Blockchain on LinuxONE

the new revolutionary transaction model

Wilhelm Mild
IBM Executive IT Architect
IBM Germany Lab
mildw@de.ibm.com

Contents

What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply Blockchain?

Transferring assets, building value

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 key …

Ledger is THE system of record for a business.

Business will have multiple ledgers for multiple business networks in which they participate.

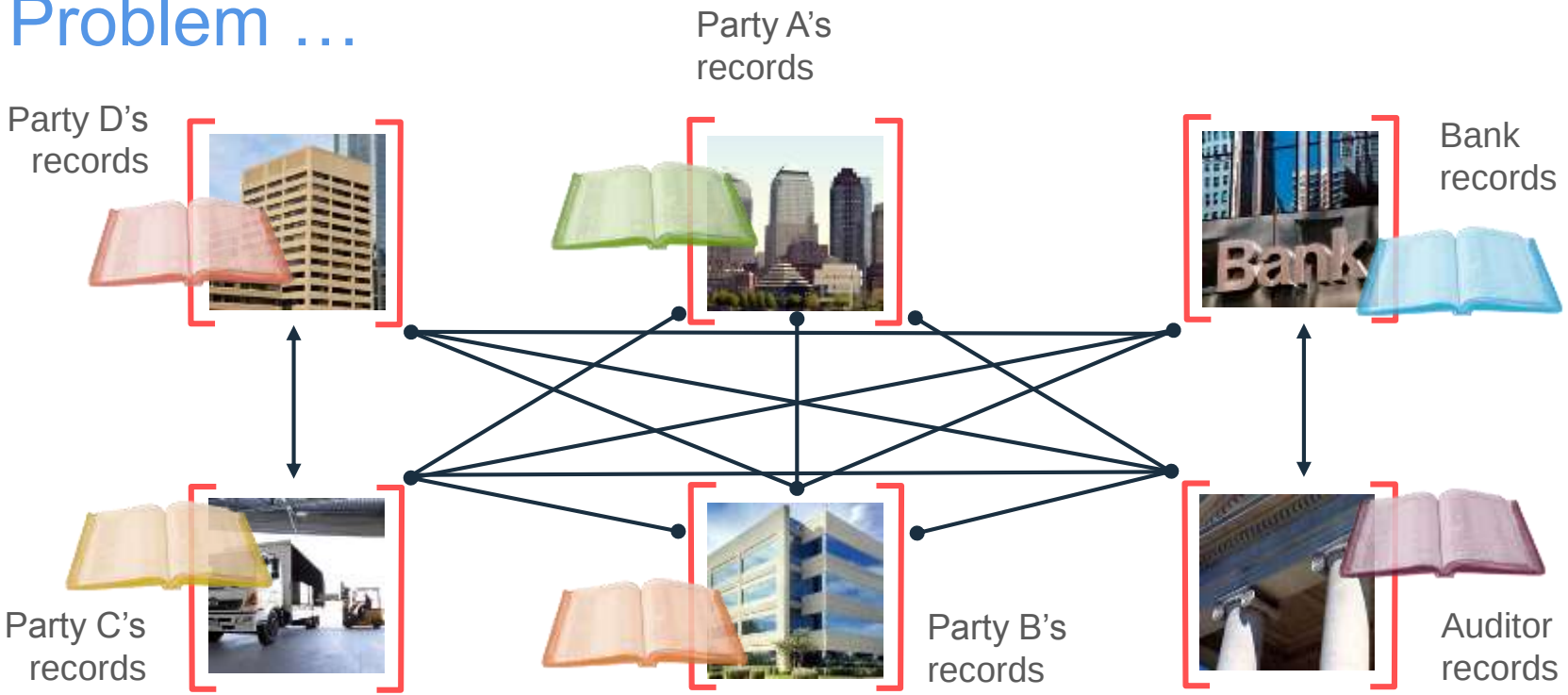
- **Transaction** – an asset transfer onto or off the ledger
  - John gives a car to Anthony (simple)
- **Contract** – conditions for transaction to occur
  - If Anthony pays John money, then car passes from John to Anthony (simple)
  - If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)

What

Introducing Blockchain

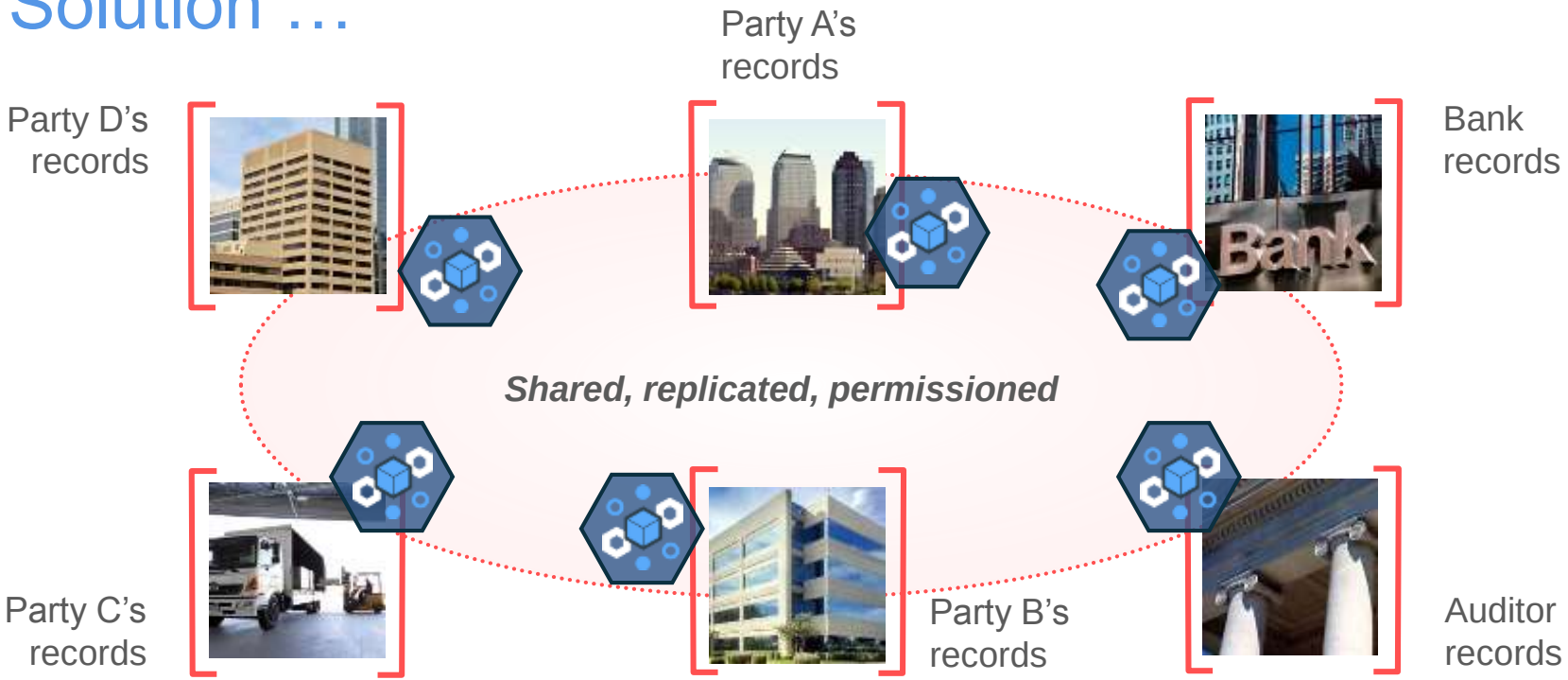
A shared ledger technology allowing any participant in the business network to see THE system of record (ledger)

