CS 731: Blockchain Technology And Applications

Sandeep K. Shukla

IIT Kanpur

C3I Center

Key Concepts and Benefits of Blockchain for Business

Append-only distributed system of record shared across business network

Shared Ledger`

Security

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

Business terms embedded in transaction database & executed with transactions

Smart Contracts

Consensus

All parties agree to network verified transaction

Reduces Time

Transaction time from days to near instantaneous

Removes Cost

Overheads and cost intermediaries

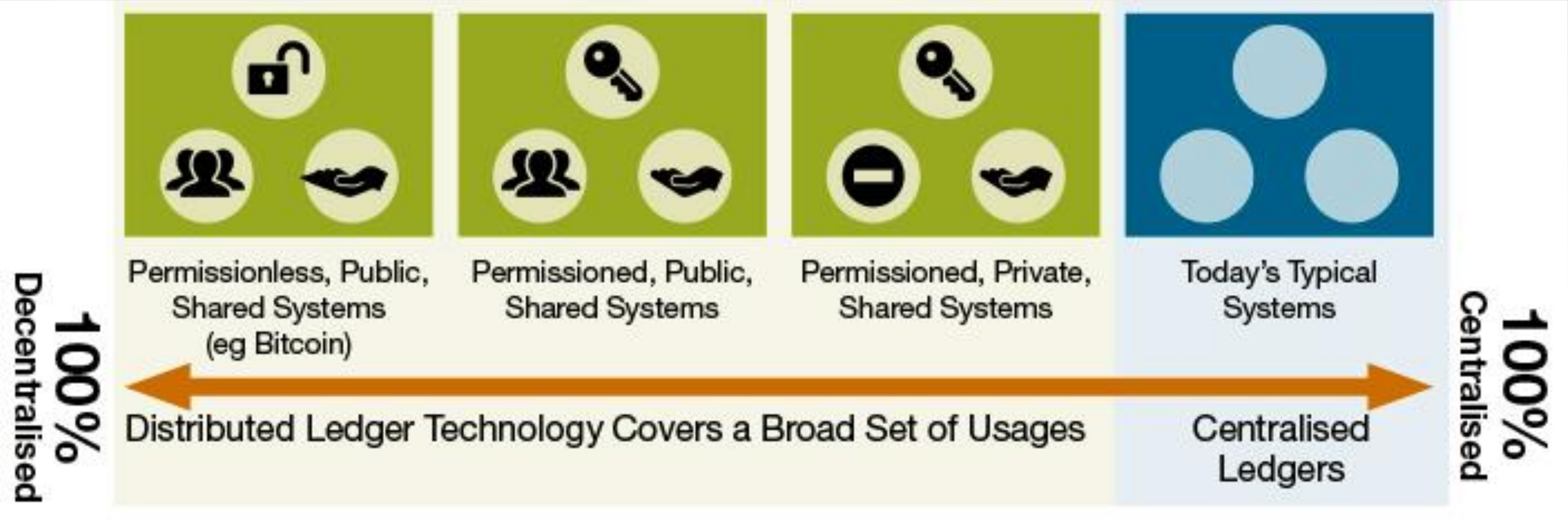
Reduces Risk

Tampering, fraud & cyber crime

Enables New Business Models

IoT Integration into supply chain

Degree of Centralisation


100% Decentralised
Permissionless, Public, Shared Systems (eg Bitcoin)
Permissioned, Public, Shared Systems
Permissioned, Private, Shared Systems
Today's Typical Systems
Distributed Ledger Technology Covers a Broad Set of Usages
Centralised Ledgers
100% Centralised

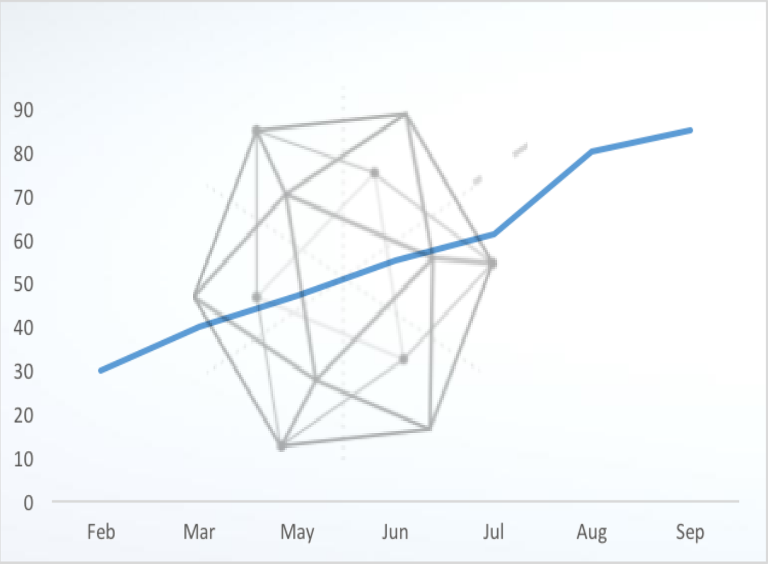
Censorship-resistant	**Privacy**
Scale to large number of nodes	**Scale in transaction throughput**
One global blockchain	**Many interacting blockchains**

Figure source: “Distributed Ledger Technology: Beyond Blockchain”, A report by UK Govt Chief Scientific Adviser

The Linux Foundation Hyperledger Project

A collaborative effort created to advance blockchain technology by identifying and addressing important features for a cross-industry open standard for distributed ledgers that can transform the way business transactions are conducted globally.

www.hyperledger.org



108+ Members, 260% Growth in 11 months

Premier

accenture High performance. Delivered.
AIRBUS
CME Group
Deutsche Börse Group
Digital Asset
DTCC
FUJITSU
HITACHI Inspire the Next
IBM
intel
J.P.Morgan
R3
万达·飞凡科技

Associate

Chamber of Digital Commerce
CSA cloud security alliance
Investrata Foundation
NXT Foundation
sovrin
INUIT

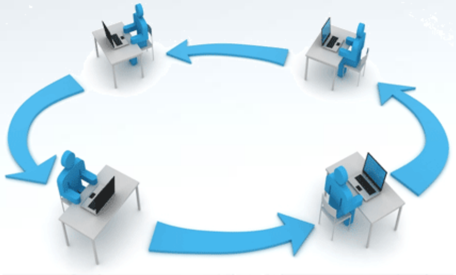
General

ABN·AMRO
Aesthetic Integration
Altoros
ANZ
博图纵横 BOTUZONGHENG
JM
MonetaGo
ML
Moscow Exchange
Murphy & McGonigle A Professional Corporation
NSE
Orchestrating a brighter world NEC
belink
bitSE
BLOCKCHAIN
blocko
Blockstream
bloq
NETKI
NOKIA
norbloc
NTT Data Global IT Innovator
onchain
橙色魔方 Orange Magic Cube
BNP PARIBAS
BNY MELLON
Broadridge
bubi.cn 布比
ca technologies
Calastone
PAXOS
PDX
redhat
Ribbit.me
SAMSUNG SAMSUNG SDS
SANY
CISCO
cloudsoft
CLS Fundamental to FX
coinplug
colu.
ConsenSys
SBERBANK
GINGKOO 金丘股份 (837901)
NEXGO
点融网 Dianrong.com
Skry
CREDITS
Cuscal The complete payments partner
Energy Blockchain Labs
Eurostep Digital
FACTOM
Gem
SORAMITSU
STATE STREET
SWIFT
swisscom
symbiont
TAI
众享比特 PeerSafe
guardtime
33.CN 复杂美
HASHED HEALTH
HUAWEI
HUNDSUN
tequa creek
THOMSON REUTERS
TMX
UMP
vmware
WELLS FARGO
趣链科技 Hyperchain
intellect
intuit
INVeSHARE
IROOTECH
KSD Korea Securities Depository
云象 YUNPHANT
梧桐树 wutongtree.com
保全网 BaoQuan.com
中国印钞造币
Financial IT Partner koscom
LedgerDomain
Libra
Lykke
Milligan Partners
MIRACL

International Trade & Supply Chain: Use Cases and Client Examples

Workflow Automation & Compliance

Automate current inefficient, manual and error-prone workflows in documentary trade finance

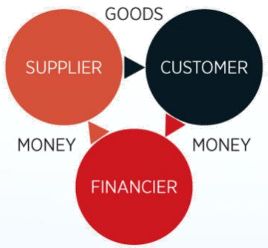


Supply-Chain Visibility

Provide single view for purchase order life-cycle across the supply-chain as the *truth*

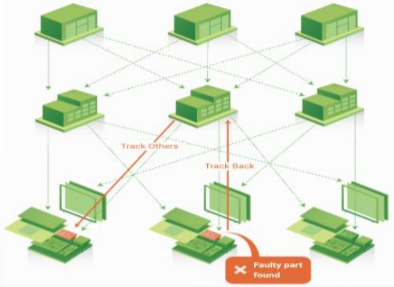
Trade/Supply-Chain Finance

Improve the efficiency of commercial financing business by sharing data in a secure and transparent manner



Supply-Chain Provenance

Provide provenance across the supply-chain cutting through complex distribution and processing ecosystems



MAERSK

Trade Logistics

Mahindra Rise.

