Co-funded by the
Erasmus+ Programme
of the European Union

DLT4All: Programa

Co-funded by the
Erasmus+ Programme
of the European Union

Índice

Introducción

El plan de estudios propuesto por el proyecto DLT4All consiste en los siguientes módulos de aprendizaje:

- **LM0** – Introducción al curso y al mundo de las DLT.
- **LM1** – Diseño de bases de datos P2P.
- **LM2** – Técnicas de cifrado.
- **LM3** – Mecanismos de consenso.
- **LM4** – Firmas digitales.
- **LM5** – Contratos inteligentes.
- **LM6** – Privacidad y derechos de propiedad.
- **LM7** – Aplicaciones descentralizadas basadas en *blockchain*.
- **LM8** – Organizaciones autónomas descentralizadas.

LM0: Introducción al curso y al mundo de las DLT

Descripción

El módulo de aprendizaje 0 se divide lógicamente en dos partes.

La primera parte proporciona una introducción al curso DLT4All, identificando diferentes audiencias objetivo y las partes del plan de estudios dirigidas a cada una de ellas, y presentando una perspectiva general de las opciones de certificación disponibles.

La segunda parte proporciona una introducción a las tecnologías *blockchain* desde una perspectiva histórica y un punto de vista técnico. Presenta una perspectiva general de la estructura de las *blockchains* e introduce los conceptos centrales que se desarrollarán en los siguientes módulos del curso. Proporciona una taxonomía de las *blockchains* basada en sus permisos de lectura y escritura e introduce los conceptos de criptomoneda, contrato inteligente y aplicación descentralizada. El módulo se cierra con una perspectiva general de los casos de uso de la *blockchain.*

Objetivos del aprendizaje

- Presentar la estructura y contenido del curso DLT4All.
- Definir las diferentes audiencias objetivo del curso DLT4All.
- Describir las opciones de certificación disponibles para los participantes.
- Presentar una perspectiva histórica general del desarrollo de la tecnología *blockchain.*
- Presentar una perspectiva general de los componentes tecnológicos de un sistema basado en *blockchain*.
- Presentar una caracterización de las *blockchains* basada en los permisos de lectura/escritura del usuario.
- Describir los conceptos de criptomoneda, contrato inteligente y aplicación descentralizada en el contexto de un sistema basado en *blockchain*.
- Presentar un conjunto de casos de uso relevantes de los sistemas basados en *blockchains*.

Resultados esperados del aprendizaje

- **Recordar** la estructura del curso DLT4All.
- **Elegir** a cuál de las audiencias objetivo pertenecen.
- **Comprender** las opciones de certificación disponibles.
- **Esbozar** el desarrollo histórico de las tecnologías *blockchain*.
- **Describir** los componentes técnicos de un sistema basado en *blockchain*.
- **Explicar** cómo pueden clasificarse las *blockchains*.
- **Explicar** los conceptos de criptomoneda, contrato inteligente y aplicación descentralizada.
- **Nombrar** y **describir** casos relevantes de uso de *blockchain*.

Programa

1. Introducción al curso DLT4ALL
   1.1. Audiencia objetivo
   1.2. Estructura del curso
   1.3. Opciones de certificación

2. Introducción a las *blockchains*
   2.1. Perspectiva histórica general
   2.2. Componentes tecnológicos de un sistema basado en *blockchain*
3. Caracterización de las *blockchains*
   3.1. Públicas *vs.* privadas, autorizadas *vs.* no autorizadas
4. De las *blockchains* a las *dApps*
   4.1. Criptomonedas
   4.2. Contratos inteligentes
   4.3. Aplicaciones descentralizadas
5. Casos de uso

LM1: Diseño de bases de datos P2P

Descripción

La posibilidad de disponer de bases de datos abiertas y compartidas con información certificada y públicamente verificable puede impulsar la participación y el empoderamiento de los ciudadanos en muchas áreas.

El módulo de aprendizaje 1 proporciona una discusión en profundidad de los problemas de diseño y arquitectura de la gestión de datos. Presenta y analiza con detalle los retos a enfrentar cuando se diseña una base de datos distribuida y descentralizada, introduciendo los principios básicos del diseño de bases de datos y los mecanismos subyacentes a las redes de comunicación P2P, y presenta las dificultades que se encuentran al desarrollar una base datos P2P fiable, junto con las soluciones potenciales que las tecnologías *blockchain* proporcionan a estos problemas.

