



Offering **trusted, reliable, and affordable biometric solutions** that are **safe, easy to deploy, and upgradeable** with minimal cost

## Building Impactful Opportunities for Quality, Universal, Biometric Empowerment

Creating solutions that **impact** lives at the **grassroots** level

### BioKYC Unified Digital KYC Platform

World's First, US Patented, **Web 3.0 enablement ready, AI Powered**

Multi-factor, Multimodal, Decentralized Biometric-Identity management Platform with Live Data Analytics



**Mr. Subodh Narayan Agrawal**  
Founder

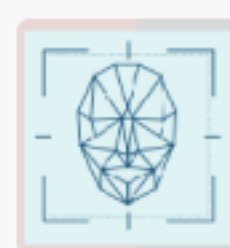
After experiencing sophisticated digital fraud first-hand, Mr. Subodh Narayan Agrawal founded BioQube in 2018, making it his mission to combat identity fraud globally through cutting-edge biometric solutions.



Feature	Problems	Solution by Bioqube	Our Competitive Edge
<b>Biometric Modalities</b>	Single – Factor : Face only or finger (using device)	<b>Multi Factor Authentication</b> (Face, finger, Voice, eyes & Palm)	Face : <b>1: N, 1:1 Match @ 26 ms</b> in a 20 Million Records in cloud
<b>Hardware Requirements</b>	<b>Fragmented hardware solutions: Specialised &amp; Costly hardware</b> , can't communicate instantaneously with global Databases	<b>Mobile first technology.</b> Mobile Tablet/ IP Camera - Based, No additional Hardware needed WEB 3 Enabled	<b>No Spares/inventory</b> required Leverage Mobile <b>Technology advancement</b>
<b>Cost and Accessibility</b>	Expensive, Urban Centric, slow deployment	Affordable, grassroots-focused, leverages Mobiles/ tablets innovation	Leverage existing <b>Infra ( IP camera), individual's mobile</b>
<b>Security measures</b>	<b>Security vulnerability</b> Basic encryption, no decentralised data OTP & Password dependent to complete end-to –end process	<b>Decentralized Data security</b> with AES 256 Encryption, data stored in customer's Cloud	<b>Patented Technology</b> - Distributed architecture for Multi-factor authentication, Local AI deployment –Online & Offline
<b>Scalability</b>	Limited scope, Expensive, Time consuming and difficult to upgrade/ replace	<b>Empowering users:</b> Highly Scalable across Diverse environment	Quick deployment <b>via app</b> , AI model works both <b>Offline and Online, Deduplication</b> check – on Device & in cloud



