6 AUGUST 2022

BLOCKCHAIN OVERVIEW AND IMPLEMENTATION

BLOCKCHAIN OVERVIEW

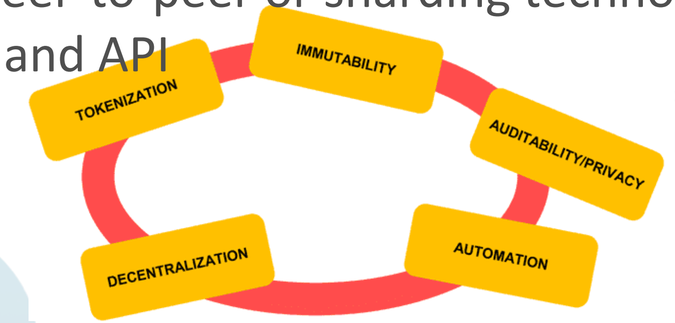
Blockchain – Agenda

- Blockchain Overview
  - What is Blockchain?
  - What does Blockchain bring?
  - Blockchain Value additions and enablers
  - Different types of Blockchain
  - How do you choose the Blockchain type?
  - How does Blockchain work?
  - Building blocks of Blockchain
  - Architectural layers of Blockchain
  - Evolution of Blockchain
  - How do you choose Blockchain platform?
  - Factors changing estimation values
  - Skills needed to develop Blockchain application
  - What do developers develop?
  - Gartner Hype
  - Blockchain future
  - Blockchain use cases heatmap
  - Simple use case
- Blockchain Implementation
  - Phases for South African Supplier Chain Network
  - Why Hyperledger Fabric?
  - Hyperledger Fabric Benefits
  - Hyperledger Various Views
  - Sample Transaction Flow
  - Phase 1
    - Identity Management and KYC
    - Identity Management Blockchain Interface
    - Identity Management Sequence Diagram
    - Identity Management - Zero Knowledge Proof (ZPK)
    - Identity Management Files Process Structure
    - Identity Management Application Layer Structure
    - dApp Chat System for Suppliers
    - Certification Standards
  - Phase 2
    - After login Business Flow for End Users
    - After login Use Case for the Business Workflow
    - Use Case for Developer End to End Workflow
    - Dashboard Screen after Login Success
    - On Clicking PIE Chart

BLOCKCHAIN OVERVIEW

Blockchain - What is it?

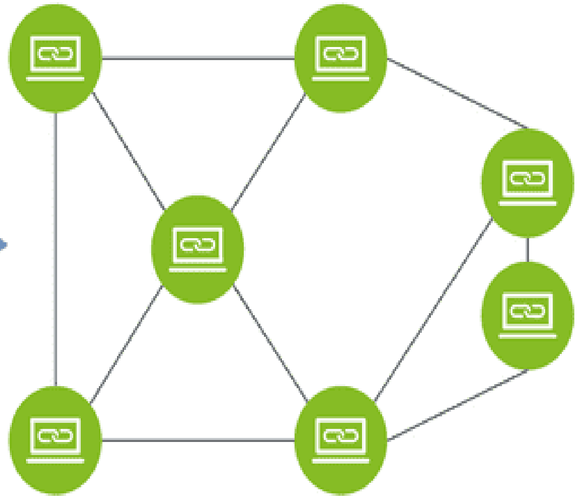
- Blockchain – What is it?
  - Aka DLT (Distributed Ledger Technology)
    - Rudimentary shared accounting system
  - Technologically, it is :
    - Distributed database – public ledger
      - you can insert, select data,
      - but can't update or delete data
    - Distributed computer – digital contracts
    - Based on peer-to-peer or sharding technology, cryptology and API



Typical System

Central authorities transfer actual value between two parties
Multiple intermediaries required to facilitate of assets and create trust

Blockchain System



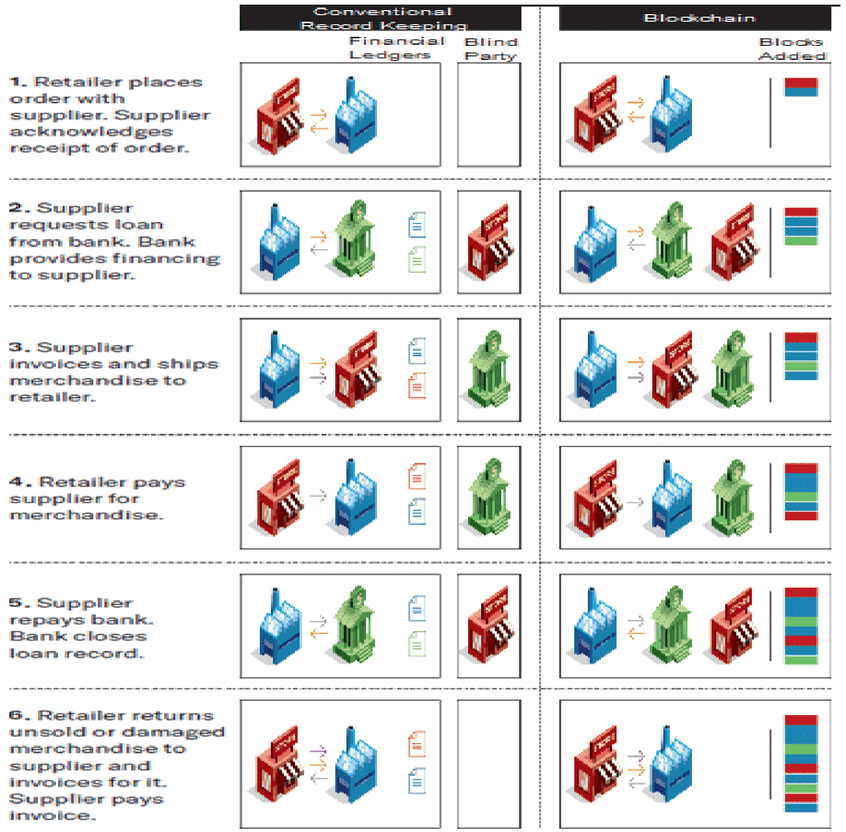
Distributed nodes that maintain a shared source of information
Trust enabled by cryptographic algorithm

BLOCKCHAIN OVERVIEW

Blockchain - What does Blockchain bring?

- Blockchain – What does Blockchain bring?

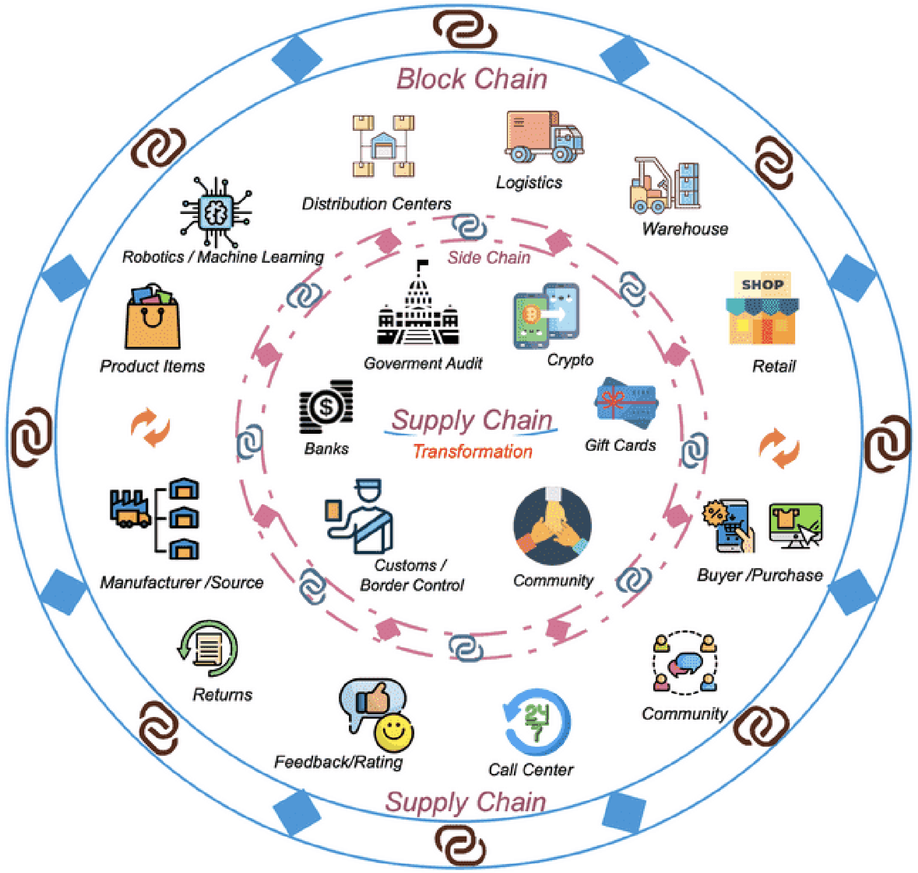
X	Trust & Transparency of data	Data integrity, immutability and auditability
X	Privacy & Security	Private permissioned blockchain
X	Administrative burden	Automation via 'smart contracts'
X	Tracking & fragmented data	Digital identities & bespoke integration
X	Time delays & tied up funds	Real-time reimbursement and settlement mechanisms
X	Many platforms and systems	One platform for all stakeholders



BLOCKCHAIN OVERVIEW

Blockchain – Value Additions and Enablers

- Blockchain – Value Additions and Enablers



BLOCKCHAIN OVERVIEW

Blockchain – Different Types

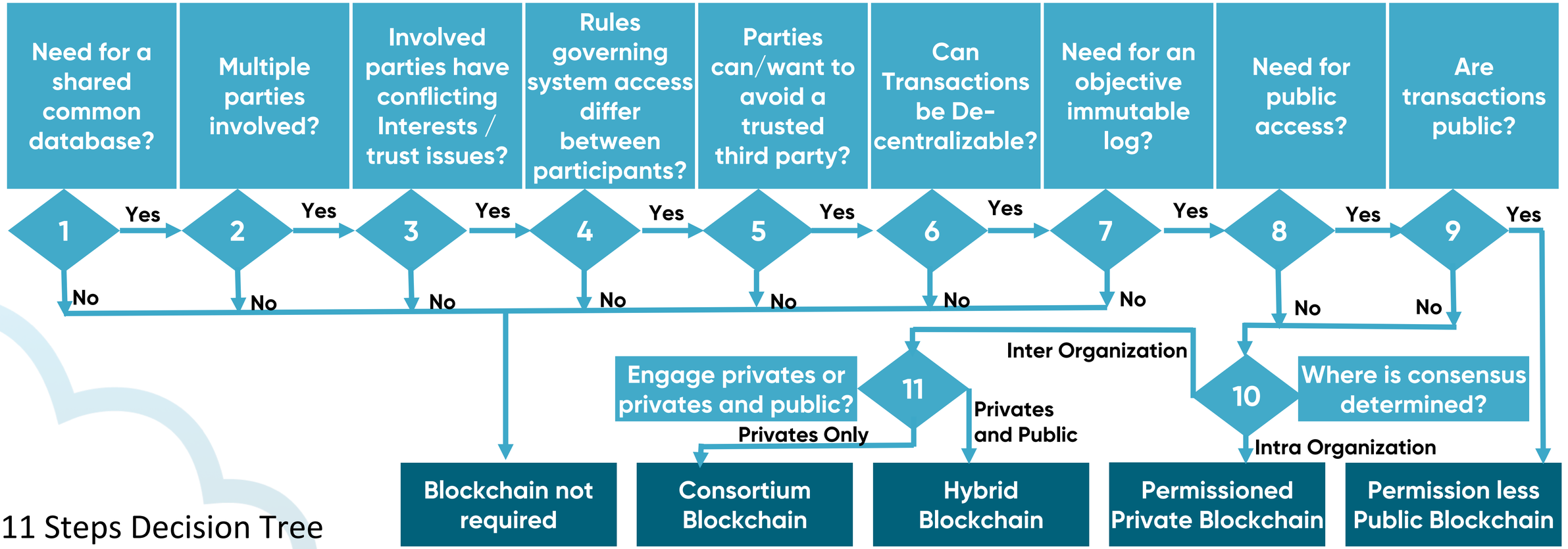
- Blockchain – Different Types

Types and Properties	Public (permissionless)	Private (permissioned)	Hybrid (combination)	Consortium (shared permissioned)
ADVANTAGES	+ Independence + Transparency + Trust	+ Access control + Performance	+ Access control + Performance + Scalability	+ Access control + Scalability + Security
DISADVANTAGES	- Performance - Scalability - Security	- Trust - Auditability	- Transparency - Upgrading	- Transparency
USE CASES	= Cryptocurrency = Document validation	= Supply chain = Asset ownership	= Medical records = Real estate	= Banking = Research = Supply chain

BLOCKCHAIN OVERVIEW

Blockchain – Choose a Type

- Blockchain – Choose a Type

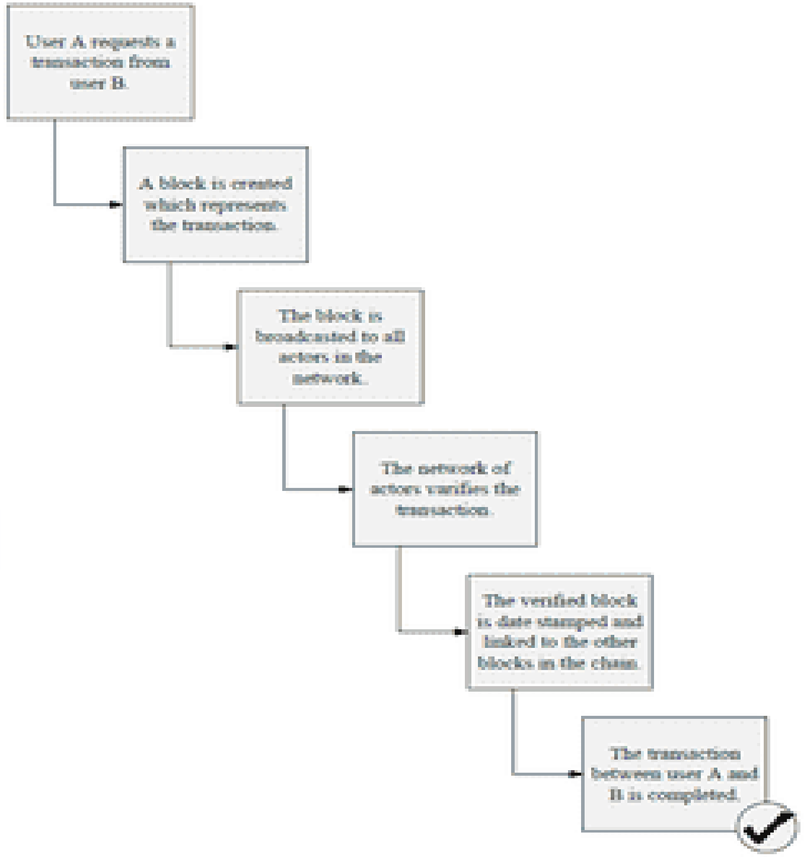


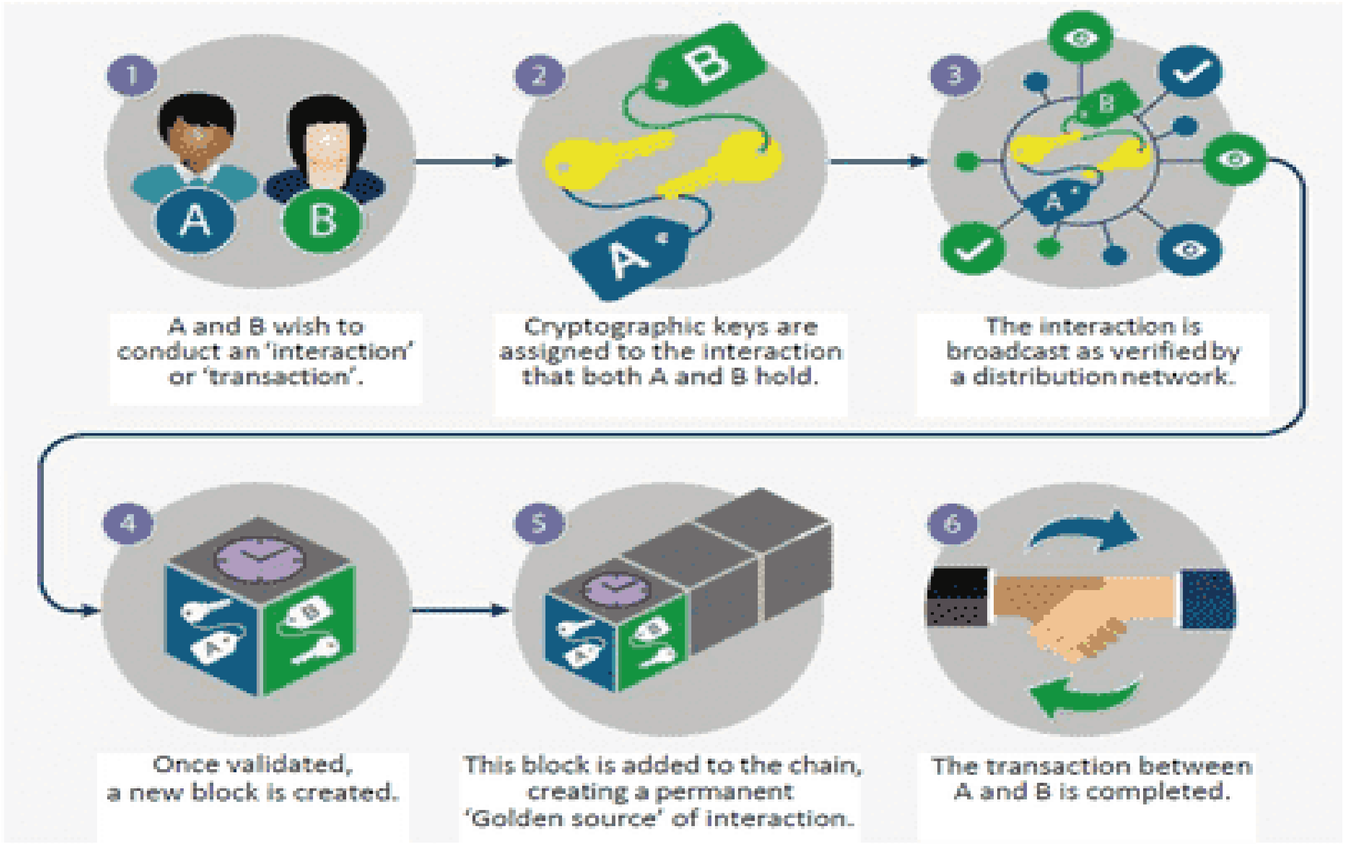
11 Steps Decision Tree

BLOCKCHAIN OVERVIEW

Blockchain – How does Blockchain work?

