WE CAN
DO SO
MUCH
TOGETHER

Blockchain y Ciberseguridad

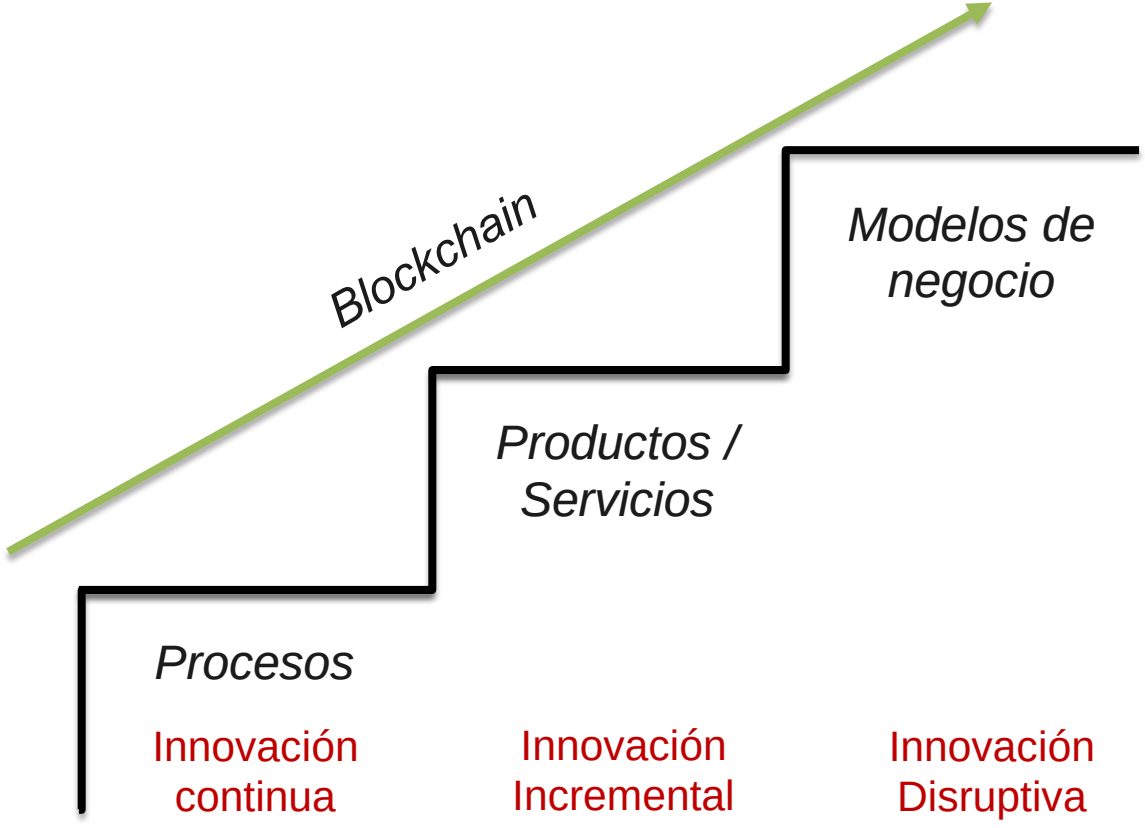
Oscar Lage Serrano
oscar.lage@tecnalia.com
@Oscar_Lage

