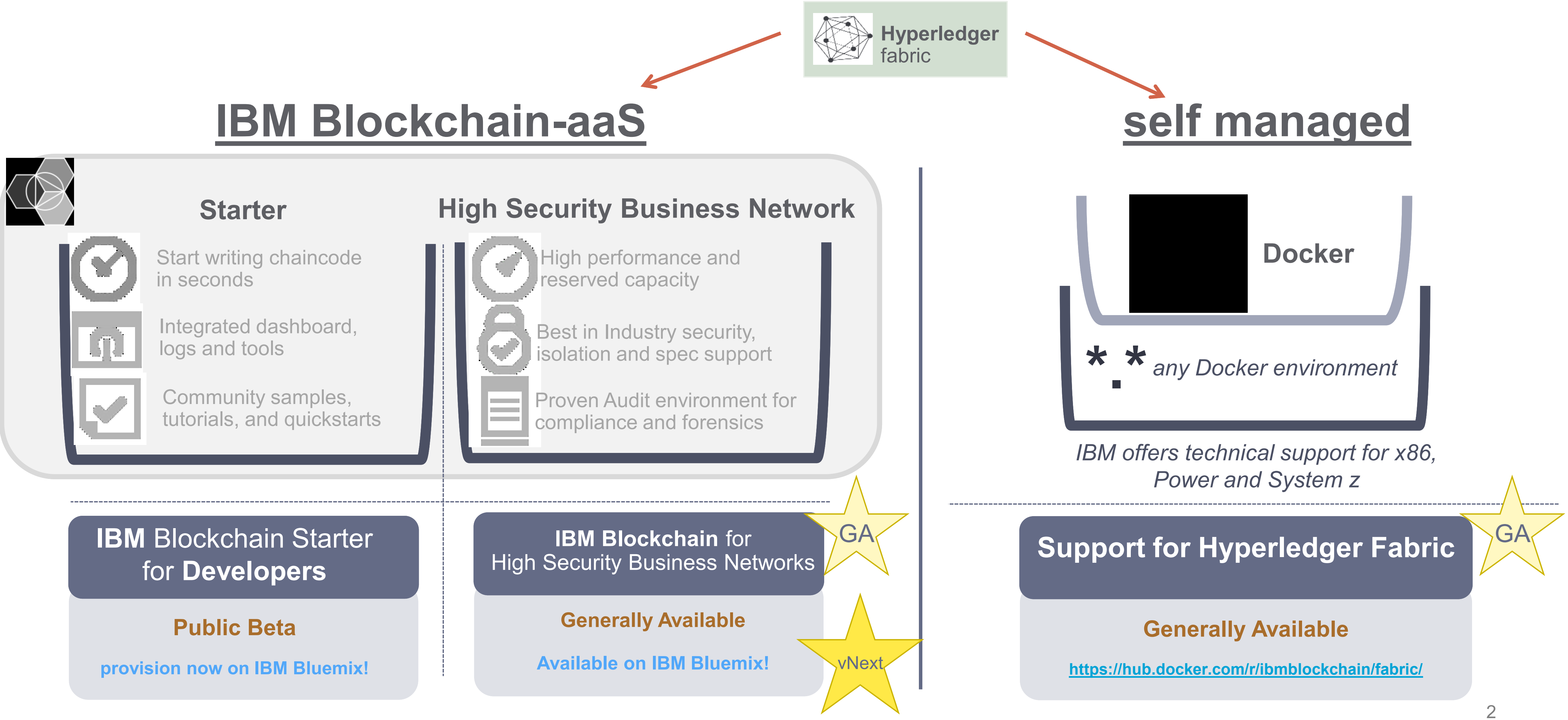
IBM Blockchain

High Secure
Business Network

Angel Nunez Mencias

May 16, 2017

IBM Blockchain Offerings



Hyperledger fabric

IBM Blockchain-aaS

Starter

Start writing chaincode in seconds

Integrated dashboard, logs and tools

Community samples, tutorials, and quickstarts

High Security Business Network

High performance and reserved capacity

Best in Industry security, isolation and spec support

Proven Audit environment for compliance and forensics

IBM Blockchain Starter for **Developers**

Public Beta

provision now on IBM Bluemix!

IBM Blockchain for High Security Business Networks

GA

Generally Available

Available on IBM Bluemix!

vNext

self managed

Docker

. *any Docker environment*

IBM offers technical support for x86, Power and System z

Support for Hyperledger Fabric

GA

Generally Available

https://hub.docker.com/r/ibmblockchain/fabric/

HSBN on Fabric 1.0—Six Keys

1. It enables **Distributed Business Networks**

Bootstrap a working Enterprise grade network in minutes

2. It is a **managed Blockchain-aaS**

A hardened config dynamically assembled to best practice

Built in monitoring and support

Easy fabric lifecycle management

3. It's built on **Hyperledger Fabric 1.0**

Channels for isolation and scoping private/public participation

Built in Identity and membership services

Scalable and loosely coupled transactions

Open, pluggable and extensible

HSBN on Fabric 1.0—Six Keys

4. It includes **Distributed Governance tooling**

Policy editor to set Democratic policies for lifecycle tasks

Workflow tools such as signature collection

5. It runs on a hardened, **high security stack**

Integrated HSM with the highest FIPS level compliance

Locked down Virtual Appliance with no privileged access

Secure boot sequence for tamper evident detection and no malware

6. It’s compute is **optimized for performance**

Fastest Linux compute and high speed network

Instruction set optimized including crypto accelerators

IBM Blockchain—aaS Evolution

	GA Today	*vNext—March 20 Beta*
What	**Enterprise Sandbox** **Fabric 0.6**	**Distributed Business Networks** **Fabric 1.0**
Why	**Private Blockchain Network** • **for blockchain exploration and pilots**	**Managed Blockchain—aaS** • **Self-service production grade network in minutes** • **Distributed ownership and Elastic Membership**
Where	US-NY, EU-LON, **JA-TOK***, **CA-TOR***	US-NY, EU-LON, JA-TOK, CA-TOR, **EU-FFT***, **BR-SPO*, SG-SGP***

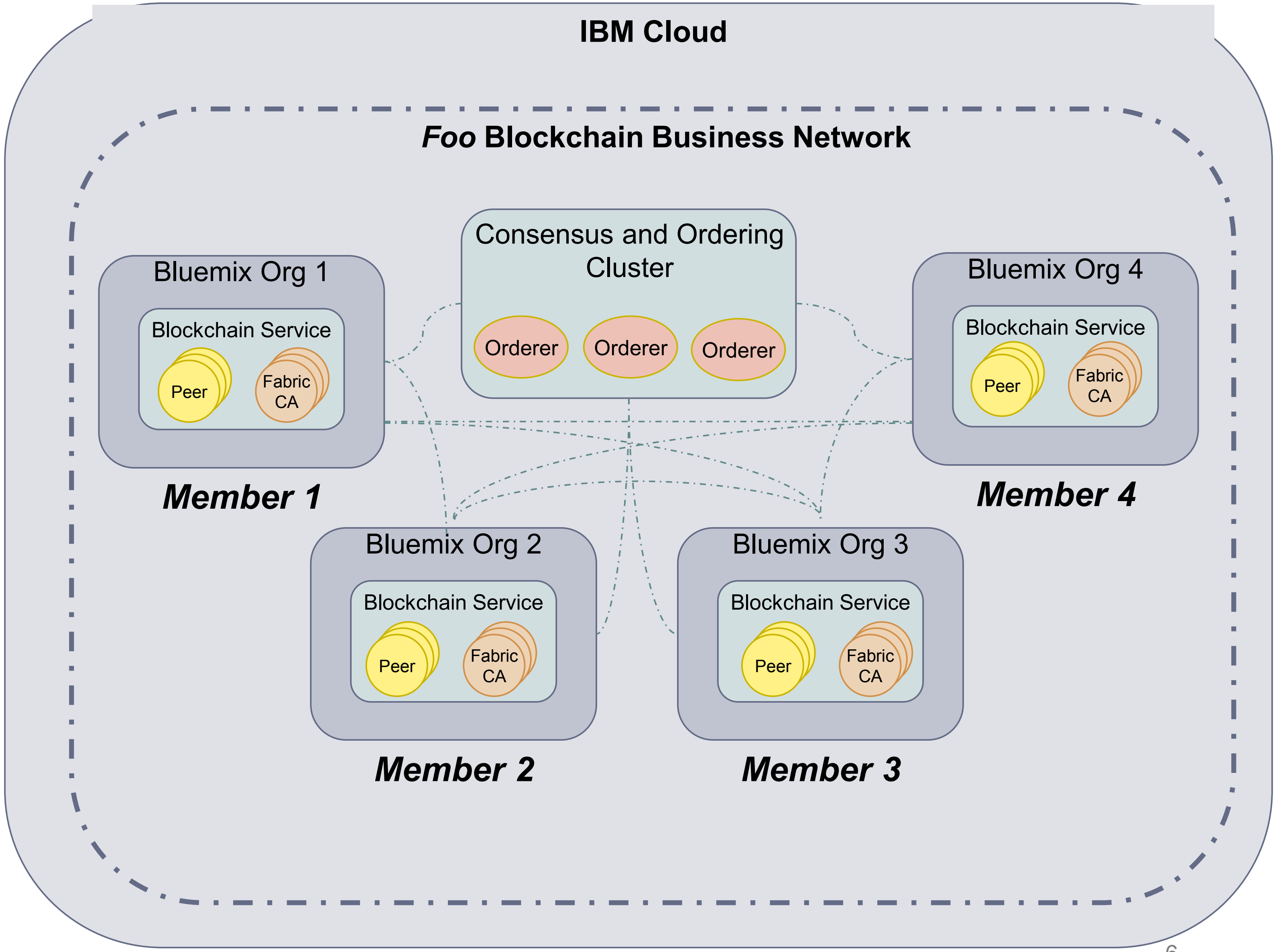
How	Pay for a Bluemix Reserved Instance:
	for a dedicated 4 peer network
		Pay as You Go for your resources:
		Peers {S,M,L}
		Certificate Authority
		Compute {Shared, Dedicated}

