El futuro digital es de todos

MinTIC

Blockchain & analítica de datos

para industrias digitales

etraining
Diseñamos nuevas formas de aprender

tecnalia Colombia
Inspiring Business

Agenda

- Estrategias de implementación Blockchain
- Programación contrato inteligente

APLICACIONES DE BLOCKCHAIN

El futuro digital es de todos

MinTIC

SEGUIMIENTO Y RASTREO DE PRODUCTOS Y SERVICIOS

Diseñamos nuevas formas de aprender

Inspiring Business

El futuro digital es de todos

MinTIC

MEDIOS DE PAGO Y SECTOR FINANCIERO

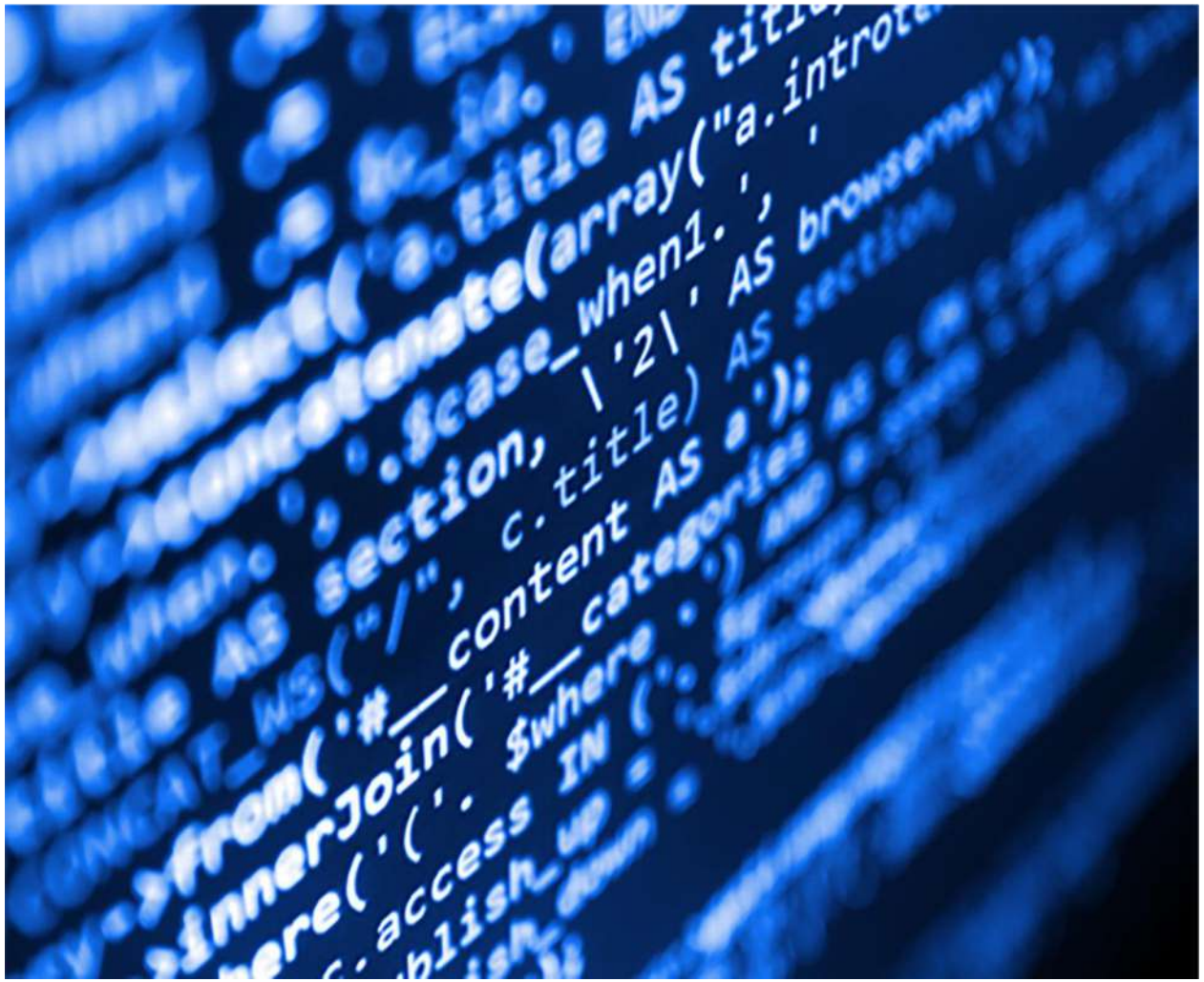
GESTIÓN IDENTIDADES

Identidad digital

El futuro digital es de todos

MinTIC

APLICACIÓN EN CONTRATOS



etraining
Diseñamos nuevas formas de aprender

tecnalia Colombia
Inspiring Business

Fidelización y recompensa

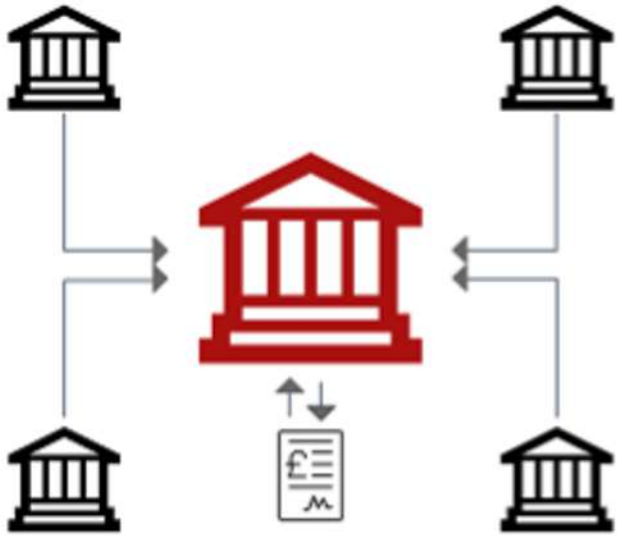

¿CUANDO USAR
BLOCKCHAIN ?

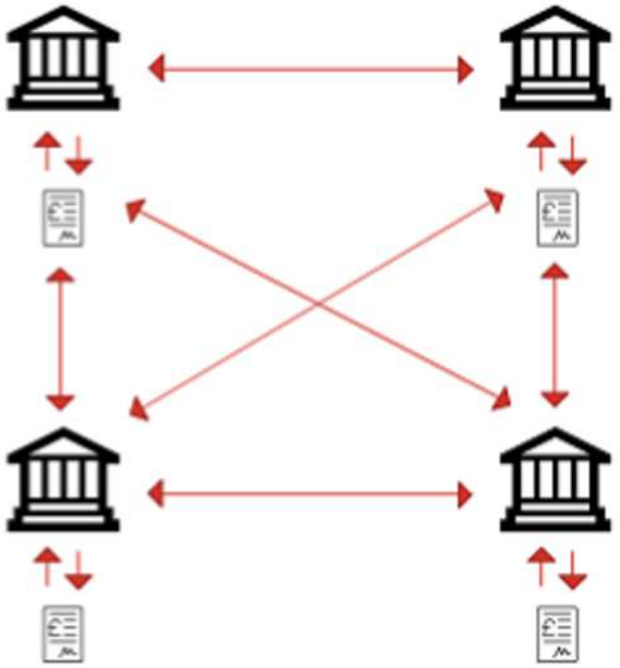
BLOCKCHAIN CAMINO DE DECISIÓN

¿Se necesita una base de datos compartida?

