Organiza

GETAFE AYUNTAMIENTO | Empresa Municipal GETAFE INICIATIVAS | GISA GETAFE | getafe innova

Colaborador Estratégico

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Cofinanciado

Comunidad de Madrid

Actividad del Proyecto "Getafe Innova" de Referencia/Acrónimo: CI2020-GISA-1.3, concedido en la Convocatoria 2020 de ayudas para potenciar la innovación tecnológica e impulsar la transferencia de tecnología al sector productivo comprendido en las prioridades de la Estrategia Regional de Investigación e Innovación para una especialización inteligente (RIS3) de la Comunidad de Madrid a través de entidades de enlace de la innovación tecnológica, financiado en un 50% por la Comunidad de Madrid.

Organiza

Colaborador Estratégico

"Blockchain: fundamentos y aplicaciones"

Víctor Sánchez Hórreo
Manager Blockchain y Tecnologías Emergentes

Minsait (An Indra Company)

01. Presentación.
02. Blockchain: cómo funciona y cuáles son sus principales aplicaciones.
03. Evidencias digitales en blockchain.
04. Principales tecnologías blockchain.
05. Ejemplos de proyectos y casos de uso.
06. Blockchain e Industria 4.0.
07. Conclusiones.

01. Presentación

Organiza

Colaborador Estratégico

getafe industria 4.0

indra

> 50.000
profesionales

>3.300 MM
ingresos

> 140
países

minsait

An Indra company

>20.000
profesionales

>1,800 MM
ingresos en soluciones innovadoras

Paradigma

the Overview effect

SIA

afterbanks

Plaiground

Estrategia digital y agilidad

Sostenibilidad

Open Banking

Ciberseguridad

Inteligencia artificial

Organiza

GETAFE AYUNTAMIENTO | Empresa Municipal GETAFE INICIATIVAS | GISA GETAFE | getafe innova

Colaborador Estratégico

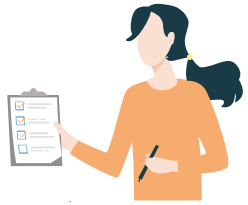
QAEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

getafe industria 4.0

Capacidades

- Sesiones formativas blockchain a medida.
- Análisis e ideación de casos de uso blockchain.
- Consultoría estratégica y tecnológica en el ámbito de blockchain.
- Análisis y selección de estándares de tokenización.

- Diseño de arquitectura de sistemas blockchain.
- Despliegue y configuración de nodos y redes blockchain.
- Despliegue y configuración de soluciones BaaS y soluciones blockchain para trazabilidad



- Instalación y configuración de sistemas de monitorización.
- Implementación de APIs para integrar aplicaciones y sistemas con blockchain.
- Diseño e implementación de contratos inteligentes.

- Análisis de rendimiento y ajuste fino de redes blockchain privadas.
- Creación de NFTs
- Desarrollo de aplicaciones.
- Servicios de soporte blockchain.

Conocimiento tecnológico

Ethereum

Quorum · HYPERLEDGER BESU · open ethereum · polygon

Fabric

HYPERLEDGER FABRIC · IBM BLOCKCHAIN · ORACLE Blockchain

CORDA

Sistemas de ficheros distribuidos

IPFS

Trazabilidad con blockchain

IBM Food Trust™

Monitorización

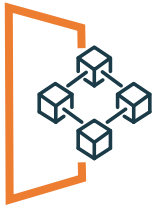
Prometheus · Grafana · HYPERLEDGER EXPLORER

02. Blockchain: cómo funciona y cuáles son sus principales aplicaciones

En un nuevo enfoque de confianza distribuida, a diferencia de los sistemas tradicionales, no hay una autoridad central, sino que la confianza se distribuye entre los participantes.

Blockchain tiene tres ingredientes básicos

Ledger distribuido



Fuente única de la verdad

- Base de datos replicada entre todos los participantes.
- Todos poseen la misma información.

Consenso

Inmutabilidad

- Garantía de que ninguno de los participantes puede alterar la información del ledger de manera unilateral.

Smart contracts

Modelado de operaciones

- Contratos en lenguaje de programación.
- Se ejecutan de manera autónoma y automática.
- Permiten modelar y automatizar operaciones.

Públicas (main chains y side chains)

ethereum

- Global y permanente.
- Funciona como un registro común, facilitando la construcción de servicios de valor añadido.
- Potencia la transparencia y la confianza.
- Facilita la interoperabilidad.

