Smart Contracts y la desintermediación de los contratos

INGENIEROS INDUSTRIALES
COLEGIO OFICIAL PRINCIPADO DE ASTURIAS

OFICINA Acelera pyme

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

OFICINA Acelera pyme

INGENIEROS INDUSTRIALES

Duración	2 años (hasta septiembre de 2023)
Objetivo	Ir de la mano de la pyme y autónomos para ayudarles en su transformación digital.
Beneficiarios	Pymes y autónomos. Multisectorial.

Líneas de actuación

de la Oficina de transformación digital "Acelera Pyme"

Gratuito y acceso libre

Objetivo: TRANSFORMACIÓN DIGITAL DE TU EMPRESA

- FORO DE TRANSFORMACIÓN DIGITAL
- VÍDEO PÍLDORAS TECNOLÓGICAS
- VISITAS A EMPRESAS Y HABILITADORES TECNOLÓGICOS
- SESIONES DE EMPRENDIMIENTO DIGITAL
- SERVICIO DE ASESORAMIENTO Y SOPORTE DIGITAL
- JORNADAS DIVULGATIVAS EN TRANSFORMACIÓN DIGITAL

KIT DIGITAL

Puedes participar en todas las acciones a través de la web WWW.OTDASTURIAS.ES

OFICINA Acelera pyme

INGENIEROS INDUSTRIALES

Duración	2 años (hasta septiembre de 2023)
Objetivo	Ir de la mano de la pyme y autónomos para ayudarles en su transformación digital.
Beneficiarios	Pymes y autónomos. Multisectorial.

Líneas de actuación

de la Oficina de transformación digital "Acelera Pyme"

Gratuito y acceso libre

Objetivo: TRANSFORMACIÓN DIGITAL DE TU EMPRESA

- FORO DE TRANSFORMACIÓN DIGITAL
- VÍDEO PÍLDORAS TECNOLÓGICAS
- VISITAS A EMPRESAS Y HABILITADORES TECNOLÓGICOS
- SESIONES DE EMPRENDIMIENTO DIGITAL
- SERVICIO DE ASESORAMIENTO Y SOPORTE DIGITAL
- JORNADAS DIVULGATIVAS EN TRANSFORMACIÓN DIGITAL

KIT DIGITAL

Puedes participar en todas las acciones a través de la web WWW.OTDASTURIAS.ES

Oficina de Transformación Digital “Acelera Pyme”

OFICINA Acelera pyme

INGENIEROS INDUSTRIALES PRINCIPADO DE ASTURIAS

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional

“Una manera de hacer Europa”

Sede del COIIAS (Oviedo)

Página web

www.otdasturias.es

RRSS

LinkedIn/Twitter/Fb/Instragram @coiias

Correo electrónico

otd@coiias.es

Suscribirse al boletín

OFICINA Acelera pyme

INGENIEROS INDUSTRIALES PRINCIPADO DE ASTURIAS

OFICINA Acelera pyme

INGENIEROS INDUSTRIALES PRINCIPADO DE ASTURIAS

Pablo Jodra Martínez

Doble Grado en Derecho y Administración y Dirección de Empresas por la Universidad de Alcalá de Henares

Máster Universitario en Gestión Internacional de la empresa

Asesor de Comercio e Inversiones Internacionales en la Oficina Económica y Comercial de la Embajada de España en Budapest

Consultor de Estrategia y Transformación Digital en Seidor

OFICINA Acelera pyme

INGENIEROS INDUSTRIALES PRINCIPADO DE ASTURIAS

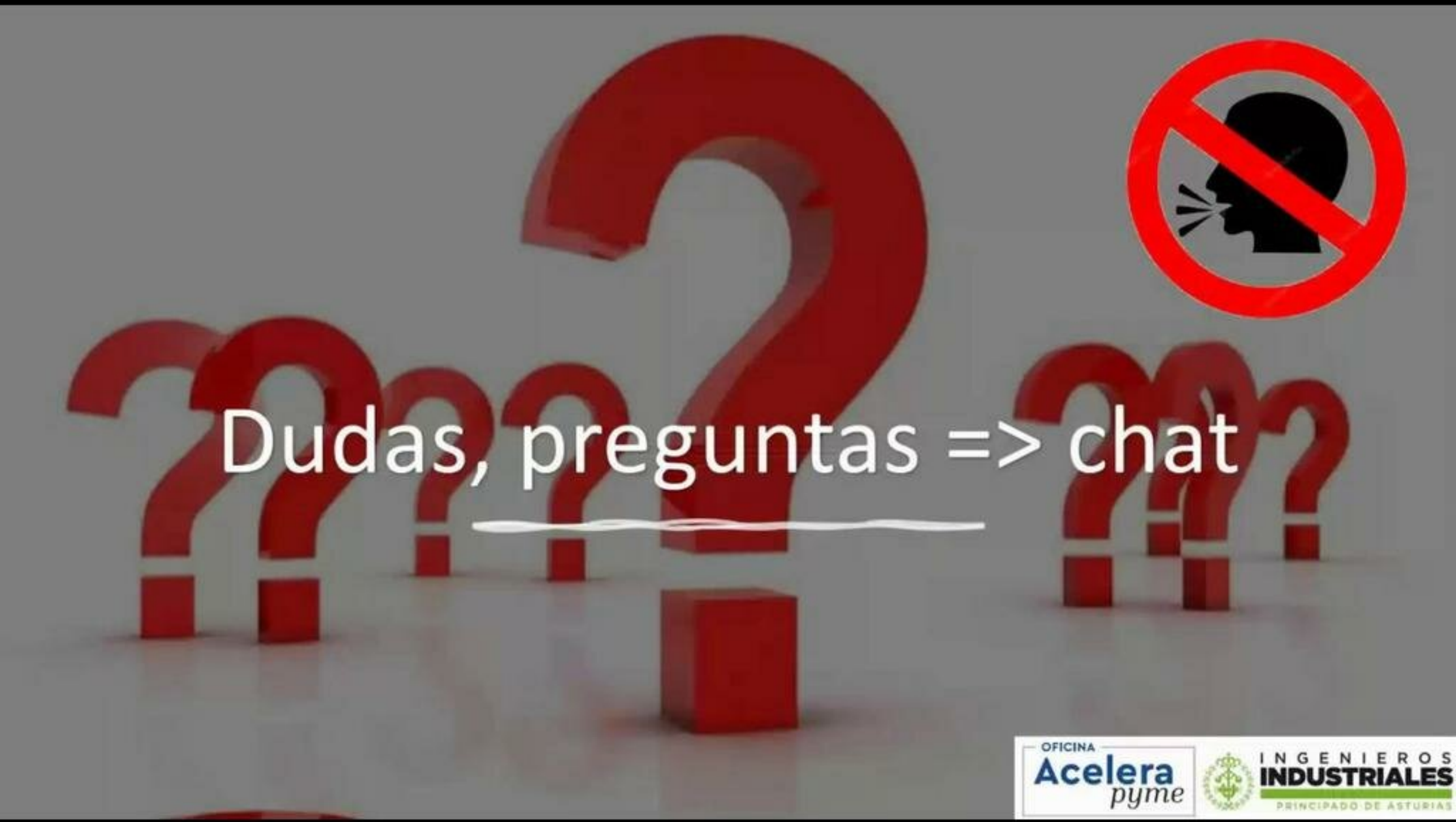
Smart Contracts y la desintermediación de los contratos

