Science Policy Initiative on Blockchain Technology:

POLICY DISCUSSION WITH SENIOR EXPERTS

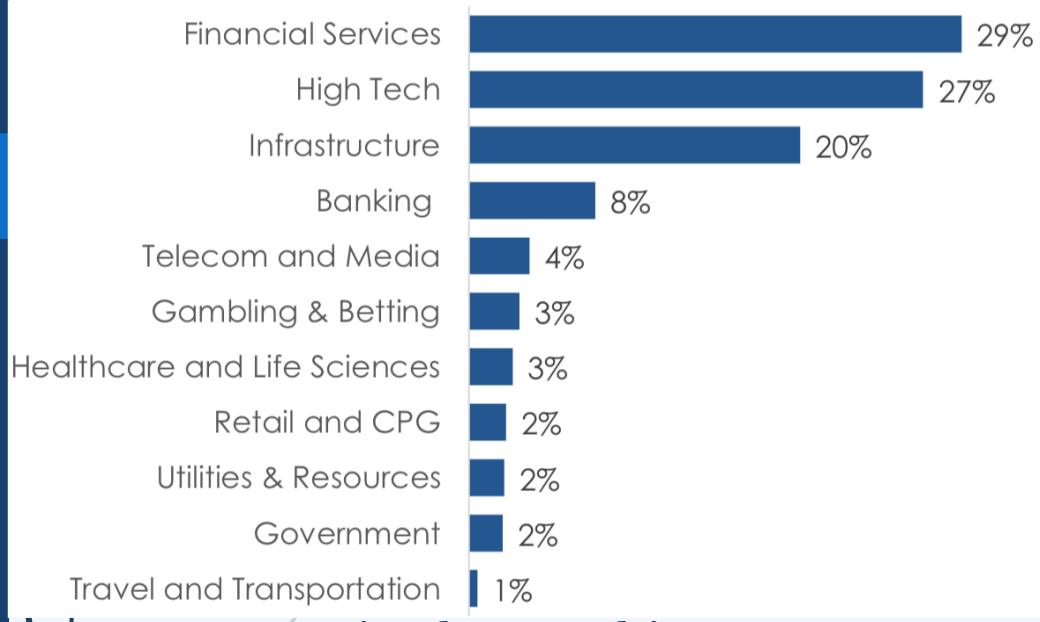
24th January 2020, Ashoka University

Landscaping Priority Areas for Blockchain: Cryptoeconomics, Capacity building, Scalability, Security

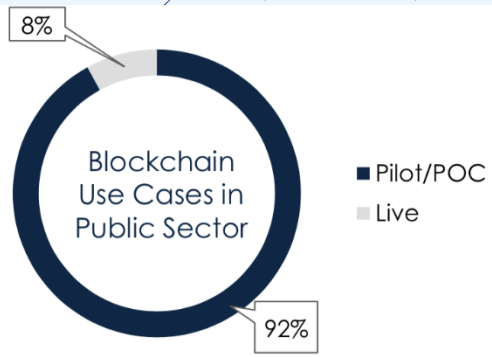
DR. ANJALI TANEJA

ASSOCIATE DIRECTOR, SCIENCE POLICY INITIATIVES,
ASHOKA UNIVERSITY

EMAIL: anjali.taneja@ashoka.edu.in



Source: Reports - Fintech 2020, Deloitte; NASSCOM 2019, WB 2018



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

- ISO: Blockchain and Distributed Accounting Technical Committee (ISO/TC 307)
- Presently: 43 - participating, 12 - observing
- Bureau of Indian Standards: participant
- Venture capital investment (2018): $ 3B+; India's contribn. : only $ 8.5 mn
- Demand for BT talent: rising at >40%/Q; Only 45 – 60 K skilled resources industry ready
- VC investments on BT start-ups : $5.6 bn ; India has been able to attract only 0.2%
- India's private sector investment : < 0.2% of global; low portfolio of BT projects in India by mid & large service providers (<5%) viz-a-viz projects globally
- BT start-ups in India: only 2% of 66% globally

Potential & Scope

Possible Challenges / Issues

Skills Development:

Talent upskilling, academia-industry disconnect, missing connect b/w demand & supply of BT-driven skills

Education:

practical / application-oriented learning shortages, theory centric curricula, limited teachings, expensive certifications, limited R&D practices

Scalability, Security:

BT applications' efficiency downgrade, duplication of data hosting, security vulnerabilities / breaches, limitations on capital efficiency & scalability

Scope & Outreach:

low investments, limited outreach of BT start-ups, open-ended BT adoption issues, technology nascence in governance, low # of live engagements

R&D:

limited, lack of interdisciplinary research .e.g. cryptoeconomics, no Centre of Excellence / specialised research centres