1

Si

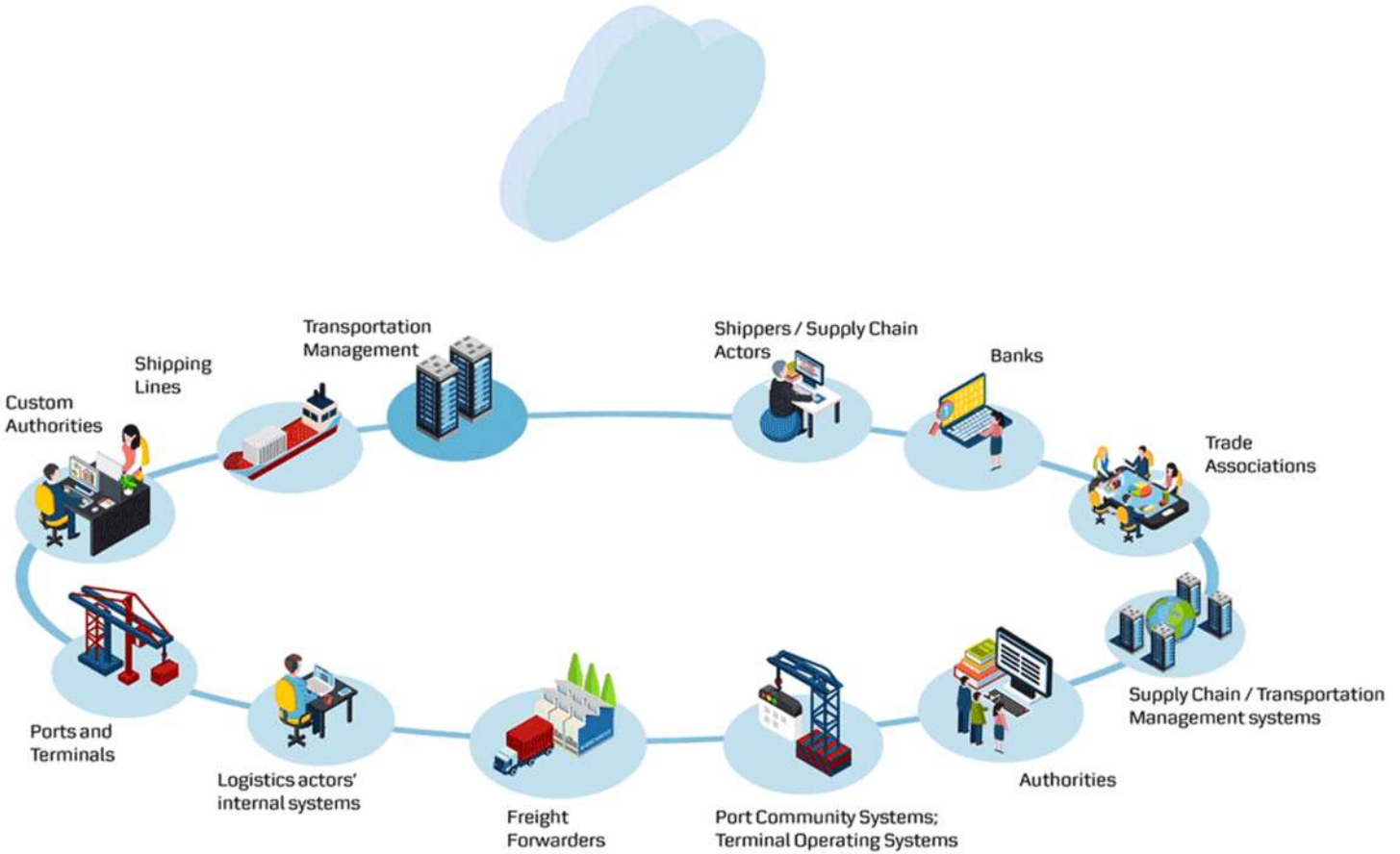




2

¿Múltiples partes involucradas?

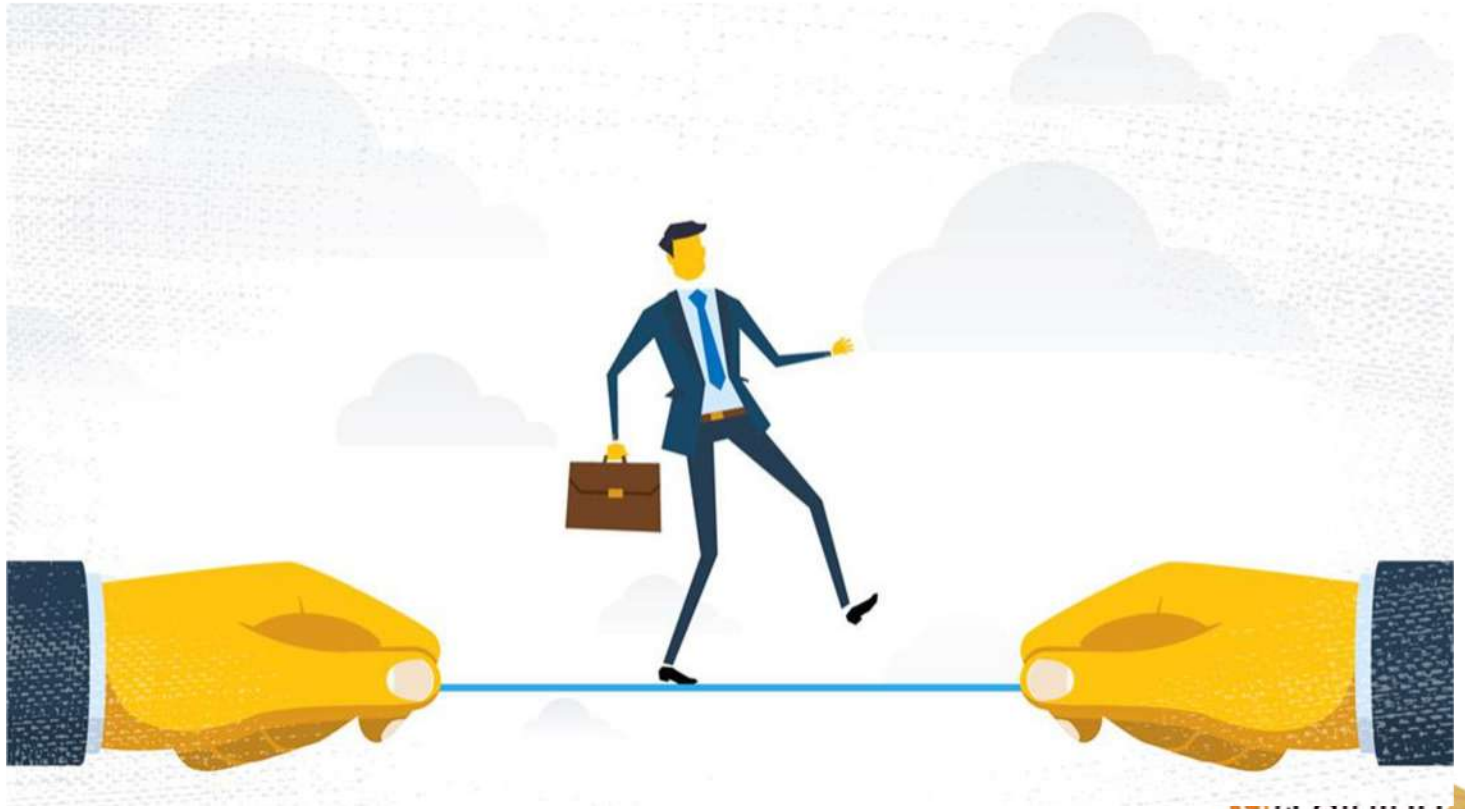
Si



3

Si

¿Las partes involucradas tienen “conflicto de interés” o no son “confiables”?



4

¿Necesidad de un registro objetivo e inalterable?

