



Hyperledger Technical Introduction

Anthony O'Dowd
odowda@uk.ibm.com
@ajodowd

Today's Session Agenda

(The Business Network Context)

Sample application – Car Leasing

The Participants in a Blockchain Network

How Applications use the Blockchain Ledger

Operating Blockchain Networks

Security and Trust

Integrating Systems

Summary and Next Steps

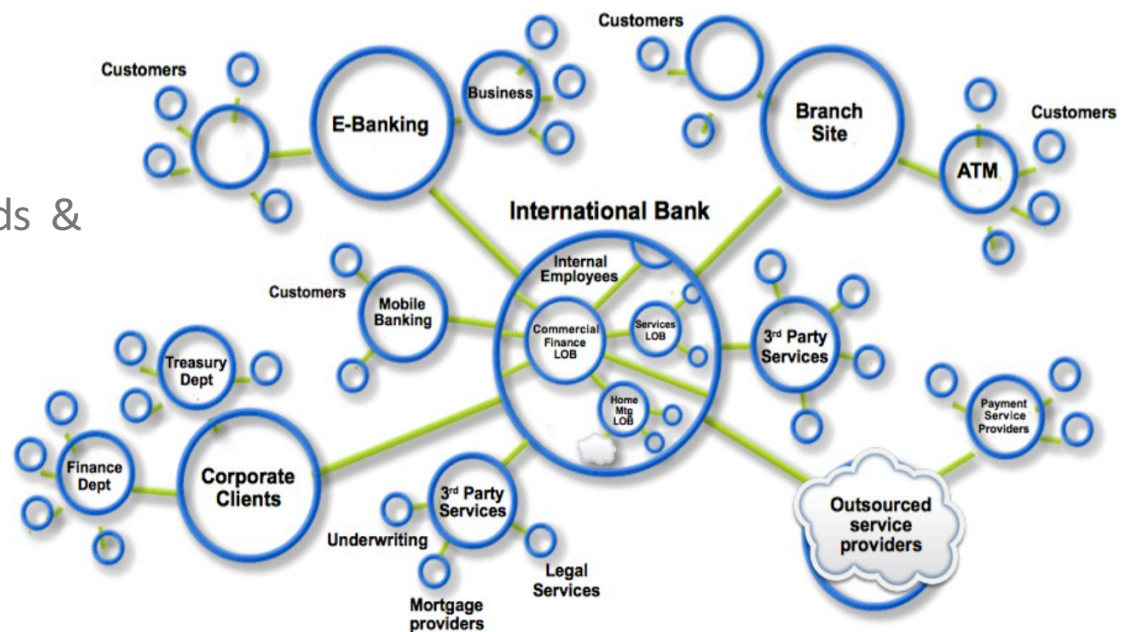


The Business Network Context

Business Networks, Assets, Ledgers, Participants,
Transactions, Contracts

Business Networks, Markets & Wealth

- Business Networks benefit from connectivity
 - Connected customers, suppliers, banks, partners
 - Cross geography & regulatory boundary
- Wealth is generated by the flow of goods & services across business network
- Markets are central to this process:
 - Public (fruit market, car auction), or
 - Private (supply chain financing, bonds)



Assets

- Anything that is capable of being owned or controlled to produce **value**, is an **asset**
- Two fundamental types of asset
 - Tangible, e.g. a house
 - Intangible e.g. a mortgage
- Intangible assets subdivide
 - Financial, e.g. bond
 - Intellectual e.g. patents
 - Digital e.g. music
- Cash is also an asset
 - Has property of anonymity



Ledgers are Important

- **Ledger** ^[1] is THE system of record for a business
 - records asset transfer between participants.
- Business will have multiple ledgers for multiple business networks in which they participate.



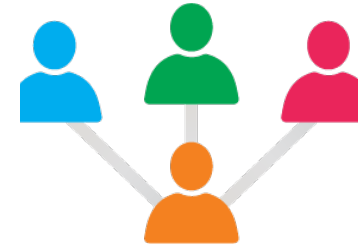
[1] The principal book (or computer file) for recording and totaling financial transactions by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.

A screenshot of a computer application titled "Accounts Ledger". The window has a title bar with "Transaction Entry" and standard window controls. Below the title bar, there's a header area with "Accounts Ledger" and a "Balance: \$43,338.50". The main area contains a table with columns: ID, Date, Account, Description, Withdrawal Amt, Deposit Amt, and Balance. The table lists various transactions from 1994 to 2005, including transportation, meals, lodging, and mutual funds. On the right side of the window, there's a "Tasks" panel with buttons for "New Reports", "Add or Delete Accounts", "Add or Delete Account Types", and "Delete All Sample Data". At the bottom, there's a "Totals" row showing a total withdrawal of \$911.50 and a total deposit of \$44,250.00.

Participants, Transactions & Contracts

- **Participants** - members of a business network

- Customer, Supplier, Government, Regulator
- Usually resides in an organization
- Has specific identities and roles



- **Transaction** - an asset transfer

- John gives a car to Anthony (simple)