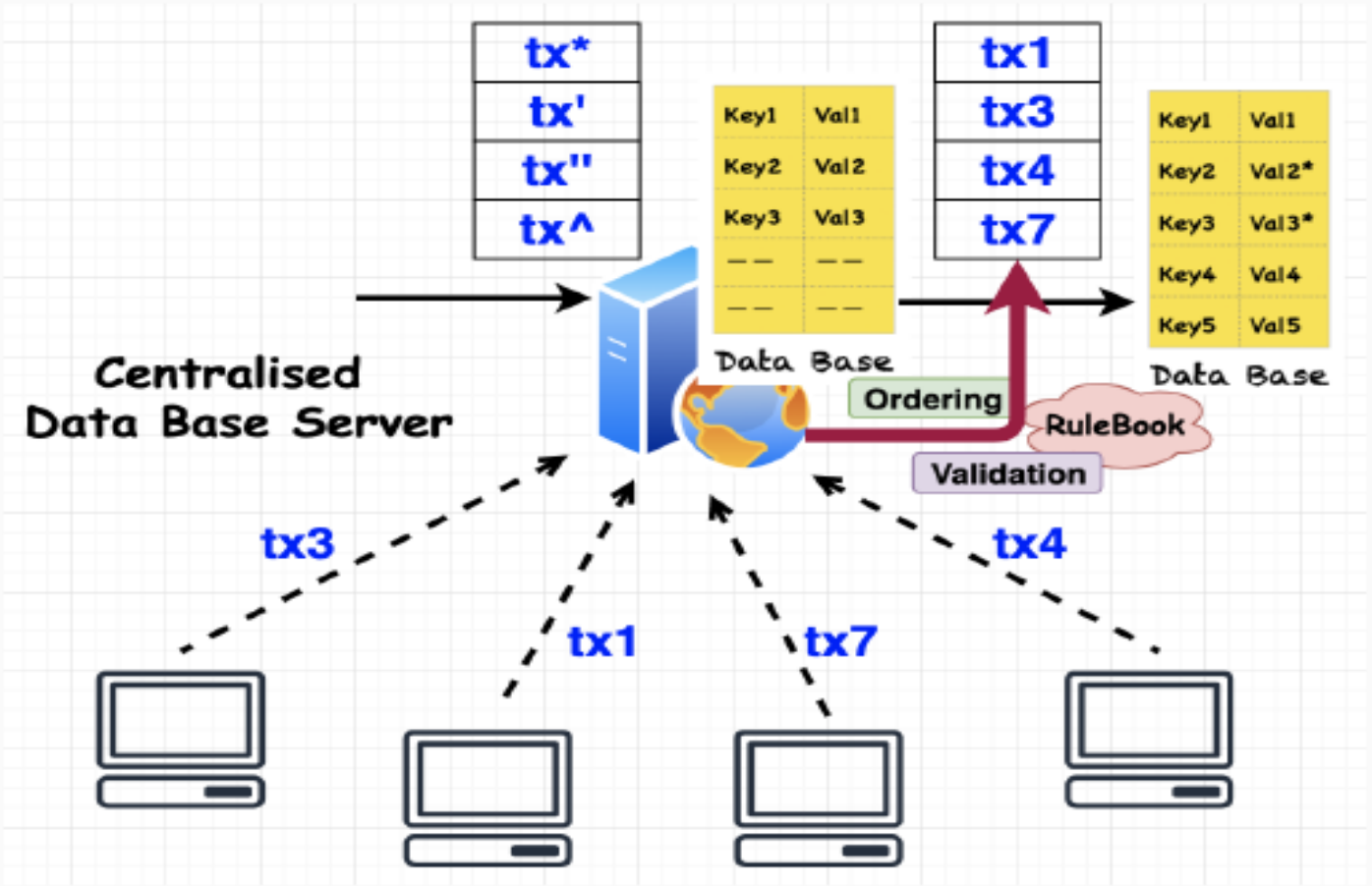
PROF. MAHAVIR JHAWAR

ASSISTANT PROFESSOR, COMPUTER SCIENCE, ASHOKA UNIVERSITY

EMAIL: mahavir.jhawar@ashoka.edu.in

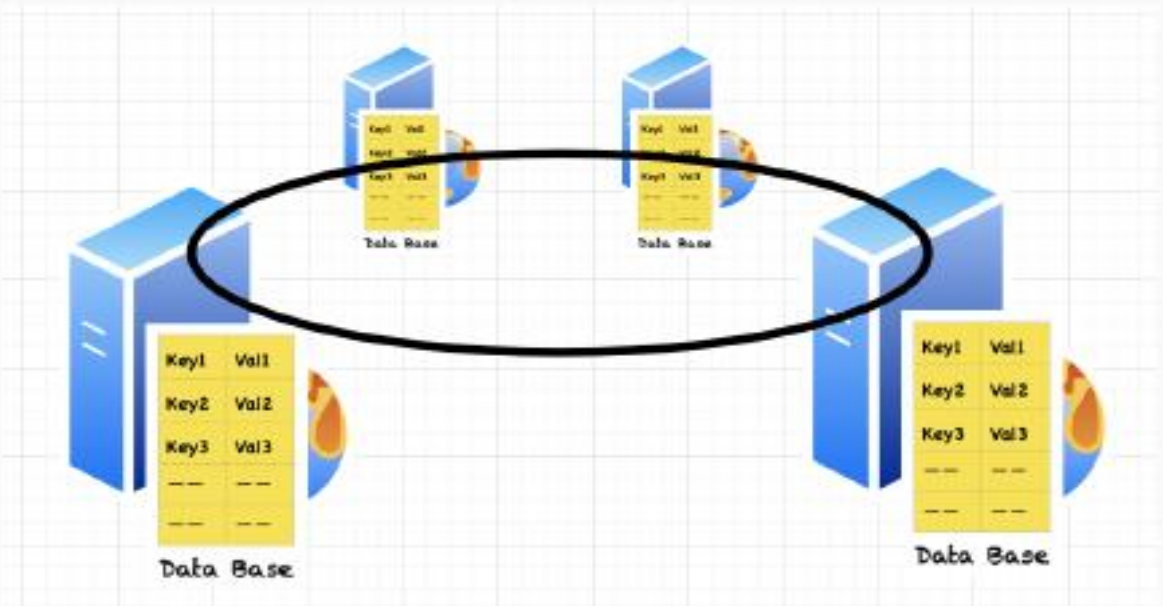
A Centralised Ledger System

- Used by a bank/insurance company, for example
- Here is a glimpse into such a system (simplified)

