

Abstract

SecureKey Technologies is launching an interoperability initiative aimed at establishing common standards and development frameworks for next generation digital identity networks.

Contributions

We will support the efforts within the Hyperledger and Decentralized Identity Foundation (DIF) communities to help create innovative distributed ledger technologies and digital identity networks. We believe that creating cross-project and cross-network standardization and interop along with common development frameworks represents the next step in transforming the digital identity space. In particular we support, and look forward to contributing to, the efforts of Hyperledger Fabric, Indy and the newly proposed Aries project along with DIF's Identity Hub efforts.

Contributions will be directed towards the community projects above as well as [open project extensions](#) within the TrustBloc initiative.

In particular, we will contribute:

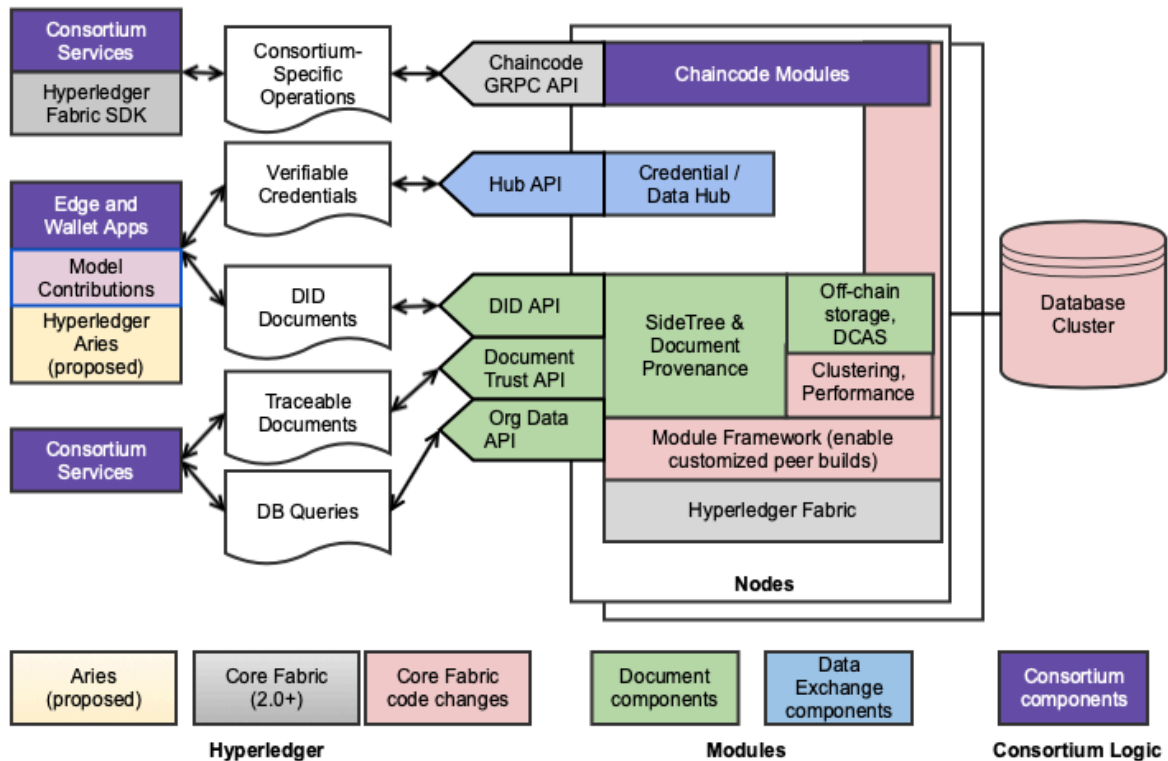
- Hyperledger Fabric performance and customization improvements. We are excited to contribute improvements we learned while building and taking our network operational.
- Enable DIDs to be managed and exposed from Fabric, and more generically enabling document provenance.
- A model for digital identity exchange based on DIDs, Verifiable Credentials, and Hubs.
- Efforts towards interoperability with the newly proposed Hyperledger Aries project, in order to use a Fabric-based ledger and our digital identity model. We think it's critical to allow variation on top of a common base.
- Tooling and demos to enhance developer experiences building digital identity networks.

About SecureKey

SecureKey builds identity networks like Verified.Me, the Canadian identity sharing Network supported by seven major banks, mobile operators, a major credit agency, and other providers in Canada. Verified.Me provides a user centric, privacy protecting identity platform for services that trust the individual's identity established at their financial institution and other connected organizations. Users can link in account information across services for a convenient but highly reliable digital identity where information is delivered in real time.

Technical Brief

In the following diagram, we provide an overview of the components related to the TrustBloc initiative. We will follow-up with additional details and data exchange flows.



The TrustBloc initiative provides a common infrastructure for consortiums to enable document provenance and data exchange, while still allowing these consortiums to differentiate based on their service offerings. We are building on top of existing community efforts from Hyperledger Fabric along with the proposed Hyperledger Aries project.

Document Provenance and Organizational Data Components

The TrustBloc initiative aims to provide consortium-based document provenance and services to reduce trust obstacles. We are enabling DIDs to be managed and exposed from Fabric, and more generically enabling document provenance. The following features are early goals of the initiative:

- Provide out-of-the-box capabilities for document provenance (including DIDs).
- Enhance Hyperledger Fabric private collections to support SideTrees – allowing identifiers and documents to be anchored to a channel without individual transactions.

- Enable off-chain distributed storage model to support transactions (e.g., transient storage, content-addressable storage).
- Support a storage and query model for data scoped to a particular organization.

Data Exchange Components

TrustBloc will also provide a verifiable credential exchange flow. We are enabling a model for digital identity exchange based on DIDs, Verifiable Credentials, and Hubs. This will be achieved by:

- Leveraging emerging community specifications (e.g., DIDs and Verifiable Credentials).
- Enabling usage of Peer DIDs to establish data exchange transactions while anchoring to ledger-based DIDs and verifiable credentials.
- Supporting a Hub-based model for efficient, real-time data exchange.