Privadas

MultiChain

HYPERLEDGER FABRIC

CONSENSYS Quorum

HYPERLEDGER BESU

- Mayor rendimiento.
- Mayor confidencialidad.
- Orientado al intercambio de información y la colaboración en escenarios complejos.
- Mayor control sobre el rendimiento de la red

Semipúblicas permisionadas

ALASTRIA

- Cualquiera se puede unir cumpliendo unos requisitos.
- Se asignan permisos a los nodos y éstos están identificados.
- Entorno inclusivo pero controlado.
- P. ej. plataformas multisectoriales



2009

Se lanza Bitcoin

2013

Bitcoin alcanza los mil millones de capitalización

2015

Ethereum empieza a funcionar con soporte para smart contracts.

La Fundación Linux prsenta Hyperledger Fabric para crear redes privadas seguras de alto rendimiento.

2018

La Comisión Europea lanza el Blockchain Observatory and Forum.

Hacia una tercera generación de de redes blockchain (EOS, Cardano…)

2019

IBM comienza las soluciones BaaS con IBM Blockchain Platform.

Walmart lanza un sistema de trazabilidad alimentaria basado en blockchain

Blockchain e identidad digital soberana

2020

Fiebre de las DeFI..

Exchanges descentralizados(DEX)

Las stable coins ganan tracción.

Polkadot y otras iniciativas de interoperabilidad

ChainLink y oráculos distribuidos

2021

La inversión cripto de vuelve “mainstream”.

Evolución de soluciones capa 2 de Ethereum.

NFTs

Pilotos de CBDC

Registros (evidencias digitales)

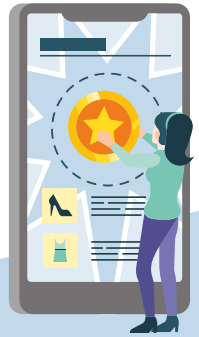
Prueba de existencia y garantía de integridad de elementos digitales.

- Propiedad intelectual.
- Licitaciones.
- Certificación y auditoria.

Trazabilidad

Cadenas complejas, con múltiples actores que tienen que colaborar y confiar entre sí a lo largo del proceso.

- Trazabilidad alimentaria.
- Comercio internacional.
- Cadena de suministro.

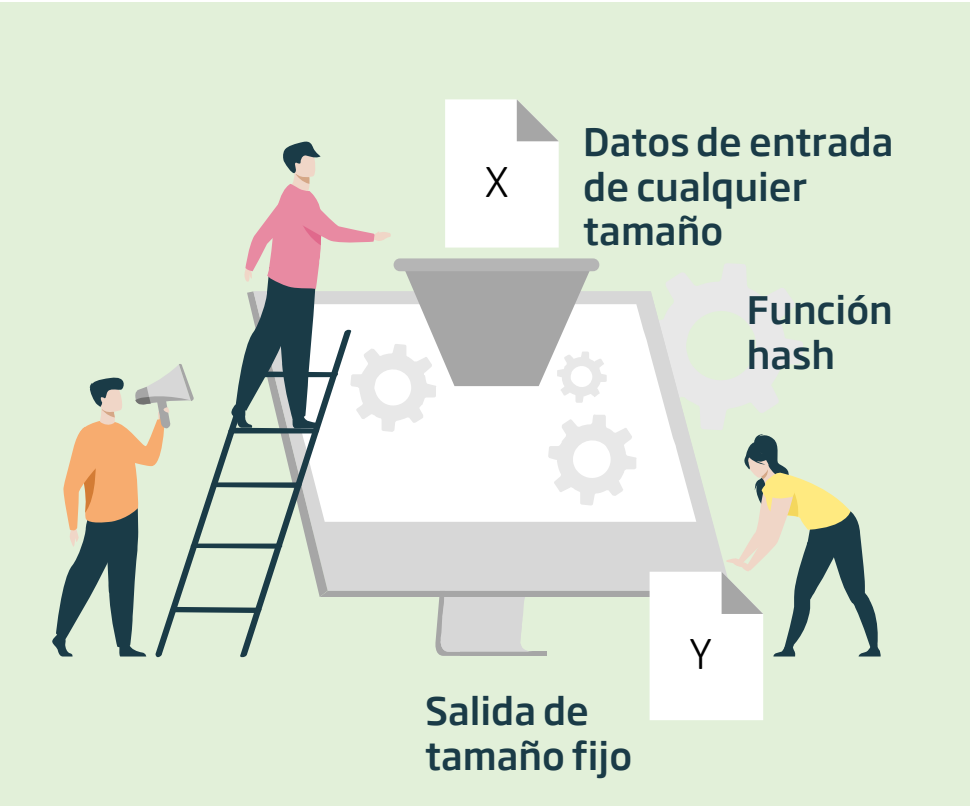


Tokenización

Uso de criptoactivos para representar activos físico, derechos de uso o cualquier otro concepto, permitiendo la definición de nuevos modelos de negocio en entornos distribuidos.

03. Evidencias digitales en blockchain

¿Qué es un hash?



