Introduction to Blockchain Technology & Benefits

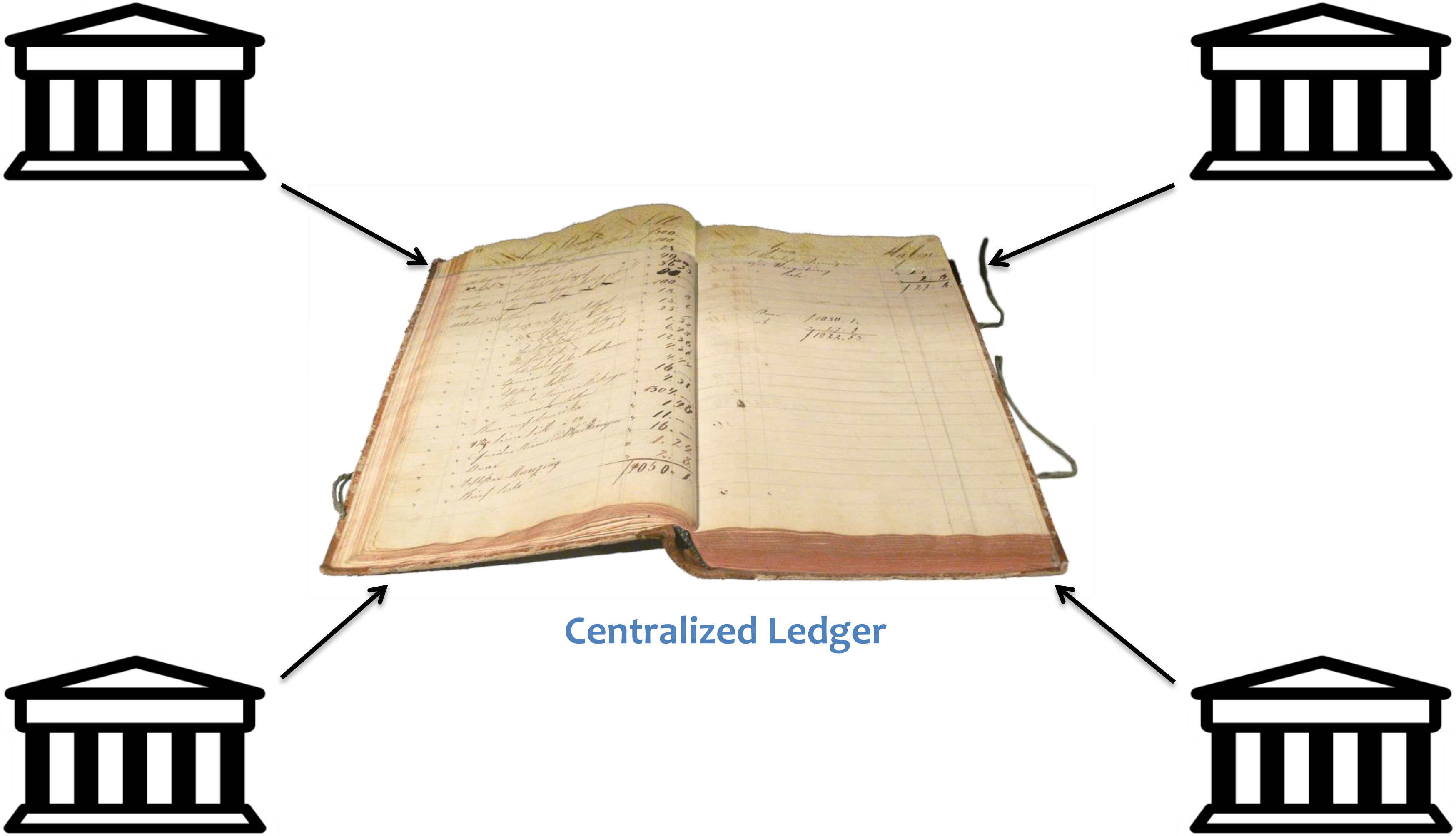
By
Ravi Kishore K,
C-DAC, Hyderabad.

What is Not a Blockchain

- Blockchain is **NOT a cryptocurrency**
- Blockchain is **NOT a programming language**
- Blockchain is **NOT a cryptographic codification**.

"Blockchain is the technology. Bitcoin is merely the first mainstream manifestation of its potential" — Marc Kenigsberg.