Los participantes comprenderán cómo puede compartirse y sincronizarse entre diferentes nodos una base de datos y por qué no es sencillo alterar posteriormente su estructura. Así, podrán determinar cuándo es apropiado utilizar una base de datos distribuida. Comprenderán por qué una base de datos distribuida es fiable y cómo esta tecnología puede hacer más seguras las transacciones y el intercambio de datos en las cadenas de suministro. Podrán reconocer cómo en algunos casos merece la pena crear una nueva *blockchain ad-hoc*, mientras en otros es mejor utilizar una *blockchain* existente para garantizar la integridad de la información intercambiada con los proveedores.

Requisitos

Este módulo no tiene requisitos previos.

Objetivos del aprendizaje

- Explicar qué es una base de datos y lo esencial de cómo funciona.
- Introducir los conceptos básicos de la tecnología de comunicación P2P y sus ventajas sobre el paradigma tradicional.
- Explicar los métodos utilizados para crear una base de datos en un entorno P2P (esto es, la blockchain).
- Tratar los límites y las desventajas de utilizar la tecnología *blockchain* en lugar de una base de datos centralizada.
- Presentar casos de uso en los que la tecnología blockchain resulta beneficiosa.

Resultados esperados del aprendizaje

- **Comprender** los conceptos básicos del diseño de bases de datos.
- **Comprender** los mecanismos básicos de funcionamiento de las redes de comunicación P2P.
- **Comprender** por qué se ha desarrollado la tecnología *blockchain* como una solución a los problemas que implica diseñar una base de datos P2P distribuida.
- **Explicar** en qué casos las bases de datos P2P pueden ser útiles o no.
- **Comprender** por qué la integridad de la información no es una garantía de exactitud de la información cuando se involucra el factor humano.

Co-funded by the
Erasmus+ Programme
of the European Union

1. Qué es una base de datos y cómo funciona
   1.1. Principios de las bases de datos, cómo funciona actualmente una base de datos
   1.2. Dónde funcionan mejor las bases de datos y por qué se necesita una nueva tecnología
2. Qué es el P2P y en qué se diferencia del paradigma tradicional de comunicación
   2.1. Mejores resultados en la distribución y descentralización de la información
   2.2. Ausencia de puntos críticos
3. Cómo crear una base de datos fiable en una red P2P, la *blockchain*
   3.1. Cómo se encajan los bloques de información
   3.2. Por qué está casi garantizada la integridad de la cadena de información
4. Límites de la tecnología *blockchain*, casos de uso en los que resulta apropiada y en los que no
   4.1. Por qué es útil sólo cuando la información ha de intercambiarse entre varios sujetos
   4.2. El escenario óptimo: múltiples actores en ausencia de total confianza
5. Casos prácticos de éxito y posibles implementaciones futuras
   5.1. Control de calidad y de la cadena de suministro
   5.2. Más transparencia en el sistema sanitario privado

LM2: Técnicas de cifrado

Descripción

Las tecnologías *blockchain* descansan sobre una amplia variedad de técnicas criptográficas para garantizar su funcionamiento. Los bloques sucesivos de una *blockchain* creciente se encaja mediante funciones *hash* criptográficas. Las cuentas en una *blockchain* se identifican mediante claves públicas criptográficas y las correspondientes claves privadas se usan para autorizar las transacciones. Las técnicas de cifrado son un concepto básico para la comprensión de las DLT en general y de las *blockchains* en particular.

El módulo de aprendizaje 2 presenta y describe en profundidad conceptos criptográficos centrales para la tecnología *blockchain*. Los principios básicos de la criptografía y el criptanálisis se presentan en una perspectiva general inicial. Se introduce el concepto de función *hash* y se proporcionan ejemplos de funciones *hash* y sus aplicaciones. Se tratan con detalle las técnicas criptográficas simétricas y asimétricas, con ejemplos y una sesión de laboratorio específica. Se introduce el concepto de *Zero-Knowledge Proofs* (ZKP) y se tratan aplicaciones de la criptografía en el área de la *blockchain.*

Requisitos

Este módulo no tiene requisitos previos.