Si

5

Si

¿Las reglas de las transacciones no cambian con frecuencia?

¿Son las transacciones publicas?

bitcoin

ethereum

HYPERLEDGER

corda

BLOCKCHAIN CAMINO DE DECISIÓN

¿Se necesita una base de datos compartida?

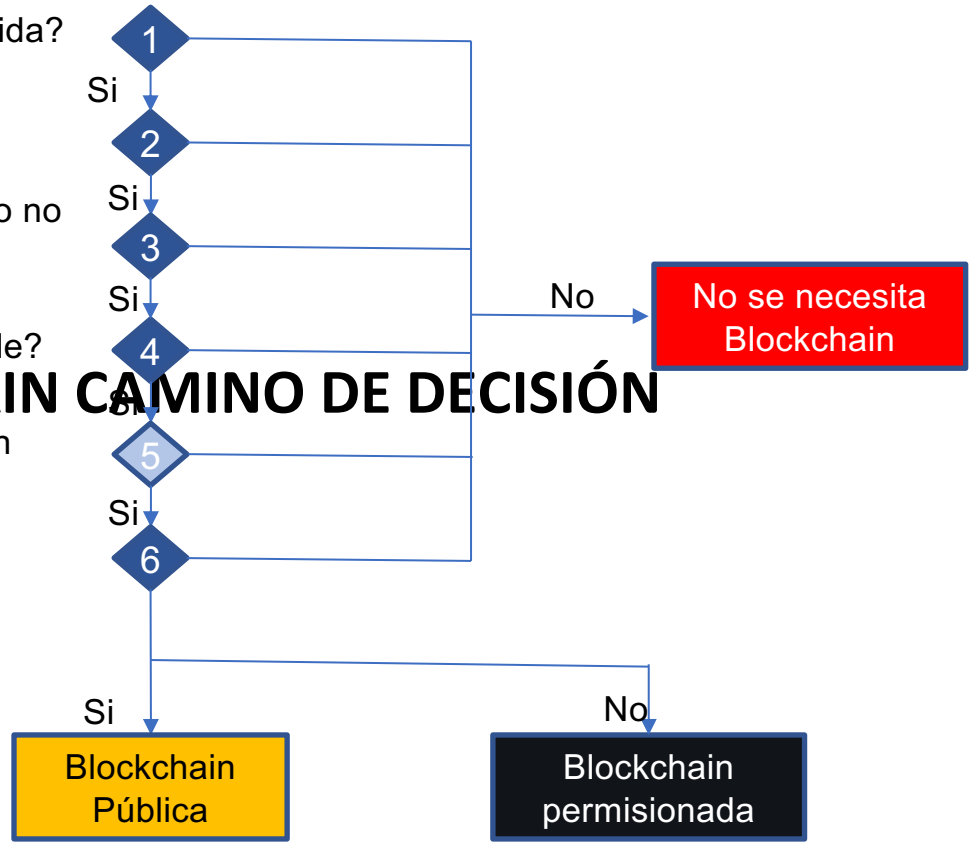
¿Múltiples partes involucradas?

¿Las partes involucradas tienen “conflicto de interés” o no son “confiables”?

¿Necesidad de un registro objetivo e inalterable?

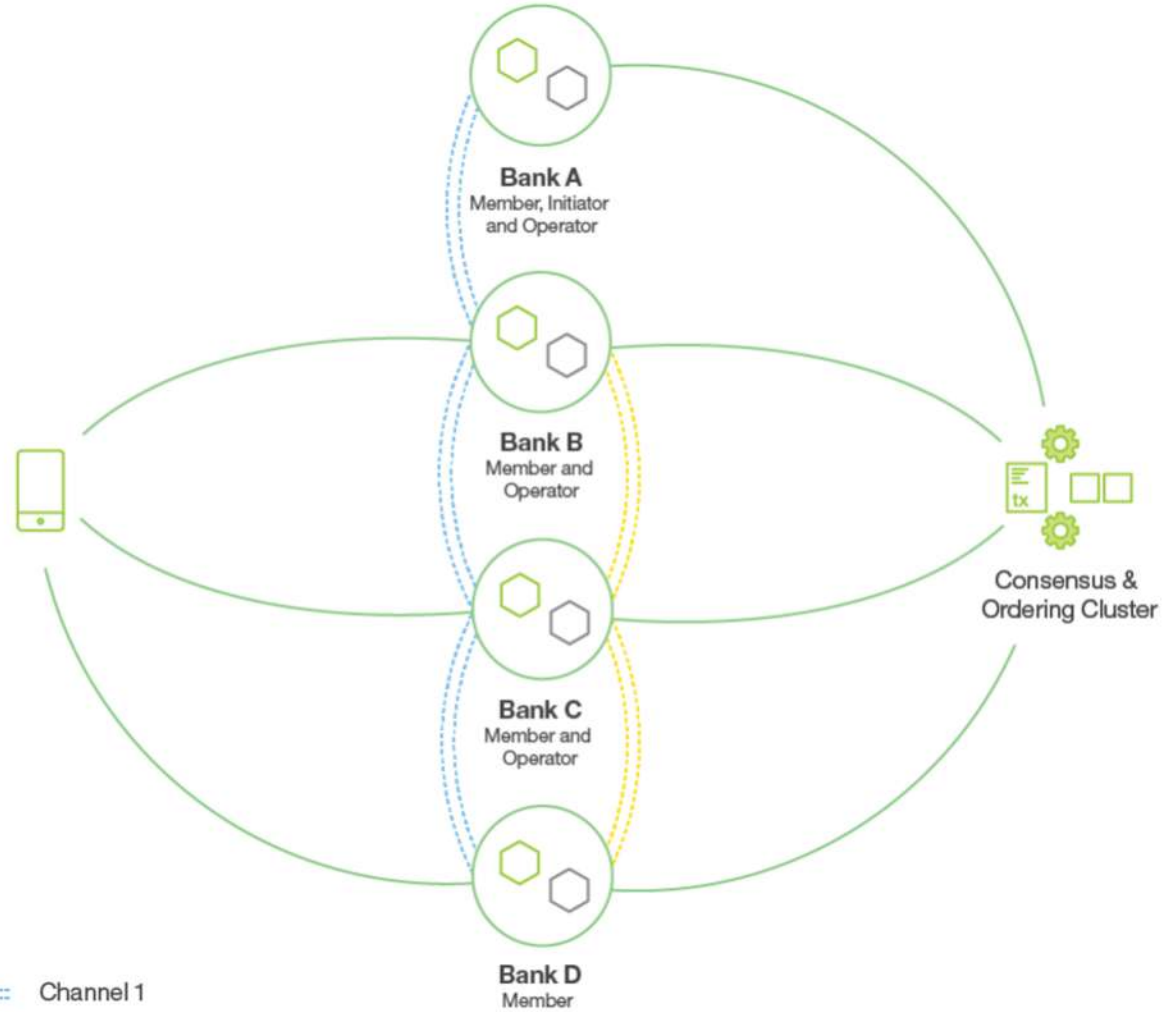
¿Las reglas de las transacciones no cambian con frecuencia?