Mobile/Tablet



Face



Voice



Finger



Eye



Palm



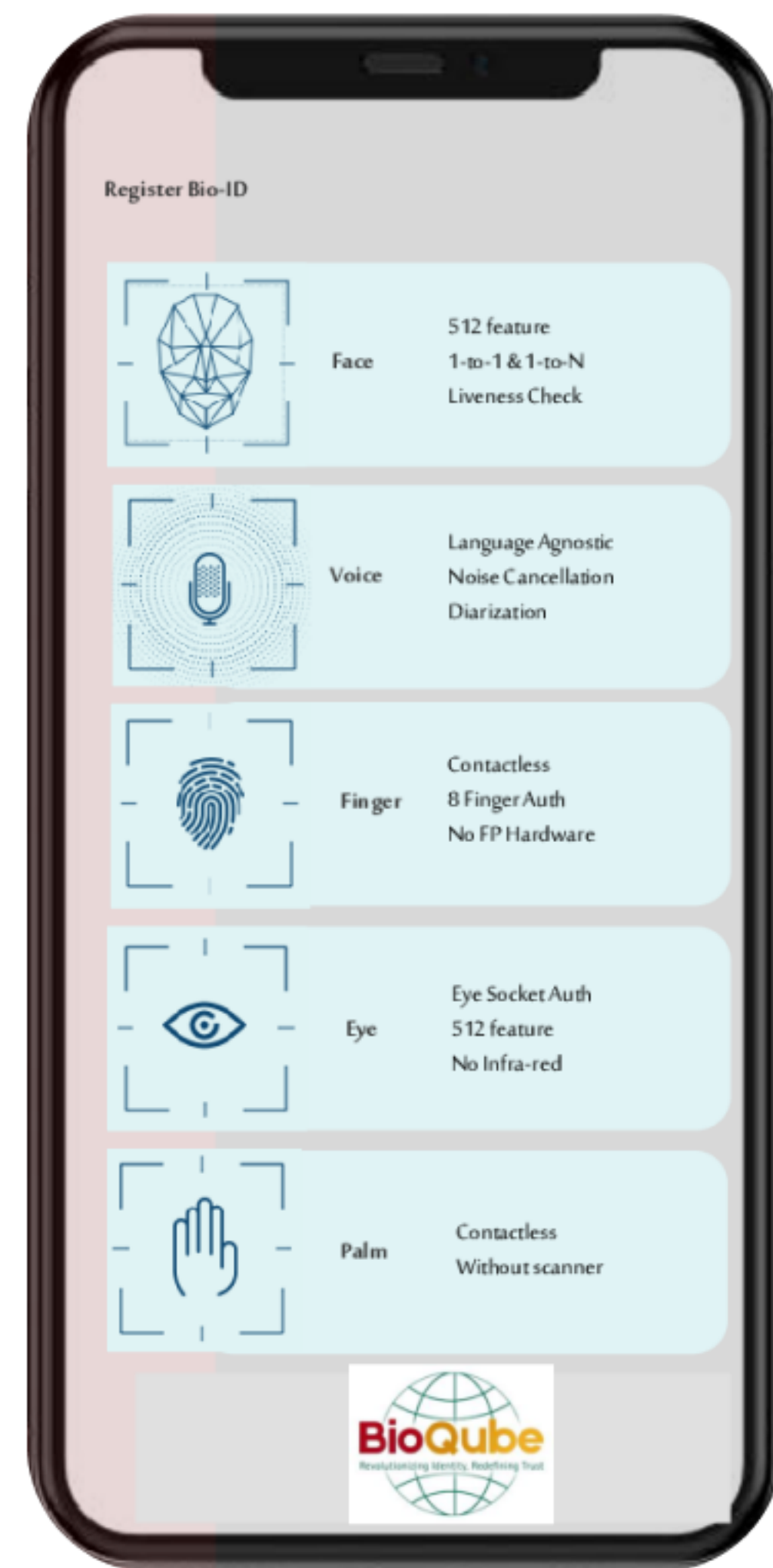