Problem …



… Inefficient, expensive, vulnerable

Solution …

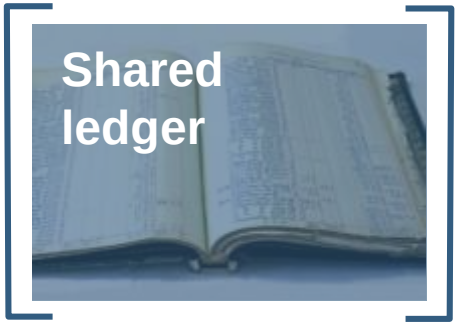


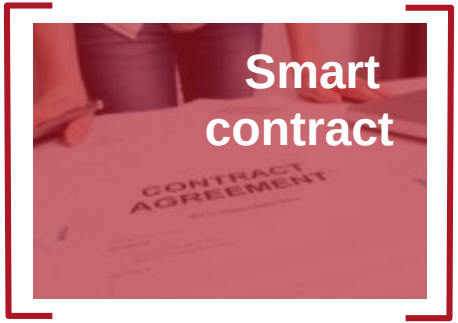
… Consensus, provenance, immutability, finality

What

Blockchain for business …

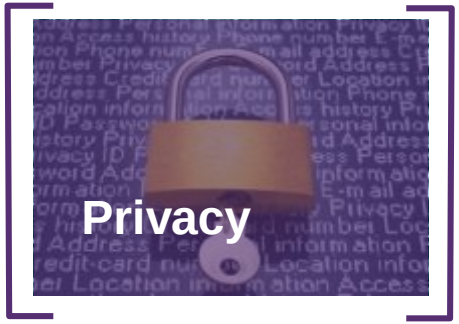
Append-only distributed system of record shared across business network

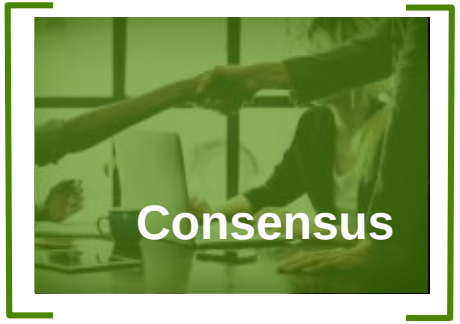




Business terms embedded in transaction database & executed with transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

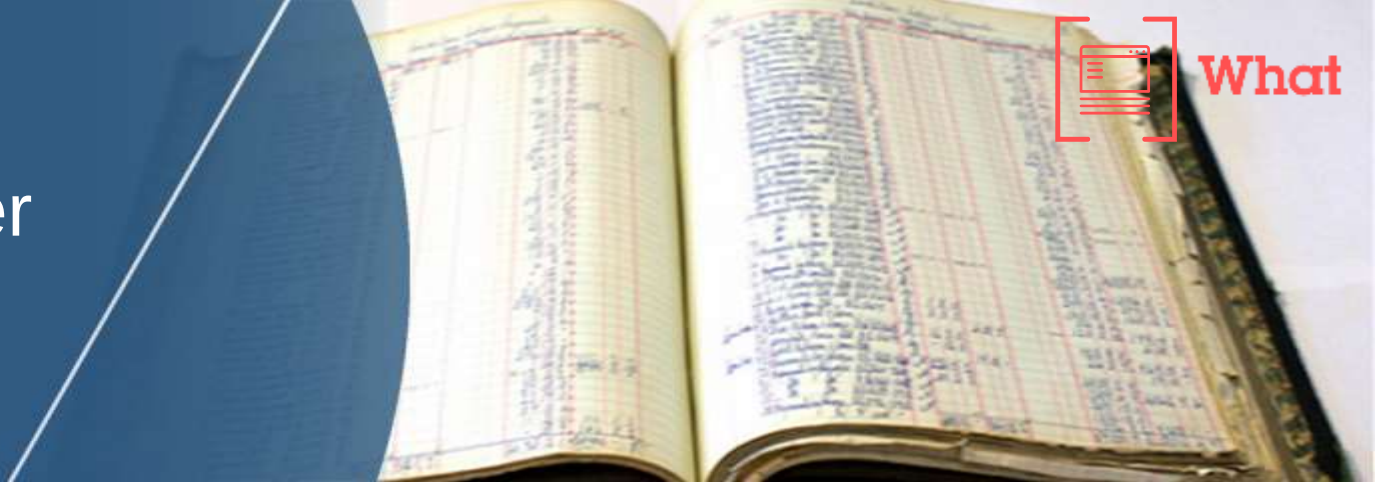




All parties agree to network verified transaction

… Broader participation, lower cost, increased efficiency

Shared ledger



What

Records all transactions across business network

- Shared between participants
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions
- THE shared system of record

Smart contract

What

Business rules implied by the contract … embedded in the Blockchain and executed with the transaction

- Verifiable, signed
- Encoded in programming language
- Example:
  - Defines contractual conditions under which corporate Bond transfer occurs

Privacy

Ledger is shared, but participants require privacy

- Participants need:
  - Transactions to be private
  - Identity not linked to a transaction
- Transactions need to be authenticated
- Cryptography central to these processes

Consensus

What

… the process by which transactions are verified

- Anonymous participants
  - Bitcoin *cryptographic mining* provides randomized selection among anonymous participants
  - Significant compute cost (proof of work)
- Known & trusted participants
  - Commitment possible at low cost
  - Byzantine fault tolerance (BFT)
- Multiple alternatives
  - Proof of stake, where influence is determined by risk of validators
  - Multi-signatures, validation needs consent from 3 out of 5 validators
- Industrial Blockchain needs “pluggable” consensus

Contents

What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply Blockchain?

