Hola, mi nombre es **Daniel Mery**....

Soy co-fundador de:
BlockMAD
HackMadrid %27
HaskellMAD
Planet Linux Caffe

https://twitter.com/dmery

danmery@protonmail.com

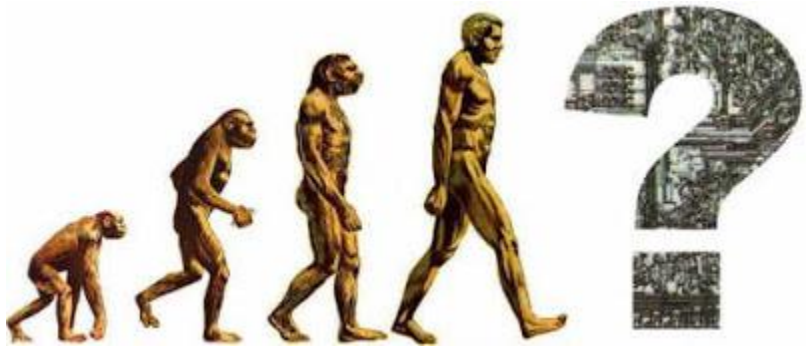
En un principio blockchain era Bitcoin .....

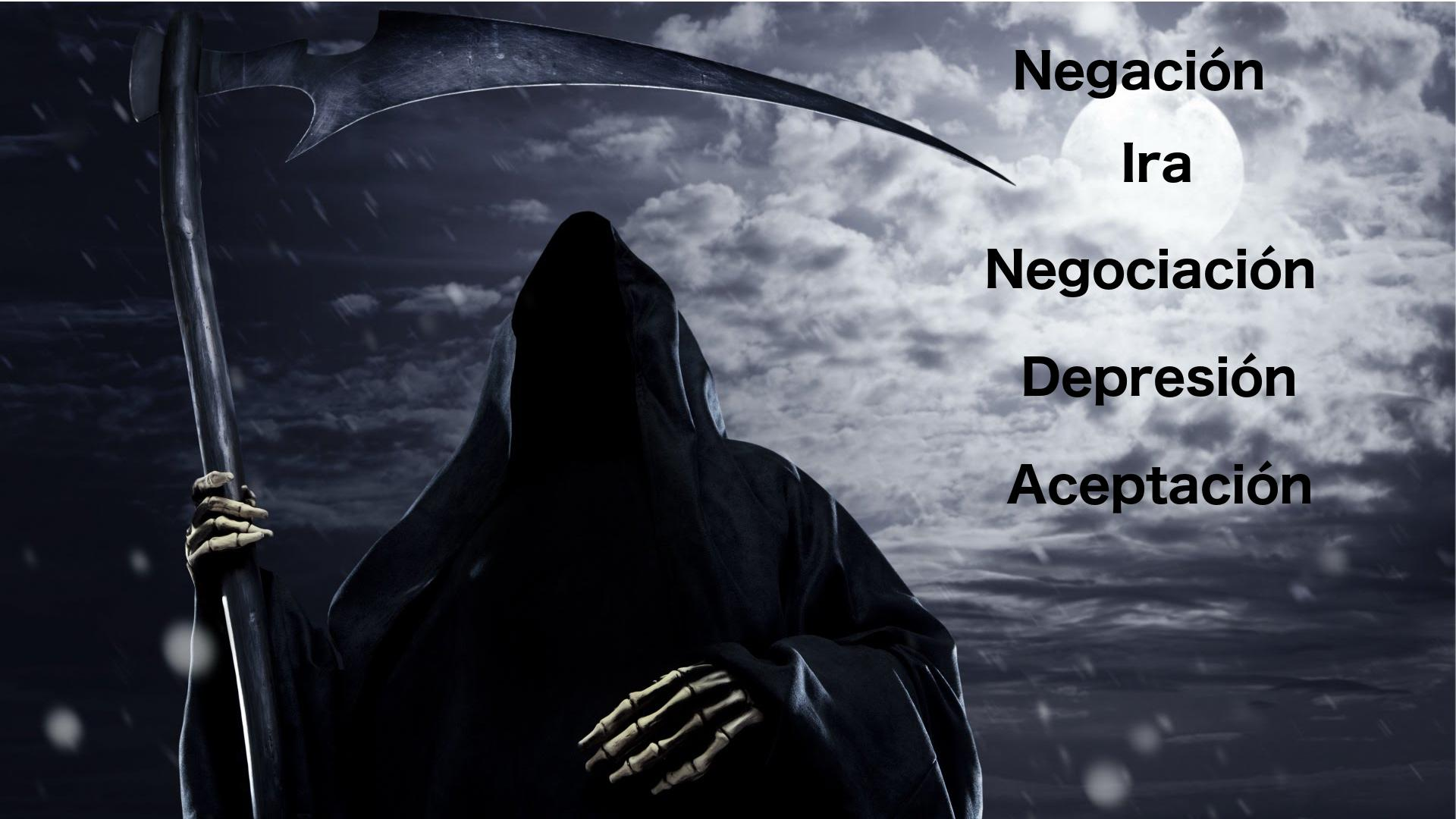
La caja de Pandora Digital

La lámpara mágica de cripto

Un largo camino hemos recorrido…..