- Blockchain – How does Blockchain work?





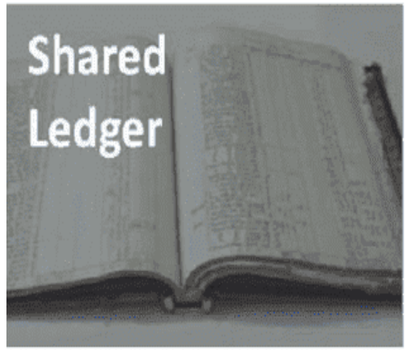
BLOCKCHAIN OVERVIEW

Blockchain – Building Blocks

- Blockchain – Building Blocks

Append-only distributed system of record shared across business network

- Shared between participants
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions



Business terms embedded in transaction database & executed with transactions

- Verifiable, signed
- Encoded in programming language
- Analogous to a stored procedure call on a database

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

- Cryptography central to these processes
- Access permission controlled via certification management

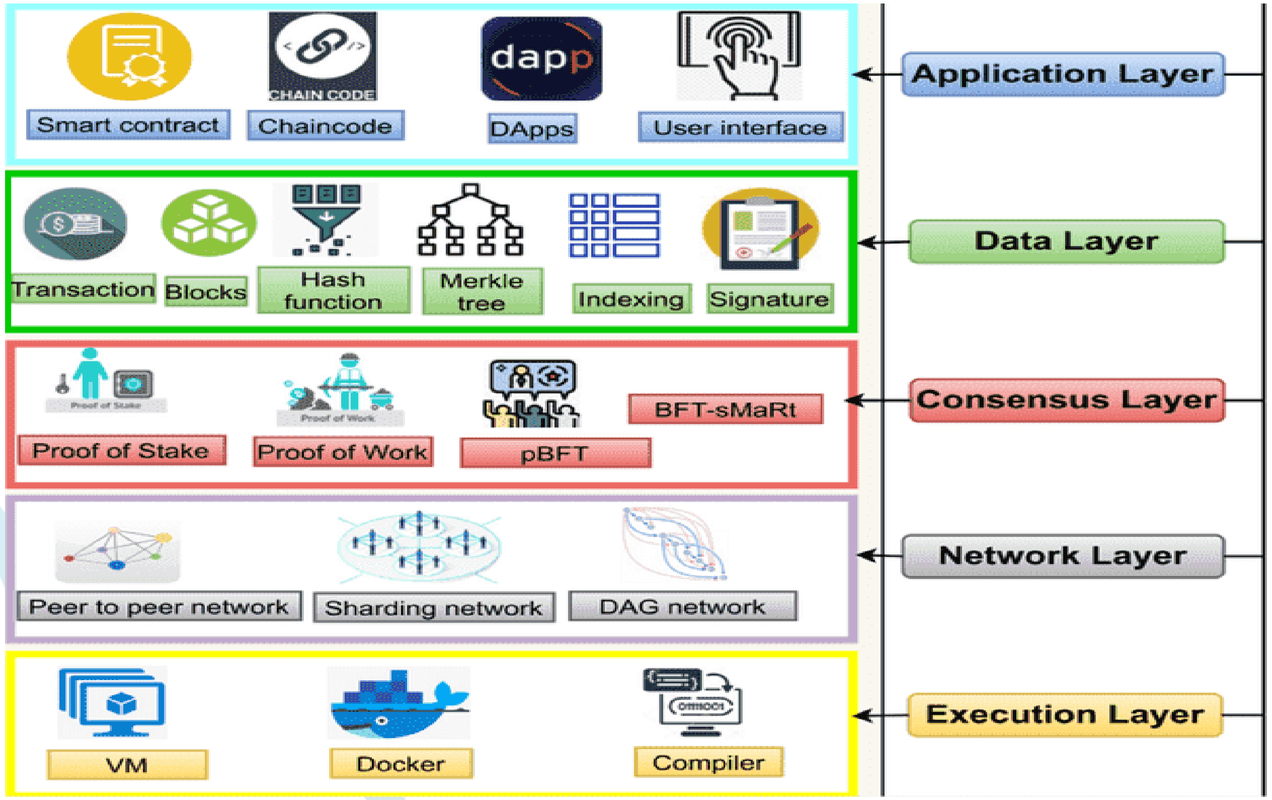
Transactions are endorsed by relevant participants

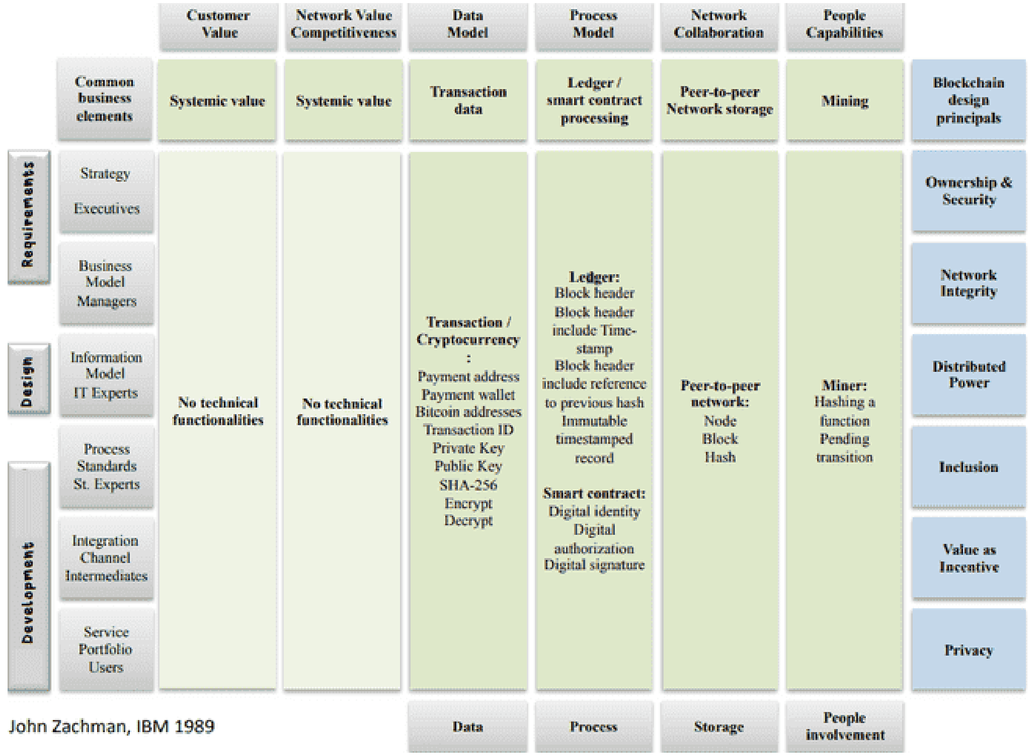
- Endorsed transactions are added to the ledger with appropriate confidentiality
- Assets have a verifiable audit trail
- Transactions cannot be modified, inserted or deleted

