2019-10-28 Indy Contributors Call

Summary

- The future of Indy Node
- Pros and cons of Plenum versus other ledgers

Timezone: APAC Morning, US mid-day and Europe evening

We will be taking advantage of the staggered adoption of daylight savings time to have a call with additional Indy contributors. The Indy Contributors call will be on October 28 at 11AM US Pacific / 19H Central European Time / 21H Moscow Standard Time / 7H October 29 in New Zealand.
Zoom link is changed too: https://zoom.us/j/715671233

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.

Introductions

Attendees

- Nemanja Patrnogic (donqui) <nemanja.patrnogic@evernym.com>
- Richard Esplin <richard.esplin@evernym.com>
- Sergey Khoroshavin <sergey.khoroshavin@evernym.com>
- Alexander Shcherbakov <alexander.shcherbakov@evernym.com>
- Cam Parra <camilop@kiva.org>

Related Calls and Announcements

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

Release Status

- Indy Node
    - October: 1.11.0
        - PBFT view change
    - November: 1.11.1
        - Bug fixes
- Indy SDK
    - October: 1.12.1
        - Bug fixes
        - Might skip the release
    - November
        - ?
    - 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)
    - Evernym: A PR with an example how the wallet can be separated; this is internal work
    - Kiva is working on a Futures implementation of threading (instead of call-backs)
- CI / CD: GitLab migration (Mike and Steve G)
- Advanced Schemas and W3C creds (Ken)
- Warnings from rust cargo clippy (Mike and Axel)
    - Epic: IS-1410
- 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
- Replacing Indy-Crypto with Ursa in Indy Node (Mike and Cam)

Main Business

- The future of consensus in Indy Node: proposal for moving from RBFT to Aardvark
    - Unable to render Jira issues macro, execution error.
- Remaining concerns with the current Indy Ledger
    - Lack of a diverse contributor community
        - Who is going to work on solutions?
    - Interpreted language (Python) is slower than a compiled language (Rust)
    - Features from general purpose ledgers we would like
        - Observer nodes
        - Smart contracts
- Strengths of Plenum
    - Battle tested
        - BFT with a 25 node pool and 10 write transactions per second (1000 reads)
    - Identity specific
    - BLS State Proofs
    - Pluggable ledgers
- Next steps: dedicate an Indy Contributors call to the future of the ledger in early 2020.

Future Calls

- Define the pull request review process for Indy Plenum/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?
        - Items from Evernym team:
            - covered by tests
            - has a link to the issue in Jira
            - fixed according to PoA
            - follows https://github.com/hyperledger/indy-node/blob/master/docs/source/write-code-guideline.md
    - Proposed Process (by Evernym team):
        - All Pull Requests can be reviewed by non-Evernym team members
        - Evernym team members will also do internal review in addition to external one
        - All interested parties are notified when a PR is sent
        - If a person wants to do an external review, he or she puts a comment or tag. This needs to be done in X hours.
        - Once a reviewer put a "want-to-review" tag, he or she need to finish review in Y hours
        - If no one wants to review a PR in X hours, or review is not finished in Y hours, we can do our internal review and merge the PR
        - An external review can be done against closed PRs as well, and Evernym team will process all findings ASAP
        - We may merge a PR with internal review only in case of urgency (critical fixes, release preparation etc.)
    - Items to be defined with the Community:
        1. A timeframe for external review (X):
           - X=12 hours, Y=2 days?
        2. What projects it should affect?
           - Plenum and Node?
           - Only Node?
           - We are not proposing SDK as it will be split to Aries in any case
        3. Who is going to commit to participate in this process?
- Migration of Indy-SDK to Aries-Core
- Requirements question: IS-1099, should we allow duplicate credentials from the same issuer?
- 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

GMT20191028-1...1474x1080.mp4