- Introducción al concepto Smart Contract

- Qué son y por qué se utilizan los Smart Contracts:
  - características
  - cómo se implementan?

- Beneficios y desafíos de los Smart Contracts

- Debate de casos de uso actuales y futuros para Smart Contracts


Dudas, preguntas => chat

INGENIEROS INDUSTRIALES
COLEGIO OFICIAL PRINCIPADO DE ASTURIAS

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

¡Gracias por Vuestra Atención!

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA

OFICINA Acelera pyme

Oficina de Transformación Digital **"Acelera Pyme"** del COIIAS

OFICINA Acelera pyme
INGENIEROS INDUSTRIALES
PRINCIPADO DE ASTURIAS

INGENIEROS INDUSTRIALES
COLEGIO OFICIAL PRINCIPADO DE ASTURIAS

Introducción a los contratos inteligentes

mayo de 2023

Agenda

1. Introducción a los contratos inteligentes
2. Tecnología Blockchain
3. Contratos inteligentes en tu negocio
4. Curiosidades de los contratos inteligentes
5. Ruegos y preguntas

01

Introducción a los contratos inteligentes

¿Qué son los contratos inteligentes?

Son **programas informáticos** almacenados en la **cadena de bloques (Blockchain)** que nos permiten convertir contratos tradicionales en paralelos digitales. Los contratos inteligentes son **lógicos** y siguen una **estructura condicional.**

¿Cómo imaginamos un contrato?

CONTRATO DE COMPRAVENTA

En Alboraya, a_____ de _____ de 2007

REUNIDOS

De una parte, y como parte vendedora:

D._____ y Dª. _____, con DNI/NIF núm._____ y _____ respectivamente, mayores de edad, con domicilio a efectos de notificaciones en la calle _____número ___pta_____de la localidad _____

De otra parte, y como parte compradora:

D. _____ y Dª._____, con DNI núm._____ y _____, respectivamente, mayores de edad, con domicilio a efectos de notificaciones en la calle_____, nº __ pta ___de la localidad de _____

Ambas partes contratantes se reconocen recíprocamente capacidad legal para firmar el presente **CONTRATO PRIVADO DE COMPRAVENTA**, haciendo constar que interviene la parte vendedora en su propio nombre y derecho, y al efecto,

EXPONEN

I.- **FINCA OBJETO DE ESTE CONTRATO**

Que D._____ y Dña._____ son dueños en pleno dominio, como bien ganancial que no constituye su domicilio familiar, de una finca sita en _____, en la calle _____ nº ___, planta __, pta. ___, con una superficie útil de _____ metros cuadrados.

INSCRIPCIÓN: inscrita a su favor en el Registro de la Propiedad de Valencia num. ____, Tomo _____, Libro ____, Folio ____, Finca_____, Inscripción_____, y con una participación en los elementos comunes de _____

Pero se parece más a esto

```
1 contract Puzzle{
2   address public owner;
3   bool public locked;
4   uint public reward;
5   bytes32 public diff;
6   bytes public solution;
7
8   function Puzzle() //constructor{
9     owner = msg.sender;
10    reward = msg.value;
11    locked = false;
12    diff = bytes32(11111); //pre-defined difficulty
13  }
14
15  function(){ //main code, runs at every invocation
16    if (msg.sender == owner){ //update reward
17      if (locked)
18        throw;
19      owner.send(reward);
20      reward = msg.value;
21    }
22    else
23      if (msg.data.length > 0){ //submit a solution
24        if (locked) throw;
25        if (sha256(msg.data) < diff){
26          msg.sender.send(reward); //send reward
27          solution = msg.data;
28          locked = true;
29        }}}}
```

Figure 3: A contract that rewards users who solve a computational puzzle.

¿De dónde viene este término?

Nick Szabo acuñó el término «contrato inteligente».

En **1994**, escribió una introducción al **concepto**.

En **1996**, exploró las **posibilidades** de los contratos inteligentes.