Legacy Ledgers

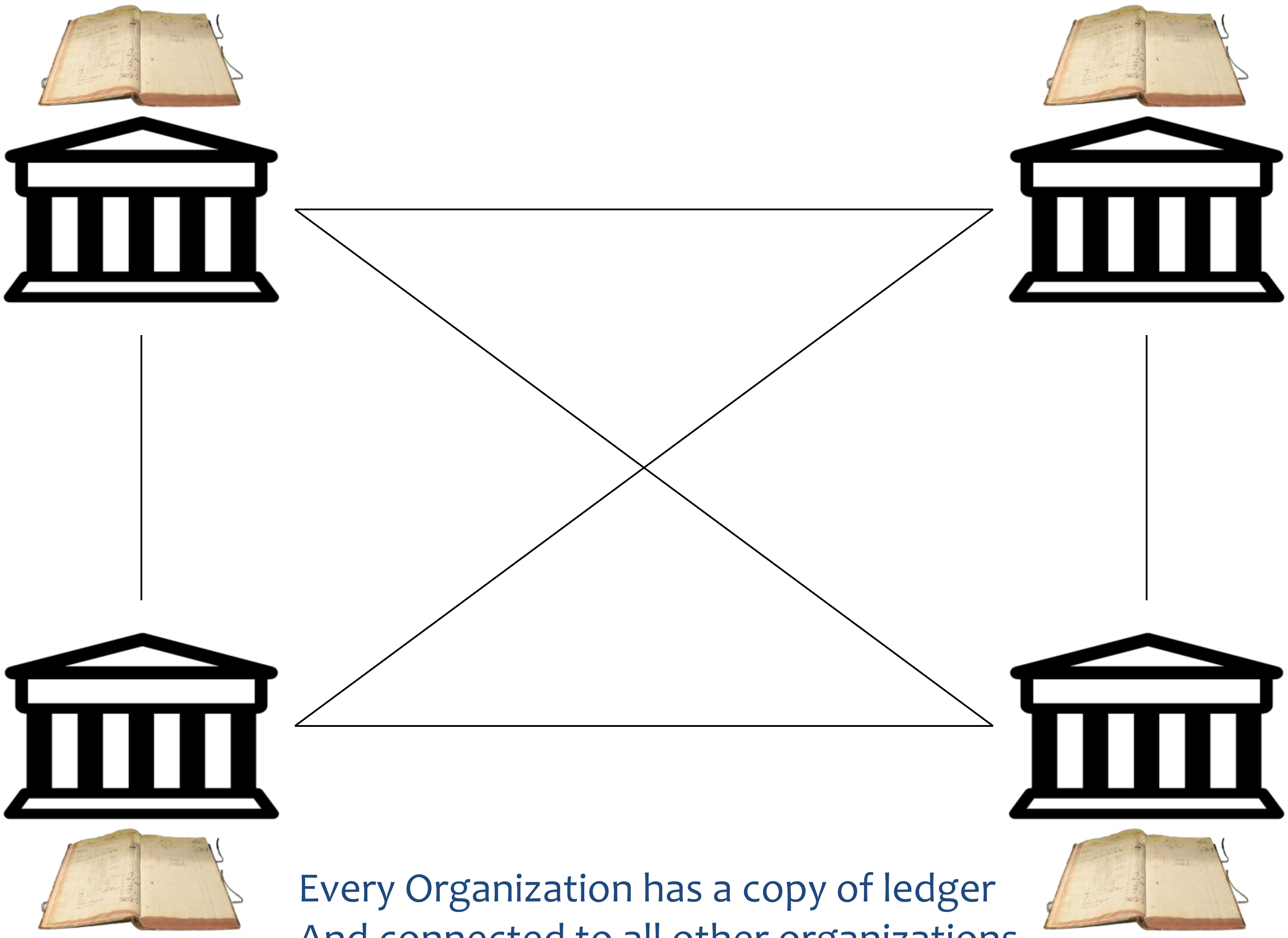


Centralized Ledger

Problems with current business ledgers

- Subject to misuse
- Tamperable
- Lack of transparency
- Inefficient

Distributed Ledger



Every Organization has a copy of ledger
And connected to all other organizations

Distributed Ledger Example

PUBLIC LEDGER

DR GULATI

Rs 1000/-

PUBLIC LEDGER

BUSINESS MAN

Rs 1000/-

PUBLIC LEDGER

CABLE WALA

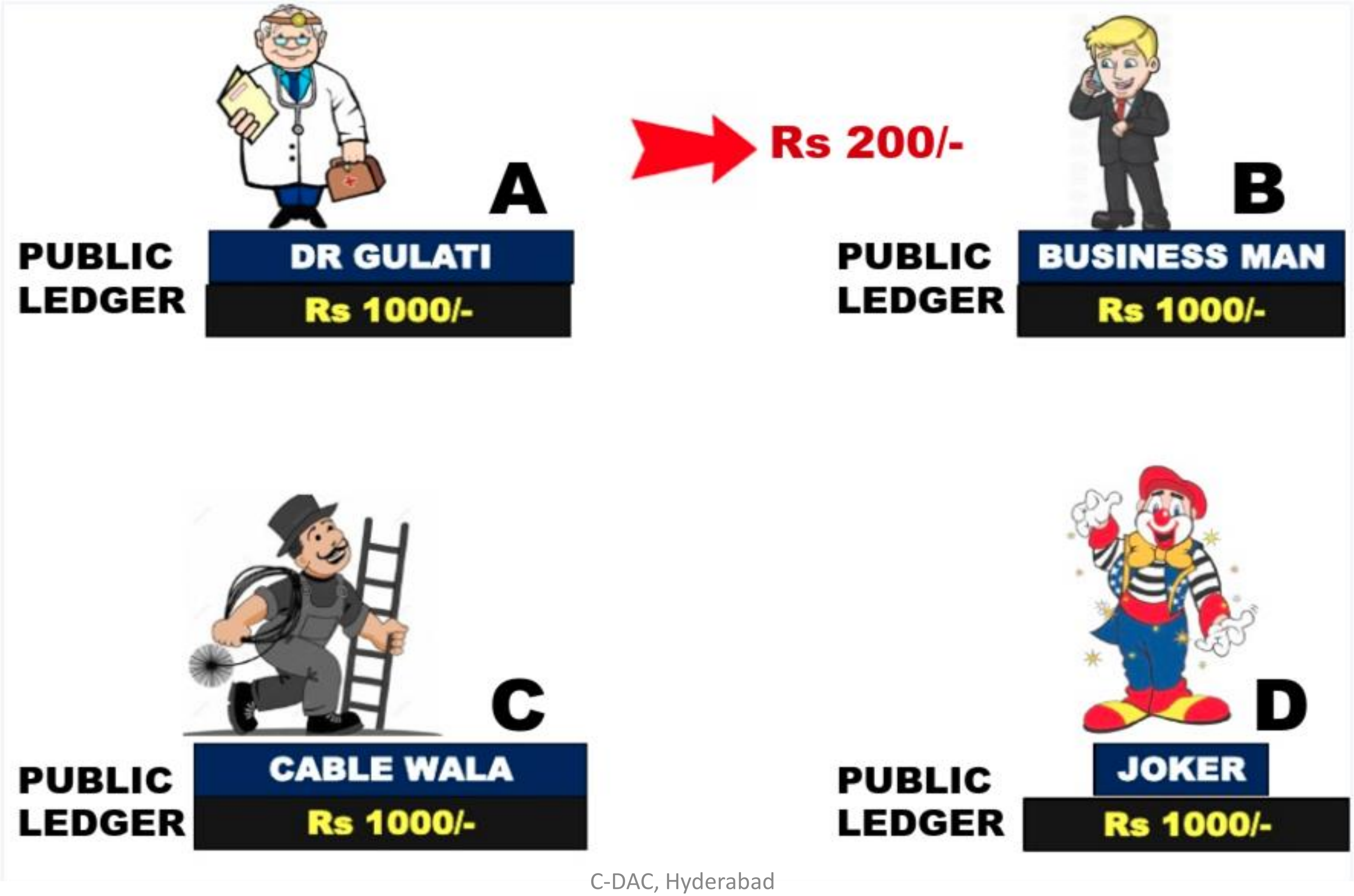
Rs 1000/-

PUBLIC LEDGER

JOKER

Rs 1000/-

Distributed Ledger Example



Distributed Ledger Example

A

PUBLIC LEDGER

DR GULATI

Rs 1000/-

A>B Rs 200

B

PUBLIC LEDGER

BUSINESS MAN

Rs 1000/-

A>B Rs 200

C

PUBLIC LEDGER

CABLE WALA

Rs 1000/-

A>B Rs 200

D

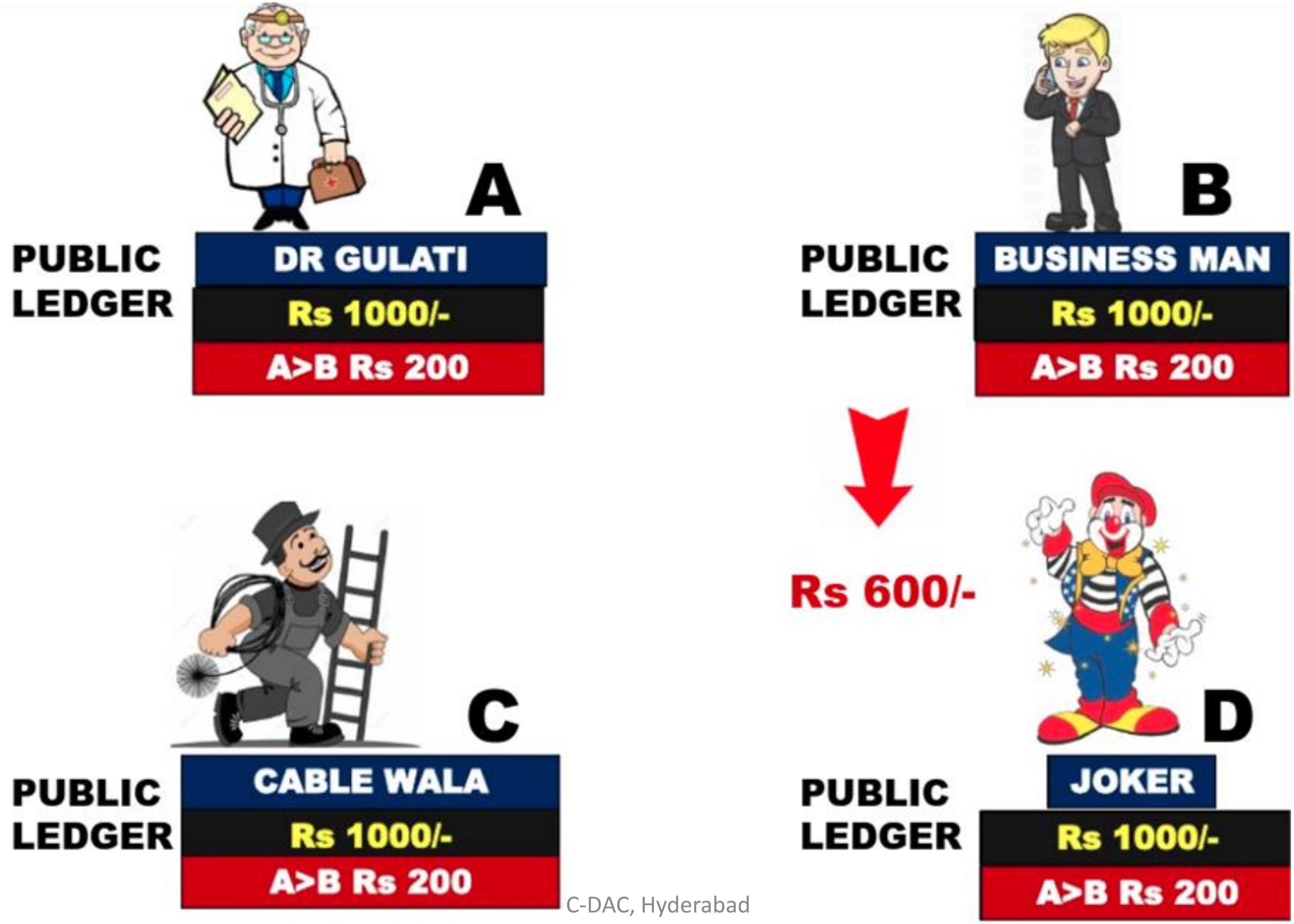
PUBLIC LEDGER

JOKER

Rs 1000/-

A>B Rs 200

Distributed Ledger Example



Distributed Ledger Example

PUBLIC LEDGER

DR GULATI
Rs 1000/-
A>B Rs 200
B>D Rs 600

PUBLIC LEDGER

BUSINESS MAN
Rs 1000/-
A>B Rs 200
B>D Rs 600

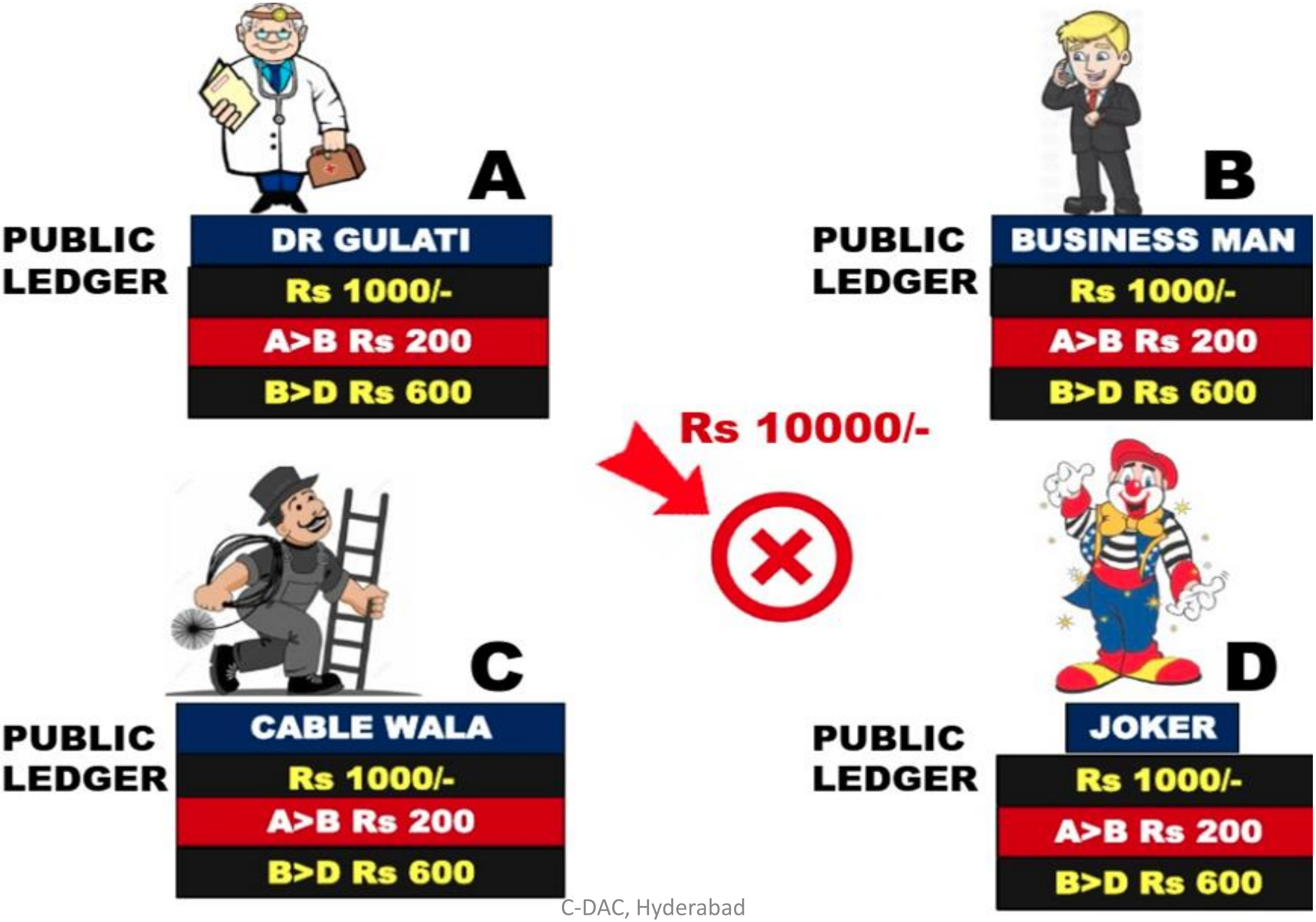
PUBLIC LEDGER

CABLE WALA
Rs 1000/-
A>B Rs 200
B>D Rs 600

PUBLIC LEDGER

JOKER
Rs 1000/-
A>B Rs 200
B>D Rs 600

Distributed Ledger Example



A

PUBLIC LEDGER

DR GULATI

Rs 1000/-

A>B Rs 200

B>D Rs 600

B

PUBLIC LEDGER

BUSINESS MAN

Rs 1000/-

A>B Rs 200

B>D Rs 600

Rs 10000/-

C

PUBLIC LEDGER

CABLE WALA

Rs 1000/-

A>B Rs 200

B>D Rs 600

D

PUBLIC LEDGER

JOKER

Rs 1000/-

A>B Rs 200

B>D Rs 600

Blockchain is a

Distributed **Ledger,**

has a network of replicated databases,

Synchronized via Internet,

visible to all network participants

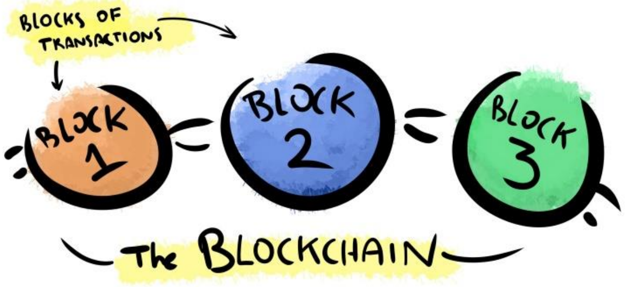
Blockchain in a nutshell

- Many computers are connected in a network without any hierarchy (peer to peer network)

- These computers verify all transactions one by one

- A set of Verified transactions over a time period are added in a “Block (similar to a page in ledger book)” of information

- All the Blocks are chained cryptographically and downloaded onto each computer



How to Sync distributed copies of Ledgers ???

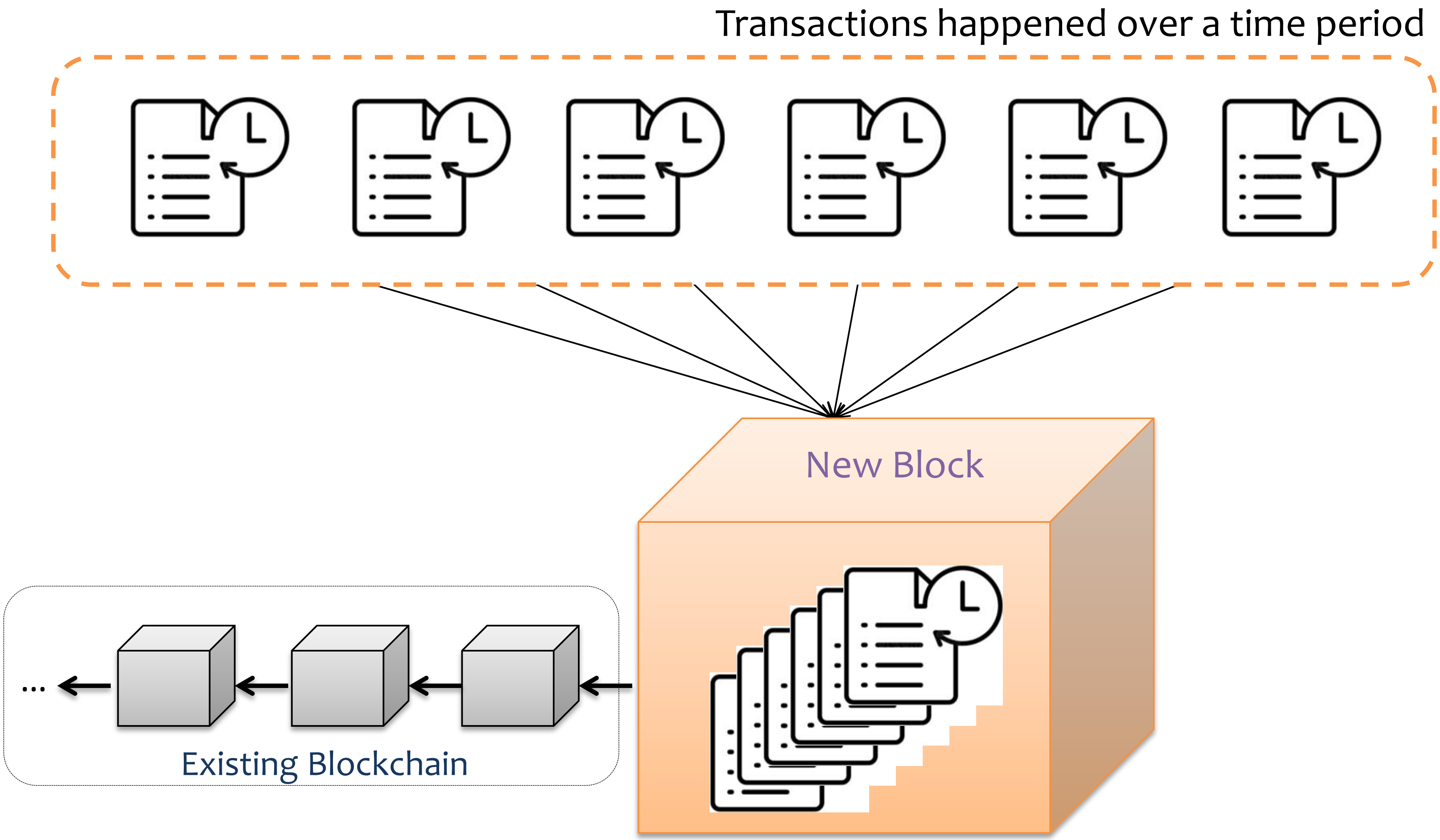
Consensus

- Instead of relying on a third party to mediate transactions, members in the Blockchain network uses a **consensus protocol** to agree on ledger content

