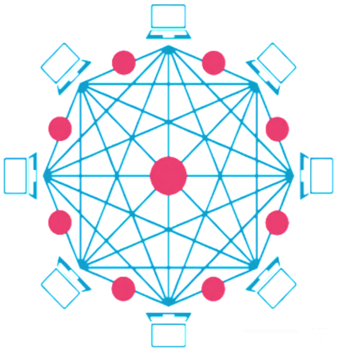
Blockchain Technology: Potential Applications and Practical Implementation

29th Nov 2019

Society for Electronic Transactions and Security (SETS), Chennai



P.R. Lakshmi Eswari

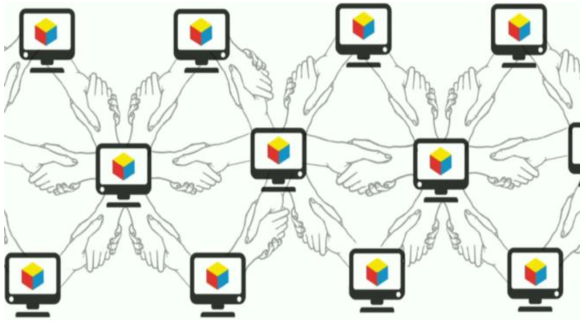
Centre for Development of Advanced Computing

Presentation Outline

- Overview of Blockchain Technology
- Global and National Scenario
- Potential Application Areas
- Efforts @ C-DAC
- Challenges to be addressed

Middleman Vs Trust Protocol

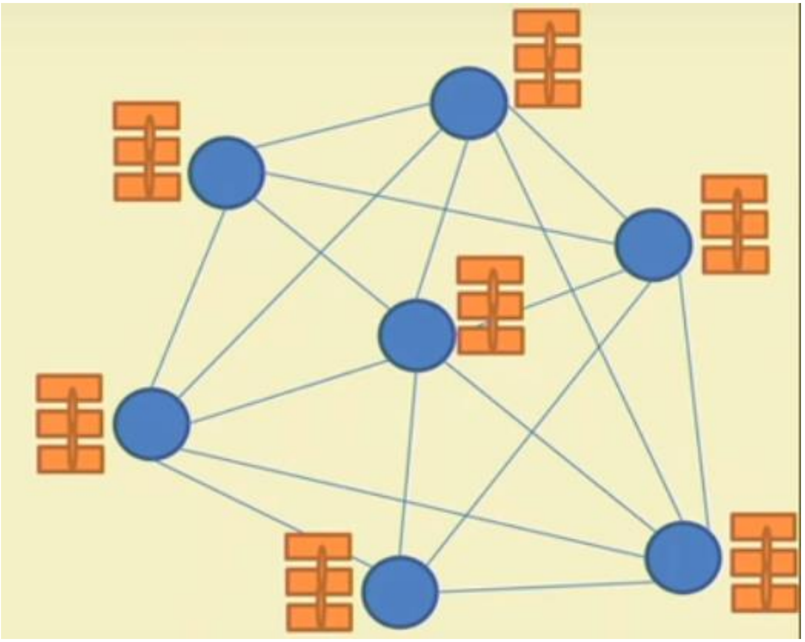
- Establishing Trust
- Verifying Identity in a transaction
- Clearing and Settling of transactions
- Keeping records of transactions



- Massive Collaboration
- Decentralized Control
- Cryptography
- Smart Code

What is a Blockchain?

- A decentralized computation and information sharing platform that enables multiple authoritative domains, who do not trust each other, to cooperate, coordinate and collaborate in a rational decision making process.
- Every node maintains a local copy of the database and they are identical.



https://blog.exchangeunion.com

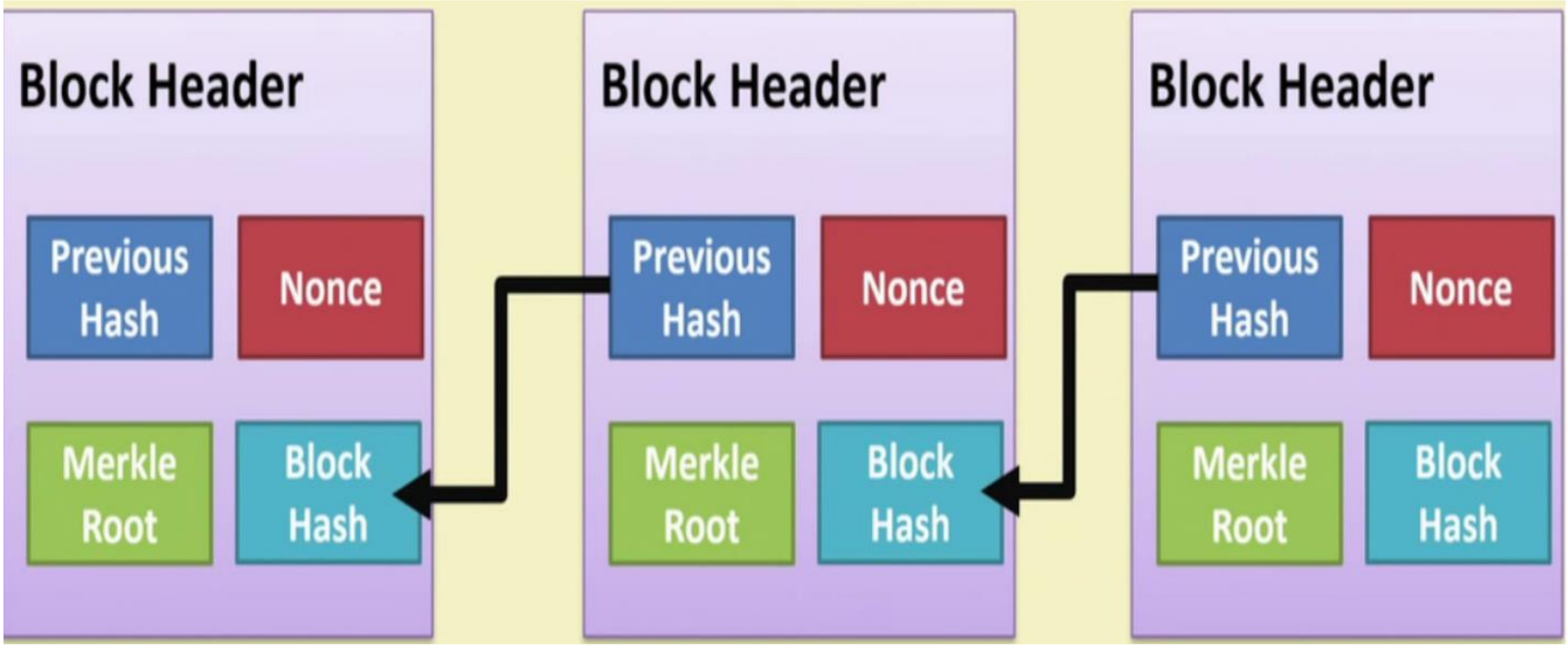
What is a Blockchain?