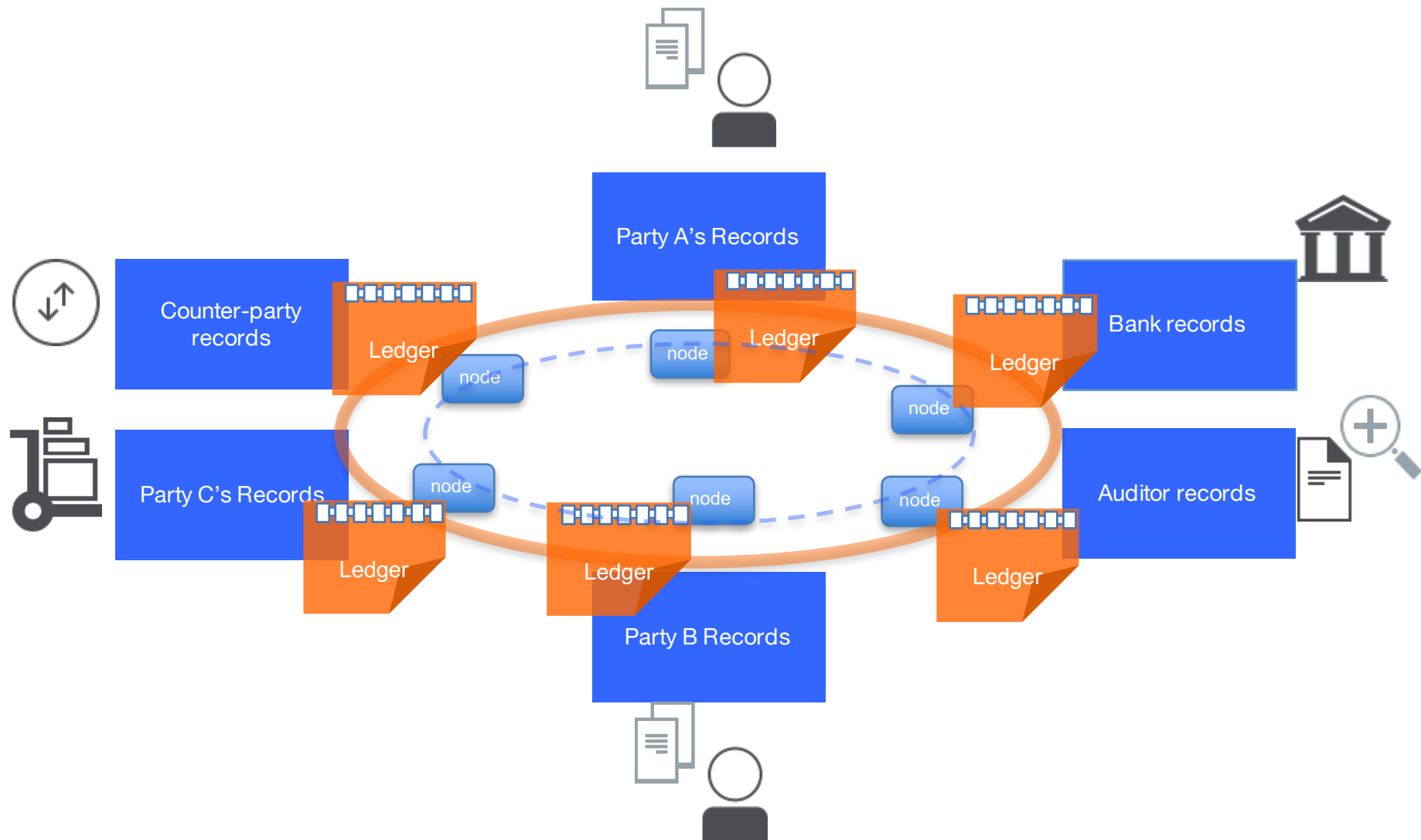


- **Contract** - conditions for transaction to occur

- If Anthony pays John money, then car passes from John to Anthony (simple)
- If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)



Blockchain – a shared, replicated, permissioned ledger



Smart contracts for trusted business processes
Consensus, provenance, immutability, finality

Blockchain Capabilities

Append-only distributed
system of record shared
across business network

Shared
Ledger

Smart
Contract

Business terms embedded
in transaction database &
executed with transactions

Ensuring appropriate
visibility; transactions are
secure, authenticated &
verifiable

Privacy

Consensus

All parties agree to
network verified
transaction

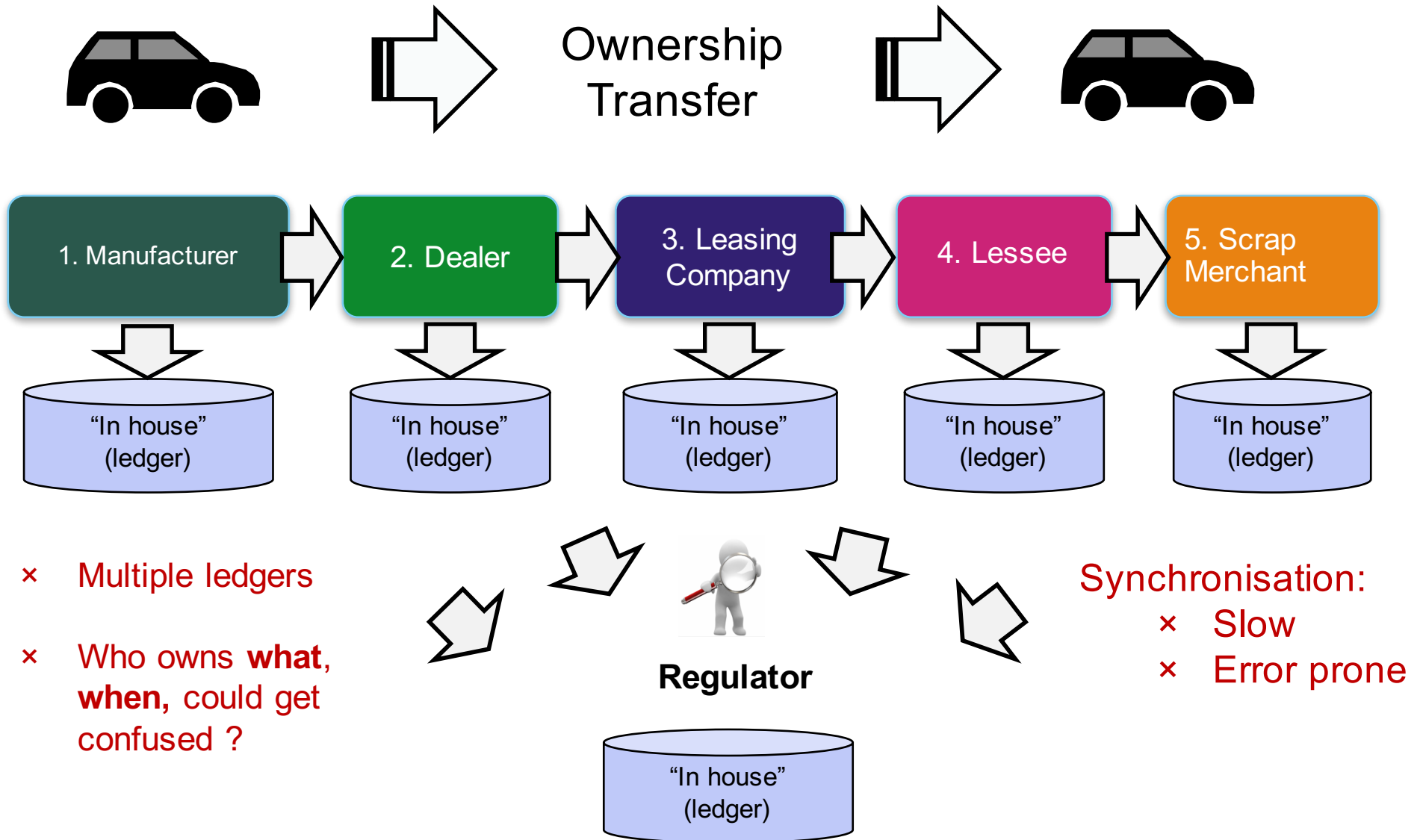
Broader participation, lower cost, increased efficiency