- **Consensus** ensures that the shared ledgers are exact copies in all the nodes of distributed systems

- For updating the distributed ledger, consensus is required among the participants of the network
    - Ensures No Malicious Transactions nor Changes can be made on the distributed network

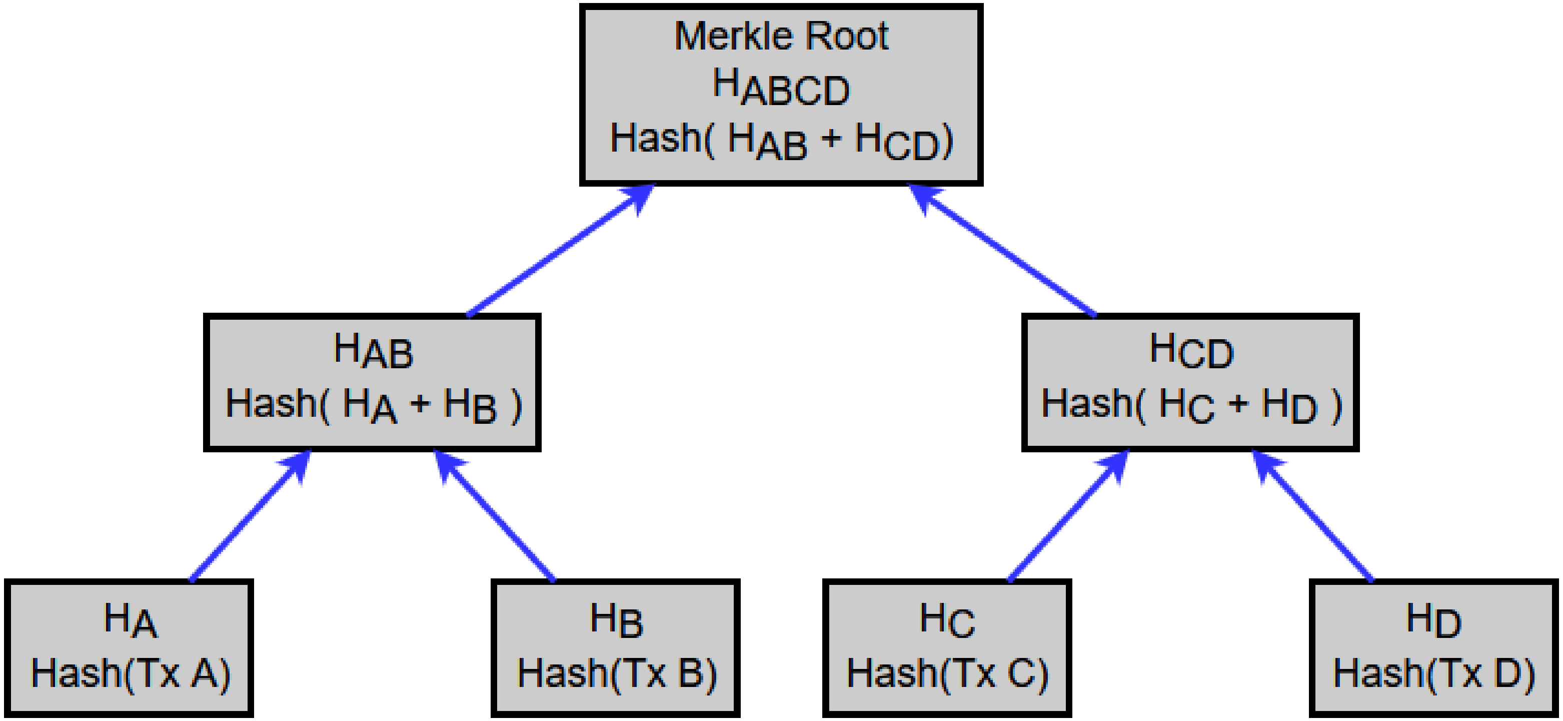
How Blockchain Creates a New Block?



Transactions

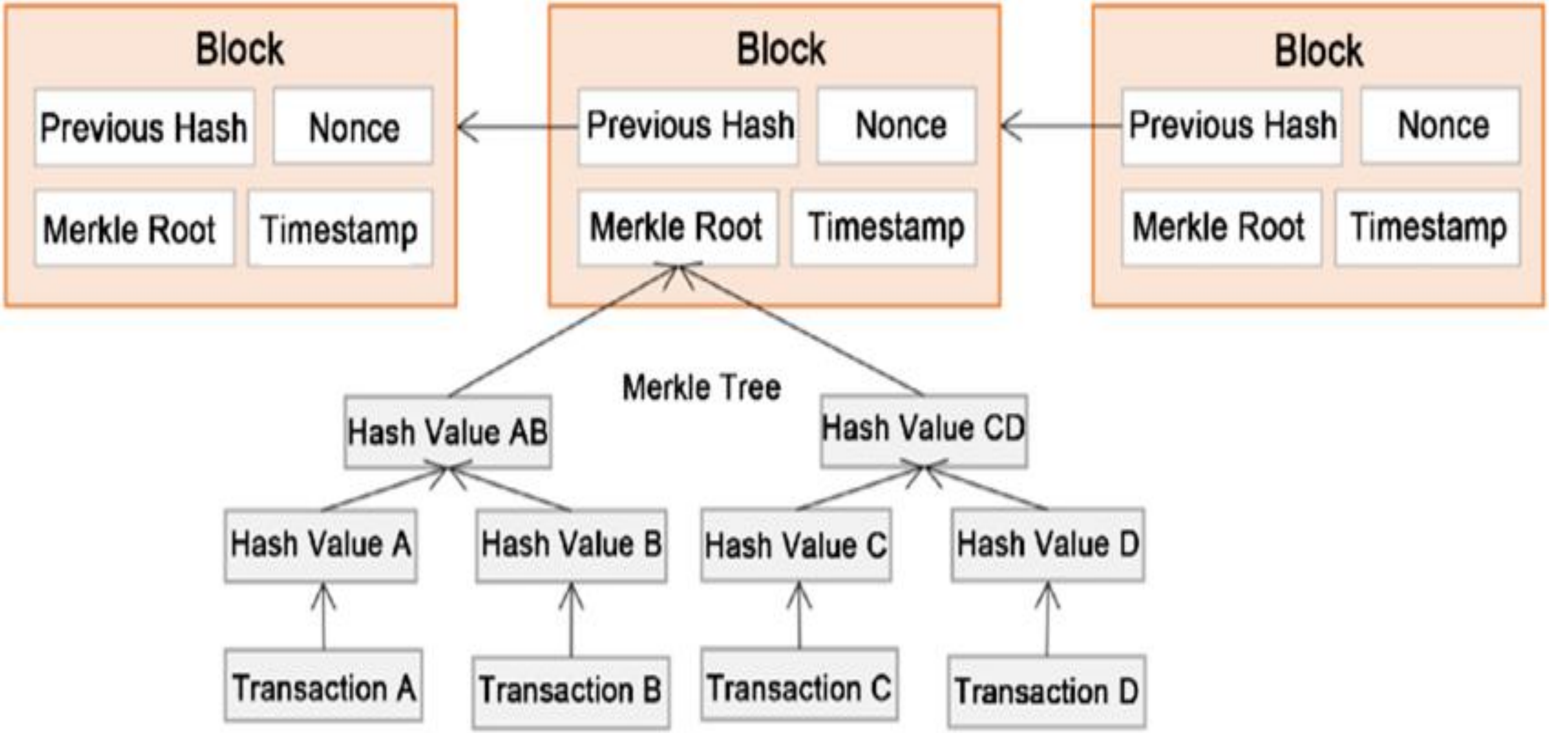
- The Blockchain records transactions and what gets transferred is the control of digital asset
- This control comes through use of cryptography
- When a digital asset is exchanged, it is placed under the control of a specific public-private key pair
- If someone is able to prove that he has the private key matching the public key, the Blockchain network lets him control the digital asset
- If the private key is lost there is no recoverability!

Merkle Tree



Each block in the Blockchain contains summary of all the transactions in the block using merkle tree

Merkle Tree in Blockchain

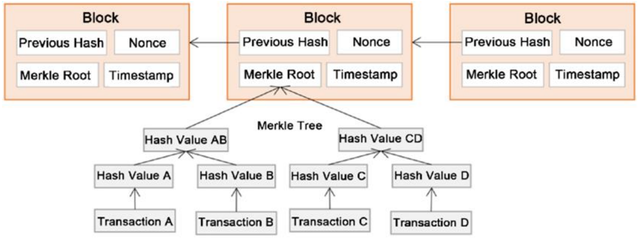


How it provides Security??

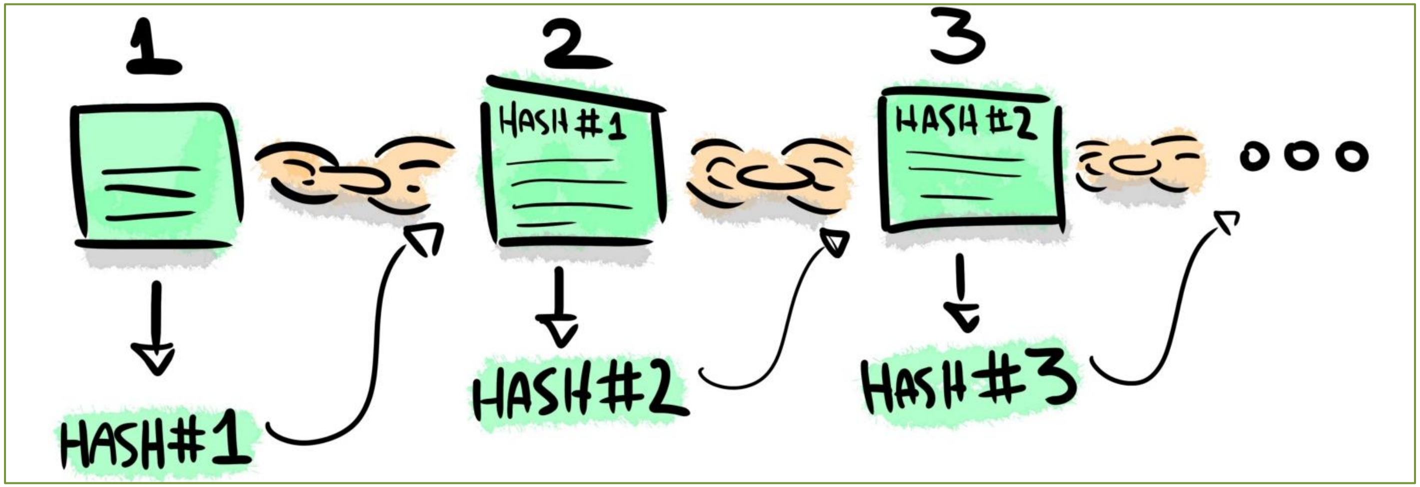
- Metadata in turn, contains Merkel Root of Transaction data

