Hyperledger In-depth with Instnt:

Enabling Portable KYC for Financial Institutions
Justin Kamerman
Chief Product Officer

Soubhratra Das
VP, Engineering
Digital Customer Onboarding Is Broken

40%

or more of good customers are rejected due to vendor orchestration rules and automated system false-positives causing financial exclusion
Why Instnt?

Risk-based Approach:
Loss liability indemnification of up to $100M
Low/No Code Integration
Why /instnt /?

Pay for performance
Centralized Identity Management

- Sovereign
- Issuers are Verifiers
- Identifiers
- Portability
- Privacy
- Cybersecurity Risk
Decentralized Identity Management

- Self-Sovereign
- Issuers and Verifiers
- Identities
- Portability
- Privacy
- Cybersecurity Risk
Why Instnt? Why

Hybrid centralized/decentralized implementation building on Instnt Accept
Portable KYC and frictionless compliance
Governance frameworks and standardized level-of-assurance LoA
Why Instnt Access™?

Passwordless Login
Product Silos
The Ecosystem
Foundation

- Distributed Ledger Technology / Blockchain
- Decentralized ID (DID)
- DIDComm protocol
- Verifiable Credential (VC)
- Level of Assurance (LOA)
- JSON-LD Schema
Decentralized ID (DID)

- Permanent
- Resolvable
- Cryptographically verifiable
- Decentralized
DID Architecture

- **DID Subject** refers to **DID**
- **DID Controller** refers to **DID Document**
- **DID URL** contains **DID**
- **DID Document** resolves to **Verifiable Data Registry**
- **DID** recorded on **Verifiable Data Registry**
Verifiable Credential

- Credential Metadata
- Claim(s)
- Proof(s)

Verifiable Presentation

- Presentation Metadata
- Verifiable Credential(s)
- Proof(s)
Roles and Information Flow

Issuer (Instnt)
issues VC

Holder (End user)
acquires, stores, presents VC

Verifier (Instnt's customer)
verifies VC

Verify identifiers and use schemas

Send presentation

Verifiable Data Registry
maintain DIDs, schemas & credential definitions

Verify identifiers and schemas
Hyperledger Tools & Frameworks
Hyperledger Identity Stack
Trust Framework

ToIP Technology Stack
- Application Ecosystems
  - Layer 4
    - Trust Task Protocols
      - Example: Credential Exchange
      - Issuer → Holder → Verifier
    - Peer-to-Peer Communication
      - DID → Connection → DID
    - Public Utilities
      - DID Method 1 → Interoperable → DID Method 2

ToIP Governance Stack
- Ecosystem Governance Frameworks
  - Governing Authority → Ecosystem Framework → Governs/Certifies
- Trust Task Governance Frameworks
  - Governing Authority → Credential Framework → Governs/Certifies
  - Credential Exchange Roles
- Agent/Wallet Governance Frameworks
  - Governing Authority → Agent/Wallet Framework → Governs/Certifies
- Utility Governance Frameworks
  - Governing Authority → Utility Framework → Governs/Certifies
Perfect Synergy

Instnt provides identity assurance which is a critical precursor of Identity management.

With the help of Hyperledger tools Instnt now enables end user to own their identity.
Enabling Instnt Access

Customers enable Access on Instnt Dashboard

Users store credentials in Instnt powered wallet
How it works
Single signup
Instnt Dashboard
Benefits

- Fraud loss indemnification
- Frictionless onboarding
- Portable KYC
- Open Standards
- Managed service
- Account Monitoring
Instnt helped a leading retail lender drive $11M of fraud losses to Zero and accommodated growth with up to $20M in fraud loss liability shift.
The Road Ahead

- IETF Governance Framework
- Standardization of KYC Level-of-Assurance
- Digital Services Marketplace
- Partnership with OSS communities

https://www.instnt.org/book-a-demo