2019-11-11 Indy Contributors Call

Summary

- Work updates
- Current state of Plenum
- The future of Plenum
- Timeline for deprecating Indy SDK wrappers in favor of Aries

Timezone: US afternoon Asia / Pacific morning

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

- Ken Ebert (Sovrin Foundation) <ken@sovrin.org>
- Richard Esplin (Evernym) <richard.esplin@evernym.com>
- Name (Employer) <email>

Related Calls and Announcements

- Previous Indy Contributors call
- Identity Implementors Working Group call
    - Main place to get project updates, release status, and announcements.
- Aries Workshop/Connectathon December 3-5 in Provo, Utah
    - https://www.meetup.com/Utah-Sovrin-Meetup/events/265714942/
- Webinar on peer DIDs Nov 21 at 1 PM MST, ssimeetup.org
    - Deep dive into the Plenum Ledger (early December)

Release Status and Work Updates

- Indy Node
    - October: 1.11.0
        - PBFT view change
    - November: 1.12.1
        - Bug fixes
        - Ubuntu 18.04 (Kiva)
        - Replacing Indy Crypto with Ursa (Kiva)
        - Additional rich schemas objects: schema object (Sovrin Foundation)
            - Just posted Indy HIPE
              https://github.com/hyperledger/indy-hipe/pull/149
            - Aries RFC
              https://github.com/hyperledger/aries-rfcs/pull/281
            - PR of schema object in progress
    - December: 1.23.0
        - Remove replicas (Aardvark BFT) ?
        - Rich Schema progress: encoding object
    - Future
        - Advanced Schemas and W3C creds (Ken)
        - Anoncreds 2.0 (Sovrin Foundation)
- Indy SDK
    - October: 1.12.1
        - Skipped the October release
    - November 1.13.0

- Issue reported by BC.gov:
  https://github.com/hyperledger/indy-sdk/pull/1893
- Need to include a manual release of iOS artifacts
- LibVCX support for some Aries protocols
- Bug fixes
- Future
  - GitLab migration alongside Jenkins (Foundation)?
  - Warnings from rust cargo clippy (Mike and Axel), epic: IS-1410
- Indy Catalyst
  - Production deployment testing: volume loads.
    - Trying to identify performance bottlenecks. Currently think it's calls to the database.
    - Performance problems is preventing going to production.
  - Not yet migrated to Hyperledger. Needs more documentation.
- 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)
  - Cloud Compass is building the Linux Foundation EdX courses for Indy and Aries
    - Overview launch date: November 21st
    - More content will follow
- 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
    - BC.gov will implement the existing revocation capability in ACA-Py for use in constrained cases
      - Not looking at building against Anoncreds 2.0

Main Business

- Problems with RBFT replicas:
  - Indy Node Epics
    - INDY-2251: Problems with RBFT Replicas
    - INDY-2250: Removing replicas (move from RBFT to Aardvark)
  - Ken's summary:
    A simplification to our current algorithm to reduce complexity and simplify the method for determining when to perform a view change making our system more resistant to attack. It takes full advantage of our recent PBFT view change and monitoring logic improvements while boosting performance of the system. The cost and risk to make these changes is low.
- Recent performance tests:
  - Indy-2262: performance problems (BLS signature?), and batch size (3 second write latency, INDY-2277)
  - https://www.youtube.com/watch?v=OSpssHQXlOI&list=PLRp0viTDxBWGLdZk0aamtahB9cpJGV7ZF
- Bug with Audit ledger history:
  - https://sovrin.atlassian.net/browse/SN-8
- Evaluating Plenum
  - Pros versus other ledgers
  - Improvements we would like to make
  - Recent performance testing (increased batch size and write latency)
    - Other ledgers worry less about delays in confirmation for transaction writes to achieve higher scalability.
  - Top level Hyperledger Project?
  - Evaluating alternatives like Tendermint and Libra HotStuff
  - How can we recruit contributors from the Sovrin Steward community?
- Timeline for deprecating Indy wrappers in favor of Aries contributions
  - Focus is on the Aries SDK, no longer on the Indy SDK
  - Moving too fast to deprecate will scare people trying to get started today, because there are no mature alternatives in Aries today.
    - Especially with the mobile wrappers.
      - .NET and Xamarin is used by Open Source Mobile Agent (OSMA), which works today.
      - Team at DIDx is struggling with React Native. Wants to open source a React Native app platform.
      - WebAssembly would be the most performant approach.
      - Problems with iOS and XCode:
        https://github.com/hyperledger/indy-sdk/pull/1664
  - BC.gov is working on a plan for building on existing Aries today.
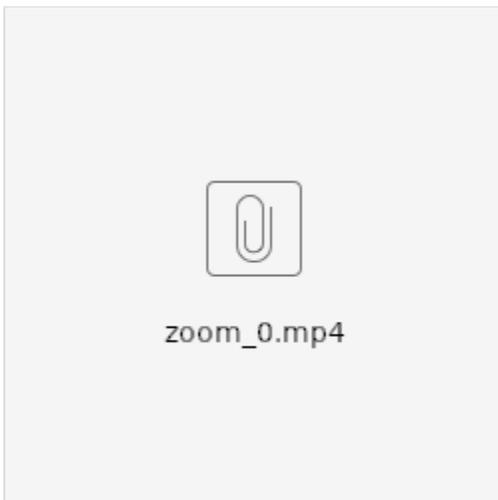
Future Calls

- 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

zoom_0.mp4

audio_only.m4a