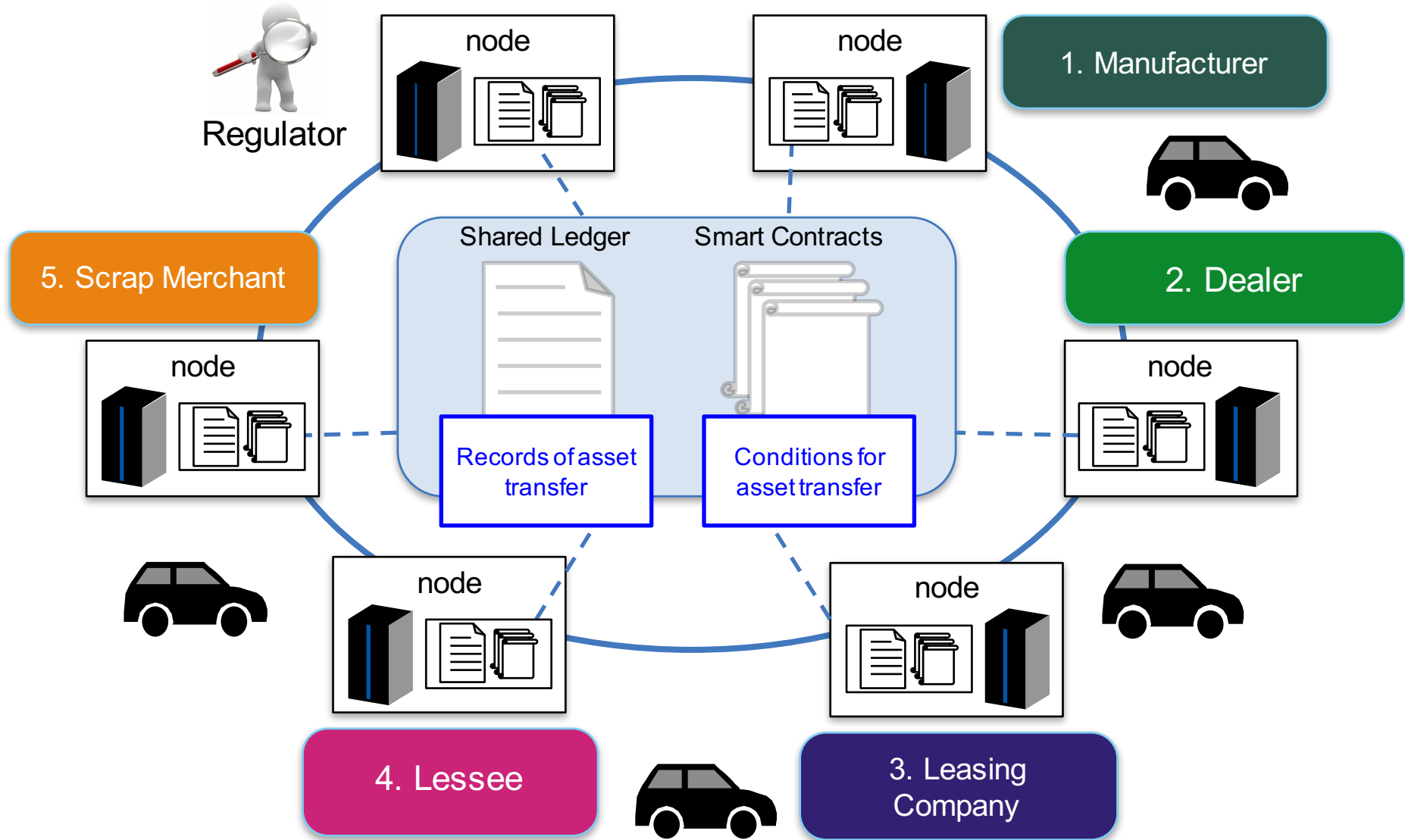
Sample Application

Car Leasing

Car Leasing Business Network



Car Leasing Business Network with Blockchain

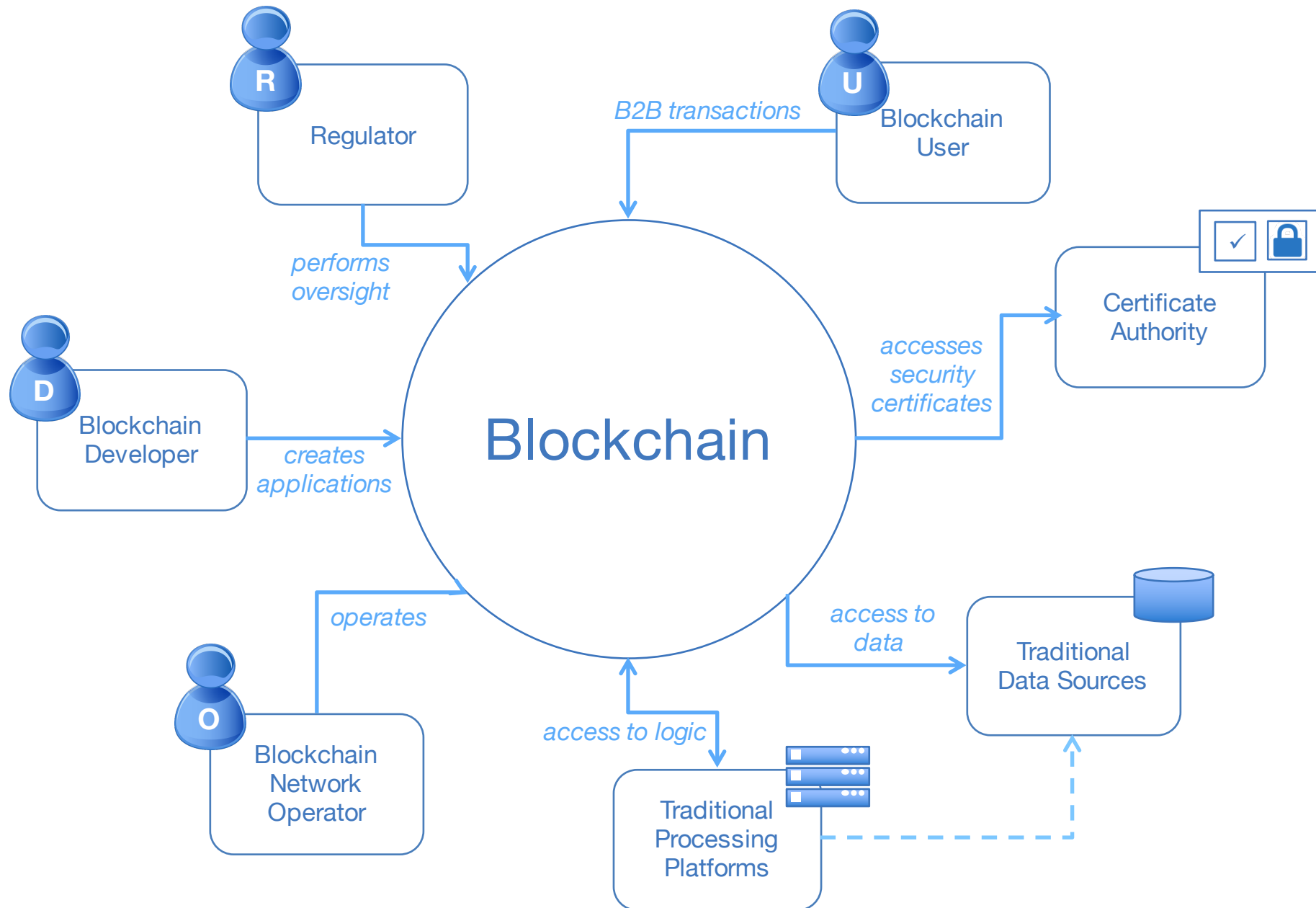











The Participants in a Blockchain Network

Systems Context

The Participants in a Blockchain Network



Blockchain Participants

Blockchain User		the business user, operating in a business network. This role interacts with the Blockchain using a LOB application. They are not aware of the Blockchain.
Blockchain Regulator		the overall authority in a business network. Specifically, regulators may require broad access to the ledger's contents.
Blockchain Developer		the developer of applications and smart contracts that interact with the Blockchain and are used by Blockchain users.
Blockchain Network Operator		defines, creates, manages and monitors the Blockchain network. Each business in the network has a Blockchain Network operator.
Certificate Authority		manages the different types of certificates required to run a permissioned Blockchain.
Traditional Processing Platform		an existing computer system which may be used by the Blockchain to augment processing. This system may also need to initiate requests into the Blockchain.
Traditional Data Sources		an existing data system which may provide data to influence the behaviour of smart contracts.



The Components in a Blockchain

Component Model

Blockchain Components

Blockchain

Ledger



contains the current world state of the ledger and a Blockchain of transaction invocations

Smart Contract



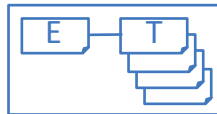
encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state

Consensus Network



a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger

Membership



manages identity and transaction certificates, as well as other aspects of permissioned access

Events



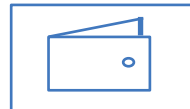
creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution.

