PHOENIX, AZ | MARCH 3-6, 2020

10 Practical Challenges for Enterprise Blockchain

Baohua Yang@*Oracle*

AGENDA

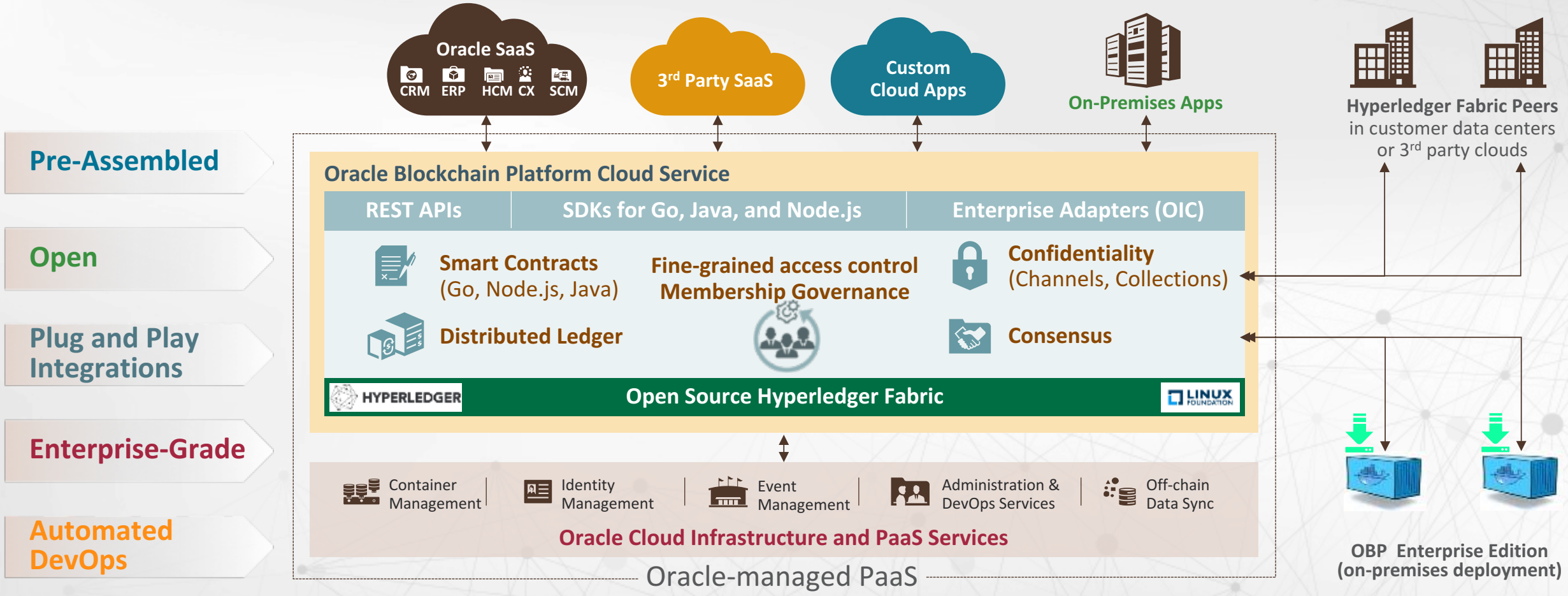
- About Oracle Blockchain Platform
- SQL in Smart Contract
- Data Backup/Recovery
- Ledger checkpoint and pruning/archiving
- Byzantine Fault Tolerant consensus
- Governance
- Performance
- Privacy Protection
- Inter-network Protocol
- Pluggable Crypto Implementations
- Auditing Capability

About Oracle Blockchain Platform

- Based on Hyperledger Fabric (with enhancements), pre-assembled and hardened for enterprise
- Cloud BaaS release (Cloud Edition) GA'ed in July 2018
- On-premises release (Enterprise Edition) GA'ed in August 2019
- Recently named to Constellation Group's shortlist as one of the leading Blockchain Technology Providers
- Serving customers in Supply Chain, Finance, Public Sector, etc.
- More information and Try for free:
  - https://www.oracle.com/blockchain/
  - https://developer.oracle.com/blockchain