¿Son las transacciones publicas?



CREANDO SOLUCIÓN BLOCKCHAIN

REDES DE NEGOCIOS



- Conocimiento básico de bitcoin y Blockchain.
- Conocimiento básico de Golang, Java o Javascript.
- Entendimiento básico de PKI (Infraestructura de clave pública).
- Docker.
- Ubuntu 18.x o 20 o Unix.
- Conocimientos de la consola de comandos de Linux.

El futuro digital es de todos

MinTIC

CREAR

Prototipo POC

MVP

Producto

etraining
Diseñamos nuevas formas de aprender

tecnalia Colombia
Inspiring Business

Investigación	Diseño Prototipo	Prueba de concepto	Producto mínimo viable	Integración de producto y soporte
Realizar una investigación de casos de uso, estudio de viabilidad y empieza a elegir una plataforma Blockchain.	Evaluar ideas comerciales y evaluar la aplicabilidad en los procesos empresariales existentes.	Desarrollar e implementar una solución básica de Blockchain que permita validar la ideas funcionales y técnicas identificadas en la etapa anterior.	Desarrollar, probar e implementar un producto en el que se ajuste o refine la prueba de concepto y que permite implementar la solución a mayor escala.	Ajustar su aplicación de Blockchain totalmente funcional y comercializarla.