Systems Management



provides the ability to create, change and monitor Blockchain components

Wallet



securely manages a user's security credentials

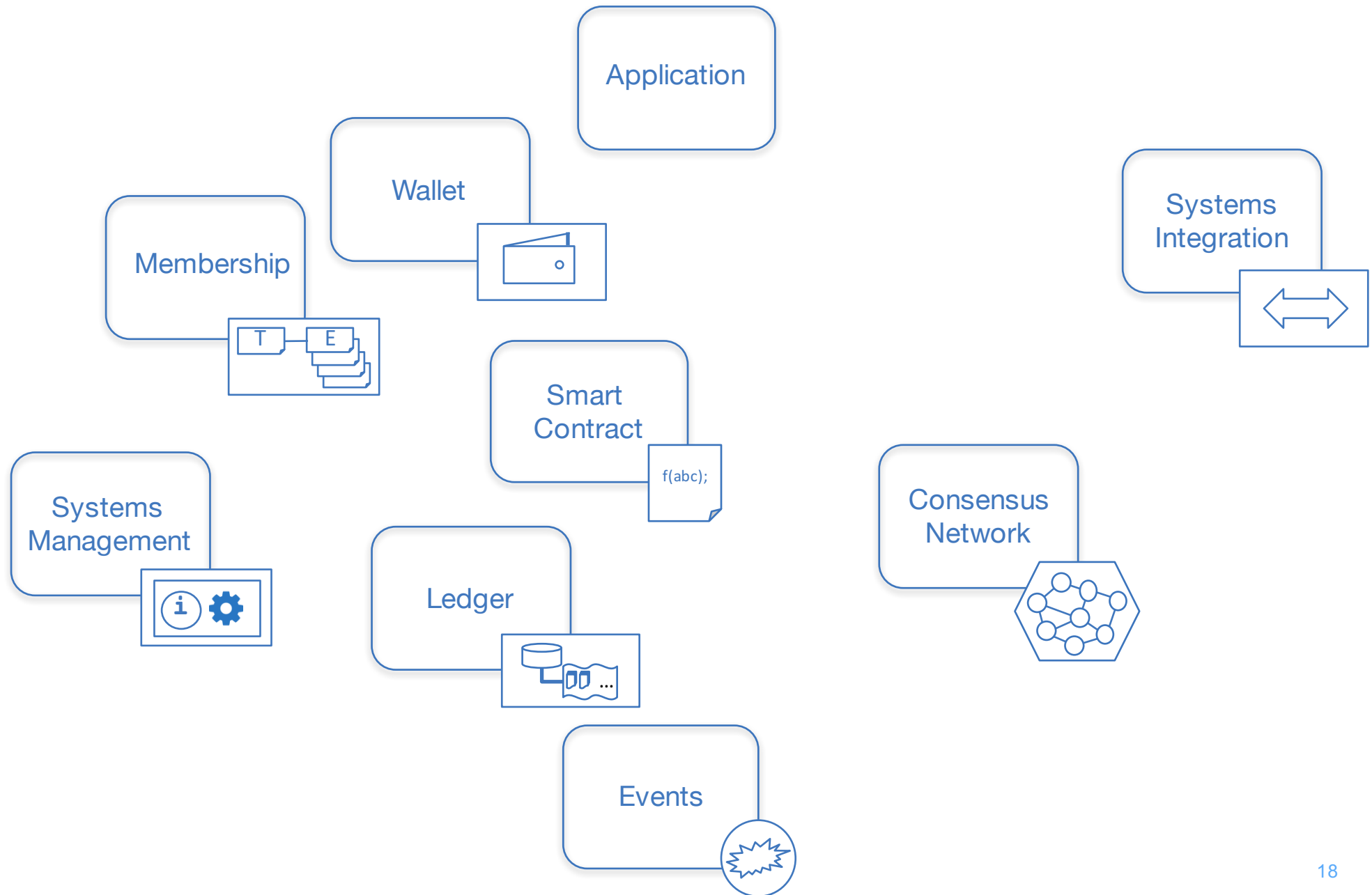
Systems Integration



responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it.