Invoice discounting

Trade finance

Walmart

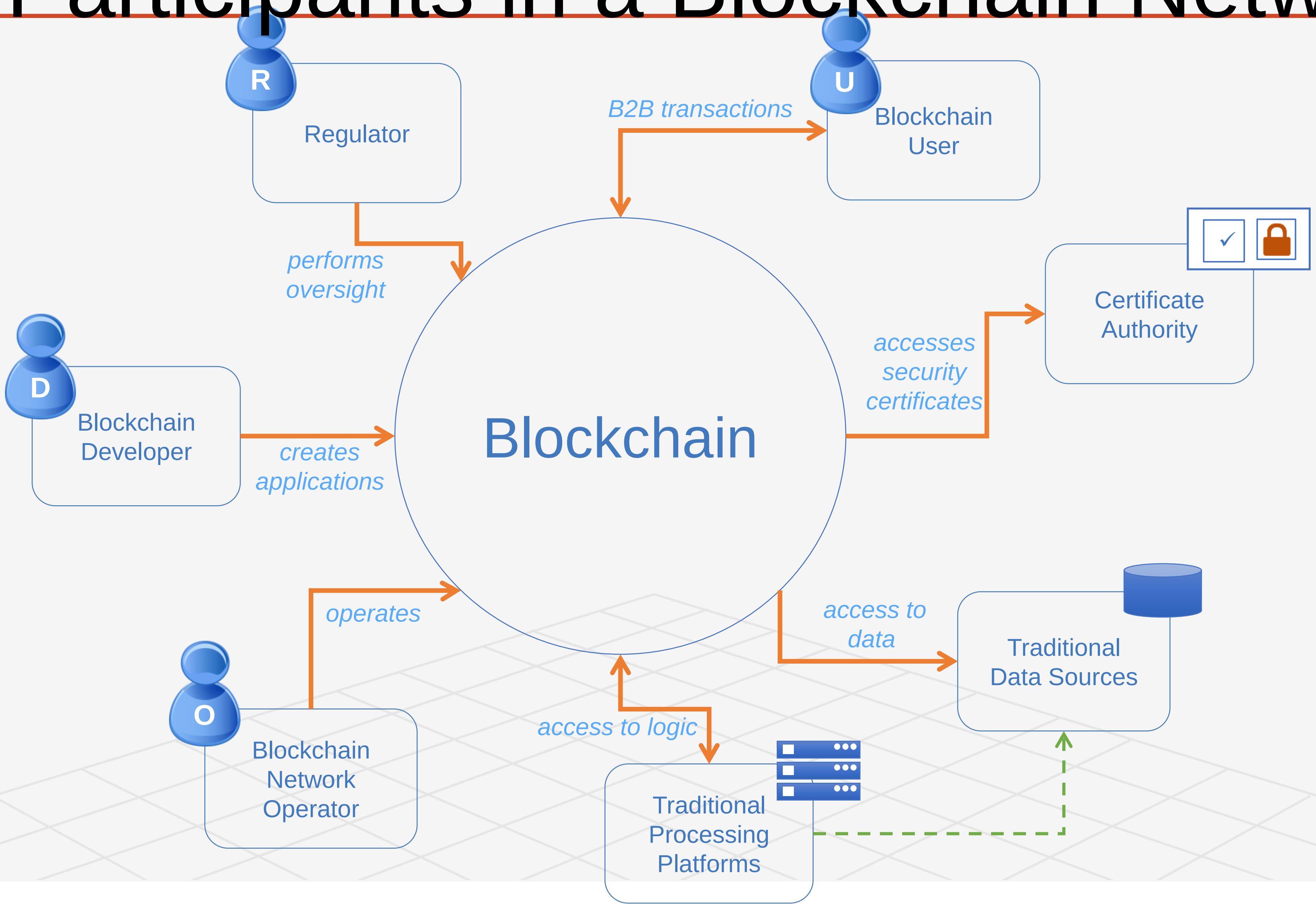
Food Safety

IBM

IBM Global Financing

Channel Financing

The Participants in a Blockchain Network

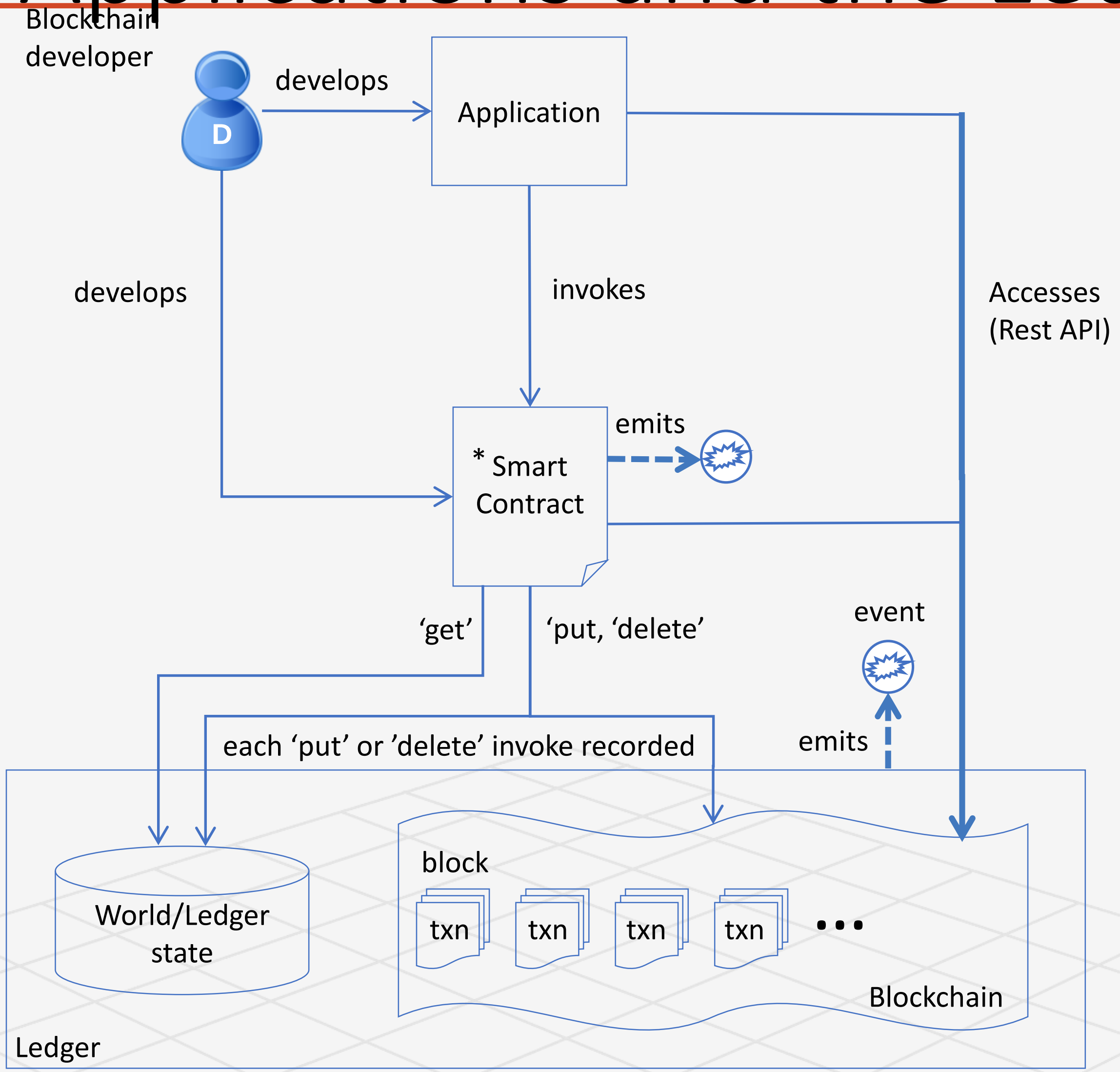


Blockchain Components

Blockchain

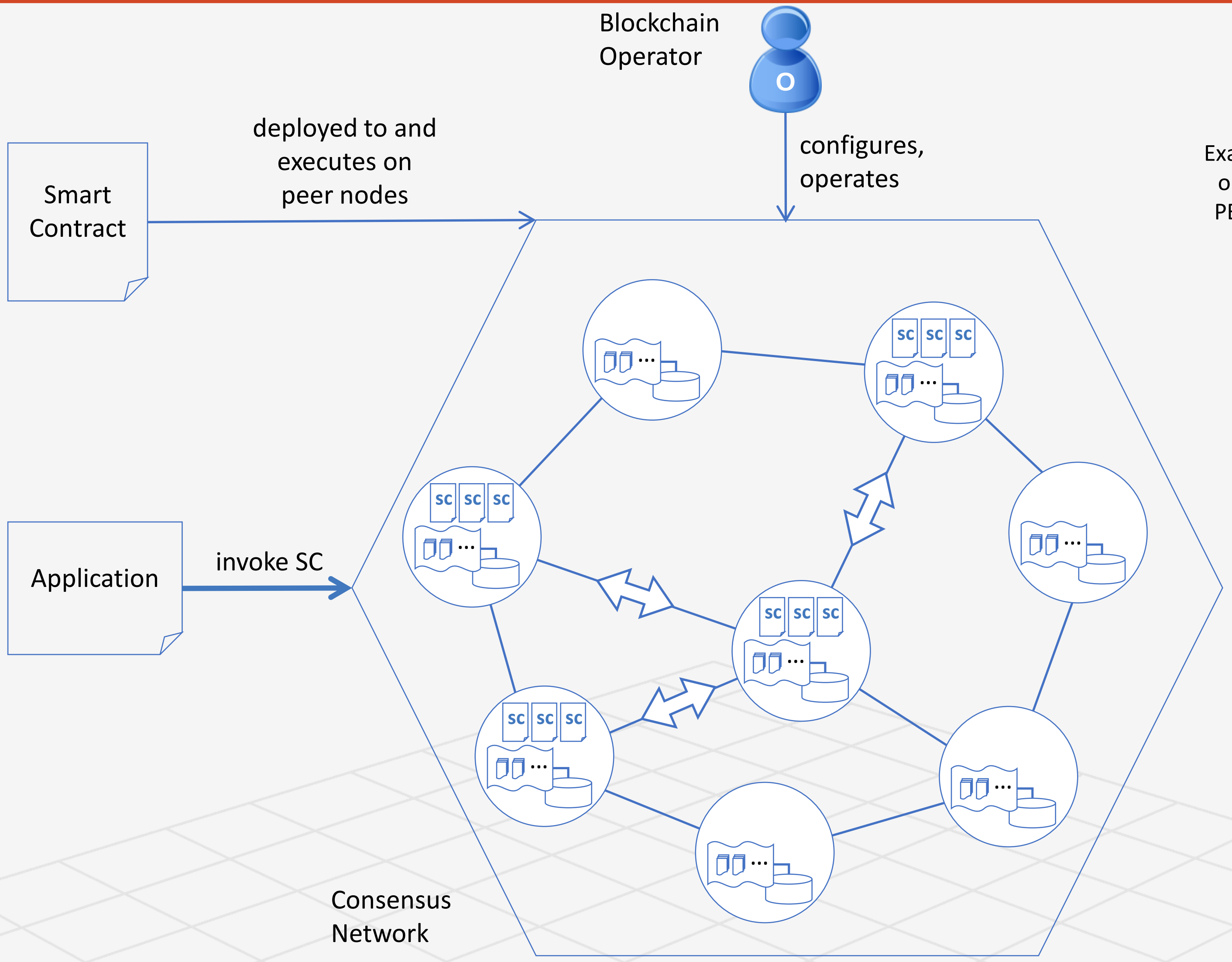
Ledger	...	contains the current world state of the ledger and a Blockchain of transaction invocations
Smart Contract	f(abc);	encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state
Consensus Network		a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger
Membership	E T	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	i	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 Applications and the Ledger



* Smart Contract implemented using chain code

Consensus and the Blockchain Network



Blockchain Operator

configures, operates

Smart Contract

deployed to and executes on peer nodes

Application

invoke SC

Consensus Network

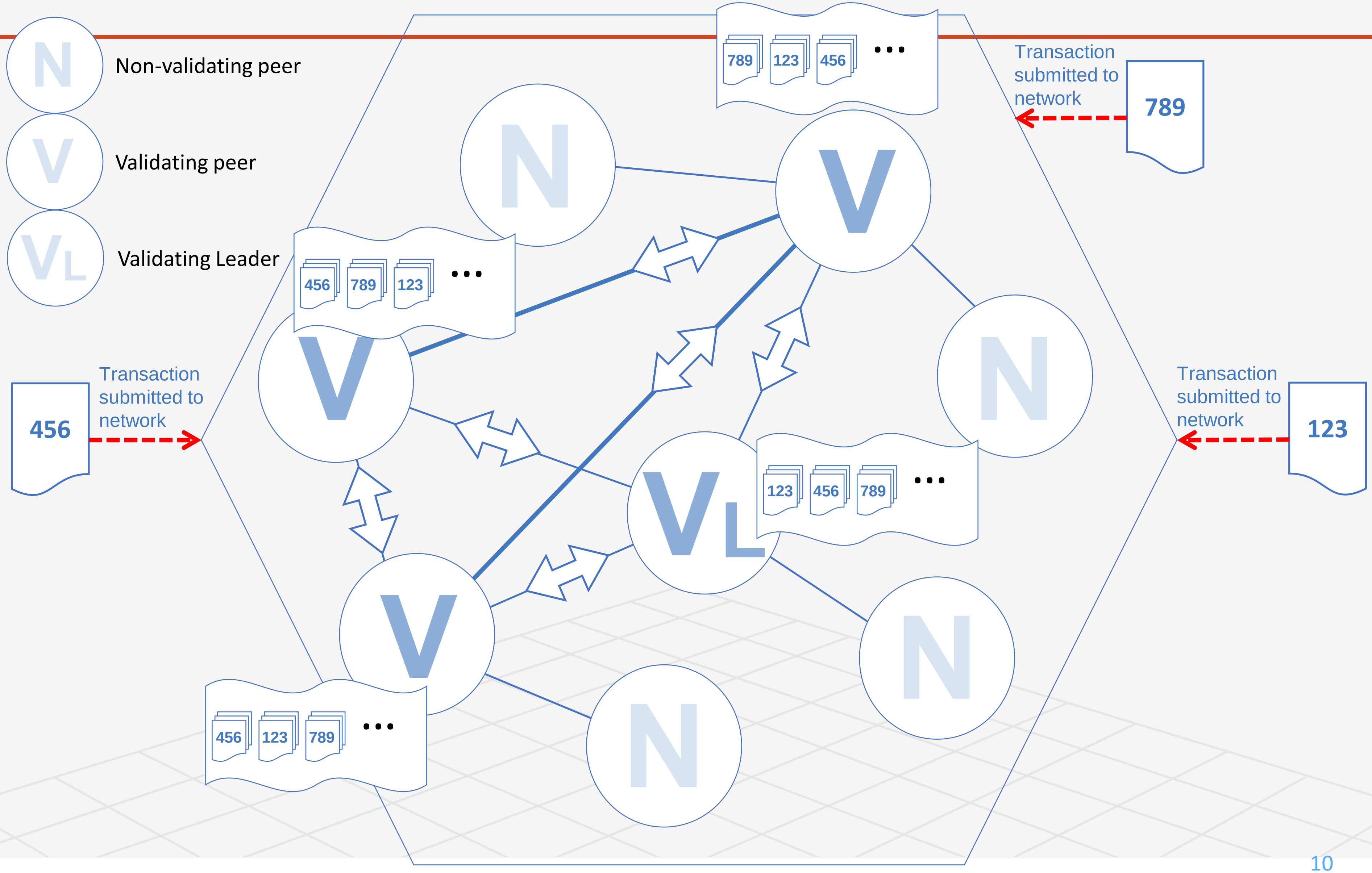
peer

Exact network structure depends on consensus mechanism. e.g. PBFT has leader, validating and non-validating peers