Un “algoritmo de hashing”, o simplemente una “función hash” es una función de sentido único que produce una huella o “hash” a partir de una entrada de tamaño arbitrario.

Da igual la cantidad de datos que se utilice (muchos o pocos), el código resultante tendrá siempre el mismo número de caracteres.

Las funciones de hash criptográfico se usan de forma extensiva en blockchain.

- Hay tres aspectos relevantes que fundamentan el uso del registro de hashes en blockchain para prueba de existencia
  - Un fichero siempre genera el mismo hash.
  - Dos ficheros diferentes no pueden generar el mismo hash.
  - No es posible inferir a partir del hash el contenido del fichero desde el cual se generó.

StampIt: prueba de existencia blockchain

REGISTRO DE UN DOCUMENTO

DOCUMENTO A REGISTRAR

CÁLCULO DEL HASH EN CLIENTE

* IDENTIFICADOR ÚNICO DE DOCUMENTO

GUARDADO EN SMART CONTRACT

ALMACENADO EN LA BLOCKCHAIN

**Este proceso es imposible de realizar en sentido inverso*

VERIFICACIÓN DE UN DOCUMENTO

DOCUMENTO PRESENTADO

CÁLCULO DEL HASH

BLOCKCHAIN

EXTRAER EL HASH

COMPARACIÓN Y VERIFICACIÓN DEL HASH

StampIt: servicio de registro en blockchain

StampIt utiliza blockchain para **prueba de existencia** mediante registro de un hash único obtenido a partir de un documento usando una función criptográfica de resumen. **El registro se realiza en un sistema descentralizado y es inalterable**.

Solamente el hash (y no el documento en sí) es enviado a la blockchain y el registro se podrá verificar en cualquier momento.

Se garantiza la existencia de un documento en un momento dado del tiempo, así como la integridad del mismo.

StampIt: usos potenciales

- Licitaciones
- Propiedad Intelectual e Industrial
- Evidencia electrónica auditoría
- Certificación medidas IoT
- Gestión documental