Nick Szabo definía un contrato inteligente

Un **conjunto de promesas**
especificadas en **formato digital**,
incluyendo los **protocolos** por medio
de los cuales las partes **ejecutan**
dichas promesas

Los principales objetivos de los contratos inteligentes

Son **satisfacer** las condiciones contractuales habituales (como **condiciones de pago**, **gravámenes**, **clausulas de confidencialidad** e incluso imposición del cumplimiento), **minimizar las excepciones** tanto maliciosas como accidentales y **reducir al mínimo la necesidad de intermediarios** de confianza.

La confianza en los contratos

Aunque se cumplan las condiciones de un acuerdo, aún **se debe confiar en que la otra parte decida cumplir el acuerdo**.

En caso de incumplimiento, se debe acudir a algún organismo de aplicación de la ley (**juzgado**), que pueda aplicar medidas como arrestos o embargos.

Imaginemos un contrato inteligente como una máquina expendedora

Las entradas específicas (**€**) garantizan salidas predeterminadas (**productos**).

1) Seleccione un producto
2) La máquina expendedora devuelve la cantidad requerida para comprar el producto
3) Inserte la cantidad correcta
4) La máquina expendedora verifica que haya insertado la cantidad correcta.
5) La máquina expendedora dispensa el producto elegido.


¿Cuáles son sus principales características?

¿Cuáles son sus principales características?

1. Automáticos
2. Inmutables
3. Autónomos
4. Transparentes
5. Inmutables
6. Lógicos
7. Eficientes
8. Interoperables
9. Descentralizados

Son automáticos

Una vez que se cumplen las **condiciones predefinidas**, el contrato ejecuta **automáticamente** las **acciones especificadas** sin necesidad de intervención manual.

Son autónomos

Los contratos inteligentes son **autoejecutables** y funcionan **sin necesidad de intermediarios**.

Eliminan la necesidad de depender de terceros como abogados, corredores o agentes de custodia para hacer cumplir los términos del contrato.

Son transparentes

Al **ejecutarse dentro de una cadena de bloques** ofrecen transparencia, ya que todas las transacciones y estados del contrato quedan **registrados** y son **visibles para todos los participantes.**

La confianza se establece mediante **algoritmos criptográficos que garantizan la integridad y la inmutabilidad de la ejecución del contrato**.

Son inmutables

Una vez que un contrato inteligente se despliega en una cadena de bloques, **su código y su historial** de ejecución son inmutables. **No pueden alterarse ni manipularse**, lo que proporciona un alto nivel de seguridad y **elimina el riesgo de fraude o manipulación**.

Siguen una lógica condicional

Los contratos inteligentes contienen **condiciones y lógica predefinidas** que determinan la ejecución de acciones.

Estas condiciones pueden ser simples (por ejemplo, desencadenantes basados en el tiempo) o complejas (por ejemplo, requisitos de firma múltiple), lo que permite acuerdos sofisticados y procesos de varios pasos.

Son eficientes

Los contratos inteligentes **reducen la necesidad de intermediarios, papeleo y procesos manuales**, lo que se traduce en un ahorro de costes.

Eliminan los gastos generales asociados a la ejecución de contratos tradicionales, como los **honorarios legales** y los **gastos administrativos**.

Son interoperables

Los contratos inteligentes pueden interactuar y **comunicarse con otros contratos inteligentes** o sistemas externos, permitiendo la **creación de aplicaciones descentralizadas complejas** (DApps) y facilitando una integración perfecta con otros servicios basados en blockchain.

Son descentralizados

En la Blockchain ninguna entidad tiene el control total.

La naturaleza descentralizada de los contratos inteligentes mejora la seguridad, la resiliencia y la **resistencia a la censura**.

02

Tecnología Blockchain

¿Qué es Blockchain?

Blockchain es un **libro de contabilidad** compartido e inmutable que facilita el proceso de **registro** de **transacciones** y **seguimiento** de **activos** en una red empresarial. Un activo puede ser tangible (una casa, un coche, efectivo, tierra) o intangible (propiedad intelectual, patentes, derechos de autor, marcas). Prácticamente cualquier cosa de valor puede rastrearse y negociarse en una cadena de bloques.

¿De dónde surge la necesidad de crear una cadena de bloques?

A lo largo de la historia, los **instrumentos de confianza**, como las monedas acuñadas, el papel moneda, las tarjetas de crédito y los sistemas bancarios han surgido para facilitar el **intercambio de valor** y proteger a los compradores y vendedores.

Importantes innovaciones han mejorado la comodidad, rapidez y eficacia de las transacciones a la vez que reducen la **distancia entre compradores y vendedores**.

¿Qué limitaciones encontramos? (1)

- El **efectivo** es útil sólo en **transacciones cercanas** y en cantidades relativamente pequeñas.

- El **tiempo** entre la transacción y la liquidación puede ser largo.

- La duplicación de esfuerzos y la necesidad de **validación por terceros** y/o la presencia de intermediarios se suman a las ineficiencias.

- El fraude, los ataques cibernéticos e incluso los errores simples aumentan el coste y la complejidad de hacer negocios, exponiendo a todos los participantes en la red al riesgo si un sistema central, como un banco, se ve comprometido.

¿Qué limitaciones encontramos? (2)

- Las **organizaciones de tarjetas de crédito** son jardines amurallados con un alto precio de entrada. Los comerciantes deben pagar los **altos costes** de incorporación, que a menudo implica un papeleo considerable y un proceso de investigación que consume mucho tiempo.

- La mitad de la población mundial **no tiene acceso a cuentas bancarias**, lo que les obliga a desarrollar sistemas de pago paralelos para realizar transacciones.

- La **transparencia limitada y la información inconsistente** obstaculizan el movimiento eficiente de mercancías en la industria naviera.