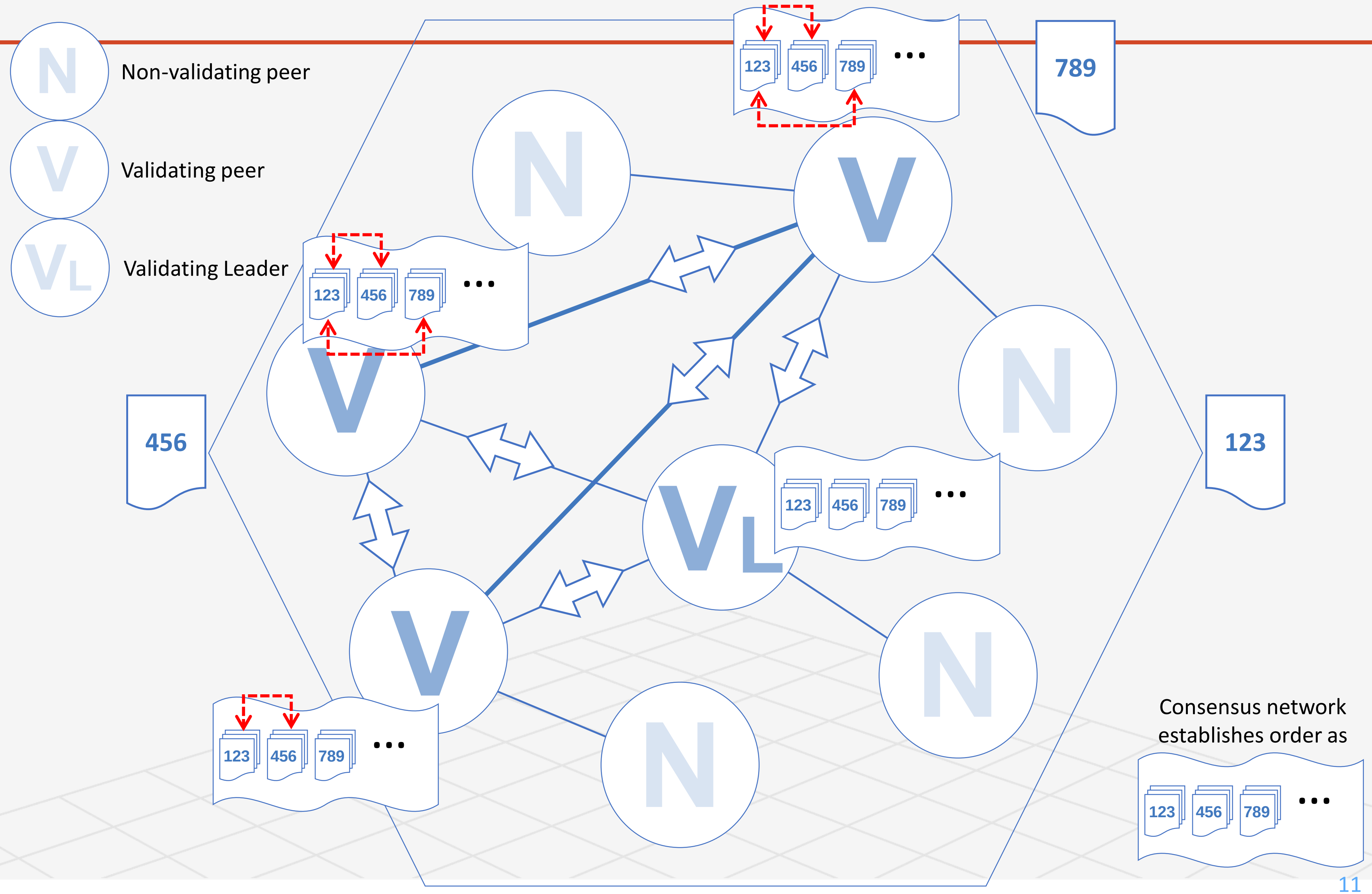
consensus msg

consensus messages flow between appropriate peers to ensure the Blockchain SC transactions are kept in order; world state is kept consistent through local transaction replay