¿Cual será nuestro destino?




Negación
Ira
Negociación
Depresión
Aceptación

Luego fuímos descubriendo que la tecnología Blockchain tiene infinitas aplicaciones que implica un cambio disruptivo

Gobierno
Gestionar los desechos
Identificación
Control de fronteras
Registros médicos
Almacenamiento de información
Música
Auditar la emisión de carbono
Cadena de suministros
Trazabilidad de los diamantes
Bienes raíces
Industria pesquera
Trazabilidad de obras de arte
Trazabilidad en el uso de energías
Bonos catastrofes

Sistemas de reservas (hoteles)
Control de envíos (transportes)
Pago de Impuestos, emisión de facturas
Registro de propiedad
Seguros
Publicidad
Periodismo
Ciudades inteligentes
Info almacenamiento de Petróleo
Logística en operaciones ferroviarias
Transferencia y propiedad en videojuegos
Leasing de vehículos
Distribución de electricidad
Protección de especies en peligro
Seguridad

¿Cómo empezo esta historia?

Máquina Universal -Alan Turing

Teoría de Juegos -Von Neumann y Forbes Nash

Criptografía -Manifesto Cypherpunks

Árbol de Merkle, marca de tiempo -Ralph Merkle

Econometría

Bitcoin -Satoshi Nakamoto

Los Cyberpunks haciendo historia

1976 -W. Diffie y M. Hellman crean el algoritmo Diffie-Hellman y propusieron romper las claves encriptadas en 2 partes: clave pública y clave privada (criptografía asimétrica). R. Merkle crea los árboles de Merkle. Árbol binario

1977 -Ron Rivest, Adi Shamir y Leonard Adleman inventaron el Algoritmo RSA (siglas de sus apellidos) para la generación de claves, el cifrado y el descifrado de mensajes

1991 -Phil Zimmermann crea PGP (Pretty Good Privacy), el primer software de encriptación utilizado

1992 -Timothy C. May escribe, uno de los textos de referencia, manifiesto cripto-anarquista

1994 -Derek Atkins, Michael Graff, Arjen K. Lenstra y Paul C. Leyland resuelven una problema criptográfico, poniendo a trabajar en ese problema a muchos ordenadores alrededor del mundo para sumar más capacidad de cómputo


Blockchai
n
Percepciones e
intuiciones

Una definición previa del Blockchain

Que es:

Open Source

Red de nodos P2P

Base de datos distribuída

Bitácora

Anónima

Que no es:

Un esquema Ponzi

Una estafa financiera

Un paraíso fiscal virtual

Una Burbúja

Una Moda

Una primera conclusión

¿Que es la confianza y que es un sistema basado en ella?

¿Son los datos la materia prima fundamental de la moderna sociedad?