tecnalia Inspiring Business


Nuestra Visión
by tecnalia

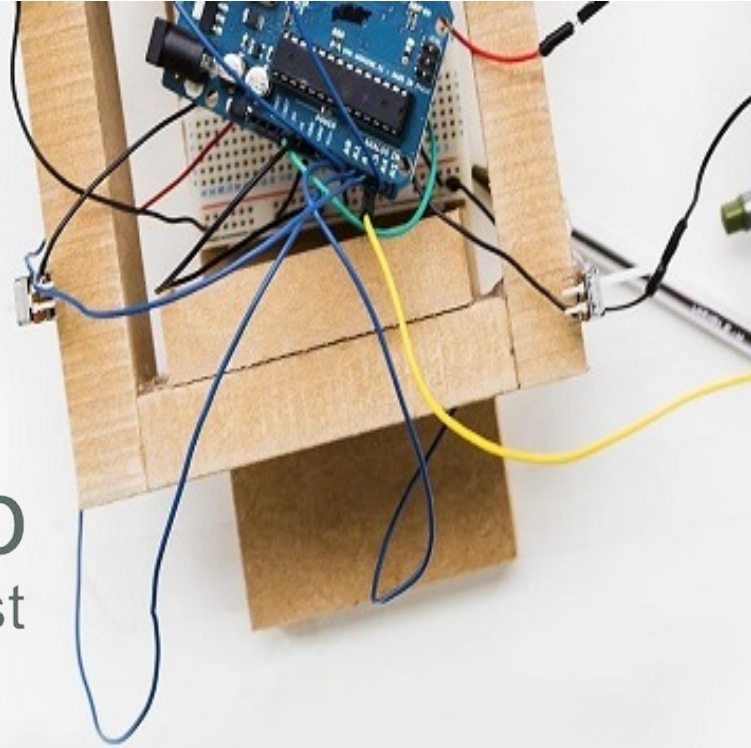
Blockchain es la tecnología más disruptiva de la actualidad, puede cambiar los procedimientos y negocios tal y como los conocemos a día de hoy.

Horizontes de la innovación



La mayor barrera de Blockchain es la propia imaginación del ser humano y la resistencia al cambio de sistemas ya establecidos.

1er Laboratorio blockchain industrial de europa



BLOCKCHAIN Lab
Inspiring Business. Enabling Trust

HYPERLEDGER

ENTERPRISE ETHEREUM ALLIANCE

ALASTRIA

Industria 4.0

Energía

Transporte

Salud

Administración

Aseguradoras

¿Qué problemas estamos resolviendo?

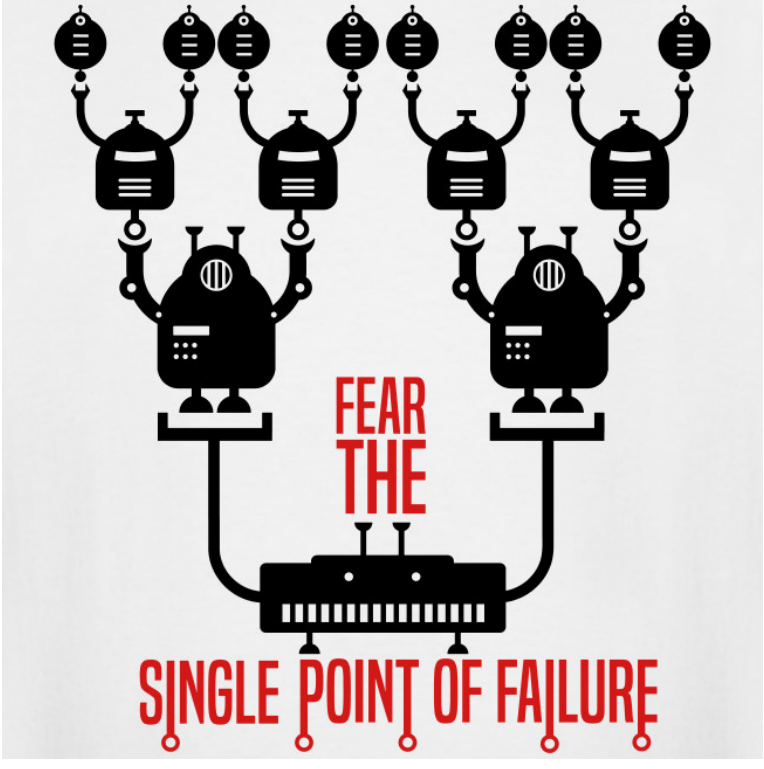
Problemas “tipo” que resuelve blockchain