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

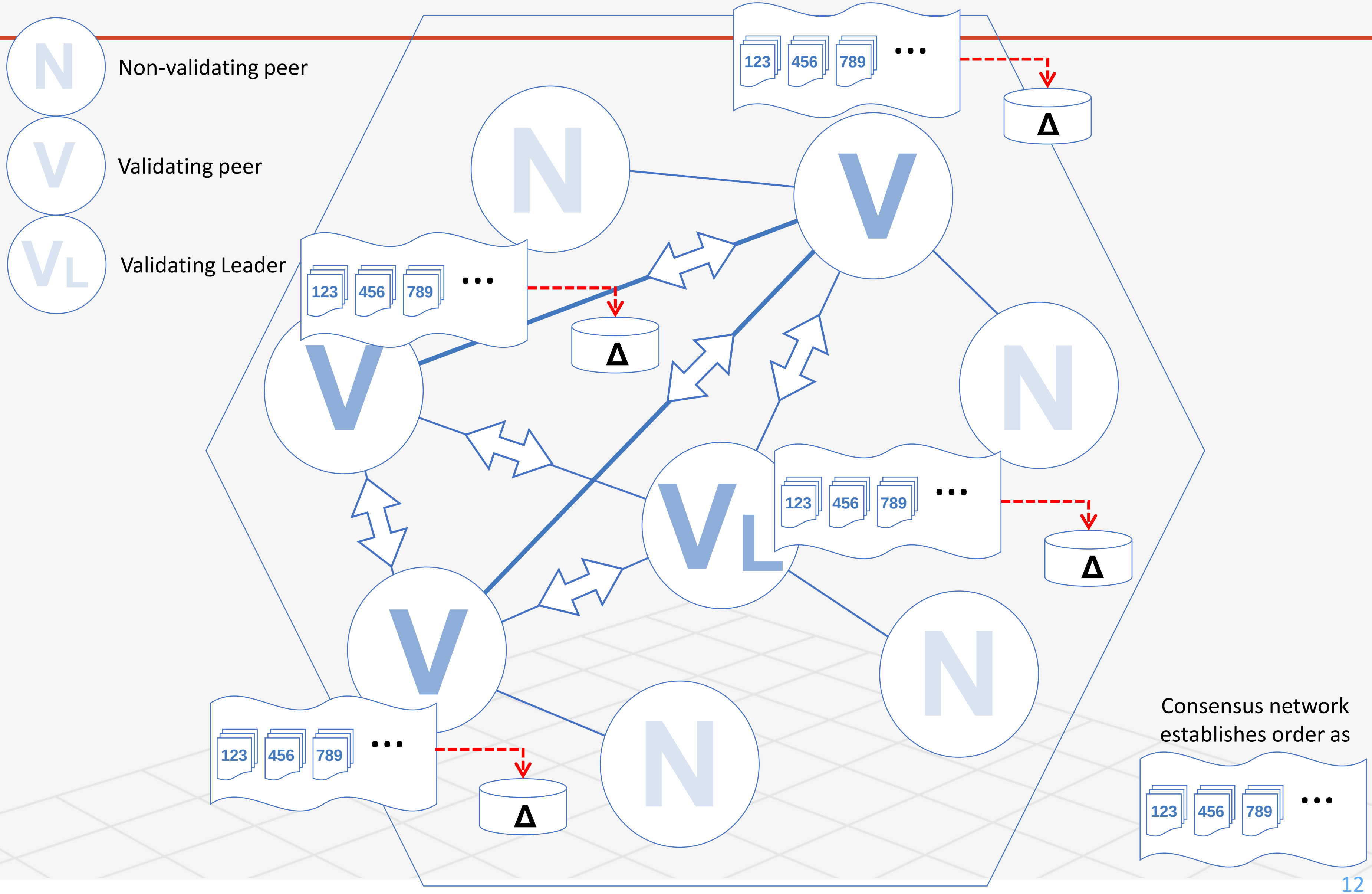


How a PBFT Network Works (2/4) – Ordering



Consensus network establishes order as

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



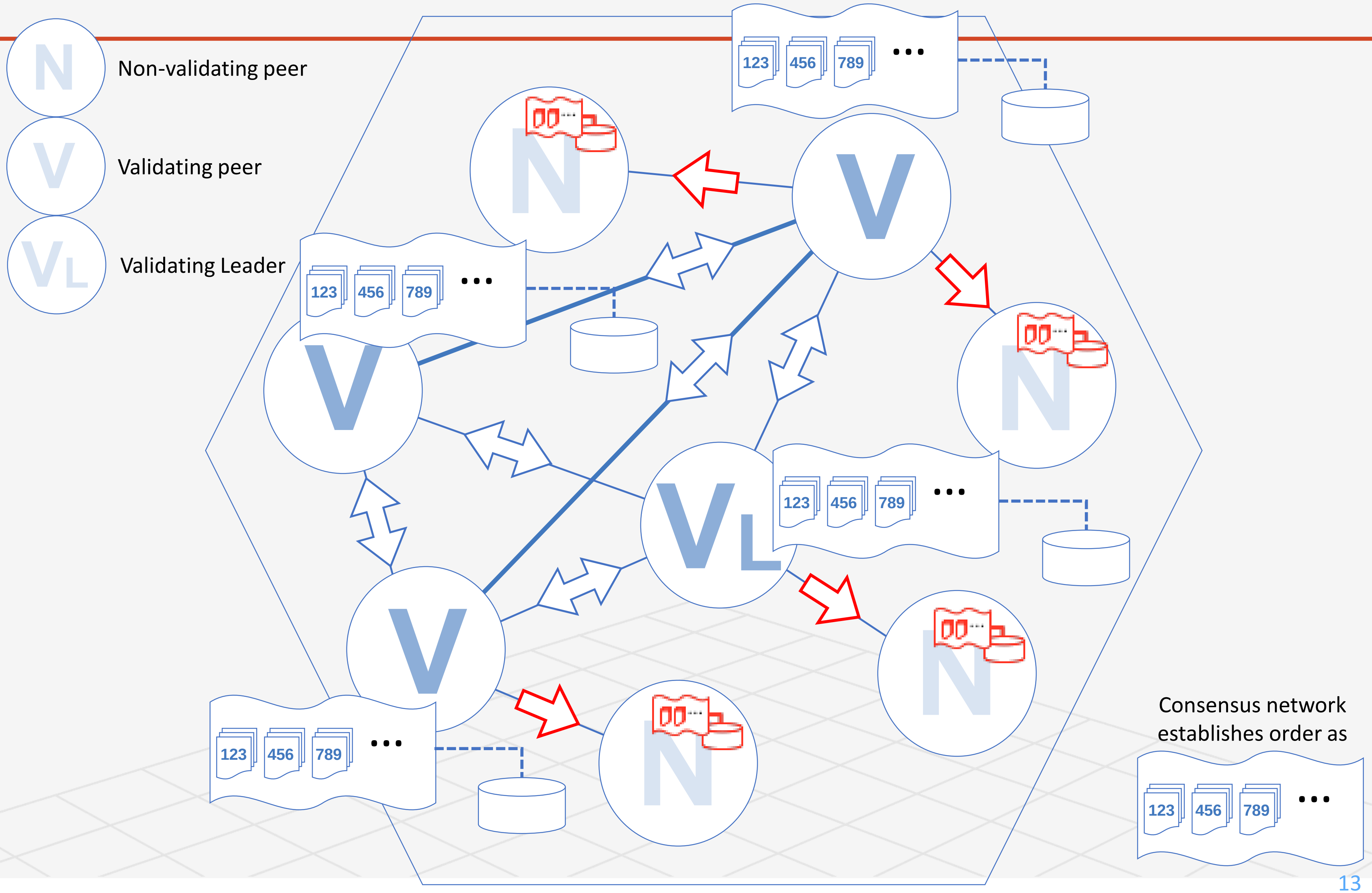
Non-validating peer

Validating peer

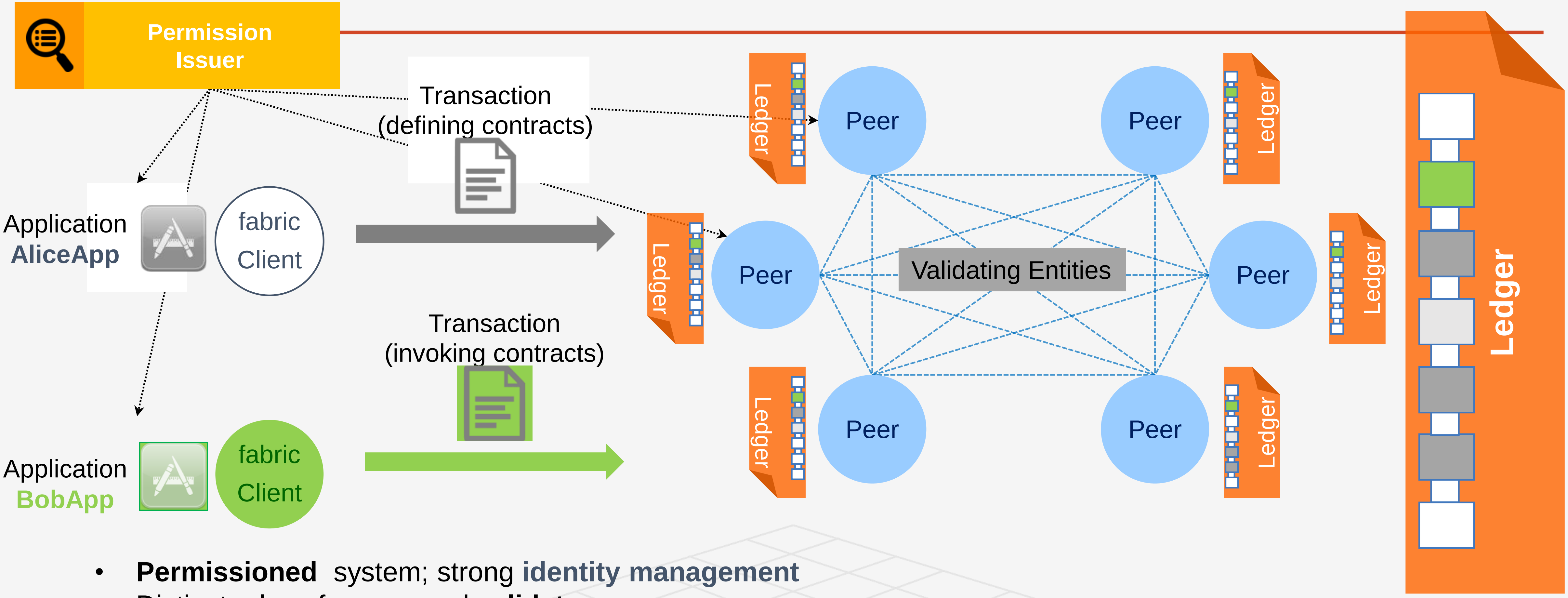
Validating Leader

Consensus network establishes order as

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



Hyperledger Fabric Model



- **Permissioned** system; strong **identity management**
- Distinct roles of **users**, and **validators**
- Users **deploy** new pieces of code (chaincodes) and **invoke** them through **deploy** & **invoke** transactions
- Validators evaluate the effect of a transaction and reach consensus over the new version of the **ledger**
- **Ledger** = total order of transactions + hash (global state)
- **Pluggable consensus** protocol, currently PBFT & Sieve

Security & privacy features

Privacy of user-participation

Each user has control over the degree to which its transaction activity will be shared with its environment