Blockchain Components

Blockchain

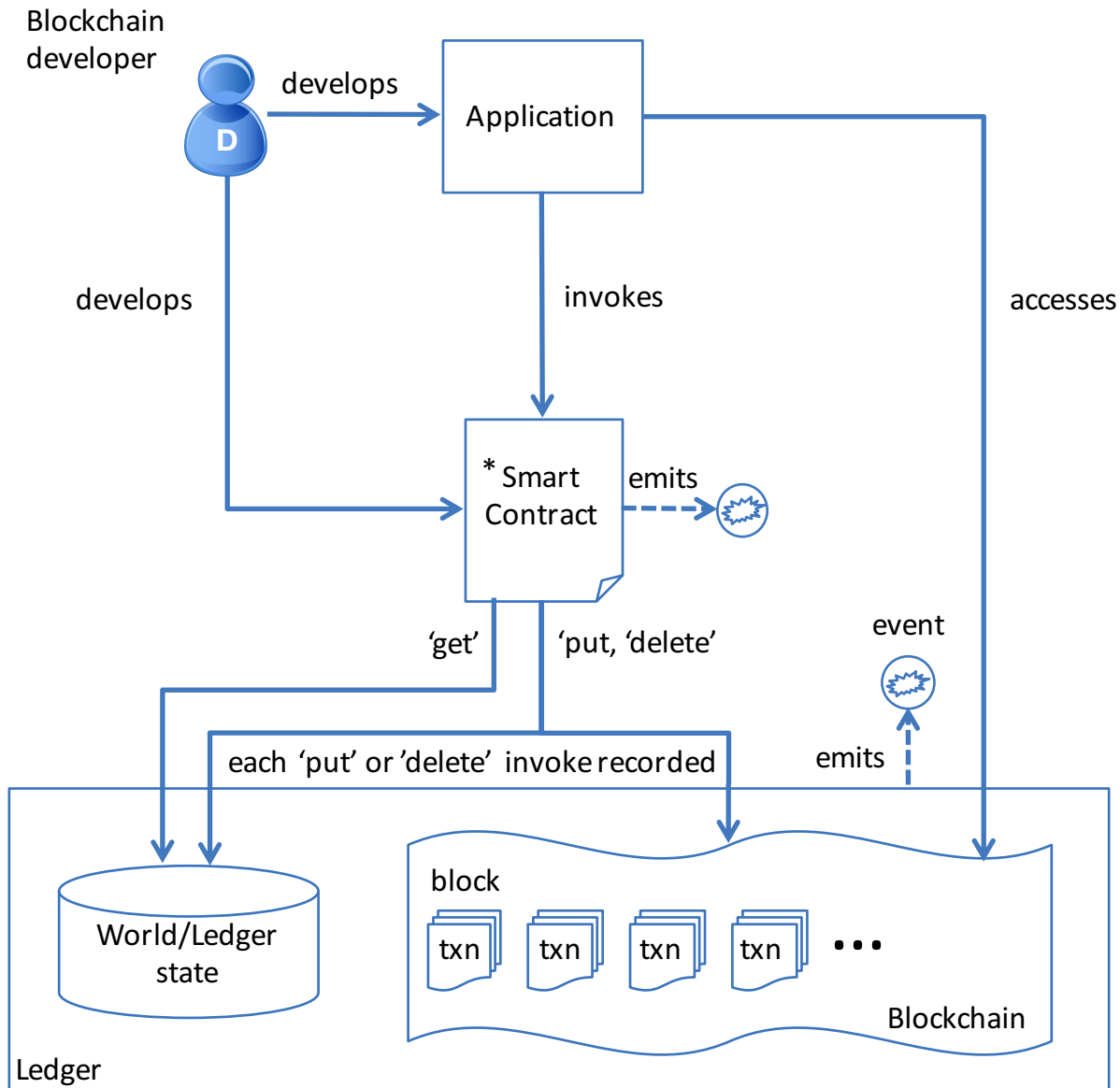




How Applications use the Ledger

The key elements of a Blockchain application

Blockchain Applications and the Ledger



* Smart Contract
implemented
using chain code

Blockchain Applications

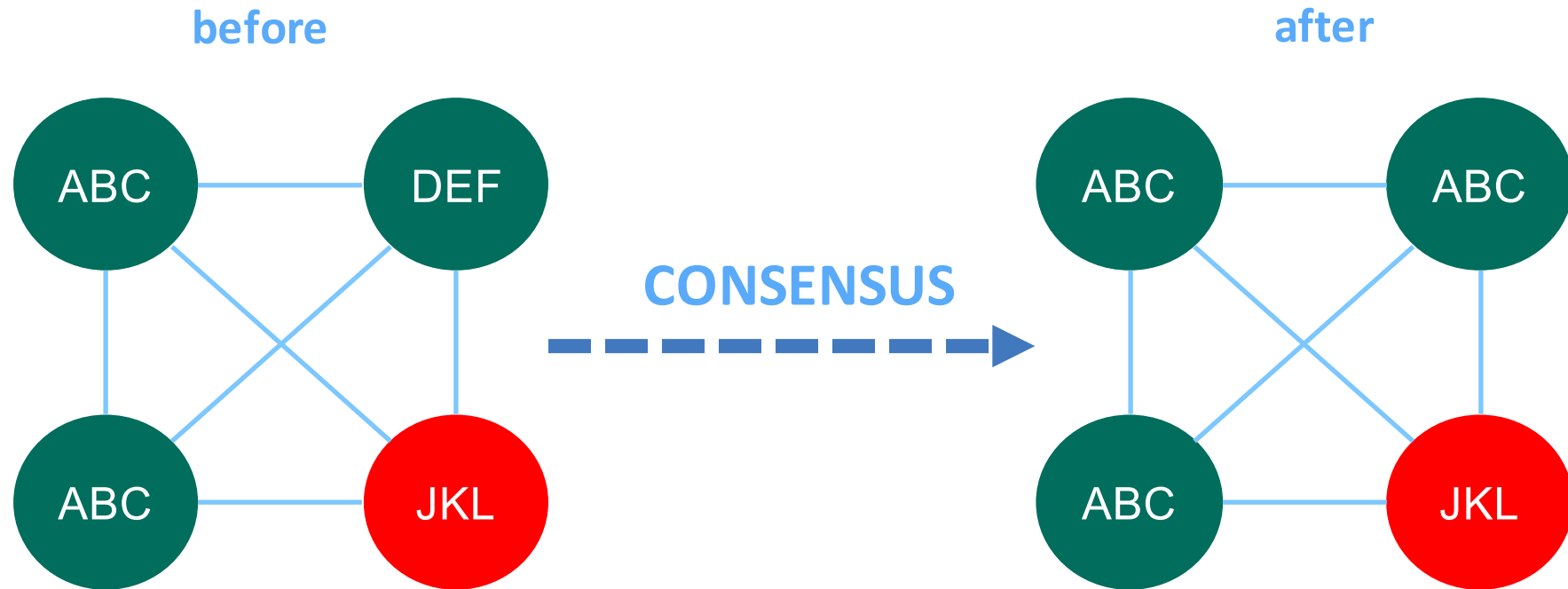
- Application
 - Focuses on Blockchain user business needs and experience
 - Calls smart contract for interactions with ledger state
 - Can access transaction ledger directly, if required
 - Can process events if required
- Smart Contract
 - Chain code encapsulates business logic. Choice of implementation language
 - Contract developer defines relevant interfaces (e.g. queryOwner, updateOwner ...)
 - Different interfaces access ledger state accordingly – consistent read and write provided
 - Each invocation of a smart contract is a “Blockchain transaction”
- Ledger
 - World/Ledger state holds current value of smart contract data
 - e.g. vehicleOwner=Daisy
 - Blockchain holds historic sequence of all chain code transactions
 - e.g. updateOwner(from=John, to=Anthony); updateOwner (from=Anthony, to=Daisy);...