Why

Blockchain benefits

Saves
time

Transaction time from days to near instantaneous

Removes
cost

Overheads and cost intermediaries

Reduces
risk

Tampering, fraud & cyber crime

Increases
trust

Through shared processes and recordkeeping

Provenance use case – Vehicle maintenance

What

- Provenance of each component part in complex system hard to track
- Manufacturer, production date, batch and even the manufacturing machine program

How

- Blockchain holds complete provenance details of each component part
- Accessible by each manufacturer in the production process, the aircraft owners, maintainers and government regulators

Benefits

1. Trust increased, no authority "owns" provenance
2. Improvement in system utilization
3. Recalls "specific" rather than cross fleet

Immutability use case – Financial ledger

What

- Financial data in a large organization dispersed throughout many divisions and geographies
- Audit and Compliance needs indelible record of all key transactions over reporting period

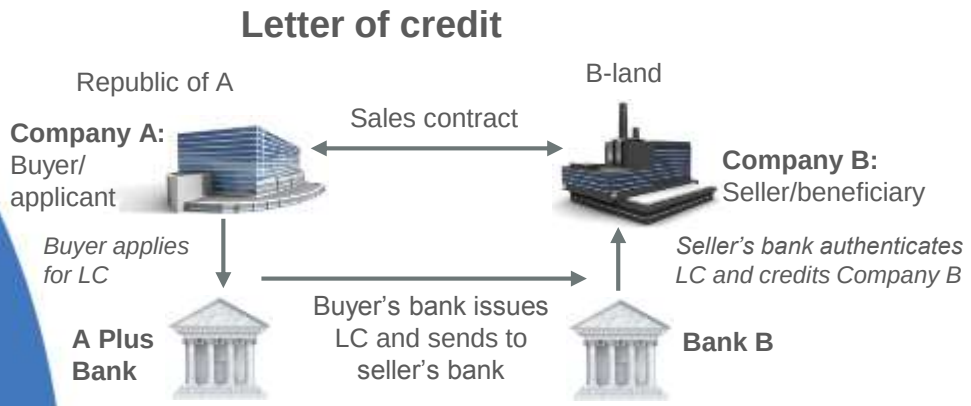
How

- Blockchain collects transaction records from diverse set of financial systems
- Append-only and tamperproof qualities create high confidence financial audit trail
- Privacy features to ensure authorized user access

Benefits

1. Lowers cost of audit and regulatory compliance
2. Provides “seek and find” access to auditors and regulators
3. Changes nature of compliance from passive to active

Finality use case – Letter of credit



What

- Bank handling letters of credit (LOC) wants to offer them to a wider range of clients including startups
- Currently constrained by costs & the time to execute

How

- Blockchain provides common ledger for letters of credit
- Allows all counter-parties to have the same validated record of transaction and fulfillment

Benefits

1. Increase speed of execution (less than 1 day)
2. Vastly reduced cost
3. Reduced risk, e.g. currency fluctuations
4. Value added services, e.g. incremental payment

Possible use cases by (selected) industries

Financial	Public Sector	Retail	Insurance	Manufacturing
Trade Finance	Asset Registration	Supply chain	Claims processing	Supply chain
Cross currency payments	Citizen Identity	Loyalty programs	Risk provenance	Product parts
Mortgages	Medical records	Information sharing (supplier – retailer)	Asset usage history	Maintenance tracking
	Medicine supply chain		Claims file	

Patterns for customer adoption

HIGH VALUE MARKET

- Transfer of high value financial assets
- Between many participants in a market
- Regulatory timeframes

ASSET EXCHANGE

- Sharing of assets (voting, dividend notification)
- Assets are information, not financial
- Provenance & finality are key

CONSORTIUM SHARED LEDGER

- Created by a small set of participants
- Share key reference data
- Consolidated, consistent real-time view

COMPLIANCE LEDGER

- Real-time view of compliance, audit & risk data
- Provenance, immutability & finality are key
- Transparent access to auditor & regulator

Contents

What is Blockchain?

Why is it relevant for our business?

How can IBM help us apply Blockchain?

How

Blockchain for Business – Our Point of View

Community + Code

Linux Hyperledger Project

Open Source Code: Blockchain for business;

Consensus | Provenance
Immutability | Finality

Open Governance – 100 member cross industry board

Cloud

IBM Blockchain

Blockchain managed service on IBM Cloud and z Systems;

Identity | Consensus | System Integration |
Hardware-assist for Performance & Security

IBM Blockchain on Bluemix

Clients

Blockchain Solutions
Blockchain Garage

Making Blockchain real for business

Blockchain Garage;
New York | London | Singapore | Tokyo

Blockchain Services Practice

Blockchain NOW

Hyperledger fabric on Docker Hub	Fastest development of blockchain solutions Certified Hyperledger fabric instances Supported by IBM – available cross platform
High security business blockchain on Bluemix	Dedicated compute power – isolated partition Secure key management (FIPS 140-2 Level 4) Tamper resistant service container Performance optimized (Operating System & Privacy Services)
Bluemix blockchain service	Fast blockchain network on Bluemix – also now China Samples for deployment, customization & usage Tool support for development and deployment

Supporting serious blockchain deployment!

Linux Foundation's Hyperledger Project

- *Open Ledger Project* announced December 17, 2015 with **17** founders, now over **100** members
- *Hyperledger Project* rebrand in February 2017
- Collaborative effort 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
- Open source, open standards, open governance

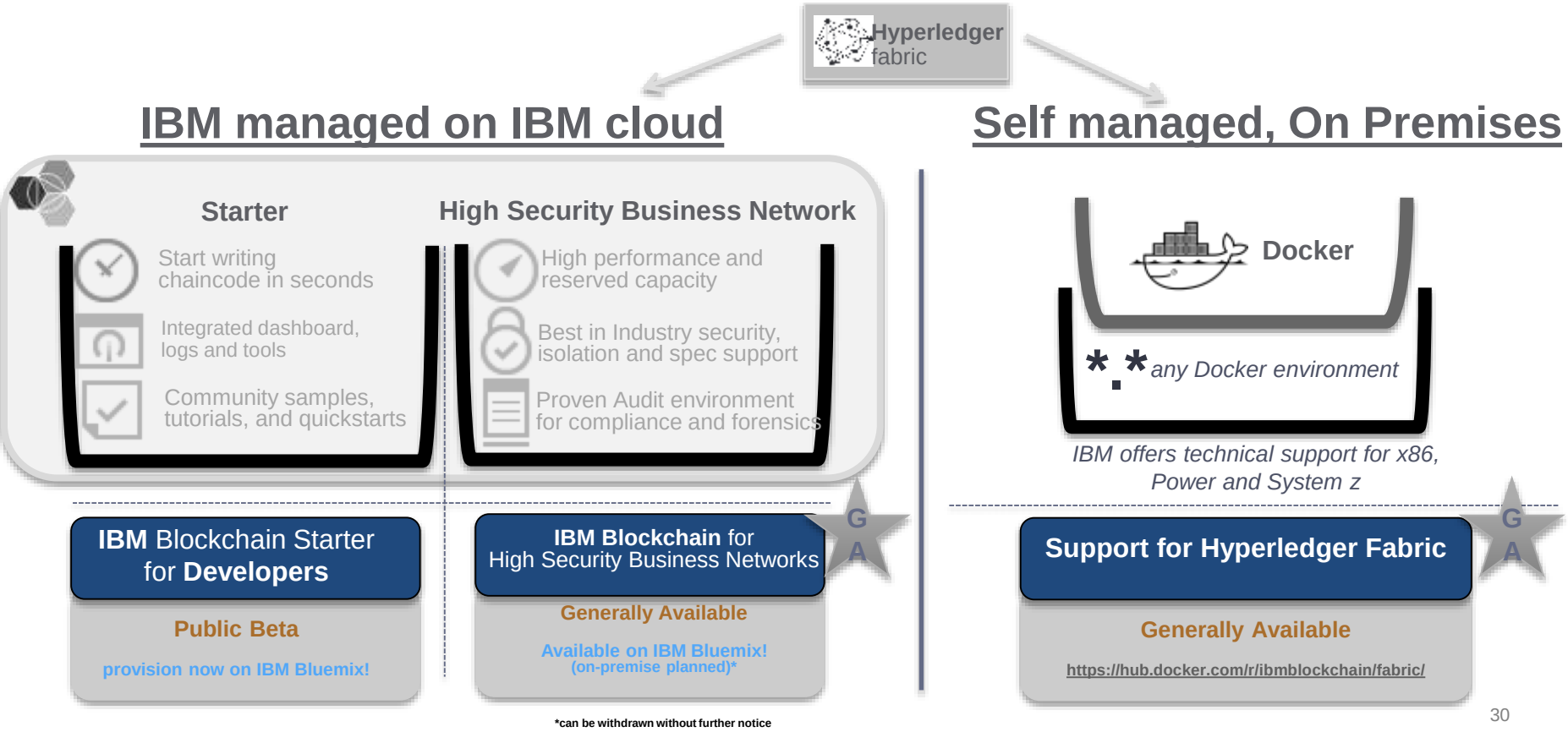
Enable adoption of shared ledger technology at a pace and depth not achievable by any one company or industry