¿A qué retos debemos hacer frente?

- El volumen de transacciones aumenta exponencialmente.

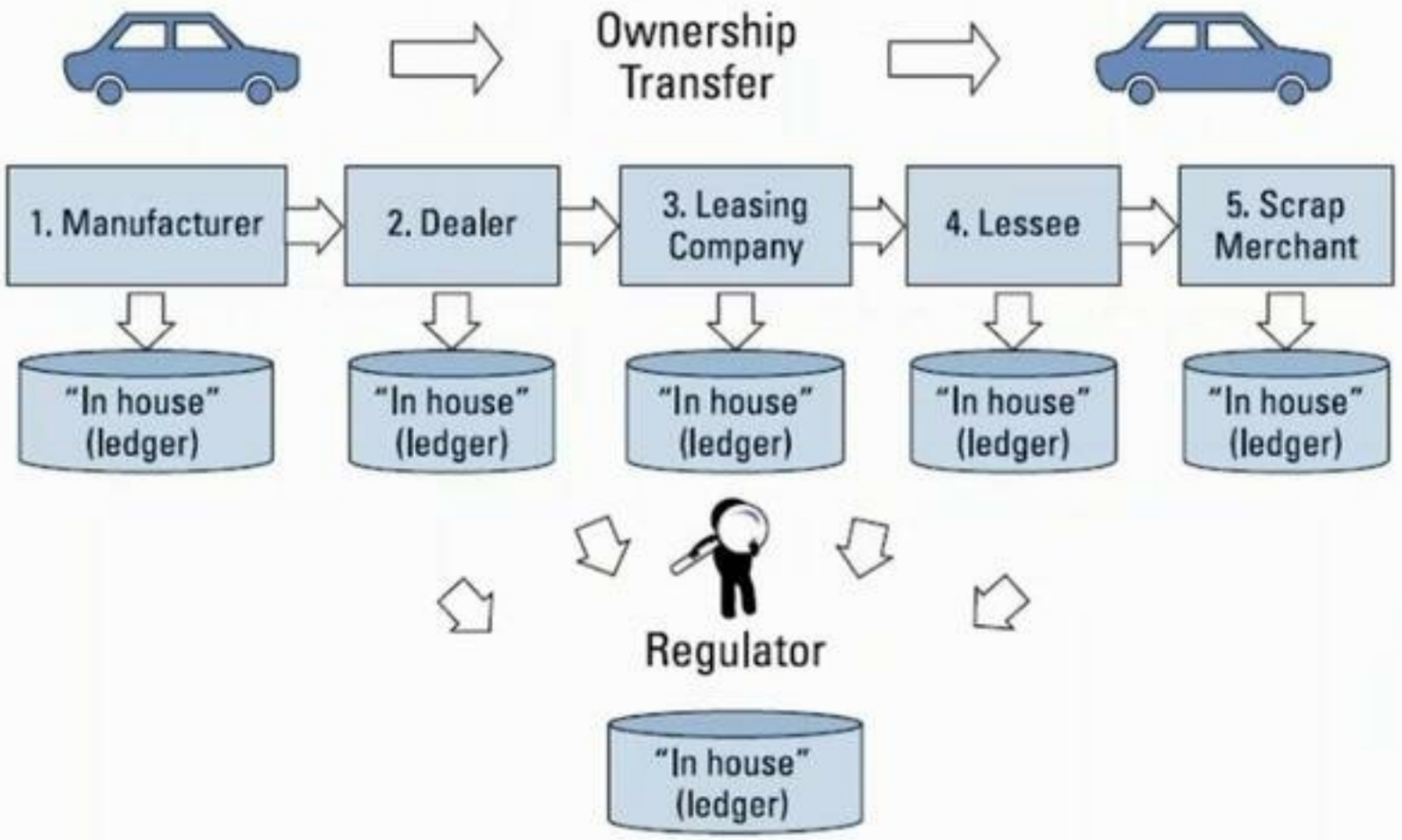
- Aumentan las complejidades, vulnerabilidades, deficiencias y costes del sistema.

- Aumenta el comercio digital, la banca online y la movilidad por el mundo.

Y más...