Oracle Blockchain Platform Cloud Service

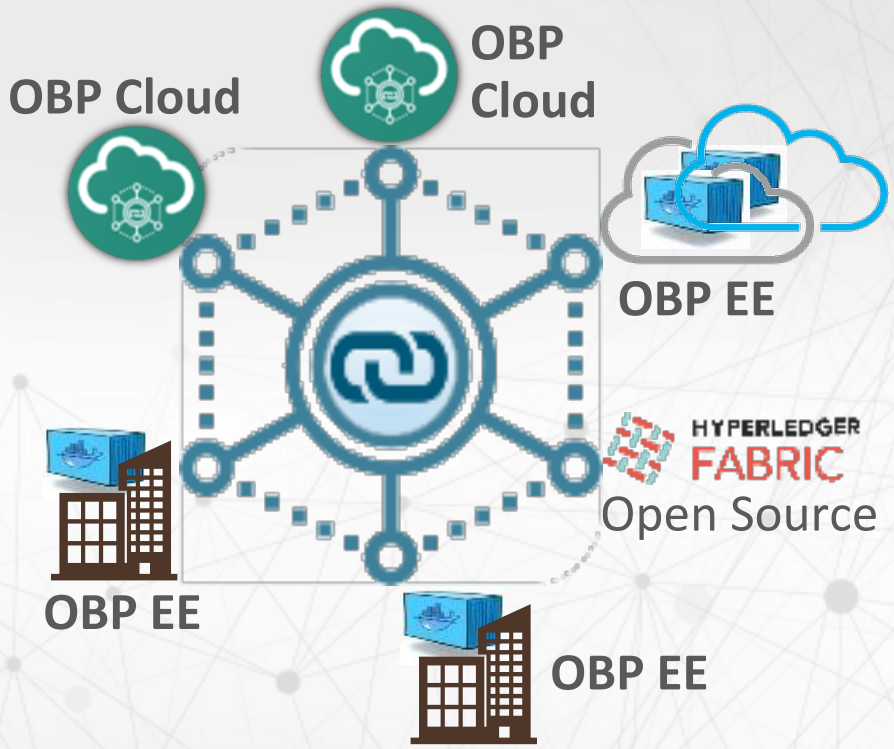
Hardened for enterprise applications



Oracle Blockchain Platform Enterprise Edition

On-premise blockchain solution for customers who must meet data sovereignty or data residency regulations

- Deploy Oracle Blockchain in your data center
  - Choice of virtualization platforms: VMware, OLVM
  - Enterprise-grade with HA and Dynamic Scalability
- Create Blockchain network with a few clicks
  - Fully pre-assembled with Hyperledger Fabric 1.4, Blockchain Platform Manager, Operations Console, REST Proxy, Identity Management
- Feature parity with Blockchain Cloud
  - Same APIs & portability of applications
- Support for hybrid, multi-cloud networks
  - Oracle Cloud, On-Premise, 3rd party Blockchains using Hyperledger Fabric



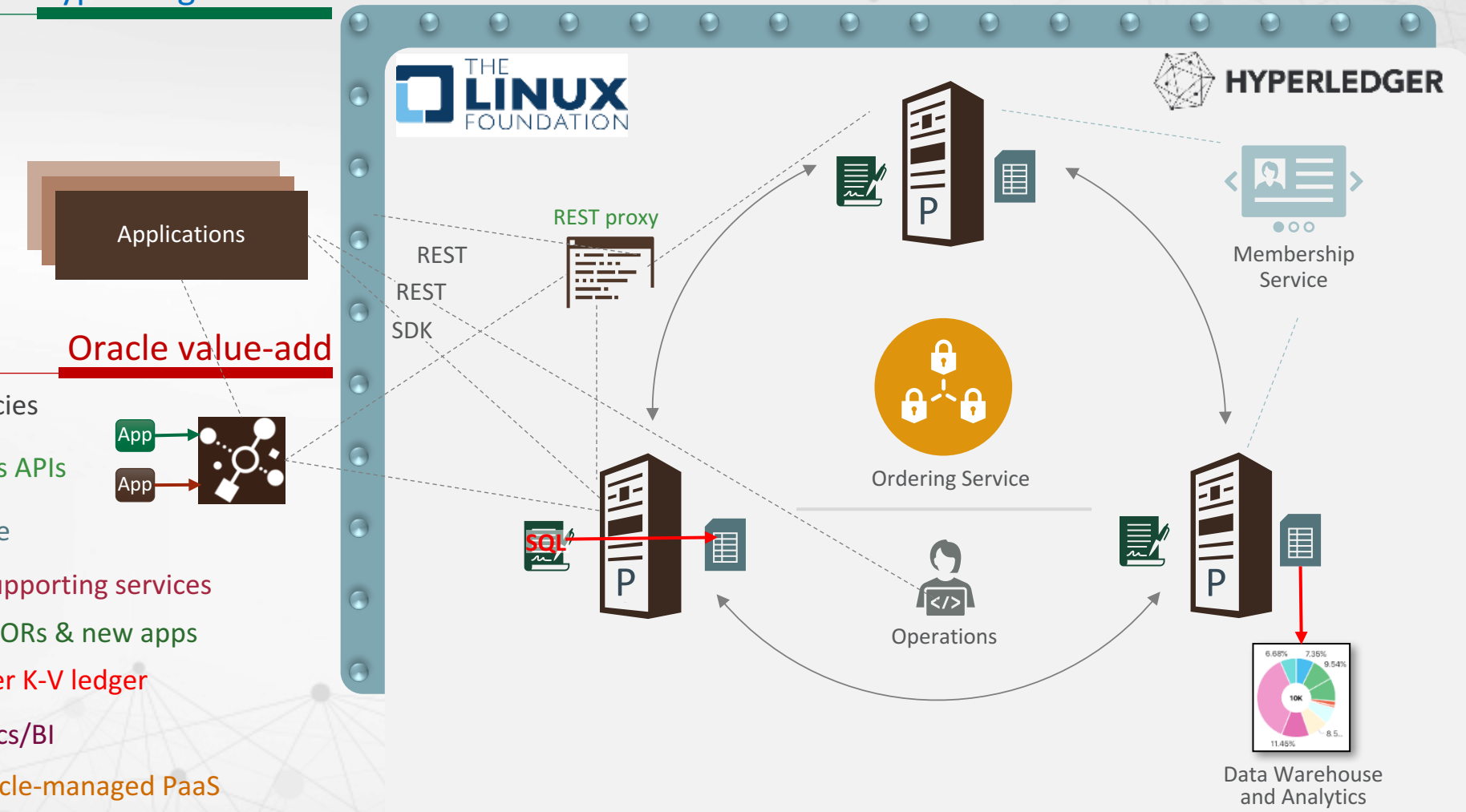
Community Verified Open Source + Oracle Value-Add