Contract Privacy

Contract logic can be confidential, i.e., concealable to unauthorized entities

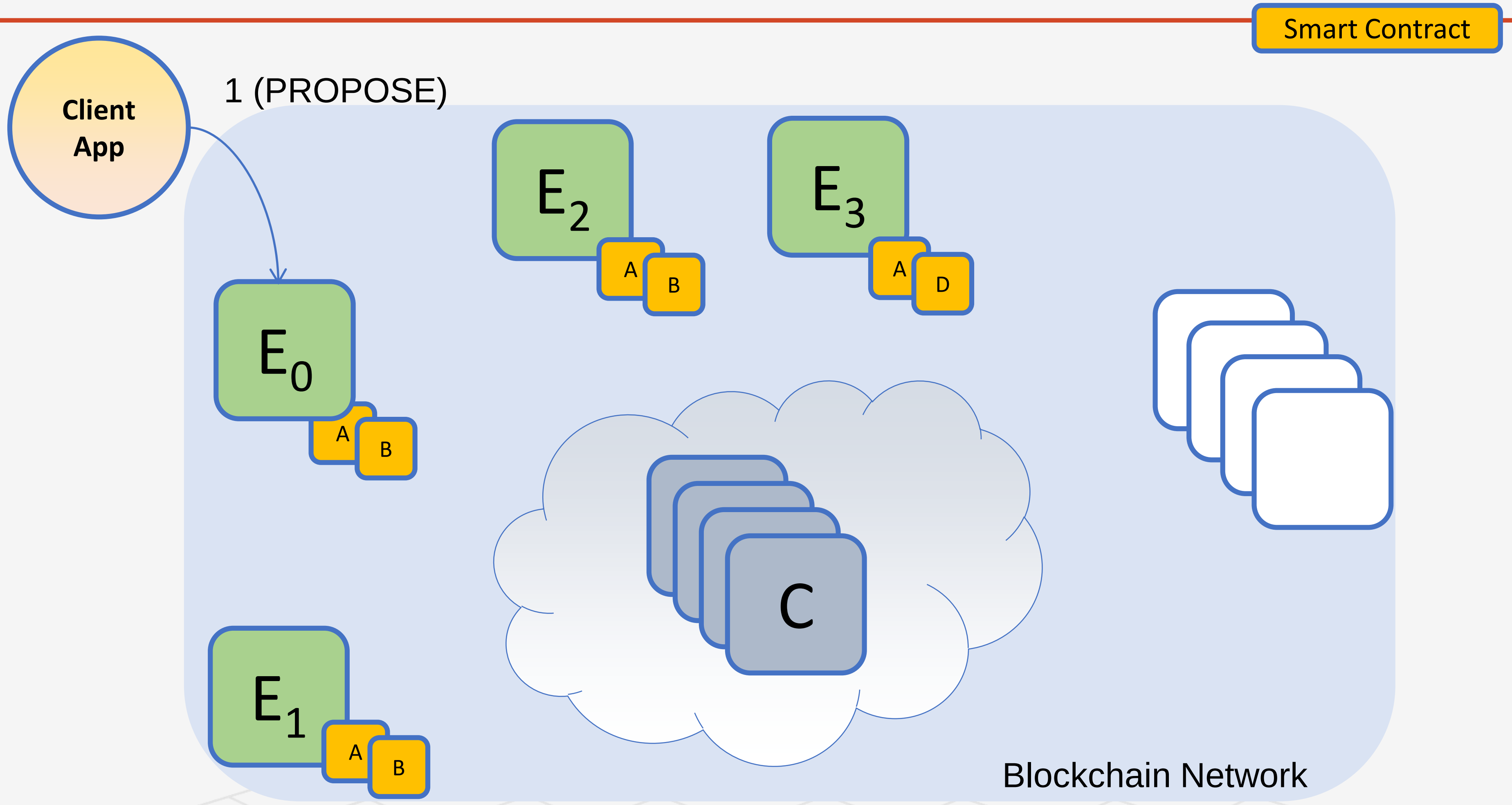
Accountability Non-repudiation

Users can be accounted for the transactions they create, cannot frame other users for their transactions, or forge other users’ transactions.

Auditability

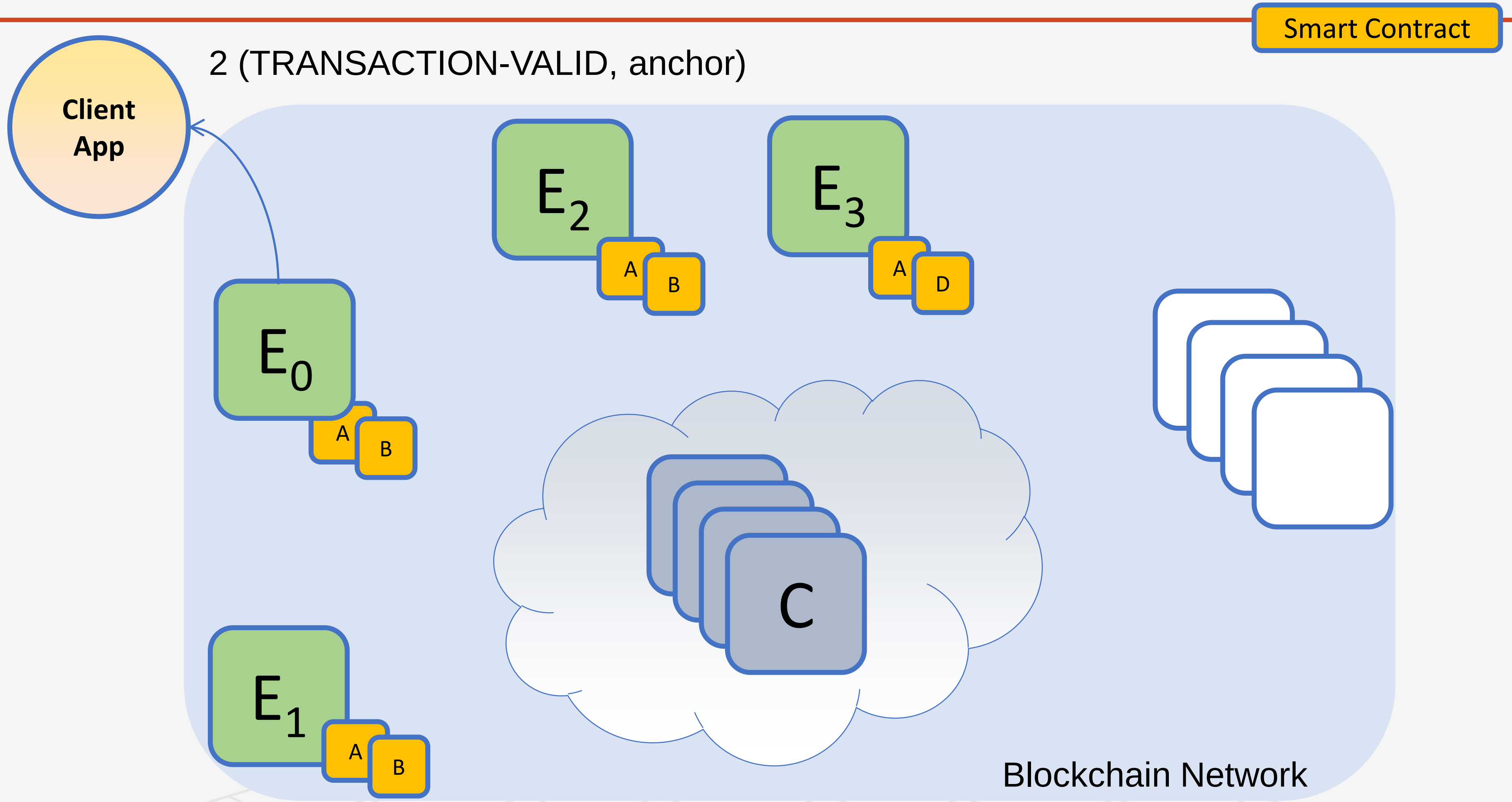
Auditors are able to access & verify any transaction they are legally authorized to

A sample transaction (1/6)