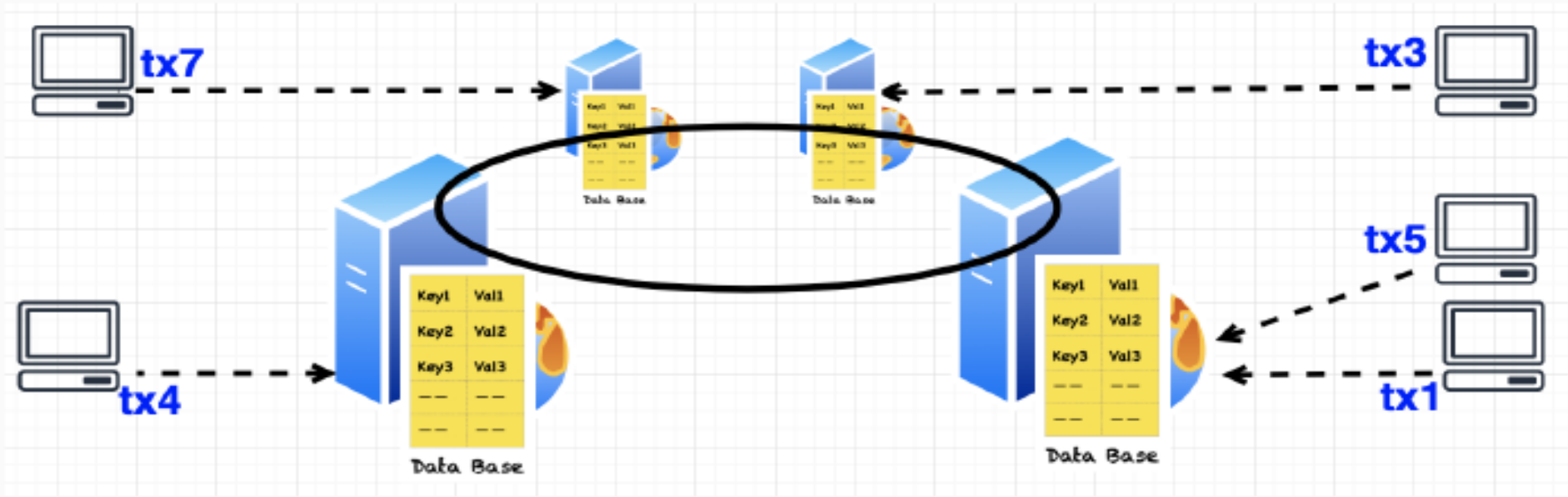


Decentralisation of the Ledger

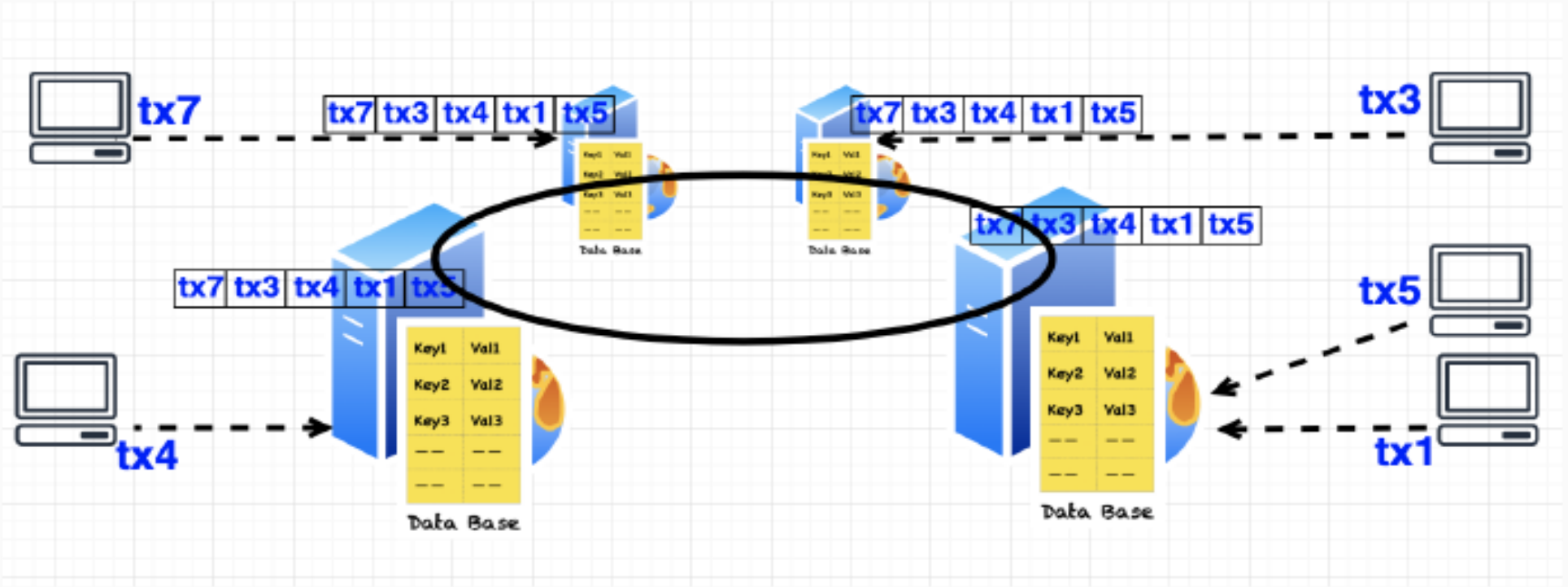
- A quick glimpse into a Blockchain-based distributed-ledger system:



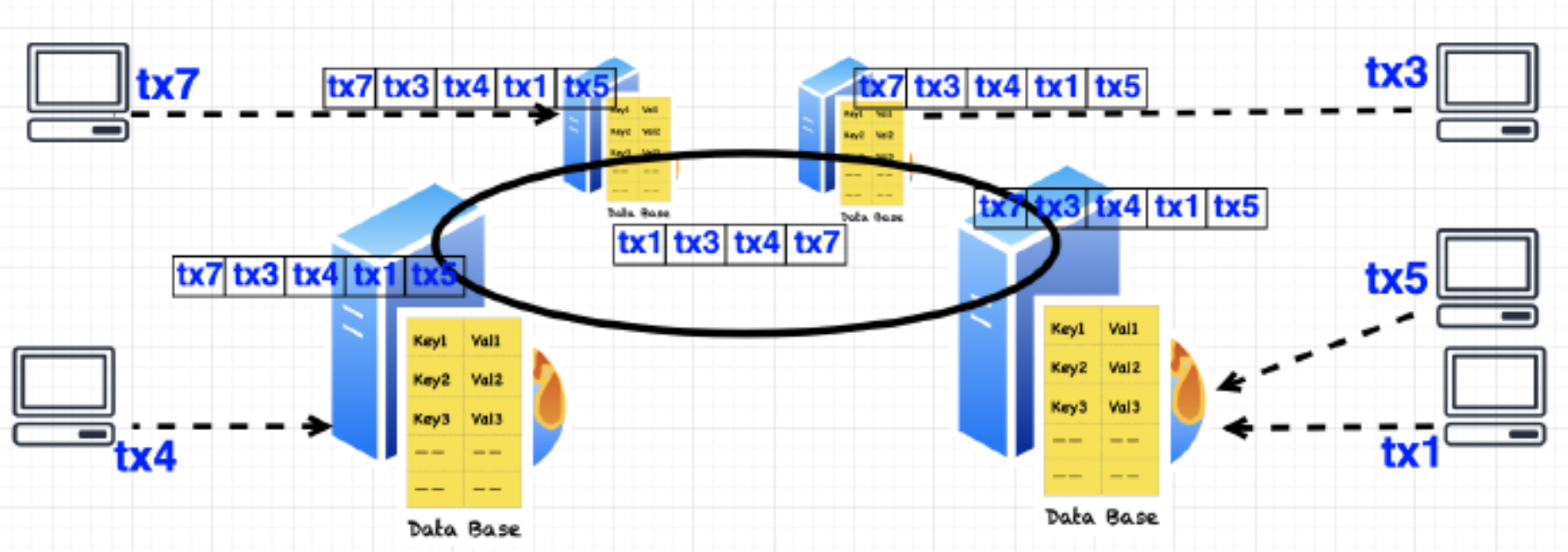
Transactions Requesting Ledger-updates



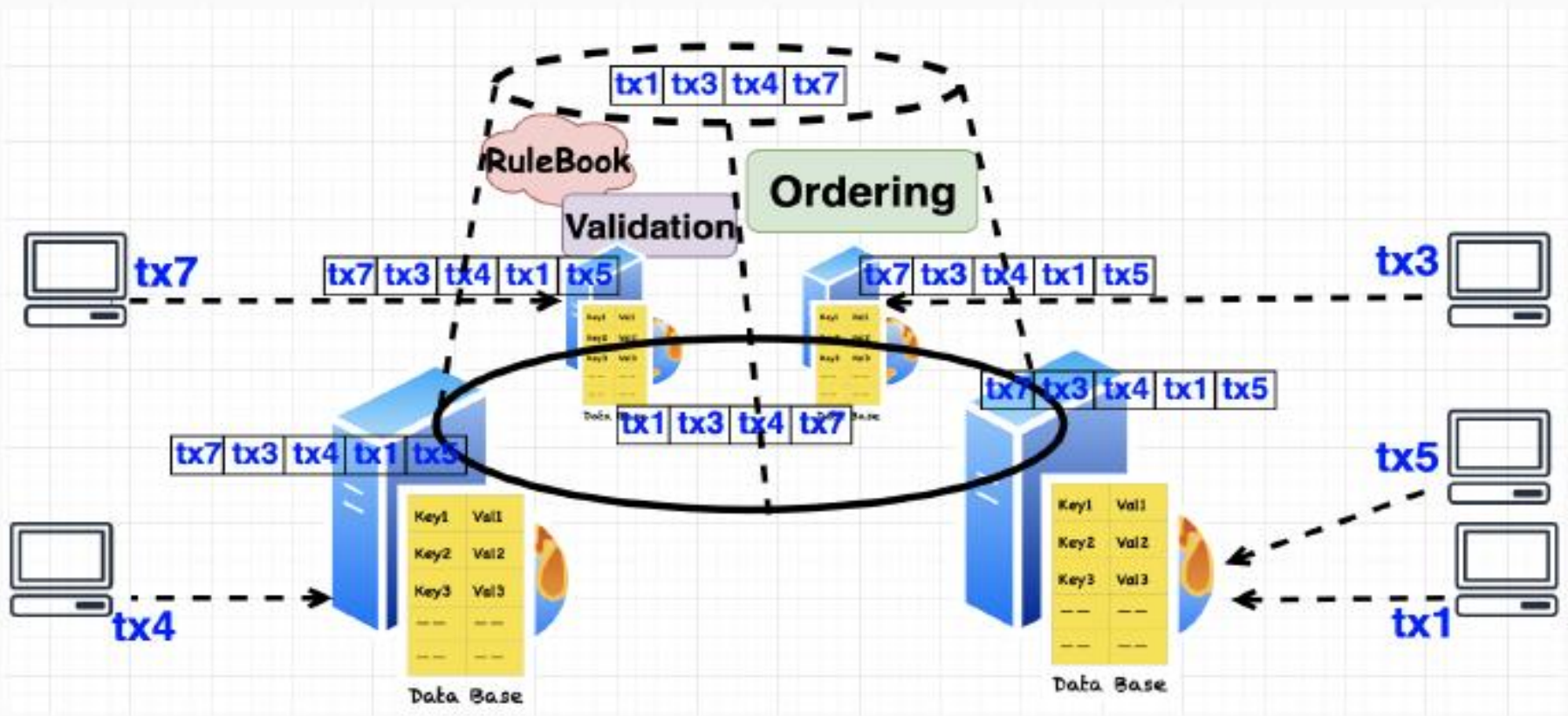