Operating Blockchain Networks

Configuring for a replicated ledger

Maintaining a consistent ledger



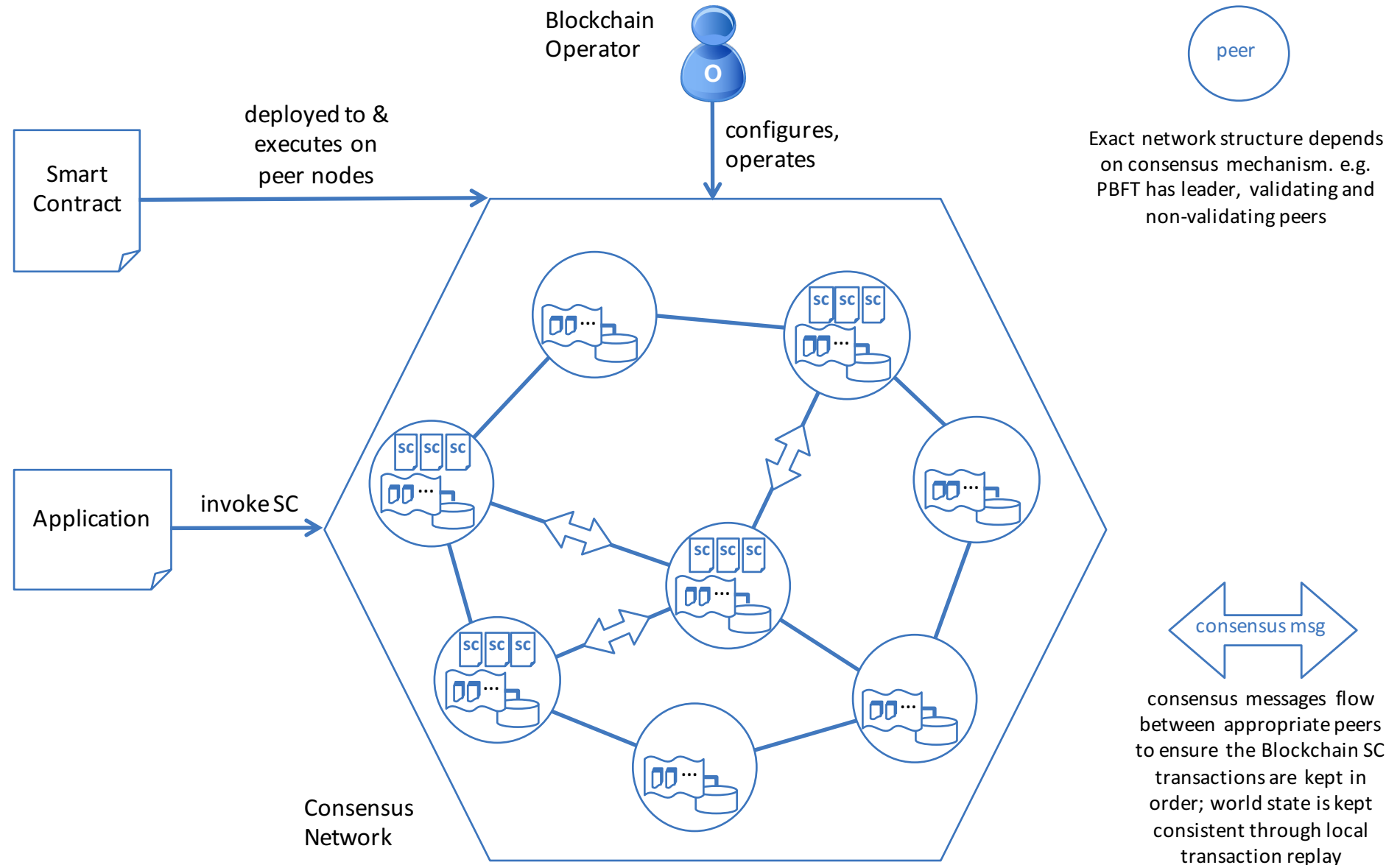
Keep all peers up-to-date

Fix any peers in error

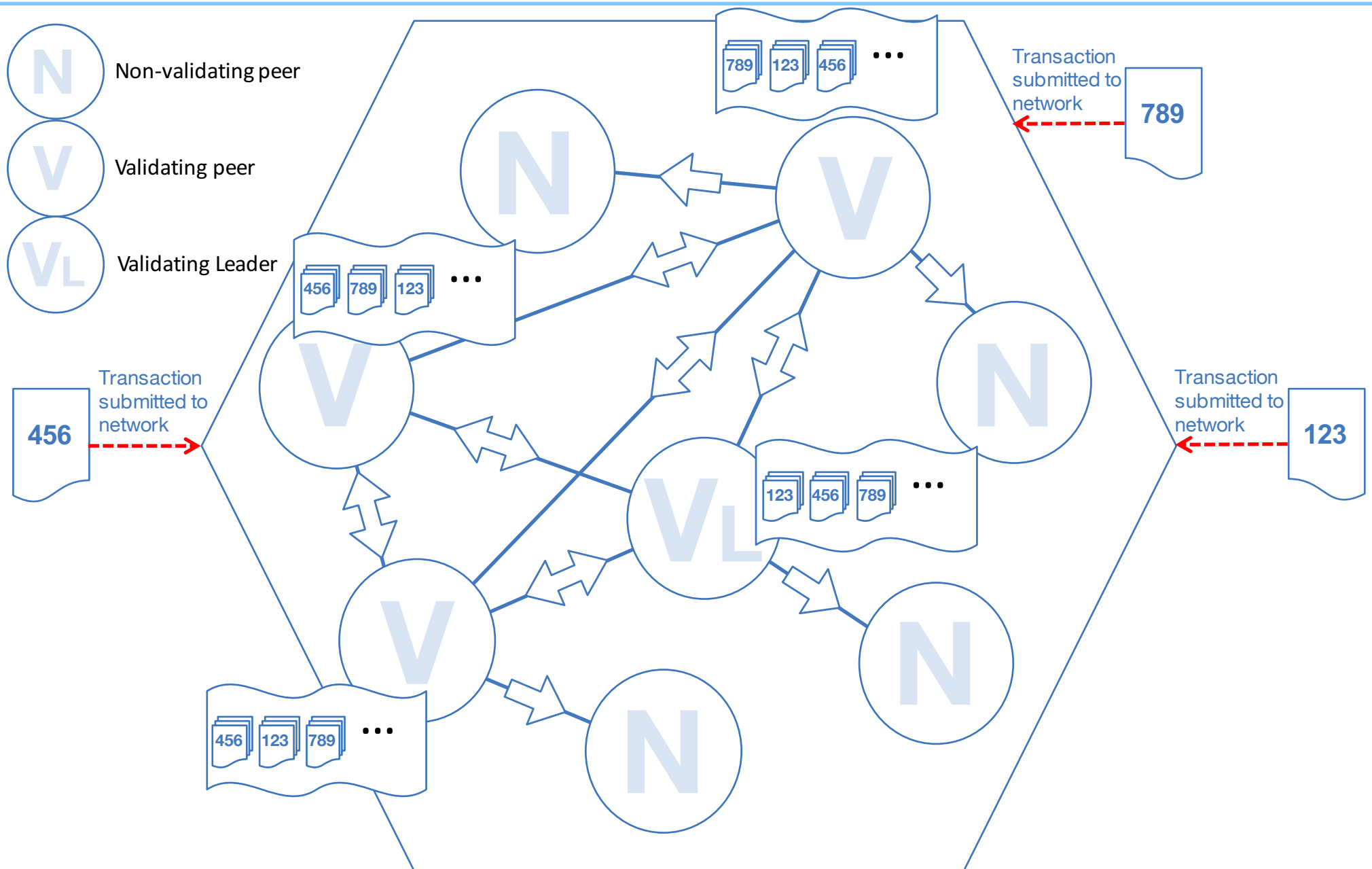
Quarantine all malicious nodes