IBM Blockchain-aaS Network Diagram

Fabric 1.0 Beta

Distributed Business Networks

- Blockchain Network comprised of multiple members
- Each member provisions peers and resources inside their Bluemix environment
- Members pay for their resources
- Consensus cluster sits at the network level and is administered democratically by members in an admin group
- Changes to the network occur democratically according to defined Governance Policies

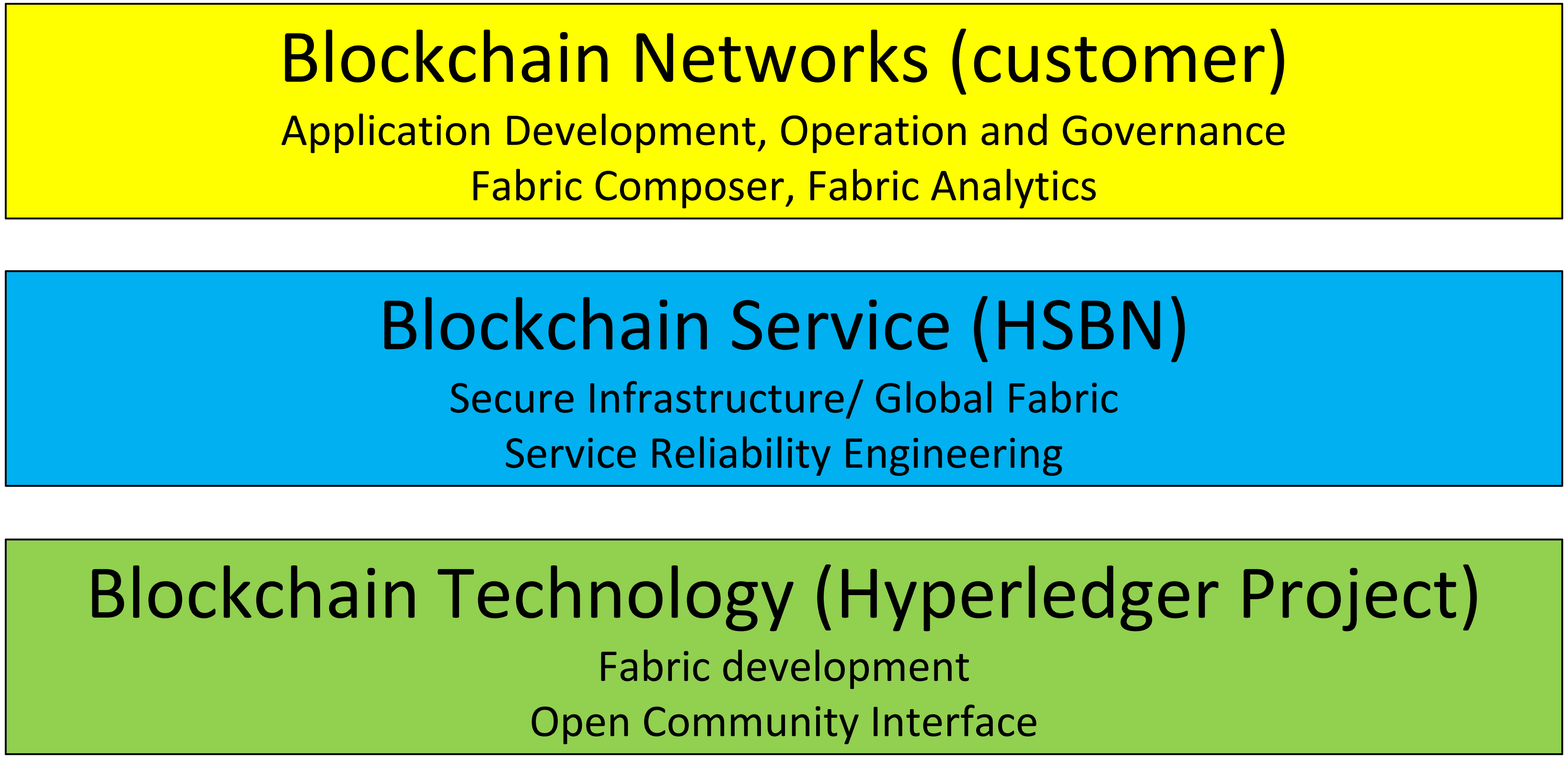


Links

- Production (limited Beta)
  - **https://console.stage1.ng.bluemix.net/catalog/services/blockchain**
- Staging (Open for all IBMers)
  - **https://console.ng.bluemix.net/catalog/services/blockchain**
- Marbles (Demo app)
  - https://github.com/IBM-Blockchain/marbles

Security Deep Dive

Why HSBN



Blockchain Networks (customer)

Application Development, Operation and Governance

Fabric Composer, Fabric Analytics

Blockchain Service (HSBN)

Secure Infrastructure/ Global Fabric

Service Reliability Engineering

Blockchain Technology (Hyperledger Project)

Fabric development

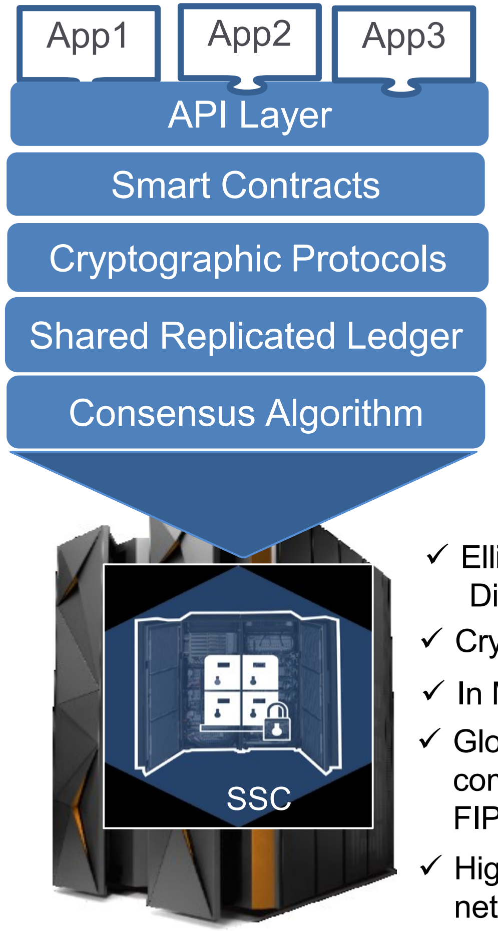
Open Community Interface

- Reduced Risk
- Lower Cost to Deliver
- Higher Security Systems
- Faster Access to new capability
- IBM’s Strategic Delivery Platform for the Hyperledger fabrics
- Support for Hybrid Model