Hyperledger Fabric

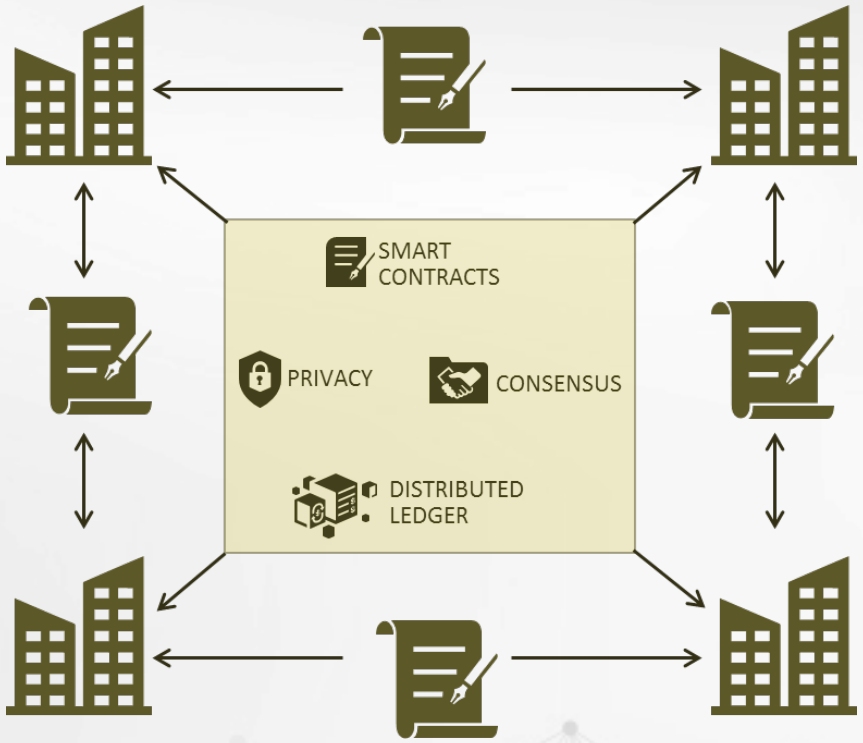
- Validating Nodes/ Peers
- Distributed Ledger (Single Version of Truth)
- Smart Contracts (aka Chaincode)
- Ordering Service
- Membership Service

Oracle value-add

- Pre-assembled Dependencies
- REST Proxy and Operations APIs
- Admin/Operations Console
- Integrated backplane of supporting services
- Rich integration tools for SORs & new apps
- SQL-based rich queries over K-V ledger
- Rich history DB for Analytics/BI
- Automated DevOps in Oracle-managed PaaS
- Flexible, global, hybrid, interoperable deployments – in Cloud and on Premises



Oracle Customer Momentum



150+
Customers

400+
Trials

Financial Services Use Cases

- Cross-border Funds Transfer
- International Loyalty Programs
- Asset & Securities Tokenization

Supply Chain Use Cases

- Food & Fashion Provenance, Conflict Minerals
- Maritime Shipping
- Cross-Border Trade Compliance

Public Sector Use Cases

- Customs & Excise Trade
- Tax Deducted at Source Certification
- HR Onboarding & Clearance

Heath Care and Pharma Use Cases

- Health Records Sharing
- Remote Patient Vitals Monitoring
- Anti-counterfeit drugs tracking

About ¼ of customers in production blockchain networks

Oracle Blockchain Use Case Examples (1/2)

PROVENANCE IN SUPPLY CHAIN

GeTS — **Trade documents registration and verification in ASEAN for Country of Origin certs & other documentation**

CANO — **Leather sourcing and shoemaker traceability for retail chain**

VOLVO, CATL, LG Chem — **Sustainable EV battery supply chain (Cobalt tracing)**

FOOD AUTHENTICITY & SUSTAINABILITY

Certified Origins — **Extra Virgin Italian Olive Oil**

THE WORLD BANK — Indonesia Palm Oil Sustainable Agriculture

ICBF.com — Farm-to-Fork beef provenance and cattle genomics tracking to reduce emissions in Ireland

INTERCOMPANY BILLING & SETTLEMENT

GE — Intercompany Ledger for Cross-ERP Billing Reconciliation & Settlement

LUXURY GOODS & COUNTERFEIT TRACEABILITY

EVERLEDGER — **Diamonds Traceability from Mining to Retail**

Beretta — A TRADITION OF EXCELLENCE SINCE 1526 — Premium Guns Certification & Tracking

Strides, Apollo HOSPITALS, NITI Aayog — Anti-counterfeit drugs tracking in distribution chain in India

TRANSPORTATION/LOGISTICS

CargoSmart — Global Shipping Business Network — **Maritime shipping documentation & logistic events tracking**

(6 carriers + 6 ports = ~50M shipments/yr.)

intelipost — Real-time pkg. delivery & tracking hand-offs in the delivery chain

ONLINE TRAINING & EDUCATION

正保远程教育 CDEL — **Diploma/Continuous Education certificate platform**

وادي طيبة TAIBAH VALLEY — **University Grade certificates**

Oracle Blockchain Use Case Examples (2/2)