BLOCKCHAIN OVERVIEW

Blockchain – Architecture OSI View and Zachman View

- Blockchain – Architecture OSI View and Zachman View

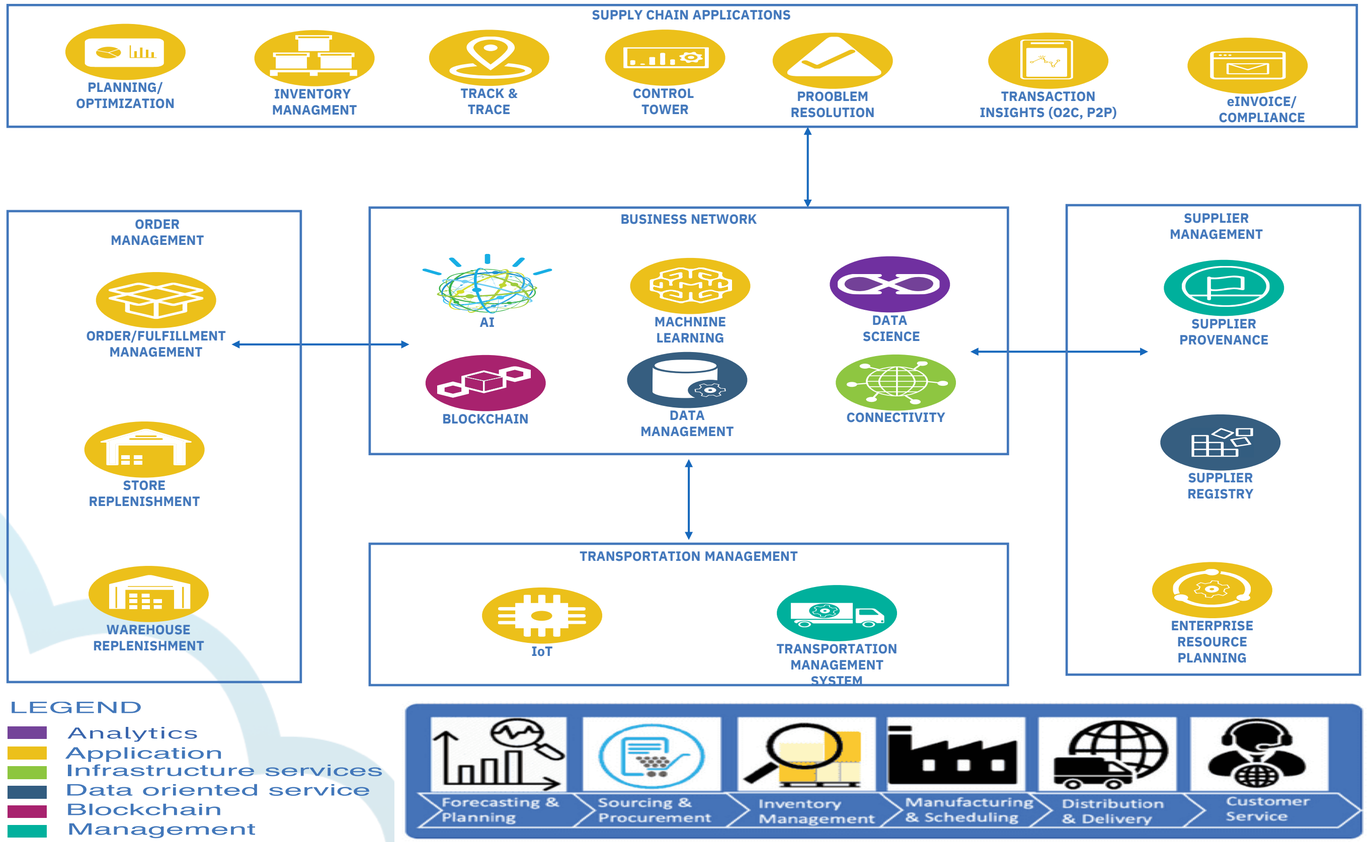


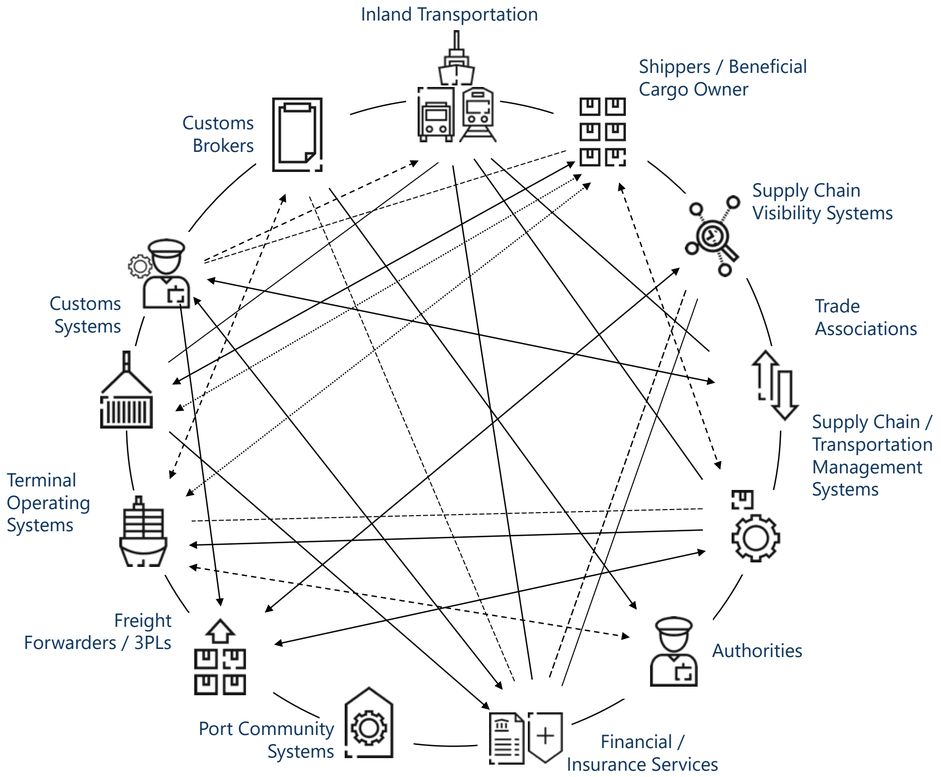


BLOCKCHAIN OVERVIEW

Blockchain – Business Architecture

- Blockchain – Business Architecture

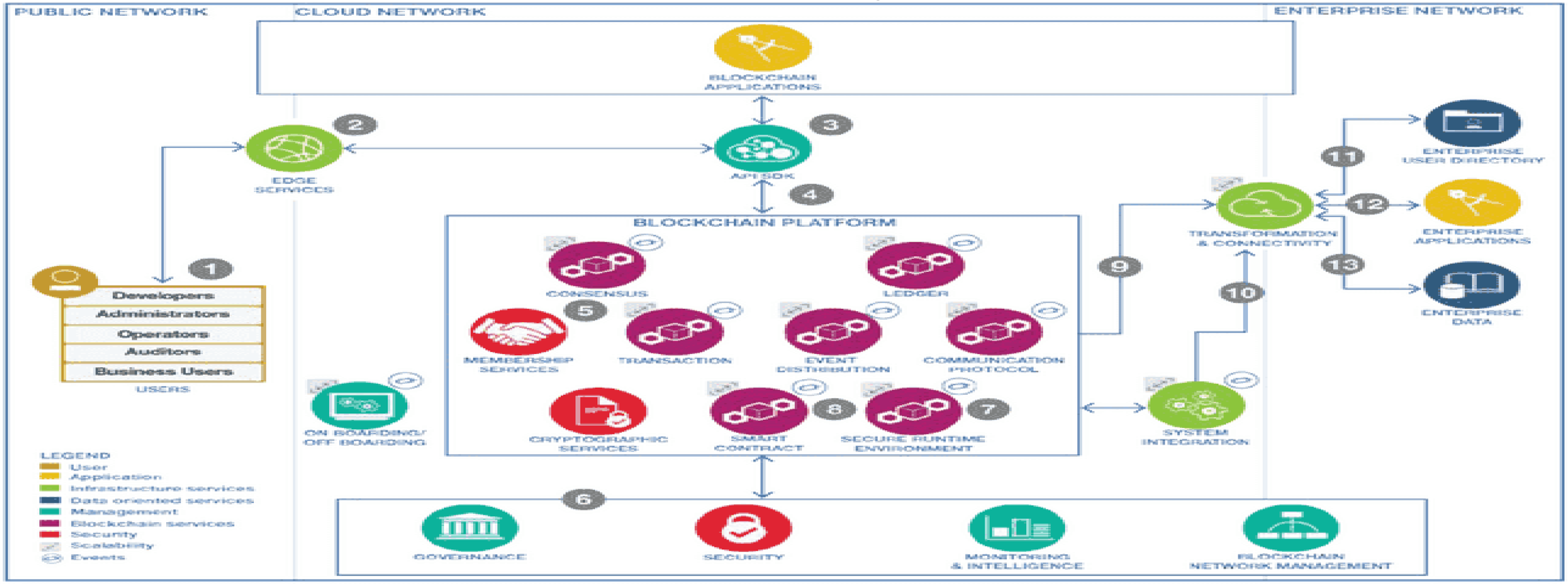




BLOCKCHAIN OVERVIEW

Blockchain – Workflow Architecture from Developers View

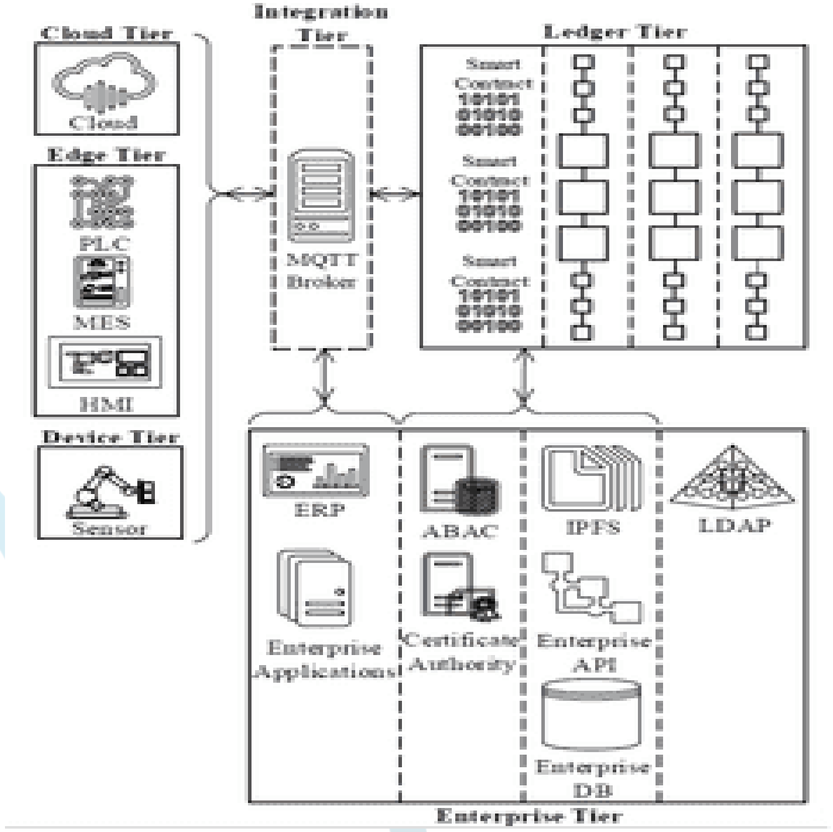
- Blockchain – Workflow Architecture from Developers View

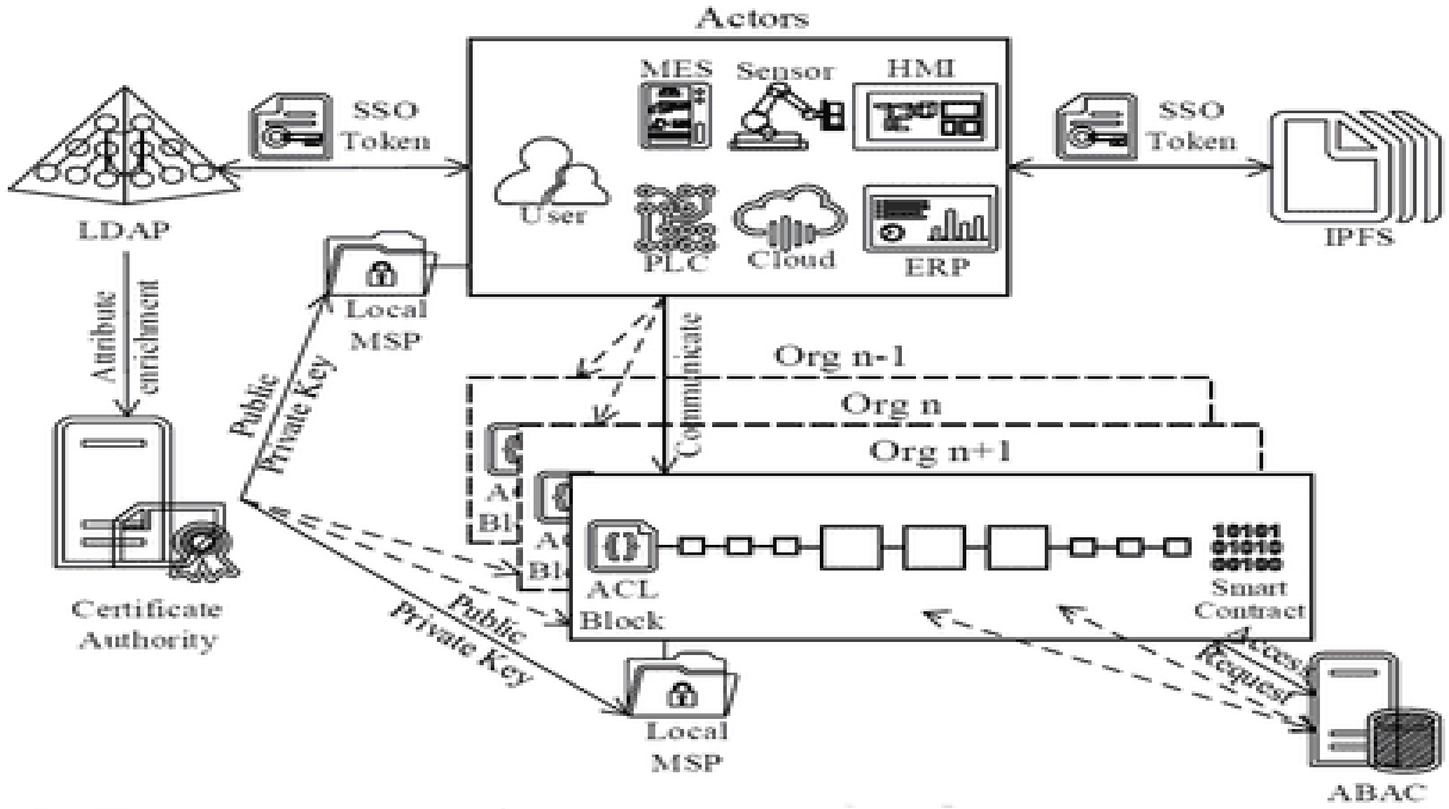


BLOCKCHAIN OVERVIEW

Blockchain – Technical Architecture from Components View

- Blockchain – Technical Architecture from Components View

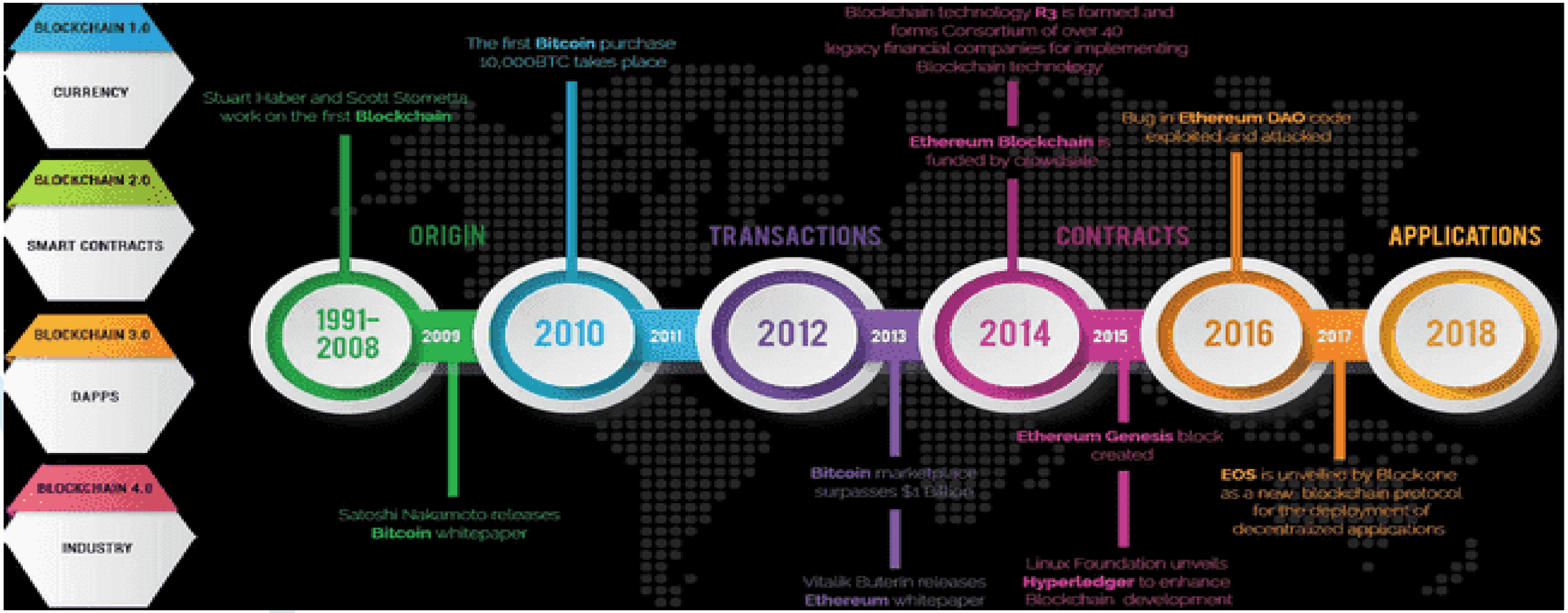




BLOCKCHAIN OVERVIEW

Blockchain – Evolution

- Blockchain – Evolution



BLOCKCHAIN OVERVIEW

Blockchain – Platforms Selection Checklist

- Blockchain – Platforms Selection Checklist
  - Whether a platform is open (that is, a public Blockchain) or closed (a private Blockchain) and how that affects speed and security. Anyone can join a public Blockchain, which can make it easier to set up for small-business users, such as farmers. The downside is that open Blockchains are not as fast. Many of the Blockchain code bases can be modified to be either open or closed.
  - Consensus mechanism, such as PoW, PoS or Byzantine fault tolerance. PoW is the older mechanism used in Bitcoin and Ethereum. The others are newer and less proven but faster and more efficient.
  - Ledger technology and how it records the transactions. This relates to how the Blockchain keeps track of information. Popular approaches include an account model and UTXO. An account model records the balance, whereas the UTXO model is analogous to cash with serial numbers in your wallet. The account model is used in the Blockchain platforms Ethereum, Stellar, Tron and EOSIO. IBM Blockchain, Hyperledger Fabric and Hyperledger Sawtooth use UTXO.
  - Intended smart contract functions for capturing business logic on the Blockchain. Popular programming languages include Ethereum Solidity, Web Assembly and Digital Asset Modeling Language.

Centralized vs. decentralized

Decentralization's strengths are redundancy, data integrity and trustless transactions, which centralized systems mostly sacrifice for better performance, price and ease of use.

Consensus mechanism

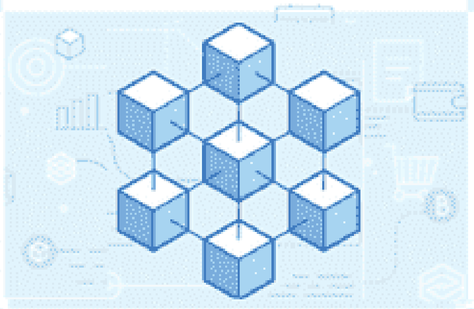
The algorithms used to verify blocks in a chain have a big impact on performance, security and compatibility with other platforms.

Cost

Products that are ostensibly free can cost more than commercial ones to deploy and use.

Development tools

The depth and breadth of support for developers often determines a platform's practicality for building enterprise applications.



Maturity

Mature platforms typically have stronger interoperability, vendor support and developer communities.

Performance

Decentralized platforms typically have much slower performance than centralized ones.

Private vs. public

AKA permissioned vs. permissionless, it largely determines performance, privacy and security—and what they cost.

Smart contracts

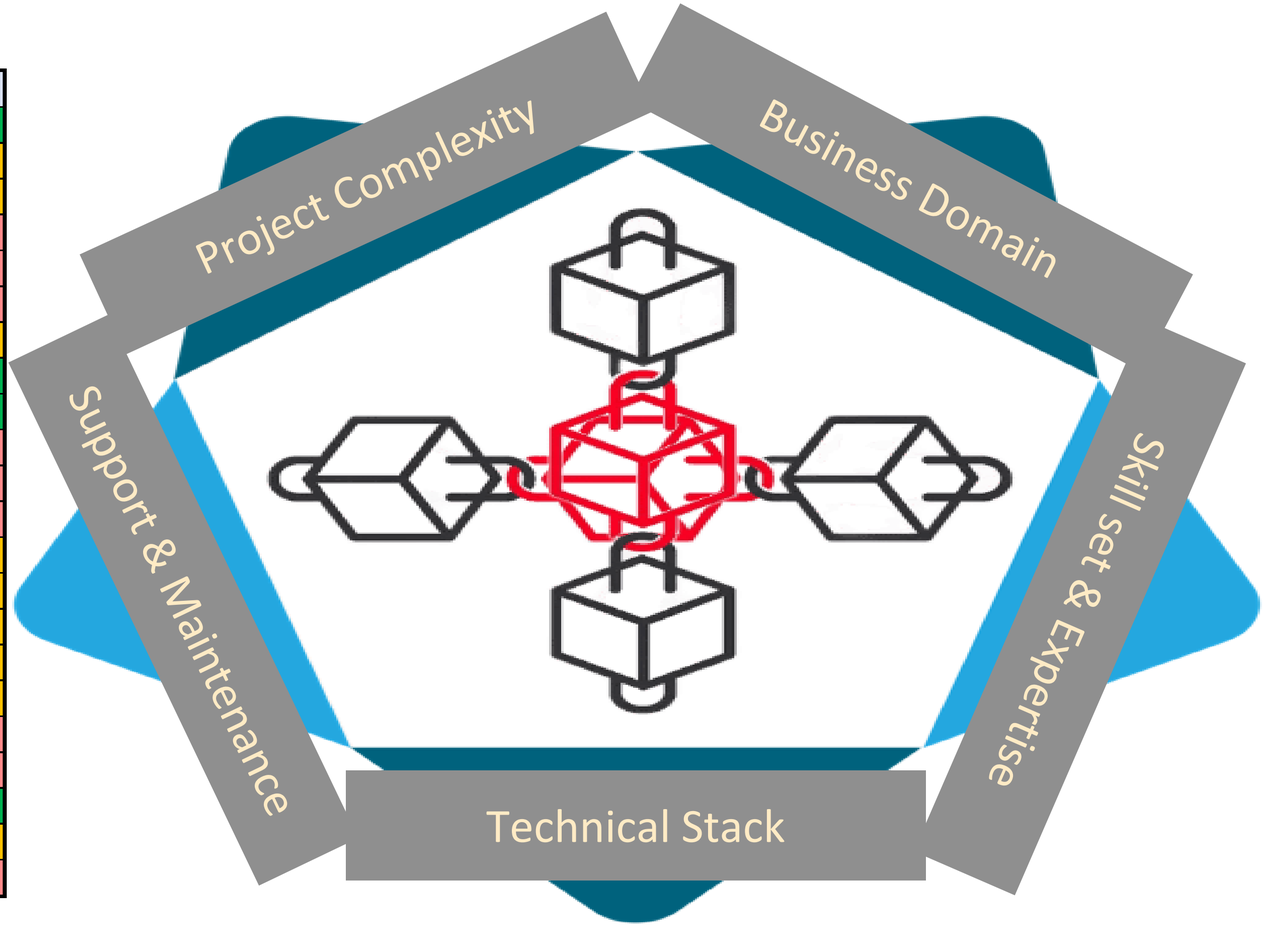
Much of a platform's value comes from the programmability and automation in its smart contract features.