- Change the metadata, block hash will change - leads to broken chain

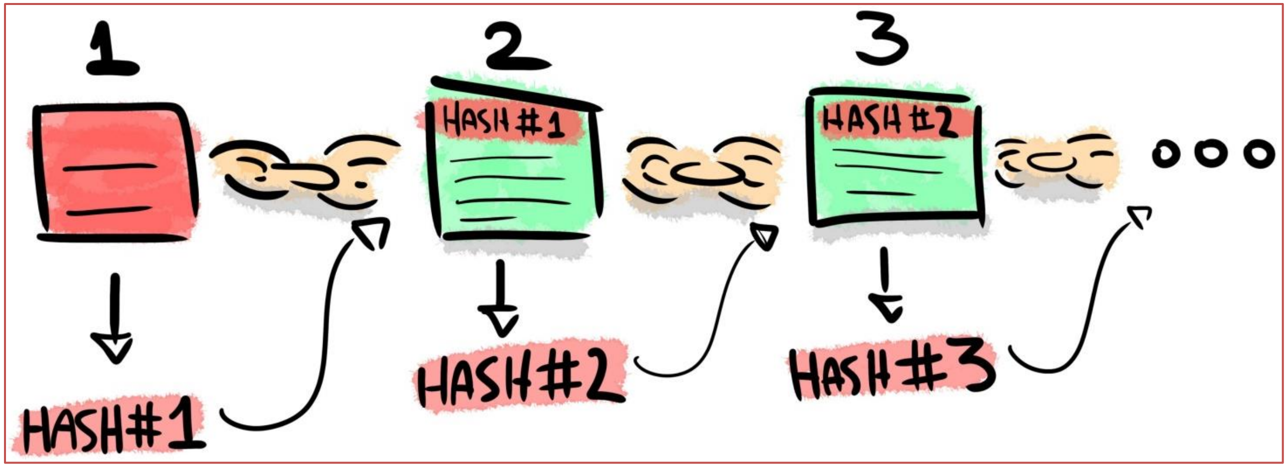
- Change the details of a transaction, the merkle root will change, which in turn changes the metadata hash, which will change the block id



Detect Tampering from Chain of Blocks



If Txn #1 is modified



What makes Blockchain Unique?

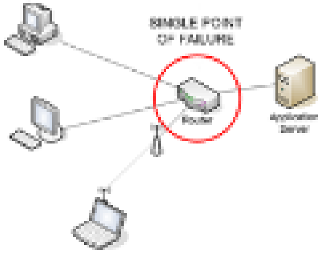
- **Decentralized:** Blockchains are managed by a network of nodes rather than a central authority
- **Transparent:** Transactions are stored on the Blockchain across nodes, all participants can view transactions on the network in real-time
- **Immutable:** Blockchains are designed to enable permanent record keeping (with the help of Cryptographic chains) so that stored data cannot be altered after being added
- **Secure:** It is hard to change or destroy block chains because of its distributed nature

What makes Blockchain Unique?

Transparency

Timestamped

Immutable



No Single Point of Failure

Irrevokable

Programmable

Features and Benefits

- Assurance related to data stored in Blockchain with respect to:
    - Immutability
    - Integrity
    - Authenticity
    - Verifiability
    - Accountability
- Malware Resistant

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

Blockchain Adoption Scenario

- FedEx - Supply chain management
- IBM
  - Supply chain management for walmart
  - Blockchain trade finance platform for Bank of Montreal (BMO), CaixaBank, Commerzbank, Erste Group, and the United Bank of Switzerland (UBS).
- Microsoft – Blockchain as a Service
- NASA - To Use Hyperledger Blockchain For Air Traffic Management
- Sweden - Land Registration
- MasterCard - Blockchain based payment gateways
- Bank of America - Banking Transactions
- JAPAN - Processing Government Tenders
- DHL-Accenture - Pharmacy
- Airbus and Lufthansa - Aviation; for tracking jet plane parts
- Lufthansa - Blockchain-based travel app for users with Winding Tree
- Air France - supply chain and to track workflows within aircraft maintenance systems

Potential Application Domains

- e-Governance
- Supply chain management
- Healthcare
- Financial Services
- Auditing & Compliance
- High Valued Asset Tracking
- Document Notarization System
- e-voting
- Access Auditing
- Log Management and etc…

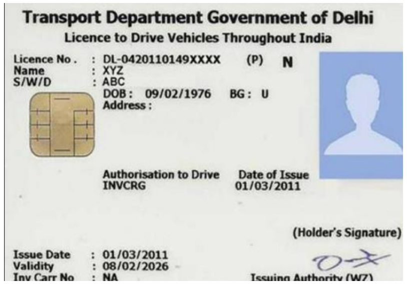
Applications Developed by C-DAC

- Property Record Management System (Land Registration)
- Blockchain based Proof of Existence for Digital artifacts
- Blockchain based Educational Certificate Verification
- PoCs
  - Blockchain based Hotel Visitor Registration System
  - Blockchain based Transportation System

BLOCKCHAIN
BASED
PROOF OF EXISTENCE(POE)

Motivation

- Number of digital artefacts are generated by ICT systems
- Fake or fabricated documents is a major issue (degree certificates, property records etc)
- Many document management systems lack
  - Transparency
  - Security
  - Efficiency
- How the problem can be solved?
  - Temporal existence
  - Verify Origin
  - Verify Content Authenticity



Transport Department Government of Delhi

Licence to Drive Vehicles Throughout India

Licence No. : DL-0420110149XXXX (P) N
Name : XYZ
S/W/D : ABC
DOB : 09/02/1976 BG : U
Address :

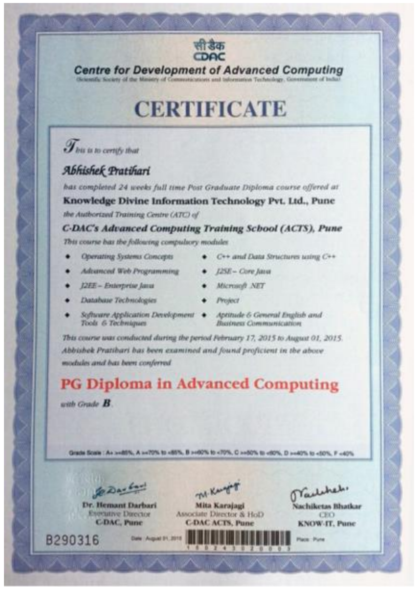
Authorisation to Drive
INVCRG

Date of Issue
01/03/2011

(Holder's Signature)

Issue Date : 01/03/2011
Validity : 08/02/2026
Inv Carr No : NA

Issuing Authority (WZ)



सीडैक
CDAC
Centre for Development of Advanced Computing
(Scientific Society of the Ministry of Communications and Information Technology, Government of India)

CERTIFICATE

This is to certify that

Abhishek Pratihari

has completed 24 weeks full time Post Graduate Diploma course offered at

Knowledge Divine Information Technology Pvt. Ltd., Pune

the Authorized Training Centre (ATC) of

C-DAC's Advanced Computing Training School (ACTS), Pune

This course has the following compulsory modules

- Operating Systems Concepts
- Advanced Web Programming
- J2EE – Enterprise Java
- Database Technologies
- Software Application Development Tools & Techniques
- C++ and Data Structures using C++
- J2SE – Core Java
- Microsoft .NET
- Project
- Aptitude & General English and Business Communication

This course was conducted during the period February 17, 2015 to August 01, 2015. Abhishek Pratihari has been examined and found proficient in the above modules and has been conferred

PG Diploma in Advanced Computing

with Grade **B**.

Grade Scale : A+ >=85%, A >=70% to <85%, B >=60% to <70%, C >=50% to <60%, D >=40% to <50%, F <40%

Dr. Hemant Darbari
Executive Director
C-DAC, Pune

Mita Karajagi
Associate Director & HoD
C-DAC ACTS, Pune

Nachiketas Bhatkar
CEO
KNOW-IT, Pune

B290316

Date : August 01, 2015

150243020003

Place : Pune

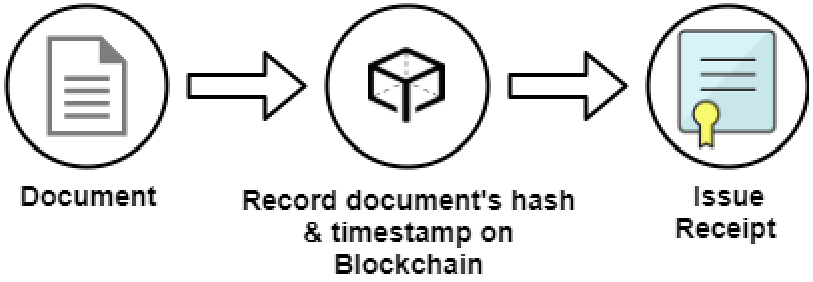
Proof of Existence (PoE)

- Records the following details on Blockchain
  - hash of digital artefact
  - timestamp

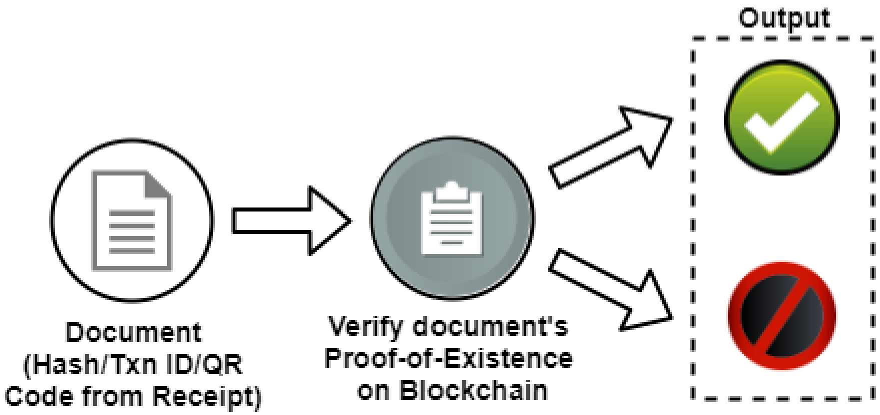
- Allows verifying
  - digital artefact hash not tampered
  - digital artefact existed at a point in time when it was recorded on Blockchain

Blockchain based Proof of Existence as a Service (PoEaaS)

Records the hash of digital artefact



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


Output
Document (Hash/Txn ID/QR Code from Receipt)
Verify document's Proof-of-Existence on Blockchain

Salient Features

- Security in terms of integrity, Authenticity and epoch of vital data
- Seamless authentication
- Physical submission of documents is not essential
- Platform records and maintains the hash of digital artefacts in a tamper proof manner
- Issued receipt includes hash and an embedded QR code which can be used for future verifications
- Dashboard for indicating match/mismatch after verifying with Blockchain details
- Malware Resistant

Benefits

- Documents are **Recorded on Blockchain - Ensures Document's Integrity & Ownership**
- Enables **Recognition of Modified or Fabricated Documents**
- Enables **Blockchain based Document Verification** by Others
- **Eases the Verification Process** by Eliminating Manual Intervention
- Provides **Proof-of-Existence of Documents for Lifetime**