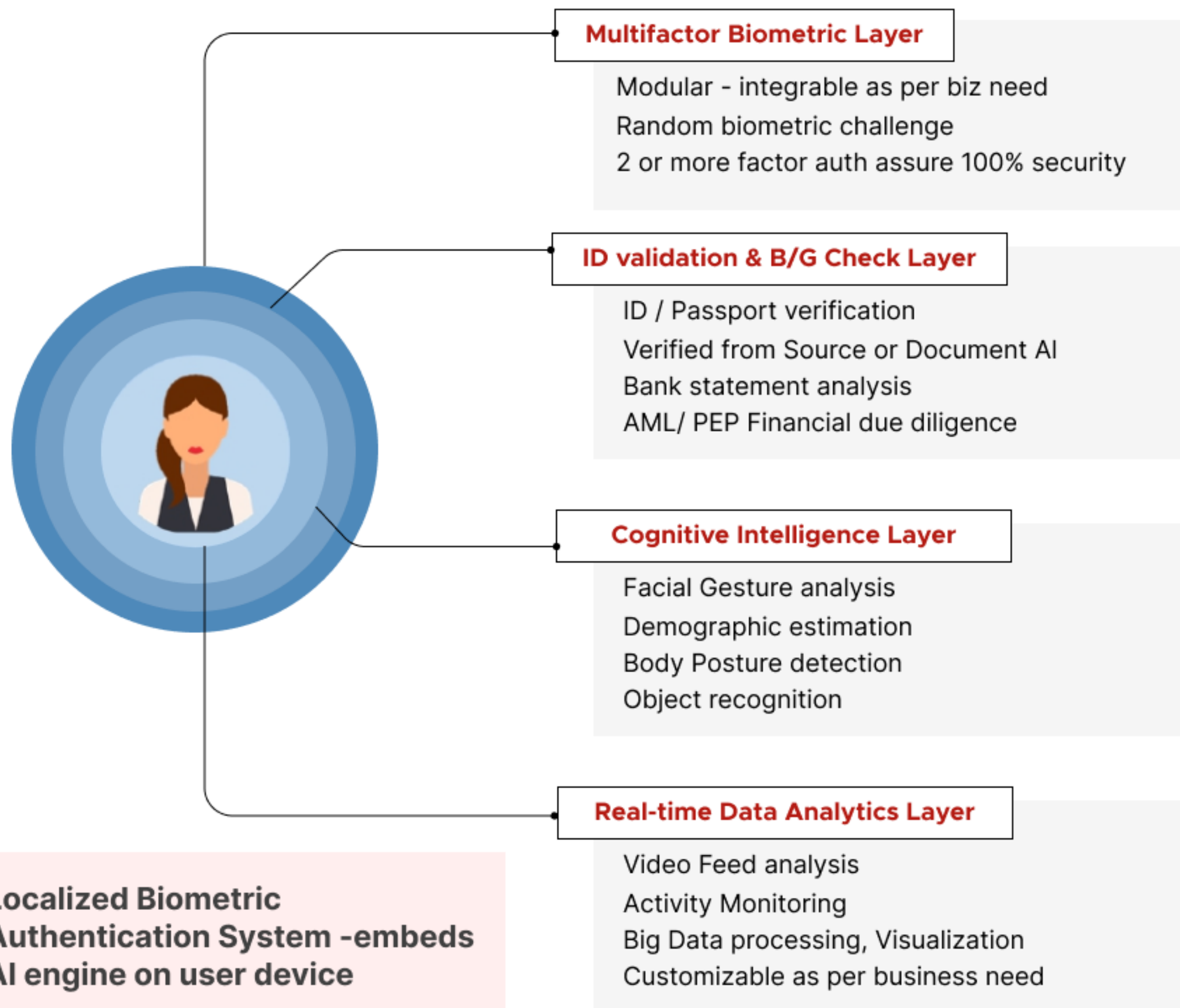
- Web3 Enabled
- Unique, Distributed Data Architecture