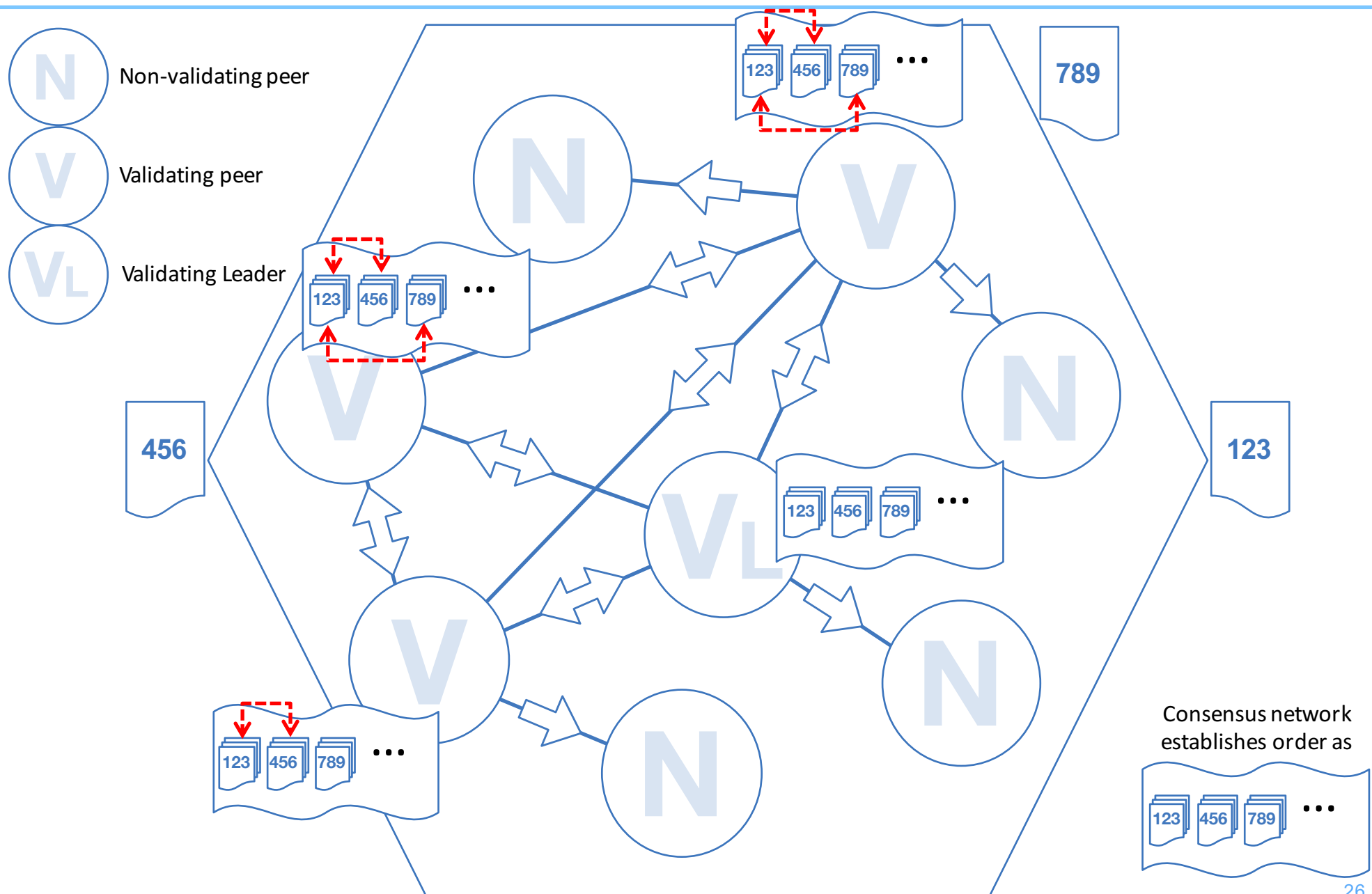
Consensus and the Blockchain Network



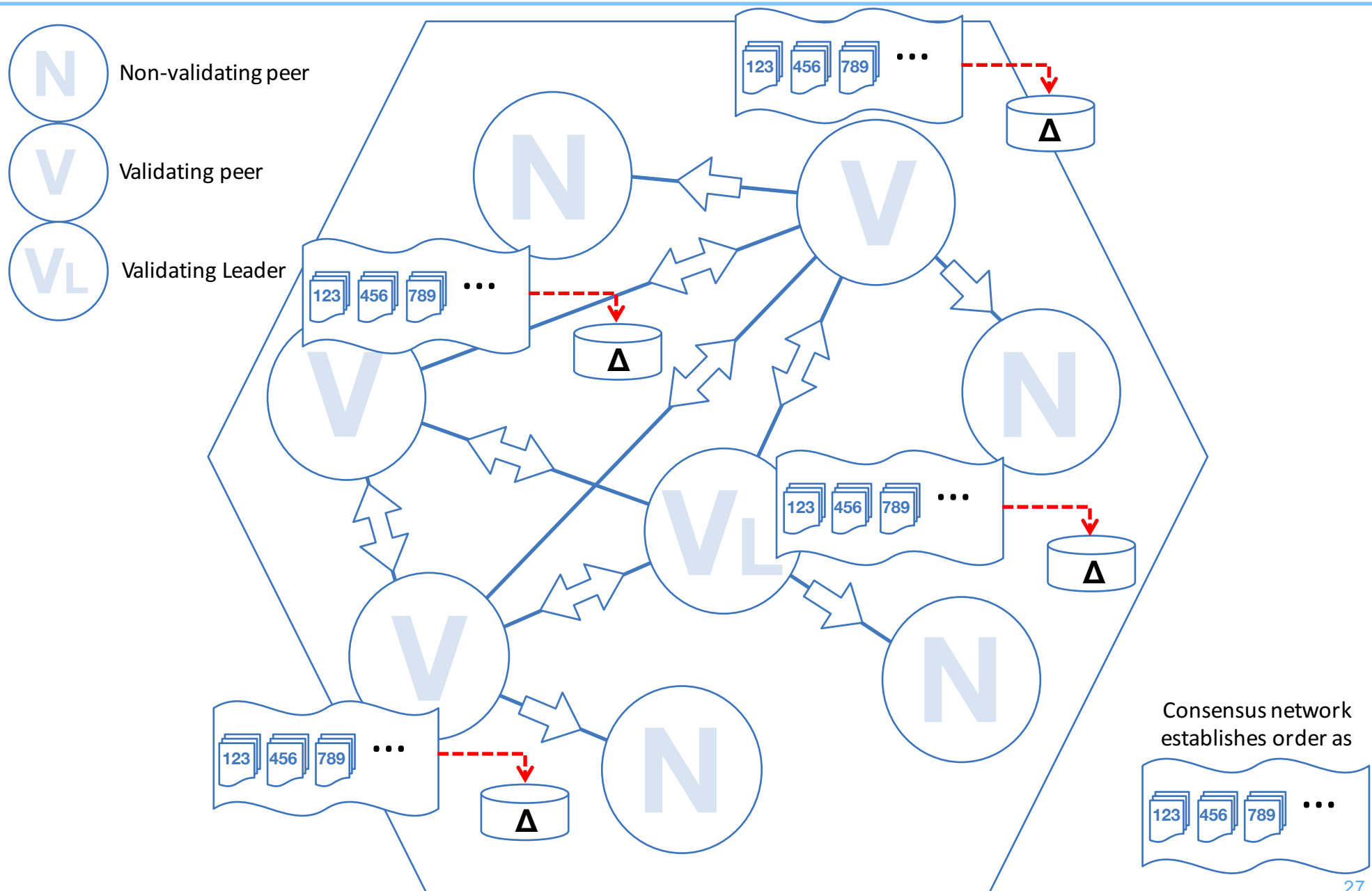
How a PBFT Network Works (1/4) – Submission



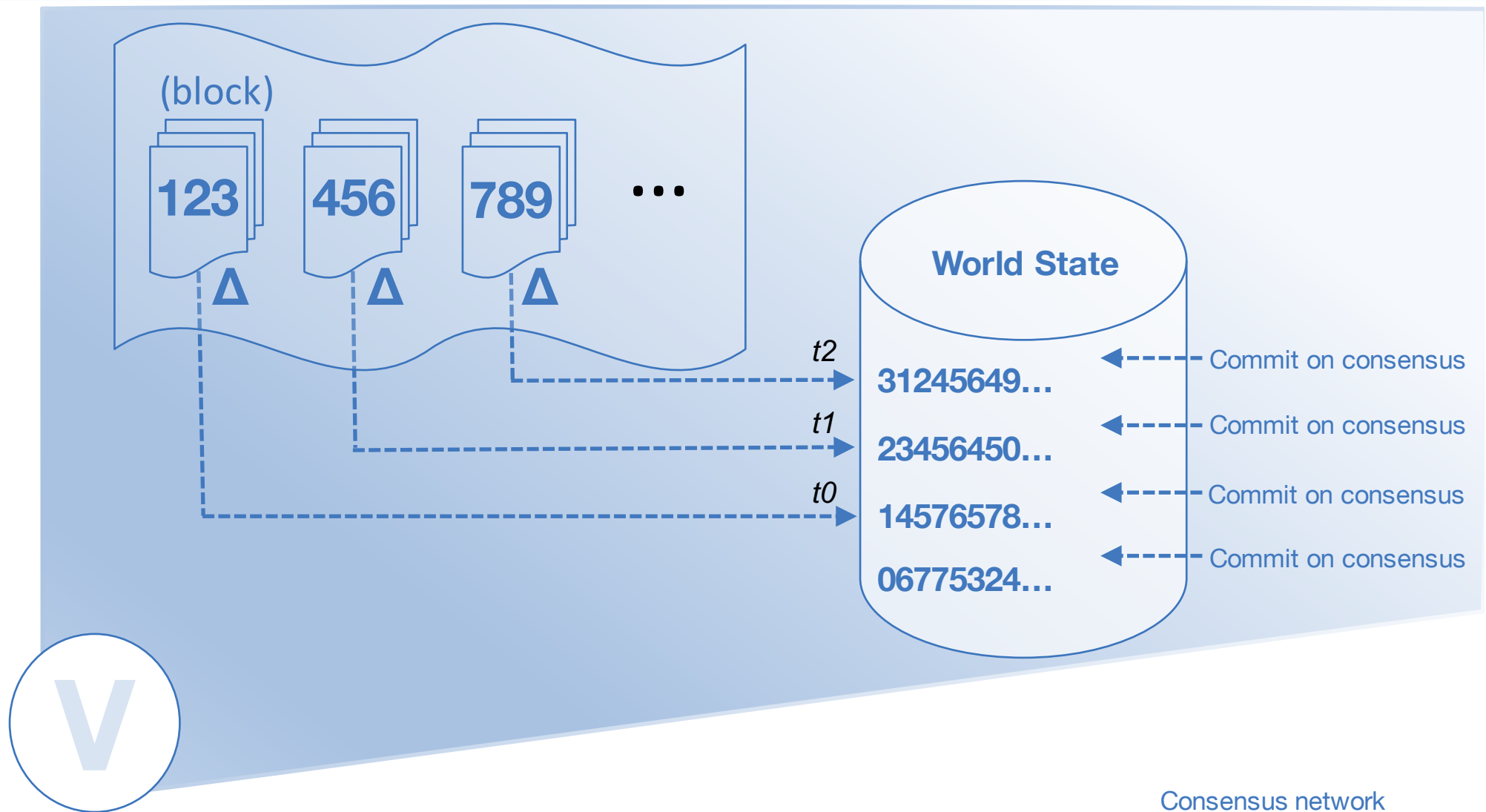
How a PBFT Network Works (2/4) – Ordering



