



Hyperledger IDENTUS

Identity Innovation

AGENDA



Welcome & Introductions



Brief history



Tech Overview & Solutions



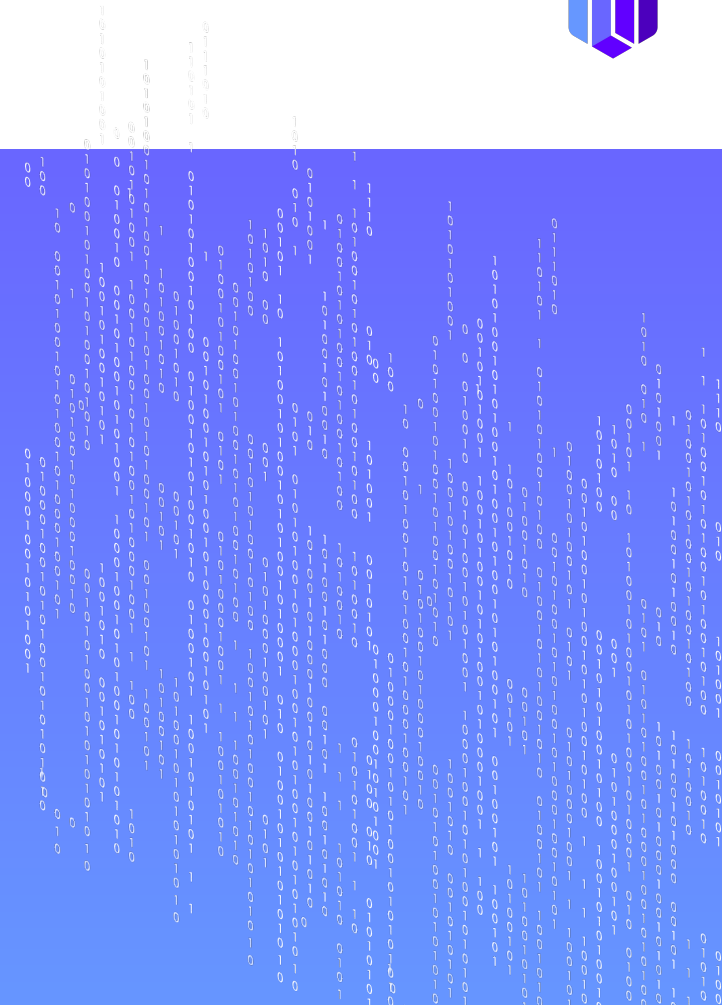
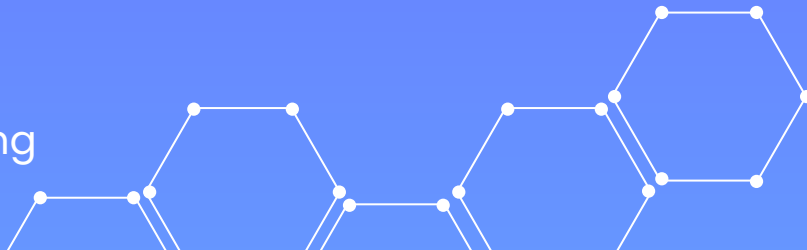
Demo



Q & A



Closing





WELCOME & INTRODUCTIONS



BRIEF HISTORY

Atala 1.4



- Prism Node
 - Cardano as VDR
- Prism SDK interfacing with Prism Node
 - Used for all applications (front-end, back-end, mobile etc)
- Features
 - DIDs
 - Only on-chain DIDs
 - Single or batch creation
 - SECP256K1
 - No registered DID method
 - Verifiable Credentials
 - JSON
 - On-chain
 - Merkle-tree
 - Batch Issuance
 - Revocation
 - Not W3C or any other standard compliant
 - Communications
 - Prism Connect (Not available to public)
 - Centralised proxy that contains all relationships between peers





Atala 2.0

- Redesigned from the ground up
- Addressed various issues such as:
 - Standards compliance
 - Communication layer
 - Crypto Agility
- Based on building blocks
- Standards/Specifications
 - W3C
 - JSON
 - JSON-LD
 - JWT / SD-JWT
 - Hyperledger Aries
 - DIDComm v2
 - Hyperledger Anoncreds
 - OID4VCI/OID4VP
- 2 years in the making
- Components
 - Prism Cloud Agent
 - Prism SDKs
 - Swift
 - KMM
 - Typescript
 - Mediator
 - Mediator Test-Suite
 - Prism Node
- Hyperledger Labs Project
 - Project Name
 - Open Enterprise Agent





Identus

- Migrated from Hyperledger Labs to Hyperledger
- Identus Components:
 - Fully contained SSI platform
 - Cloud Agent, Edge SDKs, Mediator, Prism Node (Open Source)
 - Easy to deploy and use
 - Reference SDK implementations
 - Security assessment on major releases
 - VDR
 - Cardano
- Future Objectives
 - Easy adaptation via interfaces
 - Scalability and Performance
 - Community contribution and uptake
 - Compliance
 - European / Global regulations
 - Security
 - VDR Interface Service (Agnostic)
 - Read/write integration with VDRs for DIDs
 - CRUD non-DID Resources
- Community
 - Establish and grow a strong community



TECHNICAL OVERVIEW





High-level technology overview

- Identus Platform includes services, libraries and 3rd party components:
 - Edge Agent SDKs – libraries written in Typescript, Swift and Kotlin to cover web and mobile (Android and iOS) platforms
 - Mediator, Cloud Agent, Prism Node – services written in Scala language (JVM target platform).
 - Apollo – cross-platform cryptography library written in Kotlin. Used by agents.
 - Blockchain:
 - Cardano
 - Data Access Layer:
 - Postgres – default database used by the Cloud Agent and the Prism Node
 - MongoDB – default database used by the Mediator service
 - Hashicorp Vault – secure storage service used by the Cloud Agent
 - Authentication and Authorization
 - Keycloak – IAM service used by the Cloud Agent





Recipes

Based on the requirements to the solution, the following components of the Identus platform can be used:

1. Non-custodial Identity Wallet
 - a. mobile app => Mediator + Edge Agent SDK (Kotlin, Swift)
 - b. web or Node js => Mediator + Edge Agent (TypeScript)
2. Custodial Identity Wallet (private keys are managed by the Cloud Agent)
 - a. mobile app => Cloud Agent + Mediator + Edge Agent SDK (Kotlin, Swift)
 - b. web application => Cloud Agent + Mediator + Edge Agent SDK TypeScript
3. Credential Issuance and Verification organization
 - a. custodial for issuers and verifiers => Cloud Agent + Edge Agent SDK Typescript
 - b. And non-custodial for holders => Mediator + Edge Agent SDK (Kotlin, Swift)
4. Integration with OpenID systems => Cloud Agent + Keycloak + Edge Agent SDK + Mediator



DEMO





Hyperledger Identus

May 2024 Meetup





Q & A





THANKS FOR JOINING