Making Blockchain Real for Business

IBM Blockchain Offering

Guillaume Hoareau
Certified IT Architect
Blockchain on IBM z Systems SME

V3.5, November 24th
© 2016 IBM Corporation
Linux Foundation’s Hyperledger Project

– Linux Foundation project announced December 17, 2015 with 17 founders, now 40 members

– The Hyperledger Project is a 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 and open standards-based

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

QUICK FACTS

<table>
<thead>
<tr>
<th>Chairman</th>
<th>Blythe Masters/DAH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Director</td>
<td>Brian Behlendorf</td>
</tr>
<tr>
<td>Technical Chair</td>
<td>Chris Ferris/IBM</td>
</tr>
<tr>
<td>Contribution</td>
<td>44,000 lines of code in February 2016</td>
</tr>
<tr>
<td>Sprint to one codebase with unified thinking</td>
<td>Target 3Q release</td>
</tr>
</tbody>
</table>

www.Hyperledger.org
As of 07 September 2016
How Hyperledger Works

1. It all starts with one node
   - Has an Owner
   - ID = Digital Cert
   - Copy of Ledger
   - Issues Transaction
   - Sign Transactions

2. Each node has the shared ledger
   - Blocks
   - Each block has a digital fingerprint of the previous block

3. Nodes form a peer network

4. Users submit transactions

5. Consensus

6. Execution
   - Update A = 100
   - Then A = 10
   - Now A = 100
   - Answer Validated
**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!**
IBM Blockchain offering - **On-premises**

- From Docker Container certified by IBM
- From the code source available on GitHub
Hyperledger Project Scope (Self Managed)

App Layer

Custom Applications
- API libraries and GUIs
- Specialized extensions
- Specialized consensus algos
- Membership policies
- Gateway
- Operations dashboard

Value Added Systems

Core APIs
- Code execution environment
- Ledger data structures
- Modular consensus framework
- Modular identity services
- Network peers

Out of scope

Community + Code
- Linux Hyperledger Project

Blockchain Fabric for a Permissioned, Distributed and Shared Ledger

API libraries and GUIs
Specialized extensions
Specialized consensus algos
Membership policies
Gateway
Operations dashboard

Custom Applications

Out of scope

Community + Code
Linux Hyperledger Project

Blockchain Fabric for a Permissioned, Distributed and Shared Ledger
Hyperledger Project on IBM Systems

IBM Systems

Linux Distribution

Virtualization Technology

Software Requirements

APIs, Protocol

Programming

Database

Container

Virtualization

Out of scope

APIS, Protocols

Core APIs

Blockchain Fabric for a Permissioned, Distributed and Shared Ledger

Custom Applications

GitHub

API Metrics and KPIs
Specialized consent forms
Smart contracts
Blockchain architecture
Insurance
Operations management

APIs, Protocol

CLI, REST, SDK

Programming

Database

Container

Virtualization

IBM LinuxONE™
IBM z Systems
IBM Power Systems

LPAR, KVM, SSC, z/VM

IBM Systems

IBM Systems

IBM Systems

IBM Systems

IBM Systems

IBM Systems

IBM Systems
Hyperledger Acceleration and Security on IBM Systems

- Integrate Existing Business Processes: CICS, IMS, TPF, DB2, VSAM
- Elliptical Curve Digital Signatures (ECC P256, P384)
- Hashing (SHA)
- Crypto Accelerators
- In Memory (10TB)

Global Security Compliance: Enterprise PKCS11, FIPS 140-2, EAL

Optimized network between blockchain nodes – up to 7X more throughput, 82% faster response time
Transaction Anatomy (API Query)

**Type** - The type of the transaction.

**ID** - The ID of a chaincode which is a hash of the chaincode.

**uuid** - A unique ID for the transaction.

**Payload** - Bytes defining the hash of TransactionPayload.payload.

**Cert** - Certificate of the transactor.

**Signature** - Signature of the transactor.
Eg. Hyperledger and IBM z Systems Crypto Stack

Notes:
Implement cryptographic using CPACF & SIMD assembler in the crypto module of GoLang
- Supports clear key crypto
- Allows to speed up secure hashes and clear key crypto using CPACF

➤ Let’s assess the cryptographic performance on IBM LinuxONE™.

Legend:

