# BLOCKCHAINS

## ARCHITECTURE, DESIGN AND USE CASES


**SANDIP CHAKRABORTY**
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

**PRAVEEN JAYACHANDRAN**
IBM RESEARCH,
INDIA

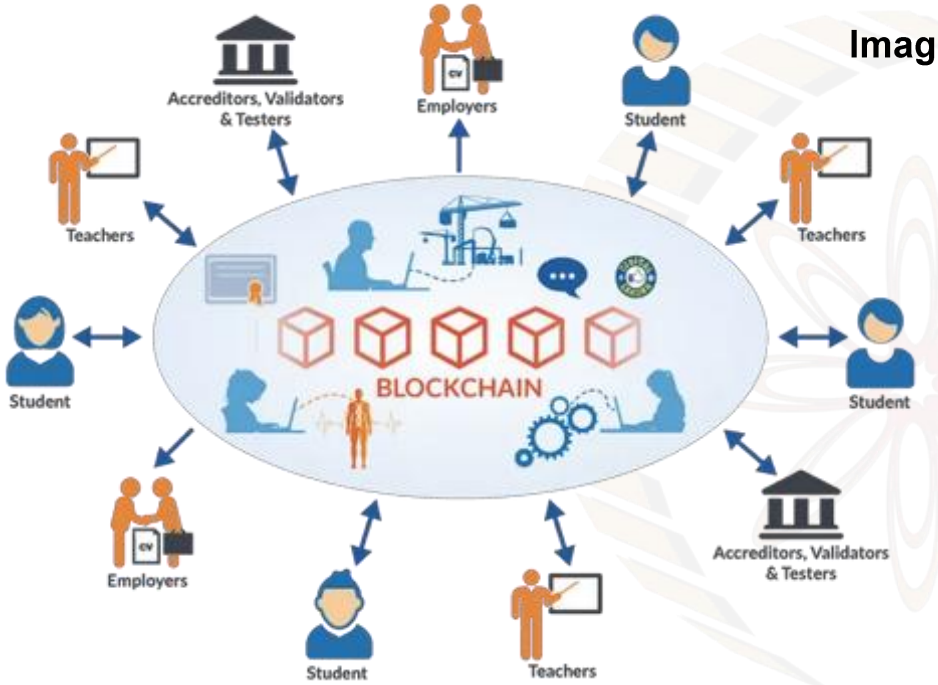



Image Source: http://blockchain.open.ac.uk/

# Blockchain in Government - II

# Case Study - Audit and Compliance

- Financial data of an organization
  - Dispersed through many departments and divisions
  - May be spread across multiple geographical locations
  - May have multiple owners and authorities to manage

- Auditing requires information about all key transactions over the reporting period

# Audit and Compliance

- What if the data is stored in a central server?
  - The problem of a central server - what if the server gets hacked?
  - Who will manage the server? The administrator of the server may not have the power to view the data
    - But the administrator can tamper the data if compromised
- What is the validity of data provided by different divisions?
  - What if the voice from two divisions do not match?