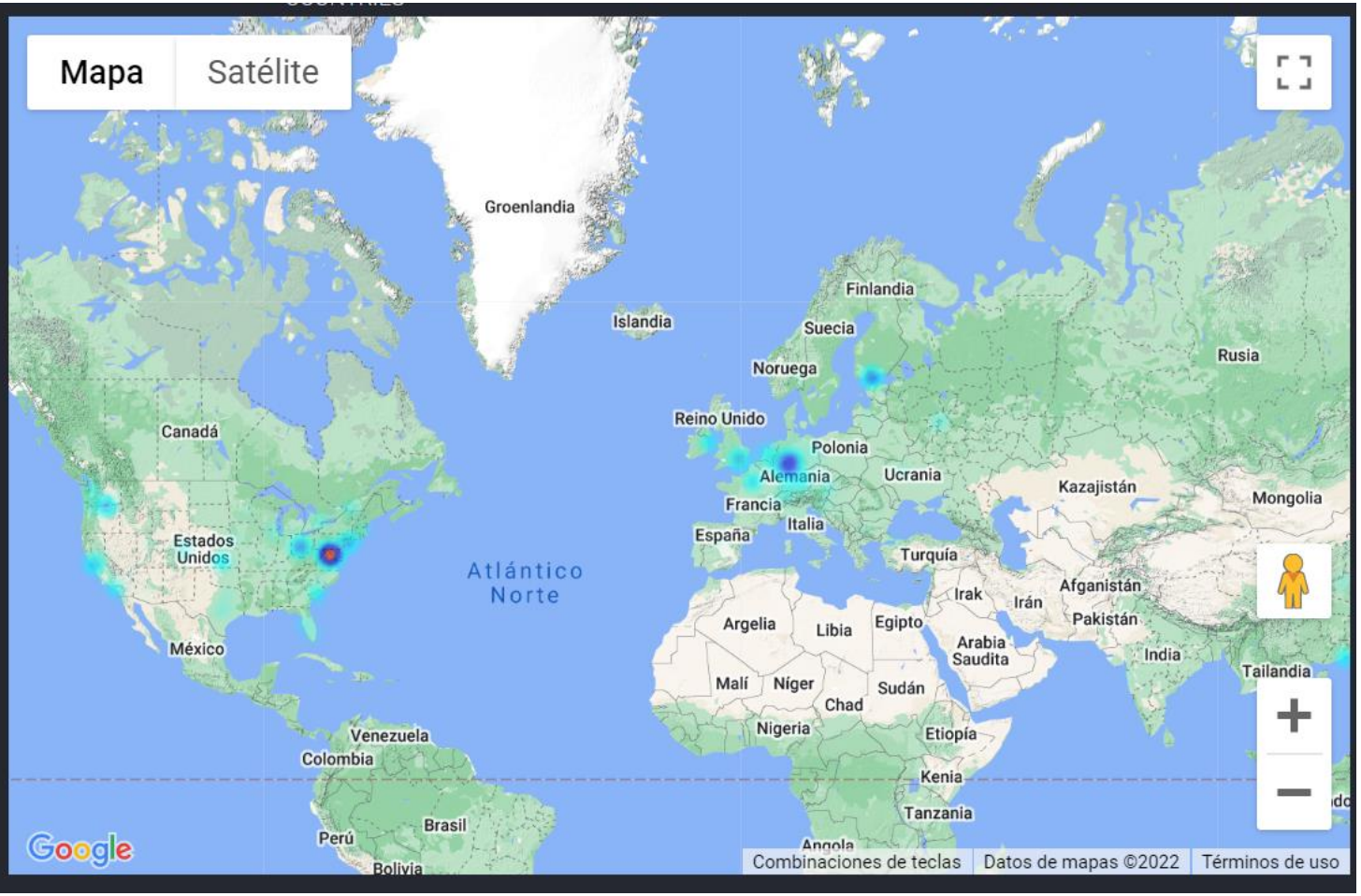
04. Principales tecnologías blockchain

Ethereum

- Plataforma blockchain para el desarrollo de aplicaciones descentralizadas basadas en **smart contracts**.
- Desarrollado por la Ethereum Foundation, organización sin ánimo de lucro basada en Suiza.
- Posee una moneda nativa, el **Ether**, que actualmente es la segunda criptomoneda por capitalización en el mundo (300.000M $)
- Utliliza el lenguaje **Solidity** (Turing completo) para la implementación de los smart contracts.
- Blockchain **pública** y posibilidad de crear redes blockchain **privadas**.
- Permite crear **criptoactivos** propios.
- Plataforma base para las **DAOs** (Decentralized Autonomous Organizations)

Ethereum Mainnet

Total	6151 (100%)
United States	2770 (45.03%)
Germany	934 (15.18%)
Singapore	274 (4.45%)
Finland	258 (4.19%)
United Kingdom	222 (3.61%)
France	157 (2.55%)
Japan	149 (2.42%)
Canada	140 (2.28%)
China	127 (2.06%)



Hyperledger Fabric

- Es el proyecto más conocido de la iniciativa Hyperledger, que tiene como objetivo la creación de **sistemas distribuidos empresariales**.
- Fabric es un **framework** para crear aplicaciones distribuidas orientadas a los procesos empresariales sobre **redes privadas/premisionadas**.
- Pone el foco en **el rendimiento y la privacidad** y ofrece una alta tasa de transferencia, resiliencia y confidencialidad para la construcción de soluciones blockchain.
- Implementa una **arquitectura modular** que permite a los arquitectos de soluciones escoger entre múltiples tecnologías, como sistemas de identidad, cifrado y consenso.
- Tiene capacidades para definir **distintos niveles de visibilidad** de la información entre los participantes y establecer canales/subredes.

Alastria

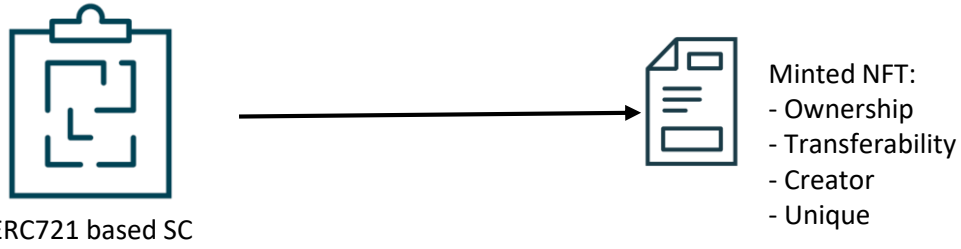
- Alastria es una **asociación** sin ánimo de lucro que fomenta la economía digital a través del desarrollo de tecnologías descentralizadas/Blockchain.
- Enfoque neutro: su misión es aportar infraestructura, y no servicios de valor añadido, por lo que tiene la finalidad de construir una **plataforma** sin caso de uso ni modelo de negocio determinados.
- Uno de los mayores esfuerzos de Alastria está enfocado en la **estandarización** y el dar una **validez legal** a blockchain a nivel estatal, europeo e internacional.
- + de 500 organizaciones. Indra/Minsait es socio fundador.
- En la actualidad se ofrecen dos redes de tipo Ethereum, una basada en Quorum y otra basada en Besu, que van a tender a converger en una sola, así como una red con tecnología Hyperledger Fabric.