- Desintermediación de procesos y modelos de negocio
- Trazabilidad y transparencia de procesos
- Visión única del dato sincronizada, consensuada e inalterable
- Confiabilidad, finalización y no repudio de las transacciones

Usos de blockchain en el ámbito de la ciberseguridad

Servicios Alta disponibilidad

- Identidad y metadatos usuarios
- PKI
- DNS
- Arquitecturas sistemas/servicios



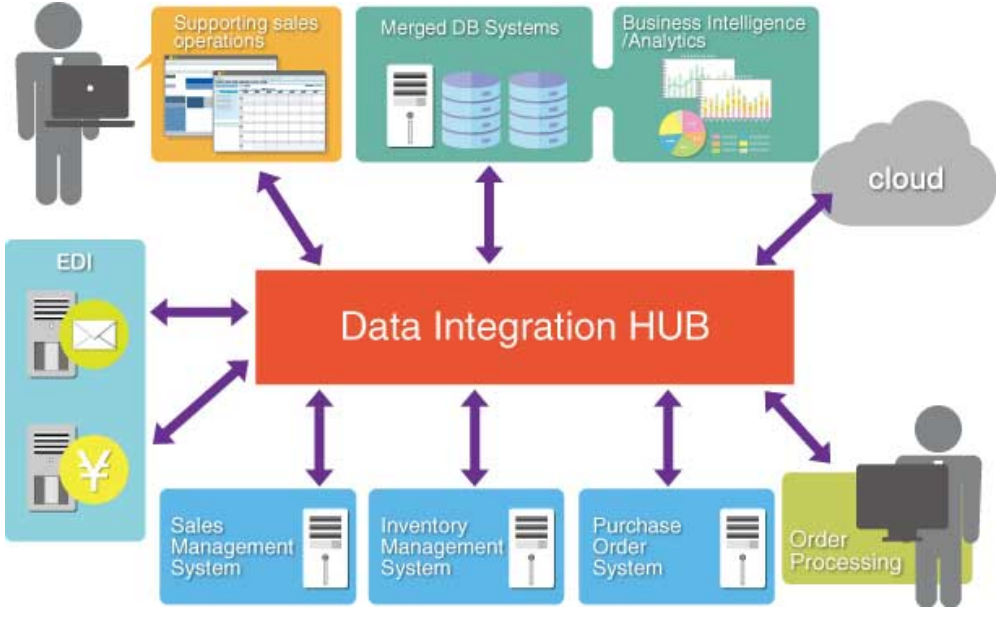
Middleware

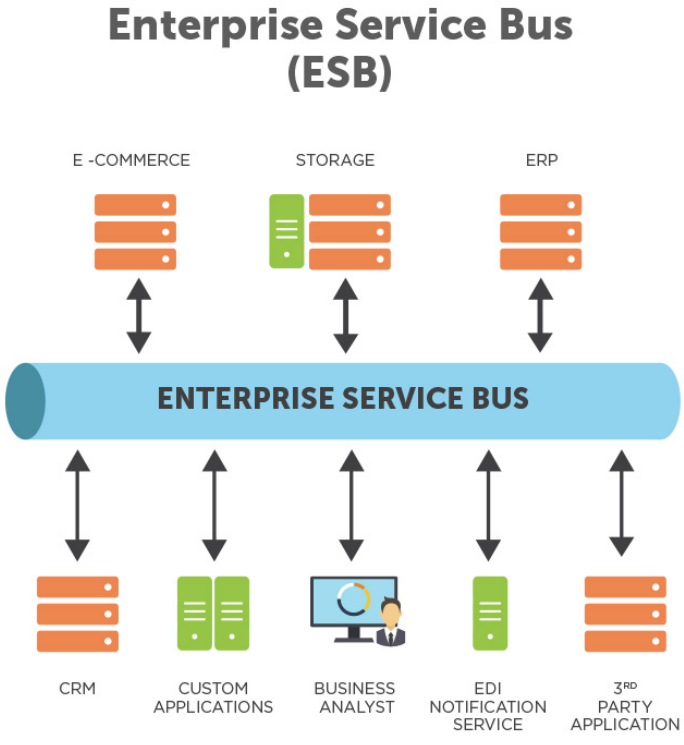
- Identidad
- Integridad comunicaciones
- No repudio