QUICK FACTS	
Chairman	Blythe Masters/DAH
Executive Director	Brian Behlendorf
Technical Chair	Chris Ferris/IBM
Contribution	44,000 lines of code in February 2017
Sprint to one codebase with unified thinking	Staged releases

www.Hyperledger.org

IBM Blockchain Offerings

IBM Blockchain Offerings



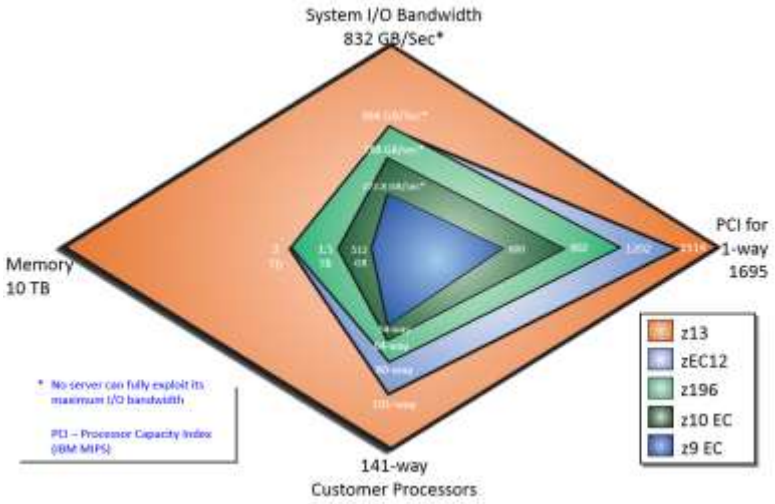
Why Blockchain on LinuxONE?

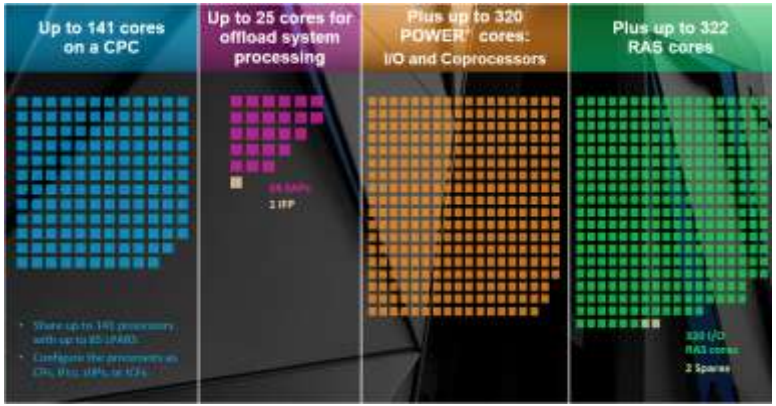
Architectural Benefits

- built-in HW-virtualization
  - z/OS & Linux enabled
    - performance benefits for Docker and KVM
  - Benefits for consolidation

- High IO-Performance due to bandwidth and HW-based IO
  - reduced CPU overhead for IOs
    - especially data oriented code benefits
  - HW compression
    - reduces data on the move

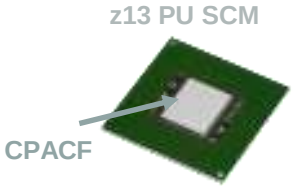
- Security
  - HW accelerated encryption
  - High degree of guest Isolation
    - Secure Service Container (SSC) to deliver secure appliances





Crypto Acceleration in LinuxONE

- CPACF – CP Assist for Cryptographic Functions
  - Designed to improve performance of crypto functions
  - Symmetric cryptography, secure hashing

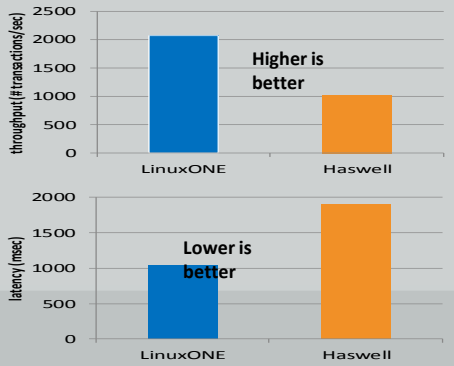


- CEX5S – Crypto Express5S Card
  - PCIe Cryptographic Coprocessor (PCIeCC)
  - Hardware to perform AES, DES, T-DES, HMAC, random number generation, SHA-1, SHA-256, SHA-384, SHA-512, MD5, HMAC, and large number modular math functions for RSA (up to 4096-bit), ECC Prime Curve and other public-key cryptographic algorithms

IBM LinuxONE™ and Containers

Extreme Virtualization with Containers

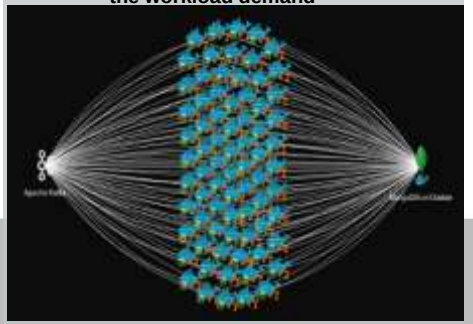
- A single LinuxONE Emperor ran more than *1 Million* containers
  - Workload: busybox httpd server (no NAT)
- LinuxONE Emperor runs *4K* containers on avg *2.0x* better than a compared Haswell-based system
  - Workload: Apache Solr
- LinuxONE Emperor can host over *10k* containers
  - Workload: 4k Apache Solr + 6k busybox httpd server (no NAT)