# Core Technology

Your Biometric is your Identity, Web 3 Enabled

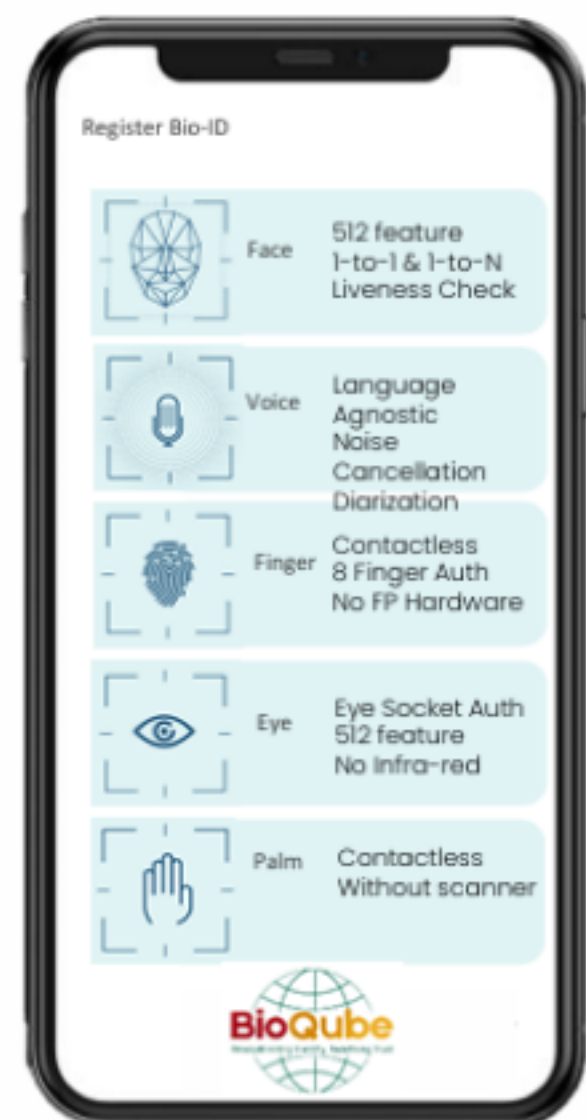
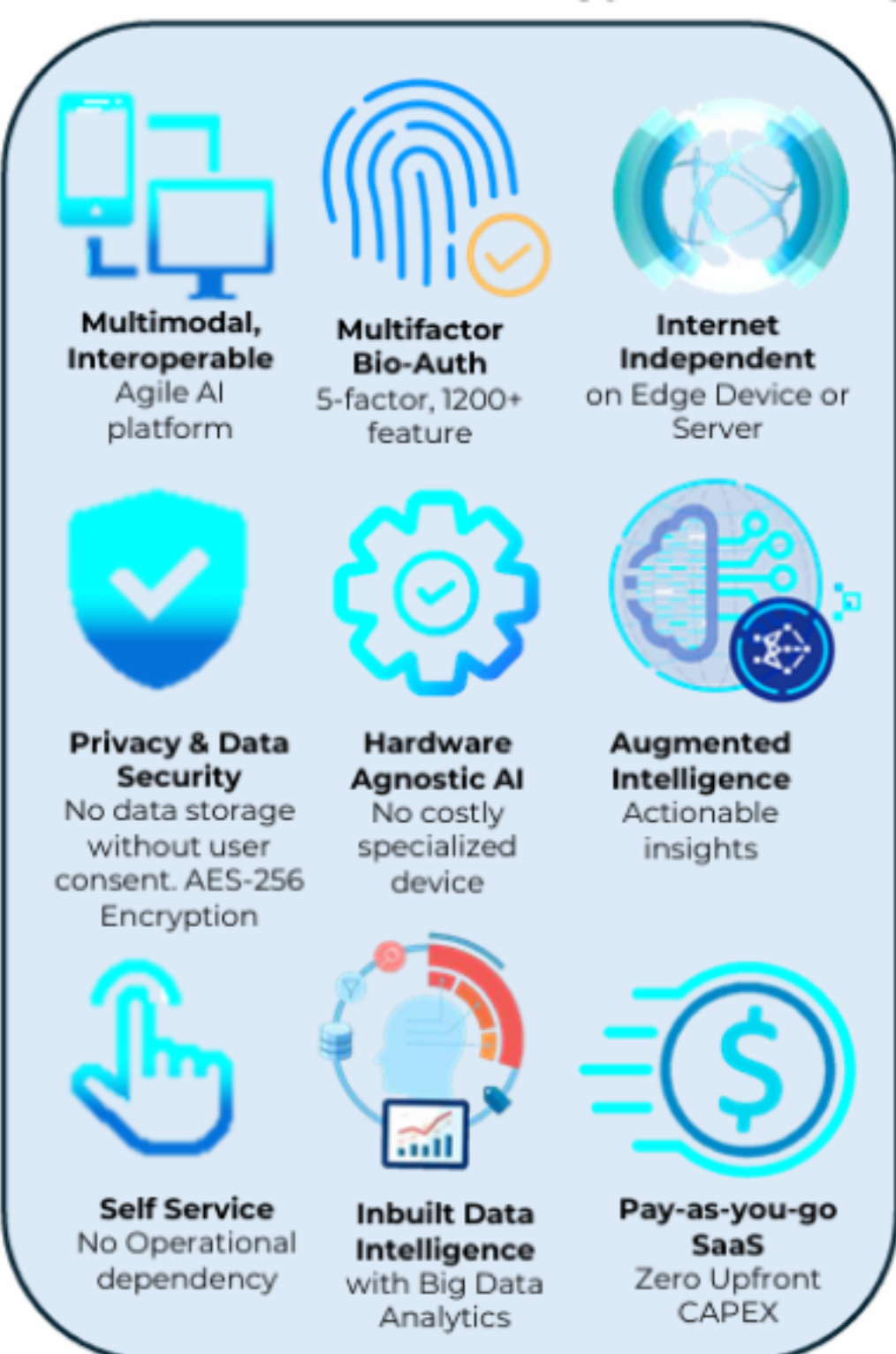
A Patented decentralized data architecture which reduces risk of hacking



**Localized Biometric Authentication System -embeds AI engine on user device**  
+ 3 More applied

## Solution Architecture

Deployable both  
Offline & Online



**No Specialised Hardware**

Deployable using any  
mobile/tablet

+  
Interpretable with legacy  
system

&

**Military grade  
data protection**

AES 256+decentralized data  
structure



**Geo-Fenced**


- Contact Less
- No Specialized Hardware








Challenges in Current KYC Processes

Client Hassle

- 


Multiple face-to-face appointments and lengthy manual documentation protocols.
- 


Difficulty in gathering and submitting extensive documentation causes delays and confusion.
- 


Delays in service access due to lengthy identity verification processes.
- 

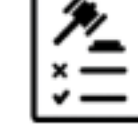
Customers worry about data privacy.