IBM Blockchain on Bluemix Service Plans

Plan Features	Starter (BETA)	HSBN (GA)
Deploy a four node (peer) blockchain network and Certificate Authority	✓	✓
Deploy chain code (business logic) to the network	✓	✓
Monitor network heath by viewing the status of peers and chain code	✓	✓
Monitor network traffic on the blockchain Analytics Dashboard	✓	✓
Use Node.js and the SDK to build blockchain business applications	✓	✓
Execute the blockchain fabric and business network within in a Secure Service Container: traditional O/S interfaces not exposed to admins, prevents misuse, insertion of malware		✓
Get security capability: cryptographic keys are stored in the HSM, and certified to the highest security level, FIPs 140-2 Level 4		✓
Execute cryptographic operations such as hashing, encryption, and digital signature on accelerators		✓
Communicate between peers over a high-speed, internal network where communications remain within the Secure Services Container, preventing data leakage		✓

- Benefit from an Enterprise Platform



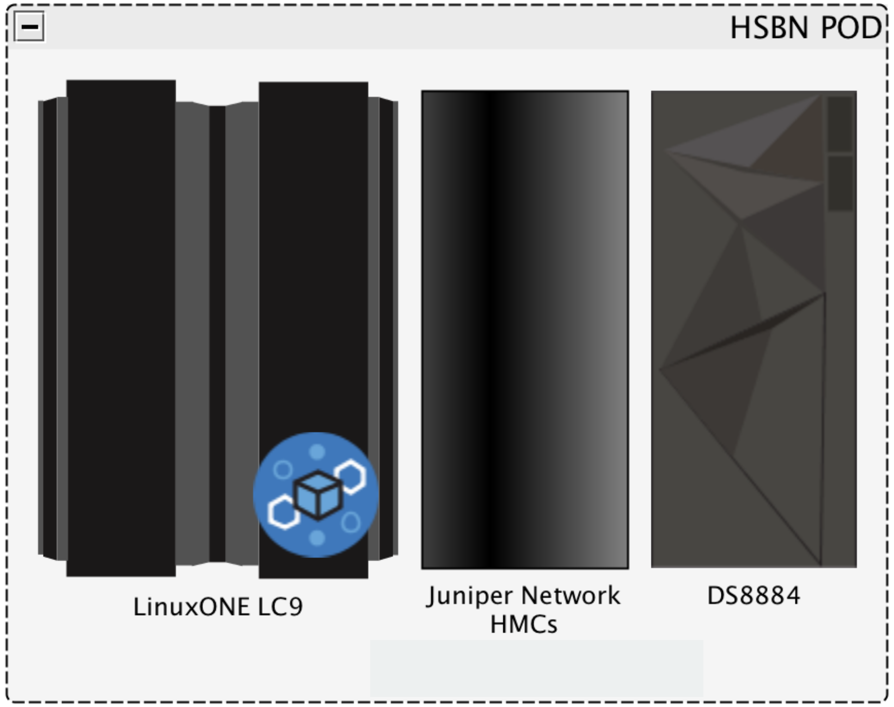
- ✓ Elliptical Curve Digital Signatures
- ✓ Crypto accelerators
- ✓ In Memory (10 TB)
- ✓ Global Security compliance PKCS11, FIPS 140-2 , Level 4
- ✓ High-speed, internal network

High Security Business Network
runs in the Secure Service Container

HSBN Co-location Pod

System Support Rack:
- 2x Juniper QFX 5100 Switches
- 2x2x16 IBM Global Console Mgr

LinuxOne – Mod LC 9:
- 4 Drawers, 129 IFLs
- 6 TB Memory
- 16 x OSA cards (mix)
- 10x16GB Ficon Express
- 4 x Crypto 5S
- Internal Battery Feature
- 2 x Rack Mounted HMC



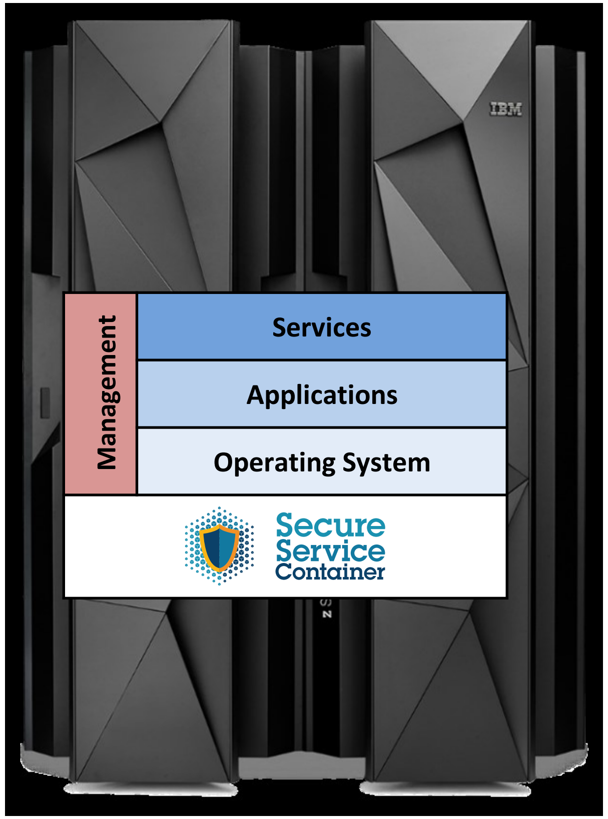
DS 8884 – Mod 984:
- 128GB Proc. Memory
- 4 x 4port 16GB Ficon
- 2.4TB Flash
- 150TB of HDD
- CSM for Back/Restore Flashing

