BLOCKCHAIN

Experiencias / PoC / Pasos a Seguir

agesic

“

Una historia de Contenedores, Scripts, Seguridad, Experimentación, Ensayo, Error y algo de Blockchain también...

TECNOLOGIAS EMERGENTES

* División del Área de Tecnología @ AGESIC.
* Investigamos Tecnologías y su Aplicación.
* Armamos PoC's, analizamos viabilidad.
* Experimentamos diferentes plataformas.
* Redes, Cloud, Plataformas, Servicios, etc.

Dinamismo, Transmisión y Buenas Prácticas.

Caracteristicas de las Blockchain

BASE DE DATOS DISTRIBUIDA

muchos nodos saben lo mismo.

BLOQUES ENLAZADOS

Datos relacionados e inmutables.

MARCADOS POR TIEMPO

Sello de tiempo inviolable.

BLOCKCHAINS PÚBLICAS

Son las utilizadas mayormente por las criptomonedas.

Bitcoin - Ethereum - Litecoin - Dash - Bitcoin Cash - Dogecoin - Ripple - Monero - NEM - EOS - Iargo etc

Por cotizaciones del mercado según moneda
check -> coinmarketcap.com

BLOCKCHAINS PÚBLICAS

* No hay confianza en participantes.
* Cualquiera puede ser participar.
* Consenso para validaciones.
* Validaciones transaccionales lentas.

Proof of Work con incremento progresivo de dificultad check -> Attacker has a lot of Computing Power

BLOCKCHAINS PRIVADAS / PERMISIONADAS

Son las utilizadas en ambientes controlados.

* Hyperledger Fabric - R3 Corda - Eth Pvr - NEM Prv - etc
* Implementaciones muy diferentes
* Diferentes tipos de confianza en participantes
* Diferentes tipos de consenso (!= PoW)
* Inferior cantidad de nodos en gral. (!anonimato)

Concepto de SMART Contract/Chaincode reafirmado

Requerimientos de la PoC Blockchain

PROCESAR UN ARCHIVO

subir sus datos al ledger.

DATOS EN BLOCKCHAIN

Hash, Timestamp y Filename.

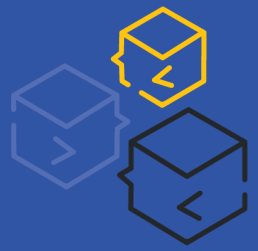
CHAINCODE CON CONTROLES

Registros Inmutables.

Software Utilizado

HYPERLEDGER
FABRIC

HYPERLEDGER
EXPLORER



HYPERLEDGER
COMPOSER

docker

Hyperledger Fabric

Framework de Blockchain Privada y Permisionada.

* Concepto de Usuarios y Organizaciones
* Cantidad de Peers configurables
* Arquitectura de producción redundante
* Chaincode (Smart Contract) programable
* SDK Multi (NodeJS/GO/Java/Python/REST)
* Backend en Base de Datos NoSQL (CouchDB)

Muy Flexible y Configurable

HYPERLEDGER FABRIC

Componentes Utilizados por la PoC.

* Docker (base de HL, DB's, imágenes)
* CouchDB (NoSQL) Backend
* Blockchain Explorer
* NodeJS para creación de UI con NodeJS-SDK
* GO Language para creación del Chaincode (SC)

HyperLedger es Software Libre gerenciado por la Linux Foundation

DEMO !

SIGUIENTES PASOS / SEGURIDAD / PLATAFORMA

* Revisar seguridad en imágenes de SO.
* Portar Hyperledger Fabric a PaaS (Openshift).
* Compilar Fabric desde 0 con imágenes propias.
* Alta de Plataforma de Modelado (Composer).
* Revisar Seguridad en Transmiciones de Datos.

Personalizar todos los componentes -> creación de Script.
Evaluar GRPCs, BCaaS, M-Tenants, NoSQL-BD, Registry, etc.