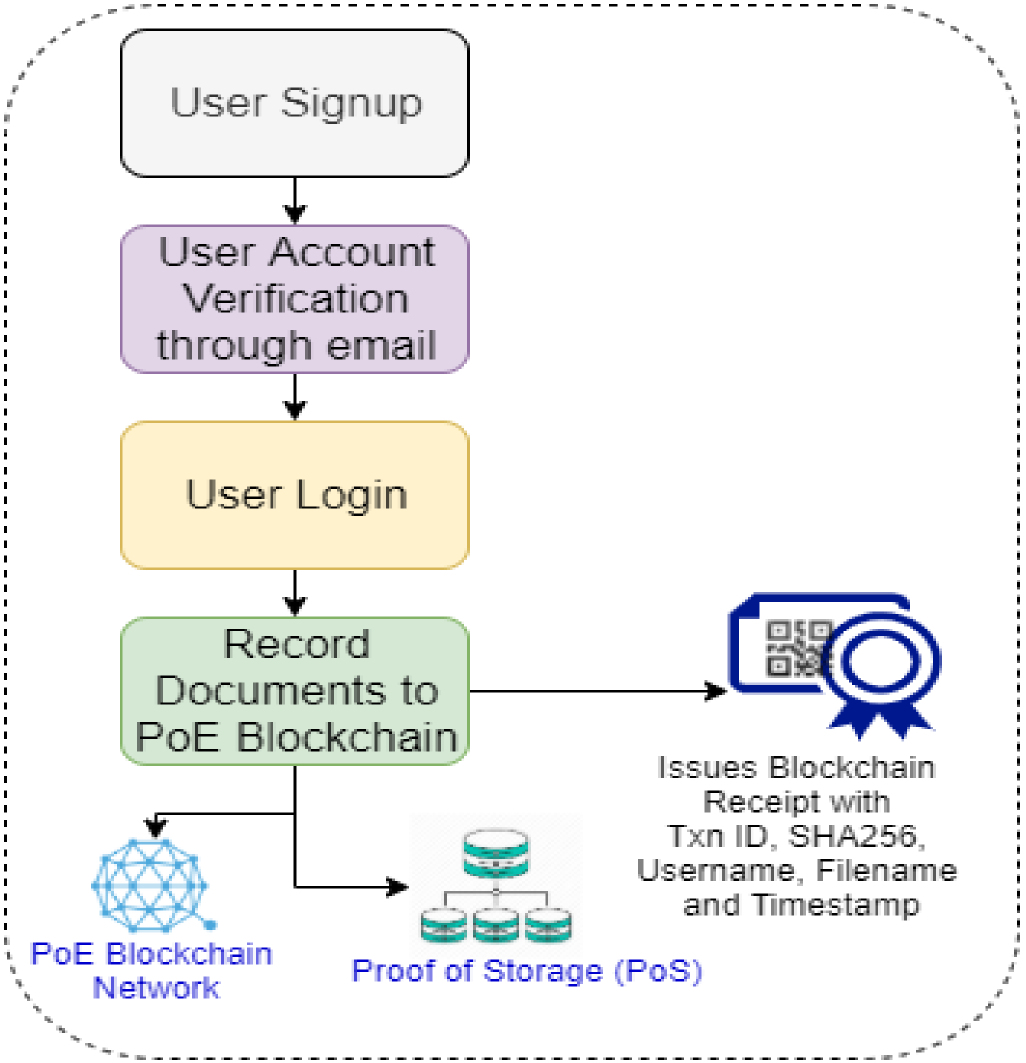
Application Overview

- Records Digital Artefacts or Documents in Blockchain

- Stores the Document in Proof of Storage(PoS) in an encoded format

- Owner can share Blockchain Receipt with Others for Proving the Integrity and Ownership of Document from Blockchain

Work Flow for Recording Documents in PoE Blockchain



User Signup

User Account Verification through email

User Login

Record Documents to PoE Blockchain

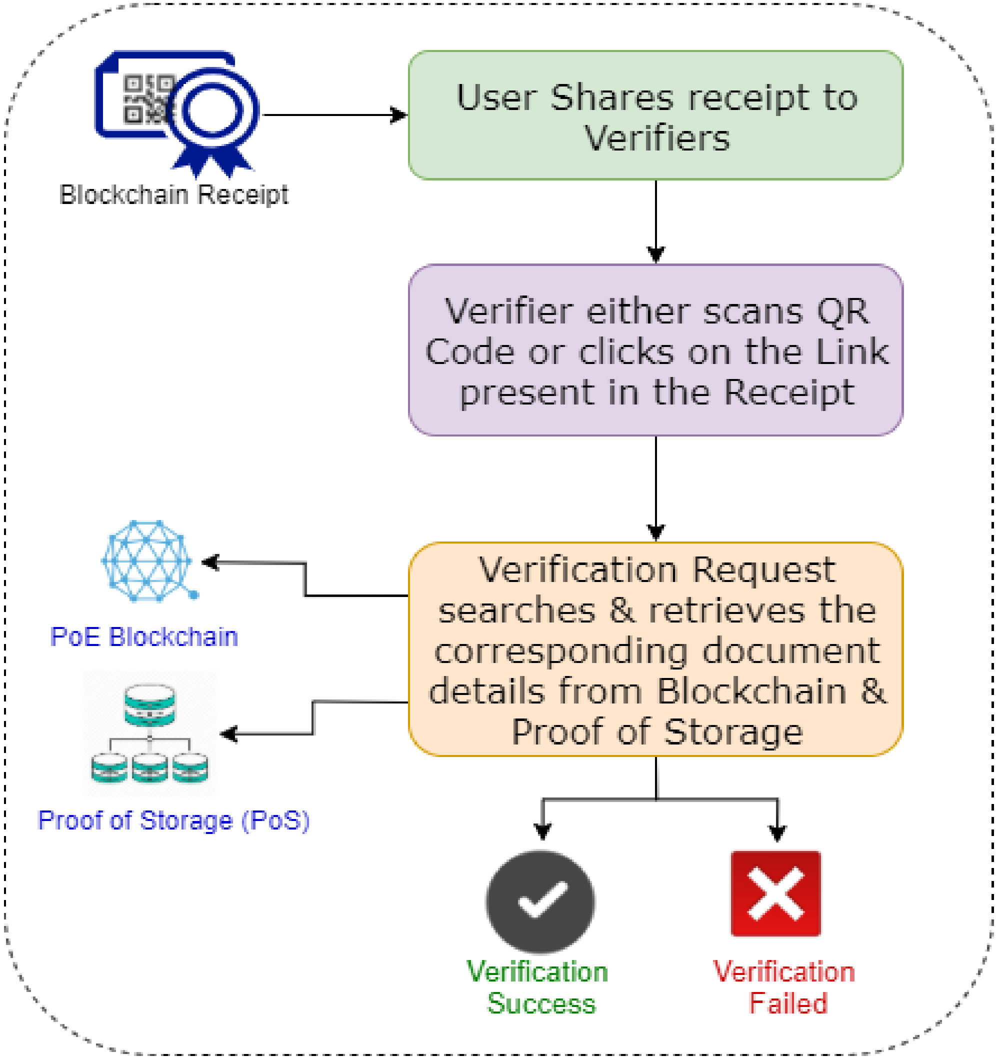
Issues Blockchain Receipt with Txn ID, SHA256, Username, Filename and Timestamp

PoE Blockchain Network

Proof of Storage (PoS)

Flow of Recording a Document in PoE Blockchain

Work Flow for Verifying Documents From PoE Blockchain


Blockchain Receipt
User Shares receipt to Verifiers
Verifier either scans QR Code or clicks on the Link present in the Receipt
PoE Blockchain
Proof of Storage (PoS)
Verification Request searches & retrieves the corresponding document details from Blockchain & Proof of Storage
Verification Success
Verification Failed

Flow of Verifying a Document From PoE Blockchain

Potential Use cases

MoUs / Agreements

Employee Service Records

Exam Results & Student Certificates

Birth/ Death Certificates

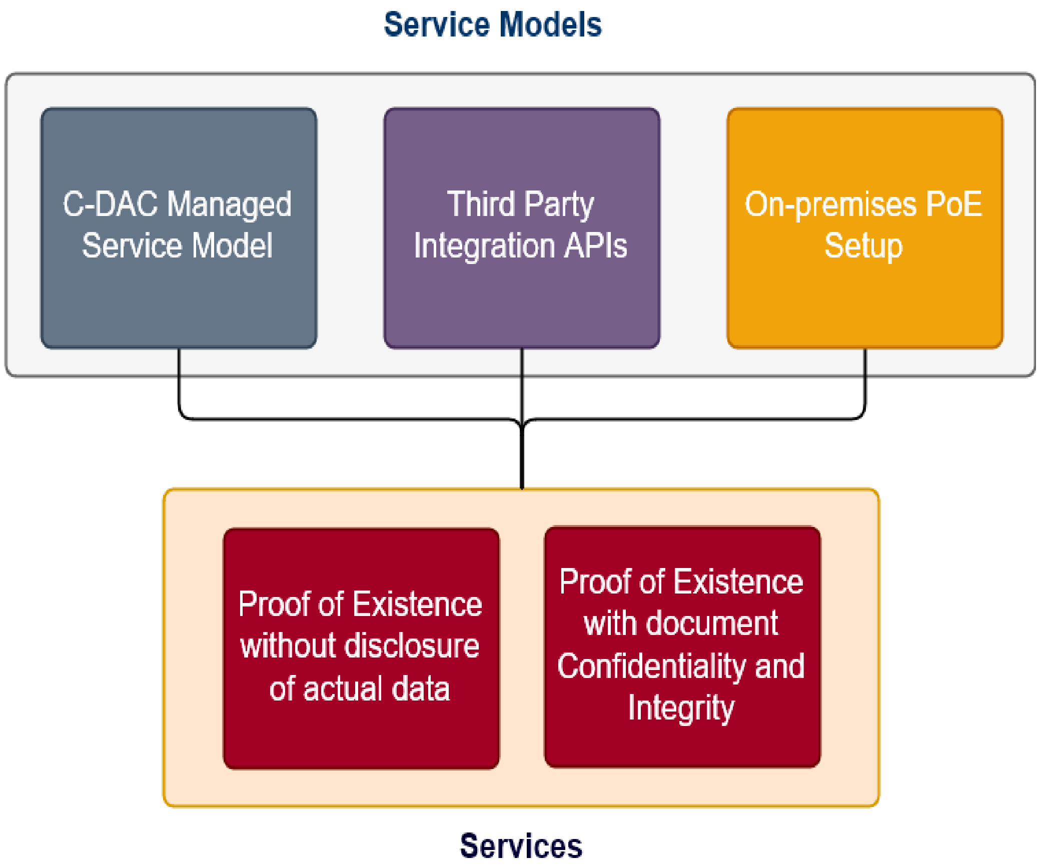
Log Management

Driving Licenses

Sale deed & Land Records

Health Records

Service Models of PoE


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

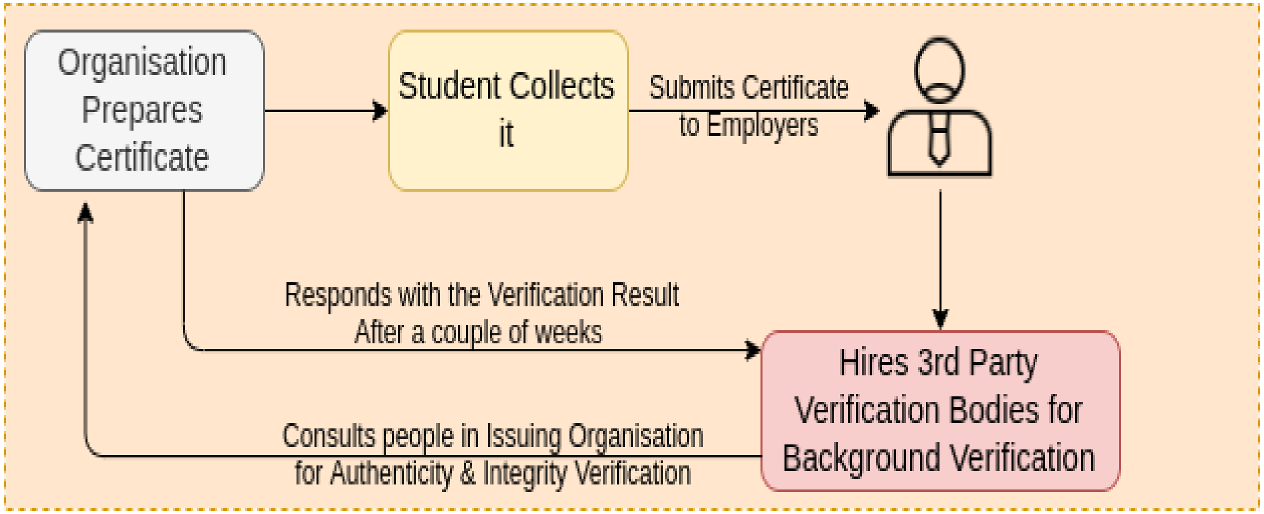
Blockchain based PoE for In-house PG Diploma Certificates