ethereum

bitcoin

corda

HYPERLEDGER

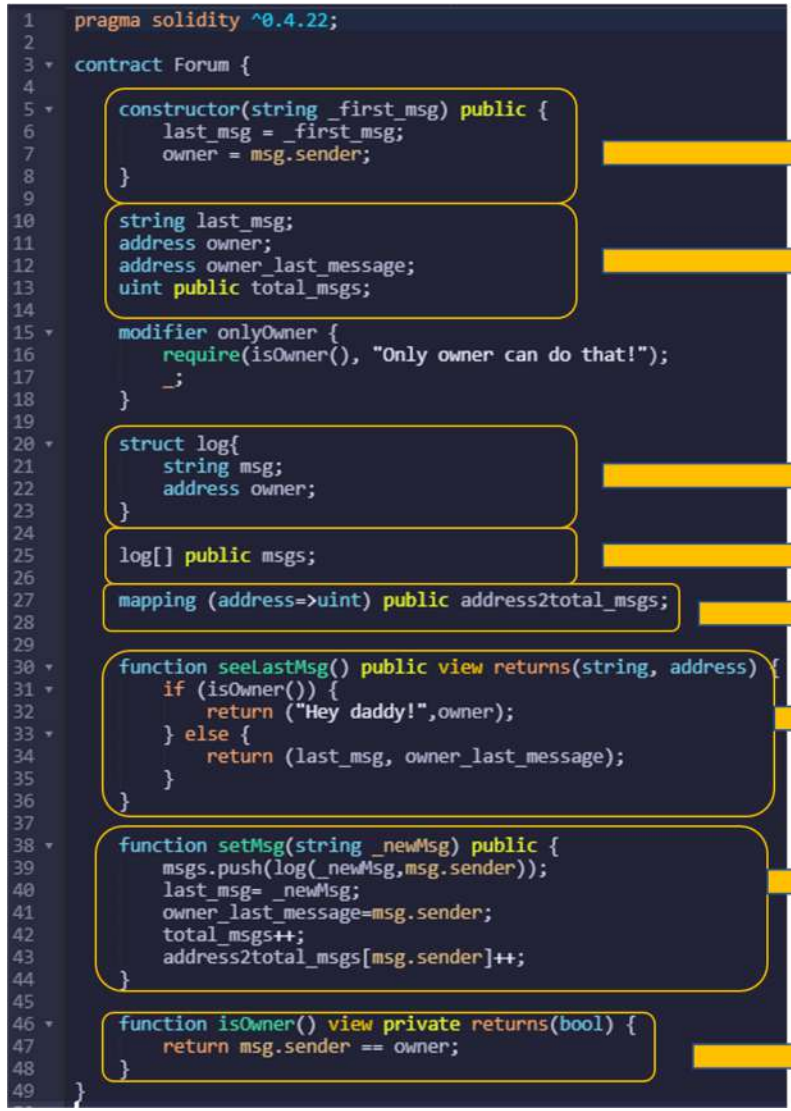
CONTRATOS INTELIGENTES

- Supongamos que se quiere crear un foro inmutable, es decir un lugar donde cualquier persona pueda escribir un mensaje y ese mensaje quede registrado junto con clave pública como el emisor del mismo. Tendremos una función para consultar el último mensaje y también estarán todos los mensajes públicos en un listado. A la función de último mensaje le programaremos una lógica especial para reconocer al dueño del contrato y darle un saludo especial (así se prueba que el contrato efectivamente reconoce la clave pública de quien interactúa con él y reconoce a su creador o administrador).

Componentes del Contrato: Forum	
Condiciones Iniciales	• Primer mensaje • Dueño del contrato
Variables	• Último mensaje • Dueño del último mensaje • Total de mensajes

Estructuras de Datos	• log
	  • mensaje
	  • dirección del dueño

Listas	Listado de logs - Público
Mapeos	Dirección hacia total de mensajes registrados
Consulta	Ver último mensaje
Registro	Registrar Nuevo Mensaje



```
pragma solidity ^0.4.22;

contract Forum {

    constructor(string _first_msg) public {
        last_msg = _first_msg;
        owner = msg.sender;
    }

    string last_msg;
    address owner;
    address owner_last_message;
    uint public total_msgs;

    modifier onlyOwner {
        require(isOwner(), "Only owner can do that!");
        _;
    }

    struct log{
        string msg;
        address owner;
    }

    log[] public msgs;

    mapping (address=>uint) public address2total_msgs;

    function seeLastMsg() public view returns(string, address) {
        if (isOwner()) {
            return ("Hey daddy!",owner);
        } else {
            return (last_msg, owner_last_message);
        }
    }

    function setMsg(string _newMsg) public {
        msgs.push(log(_newMsg,msg.sender));
        last_msg= _newMsg;
        owner_last_message=msg.sender;
        total_msgs++;
        address2total_msgs[msg.sender]++;
    }

    function isOwner() view private returns(bool) {
        return msg.sender == owner;
    }
}
```

