Self-Sovereign Identity in Govtech for Financial & Healthcare Inclusion

Debajani Mohanty, EarthId
Who am I?

- Top 30 Blockchain Influencer from India
- Blockchain Solution Architect & SSI Expert at EarthId. Implemented many pioneer projects on Blockchain globally.
- Author of Amazon Blockchain bestsellers books
- Author of “Blockchain for Self Sovereign Digital Identity”
- Keynote speaker at many national and International events, Mentor, Practitioner
The “Invisible People”

Across the globe, an estimated one billion people lack a legal form of identification. Of the 7.6 billion people on earth:

- 3.2 billion have some form of ID and a digital trait
- 3.4 billion have some form of ID but no digital trait
- 1 billion lack a legal form of ID

McKinsey & Company

Debajani Mohanty, EarthId

An estimated 1 Billion people are without an official proof of identity. 81% live in Sub-Saharan Africa and South Asia.

Source: 2018 ID4D Global Dataset id4d.worldbank.org

Legal ID coverage figures are based upon World Bank ID4D reporting or the latest registration where national ID does not exist or data are not available.

Calculated as population with active social media use, as reported in the Global Digital Report 2019, presumed to be within the population that has some form of legally recognized ID.
Introduction To Digital Identity
What is Digital Identity

Personal Data that identifies us online

Initiation of any business relationship online
Why to Protect Digital Personal Data?

Debajani Mohanty, EarthId
Evolution of Digital Identity

- Federated Identity (1999 - 2004)
- User-Centric Identity (2005 - 2013)
- Self Sovereign Digital Identity (2014 - 2023)

Mass Hack Possible
Single Point of Failure
Self Sovereign Identity

1. Issues
   Verified Credential

2. Shares
   Verified Credential

3. Reads Reference
to VC

4. Revokes
   VC

Issuer

User/Holder

Verifier

Personal Data
(Nama, DoB, Birth, Caste, Tax Certificate, Address etc.)

Public Blockchain
Trust Anchor
(Public DIDs, Reference to Claims, Revocation Registry)

Debajani Mohanty, EarthId
Self Sovereign Identity in Detail

1. Creates Schema for VC creation & Public/Private Key & Public DID

2. Creates Public/Private Key Pair & private DID

3. Sends Public Key & Personal Data Signed with Private Key

4. Creates Hash for VC Signed with Private Key

5. Issues Verified Credential

6. Shares Public Key, Issuer DID & token signed with Private Key & VC

7. Decrypts the token with Public Key to check User Ownership of Private Key

8. Searches VC to check if Issuer’s DID is valid, and if VC is valid and allocated to same Public Key as User’s

9. VC Verified Successfully

10. Revokes VC

Issuer

User/Holder

Veriﬁer

Debajani Mohanty

Public Blockchain
Trust Anchor
(Public DIDs, Reference to Claims, Revocation Registry)

Issues
- Verified Credential
- Personal Data (Nama, DoB, Birth, Caste, Tax Certificate, Address etc.)

Issuer/DID

User/DID

Verifier/DID

Public/Personal Keys

Trust Anchor:
- Public DIDs
- Reference to Claims
- Revocation Registry

Integrity
Ownership
Privacy
Security
Validity
Complexity of SSI Network

Think of the various enablers and influencers to decentralized identity as a solar system.

Different layers

1. Public Ledger
2. Private Identity Storage
3. Agent or Hub
4. Client Device

Debajani Mohanty, Earthld
System Architecture

Organization Issuer/Verifier

Public DLT
DIDs, Reference Hash of Claims, Revocation Registry
Run by Validator Nodes

Alice
Encrypted Data in Data Vault
Biometrics Templates
Local Storage

Bob
Encrypted Data in Data Vault
Biometrics Templates
Local Storage

Cloud Storage

Debajani Mohanty
Live Use Cases
TDIF, Government of Australia

Using these Attribute Verification Services:

- **Face Verification Service**
  - includes Liveness detection and biometric binding

- **Document Verification Service**
  - turns 100 points paper-based ID check into a digital experience

Singapore Government extends national digital identity program with face verification from iProov

Available to 4 million Singapore citizens

Access to 500 digital services from 180+ government agencies/commercial entities

Used by enterprises as well as government

Available on mobile and kiosk
Tell Us Once, Government of Canada

Digital Credentials using SSI

Open registry of decentralized identifiers.

