Securing Commercial Blockchain Networks

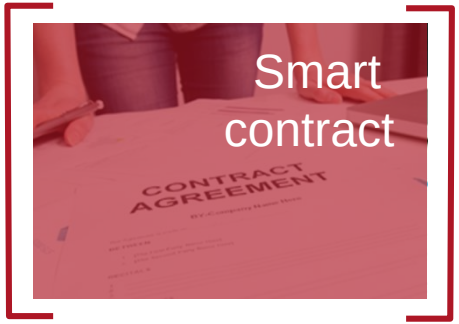
June 12, 2017

Tony Sager, CTO
Commercial Markets

www.BlackRidge.us

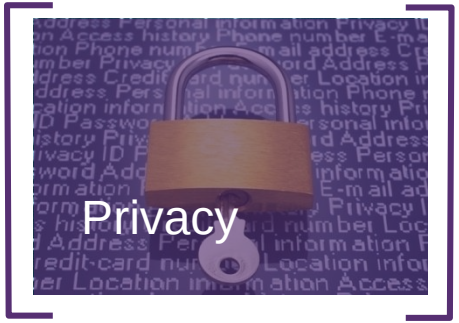
Blockchain for business …

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



Participants are able to trust the contents of the ledger

… Broader participation, lower cost, increased efficiency

Introducing Hyperledger

A **collaborative** effort created 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.

HYPERLEDGER PROJECT

IBM

Make Blockchain real for Business

Shared Ledger
single source of truth

Secure
(Cryptography)
tamper proof

Permissioned (*)
Participants Identity

Private (*)
un-linkable identity

Auditable (*)
prove identity & ownership

Consensus (*)
Modular protocol

Smart Contracts
business logic

Digital assets
Record depository

Confidential (*)
permission control

Scalable (*)
100+ year architecture

LINUX FOUNDATION COLLABORATIVE PROJECTS
HYPERLEDGER PROJECT

IBM Research

THE LINUX FOUNDATION

(*) Hyperledger additional functions

IBM Blockchain Offerings

all running Hyperledger fabric:

Hyperledger fabric

IBM managed on IBM cloud

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

Generally Available

Available on IBM Bluemix!

self managed

Docker

any Docker environment

IBM offers technical support for x86, Power® and z Systems

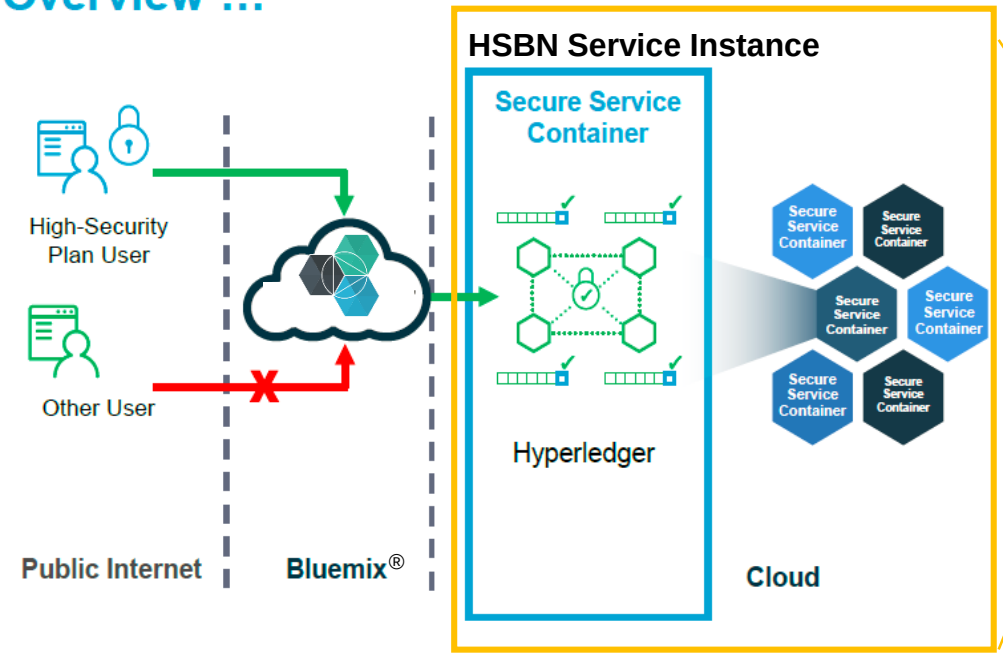
Support for Hyperledger Fabric

Generally Available

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

“Under the hood” of the High Security Business Network Service

Overview …



Runs on IBM LinuxONE™

- HSBN is deployed as a appliance into a Secure Service Container (SSC)
- The SSC runs in a Logical Partition and provides the framework and isolation for hosting the HSBN.
- The appliance combines O/S’s, management runtime services, and the software solution, to deliver full solution in a highly secure runtime environment

