2019-10-07 Indy Contributors Call

Summary

- The future of consensus in Indy Node (moving from RBFT to Aardvark?)
- Indy / Aries split

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>
- Samuel Smith (ProSapien) <sam@samuelsmith.org>
- Nemanja Patrnogic (donqui) (Evernym) <nemanja.patrnogic@evernym.com>

Related Calls and Announcements

- Previous Indy Contributors call
- Identity Implementors Working Group call
    - Main place to get project updates, release status, and announcements.
- Bootcamp Russia: Event Location

Release Status

- Indy Node
    - September Early October: 1.10.0
        - Refactoring for PBFT View Change and BLS signature
        - Bug fixes (including new bug with GET_FEES and LibNullPay
        - 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 Early October: 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?)
- 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. PR is merged.
  - 5 additional objects need to be added.
  - Currently making progress on HIPES, including updating the HIPE for the Context object.
  - Pull request for the Schema object is close.
    - github.com/burdettadam
- 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
  - 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)
  - Ursa is now publishing python wrapper debian packages. Cam is unblocked.

Main Business

- The future of consensus in Indy Node: proposal for moving from RBFT to Aardvark
  - During the implementation of PBFT View Change, we tested PBFT selection of View Change and it seemed to be much better.
  - Evaluating Aardvark versus fixing bugs with RBFT suggest that we should proceed to implement Aardvark.
  - Evernym is considering doing this in 2019, but has not made a decision.
  - Theoretical method growth in Ardvaark is n^2 instead of n^3 in RBFT.
  - In theory, view change for RBFT is faster than in Aardvark / PBFT because the nodes have more information stored in the shadow masters.
    - So there is a trade-off between faster view change versus faster throughput.
    - Under attack, RBFT is expected to have more consistent throughput than regular PBFT and Aardvark.
    - In practice, we would be using the same implementation of view change.
  - How often does view change happen in practice?
    - Under RBFT, view changes in the real world appear to be rare (days). It depends on the network conditions.
    - We can select the Aardvark performance threshold to have regular view changes with the frequency we would prefer, under good network conditions.
- Update on Indy / Aries split
  - foundation's POC on threading is currently on-hold.
  - Adam has been looking at Rust parallelization / threading libraries. (See the Rocket framework for web servers for a good example.)
  - Handlers vs Futures vs async/waits
    - Sergey's POC of async / await (IS-1371) https://www.diffchecker.com/0WkrvEnt
  - RFC for 37: Present Proof
    - Describes a new object for presentation previews. Fills a gap in LibIndy; interim solution until we have full blown W3C VCs.
  - Evernym thinks the next step is to move the Indy Wallet to Aries
    - See discussion in 2019-09-25-A Aries Working Group Call (US morning)
      - Kiva has plans for an aries-wallet
      - Evernym's proposal is that indy-sdk-wallet aries-ams (agent managed storage)
      - Aries RFC 50 already documents the Indy Wallet
- As an Indy / Aries community, do we always have to wait for consensus on the details before people can contribute code?

Future Calls

- 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.
- 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

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