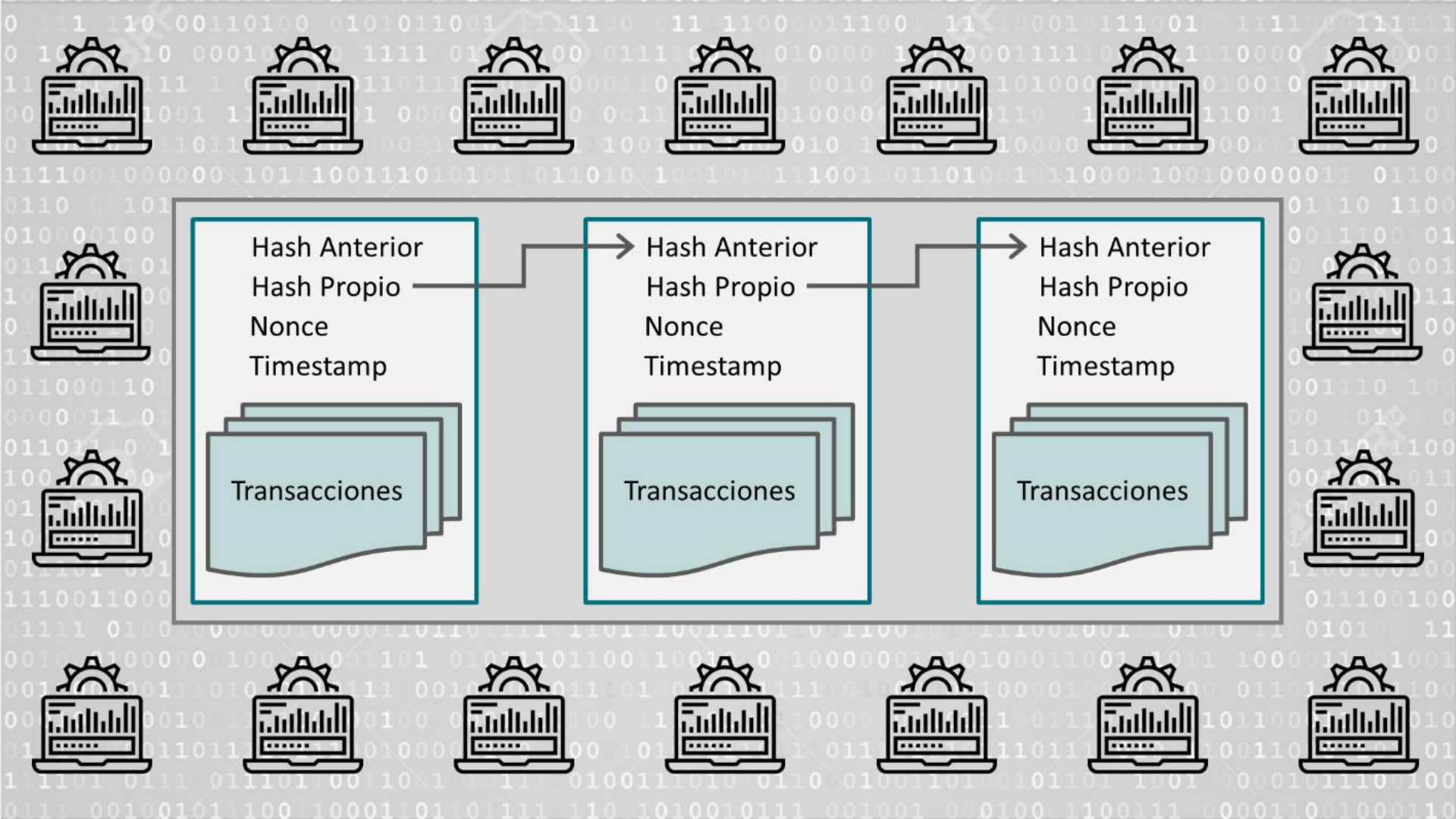
¿Cuales son en realidad los cambios profundo que propone el blockchain?

WEB 2	WEB 3
Intercambio de Información	Intercambio de valores
Credibilidad en terceros	Determinación algorítmica
Sociedad Industrial	Sociedad Inteligente

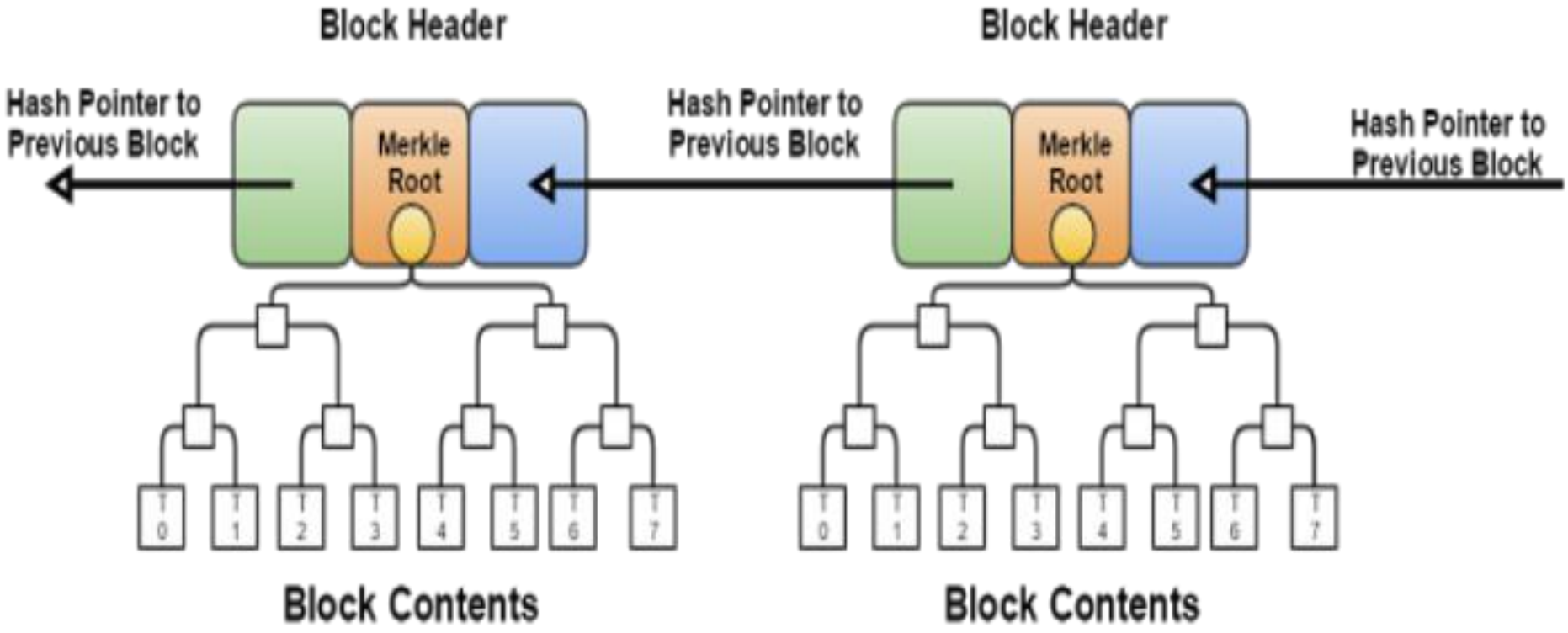
¿Definamos mejor al blockchain?