Diagrama realizado por:
Rafael SantaMaría 317 366 1439
Rafasantama@gmail.com

Condiciones Iniciales

Variables

Estructura de Datos

Listas

Mapeos

Función Pública de Consulta

Función Pública de Registro

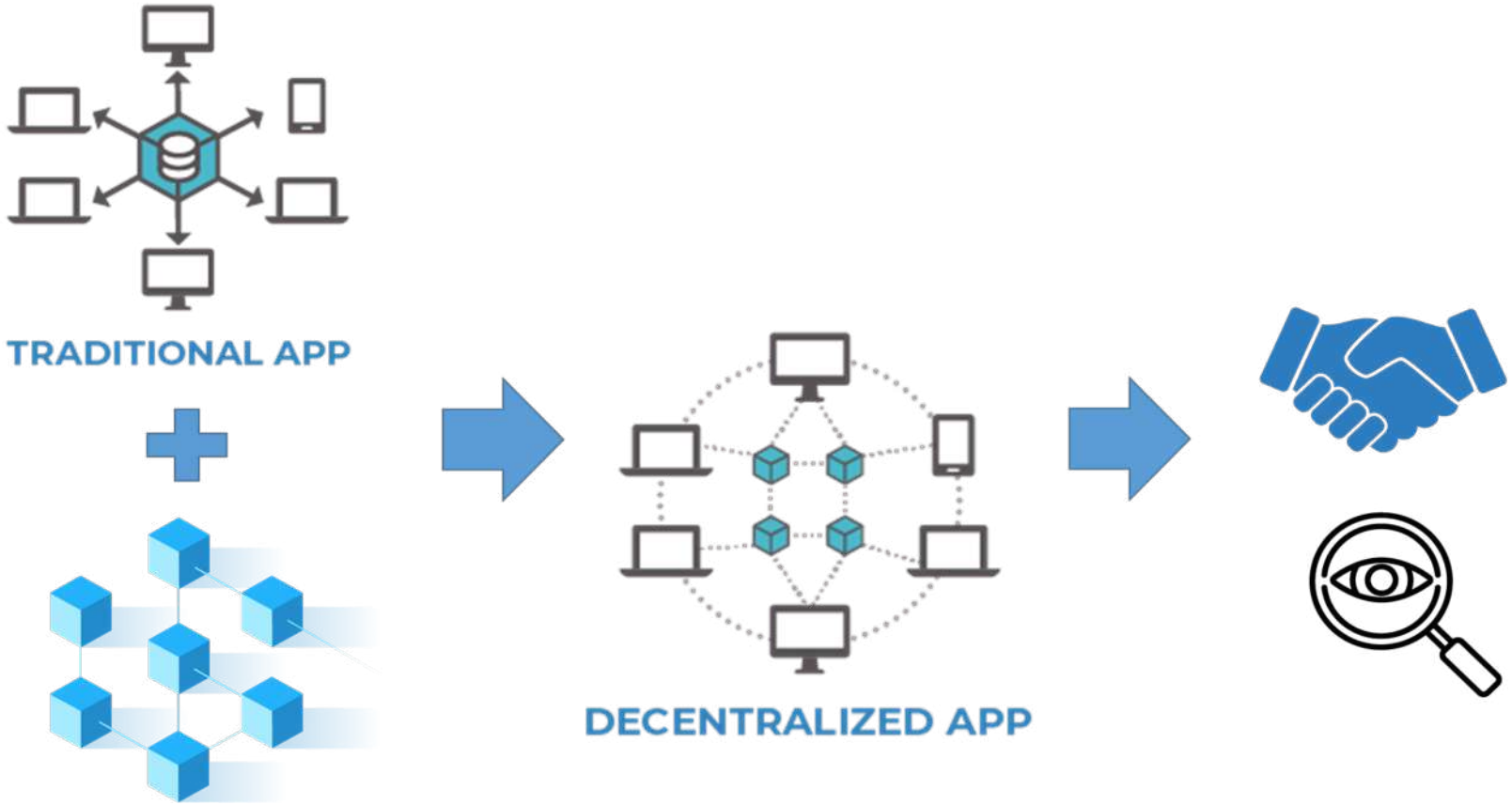
Función Interna Privada

El futuro digital es de todos

MinTIC

etraining
Diseñamos nuevas formas de aprender

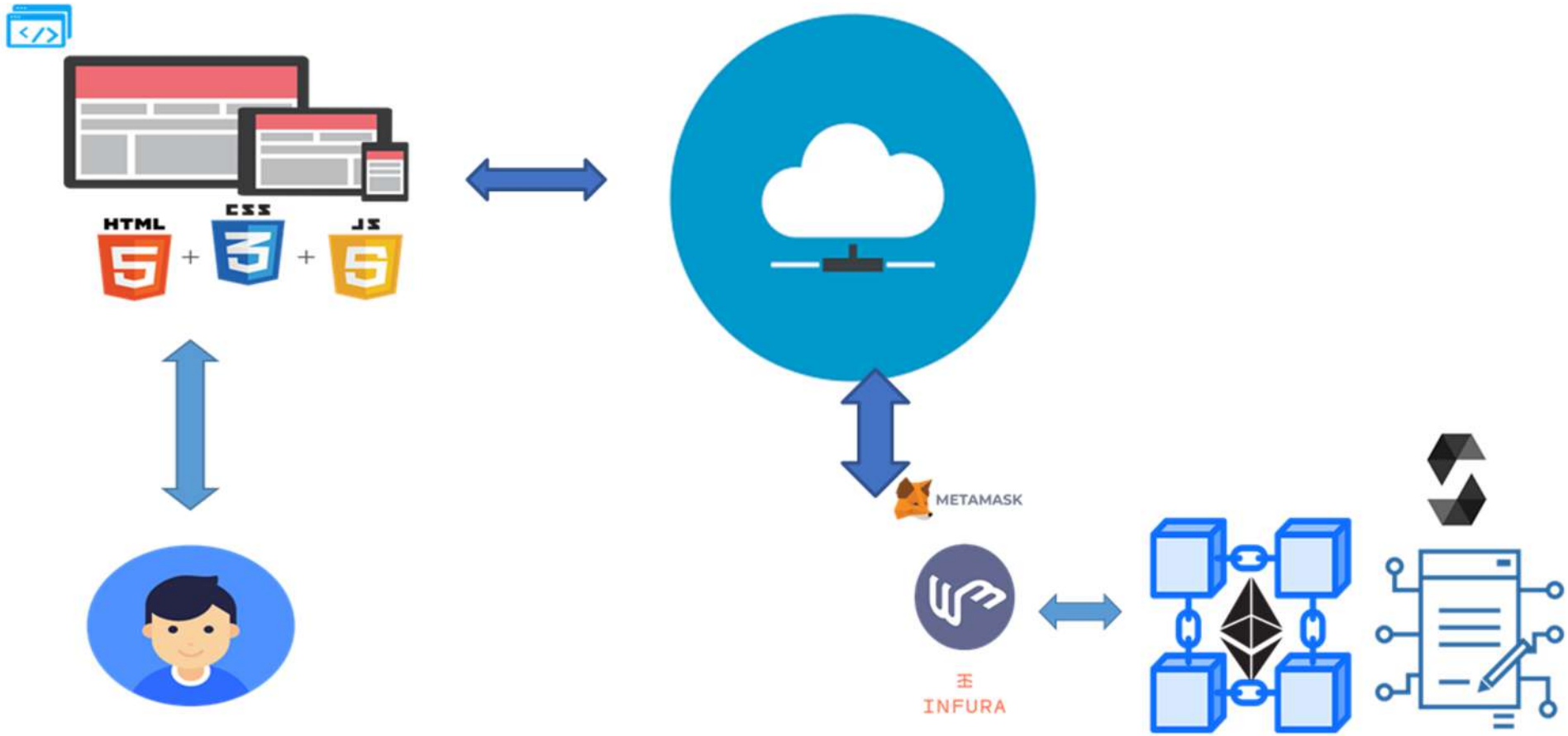
tecnalia Colombia
Inspiring Business