The throughput and response-time for a single Linux host running 4096 containers

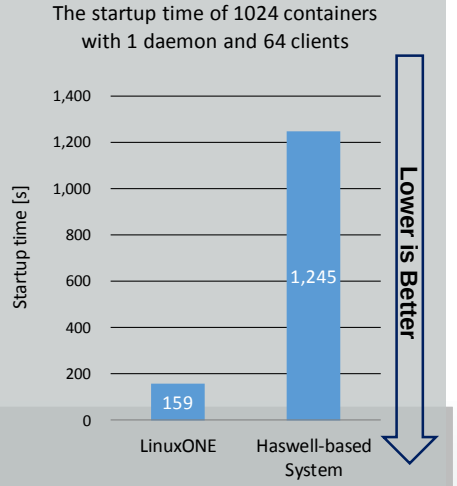
Multi-Layer Auto Scaling

- Manage multiple virtualization layers to minimize the amount of resources to meet a SLA for a wide range of workload demand.
  - Start a set of containers when an application-level bottleneck is detected
  - Start a Docker Engine daemon in the same host when a daemon-level bottleneck is detected
  - Start an OS when an OS-level bottleneck is detected
  - Adjust the hardware resources such as CPU, memory, and I/O dynamically when a HW-level bottleneck is detected according to the workload demand



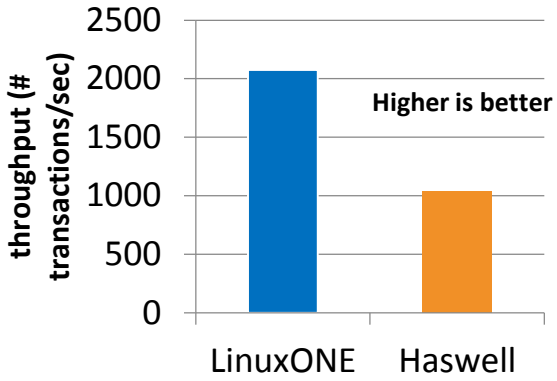
Extreme Agility with Containers

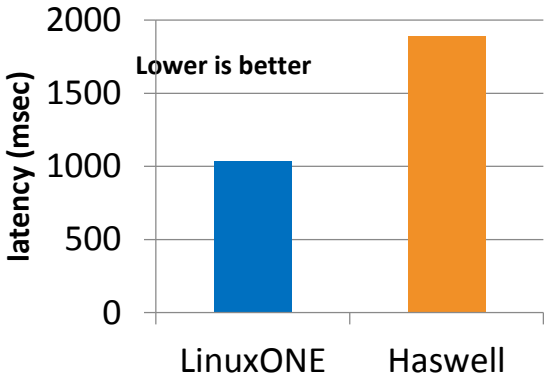
- LinuxONE Emperor can start containers *7.8x faster* than a compared Haswell-based system.
  - Workload: nginx
- Significant agility to adapt to dynamic workload behavior



Extreme Virtualization with Docker®

- **Containers**: simple way to build and deploy SW with Docker currently leading framework
- Single LinuxONE Emperor ran more than 1 Million light Docker containers
  - Workload: busybox httpd server (no NAT)
- LinuxONE Emperor runs **4K *active*** Docker containers on ave **2.0x** better than comparable Haswell-based system!
  - Workload: 50% WAS Liberty 8.5.5.2, IBM JDK 8.0, Apache Solr 4.10.0, and 50% busybox httpd server
  - With ***GOLANG*** now avail on z!
- LinuxONE Emperor can host over 10K Docker containers with mixed (heavy & light) workloads
  - Workload: 4K WAS Liberty 8.5.5.2, IBM JDK 8.0, Apache Solr 4.10.0 plus 6K busybox httpd server (no NAT)





Disclaimer:
This claim is based on results from internal lab measurements. Performance results may vary depending on the workload and other factors.Benchmark:
- Apache Solr search queries driven by Apache Jmeter'System Stack:
- LinuxONE Emperor (IBM z13): Native LPAR on 36 CPU cores with 755GB memory
- Haswell-based alternative system (Lenovo System x3650 M5 w/ E5-2699 v3 processors): Native Linux on 36 CPU cores with 755GB memory
- Heavy Docker Container: Apache Solr v4.10.0, WebSphere Liberty v8.5.5.2, IBM Java 1.8.0 SR1
- Lightweight Docker Container: BusyBox
- System SW: Docker 1.10.0-dev" w/ aufs storage backend, RHEL 7.1""

Note:
- Each active container is driven by a client thread in Apache Jmeter, which keeps sending the same Solr query repeatedly to the container to search documents that contain given key words in a pre-loaded & pre-indexed 46GB Wikipedia snapshot.

" The docker runtime was modified to increase a thread count limit, to avoid connection time-out, and to separate a dockerinit binary from a docker binary.
"" A modified Linux 4.3.0 kernel to support more than 1024 network bridge ports was installed on RHEL 7.1.