FINANCIAL SERVICES

Cross-border Funds Transfer for Same Day Funds Availability

Asset Tokenization in Securities Services for Multiple Asset Classes

Multiple Banks & Financial Groups

e-KYC Solution for Customers Onboarding & Ongoing Updates

A European Bank

E-Notary Solution for Registering Open API Requests/Responses

Brokerage Window Transfers b/w Funds and Self-Directed Accounts

Smart Insurance – Parametric Insurance Blockchain Across Banks, Insurers, Sellers, and Re-insurers

with Insurance & Banking Consortium

GOVERNMENT/PUBLIC SERVICES

Singapore DSTA – Civilian visitors identity tracking & access granting

National police criminal investigations evidence chain of custody

Asylum Case Management & Identity Sharing in Europe

HR Onboarding & clearance process documents tracking

A Customs Service in SE Asia

Export/Import certificates tracking and provenance matching

A National Tax Dep't in Major Asian Country

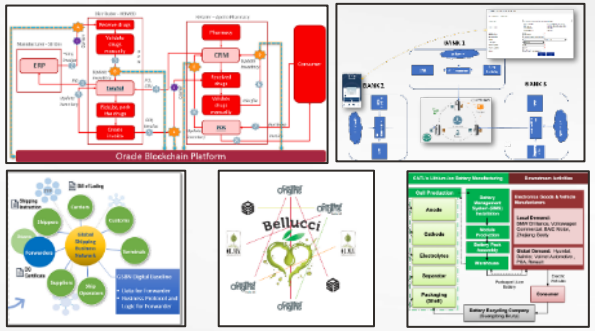
Tracking tax withholdings and relevant limits, reporting, etc.

HEALTHCARE

Self-Sovereign, Patient-Driven Electronic Healthcare Records Sharing

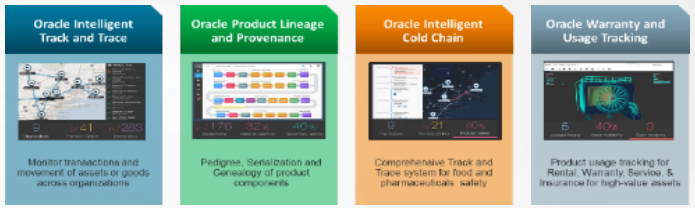
Consumer-driven Healthcare Providers & Payers Ecosystem

Growing Oracle and Partner Solutions Ecosystem



Custom Apps Prototyped by Oracle Solution Engineering

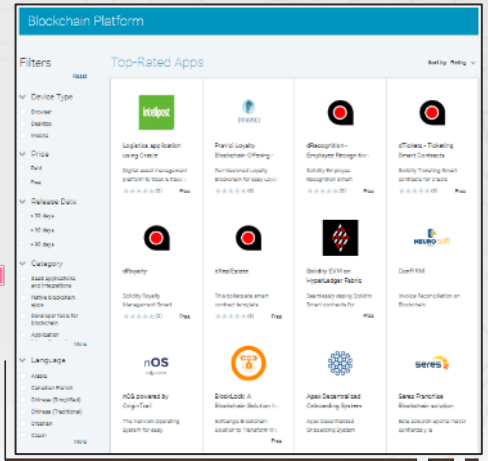
Retail | Data Cloud | Health Insurance | Health Science | Mobility



Oracle SaaS
Oracle Intelligent Track and Trace
Vertical GBU Apps

Cognizant | Tech Mahindra | KPMG | accenture | pwc | Deloitte. | Infosys

SI Solutions and Accelerators



ISV Applications

Consensus | **Smart Contracts** | **Oracle Blockchain Platform** | **Distributed Ledger** | **Confidentiality**

App Integrations | Data Repository | Off-chain Sync | DevOps | Governance | Access Control | Interoperability

Oracle Cloud Infrastructure

On-Premises Deployment

Does smart contract need SQL?

- Support
  - SQL is very popular in today's enterprise IT systems
  - Save (chaincode) developer efforts to let the DB handle the transactions consistency
- Against
  - SQL is not good in performance comparing with key-value
  - Blockchain contracts should be kept as simple as possible for security considerations

Does Enterprise Blockchain need SQL query?

- It is a good option to have SQL capability in smart contract
- After decades, NoSQL is trying to become the same as SQL
- Oracle Blockchain Platform supports SQL rich data queries against state DB using the open-source BerkeleyDB
  - The performance is good to support >2K TPS!
  - Enterprise customers like it! Save efforts in developing the smart contracts.

```
SELECT … FROM <state> st WHERE json_extract(valueJson, '$.docType') = 'vehiclePart'
AND json_extract(valueJson, '$.owner') = 'Detroit Auto' ORDER BY
json_extract(valueJson, '$.owner')
```

vs. 20-40 LOCs using CouchDB Query Language and Go/node code

```
SELECT AVG(aCount) FROM (SELECT COUNT(*) AS aCount FROM <state> st
GROUP BY json_extract(st.valueJson, '$.owner'))
```

vs. N GetState() calls from Chaincode to Peer resulting in N network hops and a huge RWSet

Is it necessary to backup/recover a node?