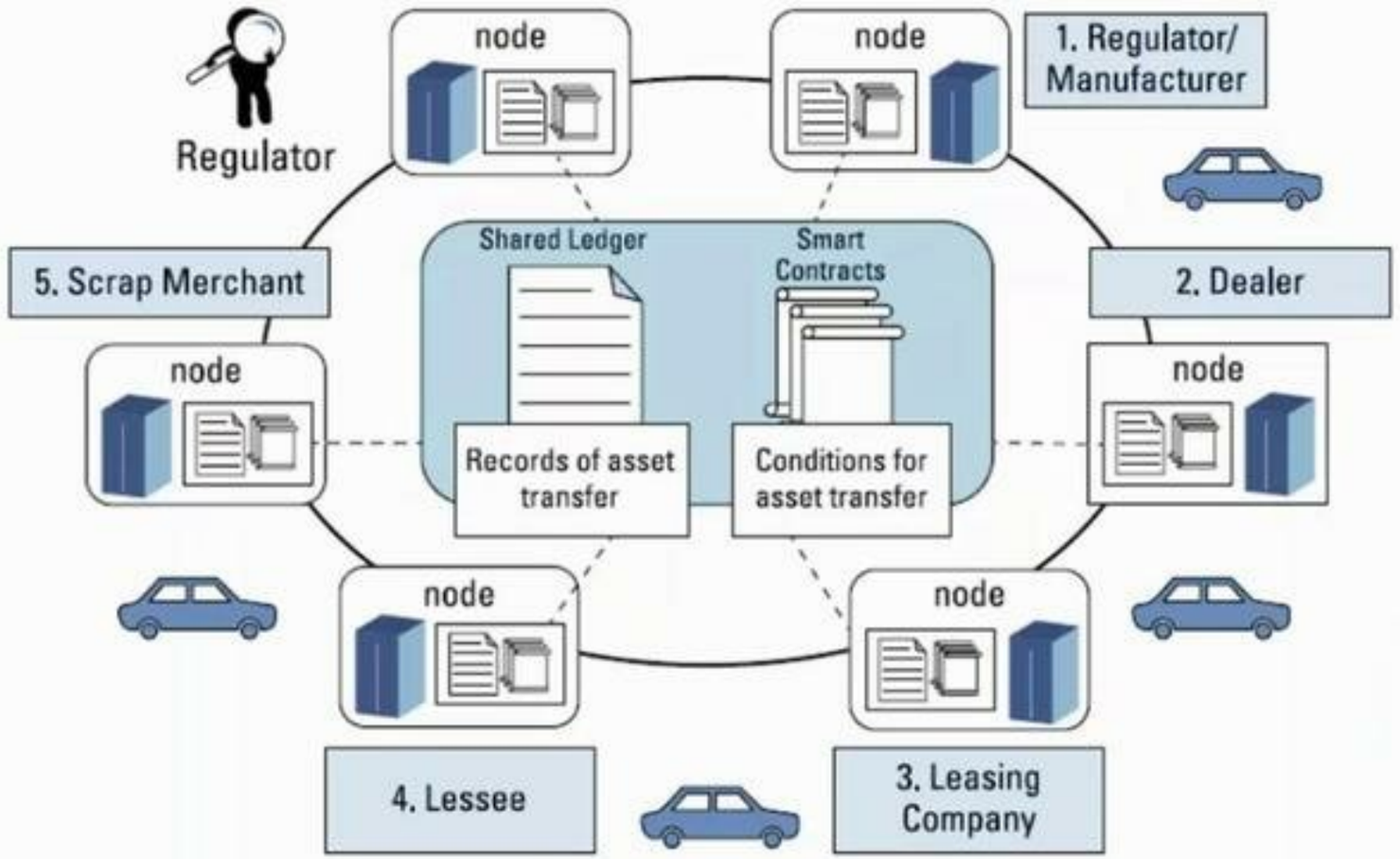
Exploremos las aplicaciones de las cadenas de bloques

Trazabilidad de la propiedad de un vehículo **sin utilizar** cadenas de bloques



Exploremos las aplicaciones de las cadenas de bloques

Trazabilidad de la propiedad de un vehículo **utilizando** cadenas de bloques



Pero, ¿cómo se protege nuestra privacidad?

Descentralización de la identidad

- Algunas formas de identificación serían: licencia de conducir, número de seguro social, número de persona en una institución educativa, número de empleado.
- Todo esto son afiliaciones a instituciones centralizadas.
- En un sistema descentralizado, donde los participantes son desconocidos, y pueden unirse y salir como deseen, ¿cómo podemos identificarlos?
- **Necesitamos una identidad segura autogenerada.**

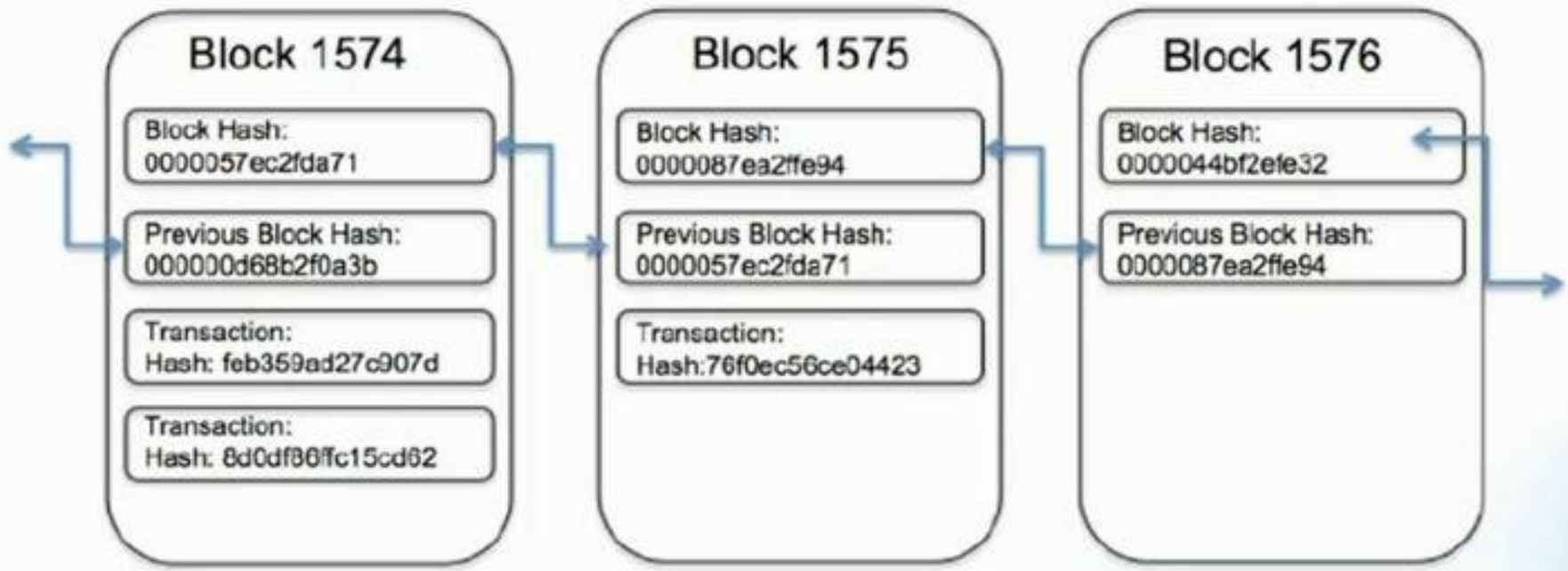
¿Cómo funciona en la red de Ethereum?