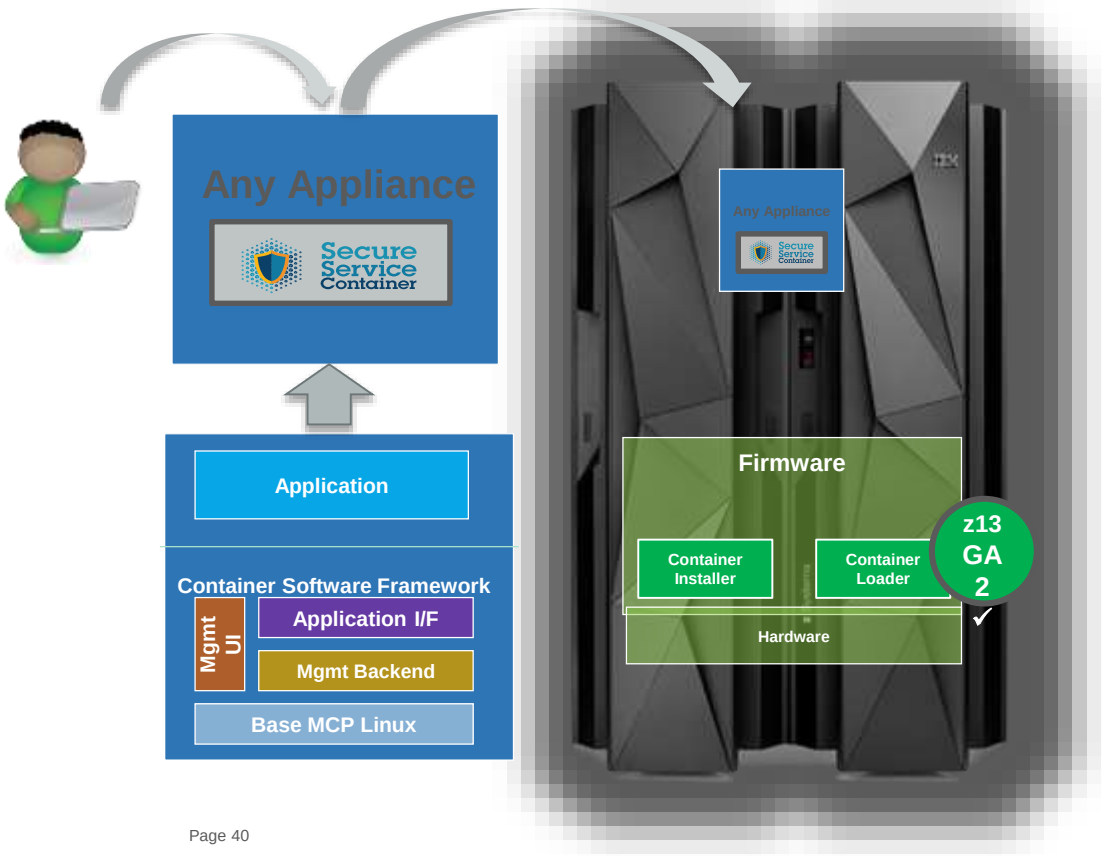
IBM Secure Services Container

Secure Service Container

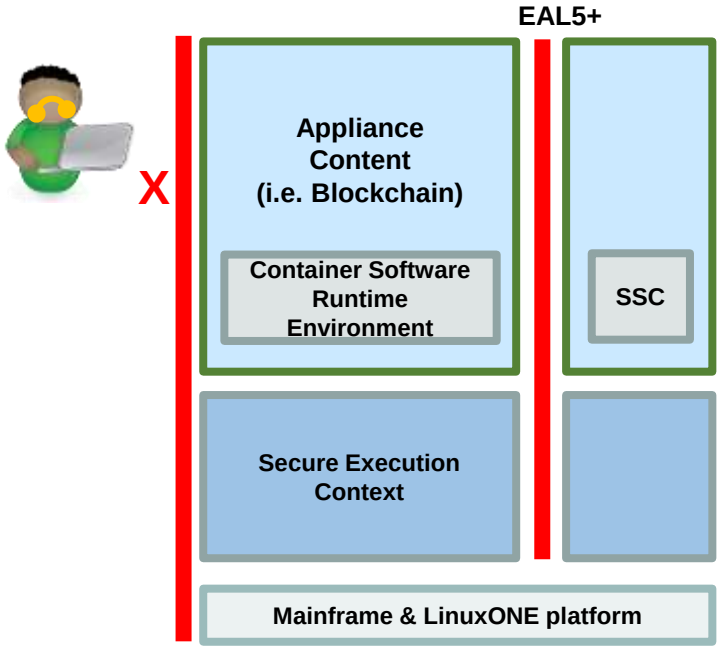
The Base Infrastructure to Host and Build Software Appliances

- **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

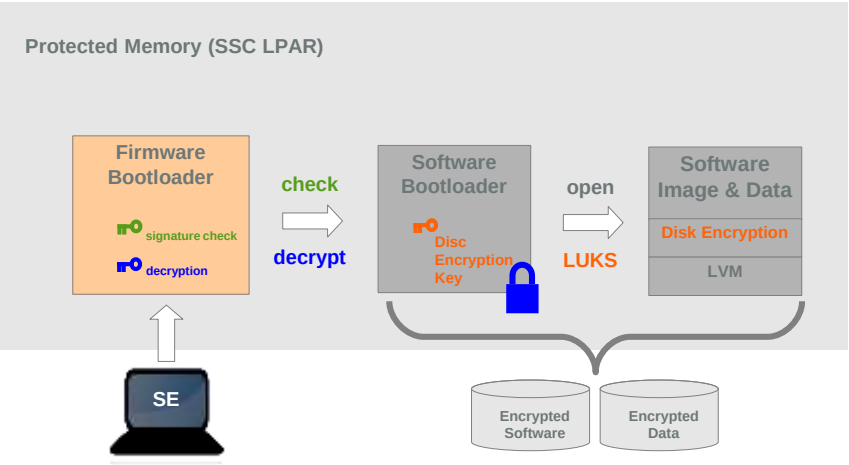


Secure Service Container Protection



- 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

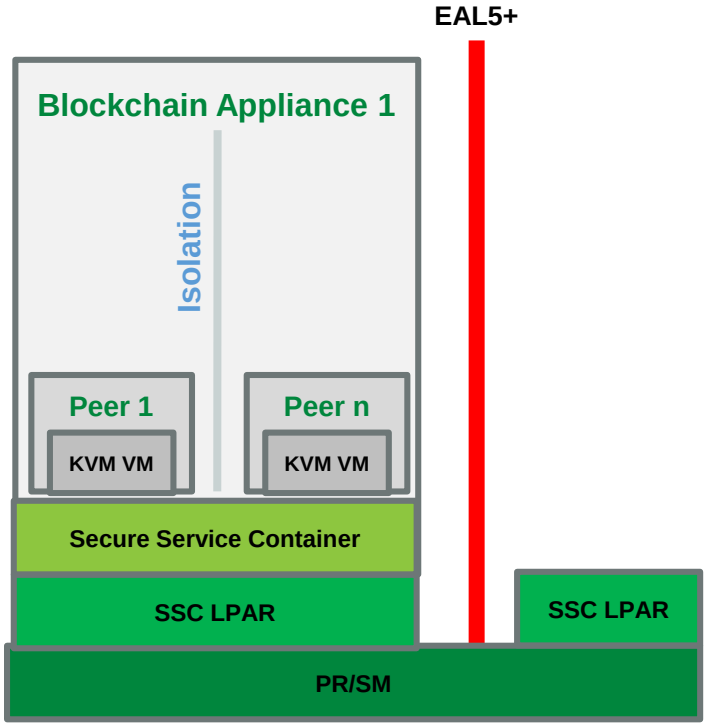
1. Firmware bootloader is loaded in memory