Organizational Hassle

- 

Slower onboarding affects customer acquisition rates.
- 

Increased workload to verify and manage.
- 

Increased vulnerability to fraud and compliance issues.
- 

Challenge of ensuring compliance with data protection regulations.

Key Features

Self-service Remote Onboarding with multi-factor biometrics

Customer can perform self-service biometric combining multiple biometric factors (e.g. Face, Finger etc.) using his own mobile device camera only.

Politically Exposed Person (PEPs)

Politically Exposed Persons (PEPs) pose higher risks for money laundering or terrorism financing, and AI/ML are used in KYC processes to continuously identify and refine PEP profiles.

ID Document Integration & Validation

ID documents are validated using source checks or OCR with auto-fill, matching biographic and biometric data through unified analysis, consistency checks, and pattern recognition.

Adverse Media Check

Adverse media checks scan global news sources to monitor individuals or entities for links to terrorism, money laundering, crime, and corruption.

Financial Due Diligence

Simplified, yet enhanced due diligence – Global AML, PEP, adverse media and sanction checklist.

Sanction File

Bioqube's API-based sanction check scans global sanctions lists to identify high-risk individuals, businesses, and nations with histories of financial crime.

AI Biometric and Documentation Validation



BIOMETRIC ID LINKING



DOCUMENT VALIDATION

Face with Liveness + Multifactor Biometrics Easy

- Passive liveness checks prevent deepfake and spoofing attacks using photos or videos.

Auto Defect Detection & Correction

- The ML model detects issues like blurriness, glare, poor lighting, multiple faces, or incorrect orientation, prompting recapture

Liveness detection

- Integrated liveness check ensures real user presence and prevents deep fake or spoofing.

ID validation & Orientation Check

- The AI/ML model detects image issues (blurriness, glare, reflection, orientation), prompts recapture, and can regenerate high-quality face images from poor inputs to enable accurate matching

Auto Text/image Extraction & Matching

- BioQube's AI-powered extraction surpasses OCR by accurately mapping text and images to the right fields for precise data capture.

Automated Image Reconstruction






- Our AI/ML model checks the document's quality, reconstructs it, and makes it human-readable



# BioKYC Benefits



Bio-KYC enables both end users as well as the financial institutions to adopt simpler, effective & efficient mechanisms without compromising security during user onboarding

- **Enhanced User Experience:** Eliminating time-consuming repeated physical visits and extensive paper-based process
- **Cost Effective:** Remote identity verification methods can fulfil KYC and AML
- **Realtime Govt. ID validation:** Source/ AI based ID validation - auto-filling the details - secure - increasing onboarding efficiency.
- **Effective Fraud Prevention:** Liveness detection + Face matching with Gov. Photo ID + Deduplication - ensures zero spoofing & eliminating multiple enrollment of same individual.
- **Easy and Interactive Admin Management:** AI assisted decisioning thereby reducing checks - precise & quick decisioning for approving authorities

## Aligned with 9 UN SDG goals



### Advisory Board

- |   |   |   |  |
|---|---|---|--|
| <b>Steven Morgan</b><br>Ex-Global Head Tech Ops, Citibank                 | <b>Rakesh Asthana</b><br>Former special director CBI, Director General BSF, Director General NCB  | <b>Roll Stephane</b><br>Chairperson, African Union Economic Council   | <b>Saumen Chakraborty</b><br>30Y exp. - IBM, Microsoft |
| <b>Capt. Harpreet Chadha</b><br>Advisory Board - California Sheriff Dept. | <b>Himanshu Gulati</b><br>Member of Parliament, Norway  | <b>Rene Bruehlhart</b><br>Former President of the Board of Directors of the Financial Information Authority (AIF) of Vatican City | <b>Gaurav Dalmia</b><br>Chairman, Dalmia Holding       |
| <b>Anil Ahuja</b><br>Former Asia head of 3i                               | <b>Brian Steven Hughes</b><br>VP- Active Security Consulting, Former President-Lupo Global Former Political Director for U.S. Congressional elections | <b>Ahmed Kassam</b><br>Advisory to NEPAD e-Africa Commission, UNDP, UNICEF, UNESCO, Commonwealth Biz Council, World Bank, WEF     |  |