- Se genera un número aleatorio de 256 bits y se designa como clave privada.
- Se aplica un algoritmo de criptográfico complejo a esta clave privada para obtener una clave pública.
- Este es el par de claves {private, public} de la cuenta.
- La clave privada está protegida mediante una contraseña y la clave pública está abierta al mundo.
- Una función hash, se aplica a la clave pública para obtener la dirección de la cuenta (o identidad, nuestra identidad).
- La dirección se representa en hexadecimal para facilitar la lectura, como lo indica el 0x como los dos primeros caracteres; por ejemplo,

0xca35b7d915458ef540ade6068dfe2f44e8fa733c.

¿Cómo funciona la blockchain?

Cómo funciona



Blockchain genera confianza a través de 5 atributos

Los 5 atributos de Blockchain que generan confianza

1. Distribuido y sostenible
2. Seguro, privado, indeleble
3. Transparente y auditable
4. Basado en el consenso y transaccional
5. Orquestado y flexible

Distribuido y sostenible

El libro mayor se comparte, **se actualiza con cada transacción**, y se replica selectivamente entre participantes casi en tiempo real. Al no ser propiedad ni estar controlada por una única organización, su existencia no depende de ninguna entidad individual.

Seguro, privado e indeleble

Los permisos y la criptografía impiden el acceso no autorizado a la red y garantizan que los participantes son quienes dicen ser. La **confidencialidad** se mantiene mediante técnicas criptográficas y/o técnicas de partición de datos para dar a los participantes una visibilidad selectiva del libro mayor; tanto las transacciones como la identidad de las partes que las realizan pueden enmascararse. Una vez acordadas las condiciones, **los participantes no pueden alterar el registro de la transacción**; los errores sólo pueden revertirse con nuevas transacciones.

Transparente y auditable

Dado que los participantes en una transacción tienen acceso a los mismos registros, pueden validar las transacciones y verificar las identidades o la propiedad sin necesidad de terceros intermediarios. **Las transacciones llevan un sello de tiempo, están ordenadas y pueden verificarse prácticamente en tiempo real.**

Basado en el consenso y transaccional

Todos los participantes deben estar de acuerdo en que una transacción es válida. Esto se consigue mediante el uso de algoritmos de consenso. Cada cadena de bloques puede establecer las condiciones en las que puede producirse una transacción o un intercambio de activos.

Orquestada y flexible

Dado que las reglas de negocio y los contratos inteligentes (que se ejecutan en función de una o varias condiciones) pueden incorporarse a la plataforma, **las redes empresariales de blockchain pueden evolucionar a medida que maduran para dar soporte a procesos empresariales integrales** y a una amplia gama de actividades.

Participantes en una cadena de bloques

Usuario de Blockchain

Un participante (normalmente un usuario de negocio) con **permisos para unirse a la red blockchain y realizar transacciones** con otros participantes de la red.

Blockchain funciona en segundo plano, por lo que el usuario no tiene por qué tener visión de ella. Normalmente hay múltiples usuarios en cualquier red empresarial.

Regulador

Un usuario de blockchain con **permisos especiales** para **supervisar** las transacciones que tienen lugar en la red.

Los reguladores pueden tener prohibido realizar transacciones.

Desarrollador de blockchain

Programadores que crean las aplicaciones y contratos inteligentes que permiten a los usuarios realizar transacciones en la red blockchain.

Las aplicaciones sirven de nexo entre los usuarios y la blockchain.

Operador de la red

Personas que **tienen permisos y autoridad especiales para definir, crear, gestionar y supervisar la red blockchain.**

Cada empresa que forma parte de una red blockchain tiene un operador de red blockchain.

Plataformas de procesamiento

Sistemas informáticos existentes que pueden ser utilizados por la cadena de bloques para aumentar el procesamiento.

Este sistema también puede tener que iniciar solicitudes a la cadena de bloques.

Fuentes de datos tradicionales

Sistemas de datos existentes que pueden **proporcionar información para influir en el comportamiento de los contratos inteligentes** y ayudar a definir cómo se producirán las comunicaciones entre las aplicaciones/datos tradicionales y la blockchain, por ejemplo, a través de llamadas API.

Autoridad de certificación

Individuo **que emite y gestiona los diferentes tipos de certificados necesarios para ejecutar una cadena de bloques autorizada**.

Por ejemplo, puede ser necesario emitir certificados para los usuarios de la cadena de bloques o para transacciones individuales.

Modificación y eliminación de los contratos inteligentes

Modificación de los contratos inteligentes

La modificación de un contrato inteligente existente en la cadena de bloques requiere, generalmente, la creación de un nuevo contrato inteligente con los términos y condiciones actualizados.

Eliminación de los contratos inteligentes

La eliminación de un contrato inteligente es aún más difícil, ya que la naturaleza inmutable de la cadena de bloques significa que los registros de la transacción que involucra el contrato inteligente permanecen en la cadena de bloques de forma permanente.

03

Contratos inteligentes en tu negocio

Aplicaciones de los contratos inteligentes

Finanzas

Los contratos inteligentes se pueden utilizar en el sector financiero para una variedad de aplicaciones como **seguros**, **trading**, **préstamos** y más.

Por ejemplo, las compañías de seguros pueden utilizar contratos inteligentes para **procesar automáticamente las reclamaciones** y las indemnizaciones sin necesidad de intervención humana.

