C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

Potentials of Smart Contracts in Digital India

Sandeep Kumar Shukla
Indian Institute of Technology Kanpur

What is a Smart Contract?

- A smart contract is a **self-executing program** that automates the actions required in an agreement or contract.

- Once completed, the transactions are trackable and irreversible.

Investopedia.com

How do you make a program self-executable?

- You need
  - An execution platform such as a Virtual Machine
  - An event handling Interface
  - A way for the program to handle events and execute appropriate event-handling function causing state transitions
  - Deterministic Execution of Event handlers

- Are Event based programs such as GUIs or Web applications smart Contracts?
  - Is the state change irreversible?
  - Is the state change history immutable?
  - Is the state trajectory trackable?
  - Is the state information highly available?
  - Is the state information transparent?
  - Is the state change verifiable by anyone?

Investopedia.com

Smart Contract Execution Eco-System

- Execution may require authentication
- Execution must be deterministic
- State must be replicated for high availability
- Public part of the State must be transparently visible
- History of the state change must be immutable
- The state changes must be verifiable by any one

Investopedia.com

Blockchain as a Smart Contract Execution Platform

- Blockchain with a virtual execution engine such as ethereum virtual machine provides:
  - An execution platform that replicates execution across multiple nodes
  - Public state change is a transaction and recorded in the blocks
  - State change history is immutable
  - Any validating node can also execute the program to verify the state change
  - The replication of execution provides availability
  - Anyone with access to the blocks can track the entire state trajectory

When does an Web Application Suffice?

- An Web Application is a self-executing program that respond to user events (transactions) and makes changes to data store and state of the program
- Why not use a web application as a “smart” contract?
  - You have no visibility to the application code and its execution states (transparency)
  - You have no access to the history of execution and whether the history of data store changes are immutable (integrity)
  - Peer to peer transactions going into a blackbox and trust is not built (trust between parties)
  - Friction in peer-to-peer transactions
  - Privacy