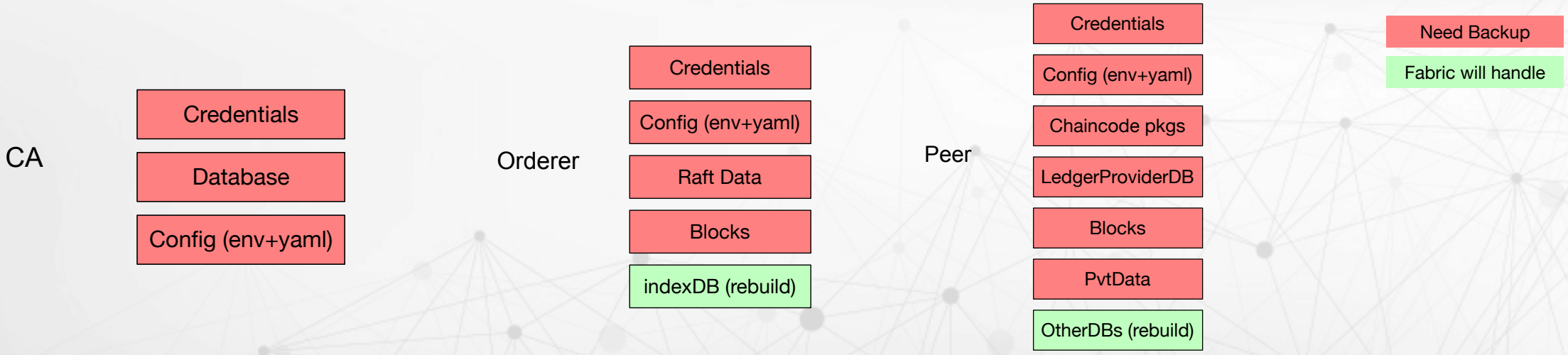
- Support
  - Useful to keep service resilient from corruption
  - Useful when you want to migrate a node
- Against
  - Blockchain is a distributed system, every node is backed up with each other
  - Blockchain node is easy to create

Is it necessary to backup/recover a node?

- In theory, single blockchain node does not need to be resilient from the entire network system
- In fact, it is very unpractical to sync up data for a new node!
  - Network I/O
  - Disk I/O
  - World State and History DB rebuilding
  - Ledger with 1M transactions may require 10s of mins
- We need to develop tools for data backup/recovery

What data should be backed up?

- In fact, most data must be backed up!
- Rebuilding DBs consumes lots of time (and CPU)!



Ledger Checkpoint and Pruning/Archiving?

- Support
  - Ability to join a peer to a channel from a checkpointed state rather than from genesis block, so that latest channel configuration can be used
  - Reduce the amount of time to join a new peer to a channel
  - Reduce the amount of storage space required for a channel
  - Help in performance and storage
- Against
  - Storage is cheap
  - More complicated to query transactions without full ledger

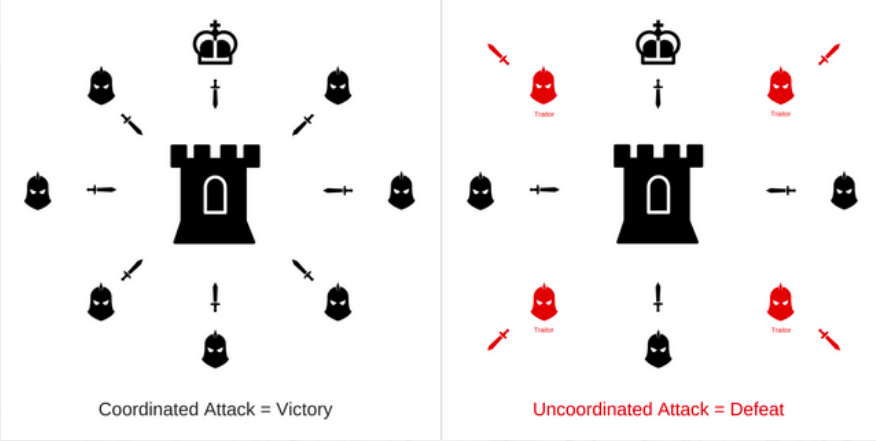
Ledger Checkpoint and Pruning/Archiving?

- It has been discussed for quite a while, since FAB-106 (Aug 15, 2016)
- We believe this is mandatory and very common for large volume users at 1000s of TPS
- Potential solutions before FAB-106 is done
  - Store block files externally, which are used only for block/tx query

Byzantine Fault Tolerant Consensus

- Support
  - BFT is more trustable than CFT
  - Numbers of blockchains have supported BFT

- Against
  - It is not necessary in enterprise scenarios because every member will be audited and identified;
  - BFT has poor performance
  - BFT can handle less failures than CFT



Byzantine Fault Tolerant Consensus

- It is not a common requirements for Enterprise blockchain, but it can be a security concern for specific scenario, e.g., finance

- Enterprise blockchain should leverage latest proven consensus algorithm from academia, and there is some progress!

Latest BFT work (1/4)

- Tendermint: Byzantine Fault Tolerance in the Age of Blockchains - unpublished 2016
  - By Ethan Buchman (University of Guelph, Canada), and is adopted by several public chains
  - 1K TPS with 1K size block

  - Simplified PBFT with blockchain data structure
  - Selected validator for consensus, and validator take the proposer role in sequence
  - View change is achieved by virtual empty block

Latest BFT work (2/4)

- Algorand: Scaling Byzantine Agreements for Cryptocurrencies - SOSP 2018
  - By MIT CSAIL
  - 30x bitcoin TPS, with simulating 50K users at 1K VMs.