# Auditing and Compliance

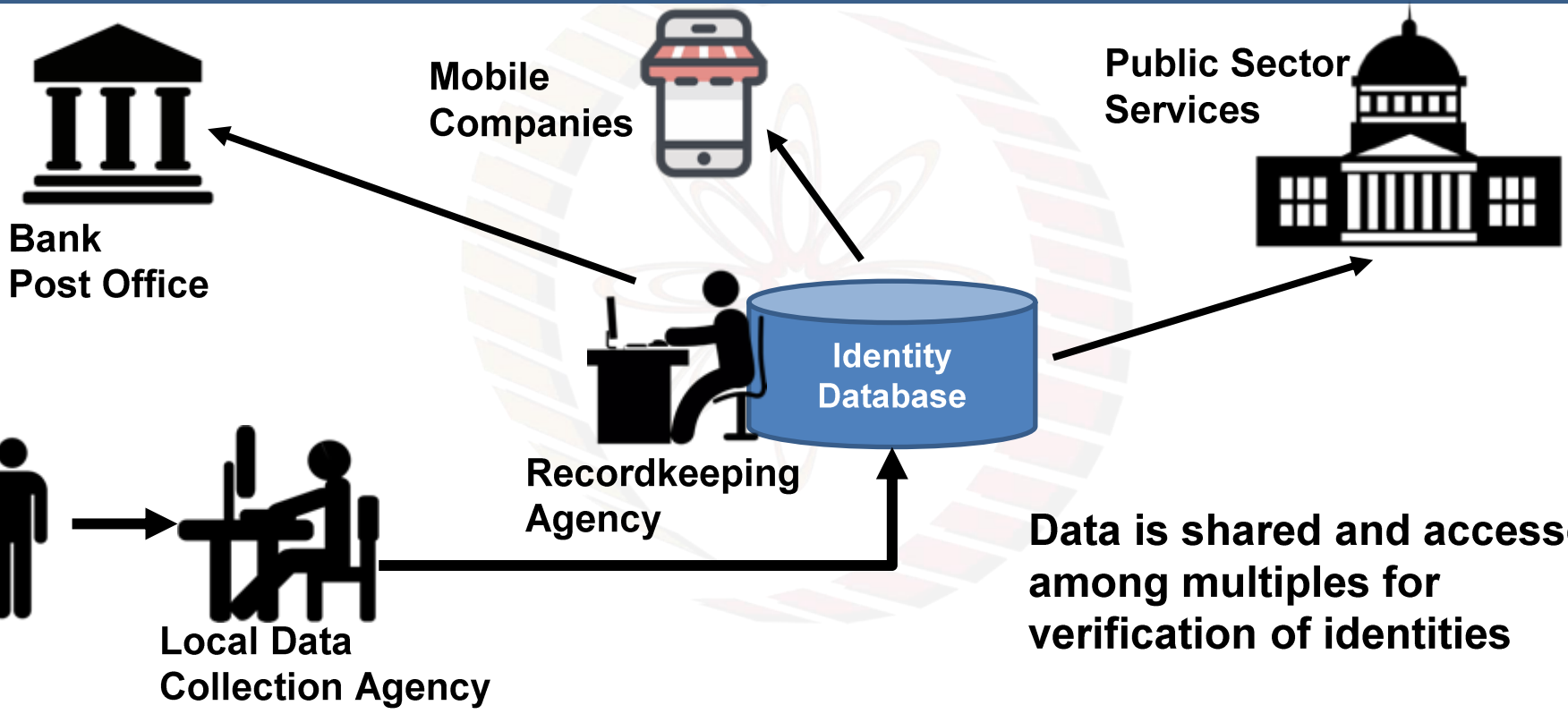
- Put the data in a Blockchain
  - Collects transaction records from diverse set of divisions
  - No one can tamper the data, but everyone can verify

- **Blockchain is append-only**
  - Once a transaction has been recorded, it cannot be removed without changing the view of others

# Auditing and Compliance

- Blockchain has multiple advantages
  - Reduces the cost of auditing - you do not need to talk individually to every division
  - Auditors have global view of the data
  - Compliance becomes passive to active
    - Can be checked and validated immediately when the transaction is recorded

# Citizen Identity



# Citizen Identity

- Control the access through a Blockchain
  - Blockchain has information about who has accessed my data
  - I can verify how my data has been accessed
  - I can verify what part of my data has been accessed
  - Everyone can verify how the overall data is getting accessed
  - "**Access auditing**"

# Blockchain for Defense

- Multi-organizational information flow
  - Tracking of information origin, flow and destination
  - Asset tracking
  - Certification of peoples and machines
  - …


# Defense Secure Messaging and Transaction Platform

- Defense cyber security relies on secrecy of information and trust among individuals
  - Both are difficult to ensure in a real environment

- Needs to ensure that
  - Only the privileged information has been accessed
  - Information logs has not been tampered
  - Provenance tracking of information origin and flow

# Let Us See a Success Story

**Estonia**

**A country in northern Europe**

- Area 45,227 $KM^2$
- Population (2011) 1,294,455
- Population Density 28/$km^2$
- GDP (2018) $43.567 Billion

# e-Estonia

- Digital ID card and decentralized distributed system

- Multiple benefits
  - File taxes within 5 minutes
  - Sign a contract electronically
  - Register a business within 30 minutes
  - i-Voting
  - You can become a e-Citizen!

**Check https://e-estonia.com/**

# e-Estonia : Let us have a tour …

# Blockchain in e-Estonia

- Securing health records - they write records for every update and every access

- Stock exchange - maintain all transactions
  - Secure voting in shareholder meetings

- Birth certificates, business contracts, marriage registrations


thank you!