Network Propagating Transactions to Every Peer



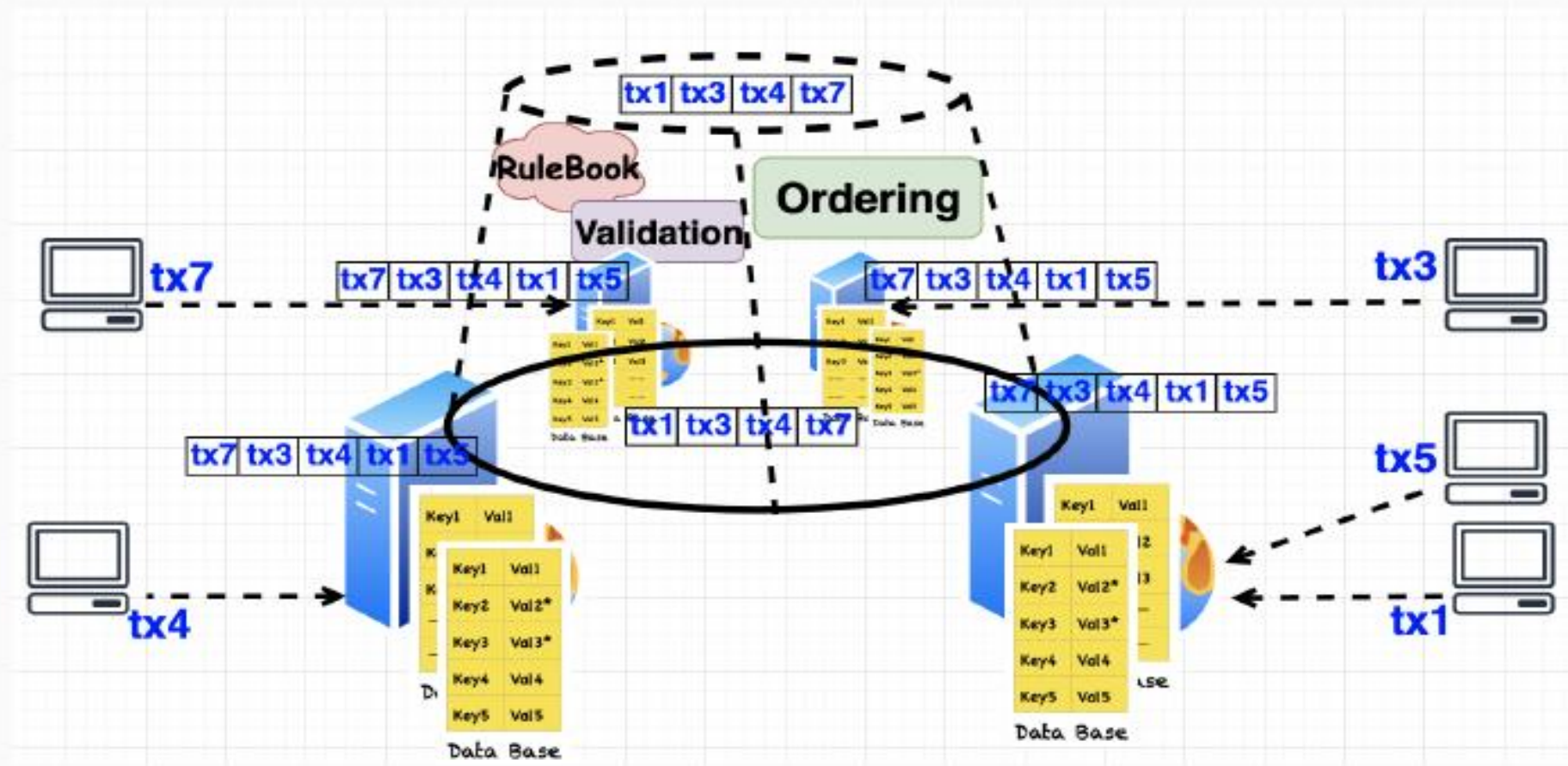
Validating and Ordering the Transactions: A Proposal