IMPLEMENTATIONs

LAND RECORDS MANAGEMENT

Implemented in Karnataka
Planned in UP

ADVANCING E-PROCUREMENT

Implemented in Karnataka

VERIFIABLE CREDENTIALS VIA SELF-SOVEREIGN MECHANISM

Implemented in IITK, IITI, IGNOU, AKTU, NITR, NSDC

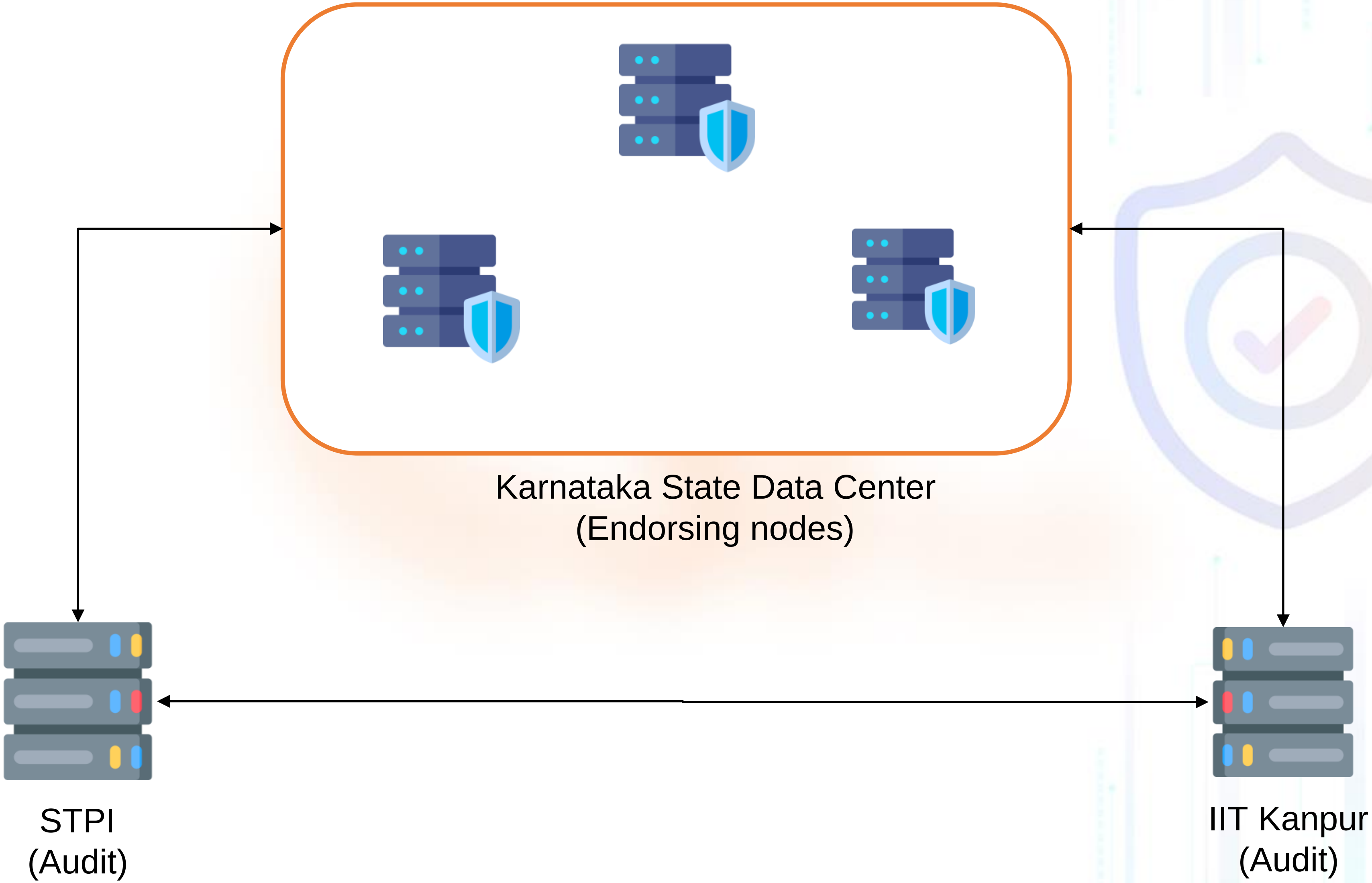
TRANSFERRABLE DEVELOPMENT RIGHTS

Being Implemented in Kanpur

4 major projects

- Blockchain Based Land Record Registry
  - Kaveri Blockchain Project – State of Karnataka
- Blockchain Based eProcurement Integration
  - Karnataka Government – eGovernance Department
- Self-sovereign Identity (SSI)
  - SSI Based Degrees at IIT Kanpur, IIT Indore, IGNOU, NIT Rourkela
- Transferrable Digital Rights
  - Kanpur Development Authority – Token based DRCs