- Distributed Ledger which records any transaction or information chronologically, permanently and unalterably
- Uses one-way hash cryptography that is computationally impractical to break
- Is visible to all users (permissioned / permission less)
- Uses Peer-to-Peer transmission, with each node forwarding new transactional information to all others
- Can trigger transactions automatically, based on business logic and custom algorithms
- Verifies transactions through node consensus with no reliance on third-party intermediaries (e.g., clearinghouses)

Formal Definition of a Blockchain

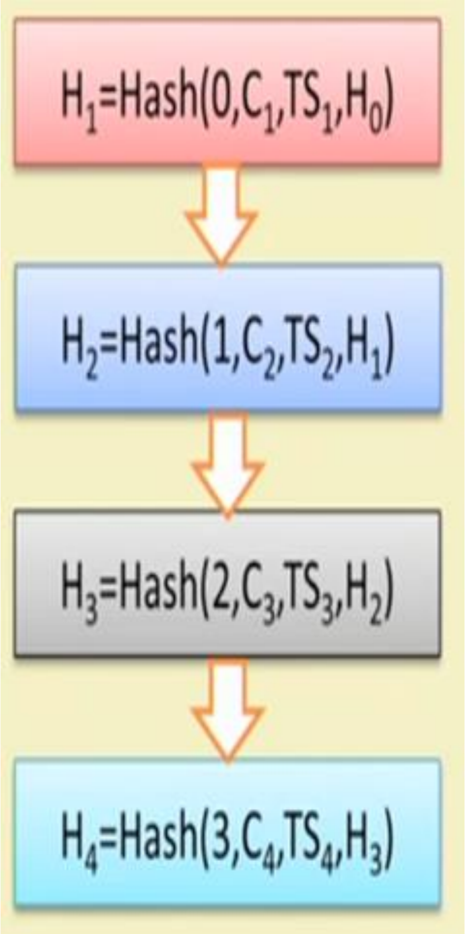
- A Blockchain is “an open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way” (lansiti, Lakhai 2017)
- Protocols for commitment, Consensus, Security and Privacy & authenticity

Blockchain as a Hashchain

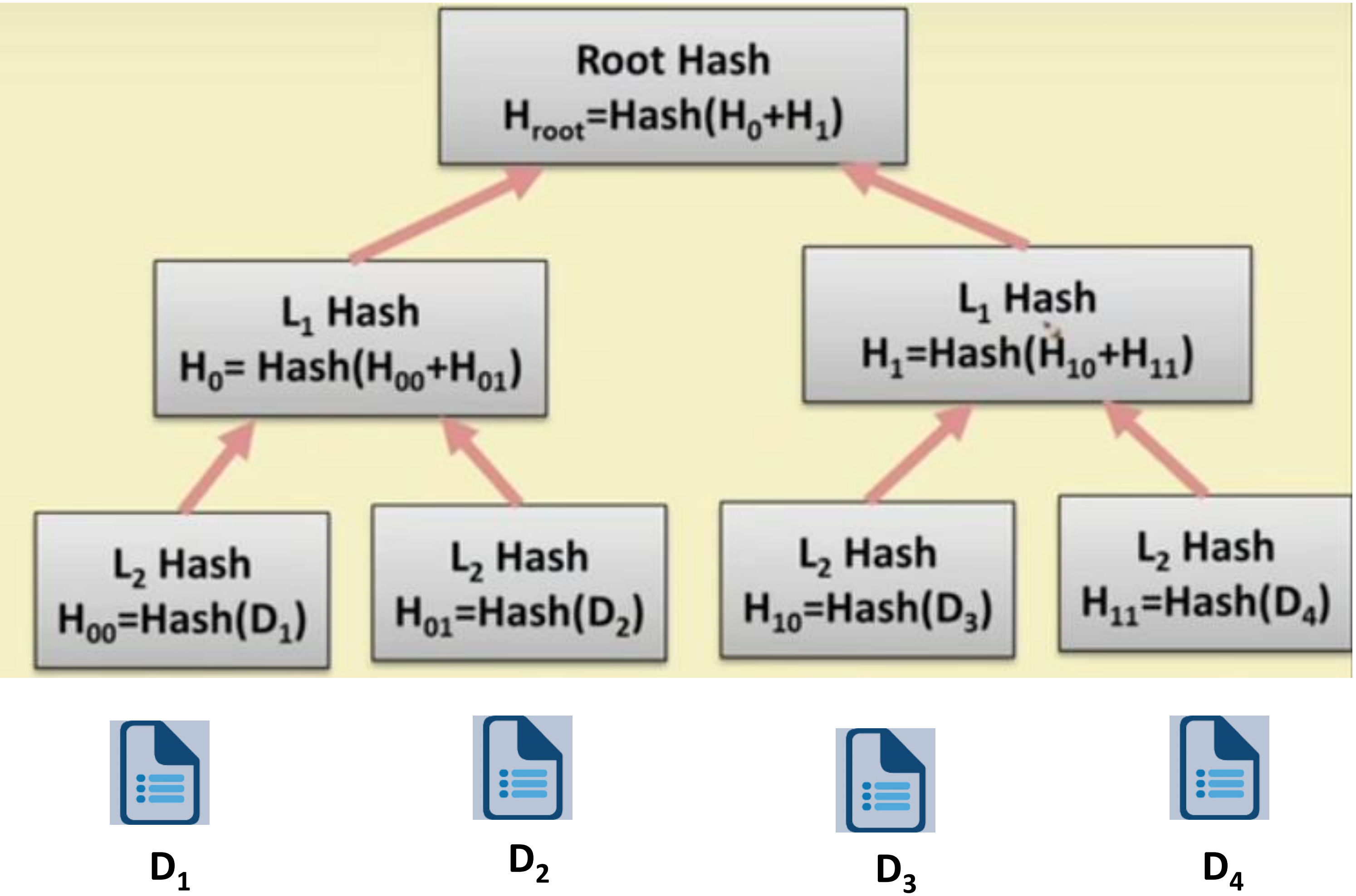


Cryptographically Secured Chain of Blocks

- The first use – **timestamp a digital document (Harber and Stometta, 1991)**
  - A sequence of timestamps [TS1, TS2, TS3, …] denoting when the document is created or edited
  - Whenever a client access a document, construct a block consisting of the sequence number of access, client ID, timestamp, a hash value from the previous request and the entire thing is hashed to connect it to the previous blocks