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

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

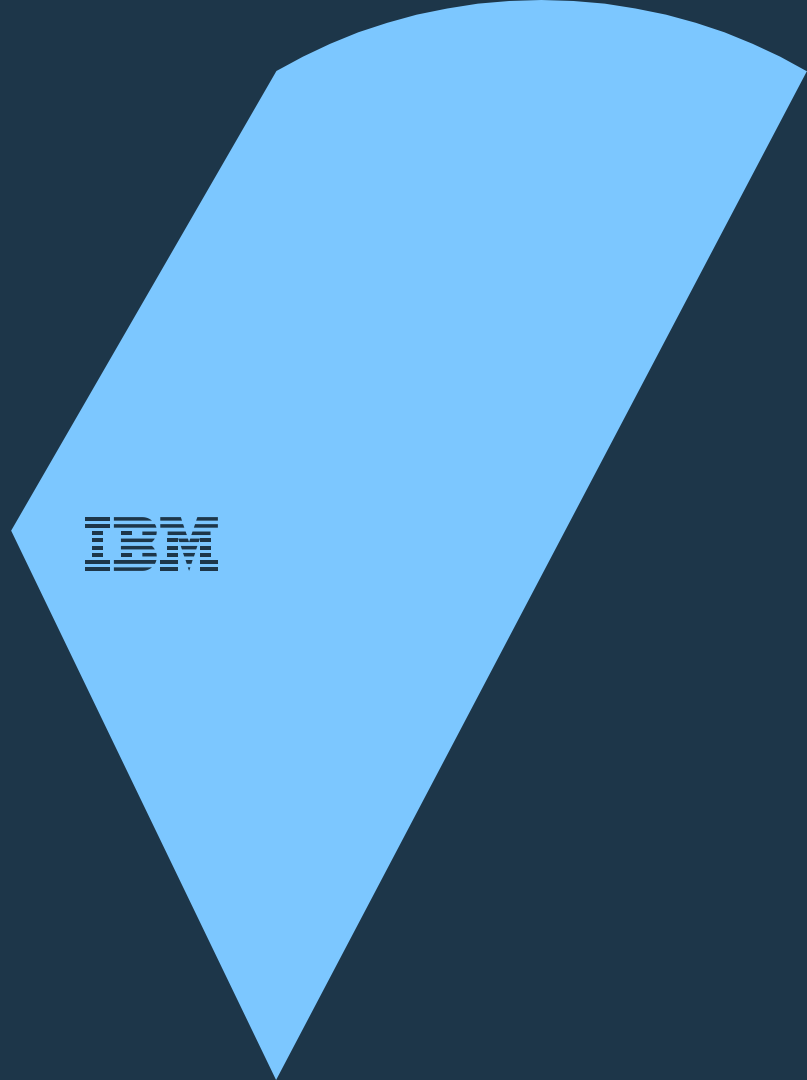
4. Appliance designed to be managed by remote APIs only
   - REST APIs to configure Linux and apps
   - No ssh (allowed in dev mode)

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

IBM Blockchain Fabric Composer



What is Fabric Composer?

What

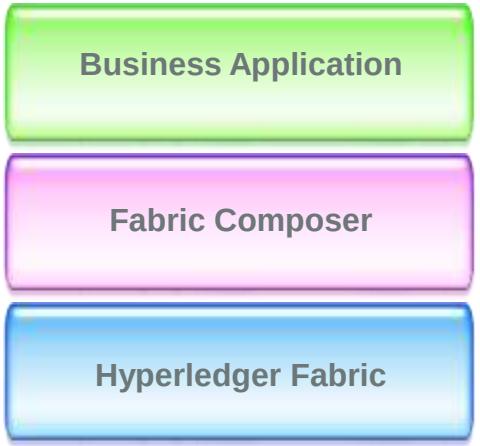
- Blockchains typically provide a low-level interface for business applications
  - Smart contract code run on a distributed processing system
  - Inputs go into an immutable ledger; outputs to a data store
  - Applications are built on top of a low level of abstraction

- Fabric Composer
  - A suite of high level application abstractions for business networks
  - Emphasis on business-centric vocabulary for quick solution creation

- Features
  - Model YOUR business networks, test and expose via APIs
  - Applications invoke APIs transactions to interact with business network
  - Integrate existing systems of record using loopback/REST

- Tools, APIs and libraries to support these activities
  - Open community initiative in support of the Linux Foundation Hyperledger project

http://fabric-composer.org/



The Enterprise Integration Hub with IBM Integration Bus (IIB)

- Flexible integration with Web, Mobile, Cloud, Analytics and IT services
- Standard Interfaces and Open source based Integration APIs like Swagger & CHEF
- Intelligent transformation and content based routing
- Universal Integration with high scalability and security incl. workflow & workload mgmt