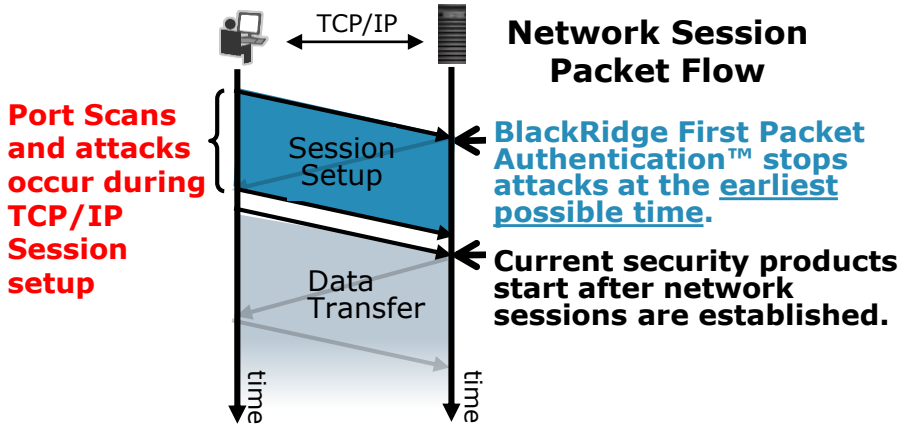
IBM HSBN Beta Overview

- The High Security Business Network plan (limited beta) is open to new subscribers and is based on Hyperledger Fabric v1.0-alpha.
  - It provides an easy mechanism to join Bluemix orgs and build a distributed blockchain network.
  - It runs in a highly secured environment on IBM LinuxONE™, where the network resources (peers, orderers, Certificate Authority, source code, and ledger) are all contained in an IBM Secure Service Container (SSC).
  - You can immediately write and test chaincode applications (business rules) without having to design and configure a private blockchain network.

- Marist College and BlackRidge are jointly conducting research on how to make the industry leading security of IBM HSBN even more secure
  - Leveraging BlackRidge for cyber defense and network segmentation

BlackRidge Stops Network-based Attacks and Addresses Network Compliance

- BlackRidge addresses the TCP/IP network vulnerability that is exploited in 100% of cyber attacks
  - BlackRidge authenticates identity and enforces security policy on the first packet, before a network session is established
- BlackRidge isolates and protects servers and applications
  - Stops port scans and network attacks
  - Provides ROI and reduces risk
  - Addresses network segmentation compliance

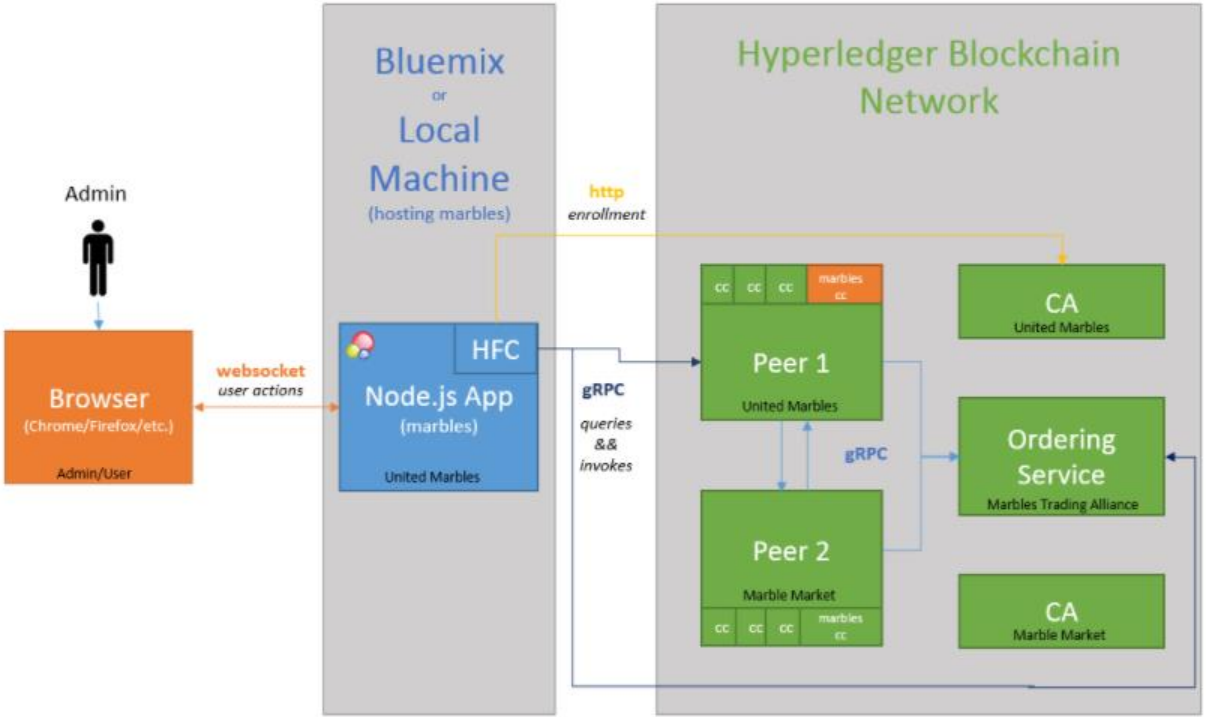


BlackRidge is like "Caller ID for the Internet."