BLOCKCHAIN OVERVIEW

Blockchain – 5 Estimation Factors

- Blockchain – 5 Estimation Factors

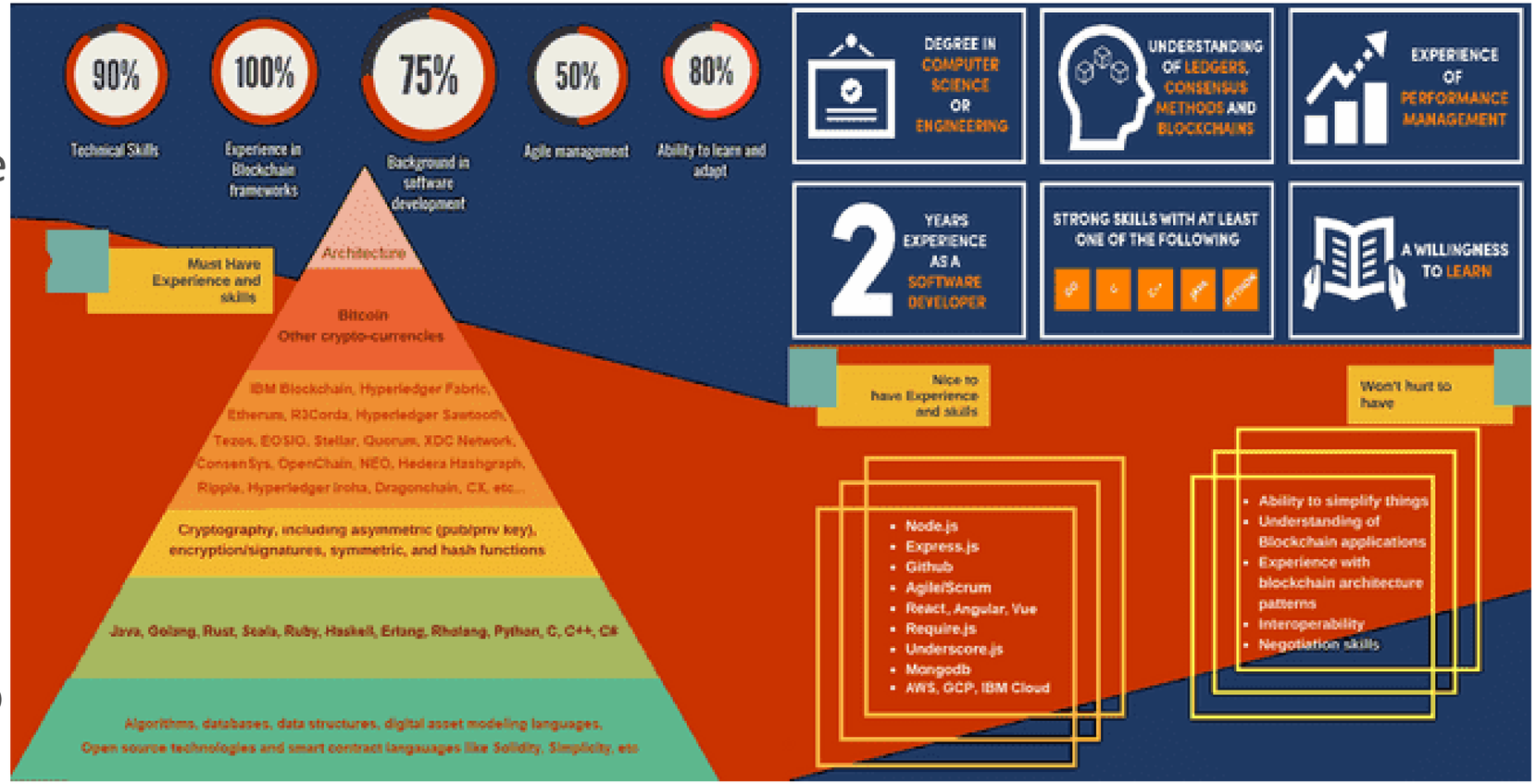
Factor	Attribute	Timeline	Effort	Cost
Project Complexity	Structural	Low	Low	Low
	Emergent	Medium	Medium	Medium
	Technical	Medium	Medium	Medium
	Temporal	High	High	High
	Socio-Political	High	High	High
	Directional	High	High	High
Business Domain	Banking, Finance Services and Insurance	Medium	Medium	Medium
	IT industry	Low	Low	Low
	Manufacturing	Low	Low	Low
	E-commerce, Retail, Wholesale	Low	Medium	High
	Online Services and marketing	High	High	High
	Logistics and Supply Chain Management	Medium	High	High
	Telecommunication	Low	Medium	Medium
Skills	Freshers	High	High	Medium
	2 years of Experience	Low	Medium	Medium
	4+ years of Experience	Low	Low	Medium
TechStack	Opensource customization	Low	Medium	Medium
	In-house Development	Medium	Medium	High
	Third Party integration	Low	Low	High
Support	1 year	Low	Low	Low
	3 years	Medium	Medium	Medium
	5+years	High	High	High



BLOCKCHAIN OVERVIEW

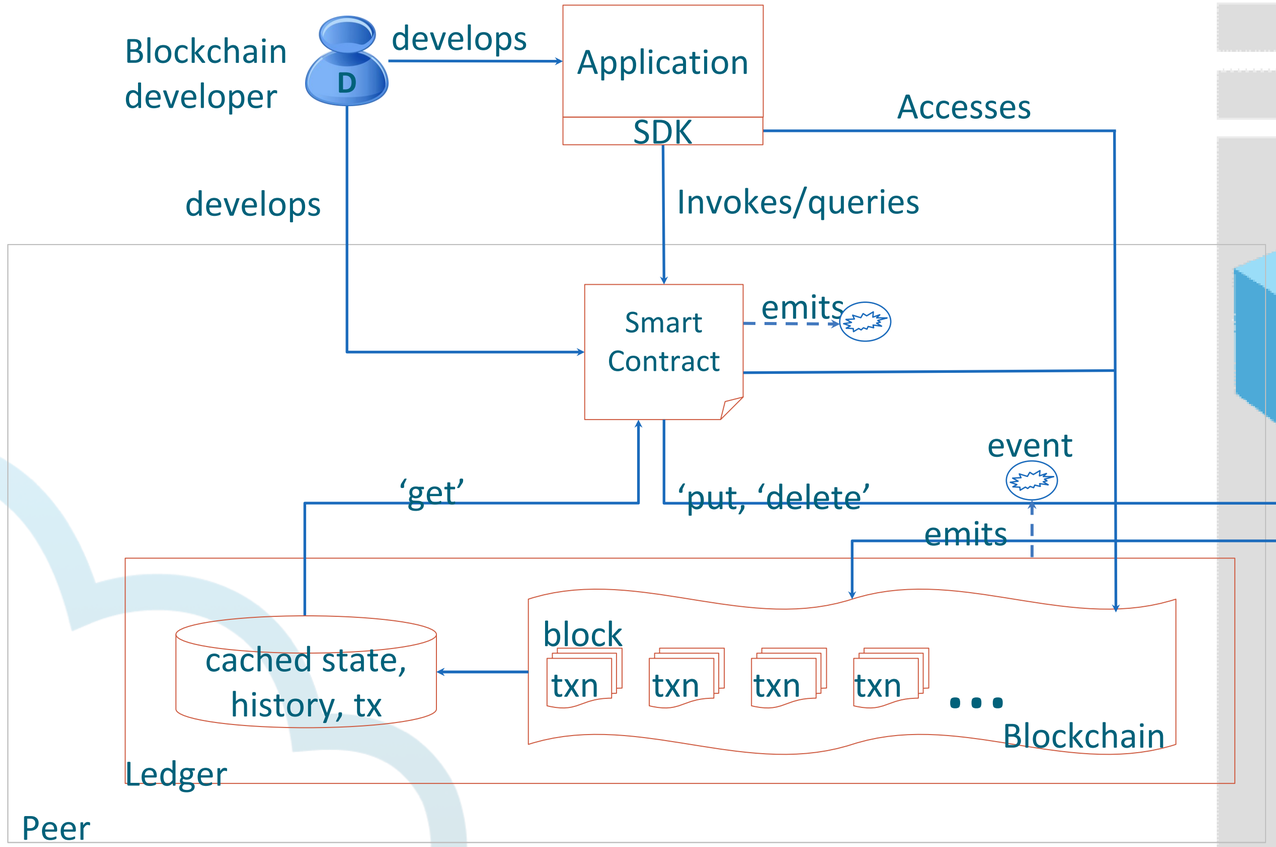
Blockchain – 8 Skills Needed

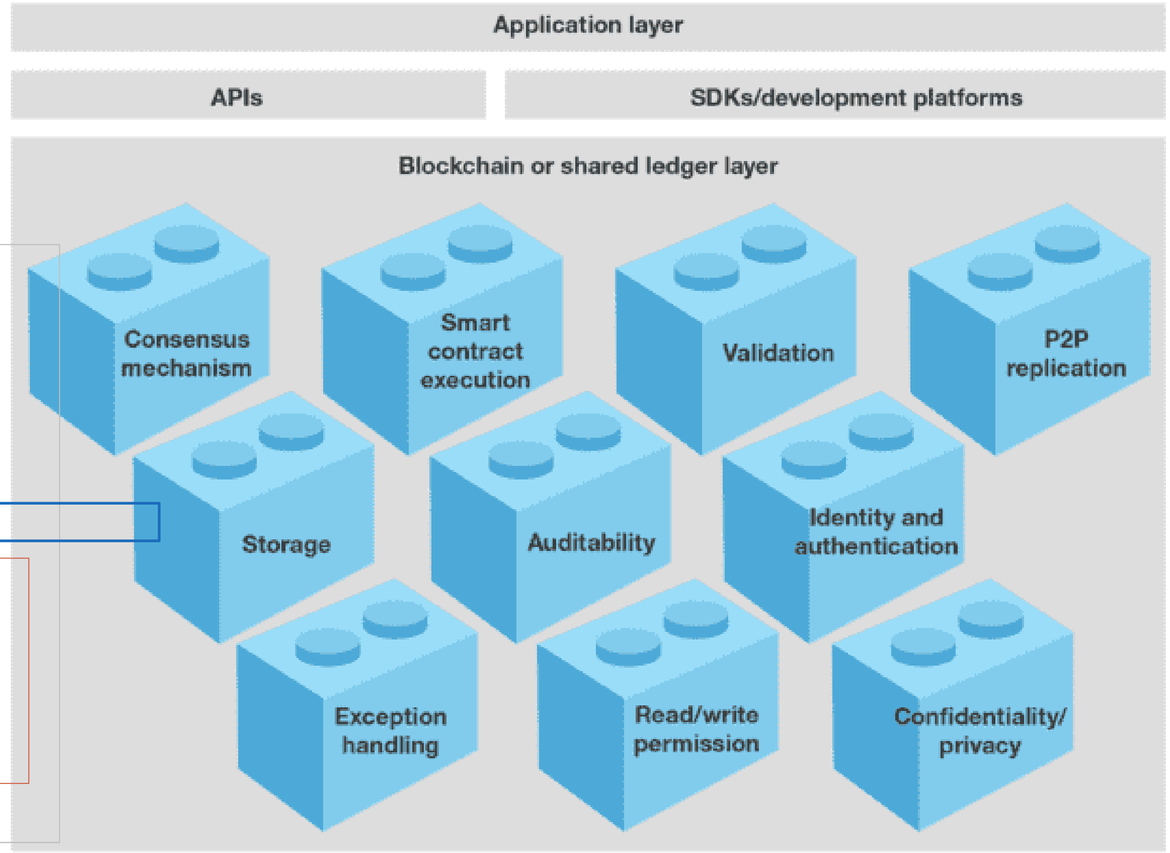
- Blockchain – 8 Skills Needed
  1. Blockchain Architecture
  2. Smart Contract Development
  3. Cryptography
  4. Web Development
  5. Data Structures
  6. OOPS
  7. Understand Standards and Eco systems
  8. Interoperability skills to integrate any systems



Blockchain – What developer does?

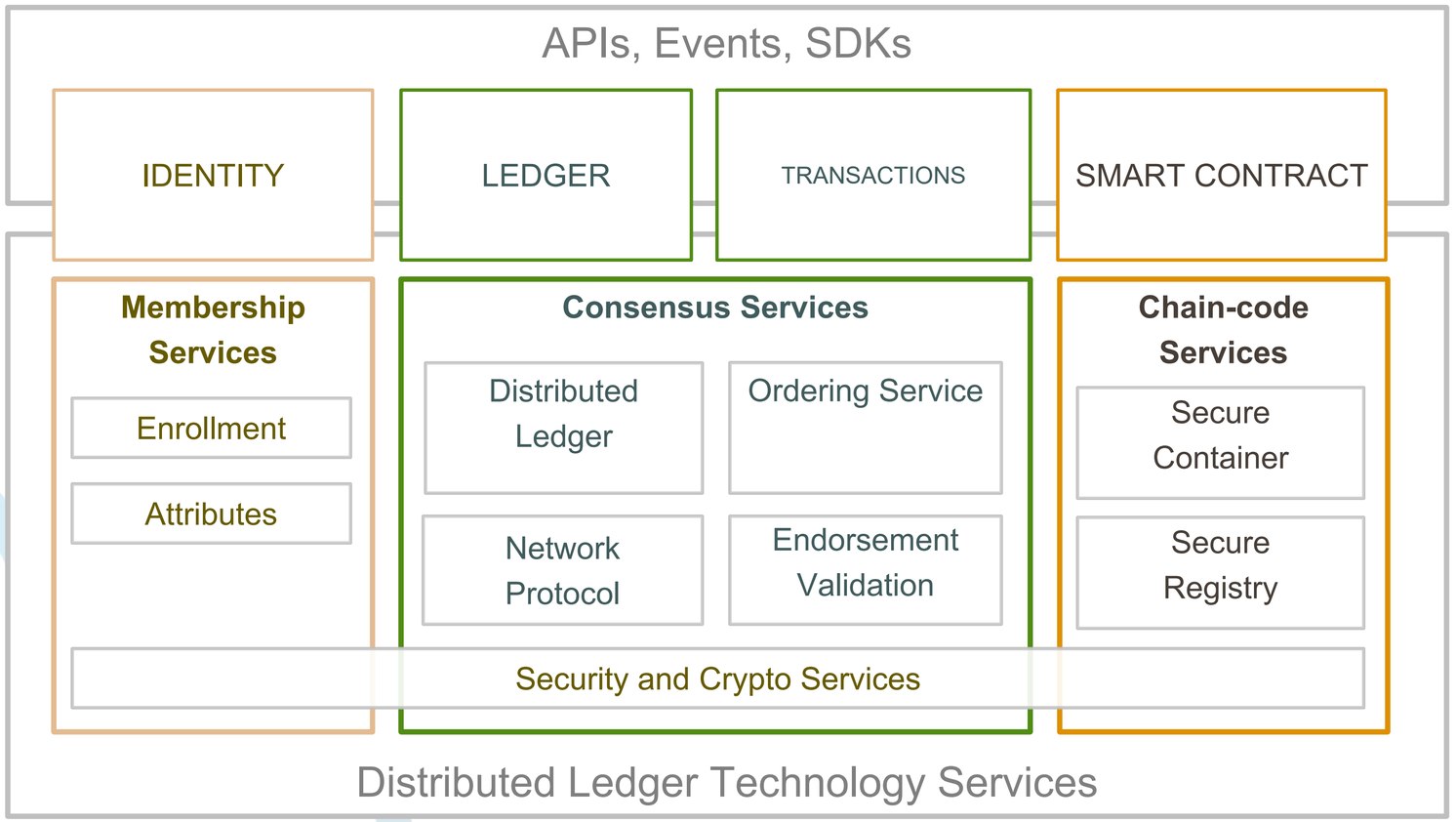
- Blockchain – What developer does?





Blockchain – What developer does?

- Blockchain – What developer does?



IDENTITY
Pluggable, Membership, Privacy and Auditability of transactions.