Registro inalterable

de alarmas y eventos críticos de la Base para la analítica forense

Integridad y sincronización perfecta de sistemas





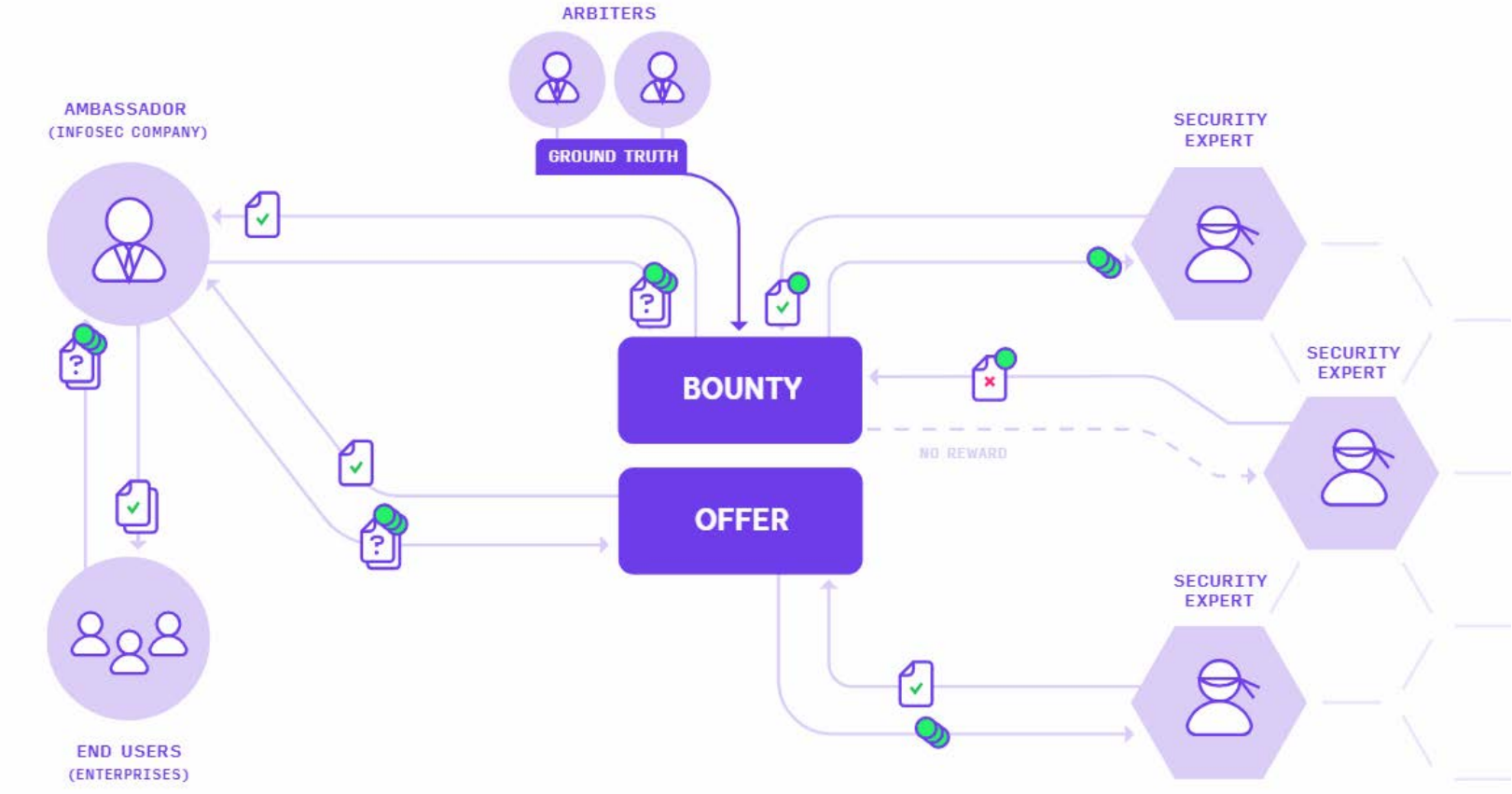
Distributed

Content Delivery Network (CDN)

Threat Intelligence