IBM Secure Services Container

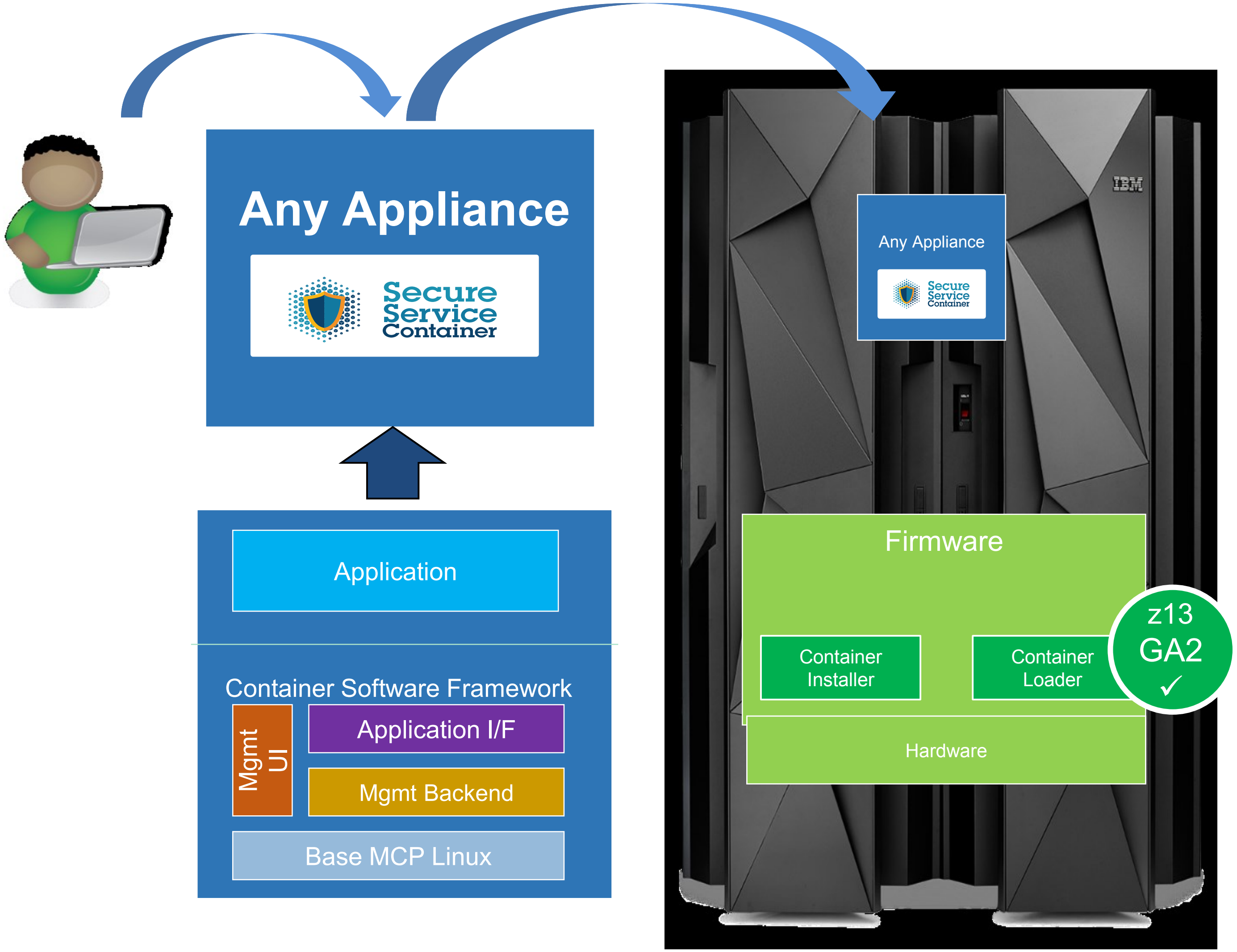
Secure Service Container

The Base Infrastructure to Host and Build Software Appliances

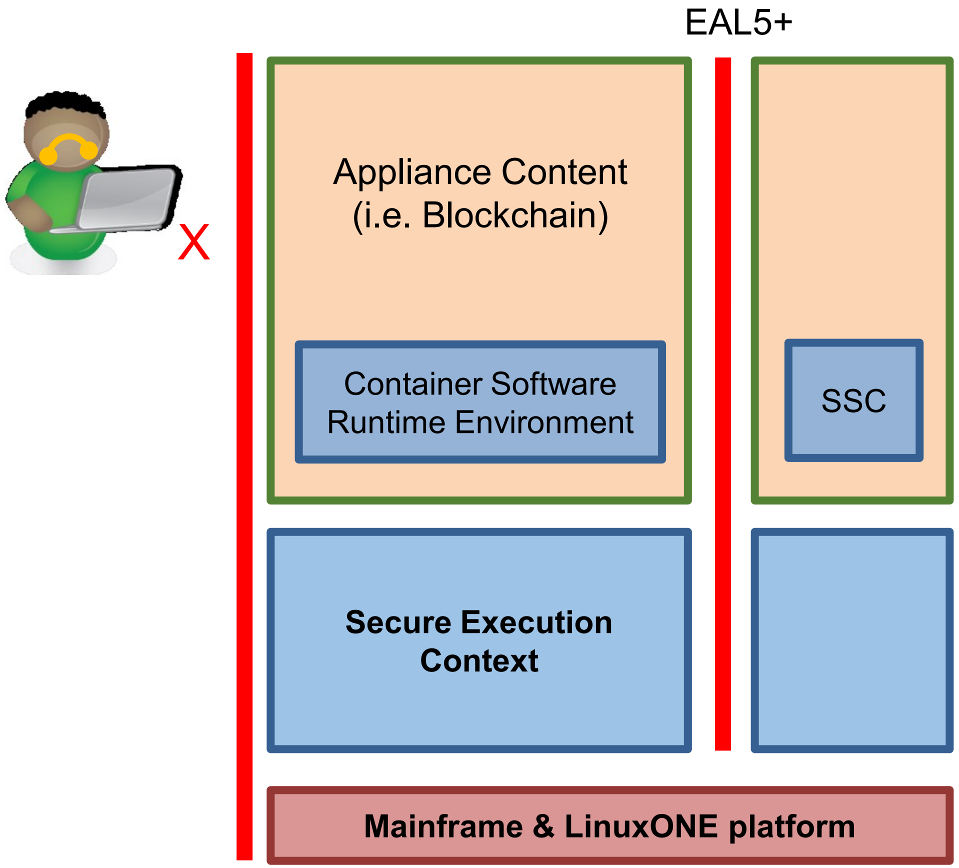
- ❑ **Easy Installation:** Provides simplified mechanism for fast deployment and management of appliance-based solutions
  - O/S, Application, Services packaged as single solution
- ❑ **Highly consumable:** Manage the appliance through Remote, RESTful, API's and web interfaces
- ❑ **Secure Runtime:** Provides tamper protection during appliance installation and runtime
- ❑ **Data Privacy:** Ensures confidentiality of data and code running within the Appliance – both in-flight and at rest
- ❑ **A Software Distribution**: Enables Appliances to be delivered via software distribution channels vs hardware – including maintenance



Secure Service Container Framework Overview



Secure Service Container Protection



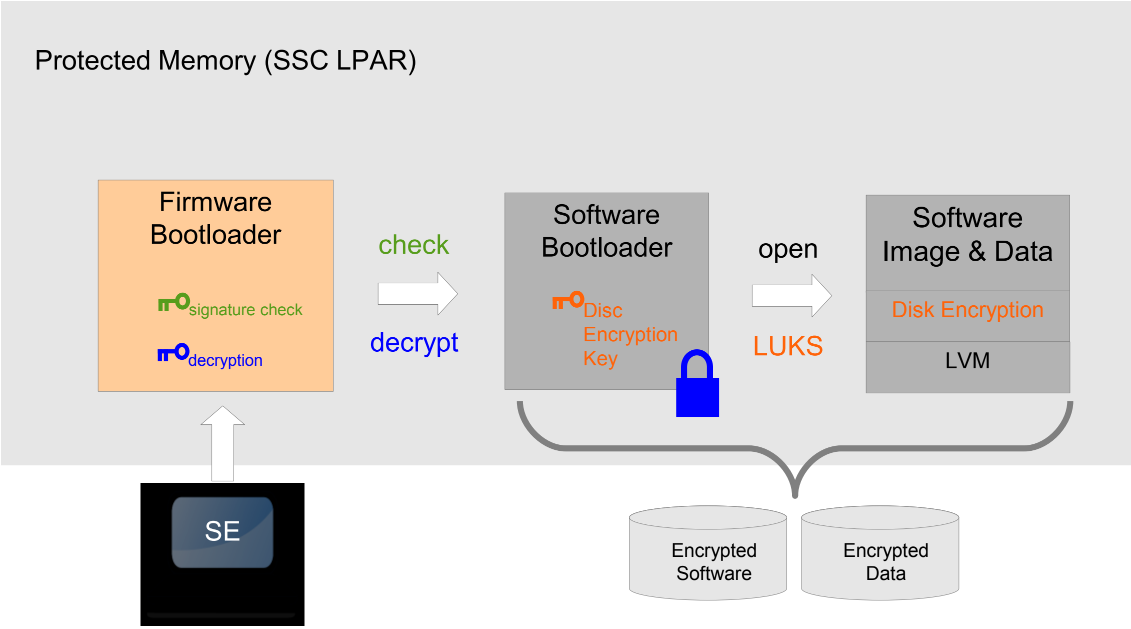
❑ No system admin access

- Once the appliance image is built, OS access (ssh) is not possible
  - Only Remote APIs available
- Memory access disabled
- Encrypted disk
- Debug data (dumps) encrypted