- clear key
- protected key
- secure key
- Explored path
### Eg. Cryptographic Performance (1 IFL)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Speed (operations/second)</th>
<th>Data Rate (bytes/second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P256Sign</td>
<td>19,356</td>
<td></td>
</tr>
<tr>
<td>P256Verify</td>
<td>7,636</td>
<td></td>
</tr>
<tr>
<td>SHA256x8</td>
<td>40,775,467</td>
<td>40.77 GB/s</td>
</tr>
<tr>
<td>SHA256x1K</td>
<td>1,470,032,300</td>
<td>1.43 GB/s</td>
</tr>
<tr>
<td>SHA256x8K</td>
<td>2,081,554,661</td>
<td>2.08 GB/s</td>
</tr>
<tr>
<td>SHA512x8</td>
<td>29,498,960</td>
<td>29.5 GB/s</td>
</tr>
<tr>
<td>SHA512x1K</td>
<td>1,682,964,910</td>
<td>1.68 GB/s</td>
</tr>
<tr>
<td>SHA512x8K</td>
<td>3,139,587,469</td>
<td>3.14 GB/s</td>
</tr>
<tr>
<td>SHA3_256x8</td>
<td>5,008,226</td>
<td>5.01 GB/s</td>
</tr>
<tr>
<td>SHA3_256x1K</td>
<td>112,317,044</td>
<td>112.3 GB/s</td>
</tr>
<tr>
<td>SHA3_256x8K</td>
<td>123,028,957</td>
<td>123.0 GB/s</td>
</tr>
<tr>
<td>SHA3_512x8</td>
<td>5,508,810</td>
<td>5.51 GB/s</td>
</tr>
<tr>
<td>SHA3_512x1K</td>
<td>69,438,021</td>
<td>69.4 GB/s</td>
</tr>
</tbody>
</table>

**Data size legend:**
- x8: 8 bytes
- x1k: 1024 bytes
- x8k: 8192 bytes

### Digital Signature
- Hardware acceleration with SIMD (x33 Improvement)

### Hash
- Hardware acceleration with CPACF

### Software operations
Hyperledger Purposed Topology Samples on IBM Systems

Extreme Isolation and Security with SSC

Horizontal Peer topology with z/VM or KVM

Vertical Peer topology with massive docker containers
IBM Blockchain offering - Cloud

Bluemix blockchain service

High security business blockchain on Bluemix
# IBM Blockchain for Business – Bluemix®

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Starter</th>
<th>High Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>SoftLayer</td>
<td>IBM LinuxONE™</td>
</tr>
<tr>
<td>Purpose</td>
<td>Development</td>
<td>Simulate a business network</td>
</tr>
<tr>
<td>Environment</td>
<td>Shared multi-tenant</td>
<td>Isolated single tenant</td>
</tr>
<tr>
<td>Secure services container</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Nodes</td>
<td>4 nodes + Certificate Authority</td>
<td>4 nodes + Certificate Authority</td>
</tr>
<tr>
<td>Confidential transactions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dashboard Monitor</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Secure Service Container

High Security Business Network

Secure Service Container (SSC) ensures ...

- Appliance Content (i.e., Blockchain)
- SSC Software Runtime Environment
- Secure Execution Context

No system admin access, ever
- 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

How the Secure Service Container boot sequence works ...

1. Firmware bootloader is loaded in memory
2. Firmware loads the software bootloader from disk
   i. Check integrity of software bootloader
   ii. Decrypt software bootloader
3. Software bootloader activate encrypted disks
   i. Key stored in software bootloader (encrypted)
   ii. Encryption/decryption done on the flight when accessing appliance code and data
IBM Secure Service Container

**Protection from system administrators**
Appliance code cannot be accessed even by platform or system administrators. Data access is controlled by the appliance, therefore unauthorized access is disabled.

This is supported through a combination of signing and encrypting all data in flight and in rest.

All the access to memory is also removed. Firmware supports this with a secure boot architecture.

System administrators have the following limitations when blockchain is secured by the IBM Secure Service Container:
- Cannot access the blockchain node
- Cannot view the blockchain

**Tamper protection**
The IBM Secure Service Container disables all external interfaces that provide LPAR memory access. An image boot loader is signed to ensure that it cannot be tampered or exchanged with a different one.

**Encrypted appliance disks**
All code and data stored on disk is encrypted at all times by using the Linux encryption layer:
- Encapsulated operating system
- Protected IP
- Embedded monitoring and self-healing

Source: [https://console.ng.bluemix.net/docs/services/blockchain/etn_ssc.html](https://console.ng.bluemix.net/docs/services/blockchain/etn_ssc.html)
Overview: High security business network

Service Plan on Bluemix

- Isolated and highly secured environment, distinguishing it from other cloud-hosted offerings
- Operating system, fabric, and nodes all exist in an IBM Secure Service Container, providing your enterprise with a high level of security
- IBM Secure Service Container also delivers performance optimization for peer-to-peer communication, availability, scalability, hardware encryption, & securely encrypted VMs
- Keys secured in HSM

Sign up:

Product documentation:
https://new-console.ng.bluemix.net/docs/services/blockchain/etn_hsn.html

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Starter Plan</th>
<th>High Security Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development</td>
<td>Simulate a business network</td>
<td></td>
</tr>
<tr>
<td>4 nodes + Certificate Authority</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dashboard for registration, monitoring, provisioning &amp; documentation provided through Bluemix</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Network Connections through SoftLayer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cloud Provisioning &amp; Self Service Enablement</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Service Management and Billing through Bluemix</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Customer Support through Bluemix</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Environment</td>
<td>Shared, multi-tenant</td>
<td>Isolated, single tenant</td>
</tr>
<tr>
<td>Secure Service Container</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Highest levels of isolation in industry</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Compliance for highly regulated industries (Keys secured in HSM)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Accelerated performance</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
## Conclusions: 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 |

---

IBM Blockchain 101: Quick-start guide for developers – Free Certification!
Thank you!
Guillaume_hoareau@fr.ibm.com