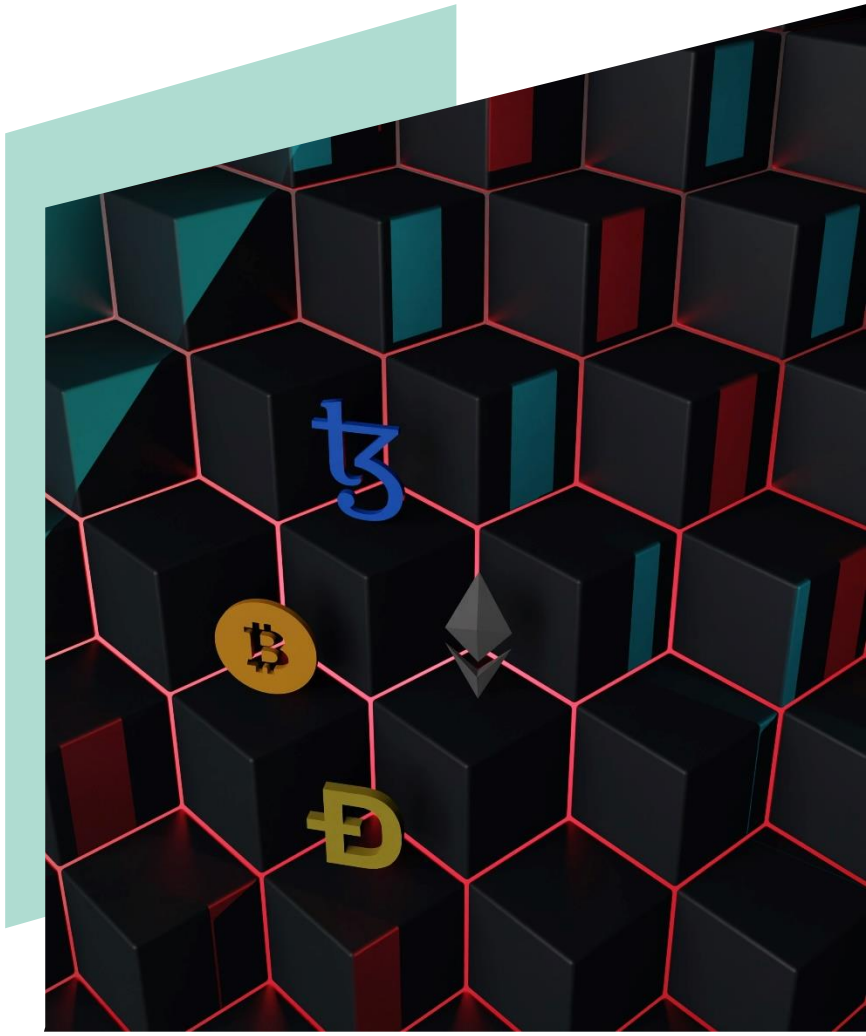
NFTs

Es el acrónimo de Non-fungible Token. Ningún token creado será exactamente igual a otro, ya que cada uno tiene sus propias características que lo definen. Solo pueden tener un propietario oficial a la vez y funcionan como prueba verificable de autenticidad y propiedad dentro de una red blockchain.

Los tokens no fungibles se utilizan para representar la propiedad de artículos únicos. Mediante NFT se puede tokenizar cualquier elemento del mundo real o virtual.

Los NFT se basan en Ethereum ERC-721 Token Standard. Es responsable de:
- Generación de nuevos tokens
- Asignar propiedad a esos nuevos tokens
- Gestionar la transferibilidad del NFT





