# Decentralised Wallets Are Coming (Hurrah!)

Trustworthy digital identity for the Global South

Espresso, Oxford · Nov–Dec 2026

# The challenges are manifold




Any one can sink a digital identity system, and in practice they pull against each other.

*When identity systems lose public trust, the consequences are not abstract.*

# A framework to measure trustworthiness

**6**

facets of assurance

**381**

metrics

**65+**

mechanisms

### Drawn from standards

ISO 27000 family, NIST CSF and SP 800, ETSI 319 411, GDPR and more

### Open and reviewed

Creative Commons licence, assessment tool ready to use; reviewed by World Bank, ID4Africa and Aadhaar teams

01

# Trustchain

A trustworthy, decentralised public key infrastructure

# Two kinds of digital ID

## Foundational

National level

Card or phone app, dedicated enrolment

Unique ID number, central database, biometrics

Nigeria, Estonia, India, Philippines

Concerns: surveillance, profiling, exclusion

## Functional (attribute-based)

Any social scale

Credentials in a wallet on your phone

No enrolment: builds on existing databases

Users control and selectively disclose data

W3C verifiable credentials, UK trust framework

# Standards exist. The technical piece is missing

### W3C standards

Verifiable credentials and data registry. No technical architecture.

### UK trust framework

Rules for organisations. Explicitly no technical architecture.

### Trustchain

Designed to fill the gap.

**Mature standards + mature frameworks = a missing technical layer**

# Example: a doctor’s medical licence

**HM Government**

gov.uk

→

**Dept of Health and Social Care**

DID

→

**General Medical Council**

gmc-uk.org

## Each link is a DID, verifiable and time-stamped

### Employer asks

Is this really the GMC’s key? Who says the GMC may issue licences?

### Time matters

Keys rotate and authority is revoked, so verifiers need trustworthy time stamps.

# A digital twin of existing trust hierarchies

We don’t replace the hierarchy that exists, we mirror it. Any community can adopt it, at any scale.

## Free

Open and permissionless access

## Global

Interoperable across communities

## Cheap

Minimal setup and operating costs

# Take a closer look

### Demo video

See Trustchain in action

### Open-source code

Mobile and desktop apps

### Articles

Technical notes and papers

*I’d love to hear from anyone who tries it.*

# Limitations and next steps

## Time stamp source

Today: the Bitcoin network, which is poor optics for a ministry.

Alternative: Fabric Time, but permissioned Hyperledger depends on verified identity. A circularity.

## Scaling consensus

Cope with network outages.

Promising new work with DAGs and the Mysteci platform.

02

# SIMple ID

Can a basic mobile phone display QR codes for digital identification?

# Biometric ID at scale: Fair Price Shops

**1**

Resident presents Aadhaar number

**2**

Fingerprint scan

**3**

Order specified

**4**

Shop submits to UIDAI: yes or no

**~75%** of authentications in India use biometric fingerprints

# All these systems depend on…

**Smartphones or contactless cards**

**Special readers**

**QR codes**

**Screens that show them**

**Cameras that read them**

*Great systems, but built for people who own the hardware.*

# C’est un problème

## 51%

Smartphone adoption among adults in India (2020). Plus price, battery, durability, repair.

## Coverage

Far from good cellular coverage, costly, little competition. Even India has no single provider.

## Cards

World Bank 2018: chip cards cost more to design, print, distribute and personalise.

# How far can a basic phone go?

## The handset

Not developer friendly

Low-resolution screen

Basic inputs

## But it hides a second computer

A separate chip, usually managed by the mobile network operator

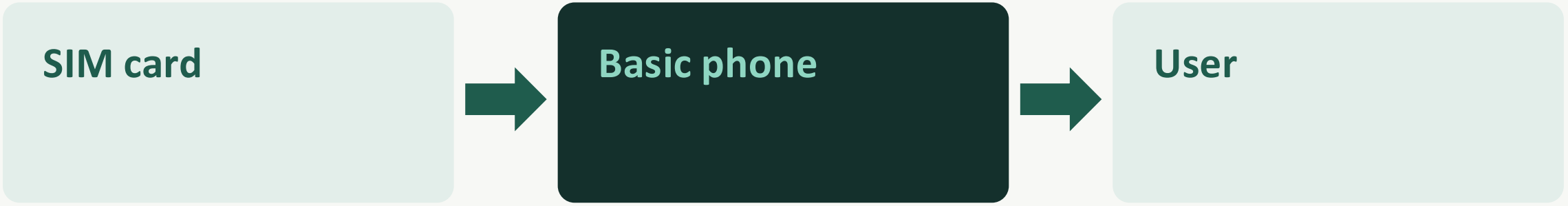
# The SIM card and its toolkit

An independent, secure cryptographic device that can run its own simple applications, using the same technology as your bank card.

| Set up a menu | Collect input | Display text | Play a tone | Send an SMS |
| --- | --- | --- | --- | --- |

**Display-text can include an icon, and the icon can replace the text.**

# Putting it together




New coding scheme for QR codes: the icon file contains JSON, not pixels, and the handset renders it.

**No app. No internet. A verifiable credential on a basic phone.**

# Deployment and standards

## To deploy

One willing device manufacturer

Usability and acceptance testing

A trust model that fits the society, with or without the operator

Privacy and security tuned to public appetite

## Standards

W3C for protocol and DID work

ITU for QR coding

Possible MOSIP adoption; interest from Airtel Africa

Smartphone-agnostic; virtual SIM possible

# The next phase: wallets

## Knowledge

DPI best practices, country self-assessment, cyber threat observatory

## Development

Privacy-enhancing tech, fraud detection, synthetic data, equitable AI

## Implementation

Partner consultations, prototypes, integration by partners

Goals: more trustworthy DPI, stronger cyber capacity, secure and private interoperable data sharing, fraud management and AI fairness.

# Decentralised wallets are coming.
# Hurrah.

Thank you. Questions welcome.