Objetivos del aprendizaje

- Introducir las características fundamentales de la criptografía y sus posibles usos en *blockchain*.
- Comparar diferentes criptosistemas y su evolución.
- Describir el concepto de función *hash* y comparar un conjunto de funciones *hash* que se utilizan en sistemas basados en *blockchain*.
- Explicar los conceptos fundamentales de los sistemas criptográficos simétricos y asimétricos.
- Presentar algunas técnicas criptográficas que protegen la privacidad y las ZKP.
- Ilustrar cómo se aplican las técnicas criptográficas en los sistemas basados en *blockchain*.
- Presentar casos de uso relevantes construídos sobre la criptografía *blockchain.*

Resultados esperados del aprendizaje

- **Comprender** los conceptos fundamentales de la criptografía.
- **Examinar** cuál es el criptosistema más adecuado dependiendo del caso de uso.
- **Identificar** y **analizar** las distintas funciones *hash*.
- **Identificar** y **analizar** las aplicaciones de la criptografía simétrica y asimétrica.
- **Discutir** y **analizar** algunos métodos criptográficos que protegen la privacidad y las ZKP.
- **Identificar** y **evaluar** las aplicaciones de métodos criptográficos en los sistemas basados en *blockchain*.
- **Examinar** cómo se utilizan las técnicas de cifrado en casos de usos relevantes de *blockchain*.

Programa

1. Introducción a la criptografía
   1.1. ¿Qué es la criptografía?
   1.2. Clasificación de los criptosistemas

1.3. Principios básicos
1.4. Los principales criptosistemas clásicos y su evolución
1.5. Las condiciones de cifrado perfecto
1.6. Criptoanálisis

2. Funciones *hash*
   2.1. ¿Qué es una función *hash*?
   2.2. Tipos de funciones *hash*: MD5, SHA-x
   2.3. Laboratorio: experimentando con funciones *hash*

3. Criptografía simétrica
   3.1. Definición
   3.2. Cifrado de Vernam, de flujo y de bloques

4. Criptografía asimétrica
   4.1. Definición
   4.2. Algoritmos fundamentales de intercambio (Diffie-Hellman)
   4.3. RSA

5. Laboratorio: experimentando con cifrado simétrico y asimétrico

6. *Zero-Knowledge Proofs*

7. Aplicaciones de la criptografía *blockchain*
   7.1. Aplicación a los intercambios QR
   7.2. Gestionar direcciones Bitcoin y Ethereum
   7.3. Prácticas de teoría de bloques

8. Casos de uso: sector financiero, salud, servicios legales, defensa, administración pública, digitalización industrial, proyectos sociales, lucha contra la pobreza, gestión de la identidad individual

LM3: Mecanismos de consenso

Descripción

Uno de los principales problemas para diseñar un sistema *blockchain* es la elección del mecanismo utilizado para que los nodos de la red alcancen el consenso sobre el estado del sistema de forma descentralizada, es decir, sin recurrir a un nodo central fiable.

El módulo de aprendizaje 3 explora los mecanismos que gestionan el acuerdo entre todos los nodos que participan en un sistema *blockchain.* Trata los mecanismos de consenso más utilizados, enfatizando por igual los aspectos técnicos y de negocio de la materia.

Al inicio del módulo se presenta la necesidad de un mecanismo de consenso en una base de datos distribuída y se tratan las soluciones para sistemas autorizados. Se presenta el papel de la teoría de juegos en el diseño de los mecanismos de consenso y se proporciona una clasificación de los distintos mecanismos de consenso que se han implementado en la práctica o se han propuesto teóricamente dentro de las dos grandes categorías de mecanismos de "prueba de trabajo" (*Proof of Work,* PoW) y "prueba de participación" (*Proof of Stake,* PoS), describiendo los potenciales ataques sobre tales mecanismos. Posteriormente, se traza la correspondencia entre los diferentes mecanismos y el intercambio entre los incentivos para mantener la *blockchain* y la seguridad frente a ataques intencionados que puedan poner en peligro la integridad de la *blockchain*, con especial consideración de la posición que ocupa cada mecanismo particular respecto de su nivel de centralización o descentralización. La última parte del módulo presenta un conjunto de casos prácticos.

Los estudiantes que completen este módulo podrán reconocer las ventajas y desventajas de cualquier protocolo de consenso en el contexto de cualquier modelo de negocio particular basado en una DLT, así como sus limitaciones en cuanto a la precisión, eficiencia de costes, grado de descentralización, escalabilidad, tasa de rendimiento y sostenibilidad de la red.