LEDGER | TRANSACTIONS
Distributed transactional ledger whose state is updated by consensus of stakeholders

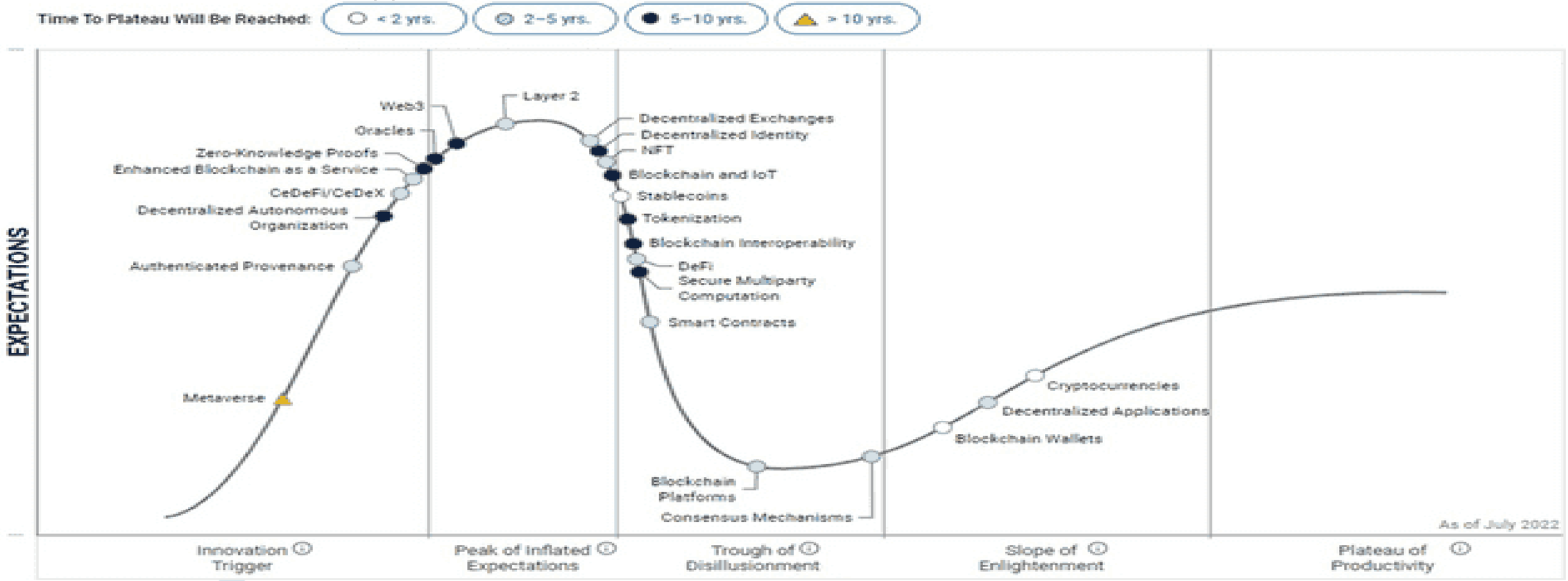
SMART-CONTRACT
“Programmable Ledger”, provide ability to run business logic against the blockchain (aka smart contract)

APIs, Events, SDKs
Multi-language native SDKs allow developers to write DLT apps

BLOCKCHAIN OVERVIEW

Blockchain –Gartner Hype chart

- Blockchain –Gartner Hype chart



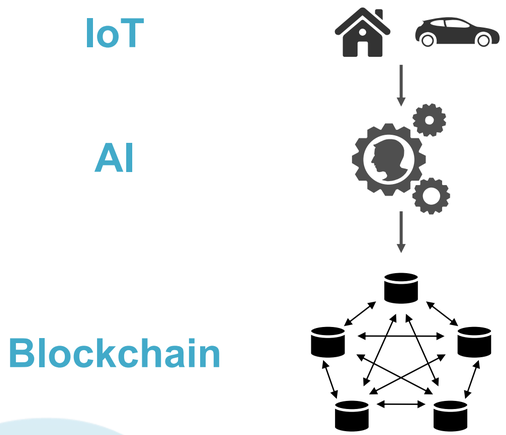
BLOCKCHAIN OVERVIEW

Blockchain – Future Vision

- Blockchain – Future Vision

[Current Short-term – 2 years]

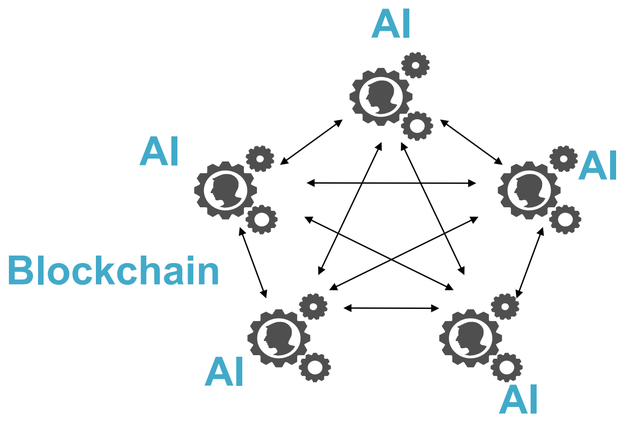
Combination of IoT, Blockchain and AI



Providing this two-way real-time interoperability between the real economy and the financial system will be disruptive

[Mid-term – 3 to 5 years]

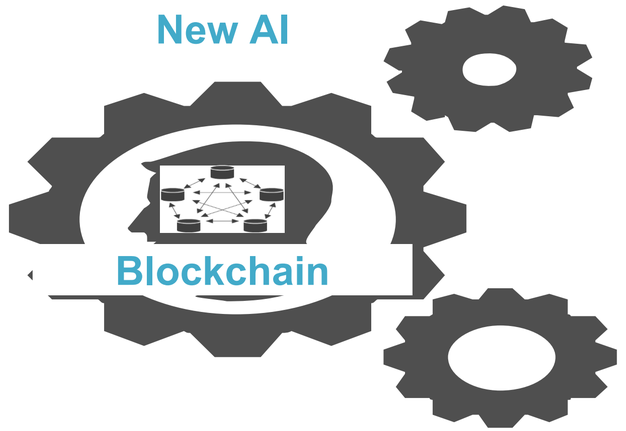
Blockchain, a guarantee to control AI



The Blockchain consensus might be a way to keep potential malicious AIs under control

[Long-term – 10 years]

Blockchain, a new architecture for a new AI

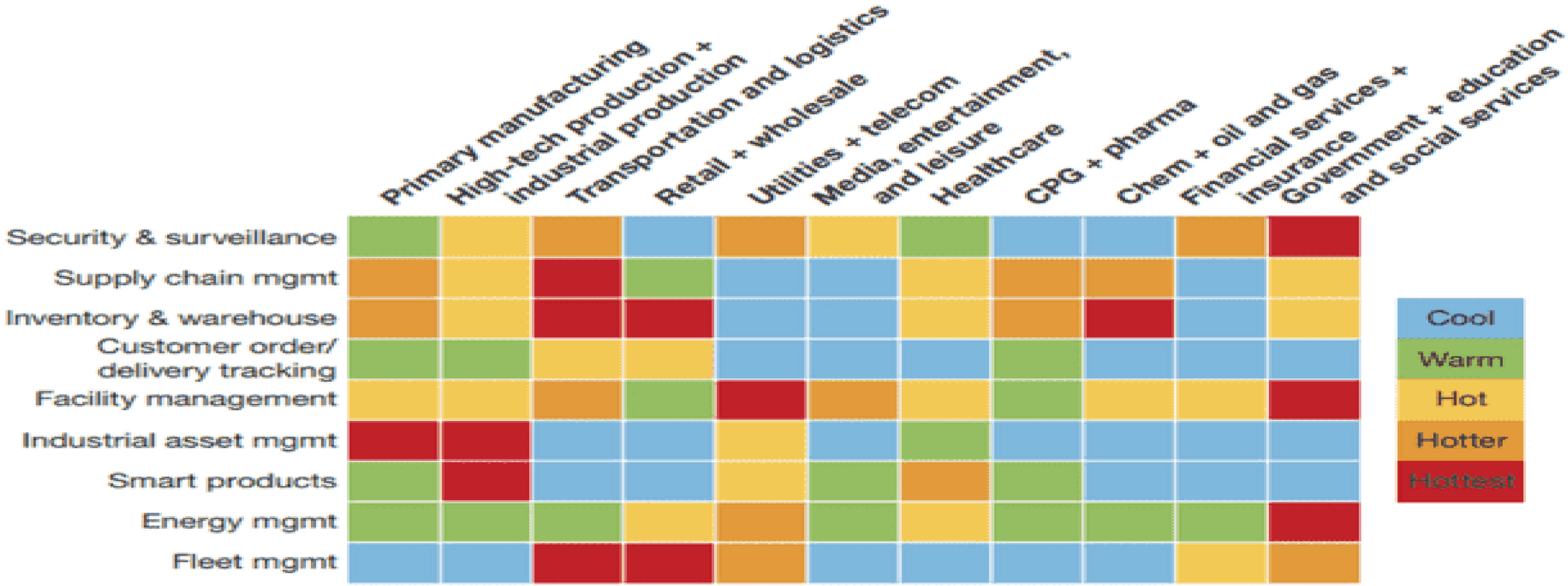


The Blockchain technology might open the way to a new type of AI by getting closer to the real neuronal behavior

BLOCKCHAIN OVERVIEW

Blockchain – Use cases Heatmap

- Blockchain – Use cases Heatmap



BLOCKCHAIN OVERVIEW

Blockchain – Simple Use case

- Blockchain – Simple Use case

Hey, I want a cup of herbal tea, should I use a Blockchain ?
With AI, can I get a correct herbal tea based on my health conditions without my initiation ?

Trusted IoT identification

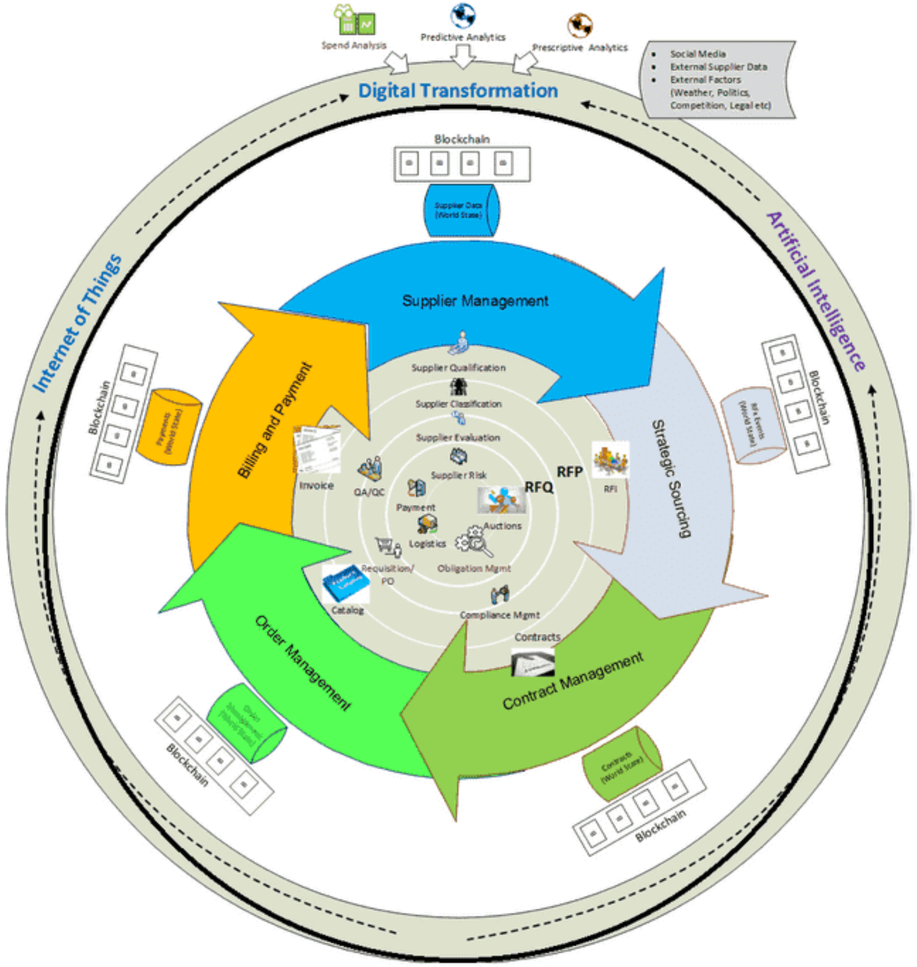
Conditions (time, temperature, stress level…)

Collaborative SupplyChain organisation

BLOCKCHAIN IMPLEMENTATION

Phases for South African Supplier Chain Network

- Phases
  - Phase 1:
    - Identity Management for Suppliers Network
    - Chat System for Suppliers Network
    - Certify the System for South Africa Network
  - Phase 2:
    - End to End Workflow for Suppliers Network Services



BLOCKCHAIN IMPLEMENTATION

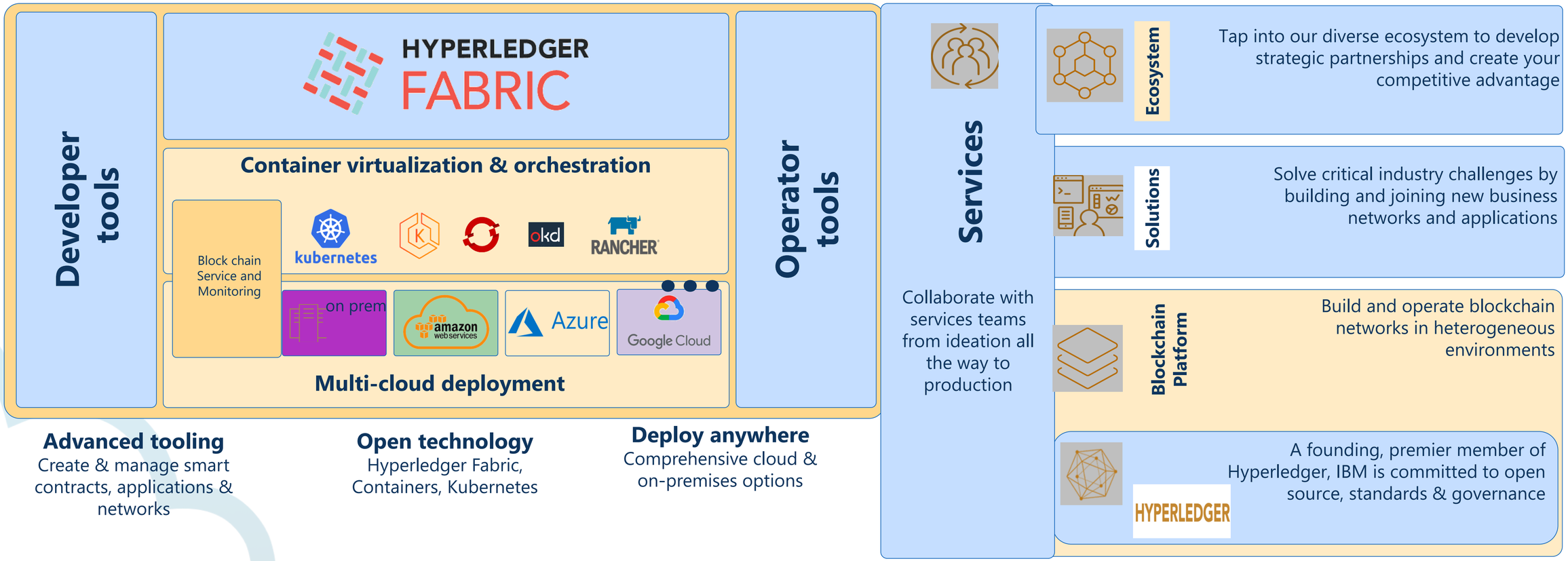
Why Hyperledger Fabric?

- Why Hyperledger Fabric?