How a PBFT Network Works (3/4) – Execution



How a PBFT Network Works (4/4) – Validation



Δ = Delta Hash

Consensus network
validates execution output
(delta hashes must match).
Changes merged on
commit

Blockchain Networks

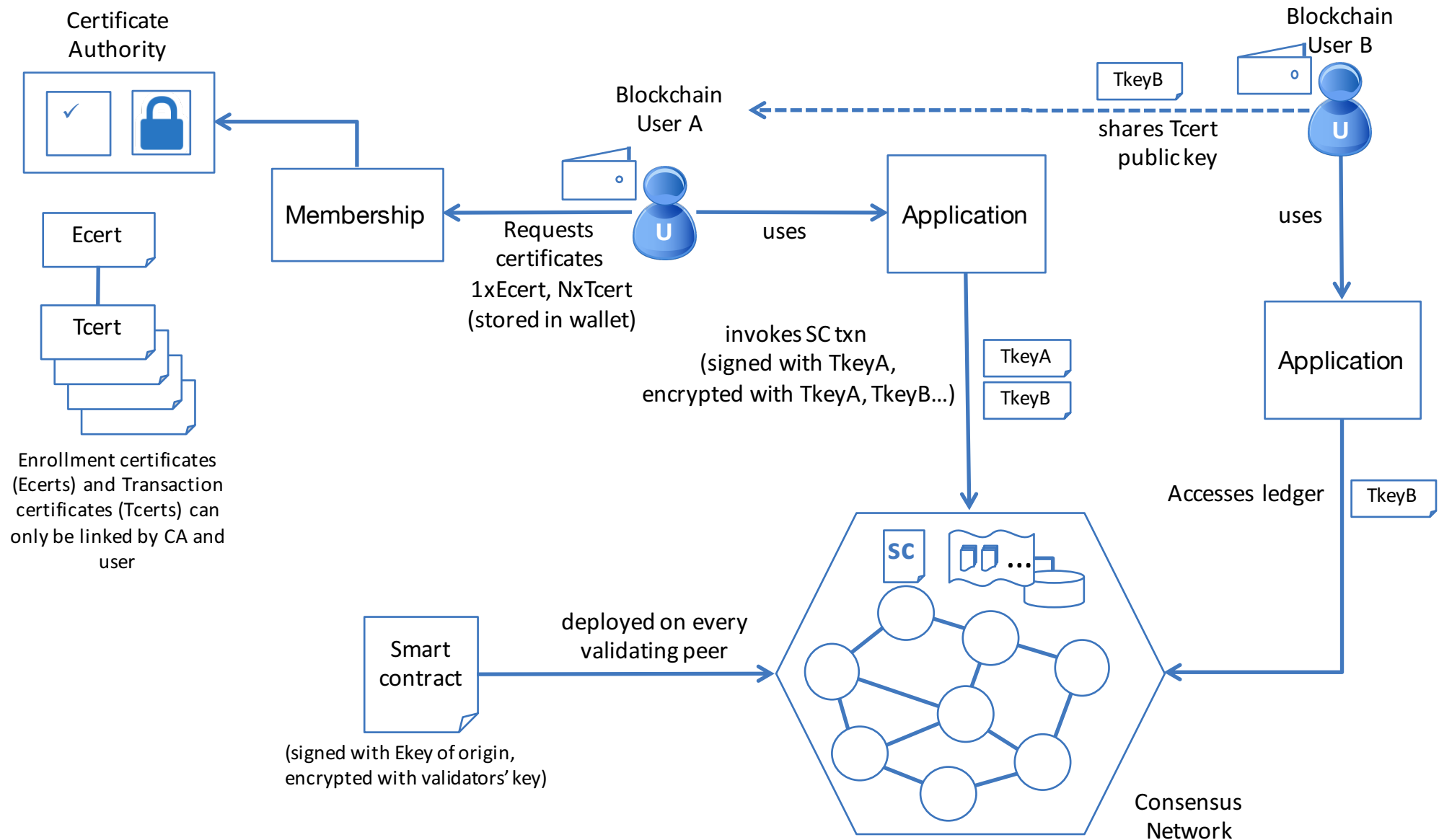
- Blockchain Network
 - Comprises a connected set of peer nodes, each owning a copy of the ledger
 - Peers collaborate to maintain consistent replicated copies of the ledger
 - Different mechanisms for collaboration – so-called “consensus protocols”
 - Peers managed by key network participants
- Consensus Protocol Options
 - PBFT excellent first choice. NOOPs (No Operation) available for starter networks
 - Other protocols can be added (non-trivial!)
- PBFT Overview
 - Defines non-validating peers, validating peers, with 1-validating leader
 - Leader receives transactions from connected applications
 - Leader organizes and distributes transactions with validator network
 - Copes with erring and malicious validators at very low compute cost
 - Each v-peer executes transactions to bring local ledger copy up-to-date
 - nv-peers' ledgers maintained from connected v-peer's



Permissioned Ledger Access

Transaction and identity privacy

Permissioned Ledger Access



Transaction and Identity Privacy

- Transaction Certificates, Tcerts
 - Disposable certificates, typically used once, requested from Transaction CA
 - Tcert derived from long term identity - Enrollment Certificate, Ecert
 - Only Transaction CA can link Ecert and Tcert
- Permissioned Interactions
 - Consumer shares public Tcert to provider
 - Provider invokes chain code transaction as usual, but
 - Signs with provider's private Tcert for authentication
 - Encrypts with provider and consumer Tcerts for subsequent access
 - Consumers can subsequently access ledger data using their private key
- Secure chain code
 - CC can also be signed and encrypted, to keep verify and secure contract details
 - Signing is by contract owner/author
 - Encryption ensures only validators can see and execute transaction chain code



Summary and Next Steps

For users

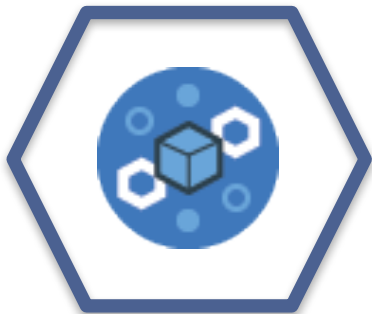
IBM Offerings Supporting Hyperledger

LINUX FOUNDATION
HYPERLEDGER
PROJECT

IBM Blockchain
ON IBM CLOUD

IBM Blockchain
SOLUTIONS

BLUEMIX SERVICE



Blockchain

Managed Service on IBM Cloud

Your private Blockchain network in 1-click

Learn with sample applications

Develop your own Smart Contracts

<http://www.ibm.com/blockchain/>

Summary and Next Steps

- We are at the beginning of the Hyperledger Blockchain journey!
- Apply shared ledgers and smart contracts to your Business Network
- Think about your participants, assets and business processes
- Spend time thinking about realistic business use cases
- Get some hands-on experience with the technology
- Do a First Project in 2016!
- IBM can help with your Hyperledger Blockchain journey

Thank You!