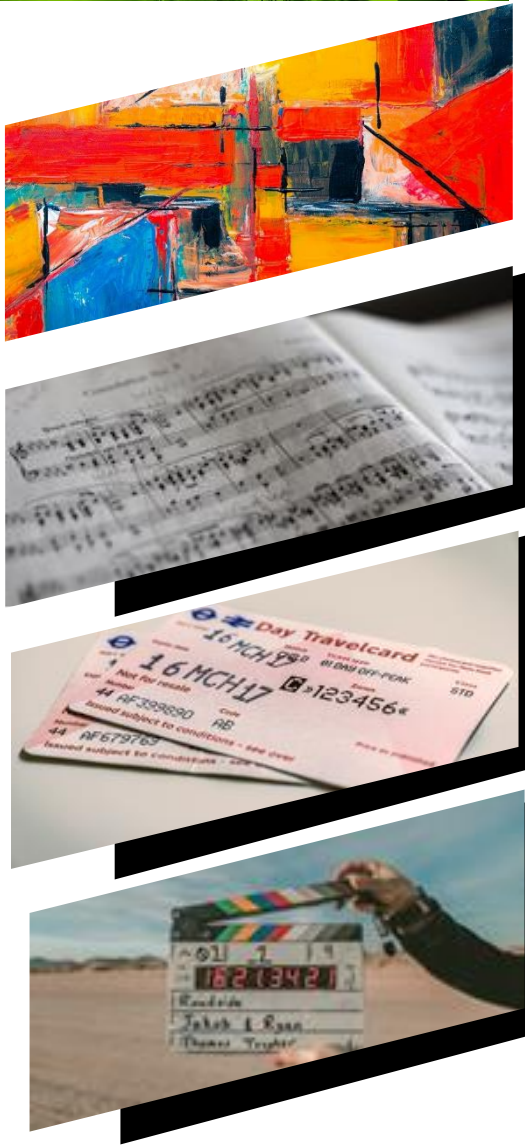
NFTs

- Cualquier artículo puede ser tokenizado. Podemos tokenizar objetos del mundo real como el arte o una participación en una propiedad, entradas, documentos legales…

- También los objetos del mundo digital se pueden tokenizar como música, video o imagen.

- Puede ser parte esencial del metaverso: elementos para personalizar un jugador en un juego virtual, espacio dentro del mundo virtual, derechos de uso en la nube,...

Decentraland



05. Ejemplos de proyectos y casos de uso

Organiza

GETAFE AYUNTAMIENTO | Empresa Municipal GETAFE INICIATIVAS | GISA GETAFE | getafe innova

Colaborador Estratégico

QAEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

getafe industria 4.0

Sistema Blockchain para el registro de secretos empresariales

Clarke Modet +

Sistema pionero

Primera aplicación blockchain productiva en el sector .
Nuevo servicio para los clientes de Clarke Modet

Mejora del proceso

Registro ágil, sencillo, altamente seguro y con un coste reducido.

Gran reducción de costes

El reto

Crear un nuevo servicio operativo basado en tecnología blockchain.

Proporcionar una plataforma basada en Blockchain para que los clientes de Clarke Modet puedan registrar la posesión de sus secretos industriales en un determinado momento y demostrar que no han sido modificados posteriormente.

La solución

Sistema blockchain en producción que permite un registro continuo del secreto industrial, sencillo y barato, con niveles de seguridad equiparables a los actuales y con ventajas adicionales como que el secreto no es necesario que sea conocido por nadie para su registro.

Registro en red Alastria y certificado de registro en red pública Ethereum.

Servicio que aporta versatilidad, al poder generar evidencias sobre formatos que no se podían registrar hasta ahora.

Organiza

Colaborador Estratégico

getafe industria 4.0

Ecosistema Blockchain para la gestión de garantías de origen

Nuevo modelo de negocio

La utilización de blockchain facilita la creación de un ecosistema y un nuevo mercado para un activo en crecimiento.

Servicio diferencial en sostenibilidad

Se ayuda a los clientes a ser más sostenibles y poder demostrar a su vez su compromiso en la consecución de los objetivos de desarrollo sostenible (ODS).

El reto

- Conseguir que una gran empresa energética gane competitividad, genere nuevos modelos de negocio y se sitúe en una posición de liderazgo mediante la creación un ecosistema basado en blockchain en al ámbito de las garantías de origen de la energía renovable.
- Garantizar en tiempo real a los clientes libres (B2B) que la energía que consumen es 100% de origen renovable.

La solución

- Creamos una red blockchain empresarial en la que los actores del proceso involucrados en la producción, distribución, comercialización y consumo pueden registrar, transferir, interoperar, acceder, certificar y compartir la información necesaria, junto con un sistema web que permite a los consumidores finales conocer con exactitud de dónde proviene la energía de origen renovable que consumen.
- Las garantías de origen de la energía renovable son tokenizadas, de modo que son representadas por tokens no fungibles (NFT) y transferidas mediante tecnología blockchain.
- Registramos en blockchain la información de generación y de consumo garantizando que no puede ser alterada, ofreciendo trazabilidad completa y auditabilidad sobre el proceso.
- Hemos ejecutado con éxito una primera fase de proyecto productivo, operacional en el mercado de Chile, resolviendo los retos de escalado y seguridad, y continuamos ampliando la plataforma para escalarla a nivel mundial.

Organiza

GETAFE AYUNTAMIENTO | Empresa Municipal GETAFE INICIATIVAS | GISA GETAFE | getafe innova

Colaborador Estratégico

QAEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

getafe industria 4.0

CircularTrust: Ecosistema blockchain para impulsar la economía circular

ecoembes

Casos de uso reales

Red blockchain para la economía circular, proporcionando una fuente única de verdad, registro de información inalterable, mayor transparencia y auditabilidad. Abaratamiento de los costes de operación y reducción de las fricciones.