Es una cadena de bloques y esta cadena de bloques es una base de datos distribuida.

Un sistema de Bases de Datos Distribuida es una estructura en la cual las bases de datos ubicadas en múltiples sitios por un sistema de comunicaciones de forma tal que: un usuario ubicado en cualquier sitio puede acceder los datos en cualquier parte de la red exactamente como si estos fueran accedidos de forma local.


Hash Anterior
Hash Propio
Nonce
Timestamp
Transacciones
Hash Anterior
Hash Propio
Nonce
Timestamp
Transacciones
Hash Anterior
Hash Propio
Nonce
Timestamp
Transacciones

A Representation of the Bitcoin Blockchain



Refinamos nuestra definición

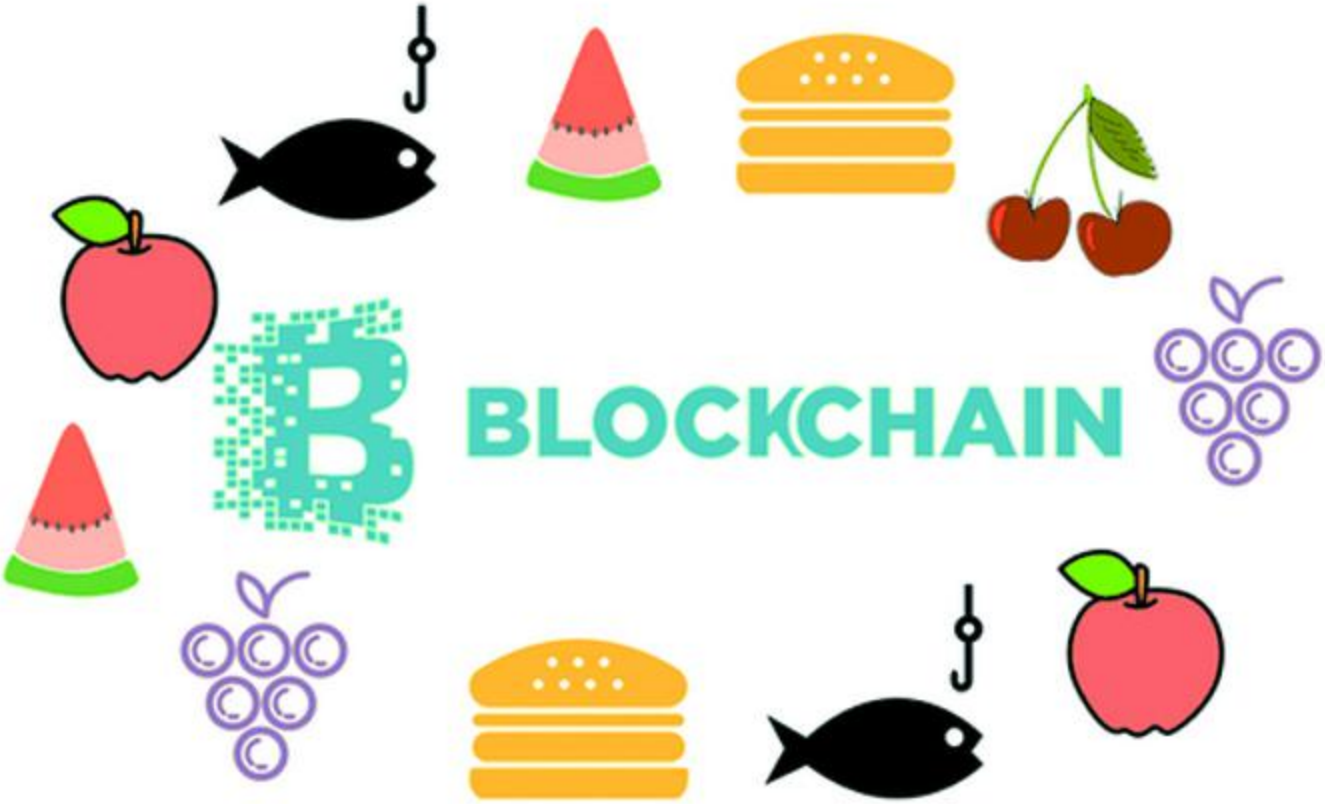
Este sistema de bases de datos distribuida, está formado por cadenas de bloque para evitar su modificación una vez que el dato ha sido publicado utilizando un sellado de tiempo confiable y enlazado a un bloque anterior. Esto permite almacenar datos en forma creciente ordenados en el tiempo e inmodificables.

