

# 2021-02-16: Indy DID Method Specification Call

## Summary

- Can we do the GET\_DIDDOC transaction?
- ATTRIB DIDDoc raw data format
- How to represent Indy Ledger Objects as DIDs?

Recording from the call: [20210216 Indy DID Method Specification Call Recording](#)

### Antitrust Policy Notice

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 Updegrave of the firm of Gesmer Updegrave LLP, which provides legal counsel to the Linux Foundation.



Hyperledger is committed to creating a safe community for all. For more information please visit the [Hyperledger Code of Conduct](#)

## Welcome and Introductions

## Announcements

## Attendees

- [Stephen Curran](#)
- [Paul Bastian](#)
- [Sergey Khoroshavin](#)
- [Christos Patsonakis](#)
- [Dan Gisolfi](#)
- [Markus Sabadello](#)

## Collaboration Channels

- Current hackmd [document](#)
- indy-did-method on RocketChat - <https://chat.hyperledger.org/channel/indy-did-method>
- indy-did-method repo: [ReSpec](#) vs. [SpecUp](#)

## Agreed Upon:

- See HackMD Document for most of what we have discussed
- To find networks we will require at least the first and perhaps the second of these approaches, while the rest are suggested:
  - Config files for one or more known networks
  - A mechanism for a ledger operator to register discovery information for other ledgers (aka "human gossip")
    - A DID/DIDDoc on a ledger will contain cross-registry information
    - A mechanism is needed for finding the DID(s) that contain the registrations – ideas have been put forward - a DID Name Directory (DND) is the likely approach.
    - [Document](#) about the DND and DNR records
  - Decentralized registries based on verifiable credentials
  - Other registry mechanisms, such as the DDNR proposal
  - The DID Method Spec will include a reference to a repo (likely) "indy-did-networks" within Hyperledger that will be a lightly managed, structured repository of folders per Indy network with at least the config file(s) for the networks. Use of the repo is voluntary, but provides a convenient way for networks to publish information about the network. Maintainers will be selected from the community and should exhibit a light hand in accepting PRs, being concerned mainly with structure of the data (not content) and that contributors are not being malicious about updating the information of other network operators. The Hyperledger governance structure may be used for disputes as appropriate. This is not a replacement for the Governance that a specific network should implement.

## Online Discussion (from RocketChat this week)

- Further discussion of State Proofs and what should the transaction be to get back a DIDDoc
- Request for input on the "nymKeyAgreement" flag. Not much in the response.

## This Week's Discussion:

- [Sergey Khoroshavin](#) on Indy state proofs and the ramifications of a GET\_DIDDoc transaction.
  - Comparison to the "get\_revoc\_reg\_delta" transaction it's state proof handling.
- Options for getting a DIDDoc, which are a trade-off of integrity and effort to implement
  1. Do (almost) nothing. Client must get NYM, ATTRIB and assemble the DIDDoc.
    - a. Lack of certainty that the client gets a consistent version.
  2. **Have a single call that gets the NYM and ATTRIB and state proofs for both with same multi-signed merkle root, and leave the assembly to the client.**
  3. ~~Same as previous but have the ledger return the assembled document.~~
    - a. ~~To verify the state proofs, must still include the NYM and ATTRIB~~
  4. Have NYM and ATTRIB transactions write the DIDDoc to state and return that
    - a. V1 txns work the same
    - b. V2 txns work this new way
  5. Update NYM transaction to allow for an ATTRIB provided at the same time.
    - a. Looks like 4, but they are processed in a single call to the ledger
  6. Create a new transaction WRITE\_DIDDOC and put the object to the ledger
    - a. What's the impact on the NYM object?
  7. For all:
    - How might a query that requests a "version\_id=" and "version\_time=" work?
    - version\_time is doable, version\_id is less clear, as we have two ids
    - Risk is losing time database
- Any thoughts on the "nymKeyAgreement" discussion?
- Is it important to remove the "content" item and just inline the rest of the ATTRIB?
- What error checking should be done on the ATTRIB. See [proposal in the hackmd document](#) (valid JSON, no NYM fields, valid DIDDoc)
- Other Indy Ledger Objects as DIDs (schema):
  - Process
  - Existing transactions
  - Putting the Ledger Objects on other ledgers using extensions

## Future Discussions:

- This meeting: Discussion on nymKeyAgreement
- Drummonds proposal: [https://docs.google.com/document/d/1f99z4Bf8F-DA8EbKjInVQv2ncJGPwF\\_Dp7I7Mfyhqs/edit](https://docs.google.com/document/d/1f99z4Bf8F-DA8EbKjInVQv2ncJGPwF_Dp7I7Mfyhqs/edit)
- What format for other objects on the ledger as DIDDocs.
- What format for existing objects on the ledger as DIDDocs?
- DNR and DND discussions
- Structure for Indy specific objects returned as DIDs
  - What is the DID?
  - What is the DIDDoc format?
  - Existing objects – backwards compatibility
    - DID vs. DID URL – how could that be done?