Challenges for Certificate Verifying bodies

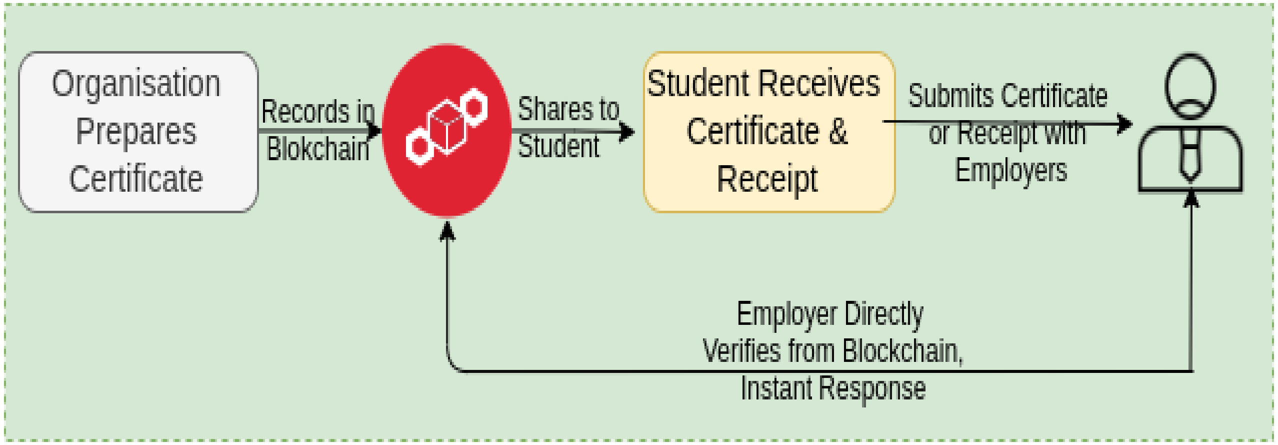
- Dealing with fake credentials
- The task of verifying documents is cumbersome and involves cost & time
- The process could take couple of weeks or a month depending on the response from the issuing authorities
- Background verifying agencies charges fee to verify documents from concerned authorities

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
Responds with the Verification Result After a couple of weeks
Consults people in Issuing Organisation for Authenticity & Integrity Verification

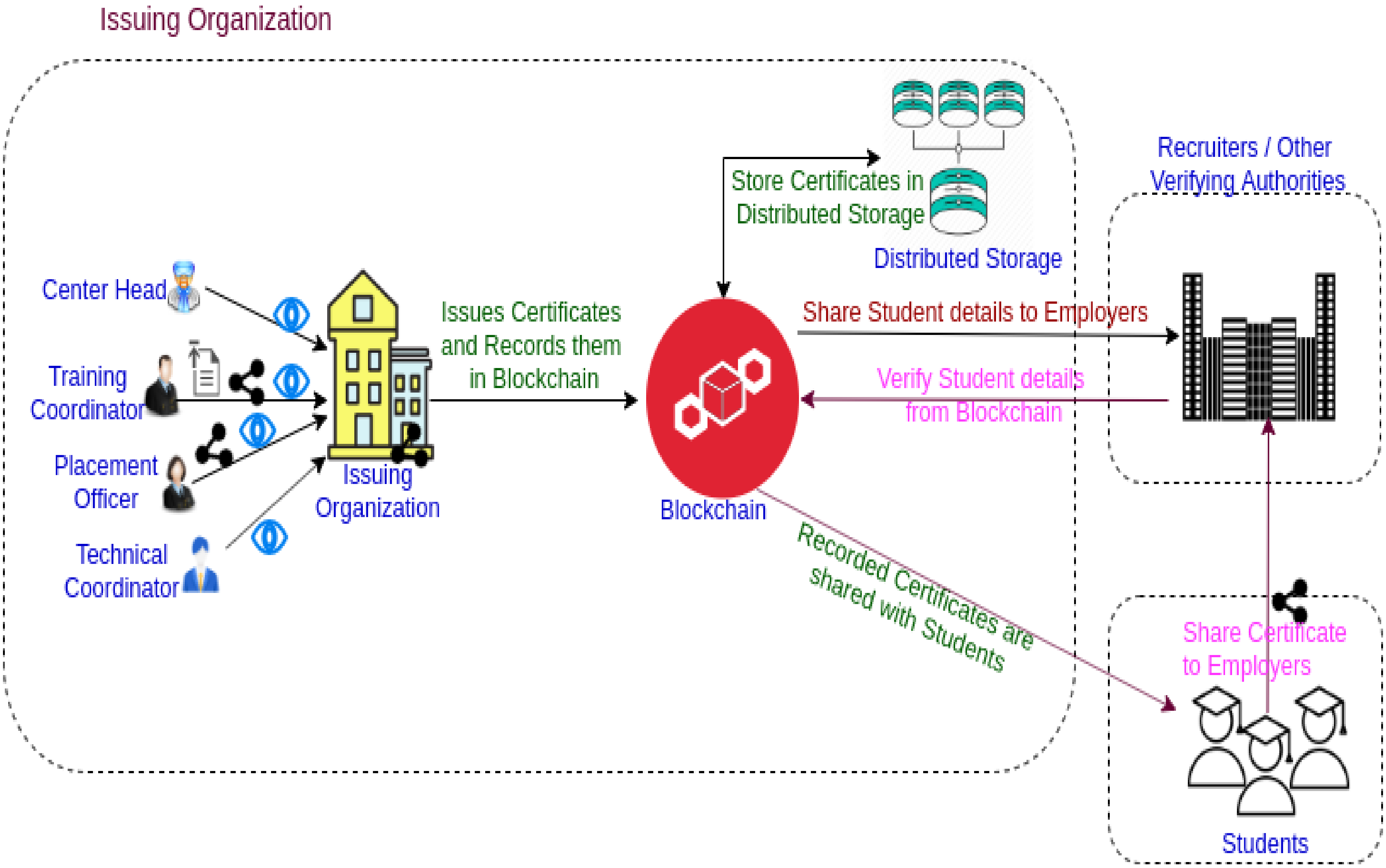
Blockchain based Certificate Verification Flow


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

Benefits

- Certificates are **Recorded on Blockchain at the Origin** itself
- Ensures Certificate’s **Integrity, Ownership and Timestamp**, which enables **Detection of Modified or Fabricated Certificates**
- **Enables Instant Verification** for Employers, Higher Educational Institutes or any other 3rd party bodies *via scanning a QR code or via the Link*
- Provides **Proof-of-Existence of Certificates for Lifetime**
- **Readily Available Certificates** in case of loss or damage

Application Overview


Issuing Organization
Store Certificates in Distributed Storage
Distributed Storage
Recruiters / Other Verifying Authorities
Center Head
Training Coordinator
Placement Officer
Technical Coordinator
Issues Certificates and Records them in Blockchain
Issuing Organization
Blockchain
Share Student details to Employers
Verify Student details from Blockchain
Recorded Certificates are shared with Students
Share Certificate to Employers
Students

Application Overview

- Blockchain based initiative for Issuing, Viewing, Sharing and Verifying educational certificates
- Students can share Receipt with Verification bodies for Proving the Integrity and Authenticity of Certificate from the Blockchain
- Or Verification bodies can directly verify the certificate details from Blockchain using the Unique ID of the student
- QR code enabled or Link based Verification

Blockchain based Property Record Management System (PRMS)

Property Registration – Potential Challenges

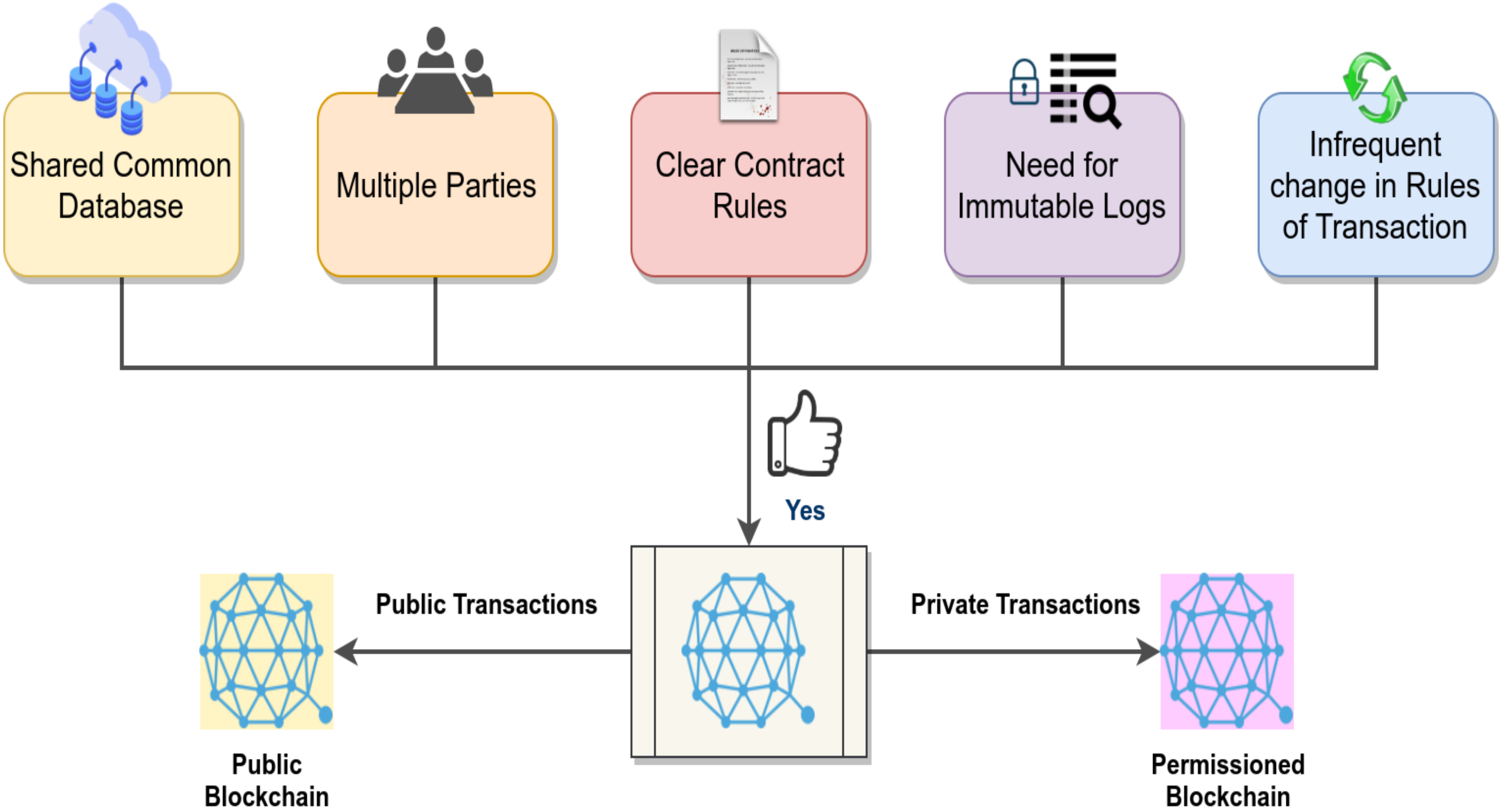
Based on the survey, following are the most common irregularities present in the existing property registration system

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

Requirements

- Electronic Ledger
  - Reliable
  - Timestamped
  - Tamper-evident
  - Providing non-repudiable proof of each transaction
- Single source of truth
- Linked Document (Title History) Verification
- Distributed Ledger 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