Tres características importantes

Almacenamiento de los datos. Se realiza utilizando la replicación de los datos de la cadena de bloques.

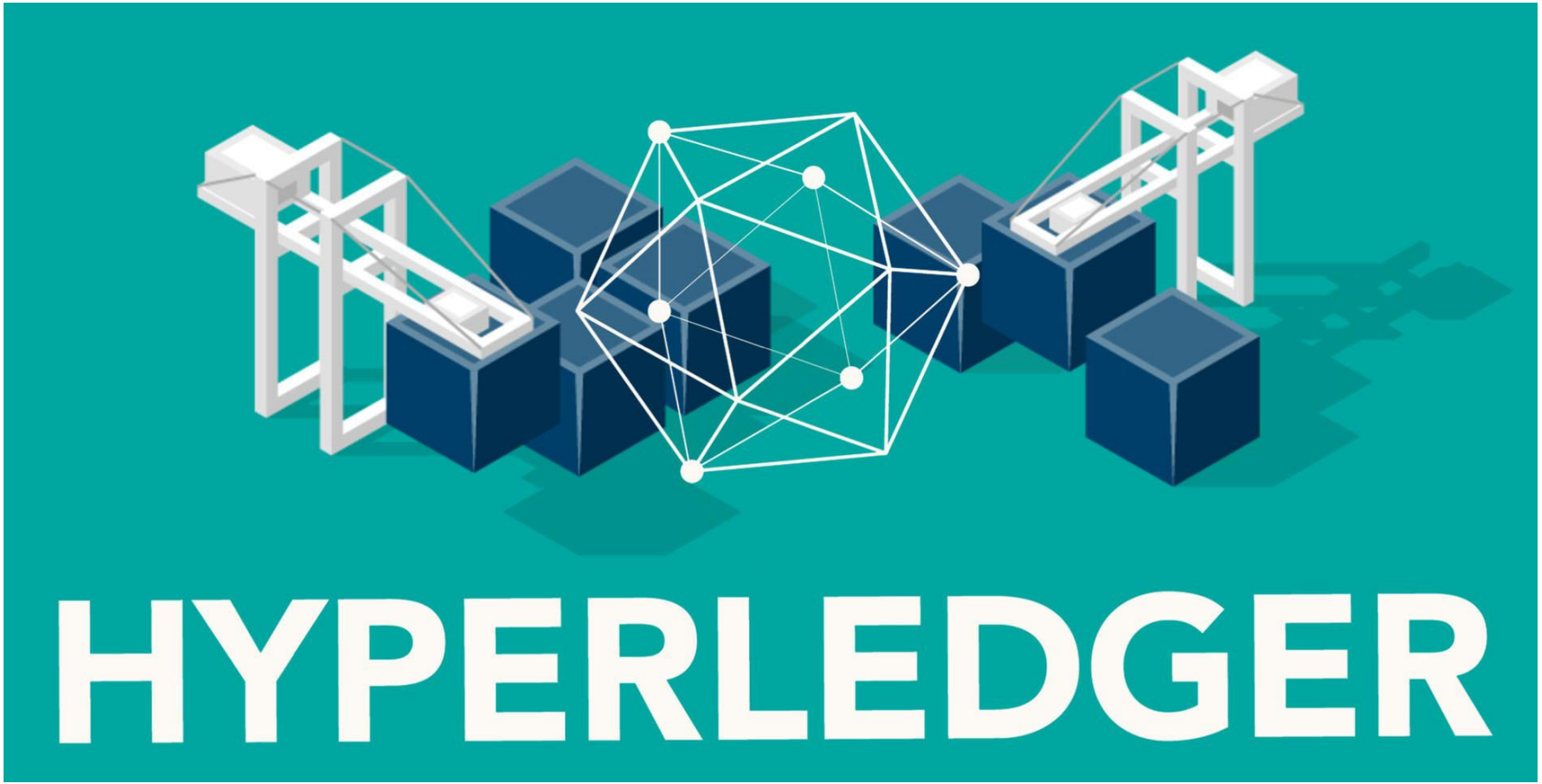
Transmisión de los datos. Peer-to-Peer (P2P), es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Confirmación de los datos. Es un proceso de “consenso” entre los nodos participantes. Es un problema que consiste en averiguar como un conjunto de procesos de computación aislados que solo pueden comunicarse con mensajes se ponen de acuerdo sobre algo. La solución a este problema es el algoritmo de consenso (POW, POS, PoET).