H_1=Hash(0,C_1,TS_1,H_0)
H_2=Hash(1,C_2,TS_2,H_1)
H_3=Hash(2,C_3,TS_3,H_2)
H_4=Hash(3,C_4,TS_4,H_3)

Merkle Trees (Ralph Merkle, 1979)



Root Hash

H_{root}=Hash(H_0+H_1)

L_1 Hash

H_0= Hash(H_{00}+H_{01})

L_1 Hash

H_1=Hash(H_{10}+H_{11})

L_2 Hash

H_{00}=Hash(D_1)

L_2 Hash

H_{01}=Hash(D_2)

L_2 Hash

H_{10}=Hash(D_3)

L_2 Hash

H_{11}=Hash(D_4)

D_1

D_2

D_3

D_4

Digital Signature

- Used to validate the origin of a transaction
  - Prevents non-repudiation
    - Alice cannot deny her own transactions
    - No one can claim Alice’s transaction as his/her own transaction

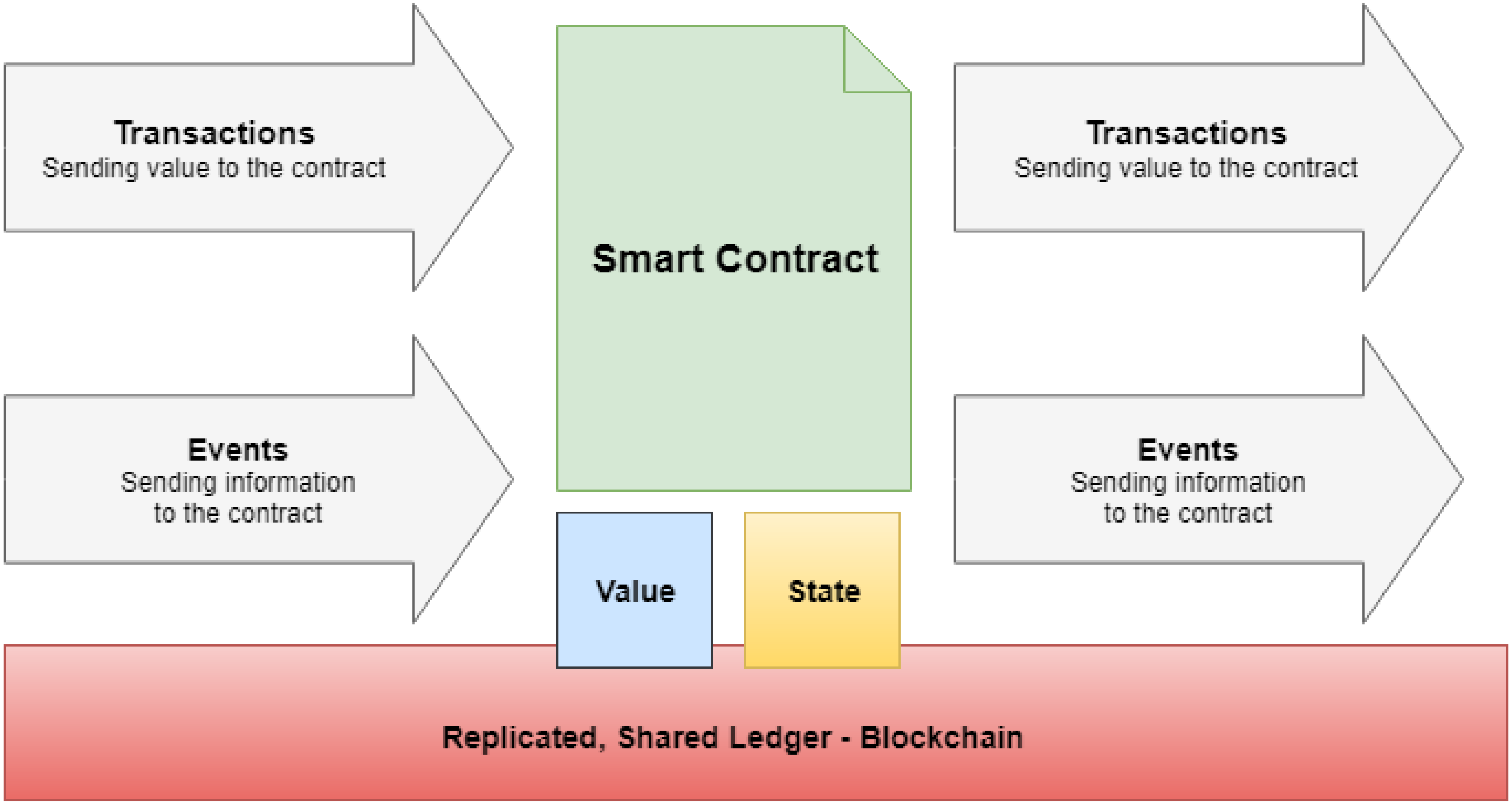
Puzzle Friendly

- Say M is chosen from a widely spread distribution; it is computionally difficult to compute k, such that $Z=H(M||k)$, where M and Z are known a priori.

- A Search Puzzle (used in Bitcoin Mining)
  - M and Z are given, k is the search solution

- Puzzle friendly property implies that random searching is the best strategy to solve the above puzzle

Smart Contract

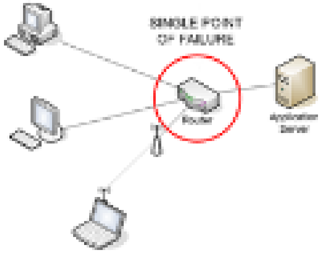


Important Characteristics

Transparency

Timestamped

Immutable



No Single Point of Failure

Irrevokable

Programmable

Blockchain - Purpose

- It facilitates the process of recording transactions and tracking assets in a business network

- An asset can be tangible a house, a car, cash, land — or intangible like intellectual property, such as patents, copyrights, or branding

- Anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved

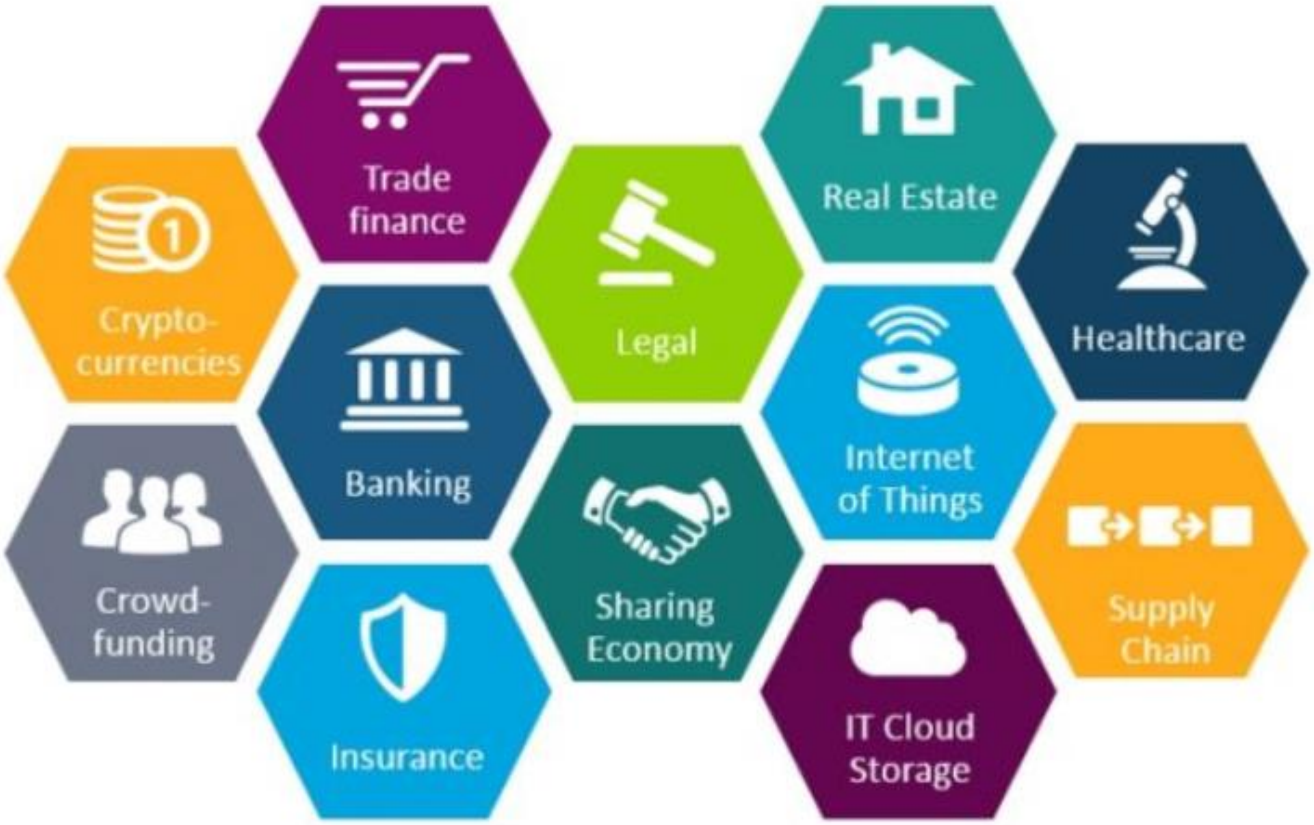
Models of Blockchain Network

- Two models of Blockchain network – Permission-less (an open environment) and Permissioned (a close environment)

- Permission-less model is suitable for open control-free financial applications like cryptocurrency -Biticoin

- Permissioned model is suitable for business applications

Application Domains



Blockchain in Government – Potential Benefits

- Building Trust with Citizens
- Improves Transparency and Accountability
- Speed up transactions
- Protecting Sensitive Data
- Reducing Costs & Improving Efficiency

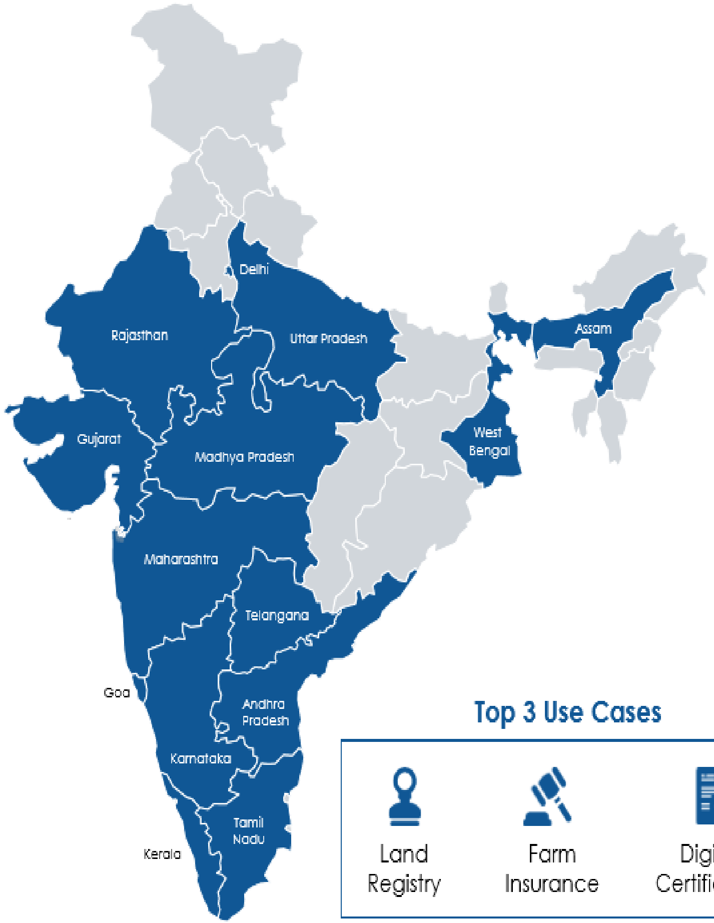
Blockchain and Government

- Identity Management (persons and legal entities)
- Official / public documents (licenses, certificates, taxes paid and so on)
- Property registration
- Government asset monitoring and management
- Government approval chain process
- Supply chain monitoring
- Government financing and budget allocations
- Voting and citizen consultations
- Energy grid management
- Healthcare monitoring and management

Global Scenario

- USA – Food and Drug inspection to address the problem of lack of transparency and security in health data processing.
- Estonia – KSI Unified platform integrates the vast quantity of sensitive data from health care, judiciary, legislature, security and commercial registries
- UK – Food standards agency – track the distribution of meat to enhance food traceability, land registration and property buy / sell process
- Brazil – public bidding of contracts with the governments, on-line bid solution to ensure secure and transparent deals for agriculture applications, student certificates and tracking student performance
- China – Secure health care data, logistic platform
- Swedan - For conducting real estate deals
- Dubai – Vision 2020 is to conduct all of its transaction using Blockchain
- Ghana - cadastral register based on the blockchain to collect property taxes on them