  - Only part nodes (committee members) participant the consensus
  - Use Verifiable Random Function (VRF) to choose committee member securely: <proof, priority, block>
    - hash, pi = VRF_sk(seed || role)

  - Strong sync requirement: most messages should arrive with acceptable latency. In worst cases, may require 10+ rounds.
  - Only suitable for crypto coins scenario

Latest BFT work (3/4)

- Mir-BFT: High-Throughput BFT for Blockchains - unpublished 2019
  - By IBM Research Zurich
  - 23K TPS performance in WAN with 100+ nodes

  - Based on PBFT model, allows multiple concurrent leaders to propose batches of requests in parallel (still 1 primary for each epoch)
  - Partitions the request hash space across replicas

Latest BFT work (4/4)

- HotStuff: BFT Consensus with Linearity and Responsiveness - PODC 2019
  - By VMWare Research, and published at PODC 2019, mentioned in FB's Libra whitepaper
  - Partially synchronous model
  - Based on PBFT model, use primary to be the center of all communications (to simplify processing)
  - Combine view change operation into normal request consensus operation
  - 2 phase confirmation → 3 phase confirmation after the first prepare phase
    - pre-commit, commit, decide
  - Use threshold signature for voting, reducing messages
  - Weaker fault tolerance at primary node

BFT work in Hyperledger Fabric

- v0.6: SBFT (batched PBFT)
  - low performance with bad scalability
  - bugs that some node may stop
- v1.0 and v1.3: non-official bft-SMART Library support (2017-09-24)
  - Joao Sousa and Alysson Bessani (Universidade de Lisboa, Portugal), Marko Vukolic (IBM Zurich Research)
  - Java based plugin with HLF non-officially
  - There are still lots of issues, esp. relate to channel configurations.
- There is a ongoing work to implement a Go base bft-SMART consensus for HLF

Governance Capability

- Support
  - The lack of governance brings big challenges for real usage, e.g., no one knows what channels exist in the network, what is the ordering service address, and which channel I can join
  - Blockchain itself is a multi-party transaction system, and governing is a fundamental requirement
- Against
  - Blockchain is decentralized, users can agree everything offline.

Governance Capability

- It is very important to bring the governance capability into enterprise blockchain.
- Agreeing offline across organizations is untrustworthy in theory, and very inconvenient in practice

- Potential solutions
  - Persist transactions and votes on a specific governance channel to commit all governance-related info
    - We already have the system channel for governing ordering services
  - System chaincode to track proposals, manage vote tabulation, evaluate against policy requirements
    - GSCC: Governance system chaincode
  - External distributed governing service by vendors

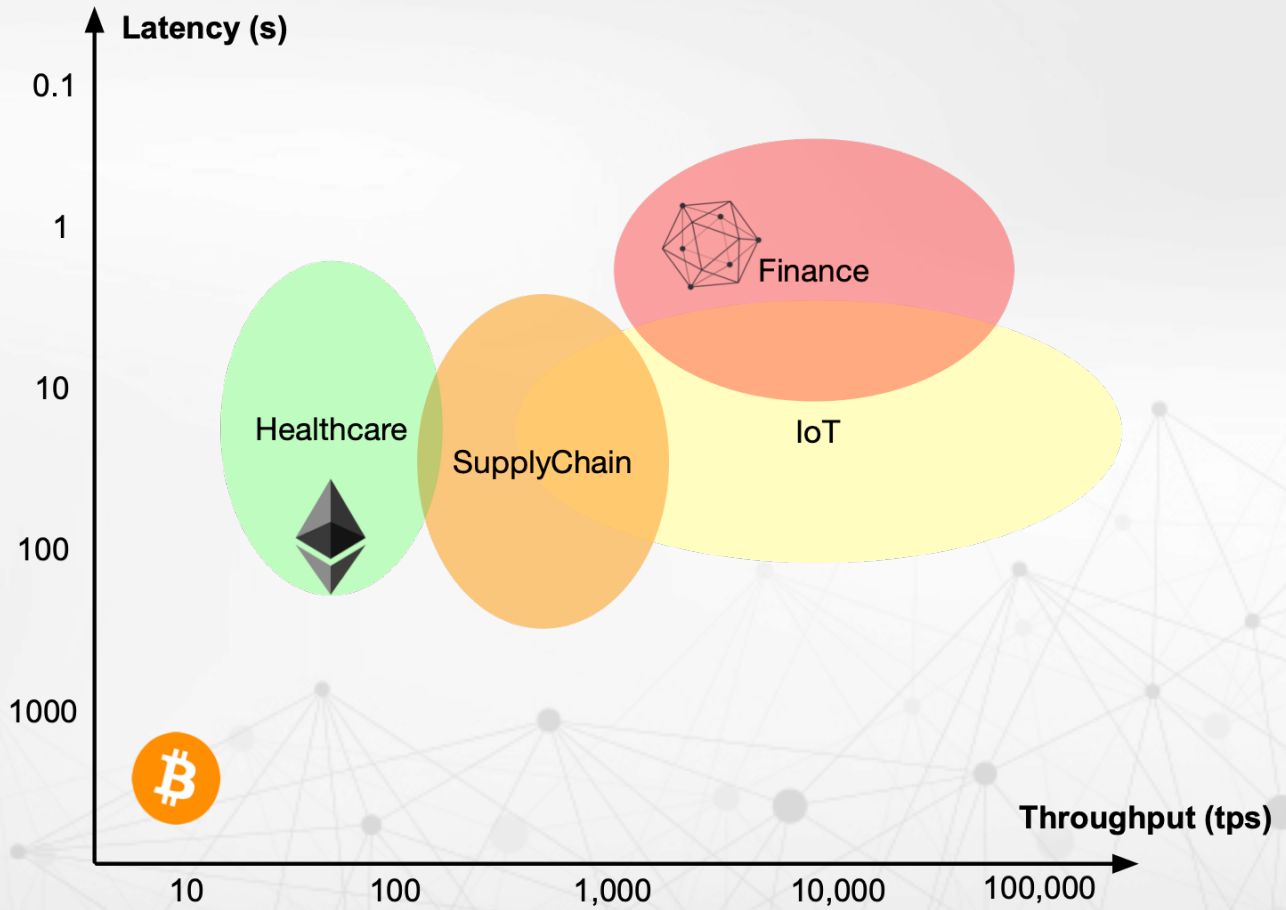
Governance System Chaincode

- We already implement voting for chaincode lifecycle in Fabric 2.0
  - Organization can vote for the definition of chaincode in the channel (using implicit collection feature)
- Extends to "organization can vote for anything"
  - Who can join a channel
  - What ordering service can be seen by which member
  - Who can modify a channel configuration
  - Etc.
- Part of the functionalities have been verified by the Fabric interop team

Do customers really care about performance?