BLOCKCHAIN

Producción Alimentaria y Sistema de Trazabilidad

¿Que tipo de blockchain utilizamos?



BLOCKCHAIN

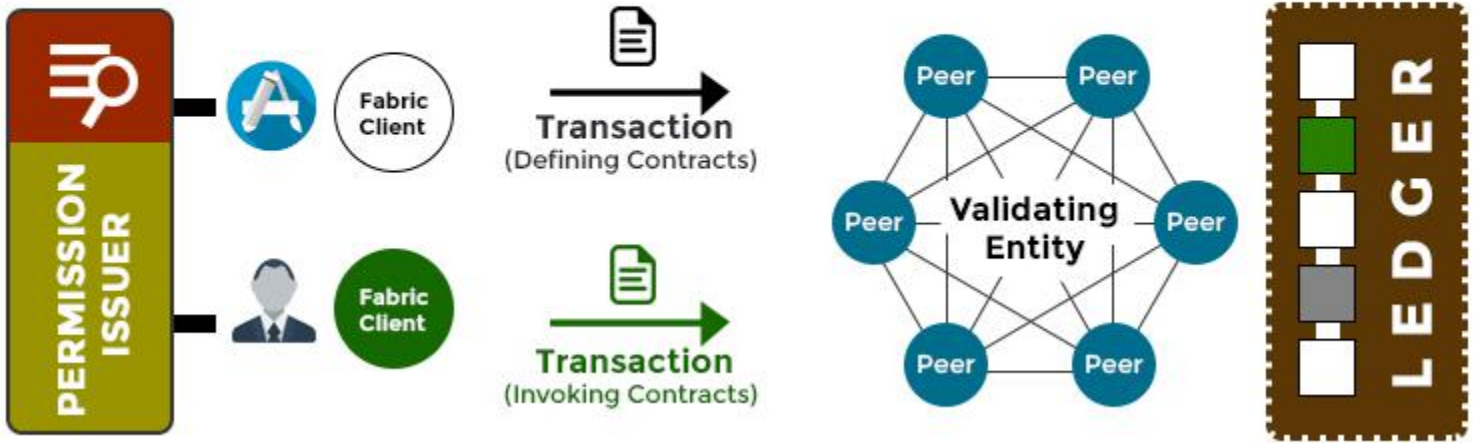
HYPERLEDGER

¿ Qué es Hyperledger ?

Es un proyecto de código abierto creado y hospedado por la Linux Foundation en el 2015. Su objetivo es promover las tecnologías blockchain en la industria para garantizar la responsabilidad, la transparencia y la confianza entre los socios comerciales. Como resultado, Hyperledger hace que la red y las transacciones comerciales sean más eficientes.

Distributed Ledger Technology -DLT- (libro mayor distribuido) es un tipo de estructura de datos que reside en múltiples dispositivos informáticos, generalmente distribuidos en ubicaciones o regiones, que incluye tecnologías blockchain y contratos inteligentes.

HYPERLEDGER FABRIC



2

Summary – HyperLedger Fabric Architecture

3 Components of Fabric

CA

- Registration of identities
- Manage Certificates

Peer

- Endorses Tx
- Simulates Tx
- Commits Tx

1

SDK

2

Orderer

- Consensus verification
- Creates Blocks

kafka

All these components can be clustered for scalability and to avoid Single Point of Failure