❑ Strong isolation between container instances

- Based on LinuxONE EAL5+ protection profile
- Requires dedicated HW

Encrypted, Signed, Tamper Resistant, Protected



Boot sequence

1. Firmware bootloader is loaded in memory

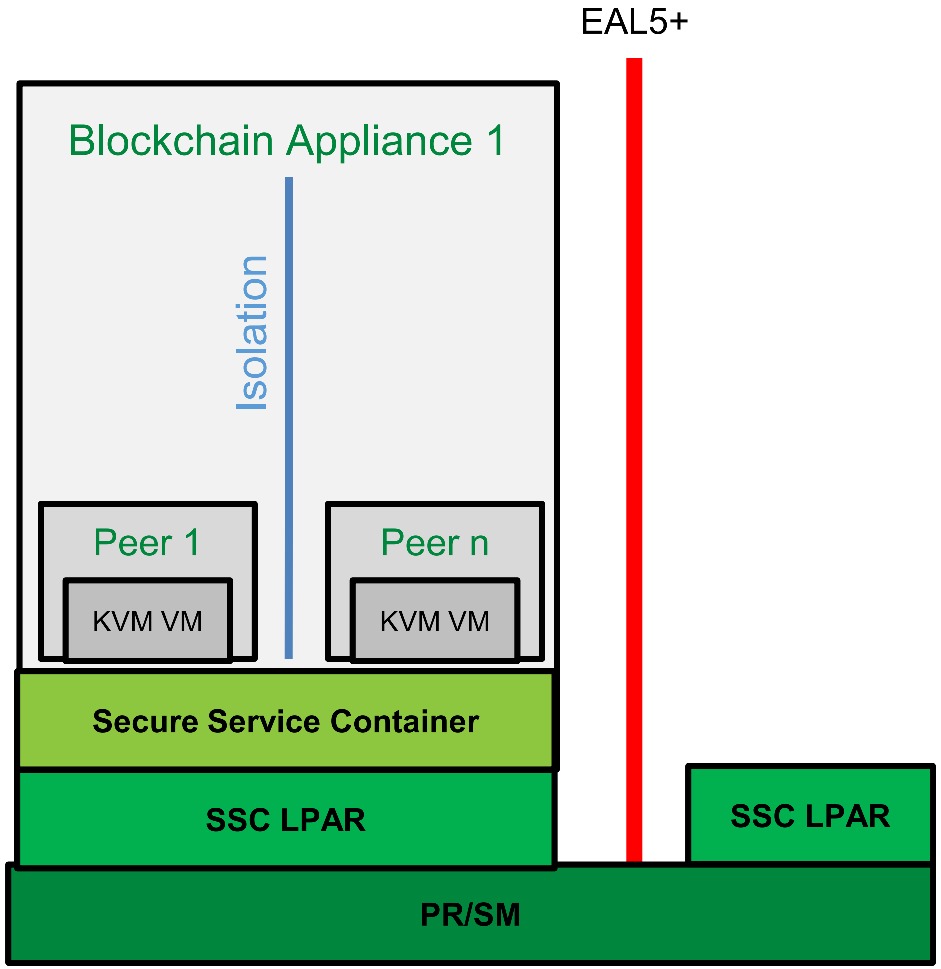
2. Firmware loads the software bootloader from disk
   - Check integrity of software bootloader
   - Decrypt software bootloader

3. Software bootloader activate encrypted disks
   - Key stored in software bootloader (encrypted)
   - Encryption/decryption done on the flight when accessing appliance code and data

4. Appliance designed to be managed by remote APIs only
   - REST APIs to configure Linux and apps
   - No ssh (allowed in dev mode)

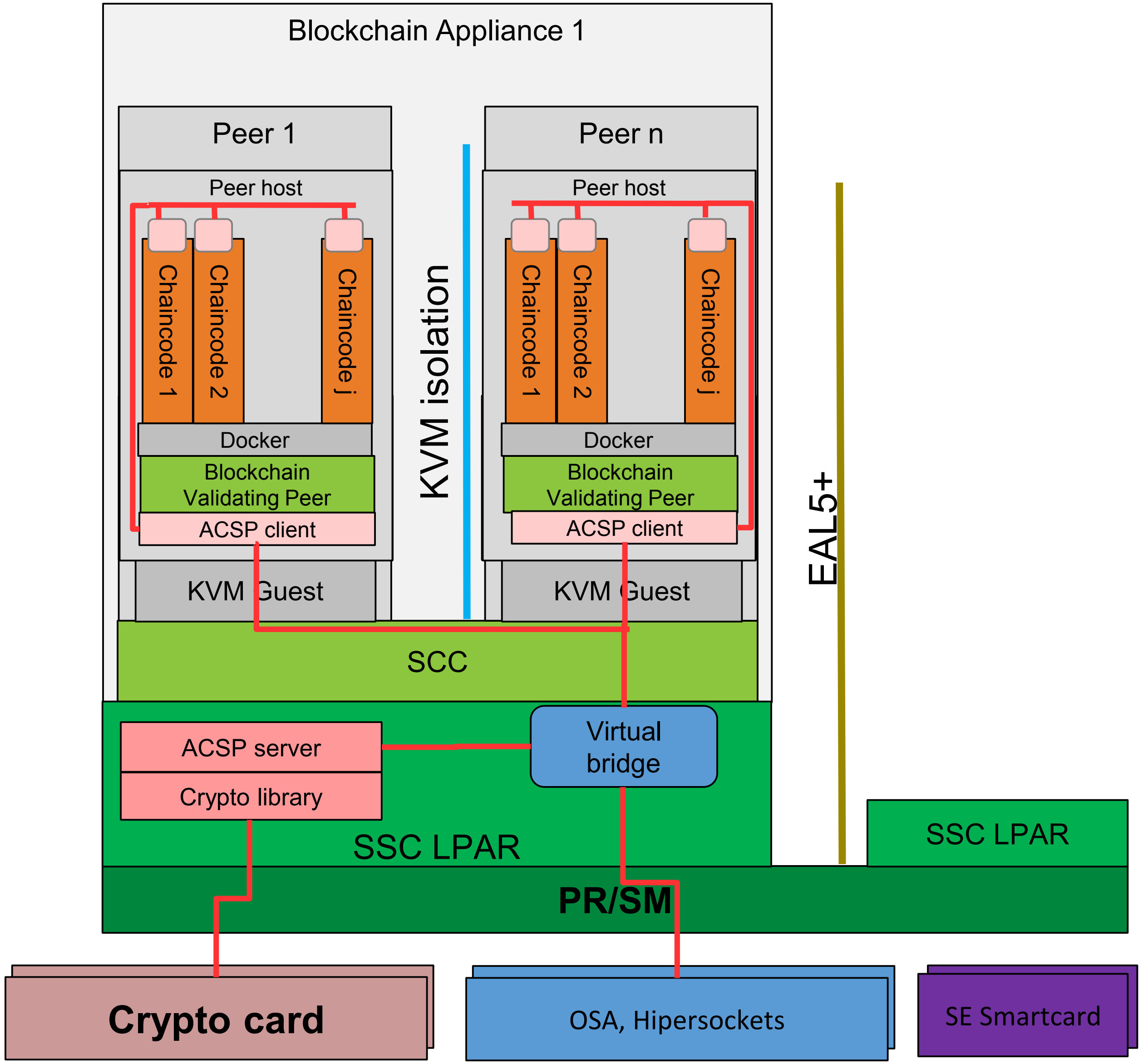
The Blockchain Appliance

IBM KVM Based Blockchain Appliance



- ❑ First create LPARs for SSC's
- ❑ Install SSC Blockchain appliance
- ❑ KVM (virtualization manager) is used to deploy blockchain peers as VM's
  - ▪ All within the SSC, providing peer isolation
  - ▪ KVM/VMs are not visible (exposed)
  - ▪ Blockchain ports for peer access are open for external access
- ❑ Multiple peers peer system
- ❑ Advantages
  - ▪ Only SSC and Blockchain API's are exposed

