2019 Q4 Hyperledger Ursa

Project Health

Ursa is moving forward, slowly but surely. We released another version 0.2.0–since the last update.

Projects: Ursa is currently the only crypto library in use for Indy-SDK (i.e., the Indy crypto library is no longer used in this case) and Indy maintainers and contributors are working towards using Ursa for all of their cryptography. We have also been recently notified that an intern has completed work on integrating Ursa into Iroha, which is more good news (this was done by the Iroha team, so they deserve the credit here–not us) (https://github.com/hyperledger/iroha/commit/b3adc310e9c797c9dd5c99e4a7b518f2c5cf50f0).

Ursa added more FFI functionality so Indy can adopt Ursa for their ledger codebase. Iroha is officially using Ursa now.

Questions/Issues for the TSC

While this is more for project maintainers than the TSC (although the overlap is heavy), we'd like to use this time to ask maintainers of projects that aren't currently using Ursa what kind of features would convince them to use Ursa. The more feedback we get, the better we can do as a project.

The issue of the lack of dunking booth funding is also deeply concerning to us, although we recognize that this is a governing board issue rather than a TSC issue.

Releases

We made one release since the last update:

v0.2.0: Oct 2

This release added some ZKP based signatures.

Overall Activity in the Past Quarter

New Code:

1. BBS+ Signatures
2. Pointcheval Sanders Signatures for threshold issuace.
3. Groth Signatures for delegatable credentials
4. Encryption Code has been implemented for symmetric cryptography – AES-CBC-HMAC, AES-GCM, and XCHACHA20-POLY1305

New RFCs:

1. z-mix are in the pipeline.

Current Plans

We have a lot of work in progress, both in our base crypto library and in our zero knowledge-focused zmix library. Some things include:

1. Crypto - Public Key crypto common interface
2. Hardware - Common interface for talking and using HSM, TEE, and TPMs.
3. Implement ZMix for generating and verifying proofs.
4. Release Ursa 0.3.0 before the end of the year.

Maintainer Diversity

Current active maintainers

- Mike Lodder (Sovrin Foundation)
- Lovesh Harchandani (Evernym Inc.)
- Brent Zundel (Evernym Inc.)
- Dave Huseby (Linux Foundation)
- Hart Montgomery (Fujitsu)
- Dan Middleton (Intel)
- Cam Parra (Kiva)
- Dan Anderson (Intel)
- Jon Geater (Jitsuin)

Contributor Diversity

Our contributor list has been relatively static, although we are optimistic of adding new contributors in the near future (e.g., for hardware support).

Current Contributors

- Sovrin Foundation
- Evernym, Inc
- Intel
- Bitwise
- Anonyome Labs, Inc.
- IdentOS
- Jitsuin
- Fujitsu

Additional Information

Reviewed by

- [ ] Angelo De Caro
- [x] Arnaud J Le Hors
- [ ] Christopher Ferris
- [x] Dan Middleton
- [ ] Gari Singh
- [x] Hart Montgomery
- [x] Mark Wagner
- [x] Nathan George
- [ ] Swetha Repakula
- [x] Tracy Kuhrt
- [x] Troy Ronda