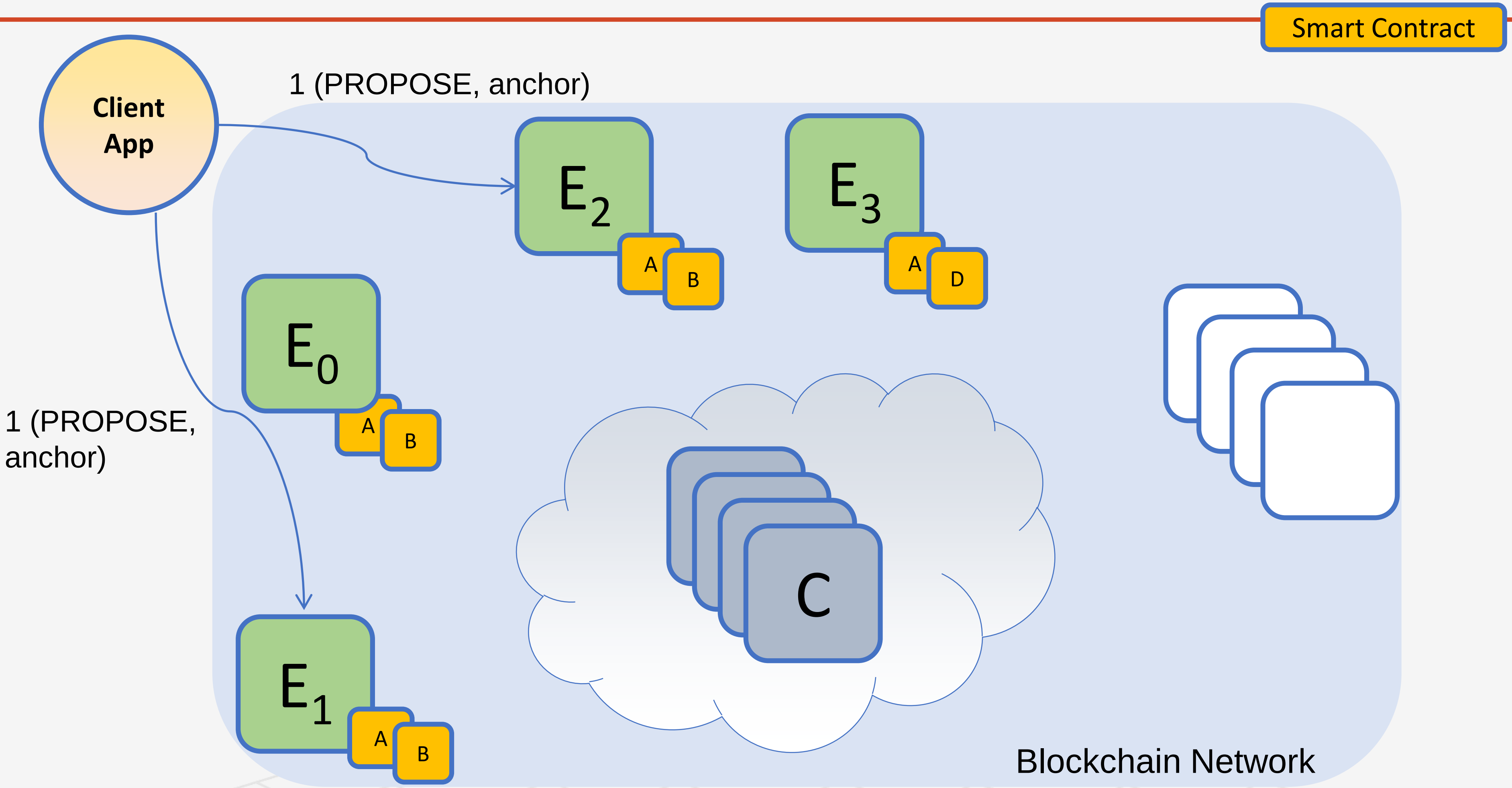
1. The Client App proposes a transaction for **Smart Contract A** to the Endorsing peer E_0. Endorsement policy: “$E_{0,}$ E_1 and E_2 must sign”. E_3 is not part of the policy

A sample transaction (2/6)



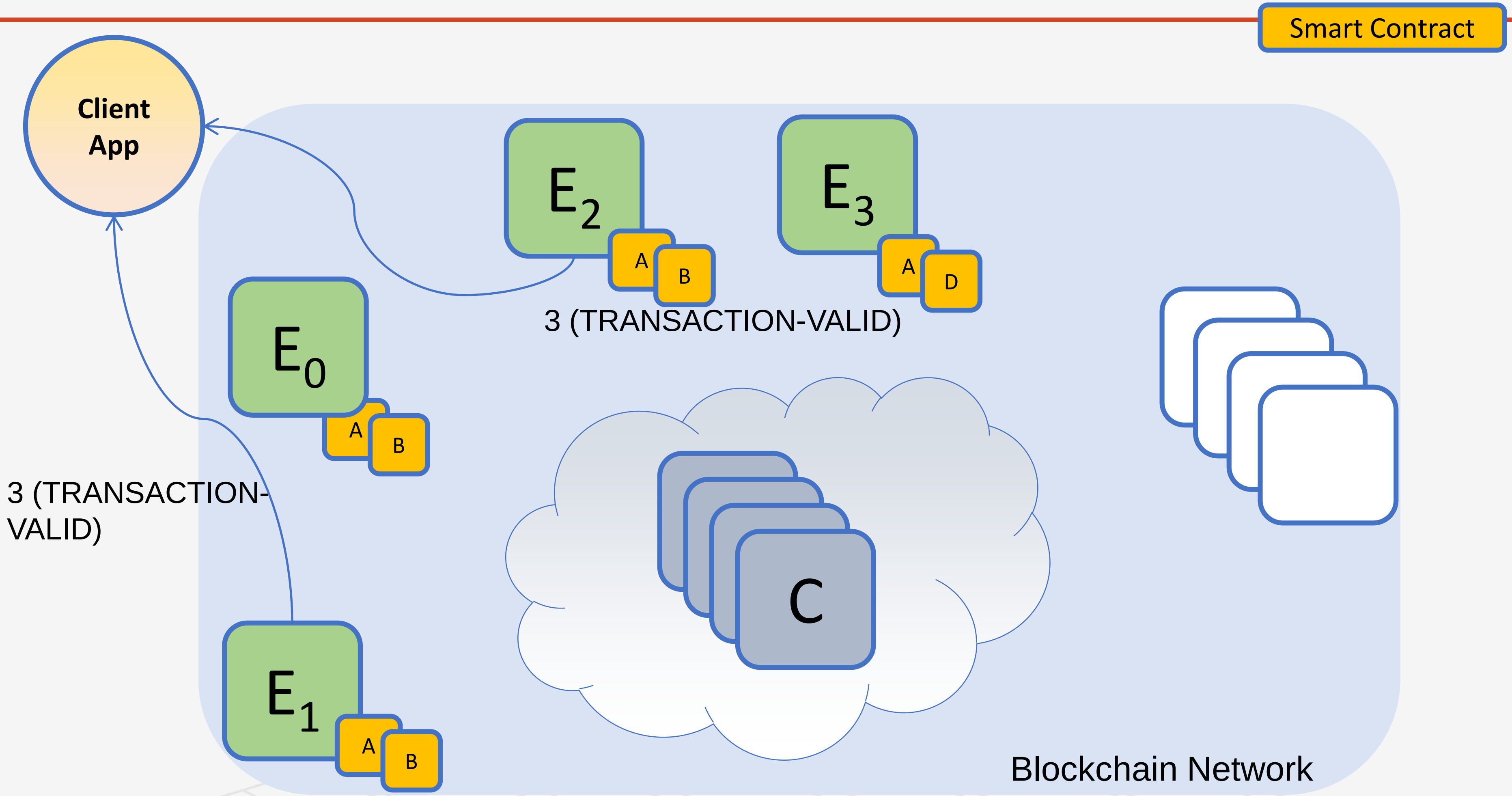
2. Endorsing peer E_0 endorses a tx and (optionally) “anchors it” with respect to the ledger state version numbers. An “anchor” contains all data read and written by contract that are to be confirmed by other endorsers.