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	— Generic blockchain platform	— Modular blockchain platform	— Specialized distributed ledger platform for financial industry
Governance	— Ethereum developers	— Linux Foundation	— R3
Mode of operation	— Permissionless, public or private[4]	— Permissioned, private	— Permissioned, private
Consensus	— Mining based on proof-of-work (PoW) — Ledger level	— Broad understanding of consensus that allows multiple approaches — Transaction level	— Specific understanding of consensus (i.e., notary nodes) — Transaction level
Smart contracts	— Smart contract code (e.g., Solidity)	— Smart contract code (e.g., Go, Java)	— Smart contract code (e.g., Kotlin, Java) — Smart legal contract (legal prose)
Currency	— Ether — Tokens via smart contract	— None — Currency and tokens via chaincode	— None

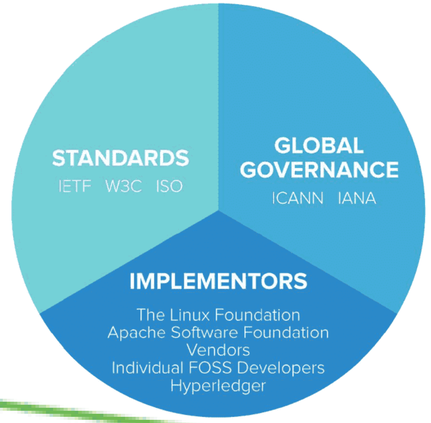
Hyperledger Fabric Benefits

- Hyperledger Fabric Benefits

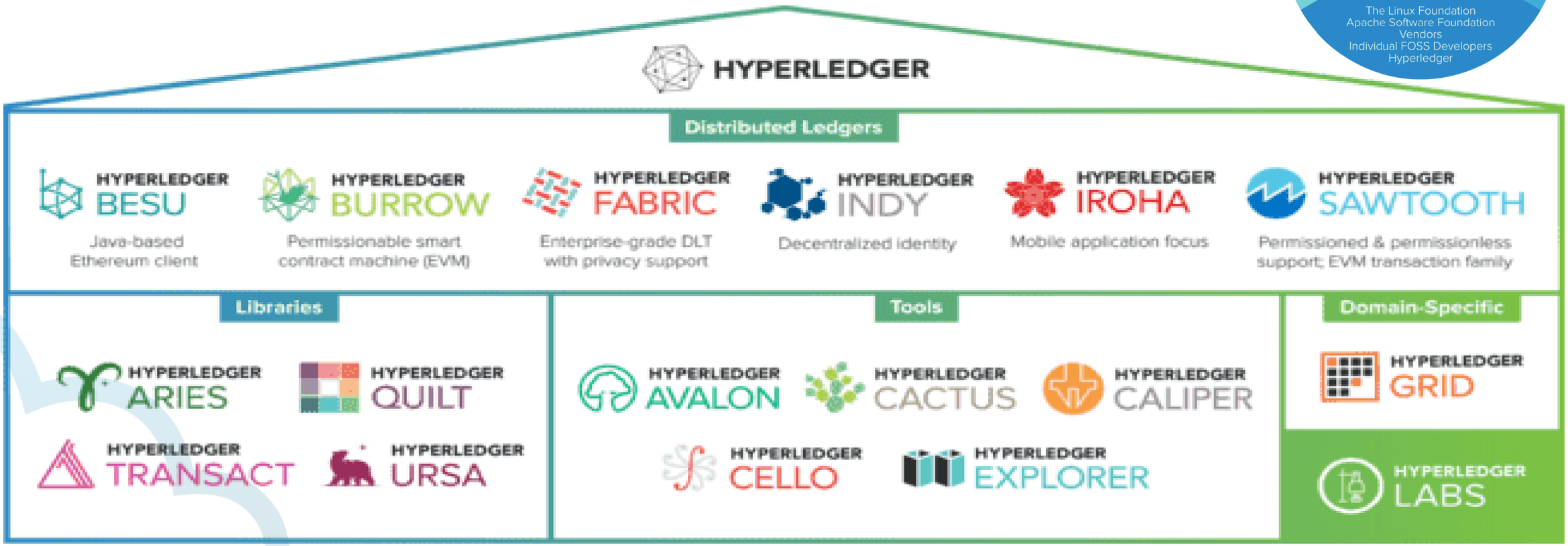


BLOCKCHAIN IMPLEMENTATION

Hyperledger End user components view



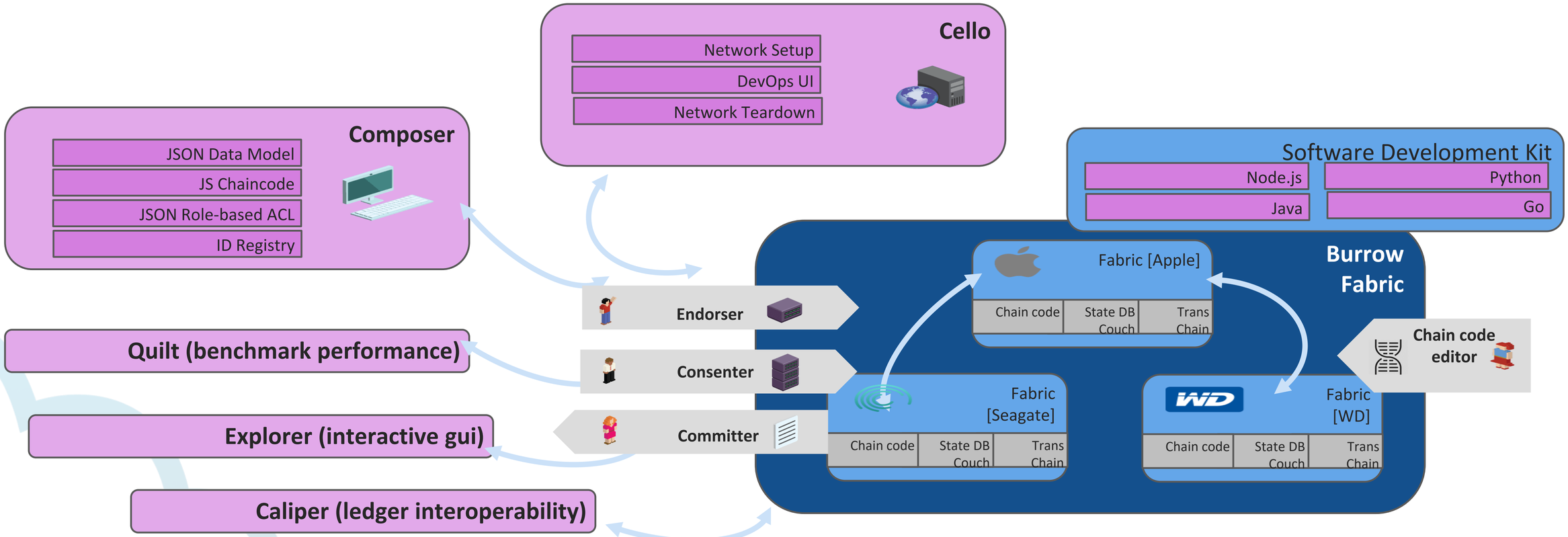
- Hyperledger End user components view



BLOCKCHAIN IMPLEMENTATION

Hyperledger Developer view

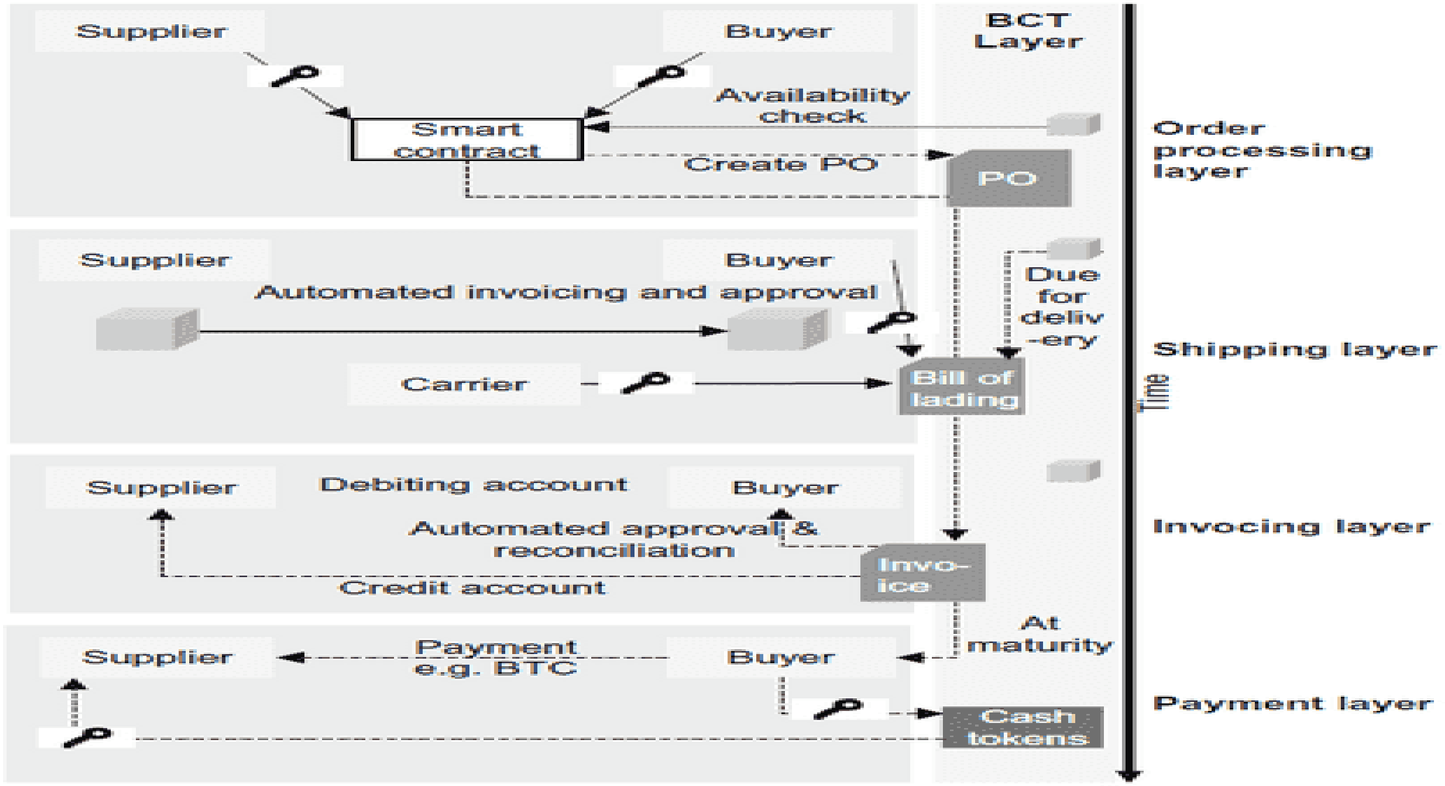
- Hyperledger Developer view

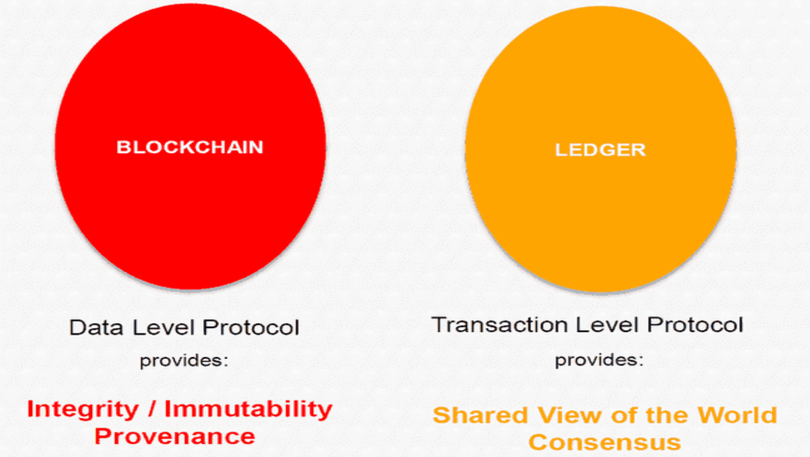


BLOCKCHAIN IMPLEMENTATION

Sample Transaction Flow

- Sample Transaction Flow