+ 150 plantas y recicladores registrando en blockchain

+ Miles de tokens en funcionamiento en la red

El reto

Crear confianza, mejorar la eficiencia de los procesos, crear incentivos y eliminar los puntos ciegos en el proceso de recogida, selección y reciclaje.
Aprovechando el papel de facilitador que juega Ecoembes dentro de la economía circular, impulsaremos un entorno de colaboración entre algunos actores de dicho ámbito donde el pilar fundamental es la transparencia, utilizando para ello una tecnología innovadora como es Blockchain.

La solución

- Hemos creado un ecosistema para gestionar el proceso de recogida, selección y reciclaje basado en Blockchain con el objetivo de reducir costes e impacto medioambiental aumentando la transparencia y el porcentaje de retorno de materiales reciclados.
- Hemos realizado el despliegue de una red blockchain con tecnología Hyperledger Fabric, sentando las bases para hacer que el sistema se pueda complementar con el proceso actual, y sea abierto a nuevos actores, su gestión sea descentralizada, y sea escalable a otros casos de uso en los cuales estamos trabajando.
- Hemos desarrollado un caso de uso completo de trazabilidad centrado en lo que se denomina Central de Retiradas, que es una parte del proceso de recogida, selección y reciclaje de envases, correspondiente a la recogida de envases en las plantas de selección y su traslado a los recicladores para su posterior tratamiento.
- Hemos incorporado un caso de uso de tokenización para incentivación al reciclaje, en el que se crean digitalmente tokens no fungibles que actúan como recompensa, son únicos y pueden ser programado mediante contratos inteligentes, incorporando información completa de trazabilidad de todo su ciclo de vida, la cual es registrada de manera inmutable en la red CircularTrust.

Organiza

GETAFE AYUNTAMIENTO | Empresa Municipal GETAFE INICIATIVAS | GISA GETAFE | getafe innova

Colaborador Estratégico

QAEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

getafe industria 4.0

SIMPLE: blockchain para trazabilidad en logística multimodal

adif

Puertos del Estado

GOBIERNO DE ESPAÑA | MINISTERIO DE TRANSPORTES, MOVILIDAD Y AGENDA URBANA

Blockchain en un proyecto estratégico para el sector logístico

Despliegue de red distribuida, Integración de información y trazabilidad garantizada mediante blockchain.

Estrategia de escalado

Sistema blockchain escalable en casos de uso, participantes y modelos de negocio futuro.

El reto

Puertos del Estado, ADIF y el MITMA lanzan la plataforma SIMPLE (SIMplification of Processes for a Logistic Enhancement) con el objetivo de integrar toda la información de transporte multimodal en España (marítimo, ferroviario y por carretera) y garantizar la trazabilidad de las mercancías, enfrentándose a los siguientes retos:

- Eliminar ineficiencias en los procesos actuales.
- Permitir la interoperabilidad entre los distintos actores y modos de transporte.
- Garantizar la trazabilidad de mercancías, medios de transporte y principales eventos.
- Obtener información en tiempo real.
- Contribuir para la redución de costes y mejor utilización de recursos.

La solución

- Implantamos un sistema tecnológico pionero que facilitará la colaboración y coordinación entre la Administración y las empresas del sector, impulsará la automatización de las operaciones y avanzará en la digitalización de los procesos para reducir la necesidad de papel y mejorar la eficiencia. Todo ello con los valores de blockchain para la confianza, la seguridad y la colaboración en lo que supone una referencia relevante de esta tecnología a nivel mundial.

- Incorporamos una red blockchain para el registro distribuido e inalterable de la información, creando una visión única, compartida y verificada de la información para las organizaciones participantes.

- La red blockchain nace impulsada por los tres promotores del proyecto, con un objetivo claro de crecimiento para incorporar nuevos actores y consolidarse como el ecosistema descentralizado y colaborativo de la logística en España.

06. Blockchain e Industria 4.0

Organiza

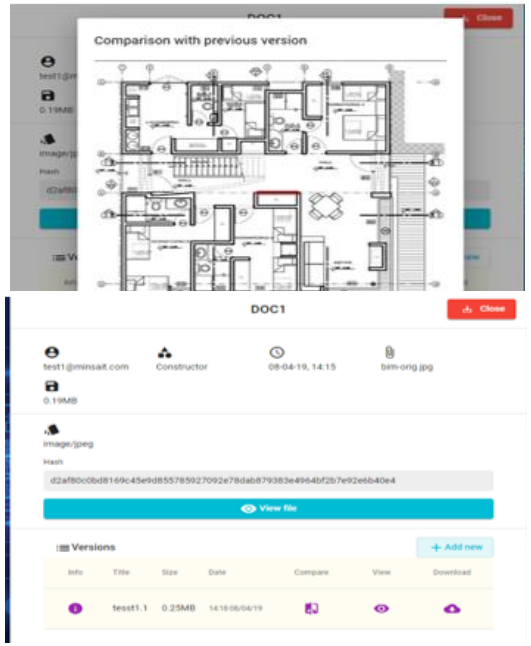
GETAFE AYUNTAMIENTO | Empresa Municipal GETAFE INICIATIVAS | GISA GETAFE | getafe innova