http://www-03.ibm.com/software/products/en/ibm-integration-bus

Deployable full active/active

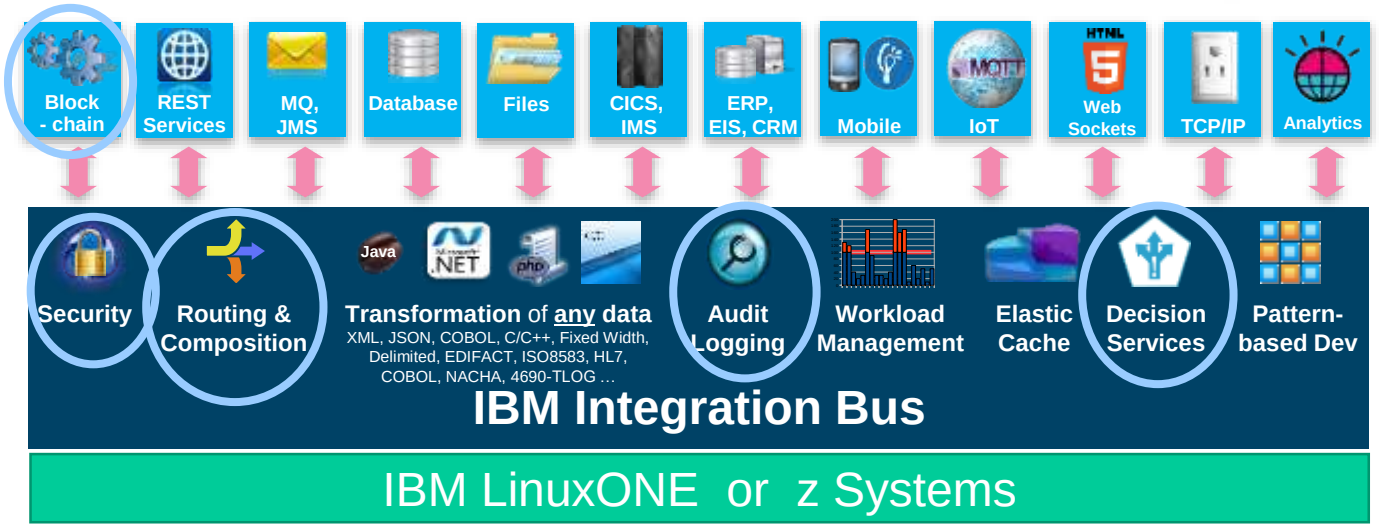
No charge for developers

Streamlined to ESB use case

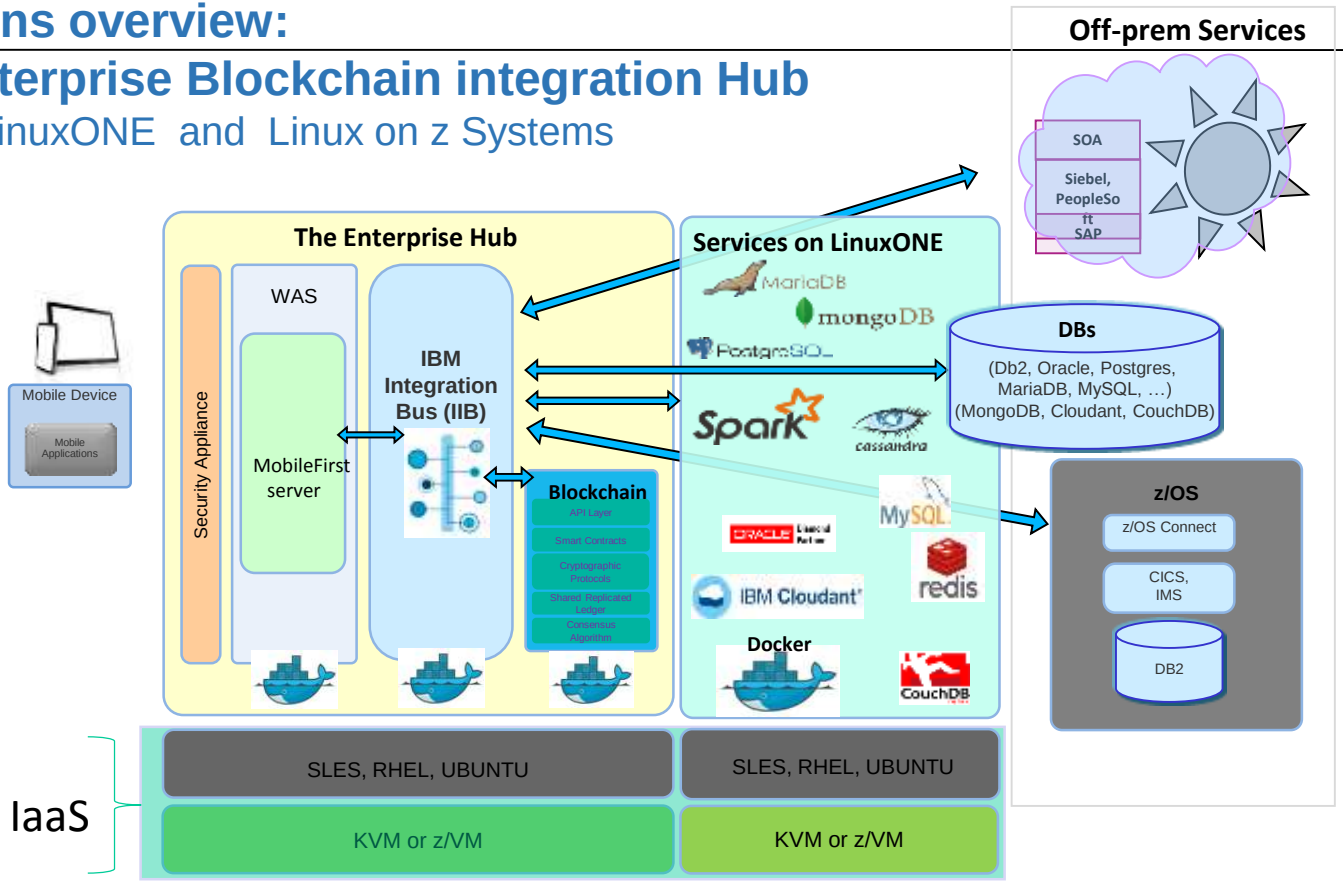
Scalable in Docker Containers

HTML5 web admin/monitoring

High scale MQ events/messaging



Solutions overview:
The Enterprise Blockchain integration Hub
on IBM LinuxONE and Linux on z Systems



IBM Integration Bus can help you simplify the connectivity between your IT assets, including legacy apps, packaged apps and web services, without requiring coding changes. It provides content and context based routing that helps you manage and simplify business-critical processes. It enables you to integrate Open Source technologies and Hybrid cloud with most of your existing IT assets quickly, simply and at a low cost.

Summary

Blockchain …

- is a shared, replicated, permissioned ledger technology
- can open up business networks by taking out cost, improving efficiencies and increase accessibility
- addresses an exciting and topical set of business challenges, which cross every industry

IBM …

- supports the Linux Foundation Hyperledger open standard, open source, open governance Blockchain
- has an easy to access, proven and incremental engagement model giving customers the confidence to get started NOW

Thank you!

Further Information – Use case Links

HSBC, Bank of America, IDA:

http://www.coindesk.com/hsbc-bank-america-blockchain-supply-chain/

ABN AMRO:

https://www.abnamro.com/en/newsroom/blogs/arjan-van-os/2017/walking-the-walk-exploring-the-power-of-blockchain.html

Crédit Mutuel Arkéa:

http://www.coindesk.com/ibm-completes-blockchain-trial-french-bank-credit-mutuel/

JPX:

http://www.ibm.com/press/us/en/pressrelease/49088.wss

Kouvola Innovation:

http://www.ibm.com/press/us/en/pressrelease/49029.wss

London Stock Exchange:

http://www.ibtimes.co.uk/linux-foundation-blockchain-consortium-digital-asset-ibm-credits-london-stock-exchange-board-1533798

Mizuho:

http://www.coindesk.com/mizuho-digital-currency-powered-blockchain-settlement/

IBM Global Finance:

http://www.coindesk.com/ibm-building-blockchain-dispute-resolution-system/

Questions?

Wilhelm Mild

IBM Executive IT Architect

IBM Deutschland Research & Development GmbH
Schönaicher Strasse 220
71032 Böblingen, Germany

Office: +49 (0)7031-16-3796
wilhelm.mild@de.ibm.com

Trademarks & Disclaimer

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

IBM, the IBM logo, BladeCenter, Calibrated Vectored Cooling, ClusterProven, Cool Blue, POWER, PowerExecutive, Predictive Failure Analysis, ServerProven, System p, System Storage, System x , z Systems, WebSphere, DB2 and Tivoli are trademarks of IBM Corporation in the United States and/or other countries. For a list of additional IBM trademarks, please see http://ibm.com/legal/copytrade.shtml.

The following are trademarks or registered trademarks of other companies: Java and all Java based trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries or both Microsoft, Windows,Windows NT and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both. Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries or both. Linux is a trademark of Linus Torvalds in the United States, other countries, or both. Cell Broadband Engine is a trademark of Sony Computer Entertainment Inc. InfiniBand is a trademark of the InfiniBand Trade Association. Other company, product, or service names may be trademarks or service marks of others.

NOTES: Linux penguin image courtesy of Larry Ewing (lewing@isc.tamu.edu) and The GIMP

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Users of this document should verify the applicable data for their specific environment. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
Information is provided “AS IS” without warranty of any kind. All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices are suggested US list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography. Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use. The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any

Notice Regarding Specialty Engines

Any information contained in this document regarding Specialty Engines (“SEs”) and SE eligible workloads provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g., zIIPs, zAAPs, and IFLs).
IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”).
No other workload processing is authorized for execution on an SE.
IBM offers SEs at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.