BlackRidge TECHNOLOGY

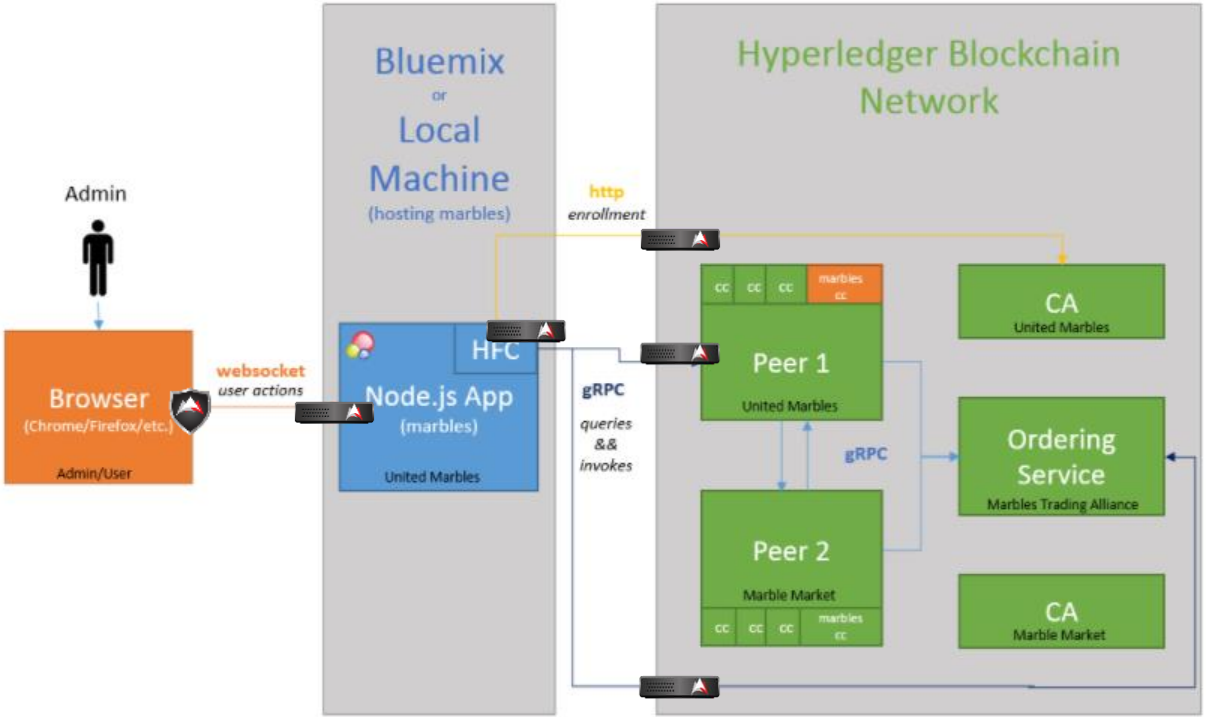
HSBN Function Split

Application Communication Flow



HSBN Function Split:- BlackRidge Placement

Application Communication Flow



BlackRidge Can Provide IBM HSBN Clients with Additional Cyber Attack Protection and Regulatory Compliance Benefits

Benefit	Value	How
Prevents cyber attacks	Isolates and protects Blockchain service from unauthorized users.	Identity-based network security controls that work end-to-end from Client site to the HSBN Secure Service Container • All network connections are cryptographically authenticated on the first packet • Authentication and policy can be based on the HyperLedger Identity management system not on IP • All unauthorized network traffic including ports scans are blocked and logged for analysis.
Regulatory Compliance	Network segmentation for compliance audits and risk reduction	Identity-based network segmentation provides traffic separation • Separation of internal network traffic between Clients and between administrative functions and Blockchain operations. • Audit trail (logs) of all authorized and unauthorized network connections to the Client's Blockchain. • BlackRidge could enhance the access control of channels in the ledger by utilizing it's policy engine

BlackRidge / Marist HSBN Beta Experience

- HSBN does allow immediate coding of Blockchain applications without having to build in-house infrastructure
  - This eliminates weeks of work to build out own peers, ordering service and a Certificate Authority
- We are using the Marbles V2 sample application as a basis for coding our new uses cases
- Through experimenting with the IBM HSBN beta we validated that browser function can be separated from the Node.js server
  - This fits the Marist use case better to outsource all aspects of application development for the blockchain to Marist and just provide Marist customers with the service
  - Moving the Node.js server next to the Hyperledger blockchain network will make it easier to deploy the technology
  - Deploying https/tls for the browser to Node.js server communication makes it secure and facilitates off loading the Node.js server and HFC function to the blockchain provider

BlackRidge / Marist HSBN Beta Next Steps

- Finish coding the Node.js and chaincode for the Marist and BlackRidge use cases
  - Eliminate fraud from philanthropic giving
  - Automate business agreements (NDA, Equipment loan …)
- Finish coding the Browser UI code to the new use cases
- Move browser to Node.js server interface to https/TLS protected by BlackRidge and test
- Test app internally at Marist
  - Prove out BlackRidge benefits to HSBN security
- Find external beta customer for additional testing of Marist use case