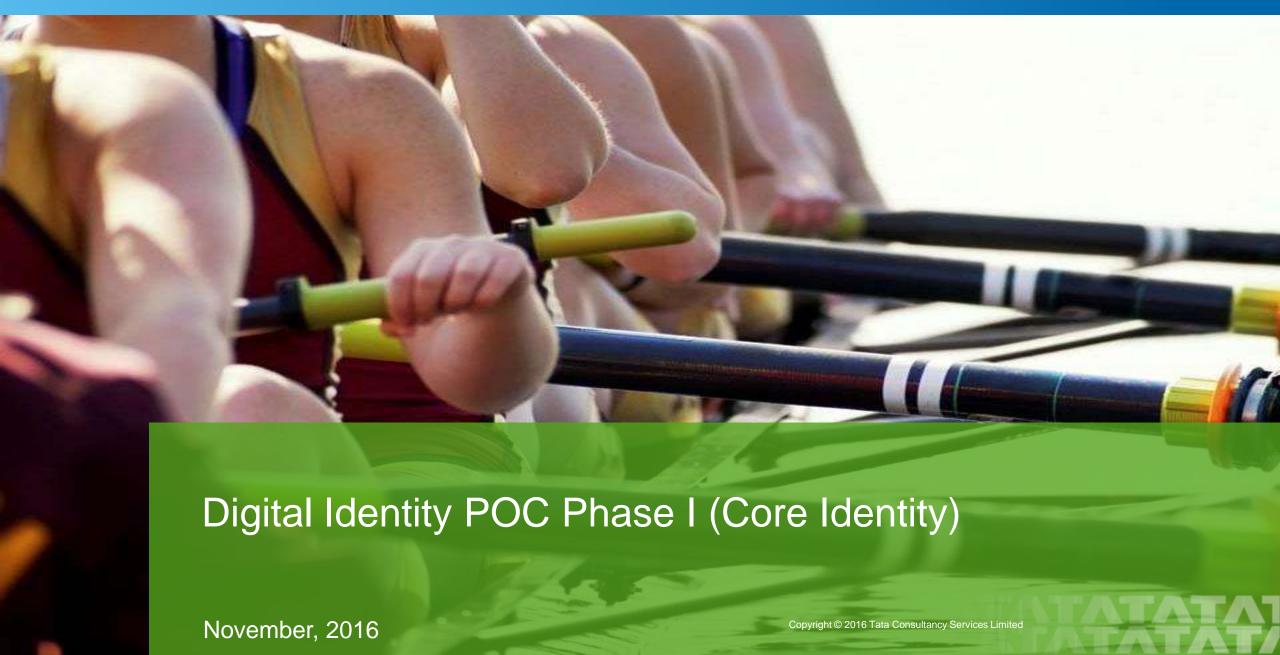
Experience certainty.

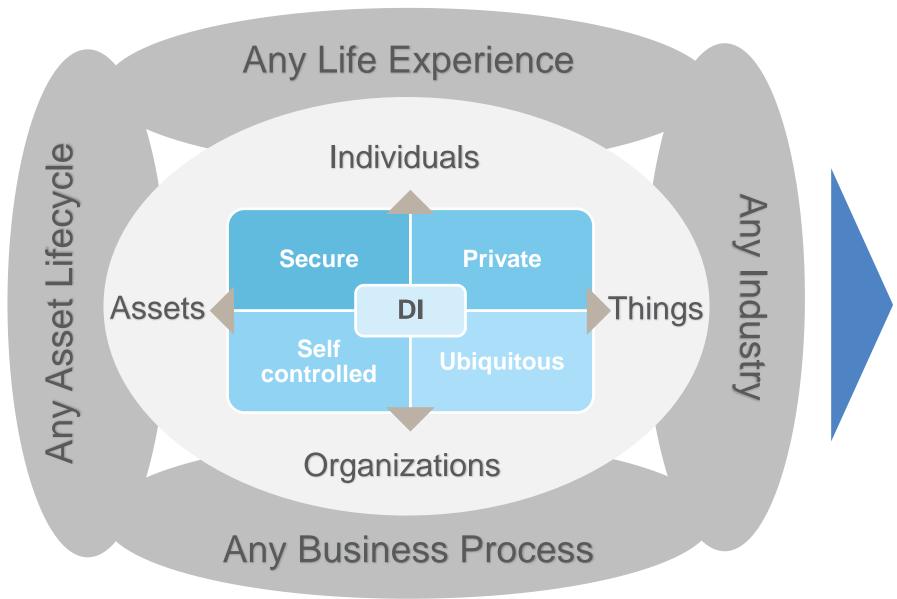




Why digital identity will become fundamental to everyone and everything ...