Ledger

Blockchain & World State

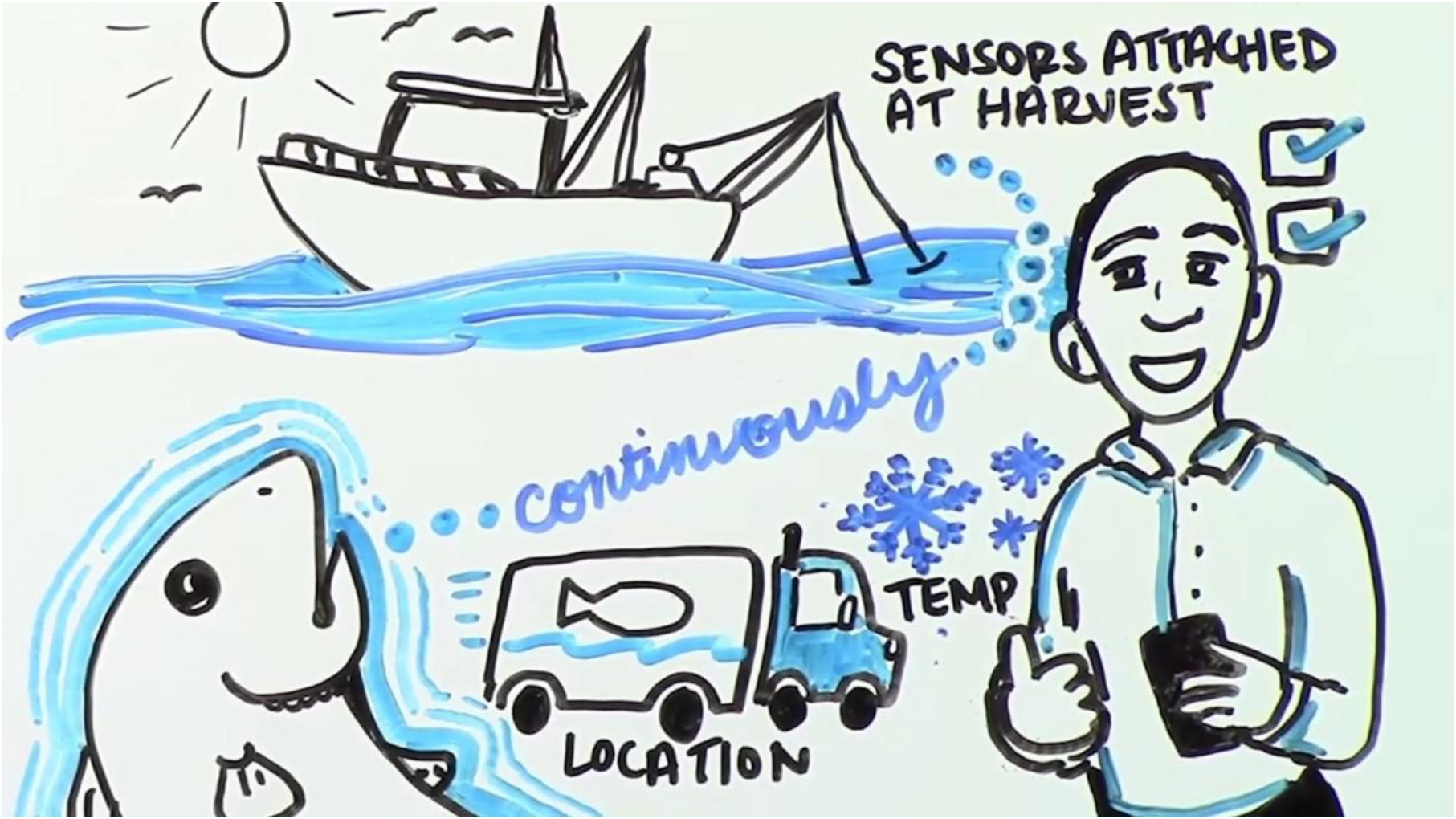
Channels

- **Private subnet** for a set of parties based on Smart contract
- **Ledger / Channel**
- **Peers** can have multiple Channels

Smart Contract

Other Concepts

- Endorsement Policies
- **Assets** : Anything that's valuable for the Organization
- **Transactions** (State changes of Assets)
- **Gossip Protocol** : The glue that keeps the peers in healthy state.


SENSORS ATTACHED AT HARVEST
continuously
TEMP
LOCATION

Problemas de la industria pesquera

El gasto, a nivel mundial, es de 3 billones de dólares por año en recursos para la industria pesquera marina

Las industria pesquera emplea más de 200 millones de personas, desde la captura hasta el procesamiento, el envío y la venta final al usuario

El 40% de nuestros océanos están afectados por la pesca ilegal

Cada año, se venden 5 millones de toneladas de atún, con un valor estimado de 40 billones de dólares.

Con la Declaración de Trazabilidad de Tuna 2020 en mente, nuestro objetivo es eliminar la pesca ilegal, no declarada y no reglamentada.

Se utiliza Hyperledger Fabric para brindar transparencia y claridad a un ejemplo del mundo real: la cadena de suministro de la pesca de atún.