KAVERI BLOCKCHAIN SOLUTION - OVERVIEW

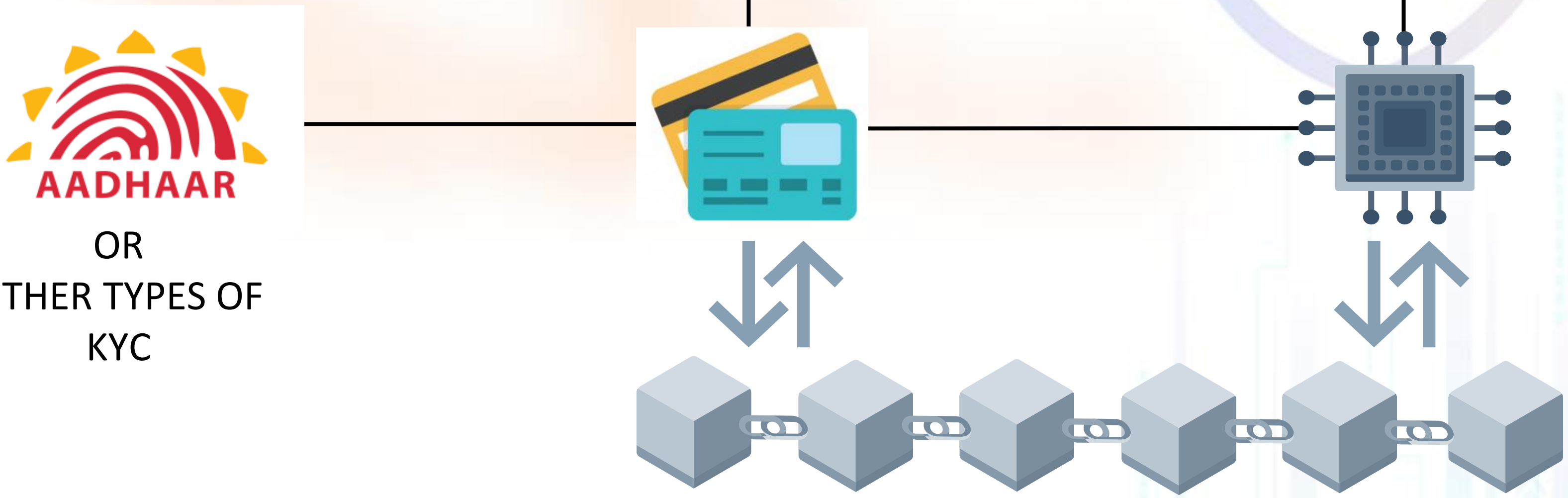


KAVERI SOLUTION - OVERVIEW

PROOF OF IDENTITY

PROOF OF OWNERSHIP

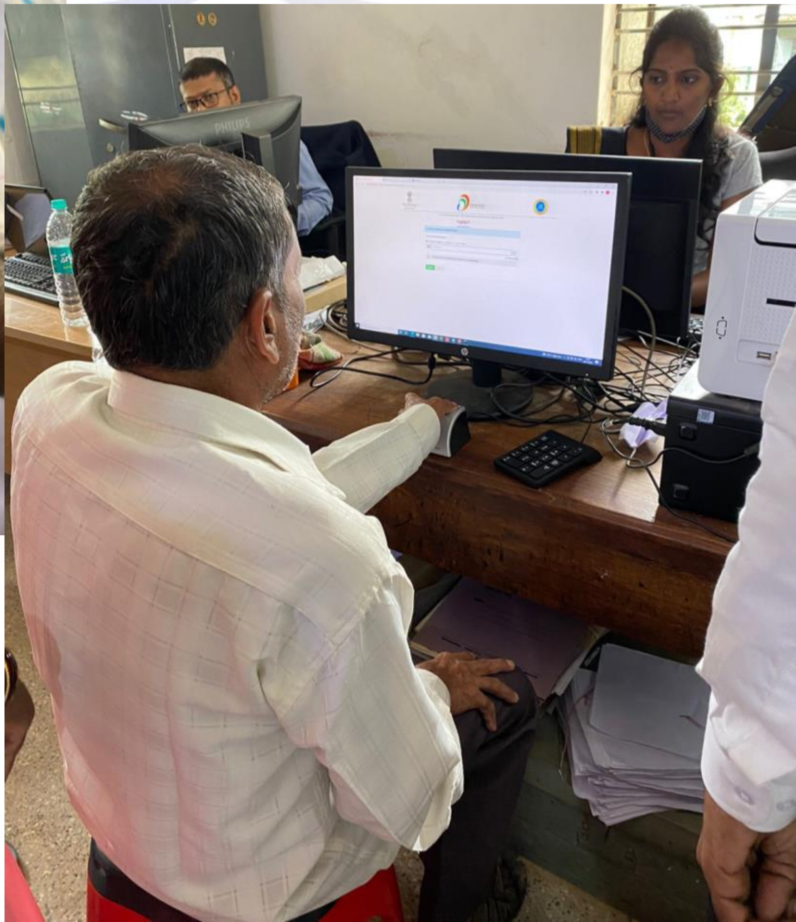
PROOF OF CONSENT



OR
OTHER TYPES OF
KYC

Permissioned Blockchain

Glimpses



eProcurement Integration Problem

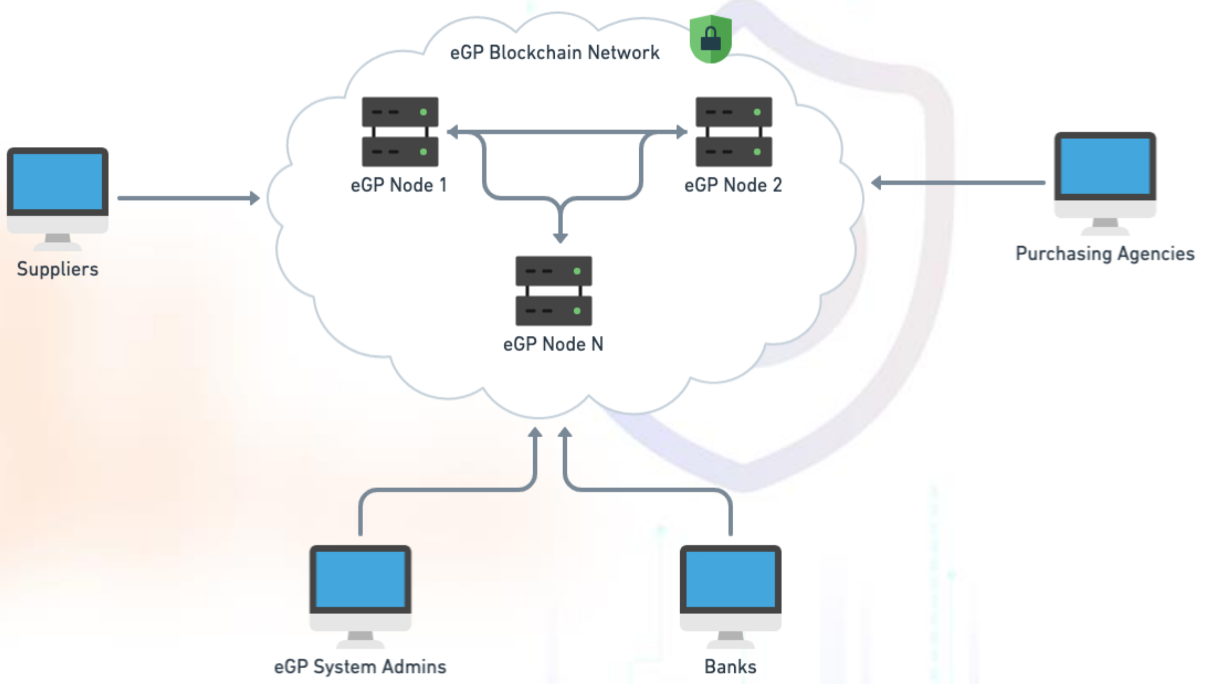
•Multiple e-Government Procurement Portals across the Country with no shared view

Suppliers manage different identities which are not interoperable

Lack of Real-time view of contracts pending completion and standardization of work experience certificates

Solution

- A permissioned blockchain network setup between the e-GP Systems across the country
- Governed by the terms and conditions decided by the consortium of these e-GP Systems
- Will act as the national de-duplicated supplier datastore, with award of contracts and work experience certificates linked to supplier identity
- The supplier will be able to retrieve all the relevant data across all the e-GP Systems



STATUS

e-Government Procurement Blockchain network went in live in January 2022. The government of Karnataka has onboarded the following States on the network