National Scenario



Top 3 Use Cases

- Land Registry
- Farm Insurance
- Digital Certificates

Andhra Pradesh

- Blockchain Database
- Cybersecurity
- Healthcare
- Land Registry
- Vehicle Title Registration

Assam

- Public Service Delivery

Delhi

- Monitoring Growth and Maintenance of Saplings and Plants

Goa

- Land Registry

Gujarat

- Fertilizer Subsidy Management
- e-Governance

Karnataka

- Agriculture
- Digital Certificates
- Forest and Land Acquisition
- Public Service Delivery
- Idea Marketplace
- IP Protection

Kerala

- Farm Insurance
- Agriculture Supply Chain

Madhya Pradesh

- Land Registry

Maharashtra

- Land Registry
- Digital Certifications
- Organ Transplants
- Rationing Distribution
- Farm Insurance

Rajasthan

- Electronic Health records (EHR)
- Land Registry

Tamil Nadu

- Agriculture
- Healthcare
- Education

Telangana

- Land Registry
- Chit Funds Operations
- Microfinance for SHGs
- Digital Education Certificates

Uttar Pradesh

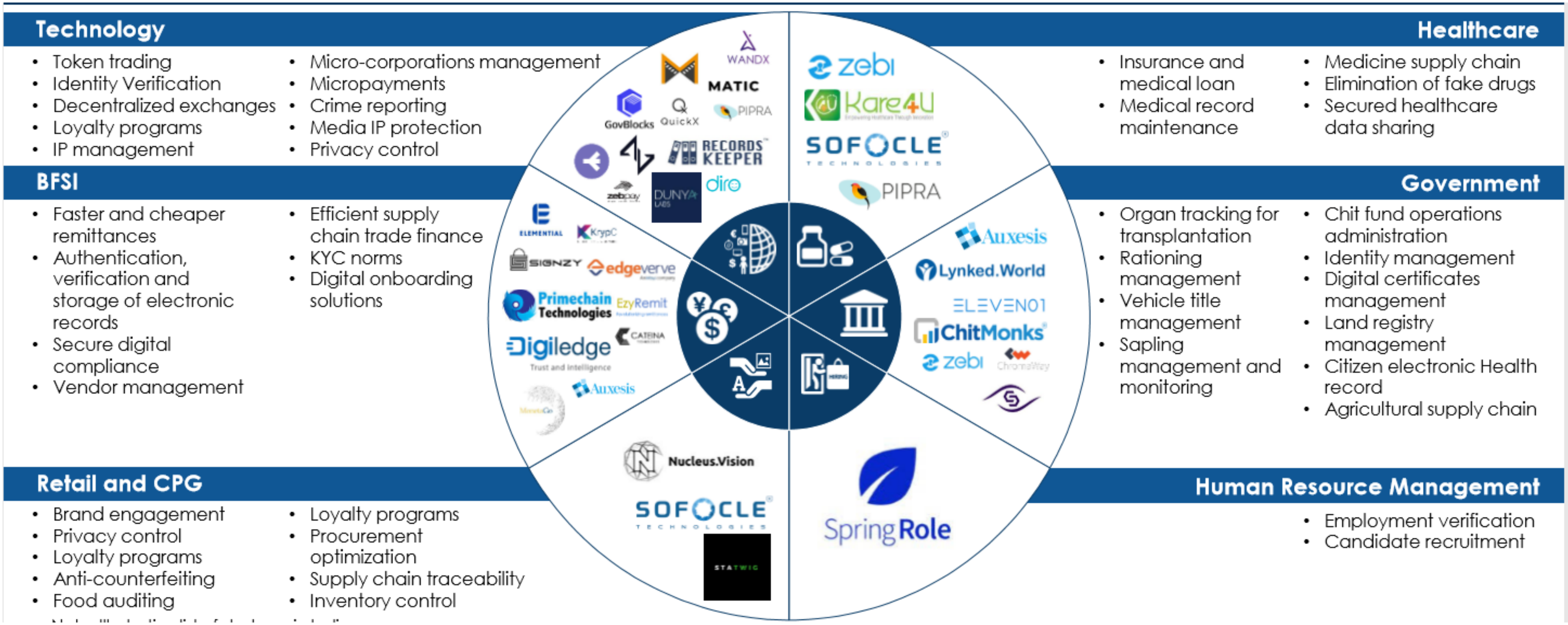
- Land Registry
- Power Sharing

West Bengal

- Land Registration
- Duty Payments
- Record Management
- Cybersecurity
- Digital Birth Certificates
- Data Management

Source: NASSCOM Avasant India Blockchain Report 2019

Start-ups in Blockchain



Technology

- Token trading
- Identity Verification
- Decentralized exchanges
- Loyalty programs
- IP management
- Micro-corporations management
- Micropayments
- Crime reporting
- Media IP protection
- Privacy control

Healthcare

- Insurance and medical loan
- Medical record maintenance
- Medicine supply chain
- Elimination of fake drugs
- Secured healthcare data sharing

BFSI

- Faster and cheaper remittances
- Authentication, verification and storage of electronic records
- Secure digital compliance
- Vendor management
- Efficient supply chain trade finance
- KYC norms
- Digital onboarding solutions

Government

- Organ tracking for transplantation
- Rationing management
- Vehicle title management
- Sapling management and monitoring
- Chit fund operations administration
- Identity management
- Digital certificates management
- Land registry management
- Citizen electronic Health record
- Agricultural supply chain

Retail and CPG

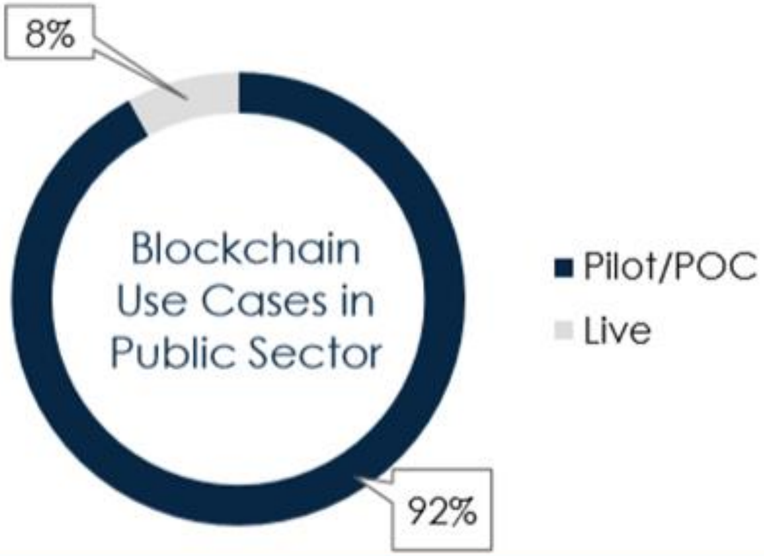
- Brand engagement
- Privacy control
- Loyalty programs
- Anti-counterfeiting
- Food auditing
- Loyalty programs
- Procurement optimization
- Supply chain traceability
- Inventory control