Conceptos destacados de Hyperledger Fabric

HYPERLEDGER FABRIC

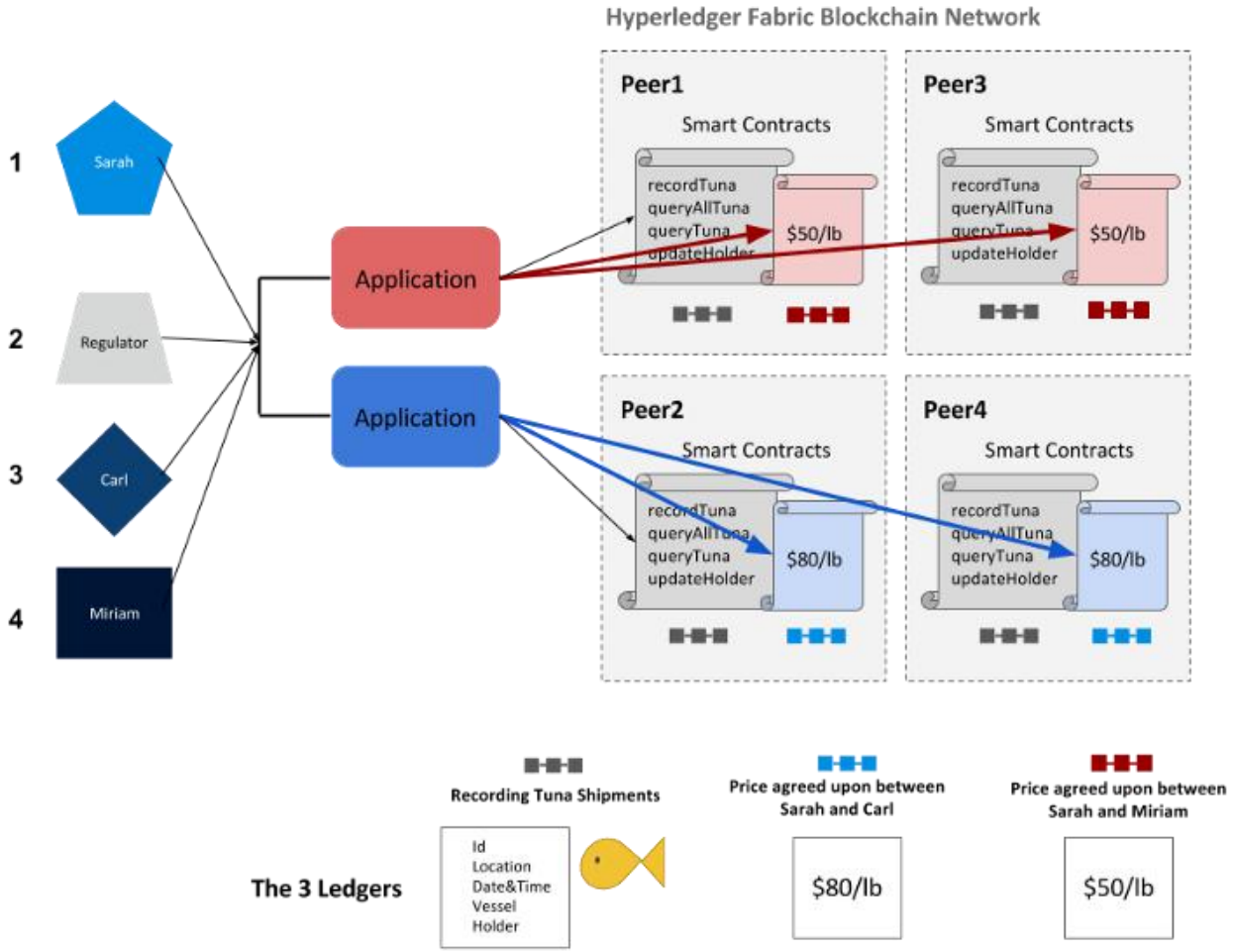
Canales. Son mecanismos para dividir datos que permitan la visibilidad de las transacciones sólo a las partes interesadas. Cada canal es una cadena independiente de bloques de transacciones que contiene solo transacciones para ese canal en particular.

Chaincode (smart contracts). Encapsula tanto las definiciones de los activos como la lógica de negocios (transacciones) para modificar estos activos. Las invocaciones de transacciones dan como resultado cambios en el libro mayor.

Ledger. Contiene la totalidad el estado actual de la red y la cadena de invocaciones de las transacciones. Un libro de contabilidad mayor compartido y permisionado es solamente un anexo de un sistema de registros y sirve como una única fuente de verdad.

Network. es una colección de pares, que forman una red de blockchain, para el procesamiento de datos. La red (network) es responsable de mantener un libro de contabilidad mayor replicado consistentemente.
Servicio de ordenamiento. es una colección de nodos que ordena todas las transacciones en un bloque.

Estado Global. Refleja el estado de los datos actuales sobre todos los activos en la red. Estos datos se almacenan en una base de datos para un acceso eficiente. Las bases de datos soportadas actuales son LevelDB y CouchDB.
MSP (Member Service Provider). Es el proveedor de servicios de membresía, administra la identidad y el acceso permitido para clientes y pares.


Hyperledger Fabric Blockchain Network
1
Sarah
2
Regulator
3
Carl
4
Miriam
Application
Application
Peer1
Smart Contracts
recordTuna
queryAllTuna
queryTuna
updateHolder
$50/lb
Peer3
Smart Contracts
recordTuna
queryAllTuna
queryTuna
updateHolder
$50/lb
Peer2
Smart Contracts
recordTuna
queryAllTuna
queryTuna
updateHolder
$80/lb
Peer4
Smart Contracts
recordTuna
queryAllTuna
queryTuna
updateHolder
$80/lb
Recording Tuna Shipments
Price agreed upon between Sarah and Carl
Price agreed upon between Sarah and Miriam
The 3 Ledgers
Id
Location
Date&Time
Vessel
Holder
$80/lb
$50/lb

Muchas Gracias!