Hyperledger Identity Projects

Richard Esplin
October 2019
Agenda

- Aries
- Indy
- Ursa
- Future
Relevant Projects
Aries
What is Aries


- Wallet infrastructure
- Blockchain client (resolvers)
- Secure Messaging
- Extensible API infrastructure

"Identity Agent"
# Aries RFCs

## Aries RFCs by Status

### ADOPTED

### ACCEPTED

- 0004: Agents (2019-01-15, 9 impls — concept)
- 0006: SSI Notation (2018-09-01, 1 impl — concept)
- 0008: Message ID and Threading (2018-10-01, 5 impls — concept)
- 0017: Attachments (2019-01-31, 1 impl — concept)
- 0019: Encryption Envelope (2019-05-04, 7 impls — feature)
- 0020: Message Types (2019-05-24, 8 impls — concept)
- 0031: Discover Features Protocol 1.0 (2019-05-01, 1 impl — feature protocol)
Active Projects

Aries Cloud Agent - Python
Aries Framework - GO
Aries Framework - Ruby
Aries Static Agent - Python
Aries SDK Java
Aries SDK JavaScript
Aries Toolbox

Join the talk by Nemanja Patrnogic: “Tools for Building Your Identity Application”
Ways to Participate

Weekly Zoom Calls: https://wiki.hyperledger.org/display/ARIES/Aries+Working+Group

Rocket Chat #aries

RFC Process https://github.com/hyperledger/aries-rfcs

Source Code https://github.com/hyperledger/aries
Indy
Hyperledger Indy

Public Permissioned Blockchain

Custom built for Identity

Join Alexander Shcherbakov’s talk: “Understanding the Indy Distributed Ledger”

RBFT Consensus
The Problem is Correlation

Correlation = Linkability

Attribute based correlation

Identifier-based Correlation

Signature or Hash-based Correlation

Timing Inferences

Including if Multiple Parties Share Information (Collusion)
Ensuring Privacy

The prover chooses when to disclose.

The prover selects what should be disclosed.

Don’t share more attributes than necessary

Don’t share with more precision than necessary
Ensuring Privacy

The verifier and the issue do not communicate.

The prover can present to any verifier.

A proof can hold multiple credentials from multiple issuers.

A credential is anonymously revocable.
You Don’t Have to Deploy Your Own

Engineered solely for privacy-enhancing self-sovereign identity

Global public utility that no single entity owns or controls

Open source, open standards, open governance

Fast, efficient—based on Hyperledger Indy
Ways to Participate

Weekly Zoom Calls: https://wiki.hyperledger.org/display/indy/Indy+Contributors+Meeting

Rocket Chat #indy

HIPE Process https://github.com/hyperledger/indy-hipe

Source Code https://github.com/hyperledger/indy-sdk
https://github.com/hyperledger/indy-node
https://github.com/hyperledger/indy-plenum
Goal: general purpose crypto library shared by HL projects

Annoncreds 1.0 (CL Signatures)

BLS Multi-Signatures

DON’T ROLL YOUR OWN CRYPTO!
Ways to Participate

Bi-Weekly Zoom Calls: https://wiki.hyperledger.org/display/ursa/Meeting+Agendas

Rocket Chat #ursa

RFC Process https://github.com/hyperledger/ursa-rfcs

Source Code https://github.com/hyperledger/ursa

Documentation https://github.com/hyperledger/ursa-docs
Identity Working Group

Goals:

- Discuss use cases
- Establish best practices (white paper)
- Cross-project coordination

Rocket Chat #identity-wg

Calls:

- Main Working Group
  https://wiki.hyperledger.org/display/IWG/Identity+Working+Group
  Every-other Wednesday at 18H Central Europe
- Implementers
  https://wiki.hyperledger.org/display/IWG/Identity+WG+Implementers+Call
  Every-other Thursday at 17H Central Europe
Other Hyperledger Projects

Fabric: W3C Verifiable Credentials

Iroha: Identity use cases

Sawtooth: Identity Transaction Family

Grid: Identity in Supply Chain

And integrations between projects.
The Future
Aries

HYPERLEDGER

ARIES

Test suite

Shared libraries

More libraries, frameworks, and agents
Aries Rust libraries

- Resolver
- Safe Wallet
  - Unsafe Wallet
- Cred Impl
  - Crypto
- Aggregate Functions
  - lang wrapper
    - C-callable API
    - Framework

- Cache

- external interface
- internal interface
Indy

PBFT View Change

Aardvark Consensus

Indy-DRI-Aries

Aries Migration
Ursa

Annoncreds 2.0
Support for additional predicates
Bullet Proofs for ZKPs
Support for hardware security modules
Annoncreds 2.0

Replace Tails Files and Accumulators with Merkle Trees

https://github.com/hyperledger/ursa-docs/tree/master/specs/anoncreds2
Governance Frameworks

Layer One: DID Networks (Public Ledgers)

Layer Two: DIDComm

Layer Three: Credential Exchange

Layer Four: Governance Frameworks
Discussion