Colaborador Estratégico

QAEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

getafe industria 4.0

Propiedad intelectual / industrial

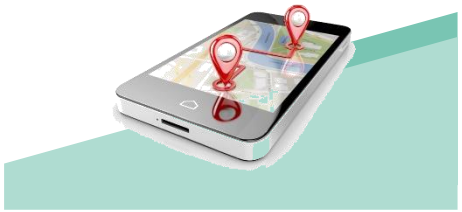


Registro de datos IoT

- Registro distribuido (ej. sensores contaminación).
- Gemelo digital.

IOTA

- Alta capacidad transaccional.
- Sin cuota por transacción.
- Adaptada a dispositivos con poca capacidad computacional y bajo consumo energético.
- Aplicable a distintos casos de uso.



Trazabilidad y cadena de suministro

- Trazabilidad de producto

Walmart

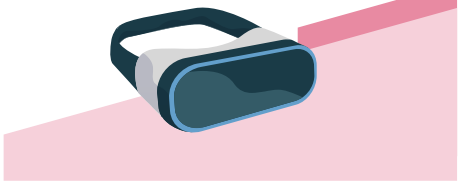
Carrefour

- Trazabilidad de piezas y componentes

BMW

- Trazabilidad emisiones de CO2 en la cadena de suministro del cobalto

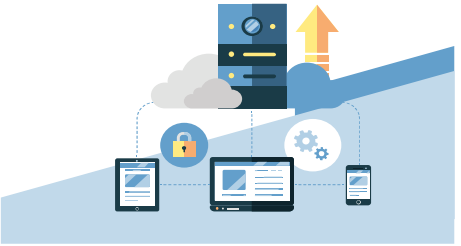
Mercedes-Benz



Automatización

Utilización de smart contracts:

- Smart maintenance: solicitud automática de reparación.
- Pedido automático de repuestos, materiales etc.
- Pagos automatizados.



M2M (Machine-to-machine)

Ejemplos:

- Carga automática de coche eléctrico.
- Comunicación entre vehículos autónomos (drones, automóviles…)
- Trading autónomo de energía entre plantas industriales.

MOBI

Mobility Open Blockchain Initiative

"La convergencia de una serie de tecnologías emergentes, que incluyen IA, IoT y Blockchain, permite que cualquier dispositivo inteligente, ya sea un vehículo, un teléfono inteligente, un sensor, una carretera u otra infraestructura de transporte, tenga una identidad, sea inteligente, se comunique y participar de forma autónoma como agente independiente en las transacciones económicas. La cantidad potencialmente grande de agentes independientes, combinada con la frecuencia y los requisitos de latencia casi en tiempo real de estas transacciones, requerirá conectividad perimetral, procesamiento, ejecución, liquidación y nuevos tipos de identificadores digitales"

07. Conclusiones

Blockchain es un paradigma	Más que una tecnología, es un nuevo modo de plantear las cosas, dando lugar a nuevos modelos
Bitcoin es un caso de éxito de blockchain	Blockchain se inventó para hacer funcionar a Bitcoin, pero Bitcoin es solamente un caso de uso.
Blockchain implica un cambio en los modelos de confianza	Es el principal cambio en la forma de pensar. Frente a los modelos de terceros de confianza y/o enfoque centralizado que tenemos muy asumido, blockchain brinda un modelo de confianza distribuida basada en el consenso.
Blockchain tiene multiples aplicaciones en todas las industrias en combinación con otras tecnologías	Transferencias bancarias, comercio internacional, cadena de suministro, marketplaces... Se adapta de forma natural a escenarios empresariales complejos con múltiples participantes que necesitan colaborar y confiar entre sí.

Organizacionales

Gobernanza

Cómo definir los criterios para ingresar a la red blockchain, los roles y responsabilidades o las decisiones sobre cambios futuros.

Estandarización

Cómo llegar a un consenso sobre un modelo de datos común para compartir en la red blockchain.

Proceso de descentralización

Cómo avanzar hacia redes descentralizadas de forma gradual y factible.

Ecosistema

Cambio cultural necesario para promover la colaboración y la creación de un ecosistema. Coopetición.

Técnicos

Escalabilidad

Rendimiento y escalabilidad.

Interoperabilidad entre redes blockchain

Víctor Sánchez Hórreo

Manager Blockchain y Tecnologías Emergentes

vsanchezh@minsait.com

minsait

An Indra company