1.5bn people do not have a legal identity and are shut out from meaningful economic activity and legal protection Ongoing cyberhacks of personal information costs tens of billions posing global threats to everyone Ongoing cyberhacks of devices can Requires endanger the lives of millions of people **Exponential** coherent global **Identity Risks** Digital Identity strategies and **Opportunities** solutions Regulations are rapidly increasing globally to protect an individuals' privacy Seamless CX requires secure, trusted and real-time authentication of individuals and things

Secure & Private Digital Identity (DI): An Ubiquitous "Killer App"



Clients like it ...

- Impacts any Ecosystem Participant & Value-Exchange
- Cross-industryImpact
- On top of legacy systems

A vision for a universal, secure and private Digital Identity

It does not matter on which Blockchain a digital identity was created, it can be used across many Blockchains and even without a Blockchain

Blockchain Agnostic

Modular: Core Identity +

- A Core Identity is established through an auditable trust process that proves uniqueness just like getting a passport
- Extended Identities are connected to a core identity e.g., ones assets, reputation, documents and activity histories

Private & User Controlled

- Identity data is encrypted and distributed
- Access to identity data can only be granted by owner
- Access to identity data is by asset/document/data object

Does not require a separate identity per use case e.g. identify yourself at a bank as you would entering a country

Core identity verification is use case agnostic

What is a Digital Identity?

Extended

Identities

Can be recovered without 3rd party intervention (forward recovery)

If compromised through changes or identified behavior, employ forward recovery mechanism e.g. escrow of changes or behaviors etc.

Blockchain becomes the trust broker for identity

Real-time, noninteractive verification without 3rd parties

Verification is trustless

One does not need to know Personal Identifiable Information (PII) to verify an identity (Keyword: NIZK)

TATA CONSULTANCY SERVICES

4

Definition of a Digital Identity and its Attestation

A **Digital Identity** is defined through

- A Core Identity (COID) Representing uniqueness and ownership and control over an identity.
 This is what we implemented in this first POC (see next slide)
- One or more Identity Dimensions relating to different aspects of an individuals or a things history and data such as financial, social, education etc. – under development
- An Identity Graph specifying all cascading owner- and control relationships an individual or a thing has under development

There are two principal ways for Identity Attestation

Earning trusted status through reputation alone without a 3rd party attestation process



Anyone can start on building their trusted digital identity through verifiable behavior



Does not guarantee the uniqueness of a digital identity, even if biometric data is included

Using a 3rd party trust providers such as a governments or banks to attest to uniqueness of an identity



Higher uniqueness guarantees, if validated by sufficient number of identity verification providers such as an **Identity Federation** as we employ to add more security



Is not 100% self-sovereign and requires external 3rd party trust providers

A Core Identity has four important aspects that give it utility

Uniqueness:

Unique ID – unique identifier of a person or thing Unique ID attributes – Attributes that do not change often such as biometric information or national ID numbers

Self-Recovery of an Identity: List of Identity Recovery IDs which are identifiers of trusted digital identities that can vouch for the compromised identity Recovery Condition – m-of-n multi-sig condition for the self-recovery of an identity

Ownership:

Ownership ID – unique identifier of ownership List of Owner IDs --unique, secure identifiers of digital identity owners

Ownership Token ID – unique identifier of tokens Ownership Token Attribute – e.g. Alice's Tokens Ownership Token Quantity -- tokens held by each owner

Control:

Control ID – unique identifier of ownership
List of Controller IDs --unique, secure identifiers
of digital identity controllers e.g. parents
Controller Token ID – unique identifier of tokens
Control Token Attribute – e.g. Alice's Tokens
Control Token Quantity -- tokens held by each
controller allowing access to identity other than
controllers

Digital Identity Phase I (Core Identity) Demo

Digital Identity Phase I (Core Identity) Demo shows the following concepts

Universal Core Identity

Use Case independent attestation

Private & User Controlled Identity

Identity
Verification is
trustless

Digital Twin as
a secure
router or
firewall for
things

Immutable Audit Trails

Secure Tiered, Integrated Blockchain(s) Architecture

Digital Identity Phase I (Core Identity) Demo Flow





Consortium Identity Validation Service





Your Identity Wallet



Digital Twin



Eris Blockchain Services



8

BigChain Big Data & IPFS



Identity Services for your everyday needs: Payments, Passport, Services Authentication, eCommerce