POLYSWARM

Threats come from every angle,
your protection should too.




Blockchain = Ciberseguridad

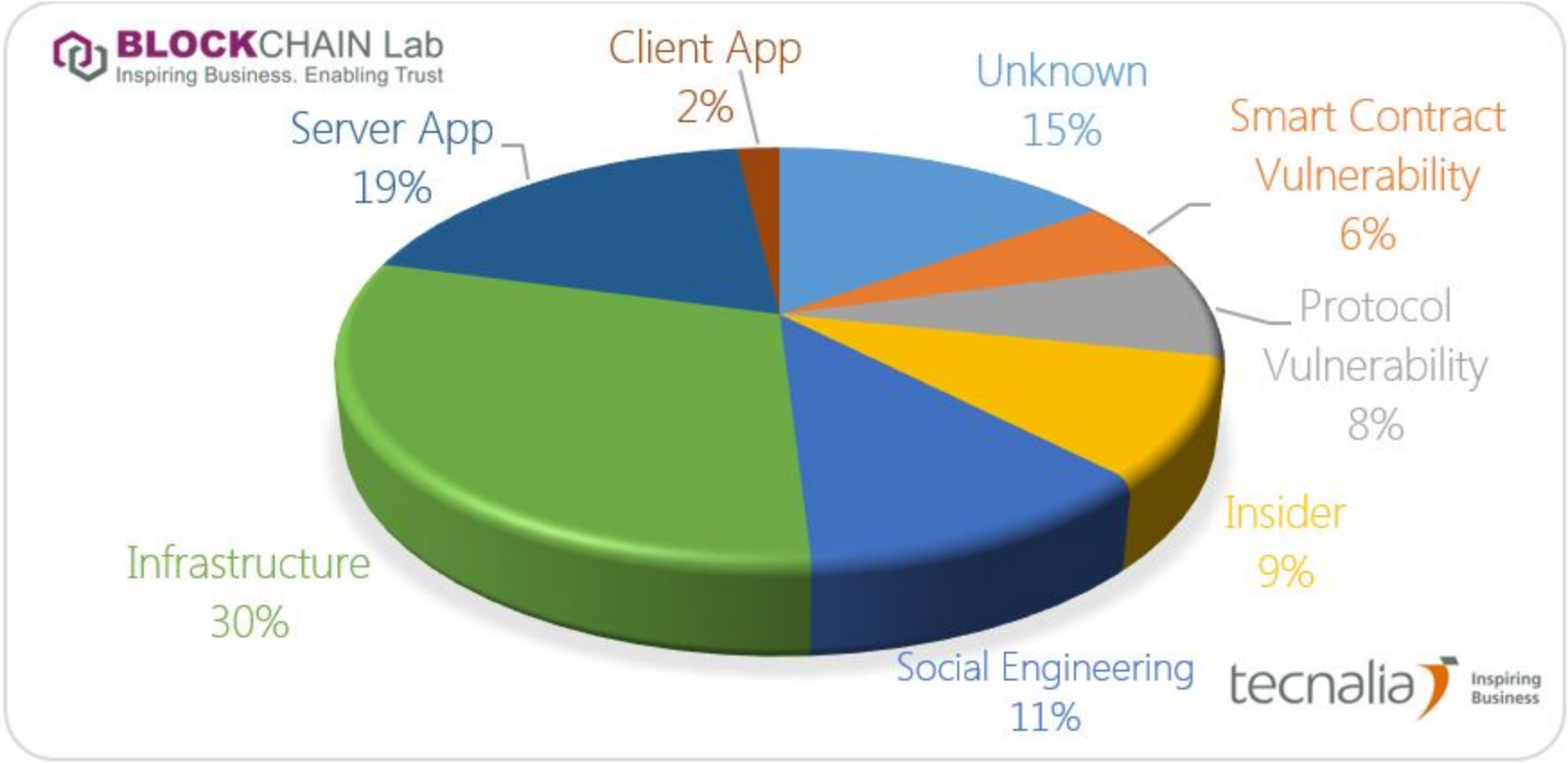
Arquitectura de ciberseguridad basada en algoritmos y tecnologías que en conjunto ofrecen por diseño:

- No-repudio de las transacciones
- Integridad de la información
- Tamper Resistant Software
- Alta Disponibilidad
- Arquitectura descentralizada (NO SPOF)
- Autenticación robusta

Cuidado! Blockchain no ofrece confidencialidad por diseño

Análisis de incidentes

Clasificación por vector

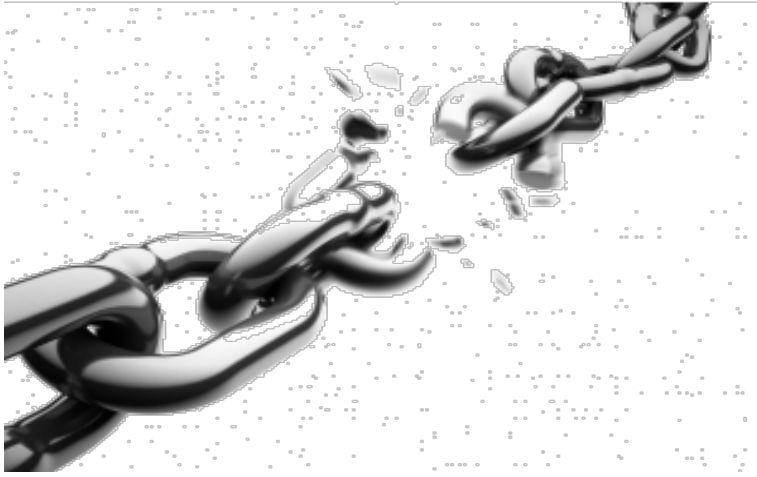


Retos de Ciberseguridad

Retos Tradicionales

Retos tradicionales de cualquier SW:

Injection, Broken **Authentication** and Session Management, Cross-Site Scriptiong (XSS), Broken **Access Control,** Security Misconfiguration, Sensitive Data Exposure, Insufficient Attack Protection, Cross-Site Request Forgery (CSRF), Using **Components with Known Vulnerabilities, Unprotected APIs, etc.**



