2019-09-04 Meeting Notes
- 2019-09-18 Meeting Notes
- 2019-10-02 Meeting Notes
- 2019-10-16 Meeting Notes
- 2019-10-30 Meeting Notes.
- 2019-11-13 Meeting Notes
- 2019-12-11 Meeting 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.
- [x] Create a rough draft of the RFC process for Ursa.
- [x] Create a rough draft of the selection criteria and checklist for adding new dependencies to Ursa

Recent space activity

Hart Montgomery

2019-12-11 Meeting Notes updated Dec 11, 2019 • view change

2019-12-10 Meeting Agenda created Dec 11, 2019

2019-11-13 Meeting Notes created Nov 13, 2019

2019-11-13 Meeting Agenda created Nov 13, 2019

2019-10-30 Meeting Notes. created Oct 30, 2019

Space contributors

- Hart Montgomery (38 days ago)
- Dan Middleton (80 days ago)
- Jon Geater (134 days ago)
- Lovesh Harchandani (164 days ago)
- Mike Lodder (192 days ago)
- ...