British Columbia VON Project

Debajani Mohanty, Earthld
iRespond - Combating Child Trafficking in Underdeveloped World
SSI All Over the World

GOVERNMENT DIGITAL IDENTITY INITIATIVES

- **British Columbia**: introduced service cards to let citizens access the provinces' services.
- **Gov.UK Verify**: can be used by British residents to prove identity online to access government services.
- **The Nordic-Baltic** eID initiative is a step towards digitally unifying the Nordic region where citizens and businesses can access cross-border digital services by using their national eIDs.
- **Estonia’s eID**: is one of the most advanced national ID card systems in the world, allowing citizens digital access to almost all government services.
- **Germany’s eID**: allows the government to authenticate German citizens’ identity.
- **Spain**: developed the Spanish National ID Cards (CNI) to be launched in 2020, designed to help residents transact digitally with the government.
- **China**: piloted its eID program in Guangzhou in April 2018.
- **India**: has enrolled 1.2 billion citizens in its Aadhaar system.
- **Peru**: launched DNI digital ID cards in 2013.
- **Chile**: has issued more than 10 million national digital ID cards to facilitate access to online government services.
- **Uruguay**: established its eID program in 2015.
- **Nigeria**: has started to issue eID cards for every citizen.
- **Algeria**: rolled out a biometric smart identity card in 2016.
- **Pakistan**: Computerized National Identity Card (CNID) helps its citizens authenticate themselves for government interactions.
- **Afghanistan**: issued its first eID in March 2018.

“By 2023, 65% of the world’s population will have its personal information covered under modern privacy regulations, up from 10% today.”

Gartner, 2020

TEN PRINCIPLES OF SELF-SOVEREIGN IDENTITY & GDPR

- **Existence**: Compliant with perspective promoted by the GDPR
- **Articles 7-16-18 of the GDPR**: Control
- **Articles 12-13-14 of the GDPR**: Access
- **Article 15 of the GDPR**: Transparency
- **Article 17+ of the GDPR**: Persistence
- **Article 1 of the GDPR**: Portability
- **Articles 4-7 of the GDPR**: Interoperability
- **Articles 5-25 of the GDPR**: Consent
- **Minimalization**: Protection

*The concept of privacy by design can be considered in contrast with the “right to be forgotten” enshrined in the GDPR (Art 17)*
Area of Research
SSI Protocols

Hyperledger Indy & Aries

Ethereum’s Civic & uPort

Microsoft’s ION

Hashgraph’s Earth ID
Architecture Diagram of EarthiD

Hashgraph Public DLT
Governed by Global Leaders

Hashgraph Public DLT

Certified Credentials

EarliD App

Individuals

Organizations
Enterprises
Governments

EarliD App Running on IOT Devices

Appnet Node

Hashgraph Public DLT

Hedera Governing Council
with Google,
IBM, Wipro,
Deutsche Telekom,
FIS,
Tata Telecom

Hedera Nodes

Mirror Nodes

User Shares Credentials

DID Creation & Issuance of Reference Hash for Issued Credentials

Issuer Appnet Node

DID Creation & Validation of Reference Hash for Shared Credentials

Requester Appnet Node

Hedera Governing Council

Handles DID Creation & Deactivation,
Reference & Revocation of Claims

User’s VC

EarliD App

Individuals

Organizations
Enterprises
Governments

Debajani Mohanty, EarliD 22
SSI Success Factors

- Crypto/Public Key Infrastructure
- Scalability & Throughput
- Cybersecurity
- Integration of Biometrics
- Validator Nodes For DLT
- Selective Disclosure & ZKP
- Interoperability

Debajani Mohanty, EarthId
EarthId’s State of Art Architecture
For Self Sovereign Identity

- Crypto/Public Key Infrastructure
- Scalability & Throughput
- Interoperability
- Selective Disclosure & ZKP
- Integration of Biometrics
- Validator Nodes For DLT
- Cybersecurity

Uses SHA-256 base Hashing & novel Ed25519 public-key signature system which is fastest and safest.
EarthId’s State of Art Architecture
For Self Sovereign Identity

- Crypto/Public Key Infrastructure
- Scalability & Throughput
- Cybersecurity
- Interoperability
- Selective Disclosure & ZKP
- Hashgraph is tested with 10,000 TPS and 1.5M Txn per day with Finality in seconds
- Integration of Biometrics
- Validator Nodes For DLT