- Telangana
- Andhra Pradesh
- Chhattisgarh
- Assam

Following banks have also been onboarded to the network

- SBI
- Canara
- HDFC

C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

Transferable Development Rights

What is TDR

A concept used in town planning where land is acquired for development projects

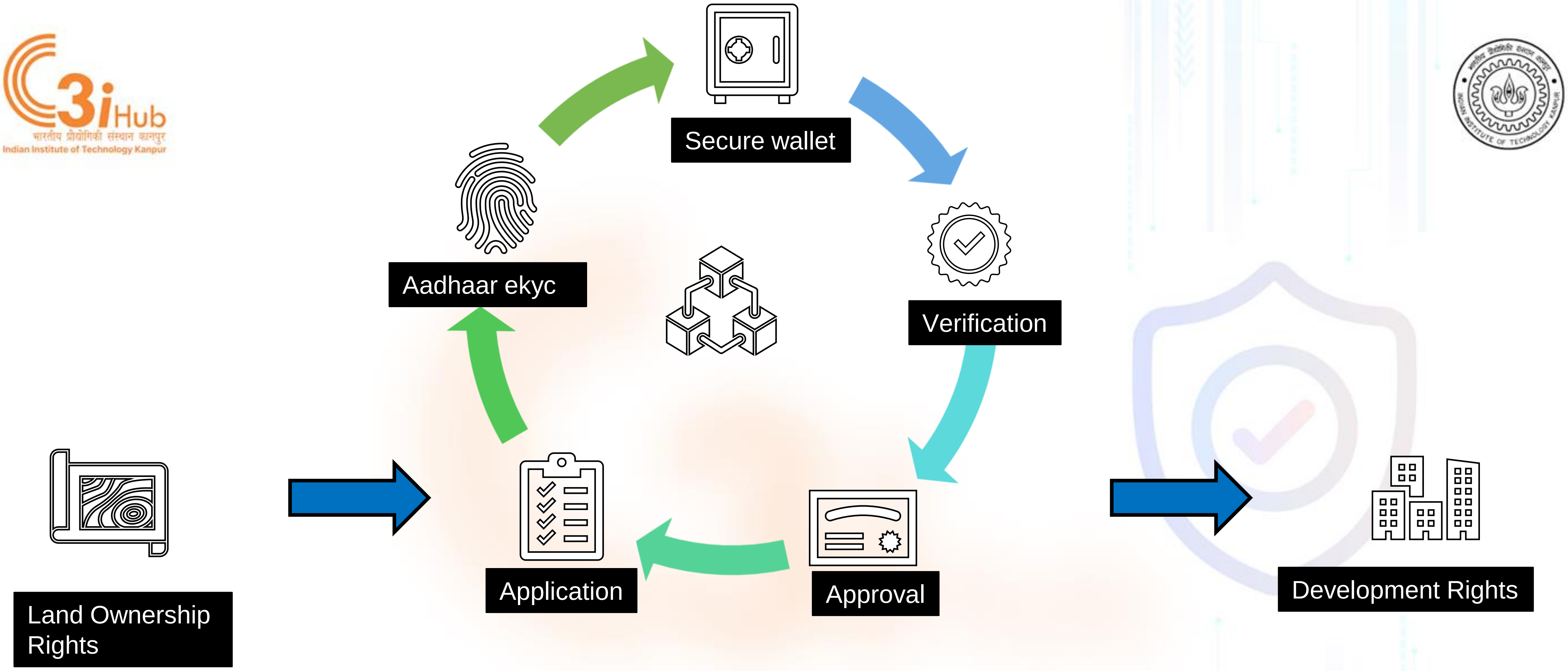
Instead of paying monetary compensation, the land owner is given development rights, which he can either use himself or sell to another entity for use in development projects.

Helps development authorities acquire land without the burden of monetary compensation and provides landowners with an alternative form of compensation.

Implemented through the issuance of certificates, known as Development Rights Certificates (DRC), which represent the development rights.

C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

Solution Overview



Land Ownership Rights

Application

Aadhaar ekyc

Secure wallet

Verification

Approval

Development Rights

Advantages

- Marketplace for Development rights
- Integrated with Building Plan Approval Portal
- Timebound Delivery of Service
- Encrypted Wallet
- Aadhar Based Identification
- Traceable Ownership of Rights
- Non-Repudiable Consent

Self Sovereign Identity

A digital identity ecosystem enabling trusted, verifiable and privacy-preserving credential exchange interactions.

Self sovereign identity

Self Sovereignty - User

- Data under complete control and ownership of the user.
- Can be shared as and when the user wants.