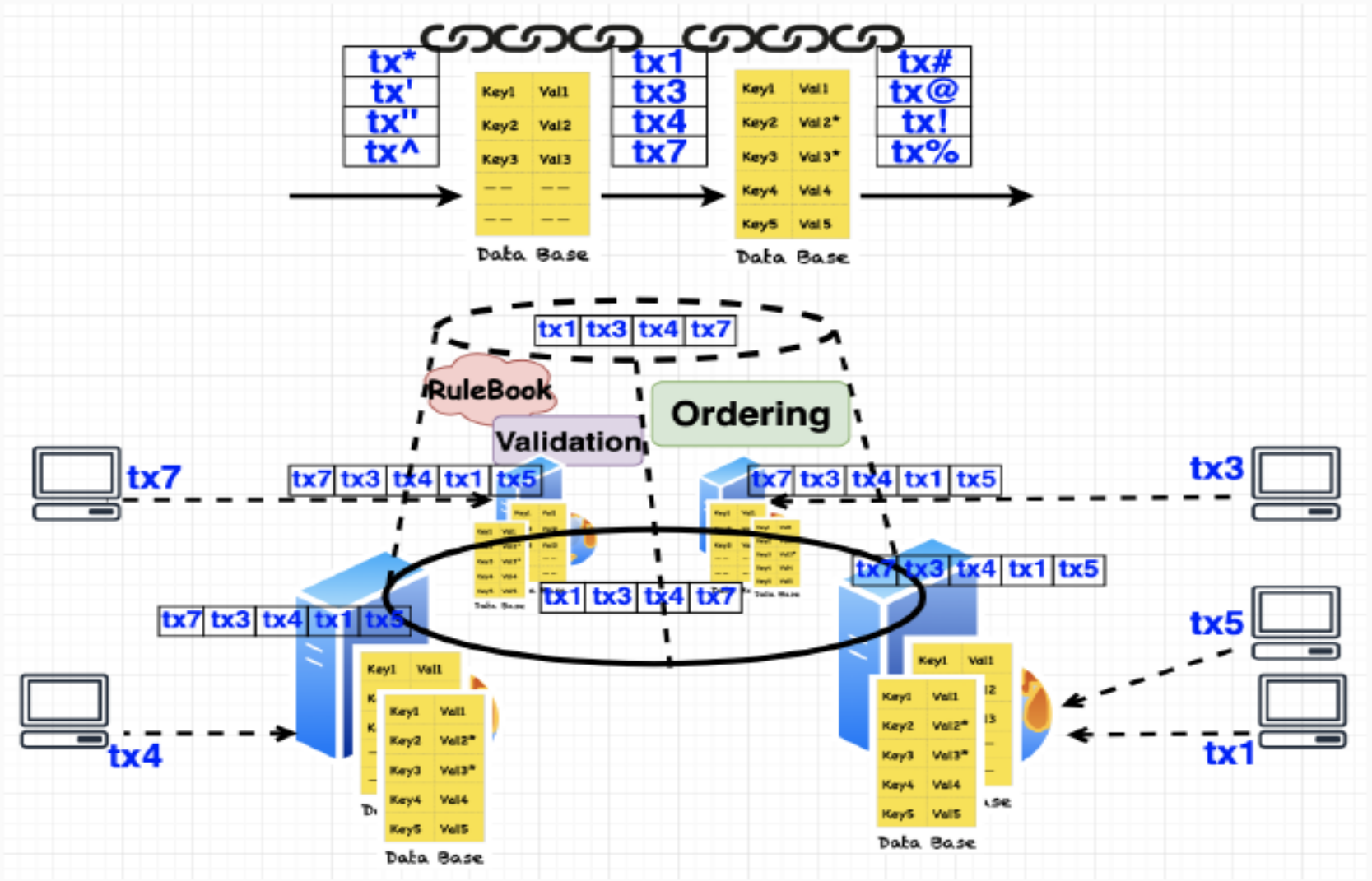
Validating and Ordering the Transactions: Approval