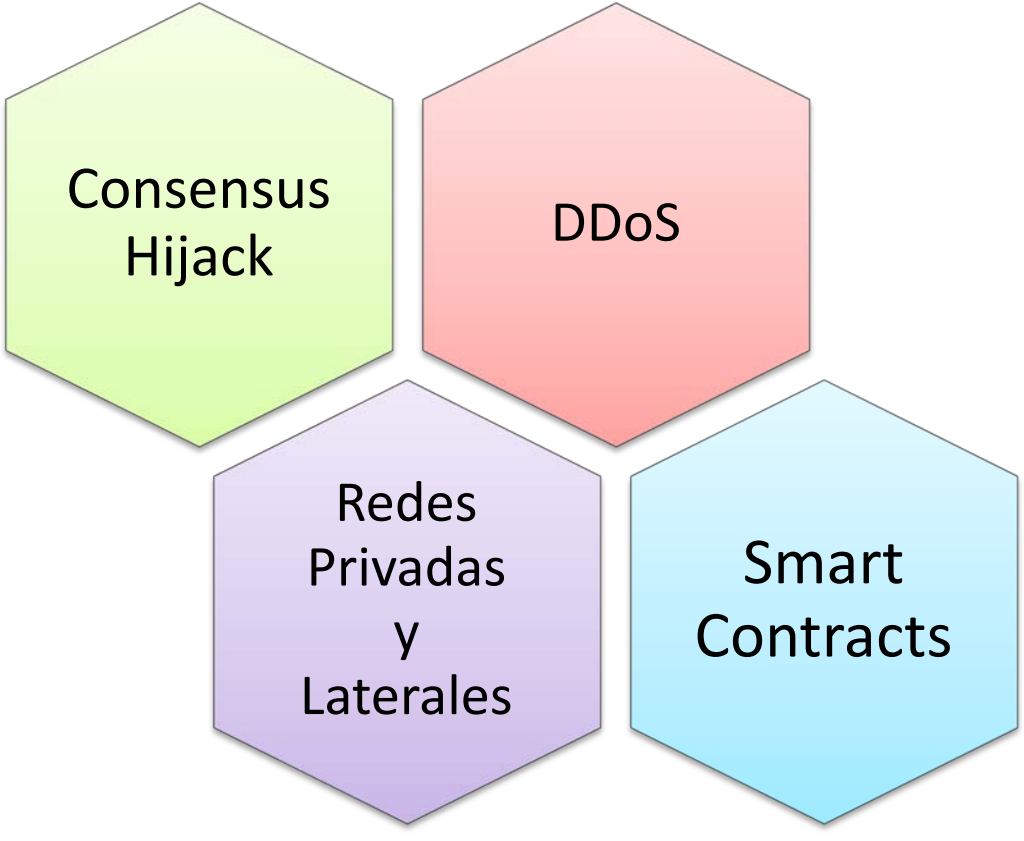
Retos tradicionales

Retos tradicionales asociados a la criptografía que aplican a la Blockchain:

- Gestión de claves
  - Custodia
  - Gestión pérdida y robo
- Generación de claves

Retos Específicos de Blockchain

Retos Específicos de Blockchain



Buenas Prácticas

Gestión de claves

- Almacenamiento seguro de claves (Elementos seguros, HW, cifrado, etc.)
- Contemplar el uso de agentes/técnicas de recuperación de contraseñas
- Implementación de sistemas multifirma para operaciones sensibles
- Generación segura de claves y tamaño/cripto adecuada usando estándares y buenas prácticas tradicionales (IETF/RFC 4107 cryptographic key management guidelines)

Privacidad

- Cifrado de las transacciones para que sólo terceros autorizados puedan acceder a la información
- Uso de algoritmos de cifrado basado en atributos (Attribute-Based Encryption)
- Técnicas de sharding (limitando los nodos que verifican ciertas transacciones)
- Técnicas de pruning para eliminar el cuerpo de los mensajes en los bloques

Código

- Implantar procedimientos de auditoría de código para las aplicaciones Blockchain y librerías asociadas o utilizar servicios de terceros y prácticas de desarrollo seguro de software
- Analizar meticulosamente la custodia de claves de wallets y librerías cliente
- Estandarización de funciones habituales en librerías

Red

- Monitorización de incrementos de capacidad de cómputo de nodos y su posible aumento de resolución de bloques.
- Restringir qué nodos pueden propagar nuevas transacciones para su validación
- Creación de una buena y transparente política (criterios) para la aceptación de nuevos miembros, así como la revocación de los mismos (REDES PRIVADAS)


"Estar preparado es la mitad de la victoria"
Miguel de Cervantes

Muchas gracias por su atención

Oscar Lage Serrano
oscar.lage@tecnalia.com
@Oscar_Lage