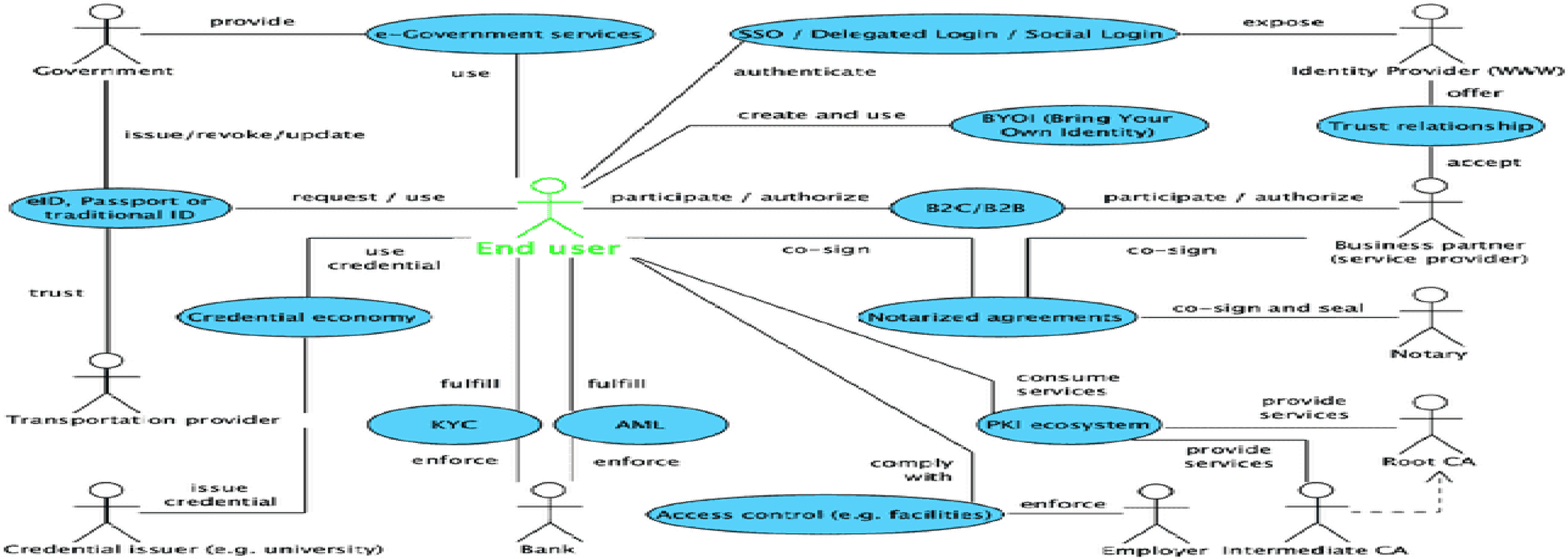




BLOCKCHAIN IMPLEMENTATION

Phase 1 – Identity Management and KYC

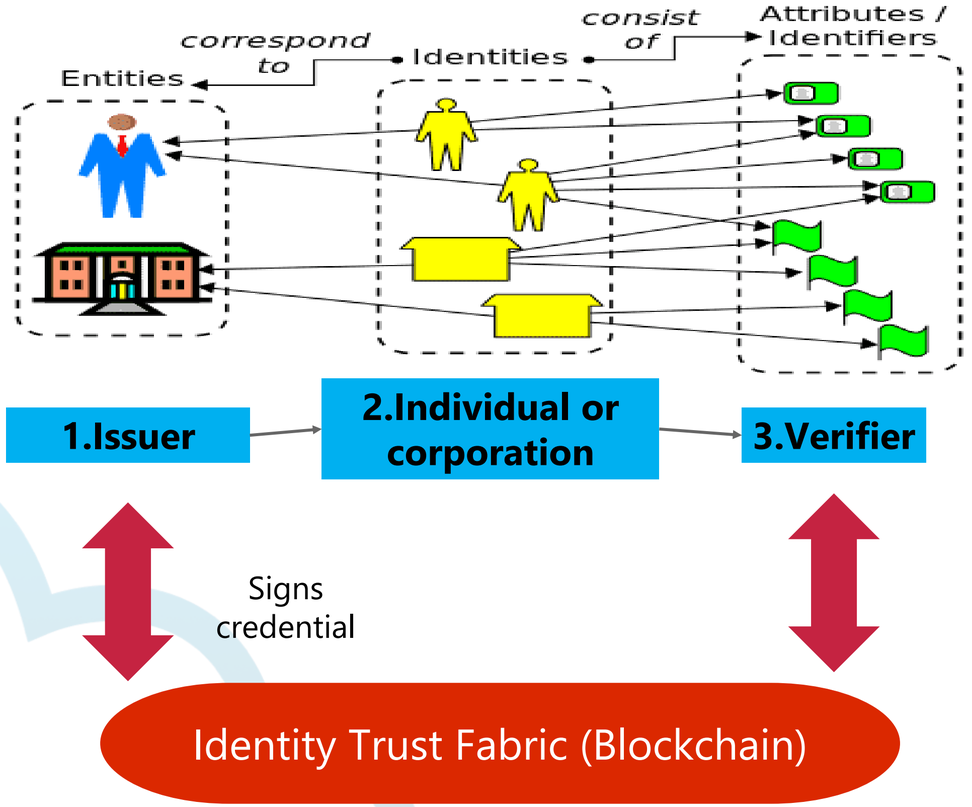
- Phase 1 - Identity Management and KYC

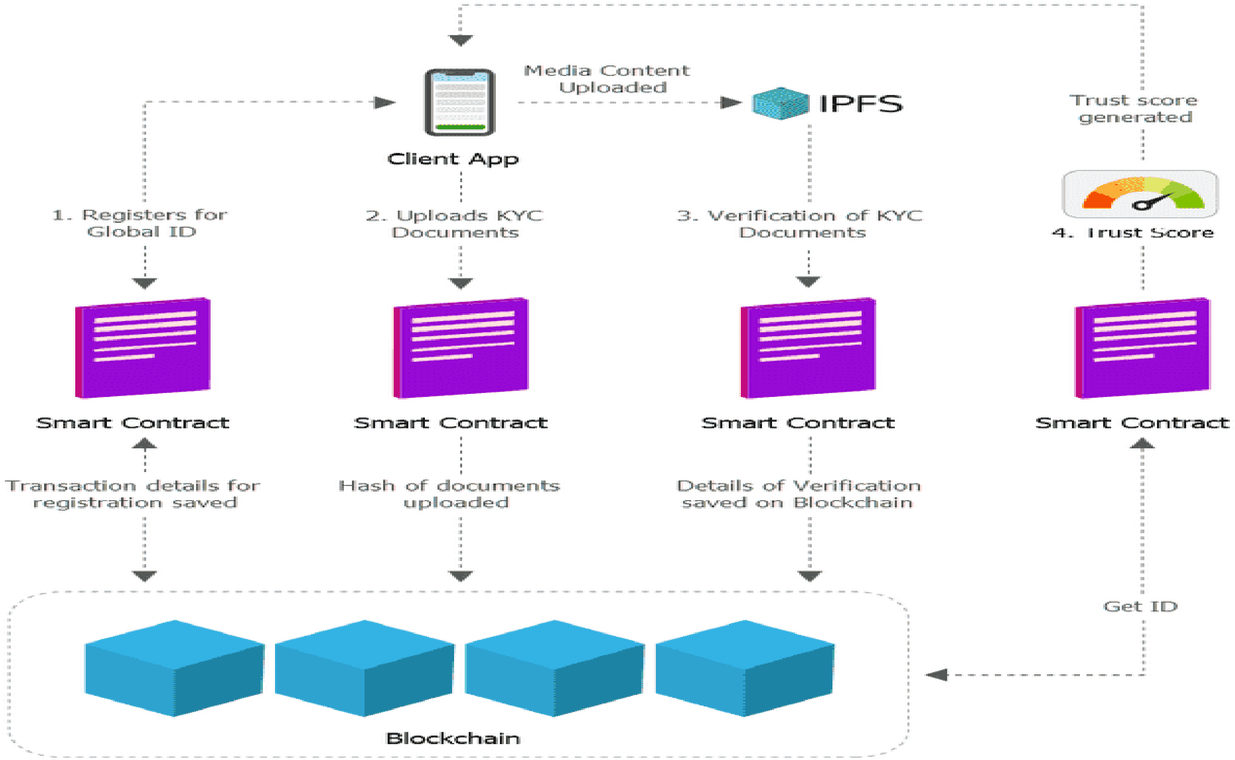


BLOCKCHAIN IMPLEMENTATION

Phase 1 - Identity Management Blockchain Interface

- Phase 1 - Identity Management Blockchain Interface

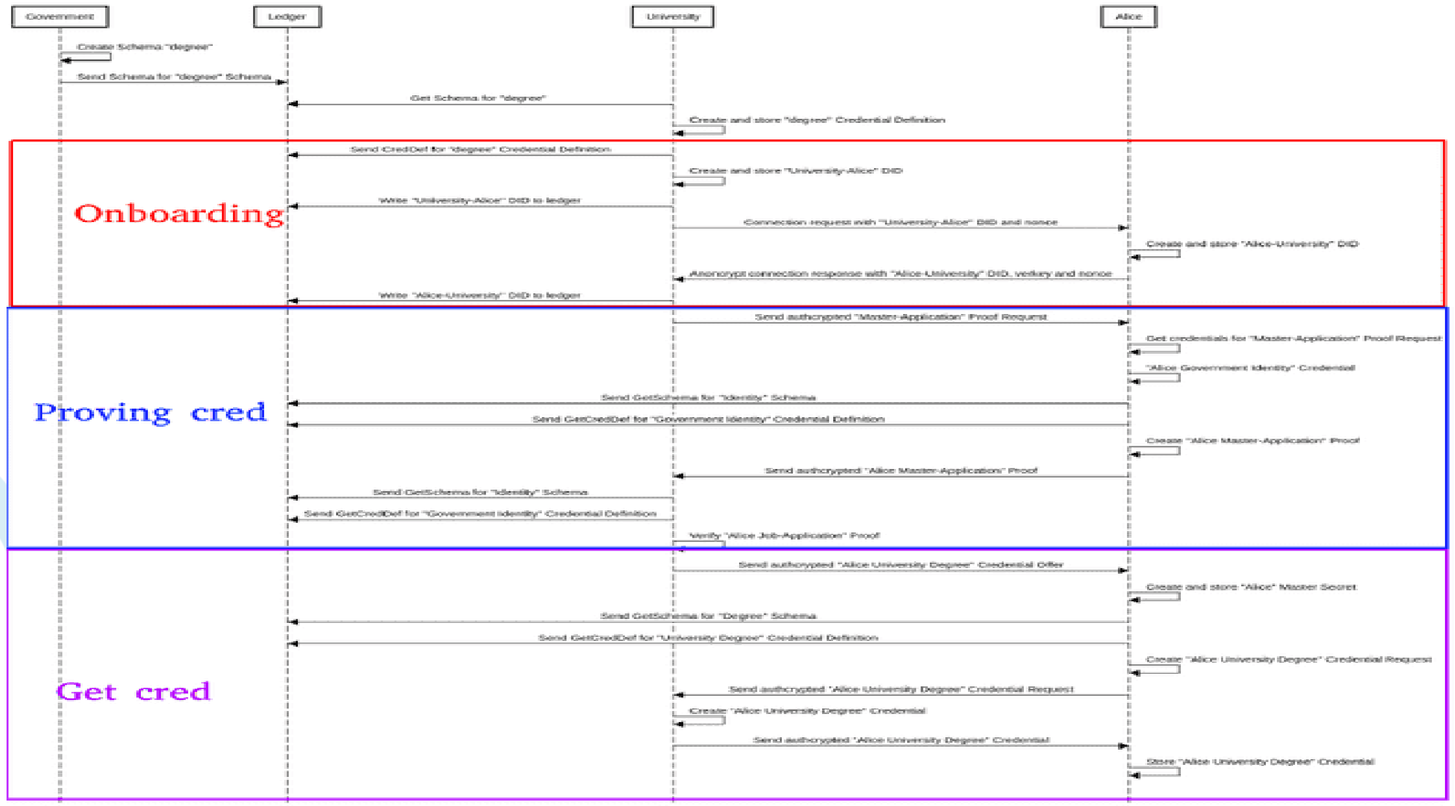


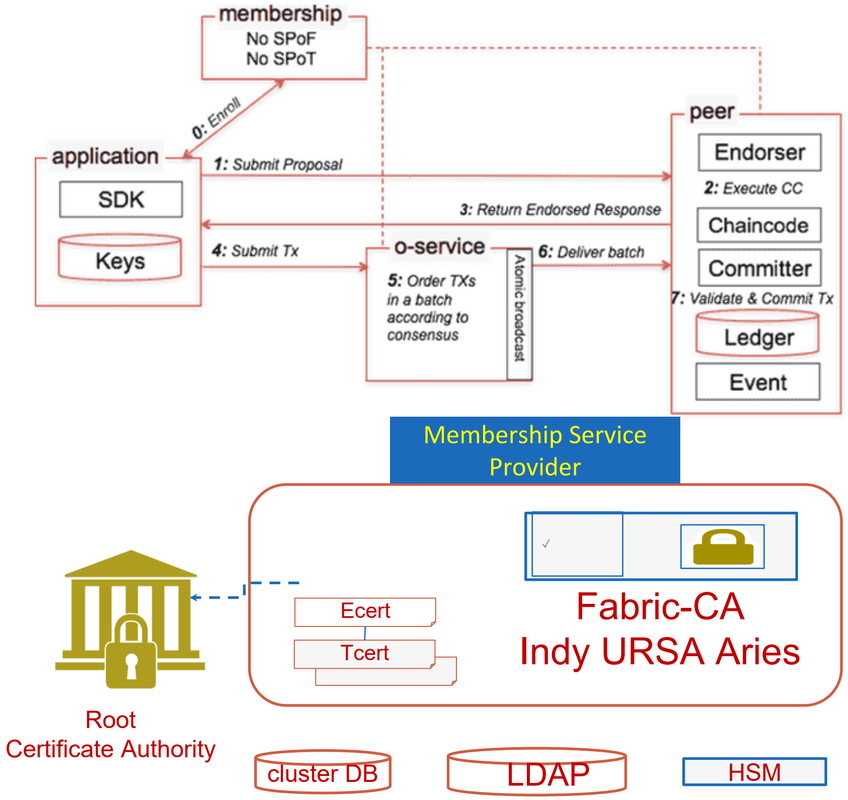


BLOCKCHAIN IMPLEMENTATION

Phase 1 - Identity Management Sequence Diagram

- Phase 1 - Identity Management Sequence Diagram

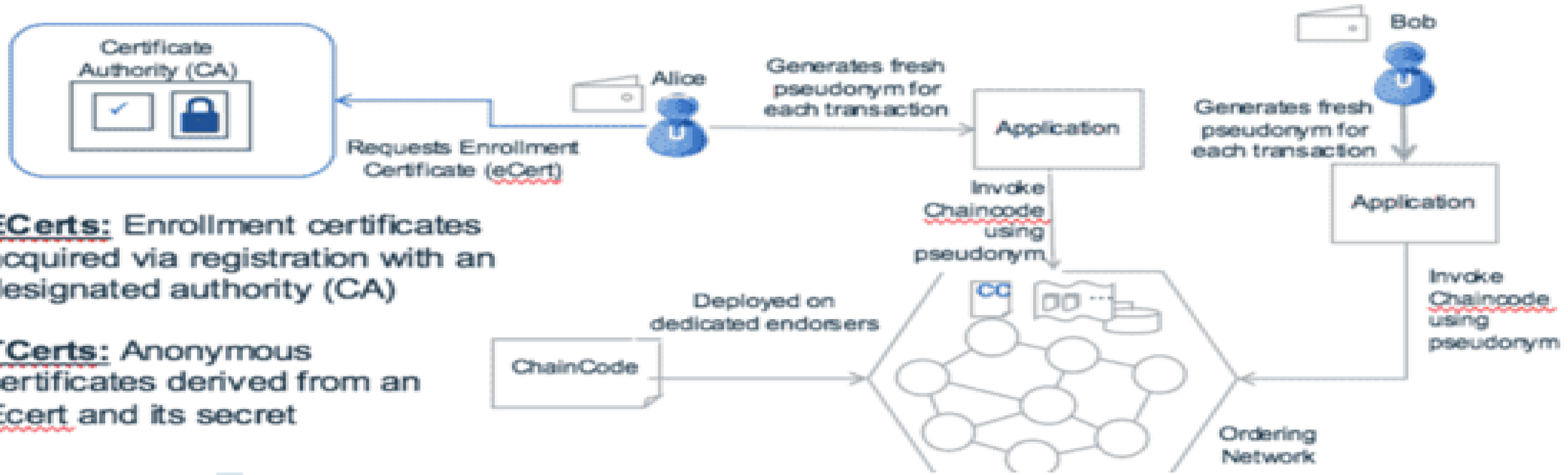




BLOCKCHAIN IMPLEMENTATION

Phase 1 - Identity Management - Zero Knowledge Proof (ZPK)

- Phase 1 - Identity Management - Zero Knowledge Proof (ZPK)
  - A new membership framework leveraging Zero Knowledge to allow for anonymous authentication of the members of an organization
  - Anonymity provisions bound by the leakage of invoked chaincode's data

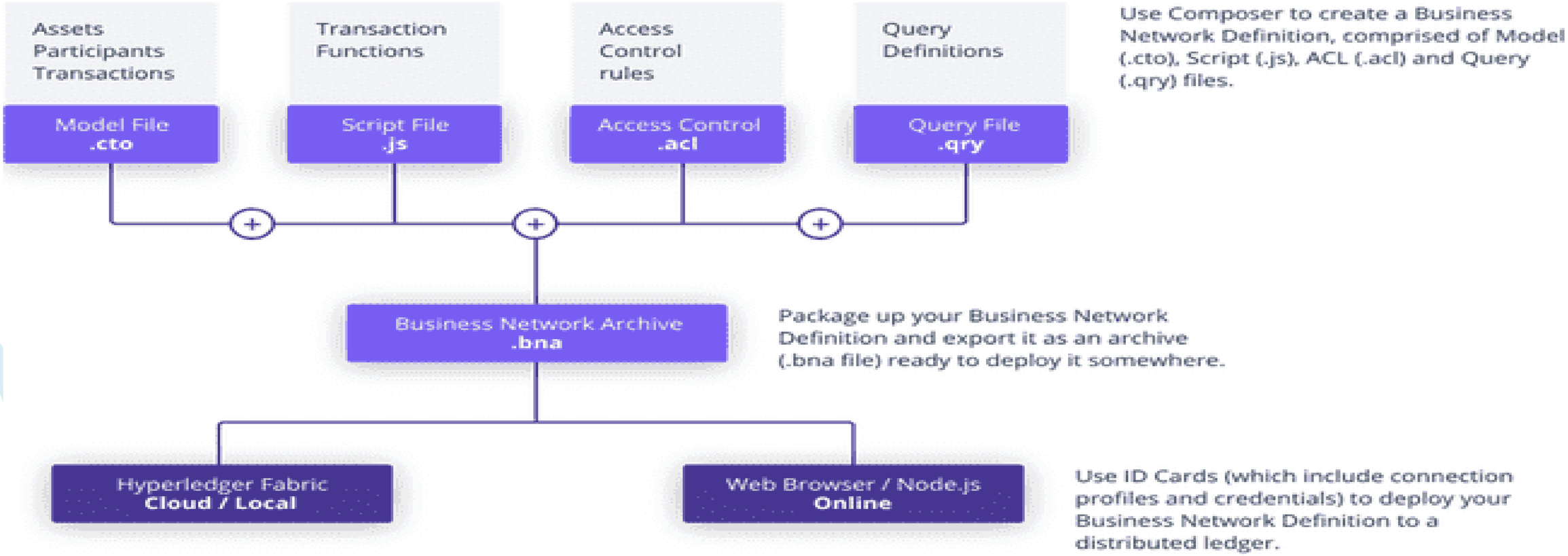


- **ECerts:** Enrollment certificates acquired via registration with an designated authority (CA)
- **TCerts:** Anonymous certificates derived from an Ecert and its secret

BLOCKCHAIN IMPLEMENTATION

Phase 1 - Identity Management Files Process Structure

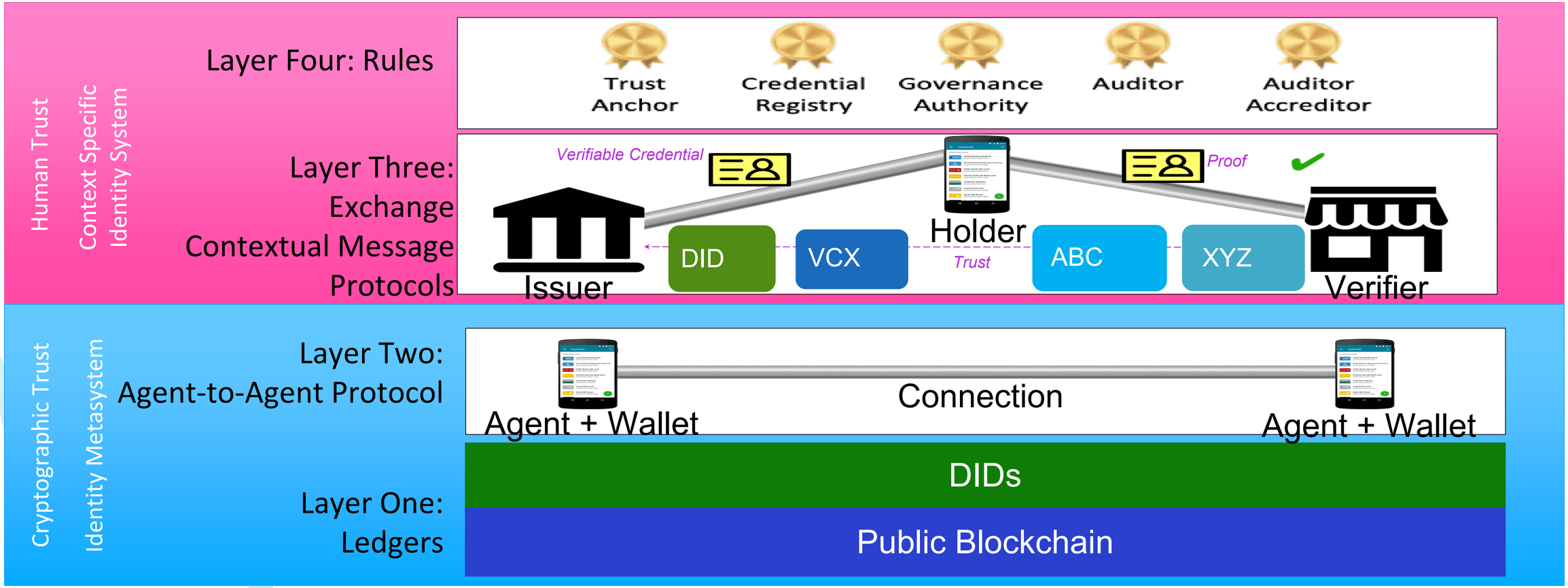
- Phase 1 - Identity Management Files Process Structure