TRADITIONAL APP
DECENTRALIZED APP

El futuro digital es de todos

MinTIC

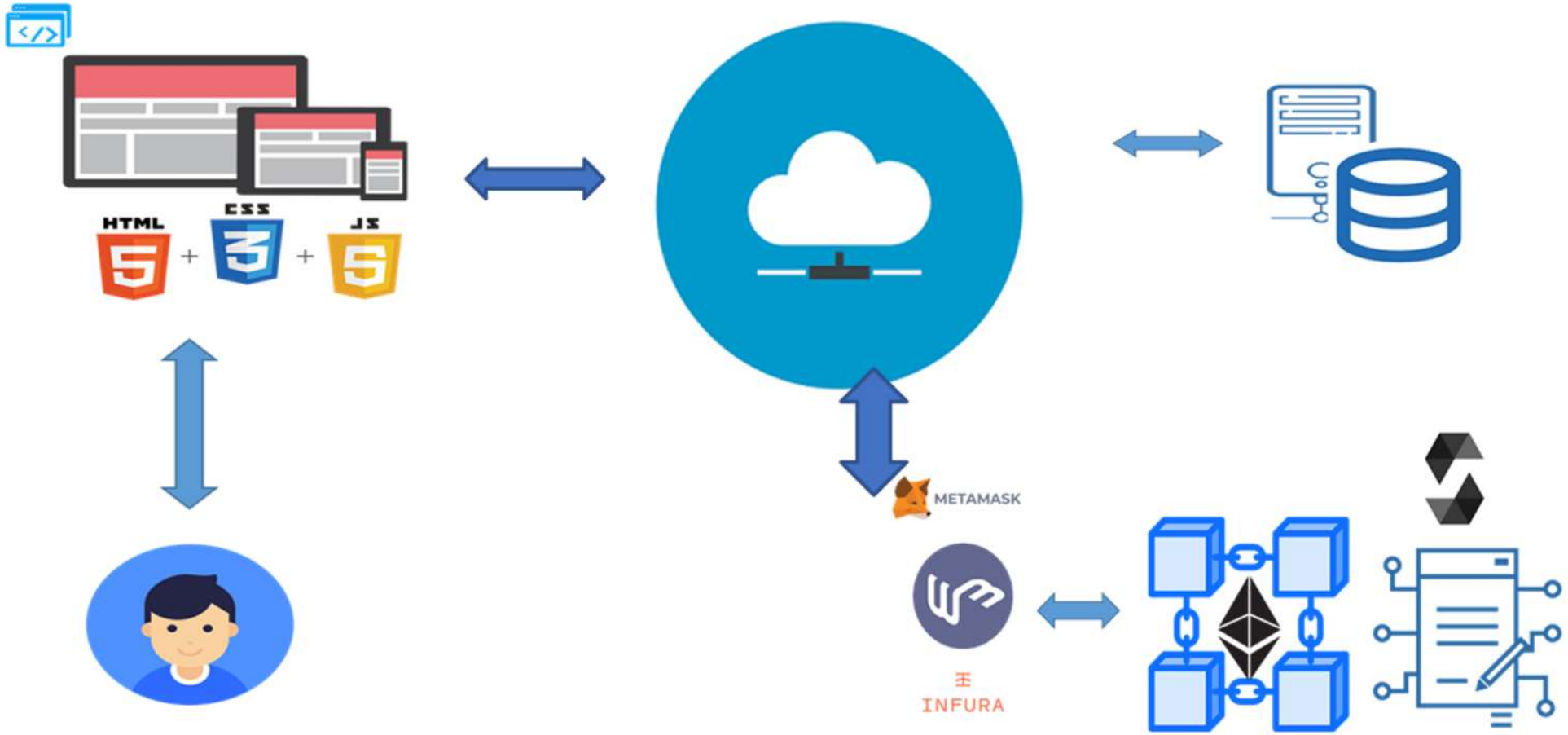
D-APP SOLO BLOCKCHAIN



El futuro digital es de todos

MinTIC

D-APP BLOCKCHAIN + DB



etraining
Diseñamos nuevas formas de aprender

tecnalia Colombia
Inspiring Business

El futuro digital es de todos

MinTIC

Gracias

etraining
Diseñamos nuevas formas de aprender

tecnalia Colombia
Inspiring Business