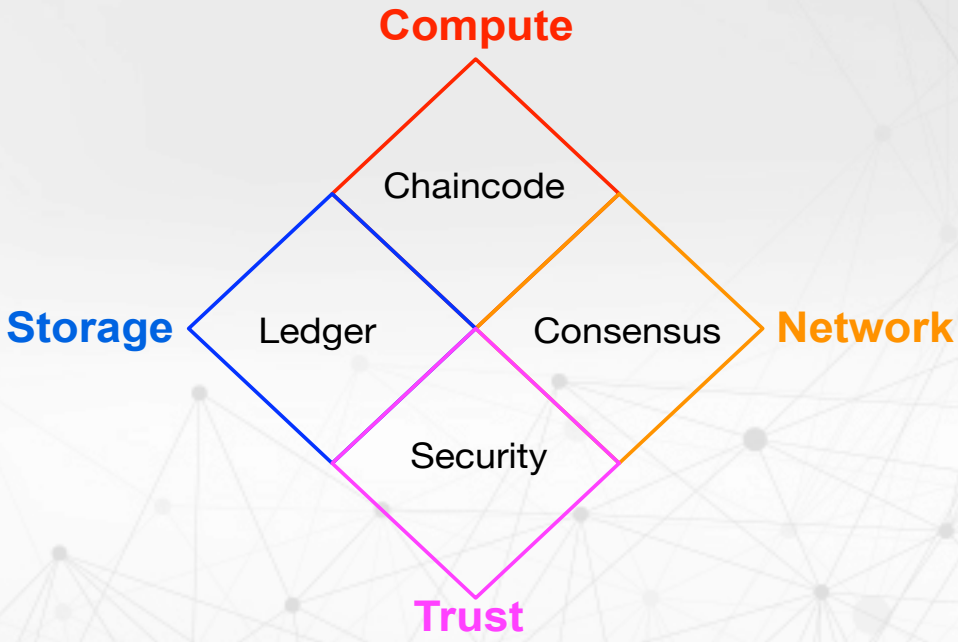
- Support
  - Yes, every customers will often ask performance number, i.e., TPS
  - 1K, 10K, 100K… papers are published
- Against
  - Not all users really understand performance
    - throughput
    - latency
    - scale
    - hardware configuration
    - application layer vs platform layer
  - Few real scenarios needs 1K TPS

Performance depends on scenario



The ART of Performance optimization

- What performance are you talking about?
- What is the goal for next 5 years?
- Performance is a systematic issue!



For performance, most people ignored…

- Performance will degrade with ledger data accumulation
- Why?
  - For each transaction, blockchain node needs to check whether it is existed already by the txId. However, more and more transactions accumulate

```
/.../
if _, err = e.Support.GetTransactionByID(up.ChannelHeader.ChannelId, up.ChannelHeader.TxId); err == nil {
    /.../
    e.Metrics.DuplicateTxsFailure.With(meterLabels...).Add( delta: 1)
    return errors.Errorf( format: "duplicate transaction found [%s]. Creator [%x]", up.ChannelHeader.TxId,
up.SignatureHeader.Creator)
}
```

- Solution? Not possible with changing to better DB
  - The txId generation algorithm needs to be changed by adding timestamp

Privacy Protection

- Support
  - Data privacy is essential requirement for person
  - Data is key to business
  - Security policy alignment

- Against
  - Blockchain is to help share data among members
  - No sensitive data should be put on chain
  - All solutions have trade-off

Privacy Protection

- Privacy has been an important bottleneck in blockchain scenario
  - Customers have to use the on-prem version of blockchain instead of cloud ones
  - Customers have to use proprietary blockchains instead of open-source ones
- PrivateDB Collection can help, but not enough
  - implicit collection is the fundament for flexible combination of members
  - Hashed result still got recorded in the ledger
- Oracle Blockchain Platform integrates the fine-grain Access Control Lists in smart contracts
- If you care about data privacy seriously, encrypt it before putting on the chain

Inter-network Operations

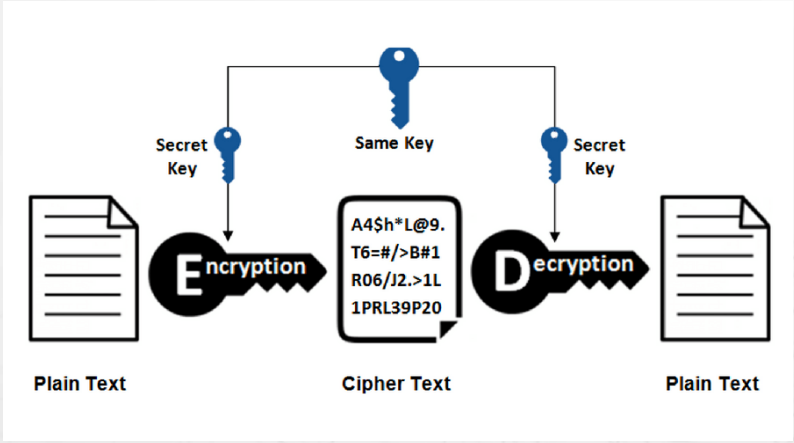
- Support
  - Allow using heterogeneous blockchains
  - Help multiple vendors connect each other
- Against
  - Enterprise consortium is usually not very large (less than 30 members), and focuses on the same business scenario