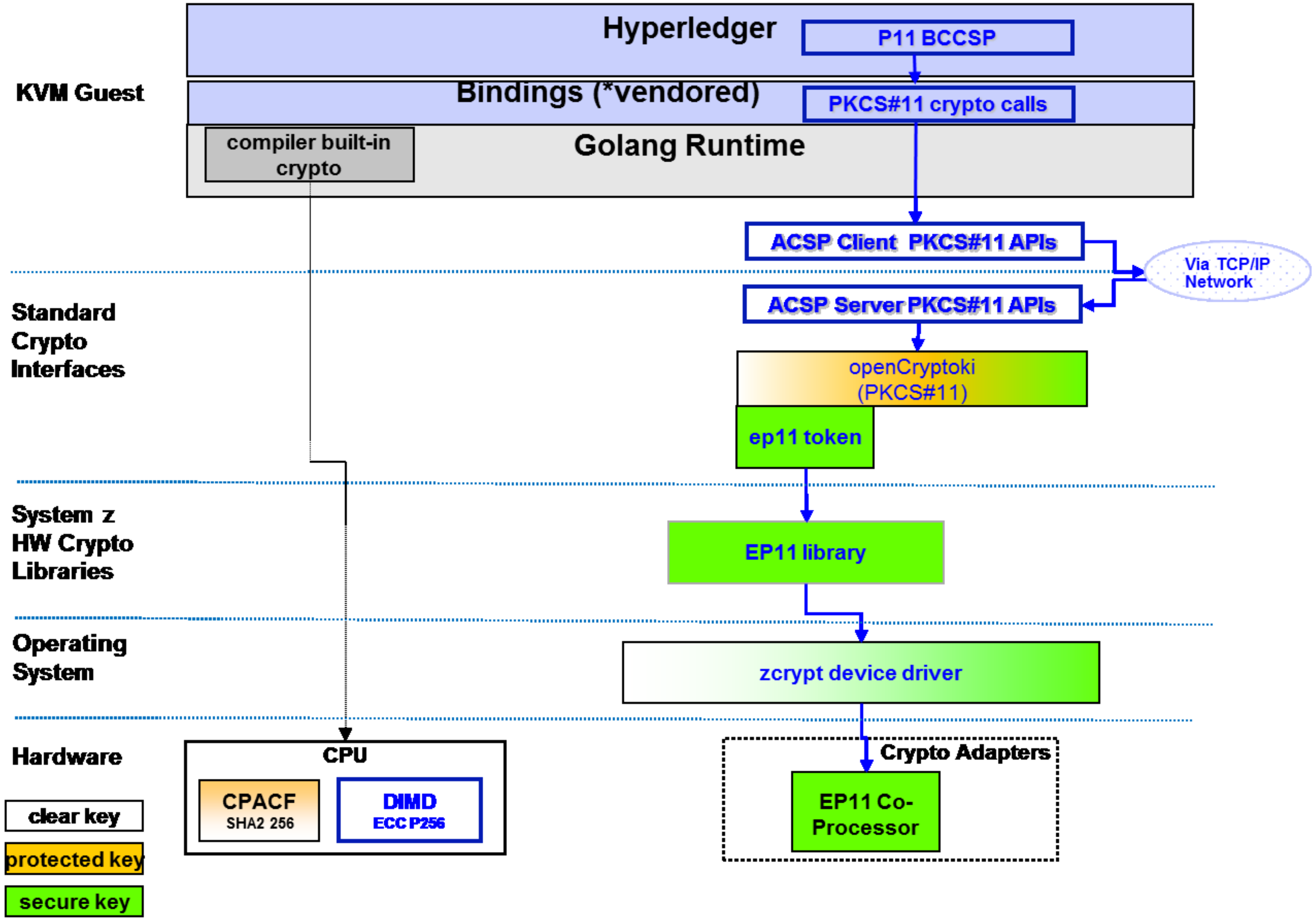
zBlockchain Appliance



- ❑ First create LPARs for SSC's
- ❑ Install SSC Blockchain appliance
- ❑ KVM (virtualization manager) is used to deploy blockchain peers as VM's
  - ▪ All within the SSC, providing peer isolation
  - ▪ KVM/VMs are not visible (exposed)
  - ▪ Blockchain ports for peer access are open for external access
- ❑ Multiple peers peer system
- ❑ Advantages
  - ▪ Only SSC and Blockchain API's are exposed