Secure Gateway to isolate applications from malicious external and internal actors



Smart Contracts: To validate and manage Identity through decentralized consensus (Identity Validation, Voting & Management & Inter Blockchain APIs)



Creates Blockchain secured, yet Blockchain independent, immutable identity and activity audit trail

Digital Identity Phase I (Core Identity) High-Level Architecture (I)

Uploading a File to IPFS for Identity Attestation Process

Your Identity Wallet



Digital Twin

2



Eris/Monax Blockchain Services





IPFS Network

Framework:

- React
- Babble
- Express
- Java Script

Security:

- DSA & Hashing: secp256k1 & keccak-256
- Encryption: AES-256

Framework:

- React
- Babble
- Express
- Java Script

Security:

- DSA & Hashing: secp256k1
- Encryption: AES-256

Framework:

- Eris Application Stack
 (Ethereum Virtual Machine
 (EVM) + Tendermint
 Consensus + Docker +
 Micro Services)
- Smart Contracts: Solidity + Java Script apps
- Using Eris/Monax IPFS Micro Service
- https://github.com/eris-ltd Security:
- DSA & Hashing: secp256k1 keccak-256, ED25519 & ripemd160
- Encryption: AES-256

Framework:

- P2P, decentralized filesharing system
- <u>https://github.com/</u> <u>ipfs/ipfs</u>

Security:

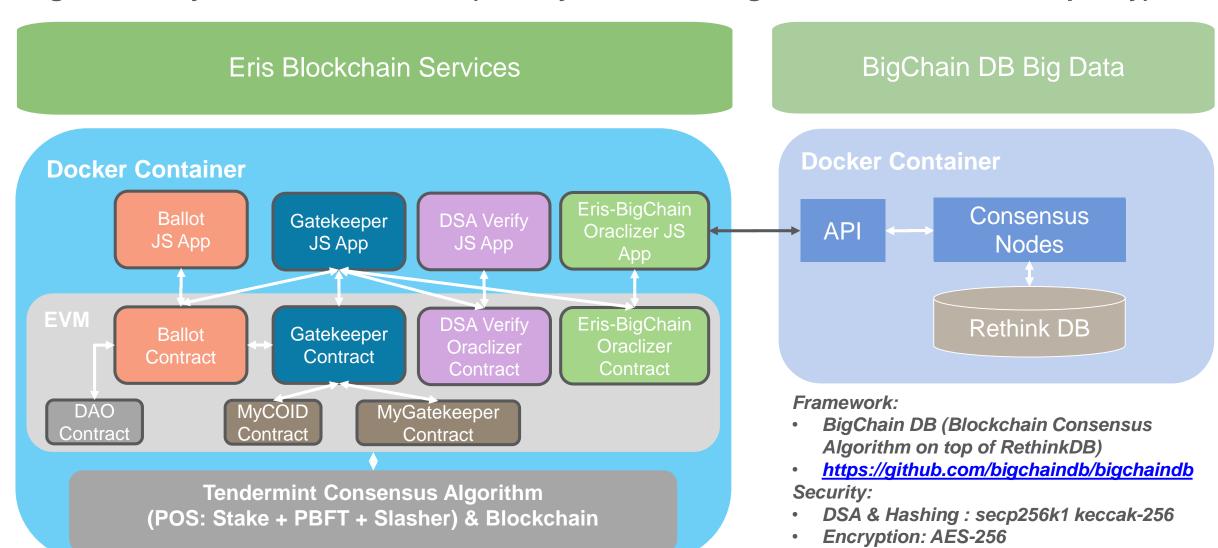
- cryptographichash content addressing
- block-level deduplication
- file integrity + versioning
- filesystem-level encryption + signing support

Security To-Dos:

- Clients and Servers run in secure enclaves Exploring Graphene OS or Intel SGX
- Clients and Servers employ secure storage Exploring Google Vault project
- Clients and Servers use asymmetric e2e encryption for messaging – exploring Whisper protocol

Digital Identity Phase I (Core Identity) High-Level Architecture (II)

Digital Identity Attestation Process (Identity Wallet and Digital Twin omitted for simplicity)



TATA CONSULTANCY SERVICES