Debajani Mohanty, EarthId
EarthId’s State of Art Architecture
For Self Sovereign Identity

- Crypto/Public Key Infrastructure
- Scalability & Throughput
- Cybersecurity
- Hashgraph is resistant against DDoS, Sybil and Spoofing attacks
- Integration of Biometrics
- Validator Nodes For DLT
- Selective Disclosure & ZKP
- Interoperability

Debajani Mohanty, EarthId
EarthId’s State of Art Architecture For Self Sovereign Identity

- Crypto/Public Key Infrastructure
- Scalability & Throughput
- Cybersecurity
- Interoperability
- Can easily be integrated with other DID networks & from other layers
- Selective Disclosure & ZKP
- Integration of Biometrics
- Validator Nodes For DLT

Debajani Mohanty, EarthId
EarthId’s State of Art Architecture
For Self Sovereign Identity

- Crypto/Public Key Infrastructure
- Scalability & Throughput
- Cybersecurity
- Interoperability
- Selective Disclosure & ZKP
- Validator Nodes for DLT
- Integration of Biometrics

Can share data in Traditional, ZKP or Self-Attested mode. Uses finest cryptology algorithms to use ZKP in various modes (>=, <=, >, <, != etc.)
EarthId’s State of Art Architecture For Self Sovereign Identity

- Crypto/Public Key Infrastructure
- Scalability & Throughput
- Cybersecurity
- Interoperability
- Selective Disclosure & ZKP
- Integration of Biometrics
- Hashgraph’s Validator nodes are industry leaders in different verticals as Google, IBM, Wipro, Deutsche Telekom, FIS, Tata Telecom etc.
EarthId’s State of Art Architecture
For Self Sovereign Identity

Integration with Different Biometrics modalities for implementation of Decentralized Biometrics

Integration of Biometrics

Validator Nodes For DLT

Crypto/Public Key Infrastructure

Scalability & Throughput

Cybersecurity

Selective Disclosure & ZKP

Interoperability

Debajani Mohanty, EarthId
EarthId’s State of Art Architecture For Self Sovereign Identity

- Crypto/Public Key Infrastructure
- Integration of Biometrics
- Scalability & Throughput
- Cybersecurity
- Interoperability
- Selective Disclosure & ZKP
- Validator Nodes For DLT

Debajani Mohanty, EarthId
Next Gen Authentication & Authorisation Architecture

Debajani Mohanty, EarthId
Best Practices in Personal Data Management For Digital Identity

Knowledge

Possession

Inheritance

Debajani Mohanty, EarthId
How Biometrics Works

1. Fingerprint scan
2. Extracting unique biometric features
3. Mapping unique biometric features
4. The biometric template: a binary representation of unique features

Debajani Mohanty, EarthId
Anti Spoofing Techniques

- Challenge-response method/Liveness Detection Test
  - Smiles
  - Facial expressions of sadness or happiness
  - Head movements
- Sensors & Dedicated hardware
- Algorithms

https://global.faceid.com/products/liveness-detection
NextGen Authentication
By CuLedger’s MemberPass & Gemalto/Thales Group

1. Write
   - Credit Union (Issuer)
   - Verifier (Requestor)

2. Sign
   - Member (Holder)
   - Verifier (Requestor)

3. Read
   - Member (Holder)
   - Verifier (Requestor)

4. Verify
   - Member (Holder)

CuLedger Credit Union

Public, Permissioned Distributed Ledger Technology

Gemalto/Thales Group

Debajani Mohanty, EarthId
EarthId’s Next-Gen Authentication
With Decentralized Biometrics

1. EarthId Captures Biometrics after Active Liveness check & Converts to template

2. Personal Data & Biometrics Template

3. Optional
   ✓ Background Verification
   ✓ Deduplication
   ✓ Template Stored

4. Reference Hash Signed with Issuer’s Private Key

5. Confirms Certification

6. User logs in matching Live Biometrics

7. Personal Data, Live Biometrics Template And Issuer Details

8. Passive Liveness test for Biometrics

9. Converts Personal data & Biometrics to Hash & Matches Hash Issued by Issuer

10. User is authenticated

Debajani Mohanty, EarthId
Thank You & Questions

- Follow me on twitter: https://twitter.com/debimr75
- Follow me on LinkedIn: https://www.linkedin.com/in/debajanimohantypmp/