Crypto for Blockchain

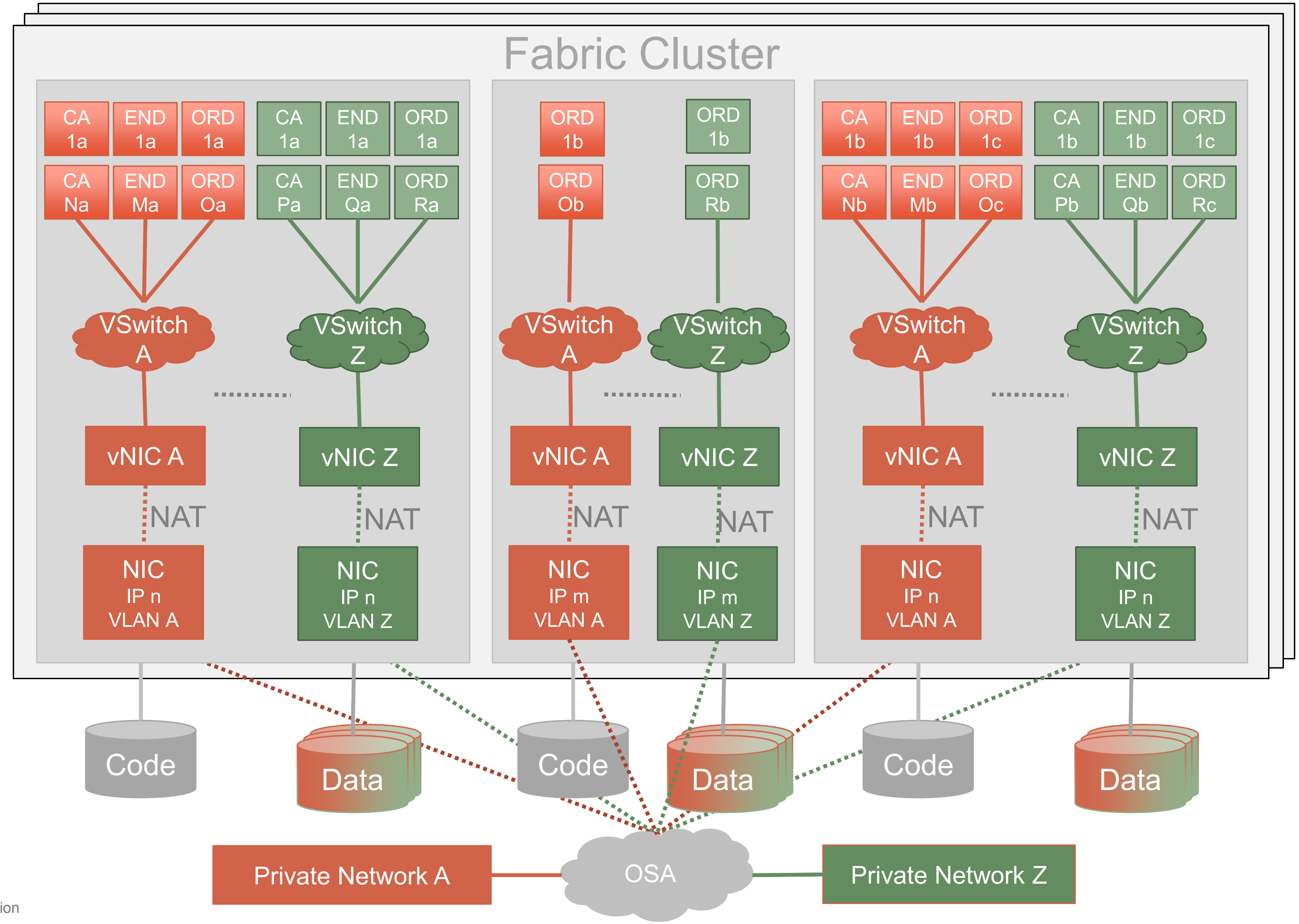
Linux for z Systems using ACSP



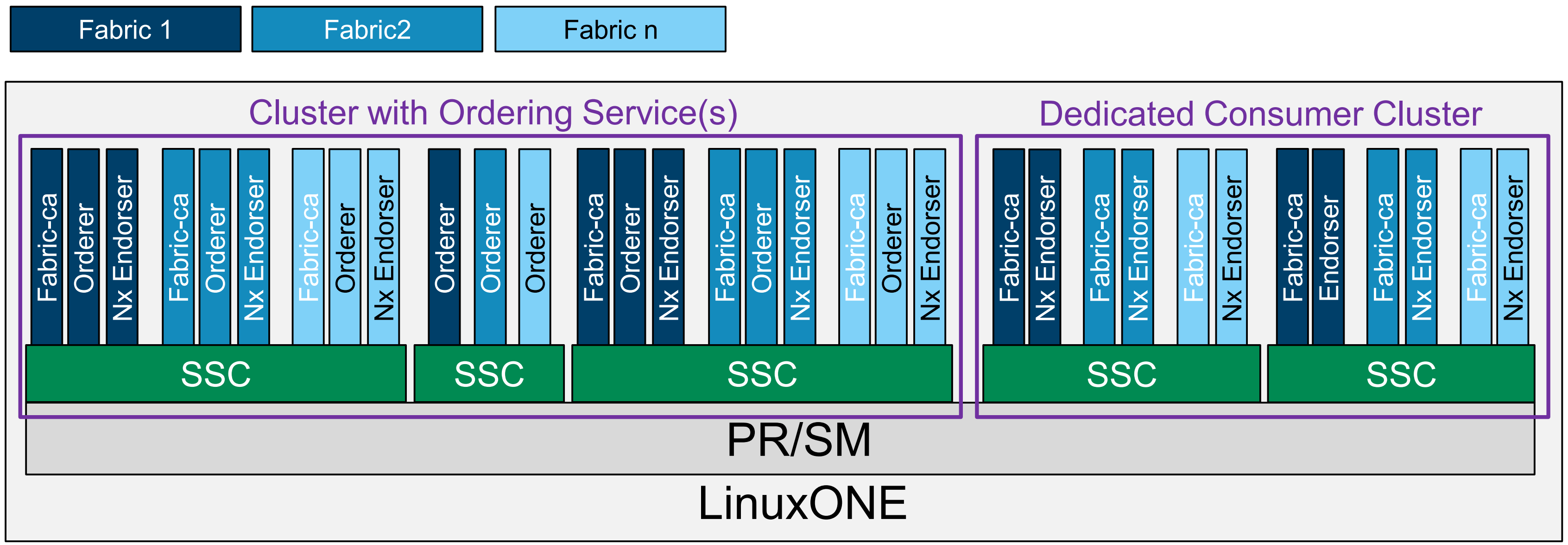
Clustering concept

Clustering overview

- Objectives:
  - Remove having one LPAR as single point of failure
  - Remove Proxies
- Distribute nodes over 3 LPARs
  - Create a Fabric Cluster
- Flexible number of nodes
  - Any number of node packs can be added to cluster
    - CA pack (2x nodes), Endorser pack (2x nodes), Ordering Pack (3x nodes)
- Multiple Fabric Clusters:
  - Multiple HSBNs per cluster or Dedicated Cluster
  - Additional HSBN T-Shirt sizing for Peer Nodes


Fabric Cluster
CA 1a
END 1a
ORD 1a
CA 1a
END 1a
ORD 1a
CA Na
END Ma
ORD Oa
CA Pa
END Qa
ORD Ra
VSwitch A
VSwitch Z
vNIC A
vNIC Z
NAT
NAT
NIC IP n VLAN A
NIC IP n VLAN Z
ORD 1b
ORD 1b
ORD Ob
ORD Rb
VSwitch A
VSwitch Z
vNIC A
vNIC Z
NAT
NAT
NIC IP m VLAN A
NIC IP m VLAN Z
CA 1b
END 1b
ORD 1c
CA 1b
END 1b
ORD 1c
CA Nb
END Mb
ORD Oc
CA Pb
END Qb
ORD Rc
VSwitch A
VSwitch Z
vNIC A
vNIC Z
NAT
NAT
NIC IP n VLAN A
NIC IP n VLAN Z
Code
Data
Code
Data
Code
Data
Private Network A
OSA
Private Network Z

Today – High availability



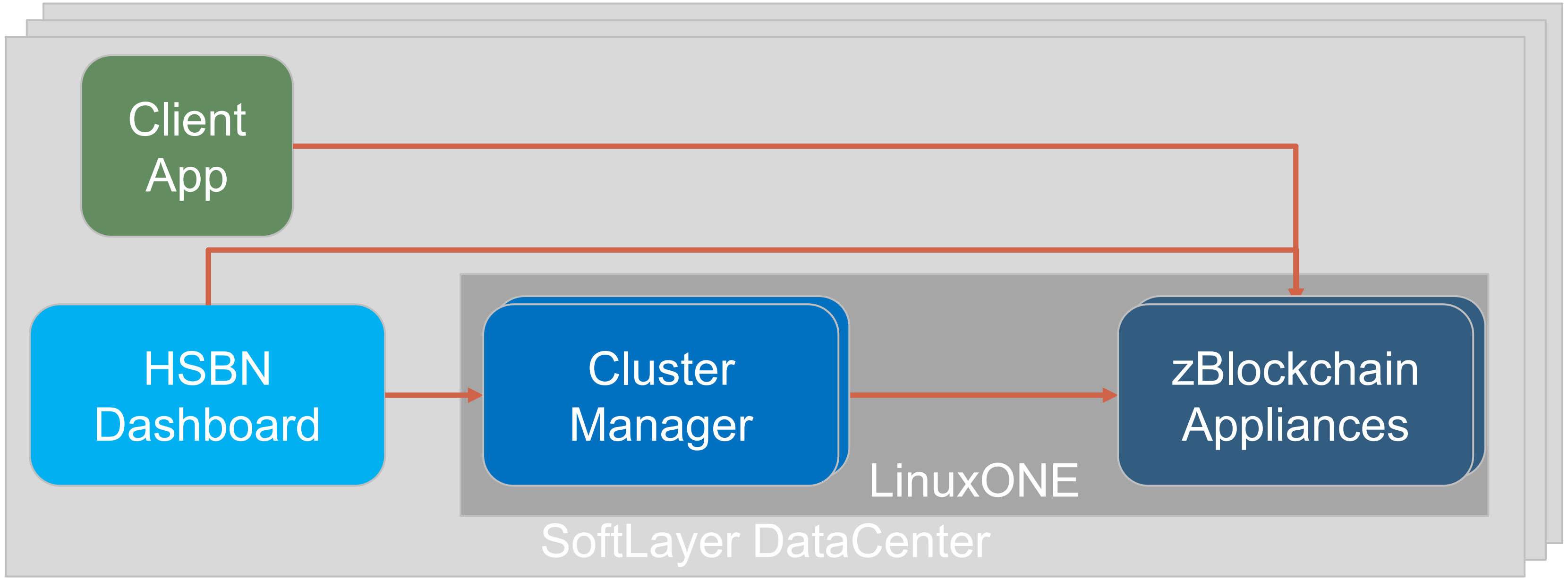
This is the topology we use for our Beta

- Fabric span multiple clusters
  - Nodes owned by different orgs
  - Nodes either in the same cluster or different clusters
- High Availabilty
  - Any LPAR can go down without affecting any service
  - Updates installed without outages
  - Single Points of Failure
    - LinuxONE box
    - Storage Box
    - Data Center
- Two types of cluster
  - Cluster with Ordering services
    - 2 large LPARs
    - 1 small LPAR
  - Cluster withour Ordering services
    - 2 large LPARs

Cluster management

- Requirements:
  - Create network
    - Call createNode for each node to acomplish HA topology
  - Install/Update SSC instaces
  - Administrate network
    - Control enrollement of new orgs
    - Manage subchannels
    - Requires using the Hyperledger SDK
- Implementation today
  - Functionally split between 2xLinux LPAR and Bluemix broker
- Future:
  - move functions into SSC for additional protection
  - re-utilize for on-prem