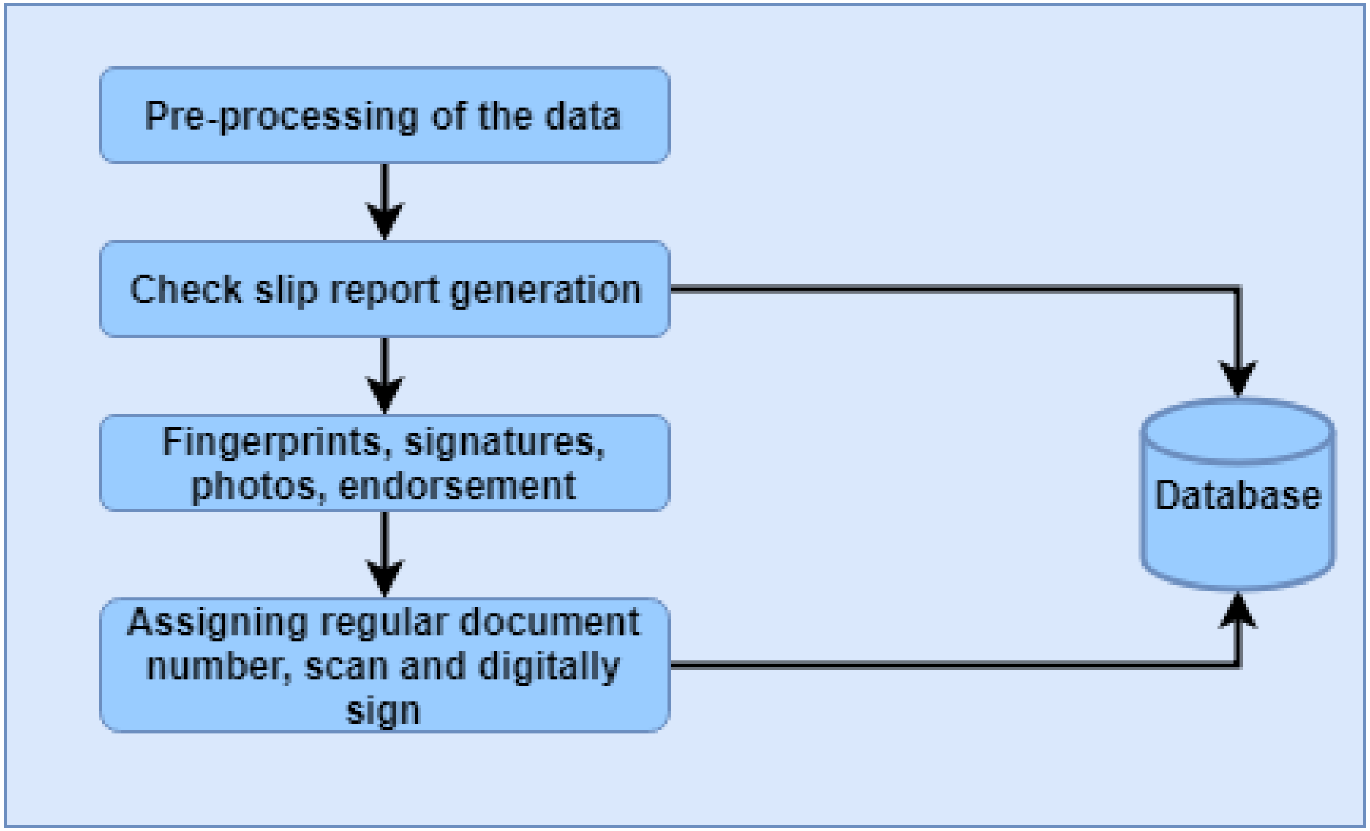
Suitability of Blockchain Technology



Benefits of Integrating Blockchain Technology in Existing System

- Title history is often incomplete and thus unclear
  - Implicit chaining of transaction details
- Inquiring / investigation is time consuming and may not be certain
  - Single source of truth from Blockchain
- Possibility for malign parties to involve in corruption
  - Audit trail details available from tamper evident Blockchain
- Centralized property registration system has a single point of failure
  - Distributed
- Vulnerable to destruction, modification and non availability
  - Tamper evident & distributed

Property Registration Management - Existing Application in Telangana Govt.


Pre-processing of the data
Check slip report generation
Fingerprints, signatures, photos, endorsement
Assigning regular document number, scan and digitally sign
Database

Existing Property Registration Application

During Check Slip Report Generation

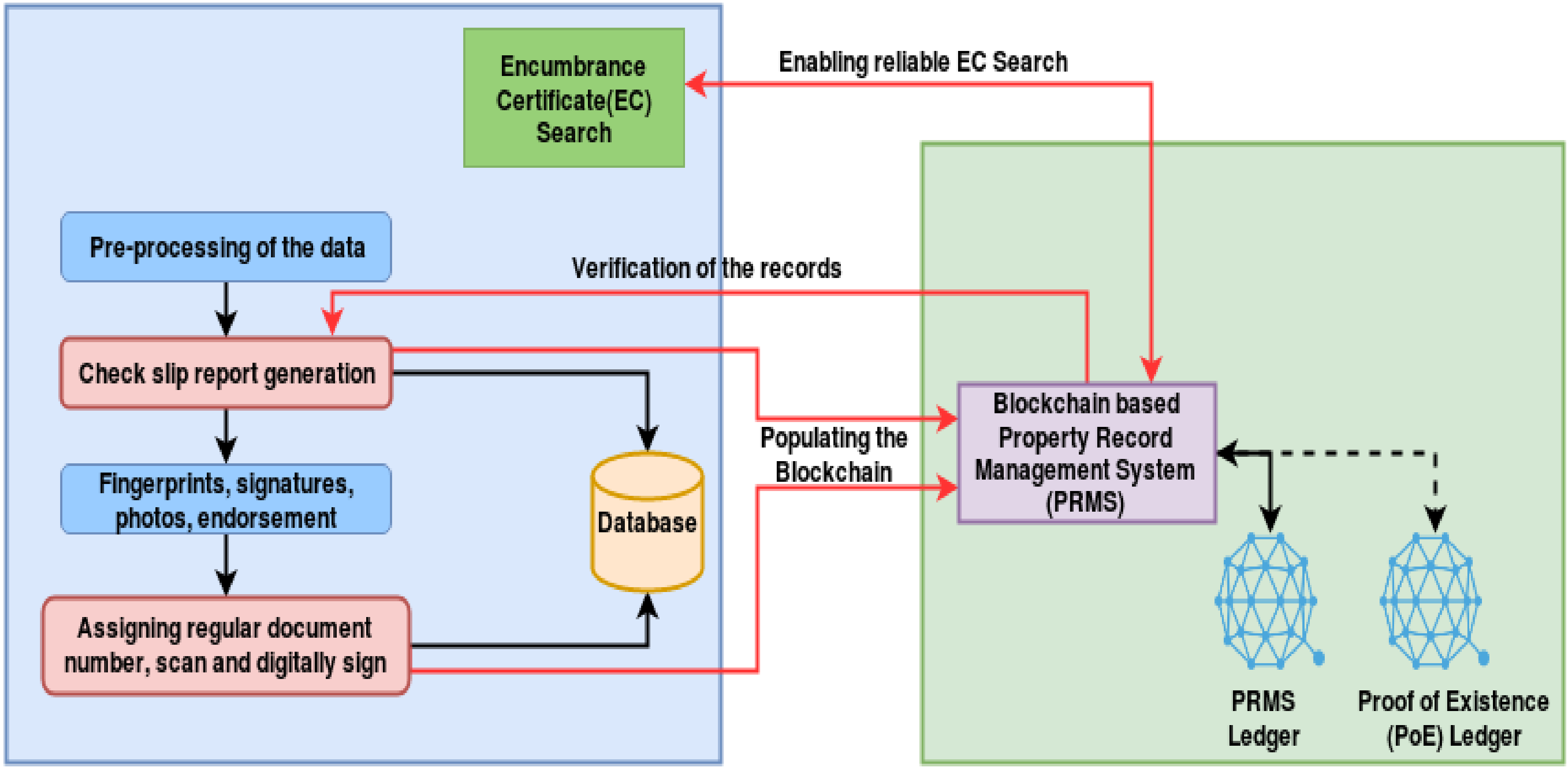
- Property details
  - Survey number (District / Mandal / Village / Survey Number / sub division)
  - Area of measurement
  - Jurisdiction / Registering SRO
- Check slip number

- Vendor(s) details
  - Name
  - Father's name
  - PAN
  - Aadhar number
- Vendee(s) details
  - Name
  - Father's name
  - PAN
  - Aadhar number

During Final Regular Document Generation

- Execution Date
- Presentation Date
- Registration Date
- Executants/ Claimants Details / Vendor vendee details
  - Name
  - Father’s Name
  - AADHAR ID
  - PAN
- Witness(s) Details
  - Name
  - AADHAR ID
  - PAN
- Regular Document Number
- Check slip number
- Property details
  - Survey number (District / Mandal / Village / Survey Number / sub division)
  - Area of measurement
  - Jurisdiction / Registering SRO
  - Category of Land (Abeyance, Prohibited, Normal …)
  - GIS (Lat, Long)

Blockchain Based Property Registration Management


Encumbrance Certificate(EC) Search

Enabling reliable EC Search

Pre-processing of the data

Verification of the records

Check slip report generation

Populating the Blockchain

Blockchain based Property Record Management System (PRMS)

Fingerprints, signatures, photos, endorsement

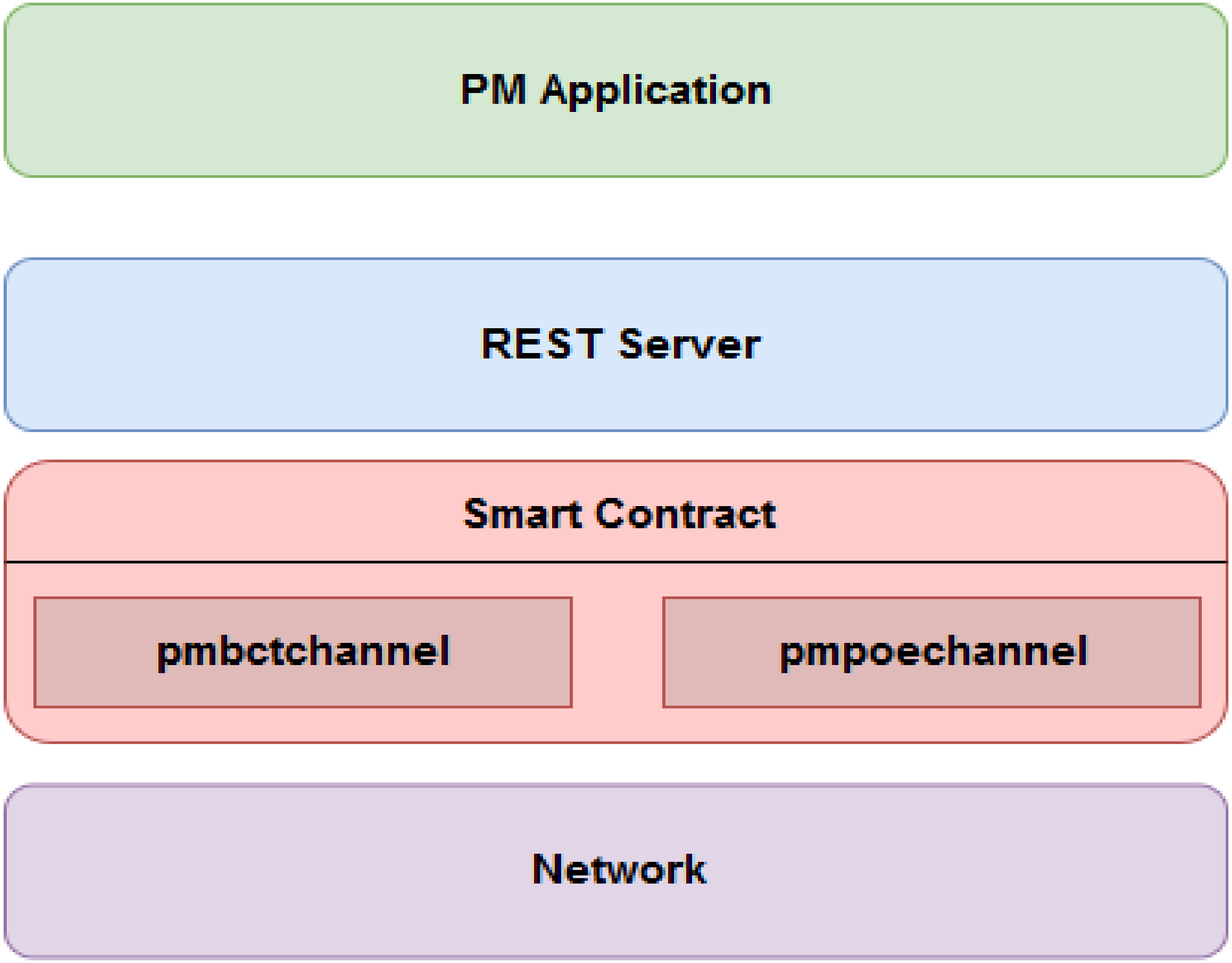
Database

Assigning regular document number, scan and digitally sign

Existing Property Registration Application

Blockchain based Property Record Management System (PRMS)

Blockchain Stack of PRMS



Features and Benefits

- Integration points with existing application using standard Web APIs
- Live Blockchain data hooks in the registration phase for early verification
  - Provision for indicating mismatch in existing database with registration department and blockchain
  - Implicit validation of vendor title ownership at the time of mutation
    - Helps to detect double selling and database modifications (if any)
- Reliable Encumbrance / link document search
- Dashboard for indicating mismatch in existing database and Blockchain details post registration
- Proof-of-Existence implementation for storing final registration document
  - Validity of the registered document can be established through PoE