Del mismo modo, las plataformas de trading pueden utilizar contratos inteligentes para **ejecutar operaciones automáticamente** cuando se cumplen ciertas condiciones, eliminando la necesidad de intermediarios.

Cadena de suministro

Los contratos inteligentes pueden utilizarse para hacer el **seguimiento** y gestionar las operaciones de la cadena de suministro de forma más eficiente.

Por ejemplo, un contrato inteligente podría utilizarse para **seguir el recorrido de un producto desde el fabricante hasta el usuario final (trazabilidad)**, garantizando que cumple todas las normas de calidad y seguridad a lo largo del camino.

Sector inmobiliario

Los contratos inteligentes pueden utilizarse en el sector inmobiliario para automatizar procesos como las **transferencias de propiedades**, los **pagos en garantía** y los contratos de alquiler.

Por ejemplo, un contrato inteligente podría utilizarse para **transferir automáticamente la propiedad** de un inmueble una vez que el comprador haya cumplido todas las condiciones de la venta.

Sanidad

Los contratos inteligentes pueden utilizarse en el sector sanitario para diversas aplicaciones, como **la gestión de datos de pacientes**, los **ensayos clínicos** y la gestión de la cadena de suministro.

Por ejemplo, un contrato inteligente podría utilizarse para gestionar automáticamente los historiales de los pacientes y garantizar que los datos de los pacientes se almacenan de forma segura y sólo son accesibles para las partes autorizadas.

Gaming

Los contratos inteligentes pueden utilizarse en la industria del gaming para garantizar el juego limpio y la **transparencia en los pagos**.

Por ejemplo, un contrato inteligente podría utilizarse para ejecutar automáticamente **apuestas** y pagos en plataformas de juego en línea, garantizando que se siguen las reglas y que los pagos se realizan de forma justa y transparente.

Servicios de depósitos de garantía

Los contratos inteligentes pueden utilizarse como un **servicio de custodia en las transacciones**, donde los fondos o activos se mantienen en una **cuenta neutral** hasta que se cumplan las condiciones acordadas.

Por ejemplo, en una transacción inmobiliaria, los fondos para la compra de una propiedad pueden retenerse en un contrato inteligente de custodia hasta que se cumplan todas las condiciones de la venta.

Tokenización de activos

Los contratos inteligentes pueden utilizarse para crear **tokens** que **representen la propiedad o el valor de un activo**, como bienes inmuebles u obras de arte. A continuación, estos tokens pueden negociarse en una plataforma basada en blockchain, lo que facilita y agiliza la transferencia de la propiedad y ofrece opciones de propiedad fraccionaria.

Crowdfunding

Los contratos inteligentes pueden utilizarse para crear plataformas de crowdfunding que **distribuyan fondos automáticamente a los proyectos cuando cumplan determinados hitos o condiciones**.

Por ejemplo, un contrato inteligente puede utilizarse para mantener los fondos recaudados en una campaña de crowdfunding y distribuirlos al proyecto a medida que alcanza determinados hitos de desarrollo.

Organizaciones autónomas descentralizadas (DAO)

Los contratos inteligentes pueden utilizarse para crear organizaciones autónomas descentralizadas, que son organizaciones **que operan enteramente en una plataforma blockchain** sin una autoridad centralizada.

Las reglas y los procesos de toma de decisiones de la organización se codifican en contratos inteligentes, y los miembros pueden votar sobre las decisiones a través de la plataforma.

Cumplimiento legal y normativo

Los contratos inteligentes operan en el ámbito del código y no siempre se alinean perfectamente con los marcos legales existentes. La traducción de los acuerdos legales al código de los contratos inteligentes puede resultar compleja, y **garantizar el cumplimiento de las normativas y jurisdicciones pertinentes puede ser todo un reto.**

En algunos casos, los acuerdos legales tradicionales y la validación de terceros pueden seguir siendo necesarios para garantizar la aplicabilidad legal.

Dependencia de los oráculos

Los "**oráculos**" son las **fuentes de datos** en las que se basan los contratos inteligentes para comprobar que se cumplen algunos de los criterios de un contrato.

Si cualquier nodo de la blockchain de un contrato es pirateado, puede registrar datos falsificados que luego se convierten en inmutables en el libro mayor distribuido, lo que podría desencadenar la ejecución automatizada del resultado del contrato inteligente.

O, con el tiempo, una empresa de oráculos podría simplemente quebrar y dejar de recopilar y distribuir información.

Retos en su usabilidad

Debido al diseño de los contratos inteligentes y a sus **aplicaciones muy específicas**, el desarrollo de contratos inteligentes requiere **conocimientos especializados de ingeniería de software**.

A diferencia del desarrollo de software tradicional, los contratos inteligentes requieren que los desarrolladores tengan **conocimientos empresariales y entiendan lenguajes de programación no tradicionales**, principalmente **Solidity**. También deben **comprender métodos formales de criptografía y redes**.

Retos de impactos y escalabilidad

En la actualidad, **Visa** puede gestionar **unas 24.000 transacciones por segundo.**

Ethereum, la mayor cadena de bloques para contratos inteligentes, sólo puede gestionar **14 transacciones por segundo.**

04

Curiosidades de los contratos inteligentes

¿Qué fue The DAO?

The DAO fue una de las primeras y más conocidas DAO, lanzada en **2016** en la blockchain de Ethereum. The DAO se creó como un **fondo de capital riesgo** descentralizado que permitía a sus miembros invertir en una serie de proyectos utilizando **Ether**, la criptomoneda de la red Ethereum.

¿Qué cuestiones surgieron a raíz de este incidente?