BLOCKCHAIN IMPLEMENTATION

Phase 1 - Identity Management Application Layer Structure

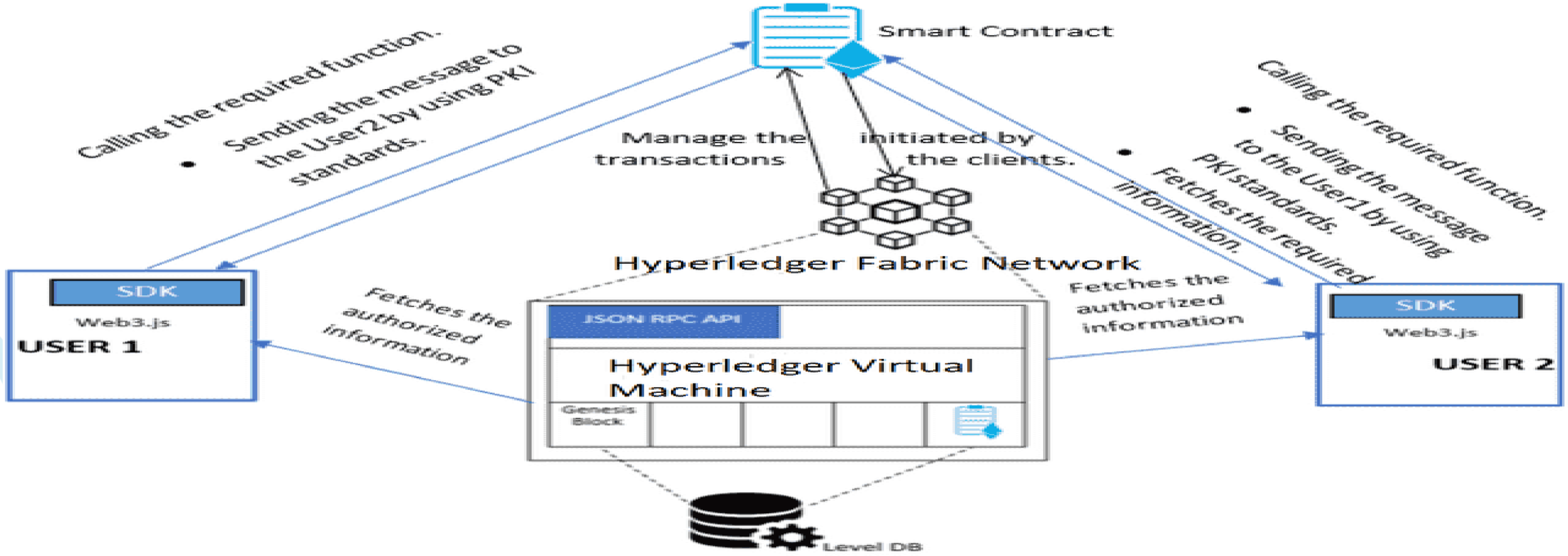
- Phase 1 - Identity Management Application Layer Structure



BLOCKCHAIN IMPLEMENTATION

Phase 1 – dApp Chat System for Suppliers

- Phase 1 – dApp Chat System for Suppliers



Phase 1 – Certification Standards

- Phase 1 – Certification Standards

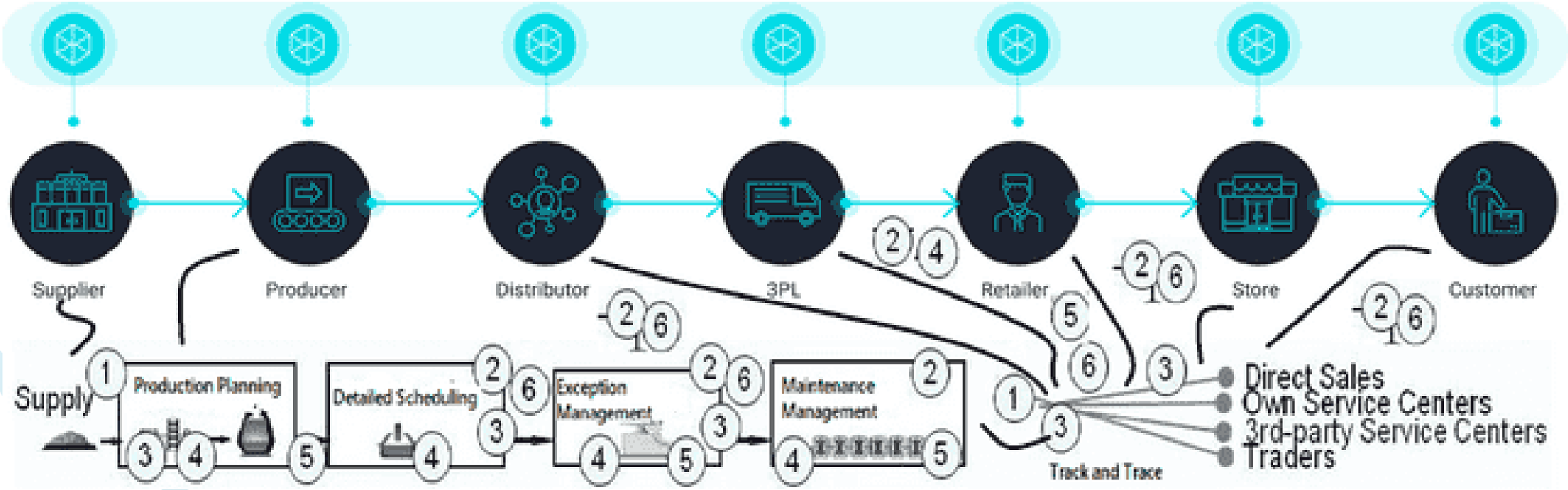
Standard	Title
ISO/IEC 27000	Overview and vocabulary
ISO/IEC 27001	Information security management systems – Requirements
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	Information security management system - guidance
ISO/IEC 27004	Information security management Monitoring, measurement, analysis and evaluation

Standard	Title
ISO/IEC 29190	Privacy capability assessment model
ISO/IEC 24760-3	A framework for identity management – Part 3: Practice
ISO/IEC 29146	A framework for access management
ITU-T X.1085 | ISO/IEC 17922	Tele biometric authentication framework using biometric hardware security module
ISO/IEC 29003	Identity proofing
ISO/IEC 29134	Privacy impact assessment – Guidelines
ITU-T X.gpim | ISO/IEC 29151	Code of practice for personally identifiable information protection
ISO/IEC 20889	Privacy enhancing data de-identification techniques

BLOCKCHAIN IMPLEMENTATION

Phase 2 - After login Business Flow for End Users

- Phase 2 - After login Business Flow for End Users

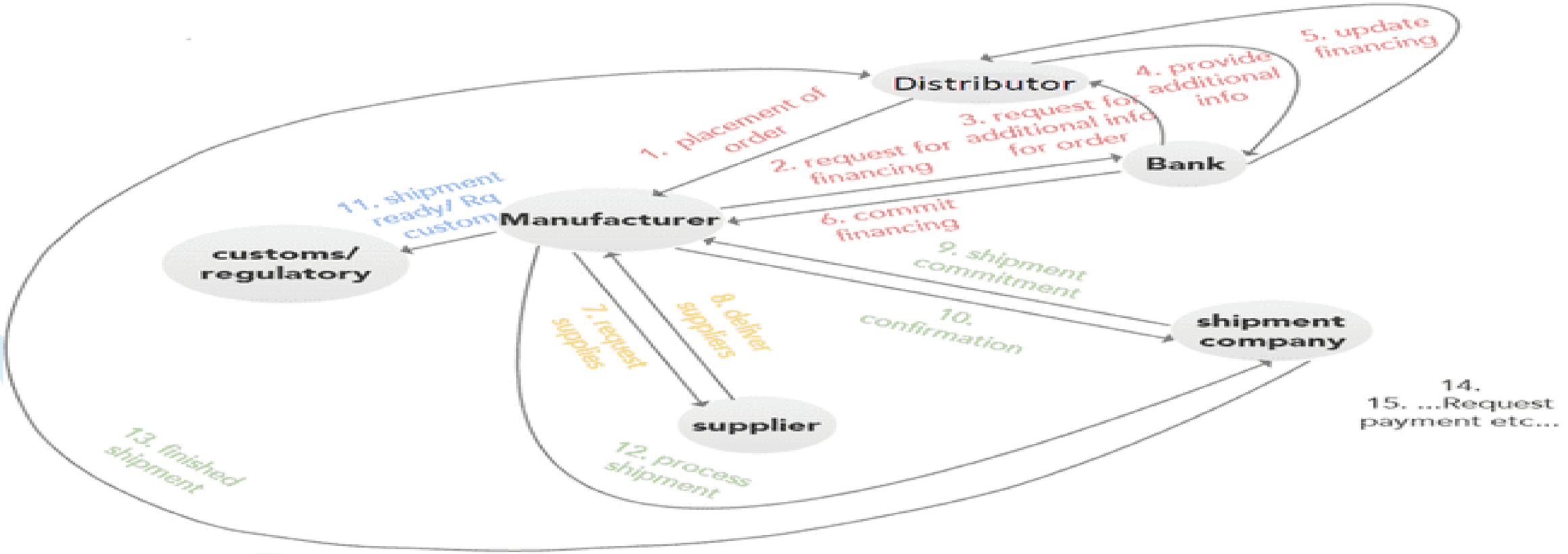


1. Production Planning and Procurement Management, 2. Financial Transactions Management, 3. Detailed Scheduling and Project Monitoring, 4. Exception Management and Performance Management, 5. Maintenance Management and Inventory Management, 6. Track and Trace Logistics along with Returns Management as Exception Management

BLOCKCHAIN IMPLEMENTATION

Phase 2 - After login Use Case for the Business Workflow

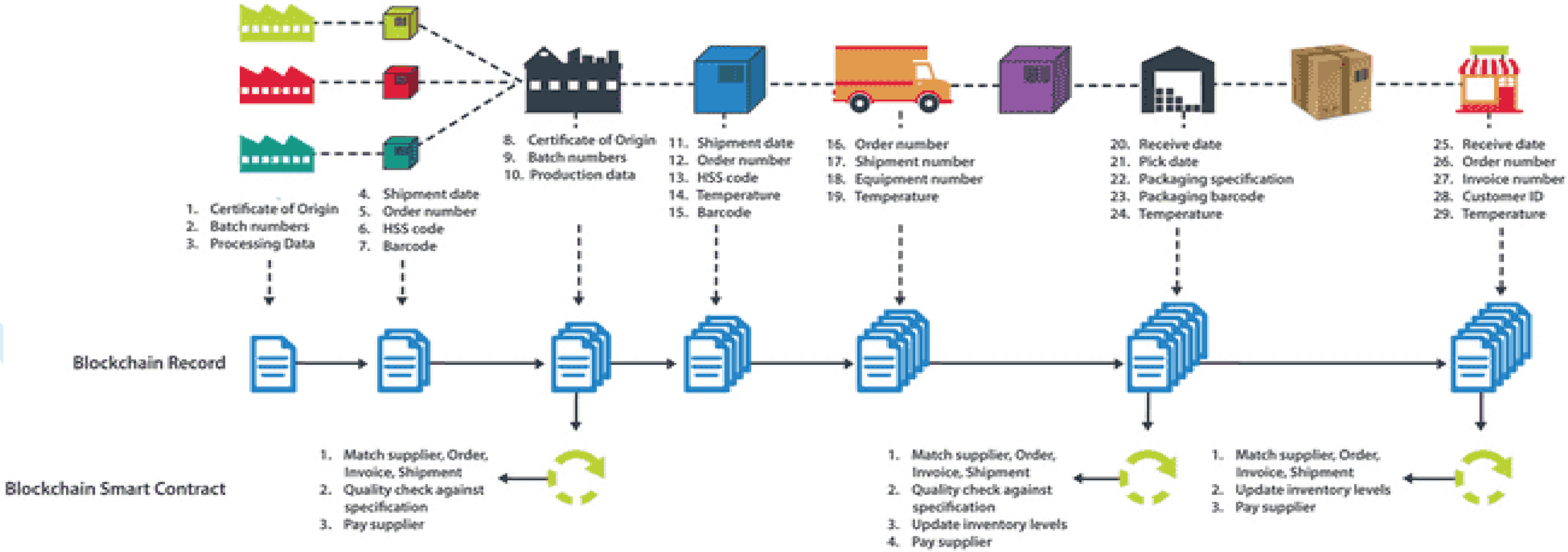
- Phase 2 - After login Use Case for the Business Workflow



BLOCKCHAIN IMPLEMENTATION

Phase 2 - Use Case for Developer End to End Workflow

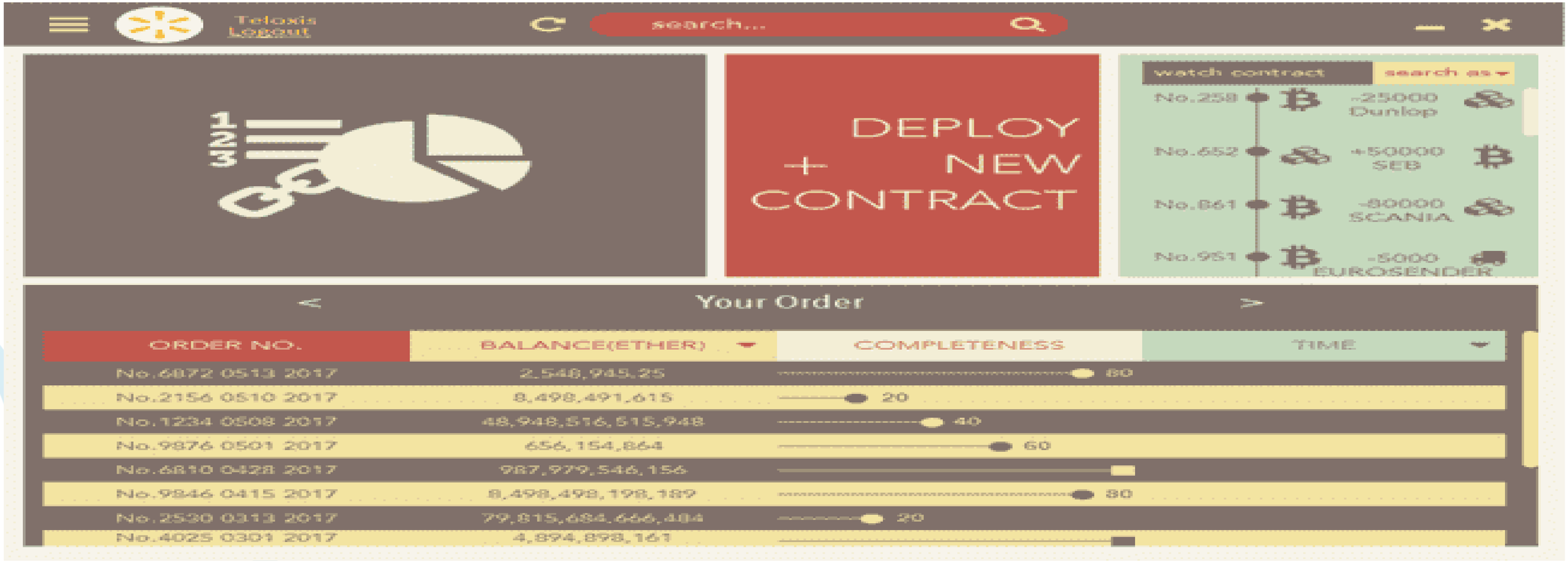
- Phase 2 - Use Case for Developer End to End Workflow



BLOCKCHAIN IMPLEMENTATION

Phase 2 - Dashboard Screen after Login Success

- Phase 2 - Dashboard Screen after Login Success



BLOCKCHAIN IMPLEMENTATION

Phase 2 - On Clicking PIE Chart

- Phase 2 - On Clicking PIE Chart

Thank you!

S. Lakshmanaraj
Lakshmanaraj.Sankaralingam@ideastoimpacts.com
https://www.linkedin.com/in/lakshmanarajsankaralingam/

"Accelerating the future of work thereby, Distributing the future evenly"

www.ideastoimpacts.com