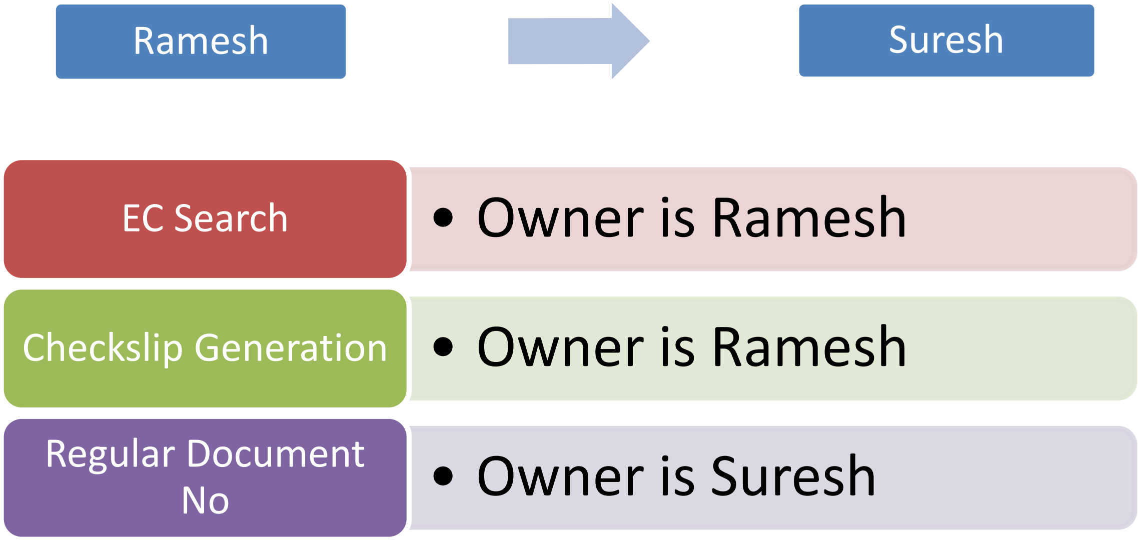
Features and Benefits

- Assurance related to Property data with respect to:
  - Immutability
  - Integrity
  - Authenticity
  - Verifiability
  - Accountability

- Malware Resistant

General flow

- Property is being transferred from Ramesh to Suresh

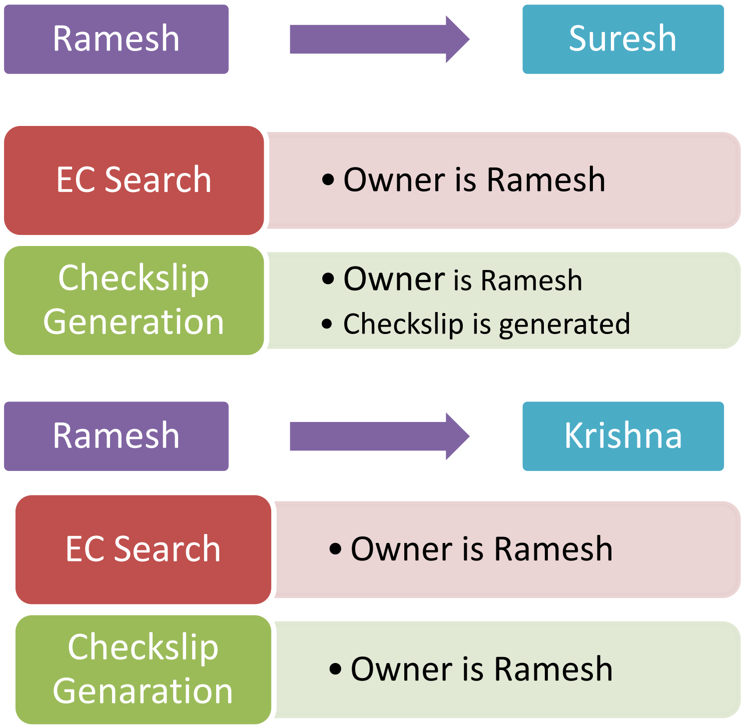


Ramesh → Suresh

EC Search	• Owner is Ramesh
Checkslip Generation	• Owner is Ramesh
Regular Document No	• Owner is Suresh

Scenario 1: Double Selling

With existing system



Ramesh → Suresh

EC Search
- Owner is Ramesh

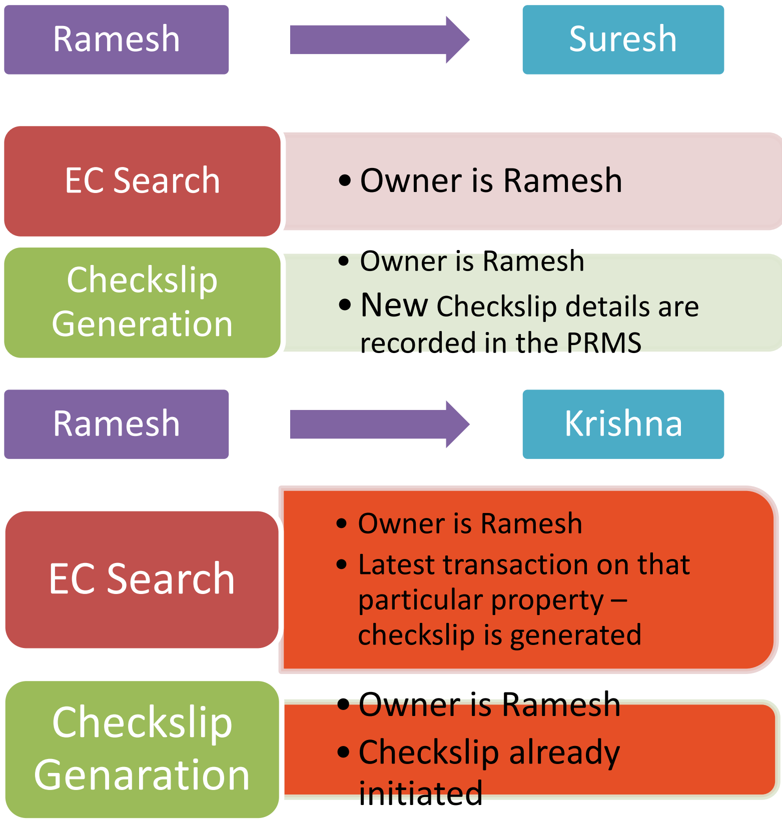
Checkslip Generation
- Owner is Ramesh
- Checkslip is generated

Ramesh → Krishna

EC Search
- Owner is Ramesh

Checkslip Genaration
- Owner is Ramesh

With Blockchain based PRMS



Ramesh → Suresh

EC Search
- Owner is Ramesh

Checkslip Generation
- Owner is Ramesh
- New Checkslip details are recorded in the PRMS

Ramesh → Krishna

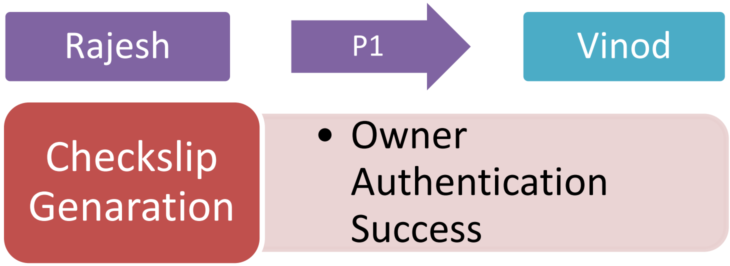
EC Search
- Owner is Ramesh
- Latest transaction on that particular property – checkslip is generated

Checkslip Genaration
- Owner is Ramesh
- Checkslip already initiated

Scenario – 2: Fake Document

With existing system

1. Ramesh is the owner of Property P1
2. Rajesh has created a fake document



Rajesh

P1

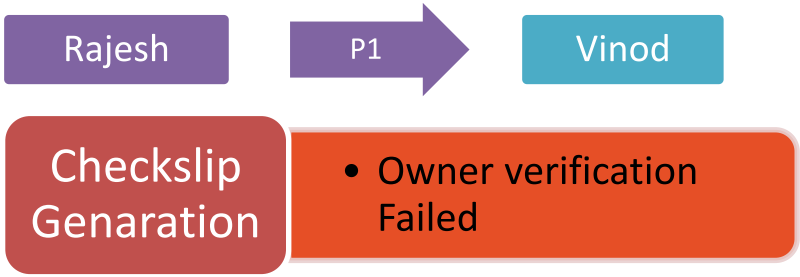
Vinod

Checkslip Genaration

- Owner Authentication Success

With Blockchain based PRMS

1. Ramesh is the owner of Property P1
2. Rajesh has created a fake document



Rajesh

P1

Vinod

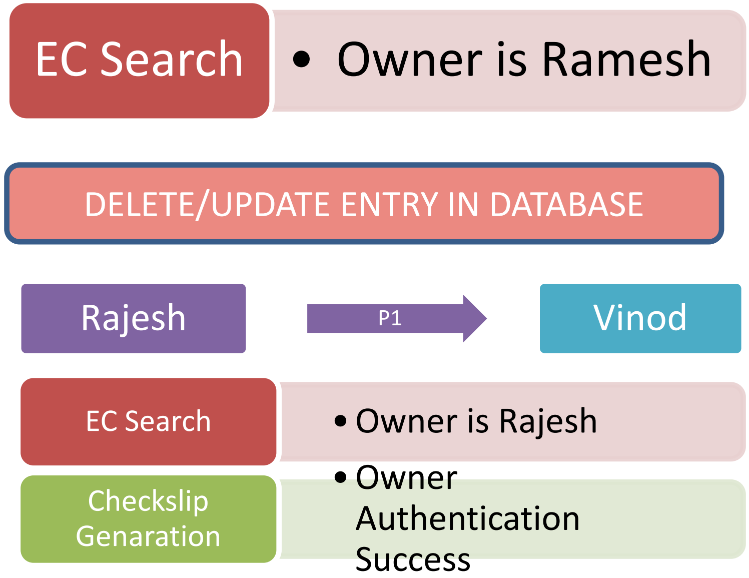
Checkslip Genaration

- Owner verification Failed

Scenario – 3 : Database Modification

With existing system

Ramesh is the owner of Property P1



EC Search

- Owner is Ramesh

DELETE/UPDATE ENTRY IN DATABASE

Rajesh → P1 → Vinod

EC Search

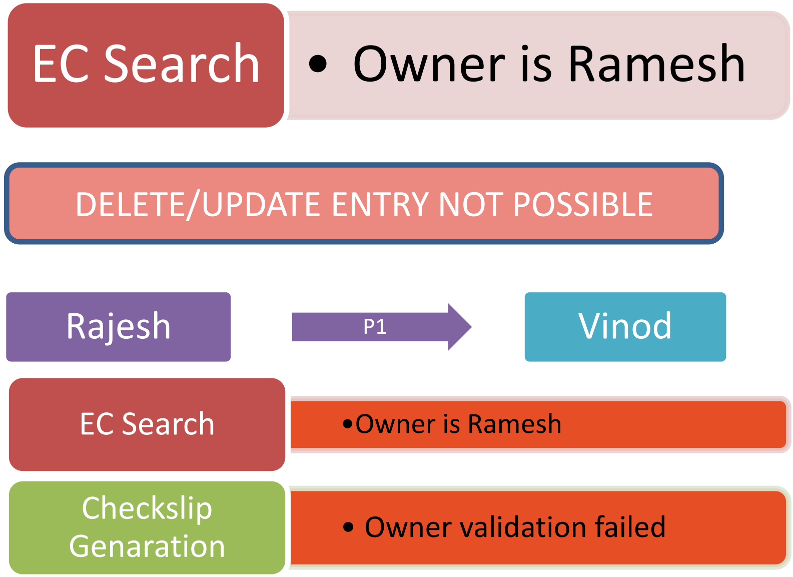
- Owner is Rajesh

Checkslip Genaration

- Owner Authentication Success

With Blockchain based PRMS

Ramesh is the owner of Property P1



EC Search

- Owner is Ramesh

DELETE/UPDATE ENTRY NOT POSSIBLE

Rajesh → P1 → Vinod

EC Search

- Owner is Ramesh

Checkslip Genaration

- Owner validation failed

Thank You

Contact us at:
cdacchain@cdac.in