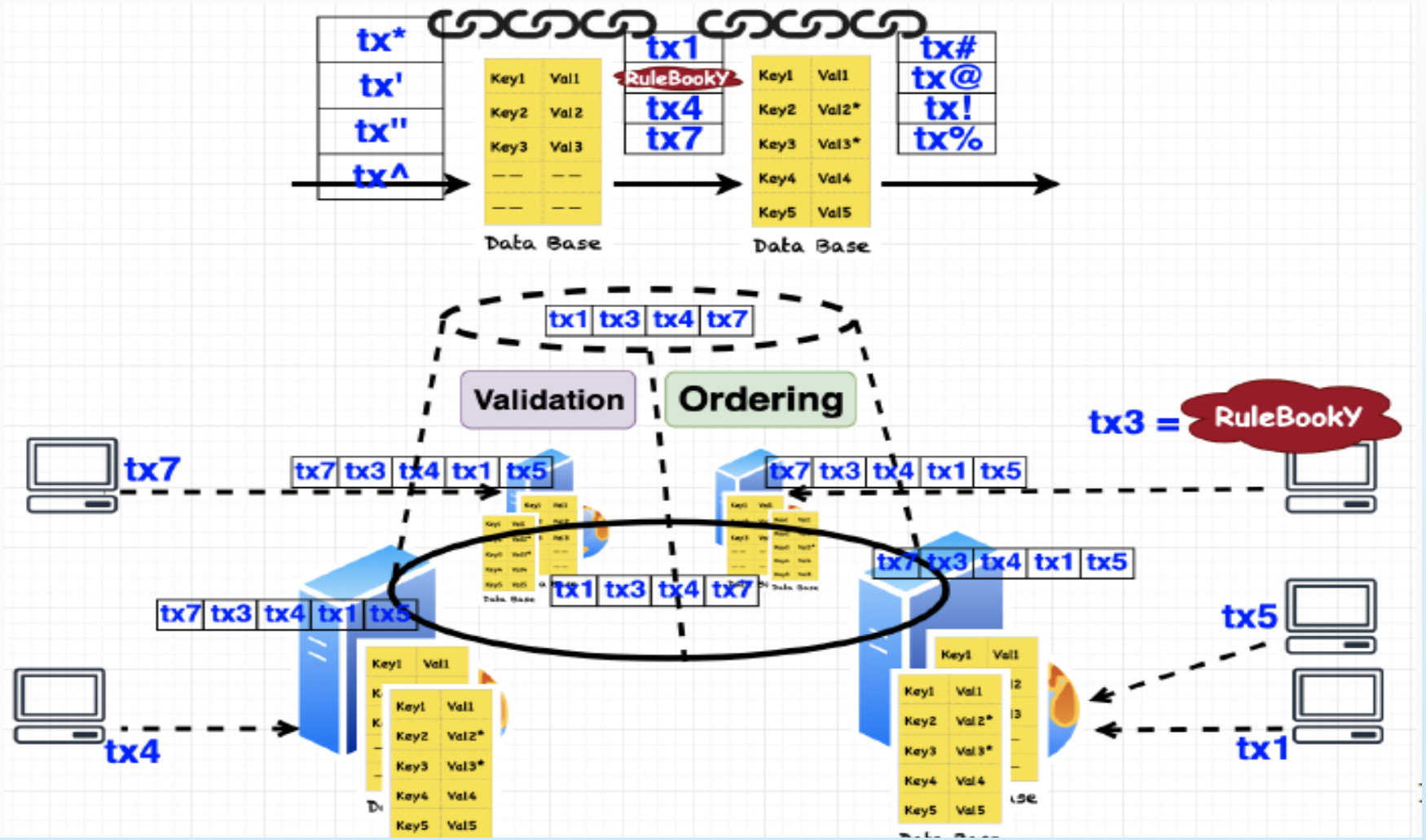
Network-wide Ledger-update



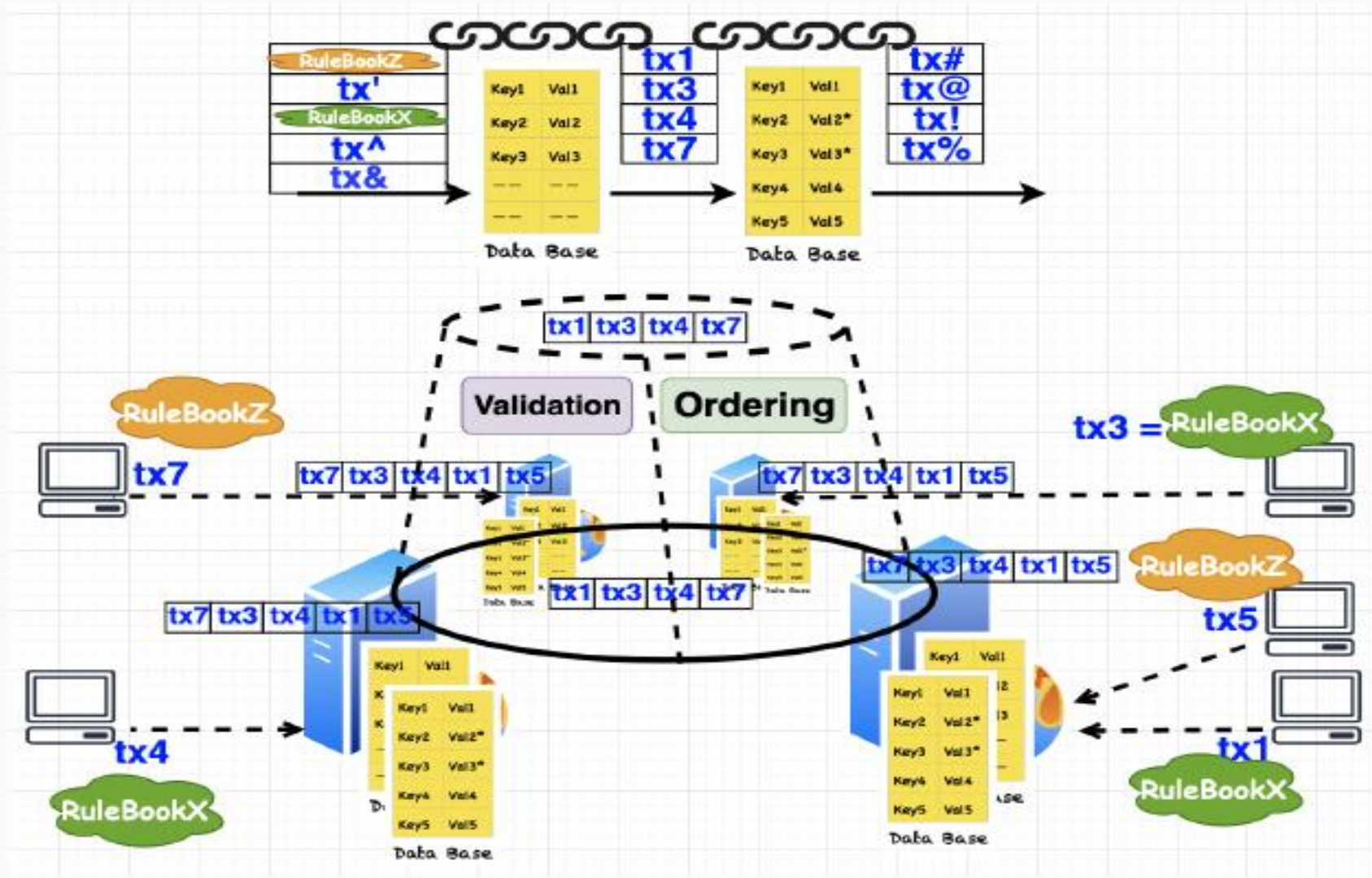
Consistent Ledger View; Immutable Transaction History



Building Blockchain: One Application Vs Many



Smart Contracts Enabled Blockchain



MR. KRISHNASURI NARAYANAM

SENIOR RESEARCH SOFTWARE ENGINEER, IBM MASTER INVENTOR, IBM RESEARCH, INDIA

EMAIL: knaraya3@in.ibm.com

Capacity building

- Concept note suggests “training & education” on a variety of topics for skill upgrade of the developers.
  - ➢ It’s also important to include training & education on development toolkits (e.g., Azure Blockchain Workbench, Hyperledger Composer, etc.), IDEs, etc. that are helpful specifically for the development and maintenance Blockchain solutions.
- Other advanced topics for “training & education” for skill upgrade of the developers are:
  - ➢ Concepts related to interoperability among different blockchain networks.
    - ○Interoperability is a key challenge to increase the value of any blockchain network.
    - ○E.g., recent works like “Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (Industry Track)”, Abebe et al., Middleware 2019.
  - ➢ Concepts related to design/development of Smart Contracts portable to different networks.
  - ➢ Concepts related to value added services that can be offered on top of the existing blockchain networks.

Scalability & Security

- Scalability:
  - Permissioned:
    - Node scalability (performance of the network with the increase in the number of nodes in the network) is an issue, while transaction throughput is good.
    - New protocols for consensus (e.g., MirBFT, etc.) are evolving to push the transaction throughput further.
  - Permissionless:
    - Node scalability is not an issue, while transaction throughput is a concern.
    - Permissionless networks typically use Proof-of-Work as the consensus algorithm. However, community is trying to adopt paradigms like Proof-of-Stake (e.g. Ethereum's upcoming Casper implementation), etc. for better throughputs.