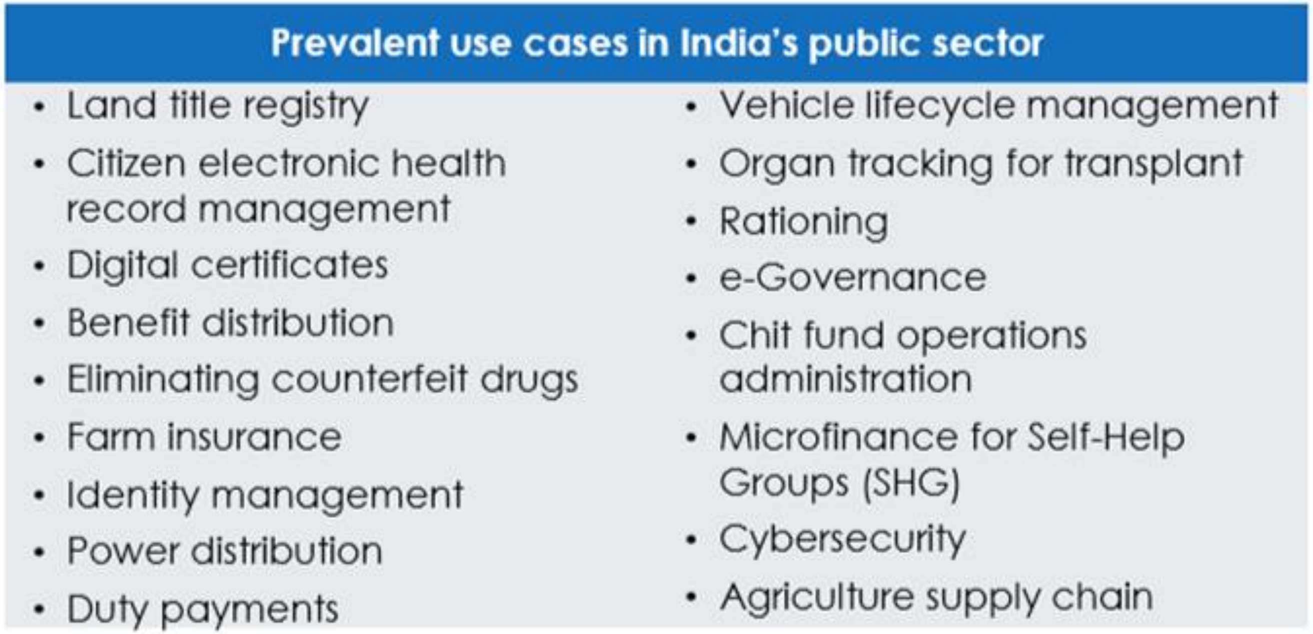
Human Resource Management

- Employment verification
- Candidate recruitment

Source: NASSCOM Avasant India Blockchain Report 2019

Blockchain based Application - Status





Prevalent use cases in India's public sector

- Land title registry
- Citizen electronic health record management
- Digital certificates
- Benefit distribution
- Eliminating counterfeit drugs
- Farm insurance
- Identity management
- Power distribution
- Duty payments
- Vehicle lifecycle management
- Organ tracking for transplant
- Rationing
- e-Governance
- Chit fund operations administration
- Microfinance for Self-Help Groups (SHG)
- Cybersecurity
- Agriculture supply chain

Source: NASSCOM Avasant India Blockchain Report 2019

Property Registration Management System

Property Registration – Potential Challenges

Based on the survey, following are the most common irregularities present in the existing property registration system

- Double Registration
- Producing Fake Documents for registration
- Insider Attack / Traditional database related attacks
  - DB Modification

Requirements

- Electronic Ledger
  - Reliable
  - Timestamped
  - Tamper-evident
  - Providing non-repudiable proof of each transaction
- Implicit Linked Document (Title History) Verification
- Ledger should be distributed to avoid single point of failure
- If any node is compromised, data can be recovered from other nodes
- Make records and contracts completely digital to facilitate automation

Proof-of-Existence

Motivation: Proof-of-Existence Framework

- Number of digital artefacts are generated by ICT systems
- Fake or fabricated documents is a big problem for important documents such as degree certificates, property records etc
  - Modification of content
  - Timestamp
  - Change of ownership
- Many document management systems lack
  - Transparency
  - Security
  - Efficiency

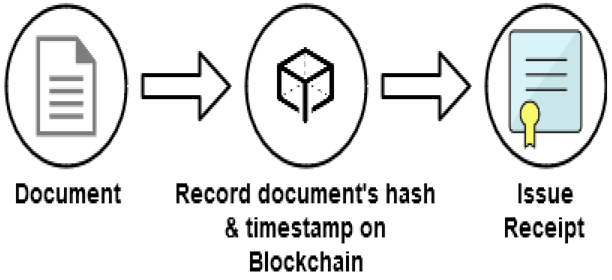
Blockchain based Proof of Existence as a Service (PoEaaS)

Benefits of PoE

1. Proves document ownership without revealing actual data
2. Records time stamp & proves digital artefact exists at a certain moment of time
3. Certify the existence of document without the need of a Central Authority
4. Ensures document integrity
5. Ensures that timestamp and hash of the documents cannot be tampered
6. Overcomes the limitation of storing large data directly in Blockchain Ledger with PoS