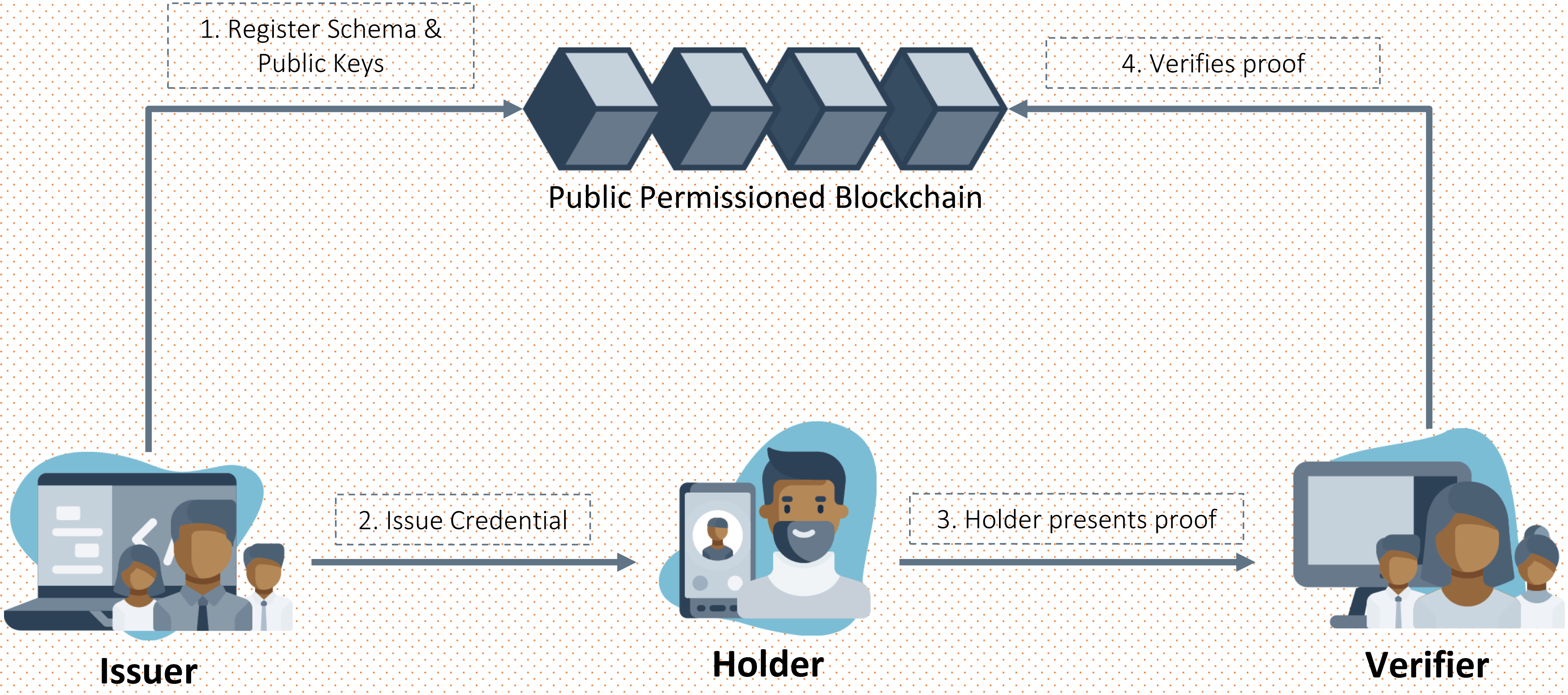
Verifiable Credentials

- Digital counterparts of credentials like Aadhaar, D/L, PAN, etc. with added features like digital signatures.
- Standardized at World Wide Web Consortium (W3C)

Digital Wallet

- Data is stored locally in an encrypted format.
- It is used to create and share cryptographic proofs with verifiers.
- Each user owns a wallet.

Self sovereign identity – how it works?