Inter-network operations

- What does inter-network operation mean?
  - Read data from multiple ledgers
  - Update data on multiple ledgers with consistency
  - Achieve consensus using nodes across different blockchain stacks
- Many platforms are build on top of Hyperledger, Ethereum, Quorum
- No easy inter-network solutions, most practical solutions are based on external data gateway – centralized intermediary

Pluggable Crypto Implementations

- Support
  - More flexible to adopt different crypto standards
  - Diversity if the international standard is flawed
  - Security policy compliance
- Against
  - Should encourage to adopt the international standards
  - More standards will expose more security risks



Pluggable Crypto Implementations

- It is difficult for HLF to have a true pluggable crypto components due to the Go based library
- Numbers of users in Asia, Russia (and EU potentially) need to enhance the blockchain to align with the regional standards
- FAB-5496 (July 27, 2017) is created to track this

Auditing Capability

- Support
  - Enterprise needs auditing for charging, access control, etc.
  - Security policy compliance
- Against
  - Auditing is already built in the blockchain with the ledger history
  - Auditing can be implemented out side of blockchain
  - Can leverage existing statistics functionalities

Auditing Capability

- Auditing is a highly demanded in finance industry
- Auditing is different from logging, operational statistics, tracking

- It is convenient to provide some auditing APIs from HLF core
  - Currently can use the statistic metrics + logging

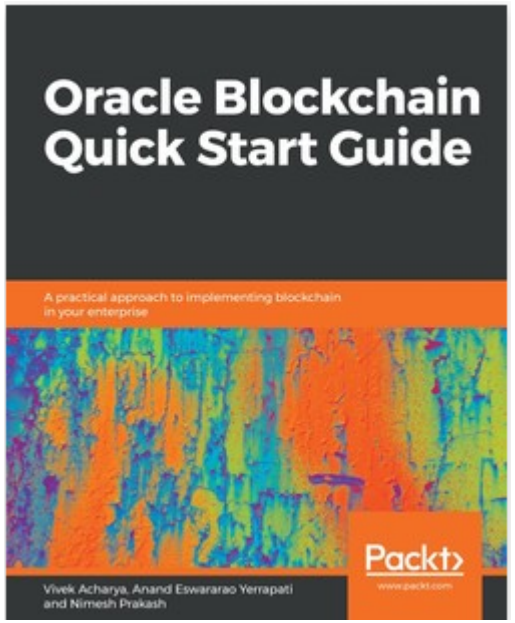
- Tracked in FAB-105

Questions and Answers

HYPERLEDGER GLOBAL FORUM PHOENIX, AZ | MARCH 3-6, 2020

- Welcome to try Oracle Blockchain for free
  - Managed cloud PaaS: https://www.oracle.com/application-development/cloud-services/blockchain-platform/
  - On-premises Enterprise Edition: https://www.oracle.com/database/technologies/blockchain-platform-enterprise-edition.html
- Oracle Blockchain Developer eBook
  - https://developer.oracle.com/blockchain
- A book is publishing soon to introduce enterprise blockchain technologies based on Hyperledger Fabric v2.x

Vivek Acharya, Nimesh Prakash, Anand Eswararao Yerrapati



https://www.oreilly.com/library/view/oracle-blockchain-quick/9781789804164/

Oracle Blockchain Platform Focus Areas

Development

- **On-chain fine-grained access control**
- **Trusted Data Source** ("oracle") framework for including external data in blockchain transactions
- **Chaincode Development Aids**
  - IDE/Web-based dev/test env
  - Blockchain data modeler/code gen
  - CI/CD for automated deployment
- **Token-based chaincode and higher level APIs for issuing and exchange**
- Execution environment for Ethereum smart-contracts on Fabric peers
- API-driven abstraction models for common application patterns and library of related chaincode building blocks
- Rules engine-based chaincode execution for business user friendly chaincode specification

Operations

- **Governance for Consortia networks**
  - Policy-based with Voting mechanism
  - Automated onboarding via member voting
  - Policies for channel access, chaincode deployment, etc.
- **Consortium-wide management & monitoring**
  - Blockchain network dashboard for monitoring across multiple instances
  - Extended directory service
  - Chaincode deployment across organizations
- Simplified member on-boarding process
- Access to world state DB from console
- Dynamic creation of custom indices for world state DB from console
- Admin events/log subscription API
- **Ledger Checkpointing/Pruning**
- Integration with AI/ML tooling for autonomous diagnose/resolution of common issues

Infrastructure

- **Enhanced OBP Enterprise Edition (On-Premise)**
  - Enhanced security integration using MS AD/IdM, KMS, HSM, etc.
  - Adoption of RAFT ordering
  - Migration from open source HLF
- **OCI gen2 Architecture cloud service**
  - Scale up/down, scale out/in
  - Enhanced integrations for HSM/KMS, IDMs
  - Deployment across availability domains/data centers
  - Advanced container management
  - Adoption of RAFT ordering
  - Migration utility from Kafka instances
- **Interoperability with other blockchain networks**
  - Fabric to Fabric interoperability for cross-network transactions
  - Fabric to Stellar, Ethereum, Corda
- **Byzantine Fault-tolerant Ordering**
  - Deterministic BFT implementation
  - RAFT evolution based on latest research