Technology Overview

Records the hash of digital artefact

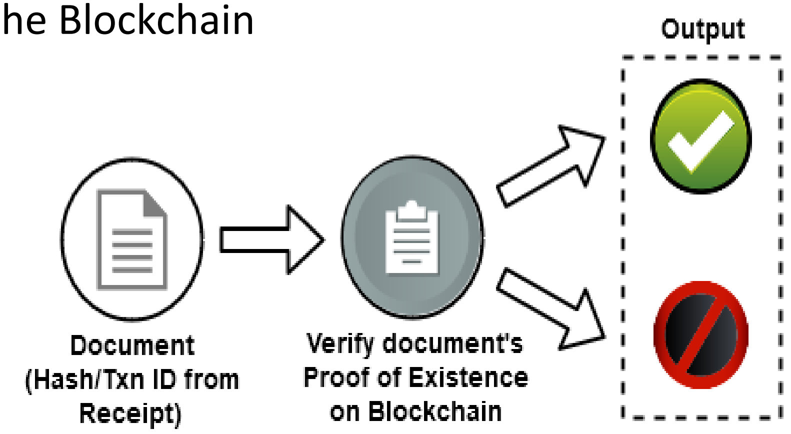


Document

Record document's hash & timestamp on Blockchain

Issue Receipt

Allows verifying the existence of a digital artefact's hash on the Blockchain

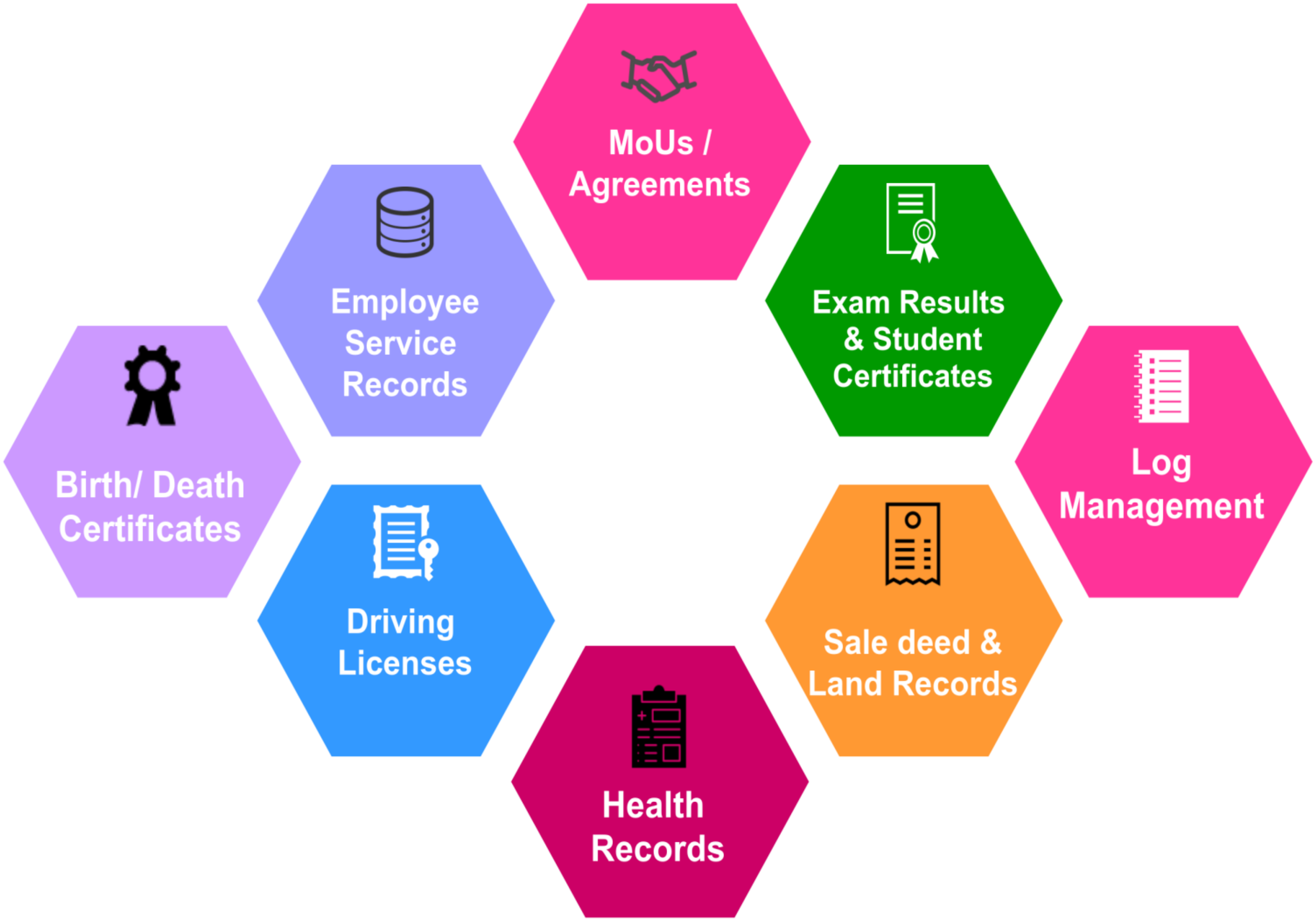


Output

Document (Hash/Txn ID from Receipt)

Verify document's Proof of Existence on Blockchain

Application Domains in Government



MoUs / Agreements

Employee Service Records

Exam Results & Student Certificates

Birth/ Death Certificates

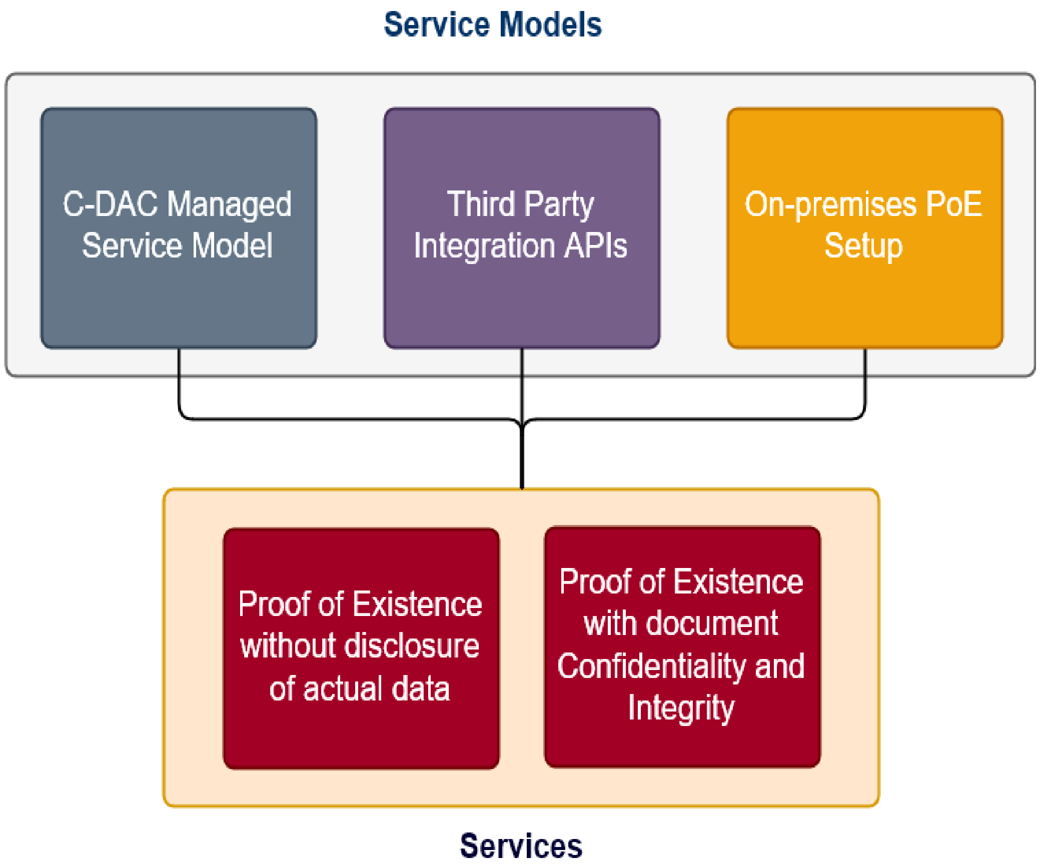
Log Management

Driving Licenses

Sale deed & Land Records

Health Records

Blockchain based Proof of Existence as a Service (PoEaaS)