1. Register Schema & Public Keys

4. Verifies proof

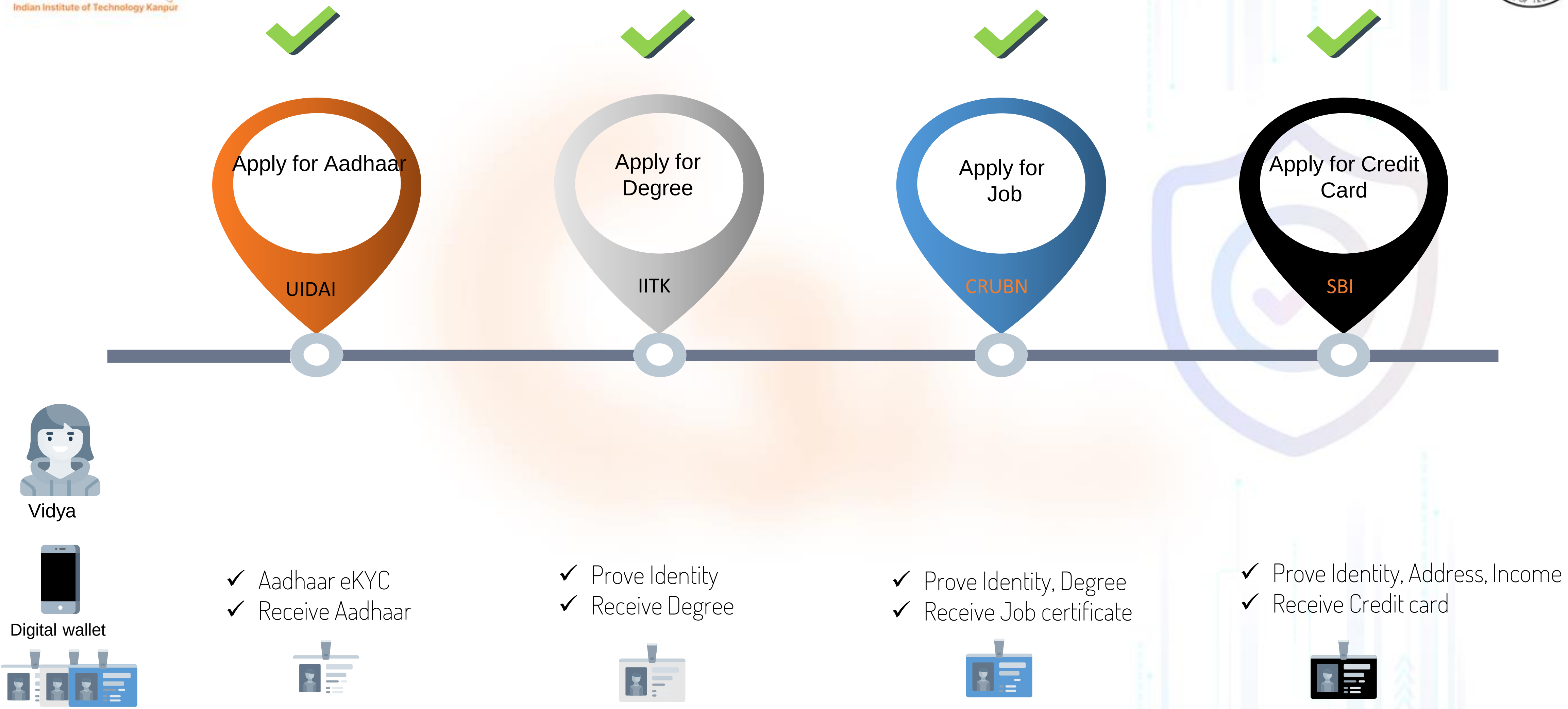
Public Permissioned Blockchain

2. Issue Credential

3. Holder presents proof

Note: The issued credential is stored on the mobile device of the holder

A Sample Journey



Apply for Aadhaar

UIDAI

Apply for Degree

IITK

Apply for Job

CRUBN

Apply for Credit Card

SBI

Vidya

Digital wallet

- ✓ Aadhaar eKYC
- ✓ Receive Aadhaar

- ✓ Prove Identity
- ✓ Receive Degree

- ✓ Prove Identity, Degree
- ✓ Receive Job certificate

- ✓ Prove Identity, Address, Income
- ✓ Receive Credit card

Features & benefits – SSI Ecosystem

Features

- Digital Wallet
- Selective Disclosure
- Non-transferable Proofs
- Zero-Knowledge Proofs
- Multi-credential Proofs
- Interoperability
- Secure and Private Channels
- Autofill

Benefits

- Reduced Correlation
- Data Minimization
- Reduced Identity Fraud
- Fewer Obligations (Verifiers)
- Instant Verification of documents
- Data Security
- Password-less login
- Extensible & Flexible