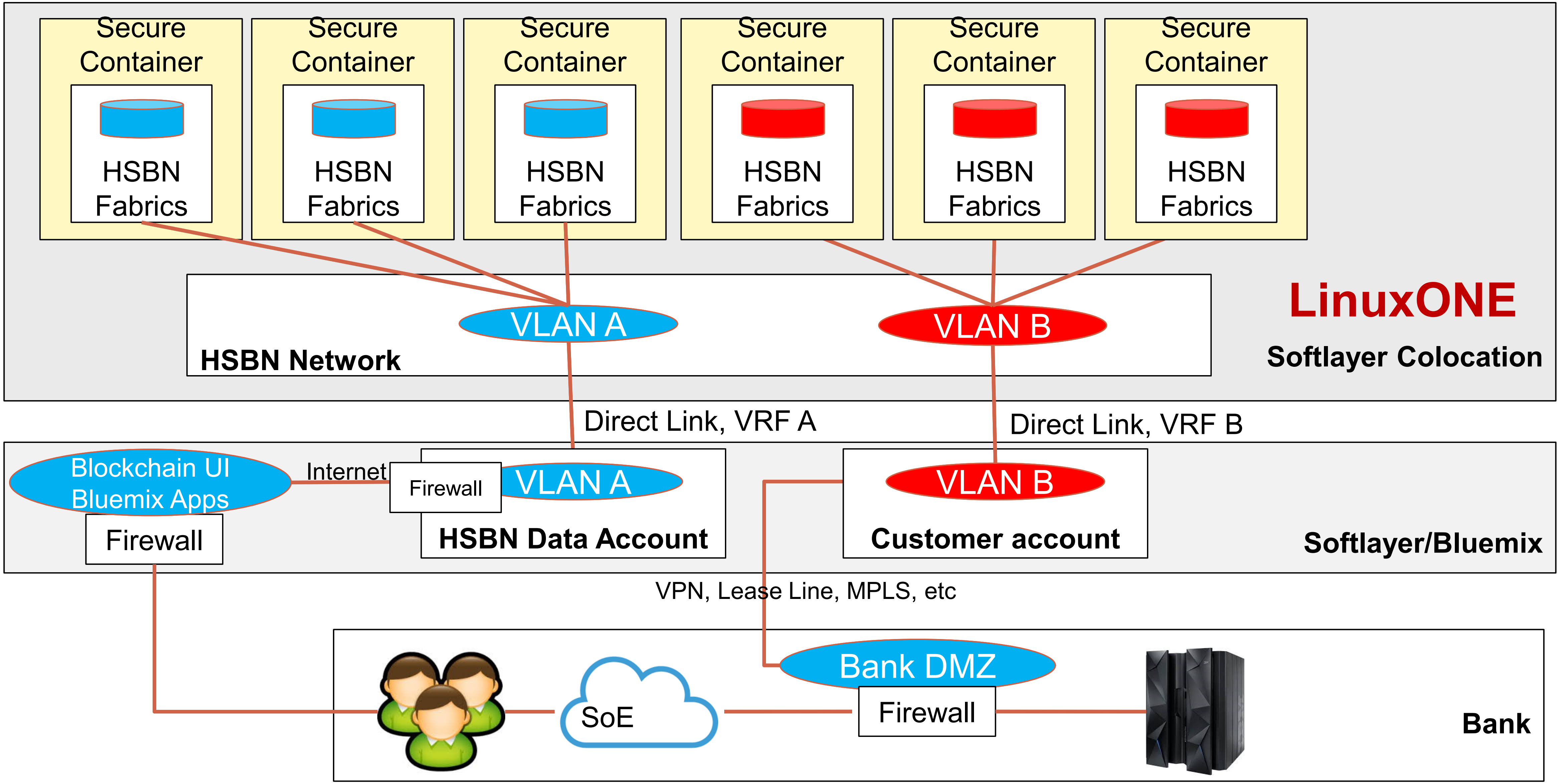
HSBN overview



Levels of Data Redundancy

1. The storage unit (DS8K) uses RAID6 on top of its physical drives in order to provide its logical disks (ECKD volumes) to the LPARs
2. All the Secure Service Container disks are backed up every day via storage flashing
   - Two backups are keep (but can be modified)
3. Within the SSC each container will be snapshoted in a regular base
   - Each node can be recovered to a previous state
4. A crash of an LPAR does not affect the fabrics
   - Data is duplicated over the nodes – shared ledger
   - Remaining nodes are enough to operate the fabric

Access methods to the HSBN V1.0 fabric: Public and Private

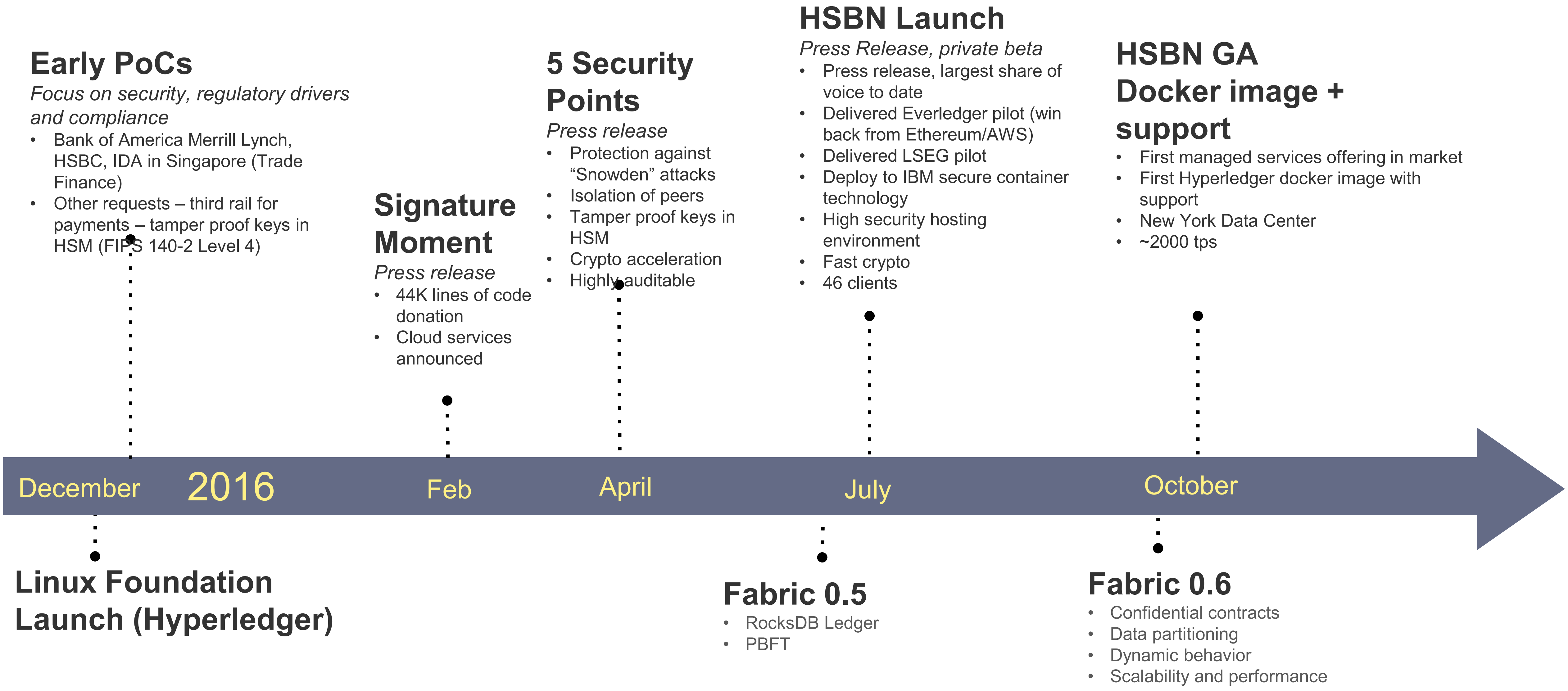


BBC-1454

Thank You

InterConnect
2017

Looking back



Early PoCs

Focus on security, regulatory drivers and compliance

- Bank of America Merrill Lynch, HSBC, IDA in Singapore (Trade Finance)
- Other requests – third rail for payments – tamper proof keys in HSM (FIPS 140-2 Level 4)

Linux Foundation Launch (Hyperledger)

Signature Moment

Press release

- 44K lines of code donation
- Cloud services announced

5 Security Points

Press release

- Protection against “Snowden” attacks
- Isolation of peers
- Tamper proof keys in HSM
- Crypto acceleration
- Highly auditable

HSBN Launch

Press Release, private beta

- Press release, largest share of voice to date
- Delivered Everledger pilot (win back from Ethereum/AWS)
- Delivered LSEG pilot
- Deploy to IBM secure container technology
- High security hosting environment
- Fast crypto
- 46 clients

Fabric 0.5

- RocksDB Ledger
- PBFT

HSBN GA Docker image + support

- First managed services offering in market
- First Hyperledger docker image with support
- New York Data Center
- ~2000 tps

Fabric 0.6

- Confidential contracts
- Data partitioning
- Dynamic behavior
- Scalability and performance

Blockchain is here, now. Get started today

1 Learn

- Blockchain and Hyperledger
- Industry insights and use cases
- Self-paced education

2 Build

- IBM Blockchain on Bluemix
- Hyperledger Fabric on DockerHub
- IBM Bluemix Garage for Blockchain

3 Connect

- Hyperledger Community Chat
- IBM Blockchain Ecosystem Program

Visit ibm.com/blockchain for further information

Further information

1 LEARN

IBM Blockchain https://www.ibm.com/blockchain

The Hyperledger Project https://www.hyperledger.org/

Blockchain @ IBM Institute for Business Value (IBV) ibm.biz/blockchainseries

Industry use cases https://www.ibm.com/blockchain/business-use-cases.html

For developers: Self-paced course and quick-start guide https://developer.ibm.com/blockchain/

2 BUILD

IBM Blockchain on Bluemix https://console.ng.bluemix.net/catalog/services/blockchain

Hyperledger Fabric on DockerHub (IBM-certified image) https://hub.docker.com/u/ibmblockchain/

3 CONNECT

IBM Blockchain Ecosystem https://www.ibm.com/blockchain/ecosystem.html

Hyperledger Chat https://chat.hyperledger.org/