

2019-08-26 Indy Maintainers Call

Summary

- Release updates
- Moving the PostgreSQL wallet out of experimental
- Proposal to improve performance of the Indy SDK CI test pipeline
- Proposal to support Fully Qualified DIDs

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>
- [John Jordan](#) (Province of British Columbia)
- Ian Costanzo (Anon Solutions)
- [Cam Parra](#) (Kiva) <camilop@kiva.org>
- Alexander Shcherbakov (Evernym) <alexander.shcherbakov@evernym.com>
- [Ken Ebert](#) (Sovrin Foundation) <ken@sovrin.org>

Announcements

- Hyperledger voting is about to happen. Make sure you have received an invitation to hyperledger-contributors mailing list to get voting instructions.

Summary of Prior Call


Release Status

- Indy Node
 - August: 1.9.2
 - Bug fix release
 - Important bug fix for ledger corruption INDY-2211
 - September: 1.10.0
 - PBFT view change
- Indy SDK
 - August: 1.11.1
 - Finish Authors vs Endorsers
 - Finish proof of possession of payment address
 - Platform Updates: Ubuntu 18.04
 - September: 1.12.0
 - Fully qualified DIDs
 - Dependent on DIDDoc support? (Daniel's document and David Huseby's work)
 - Platform Updates: MacOS, CentOS
 - Future
 - GitLab migration alongside Jenkins (Foundation)?
 - Aries / Indy split
 - Anoncreds 2.0 (Sovrin Foundation, [BC.gov?](#))
- Ursa
 - Working on release of 0.2.0
 - ZKP / ZKLang improvements
 - Debian packages
 - Refactor internal plumbing for anoncreds 2.0, shouldn't impact external interfaces
 - Refactor multi-signature BLS in addition to aggregated signature
- Aries

- Agent from Indy Catalyst migrated to aries-cloudagent-python (BC.gov)
 - Initial code migration from Indy SDK repositories
- Indy Catalyst
 - Migrated?

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?)
- SDK 2.0 architecture / Indy-Aries split (Sergey)


 Unknown macro: 'lref-gdrive-file'

 - Indy SDK Architecture Questions:
 - Sovrin Foundation team and Daniel making progress
 - Will work on defining the API surface in order to better understand what the threading model should be underneath
 - Need to define how we want to handle private keys. Shouldn't expose them to the end users, but need to access them from multiple libraries.
 - Feels pressure to make short term decisions that can be improved incrementally. Will also help Kiva to contribute.
- GitLab migration (Mike and Steve G)
 - Demos in the Identity Implementers WG calls
 - Issues with Jenkins machines because Rust builds run out of memory—workaround increased build time but is a temporary solution
- 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.
- 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

- Name change: Indy Maintainers call Indy Developers call
 - Approved
- Sovrin specific upgrade script for Indy Node 1.9.2 due to auth_rules bug (INDY-2211)
- Replace Amazon Linux with CentOS in the build pipeline
 - Adding CentOS increases the build pipeline by another 30 minutes.
 - Approved. Need to be clear about this change in the release notes.

- Improving the performance of the Indy SDK CI pipeline:

 Unable to render Jira issues macro, execution error.

- <https://github.com/hyperledger/indy-post-install-automation> is superseded by indy-qa-automation, so it was archived.
- What should be done in Indy SDK next:
 - Aries architecture (Ken's proposal)
 - Evonym: OSX support and architecture investigation
 - BC.gov:
 - New Ursa features?
 - Proving that a link secret has been seen before,
 - Repudiability as an option for proving
 - New predicates
 - Anoncreds 2.0
 - Architecture investigation
- PostgreSQL wallet to graduate from "experimental" status?
 - BC.gov and Kiva are using the plugin
 - Need an update on the open issues.
 - Need testing to be part of the automated CI / CD pipeline: publish to repo.sovrin.org
 - Sergey will look to see if there are any concerns with repo.sovrin.org
 - Need to define the release process: who fixes issues and when does PostgreSQL reliability prevent releases?
- Need an apt-get artifact of Ursa that can be used by Indy Plenum and Indy SDK
- Progress on Fully Qualified DIDs: IS-1358, IS-1359

Future Calls

- 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
...
- New pack / unpack requires disclosure of recipient
 - Cannot hide the receiver of the message like we could with msg_pack
 - Allows having multiple recipients of the same message
 - Should list the drawback in the Aries-RFC? Is there an alternative way that preserves the capability to selectively disclose the recipient?
 - From [Kyle Den Hartog](#)
msg_pack presents problems when dealing with an agent that maintains more than one relationship. For example, if I receive a message, I don't know which key in my agent I should be using to decrypt the message. We can get sender anonymity or receiver anonymity, but I don't believe it's possible to get both and still determine who the message is for.
 - Pack/unpack only exposes the Verkey of the recipients. It does not do forward secrecy.
- Ursa and AMCL: Discussed in the Ursa call (August 21), but no decision yet.
- Architecture questions for Indy SDK:



Unknown macro: 'lref-gdrive-file'

- Partially completed refactoring of the Request format: INDY-1375 and IS-567
- Maintainership requirements for Indy Node and Indy SDK
- How to handle old pull requests that failed DCO Checks? Close?
- 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>

Action items

- ☒ Nathan (Daniel)
 - Set up alternate meeting hosts to record
- ☐ HIPE #138, Issue #144 (Ken and Brent)
 - Create a PR for changing status to ACCEPTED
 - Check for an Aries RFC
- ☐ Rename Indy Maintainers Indy Developers in the calendar invitation (Richard)

Call Recording



zoom_0.mp4