- Privacy:
  - In Hyperledger Fabric, if a group of organizations on a network need to keep data private from other organizations, they have an option to create a new channel comprising just the organizations who need to access the data.
    - At the cost of administrative overheads like maintaining chaincode versions, policies, MSPs, etc.
  - Alternative to creation of separate channel in Hyperledger Fabric is to use private data collection/SideDB (private data is sent peer-to-peer via gossip protocol to only authorized organizations).

Scalability & Security

- Privacy:
  - Enigma protocol lets anyone perform computations on encrypted data, bring privacy to smart contracts and public blockchain.

- Scalability:
  - Sharding:
    - A database partitioning technique that will be used to dramatically scale Ethereum's blockchain and enable it to process more transactions per second.
  - Hashgraph:
    - It’s is DLT that claims to be more secure and fast.

Approaches for transforming existing Business Processes

- Concept note captures that the Blockchain community is undertaking several initiatives ranging from “tracking of the advancements within the field” to “understanding and evaluation of its popular applications”.

- However, it’s very important to look at approaches for transforming existing Business Processes with the help of Blockchain Technology.
  - E.g., Supply Chain industry is one which can get impacted by the use of Blockchain Technology since multiple parties are involved often in any supply chain process, where
    - these parties are either competing with each other
    - or work in silos
  - IBM’s solutions like **TradeLens & IBM Food Trust** are 2 such examples which are helping the transformation of the supply chain networks.
    - TradeLens – for Global Shipping supply chain
    - IBM Food Trust – for Food supply chain
  - The idea here is to provide space for increased collaboration & innovation thus helping all the parties involved in the respective domain get benefitted.

Thank You