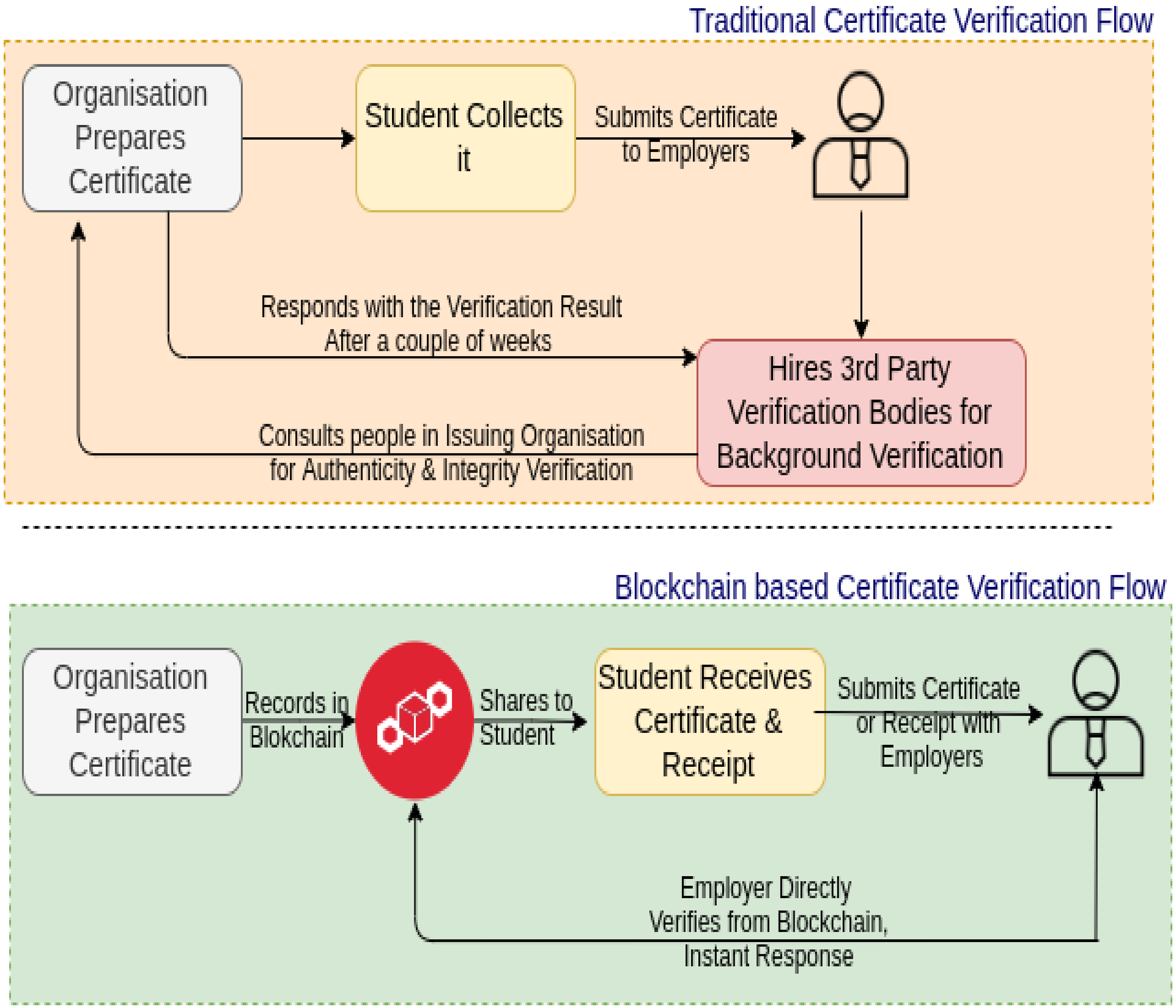

Service Models
C-DAC Managed Service Model
Third Party Integration APIs
On-premises PoE Setup
Proof of Existence without disclosure of actual data
Proof of Existence with document Confidentiality and Integrity
Services

- **Managed Service Model:**
  - C-DAC maintains the required infrastructure for the application
- **Third party Integration APIs:**
  - Applications can easily integrate PoE by calling REST APIs while C-DAC would maintain all the required infrastructure
- **On-Premises PoE Setup:**
  - C-DAC would provide the consultancy in architecting, designing, and hand-holding for a full fledged in-premise deployment.

In all the service models, the user can optionally store the document (Proof of Storage) along with the hash of the document

Blockchain based Educational Certificate Verification Application

Traditional vs Blockchain based Certificate Verification System


Traditional Certificate Verification Flow

Organisation Prepares Certificate

Student Collects it

Submits Certificate to Employers

Hires 3rd Party Verification Bodies for Background Verification

Consults people in Issuing Organisation for Authenticity & Integrity Verification

Responds with the Verification Result After a couple of weeks

Blockchain based Certificate Verification Flow

Organisation Prepares Certificate

Records in Blockchain

Shares to Student

Student Receives Certificate & Receipt

Submits Certificate or Receipt with Employers

Employer Directly Verifies from Blockchain, Instant Response

Challenges to be addressed

- Scalability and Transaction Speed (achieving higher number of transactions per second)
- Security Analysis
- Data Security and Privacy
- Standardization and Interoperability (cross-platform and cross-chain protocols)
- Regulatory Aspects
- Ecosystem and supporting framework
- Decentralized Infrastructure
- Skilled Manpower (Talent)

Acknowledgements

- Ministry of Electronics and Information Technology (MeitY), Government of India
- Working Group members and Project Review and Steering Group (PRSG) members
- Telangana State Government
  - Information Technology, Electronics & Communications Department (ITE&C Department)
  - Stamps & Registration Department
  - National Informatics Centre (NIC)

Thank You

(cdacchain@cdac.in / esuraksha@cdac.in)