

# 2019-09-23 Indy Contributors Call

## Summary

- Updates on releases and work projects
- Ubuntu 18.04 for Indy Node
- Future of Apache Milagro
- Fuzzing LibIndy
- Dealing with old pull requests

Timezone: US morning and Europe afternoon

We intend to record this call.

Remember the [Hyperledger Code of Conduct](#)

## Anti-Trust Policy

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at <http://www.linuxfoundation.org/antitrust-policy>. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

## Attendees

- Name (organization) <email>
- [Richard Esplin](#) (Evernym) <[richard.esplin@evernym.com](mailto:richard.esplin@evernym.com)>
- Axel Nennker
- [Cam Parra](#) (Kiva) [camilop@kiva.org](mailto:camilop@kiva.org)
- [Matt Raffel](#) (Kiva) [mattr@kiva.org](mailto:mattr@kiva.org)

## Announcements

- Hyperledger Meetup in Belgrade
- [Internet Identity Workshop](#) — want to coordinate demos
- Bootcamp Russia: [Event Location](#)
- Hyperledger [Maintainers Summit](#): Minneapolis October 8-10
- Aries Workshop/Connectathon December 3-5 in Provo, Utah (details to follow)

## Summary of Prior Call

### Release Status

- Indy Node
  - September: 1.10.0
    - Refactoring for PBFT View Change and BLS signature
    - Bug fixes
    - Indy Node and Indy Plenum support for Ubuntu 18.04 is at risk for September
  - October: 1.11.0
    - PBFT view change
- Indy SDK
  - September: 1.12.0
    - Fully qualified DIDs
    - Platform Updates: MacOS, CentOS
  - Future
    - GitLab migration alongside Jenkins (Foundation)?
    - Aries / Indy split: next step is aries-core-wallet
    - Anoncreds 2.0 (Sovrin Foundation, BC.gov?)
- Ursa
  - September: 0.2.0
    - ZKP / ZKLang improvements
    - Debian packages
    - Encryption for Anoncreds 2.0
    - Refactor multi-signature BLS in addition to aggregated signature
- Aries
  - Lots of progress on language libraries, frameworks, and agents.

- Indy Catalyst
  - Production deployment testing: volume loads.
  - Won't go live in production at BC.gov until October.
  - Not yet migrated to Hyperledger. Needs more documentation.

## Work Updates

- Documentation improvements: Michael B and Stephen C
  - Need to review and prune out-of-date documentation (Alice / Faber treatment of pairwise DIDs is a key pain point)
  - Michael is working on Indy Agent walkthrough using C#
  - Finishing work on ReadTheDocs (2 more weeks?)
  - Cloud Compass is building the Linux Foundation EdX courses for Indy and Aries
- SDK 2.0 architecture / Indy-Aries split (Sergey)
  - Kiva is working on a Futures implementation of threading (instead of call-backs) (<https://github.com/kiva/aries-sdk.git>)
- CI / CD: GitLab migration (Mike and Steve G)
  - Demos in the Identity Implementers WG calls
  - Hyperledger is also evaluating Azure Pipelines
- Advanced Schemas and W3C creds (Ken)
  - Can successfully write and retrieve the Context object from the node code. Will track through all layers up to Aries.
    - <https://github.com/ken-ebert/indy-node/commits/master>
  - 5 additional objects need to be added.
  - Working on the HIPE for the new Schema object.
- Warnings from rust cargo clippy (Mike and Axel)
  - IS-1270 through IS-1274
- New design for revocation / Anoncreds 2.0 (Mike)
  - Would be useful to have a comparison in performance between Anoncreds 1.0 and Anoncreds 2.0
  - First draft is latex document in Ursa repo. Will be published as PDF and HTML.
    - <https://github.com/hyperledger/ursa-docs/tree/master/specs/anoncreds2>
  - Need a plan for changes to Indy Node
    - HIPE for overall changes, then a design PR for the changes specific to the different repos.
      - <https://github.com/hyperledger/indy-node/tree/master/design>
- Getting Ursa artifacts published that can be used by Indy Node and Indy SDK (Mike and Cam)

## Other Business

- Future calls:
  - Cancel the call September 30 for IIW
  - Cancel the call October 14
- Ubuntu 18.04 on Indy Node
  - Want to support 18.04 and 16.04 simultaneously (until 20.04 comes out).
  - Cam has a PR, and is working on incorporating feedback.
- Security reports
- Ursa and AMCL: Ursa will provide an AMCL crate, but no timeline yet.
- fuzzing libindy <https://github.com/AxelNennker/indy-sdk/tree/fuzzing/>

```
`cargo +nightly fuzz run fuzz_target_1 -- -only_ascii=1`
Worried about unsafe code in libindy
...

ignisvulpis@namenlos:~/development/hyperledger/indy-sdk/libindy$ find src -name '*.rs' -exec fgrep unsafe {} \; | wc -l
61
...

```

  - Should be testing deeper: can we pass unexpected values across the unsafe boundary? Should do more fuzzing. Would make a good internship.
  - It looks bad. Some unsafe code is required to have a C-API. FFI support doesn't really help.
  - Mike wants to review the 61 cases and figure out if they are justified.
- Fully Qualified DID support in Indy SDK: [Evernym demo video](#).
- Handling pull requests.
  - How to handle old pull requests that failed DCO Checks? Close?
    - Closing the PR doesn't get rid of the work. The author can reopen at any time.
  - How to handle pull requests for IOS / Swift wrappers? Close and encourage the move to Aries?
  - How to handle pull requests for LibVCX? Deprecate?
  - Close PR <https://github.com/hyperledger/indy-sdk/pull/1048> as something that will be replaced by the advanced schema work?
  - HIPE pull requests: <https://github.com/hyperledger/indy-hipe/pulls>
  - Kyle will continue reviewing PRs, but does not want to be a bottleneck slowing down the process.
  - Would be best to put in a comment notifying the author of our intention to close in 1-4 weeks.

## Future Calls

- Non-secrets in the Indy Wallet
  - Cam is working on pluggable crypto. They wallet shouldn't decide what encryption you should be using.
  - Use cases where we would want to move keys between wallets
    - Moving the link secret / credential data from one device to another (synchronized storage).
    - Debug use cases
    - Richard's hit other uses cases that were better solved with DID Doc, pre-signing, signing API.
  - Work-around with the web-crypto API
- Define pull request review process for Indy Node.
  - Should define the process, including how we handle exceptions (emergency fixes shouldn't be blocked, but would require notification)

- What is important in a good review?
- If a review must be skipped, should note it in the Git commit message.

## Action items

- ☐ HIPE #138, Issue #144 (Ken and Brent)
  - Create a PR for changing status to ACCEPTED
  - Check for an Aries RFC
- ☐ PR to RFC #0019 to compare pack/upack to msgpack (Sergey)
- ☐ Richard and Sergey will close old pull requests with a descriptive comment.
- ☐ Mike wants to review the 61 cases of "unsafe" libindy calls and figure out if they are justified.

## Call Recording

Call was not recorded due to a problem with Zoom permissions.