CUSTOMIZED

IMAGES

```
nicolaspence/fabric-peer                amd64-1.2.1
nicolaspence/fabric-orderer             amd64-1.2.1
nicolaspence/fabric-ca                  amd64-1.2.1
nicolaspence/fabric-couchdb             amd64-0.4.11
nicolaspence/fabric-tools               amd64-1.2.1
nicolaspence/fabric-testenv             amd64-1.2.1
nicolaspence/fabric-buildenv            amd64-1.2.1
nicolaspence/fabric-ccenv               amd64-1.2.1
nicolaspence/fabric-baseimage           amd64-0.4.11
nicolaspence/fabric-basejvm             amd64-0.4.11
nicolaspence/fabric-baseos              amd64-0.4.11
```

SEGURIDAD EN IMAGENES

< Projects < Repositories < nicolaspence/hyperledger-fabric-peer

nicolaspence/hyperledger-fabric-peer:latest

Author	anonymity
Architecture	amd64
OS	linux
Docker Version	18.03.1-ce
Scan Completed	Jul 25, 2018

0 highLevel Vulnerabilities
2 mediumLevel Vulnerabilities
7 lowLevel Vulnerabilities
0 unknownLevel Vulnerabilities

SCAN

Vulnerability	Severity	Package	Current version
CVE-2017-8804	medium	glibc	2.23-0ubuntu10
CVE-2015-5180	low	glibc	2.23-0ubuntu10
CVE-2016-10228	negligible	glibc	2.23-0ubuntu10
CVE-2018-6485	medium	glibc	2.23-0ubuntu10
CVE-2017-12133	low	glibc	2.23-0ubuntu10
CVE-2017-12132	medium	glibc	2.23-0ubuntu10
CVE-2015-8985	low	glibc	2.23-0ubuntu10
CVE-2016-2781	low	coreutils	8.25-2ubuntu3~16.04

SEGURIDAD

EN IMAGENES

< Projects < Repositories < nicolaspence/fabric-peer

nicolaspence/fabric-peer:latest

Author	anonymity
Architecture	amd64
OS	linux
Docker Version	18.03.1-ce
Scan Completed	Jul 25, 2018

0 highLevel Vulnerabilities

0 mediumLevel Vulnerabilities

0 lowLevel Vulnerabilities

0 unknownLevel Vulnerabilities

AUTOMATIC

SCRIPT

```
#!/bin/sh

# Variables Globales
CHANNEL_NAME="agpocchan"
CHAINCODE_NAME="agchaincode"
CLI_TIMEOUT=10000
OS=$(uname -s)
HL_IMAGES_DEFAULT_VERSION="x86_64-1.0.6"
HL_COUCHDB_DEFAULT_VERSION="x86_64-1.0.6"
HL_BASE_DEFAULT="hyperledger"

##
# Validacion de Sistema Operativo para tomar acciones segun comandos
##
if [ $OS == "Linux" ]
  then
    ECHOFIX="-e"
elif [ $OS == "Darwin" ]
  then
    ECHOFIX=""
  else
    echo "Operating System '$OS' not recognized."
    exit 1
  fi
```

AUTOMATIC

SCRIPT

```
$ docker ps --format '{{.Image}} ---> {{.Names}}' | grep --color agpoc.agesic.gub.uy
nicolaspence/fabric-tools:amd64-1.2.1 ---> cli.agpoc.agesic.gub.uy
nicolaspence/fabric-peer:amd64-1.2.1 ---> peer0.agpoc.agesic.gub.uy
mariadb ---> explorerdb.agpoc.agesic.gub.uy
nicolaspence/fabric-peer:amd64-1.2.1 ---> peer1.agpoc.agesic.gub.uy
nicolaspence/fabric-couchdb:amd64-0.4.11 ---> couchdb0.agpoc.agesic.gub.uy
nicolaspence/fabric-ca:amd64-1.2.1 ---> ca.agpoc.agesic.gub.uy
nicolaspence/fabric-orderer:amd64-1.2.1 ---> orderer.agpoc.agesic.gub.uy
nicolaspence/fabric-couchdb:amd64-0.4.11 ---> couchdb1.agpoc.agesic.gub.uy
```

🎓 LECCIONES APRENDIDAS

* SDK’s disponibles para varios lenguajes (algunas en beta)

* Flexibilidad en la Chaincode/Smart Contract

* PaaS ready / Escalable / Distribuido

* Interacción entre diferentes Entidades

* Posee Organizaciones/Canales/Usuarios/Permisos

* Autorización Granular pensada para entornos Empresariales

agesic

LECCIONES APRENDIDAS

* Falta de documentacion precisa para desarrollo (SDK/CC)
* Imagenes de software con vulnerabilidades de seguridad
* Curva de aprendizaje larga para el despliegue
* SDK’s disponibles para varios lenguajes (varias en beta)

agesic

PREGUNTAS ?

agesic