A sample transaction (3/6)



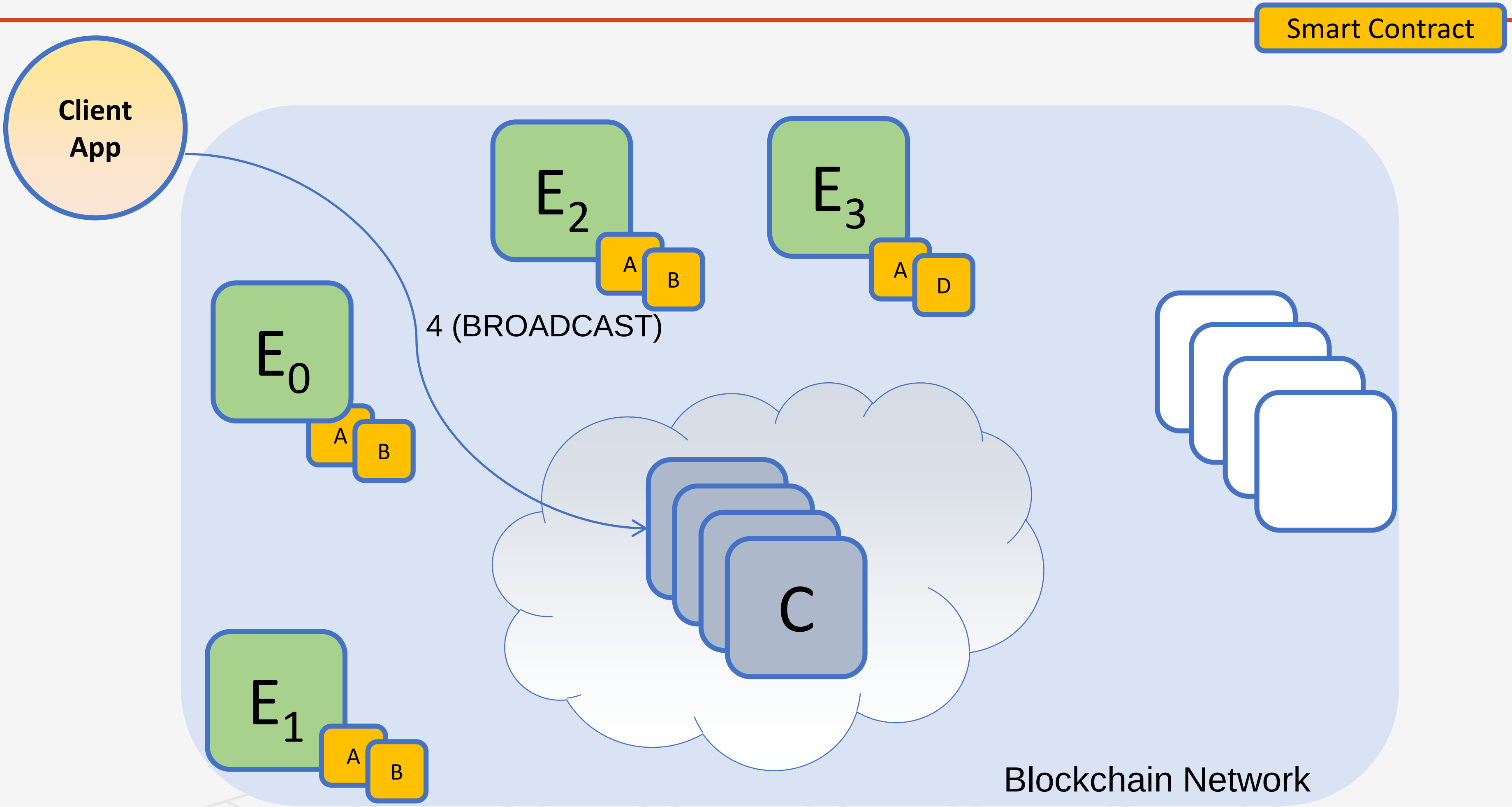
3. The client requests further endorsement from E_1 and E_2.The client may decide to suggest an anchor obtained from $E_{0.}$ to E_1 and $E_{2.}$

A sample transaction (4/6)



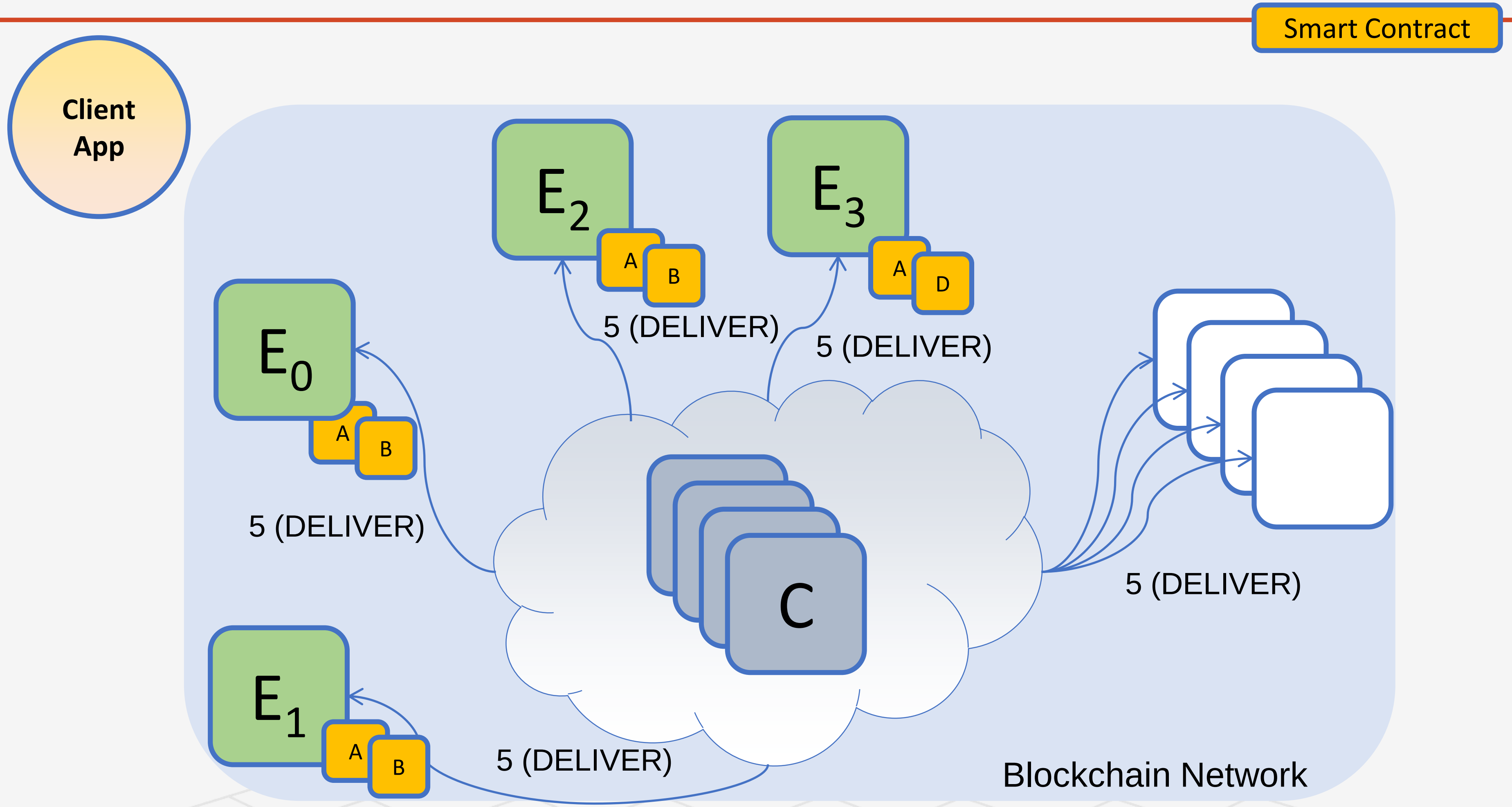
4. The Endorsing peers E$_1$ and E$_2$ send the endorsement to client.

A sample transaction (5/6)



5. Client formats the transaction and broadcasts it to the consenters for inclusion in the ledger

A sample transaction (6/6)



6. The consensus service delivers the next block in the ledger with the consented transaction.