The DAO fue pirateada, lo que provocó la pérdida de aproximadamente 50 millones de dólares en Ether.

El incidente planteó importantes cuestiones sobre la seguridad y la gobernanza de las DAO, pero también puso de relieve su potencial como nueva forma de organización descentralizada.

Relación entre la firma digital y los contratos inteligentes

Tanto la firma electrónica como el contrato inteligente son tecnologías digitales utilizadas en el contexto de acuerdos y contratos, pero tienen propósitos y características diferentes.

Firma digital

Se utiliza para indicar la aprobación o el consentimiento del firmante a un documento o acuerdo.

Puede adoptar diversas formas, como una imagen escaneada de una firma manuscrita, una firma mecanografiada o una firma digital creada con software especializado.

Similitudes

Tanto la firma electrónica como los contratos inteligentes son tecnologías digitales que se utilizan para facilitar acuerdos y contratos.

Ambas pretenden ofrecer una forma más eficiente y segura de realizar transacciones y reducir la necesidad de intermediarios o terceros de confianza.

Además, ambas tecnologías se basan en la criptografía para garantizar la seguridad y autenticidad de la transacción.

Diferencia

Principalmente, sus finalidades son diferentes.

Un contrato inteligente es un acuerdo autoejecutable que aplica automáticamente los términos de un acuerdo.

Relación entre los NFT y los contratos inteligentes

¿Qué es un NFT?

Un NFT, o token no fungible, es un tipo de **activo digital** que representa un artículo o **contenido único**.

A diferencia de las criptomonedas, que son fungibles y pueden intercambiarse por el mismo valor, los NFT **no son fungibles ni intercambiables**.

Nociones generales de un NFT

Las NFT se crean y almacenan en una red blockchain, como Ethereum, que permite un alto grado de transparencia y seguridad.

Cada NFT tiene un **identificador único** que se registra en la blockchain, junto con los **metadatos** asociados, que pueden incluir información como el creador, la fecha de creación y la descripción del NFT.

¿A qué representan?

Activos digitales, como obras de arte, música, vídeo, bienes inmuebles virtuales y otros.

A menudo se utilizan en el contexto del **arte digital**, donde permiten a los creadores vender y autenticar sus obras como únicas y originales.

¿Están relacionados los NFT con los contratos inteligentes?

Los NFT (tokens no fungibles) y los contratos inteligentes están estrechamente relacionados, ya que los NFT suelen crearse y gestionarse mediante el uso de contratos inteligentes.

Aumento en su adopción

A medida que la tecnología blockchain se adopta más ampliamente y se integra en diversos sectores, se espera que el uso de contratos inteligentes crezca significativamente.

Es probable que **sectores** como las **finanzas**, la gestión de la **cadena de suministro**, **el sector inmobiliario**, la **atención sanitaria** y los **derechos de propiedad intelectual** aprovechen los contratos inteligentes para **aumentar la eficiencia**, la transparencia y la automatización.

Crecimiento de la interoperabilidad de estos

Actualmente, la mayoría de los contratos inteligentes se construyen en plataformas blockchain específicas, lo que limita su interoperabilidad.

Sin embargo, se están realizando esfuerzos para desarrollar **normas y protocolos** que permitan que los contratos inteligentes **funcionen sin problemas en diferentes redes de cadenas de bloques**.

Esto permitiría una **mayor flexibilidad, eficiencia y colaboración entre diferentes ecosistemas de blockchain.**

Aumento de su potencial gracias a la integración con IoT y AI

La integración de los contratos inteligentes con el Internet de las Cosas (IoT) y las tecnologías de inteligencia artificial (AI) tiene un potencial significativo.

Los **contratos inteligentes pueden permitir transacciones autónomas y autoejecutables entre dispositivos IoT,** haciendo que los procesos sean más eficientes y seguros.

Además, los **algoritmos de IA pueden analizar datos y desencadenar acciones dentro de los contratos inteligentes**, lo que permite una toma de decisiones dinámica e inteligente.

Mayor privacidad y escalabilidad

Las plataformas actuales de cadena de bloques se enfrentan a desafíos en términos de escalabilidad y privacidad.

Los futuros avances en la tecnología blockchain, como la **fragmentación**, las **cadenas laterales** y las **técnicas criptográficas avanzadas**, pueden abordar estas limitaciones.

Esto permitiría a los contratos inteligentes gestionar mayores volúmenes de transacciones, mantener la privacidad de la información sensible y garantizar el cumplimiento de la normativa sobre protección de datos.

Adopción de enfoques Híbridos

Aunque los contratos inteligentes totalmente autónomos tienen sus ventajas, puede haber escenarios en los que se adopten enfoques híbridos.

Estos enfoques podrían **combinar las ventajas de los contratos inteligentes con los marcos jurídicos tradicionales**, permitiendo la inclusión de disposiciones legales, mecanismos de resolución de conflictos y supervisión humana en acuerdos complejos.

Integración de datos del mundo real

Se espera que la integración de los contratos inteligentes con fuentes de datos del mundo real a través de **oráculos de confianza** mejore sus capacidades.

Esto **permitiría a los contratos inteligentes acceder a datos externos**, como los precios del mercado financiero, las condiciones meteorológicas o la información de la cadena de suministro, **mejorando su funcionalidad y aplicabilidad en escenarios del mundo real**.

Avances normativos

A medida que crece la adopción de contratos inteligentes, **es probable que los reguladores desarrollen marcos y directrices para abordar los aspectos legales y normativos**.

Esto aportaría **claridad** y establecería un entorno más favorable para que **empresas** y **particulares** participen en acuerdos basados en contratos inteligentes.

Turno de ruegos y preguntas

MUCHAS GRACIAS

pablo.jodra@seidor.com