Requisitos

Este módulo de aprendizaje tiene los siguientes requisitos previos:

- Diseño de bases de datos P2P (LM1)
- Técnicas de cifrado (LM2)

Objetivos del aprendizaje

- Explicar la necesidad de mecanismos de consenso en un sistema basado en *blockchain*.
- Presentar los mecanismos de consenso utilizados en sistemas de *blockchain* autorizados.
- Tratar el papel de la teoría de juegos en el diseño de un mecanismo de consenso.
- Presentar los protocolos de consenso del tipo *Proof-of-Concept* (PoX) más ampliamente utilizados en sistemas *blockchain.*
- Tratar posibles ataques sobre los protocolos de consenso distribuidos.
- Introducir y describir las estructuras de incentivos utilizadas por los protocolos de consenso distribuidos.
- Presentar los ataques sobre los protocolos de consenso relacionados con las estructuras de incentivos.
- Tratar los costes de los protocolos de consenso distribuidos más comunes.

- Tratar las propiedades de rendimiento y escalabilidad de los protocolos de consenso distribuidos más utilizados.
- Presentar soluciones a los problemas de escalabilidad basados en alternativas a los protocolos de consenso distribuidos utilizados en los sistemas *blockchain*.
- Presentar casos de uso de distintos mecanismos de consenso distribuidos en distintos sistemas *blockchain*.

Resultados esperados del aprendizaje

- **Comprender** el papel del consenso en los sistemas DLT y *blockchain*.
- **Comprender** el funcionamiento de los protocolos de consenso distribuidos tipo PoX.
- **Comprender** los posibles ataques sobre los protocolos de consenso distribuidos.
- **Comparar** costes, rendimiento, escalabilidad y seguridad entre protocolos de consenso analizando las especificaciones de su diseño.
- **Evaluar** las características deseadas de un protocolo de consenso para un modelo de negocio específico.

Programa

1. Introducción
   1.1. La necesidad de mecanismos de consenso
   1.2. *Blockchains* autorizadas: consenso mediante mecanismos de votación *Byzantine-Fault Tolerant* (BFT)
2. El papel de la teoría de juegos en el consenso
3. Protocolos *Proof-of-Concept* (PoX)
   3.1. El concepto de consenso probabilístico y sus propiedades
   3.2. Las loterías de puzles criptográficos y sus propiedades
   3.3. Principales protocolos: *Proof-of-Work* (PoW), *Proof-of-Stake* (PoS), PoS delegada, *Proof-of-Authority* (PoA).
   3.4. Una taxonomía de ataques potenciales: *Sybil, race, Finney, 51%.*
4. Incentivos
   4.1. La teoría básica: costes hundidos, problemas de agente y principal y compatibilidad en incentivos.
   4.2. Compatibilidad en incentivos en protocolos PoX: *tokens*, “botes” y cárteles de “mineros”.
   4.3. Los mercados de *tokens*.
   4.4. Las vulnerabilidades de los protocolos PoX: minería “egoísta”, retirada de bloques, botes de mineros “a la espera”, “escapadas” de los botes.
5. Costes
   5.1. La naturaleza costosa de los protocolos PoX.
   5.2. Los protocolos PoS y el problema de la “tragedia de los comunes”.
   5.3. Problemas de seguridad en los protocolos PoS: ataques *nothing-at-stake* y *grinding*.
6. Rendimiento
   6.1. Limitaciones al rendimiento de las *blockchains* no autorizadas.
   6.2. Protocolos híbridos
   6.3. Interoperabilidad de las *blockchains.*

6.4. Redes *blockchain* no lineales: el protocolo *Greedy Heaviest-Observed Sub-Tree* (GHOST)
6.5. Protocolos basados en grafos dirigidos acíclicos (*Direct Acyclic Graphs* - DAGs)

7. Ejemplos
7.1. Hyperledger Fabric (BFT)
7.2. Bitcoin (PoW)
7.3. Primecoin (PoUS)
7.4. Filecoin (UPoW)
7.5. SpaceMint (PoSP)
7.6. Bytecent (PoH)
7.7. Peercoin (PoS)
7.8. Algorand (Protocolos híbridos)
7.9. Teechain on Bitcoin (Redes laterales a la cadena)
7.10. La implementación del protocolo Casper en Ethereum (GHOST)

Co-funded by the
Erasmus+ Programme
of the European Union

LM4: Firmas digitales

Descripción

Las firmas digitales son la extensión de las firmas en papel al terreno digital, hechas posibles gracias al desarrollo de la criptografía asimétrica. Como las firmas reales, son una forma de probar la propia identidad y de certificar el origen de un mensaje.

El módulo de aprendizaje 4 describe las propiedades, los requisitos técnicos y los pre-requisitos matemáticos necesarios para implementar firmas digitales. Presenta las características genéricas de los algoritmos de firma digital y trata con detalle los algoritmos específicos que se usan habitualmente en la implementación de sistemas *blockchain*. Los algoritmos de firma digital que protegen la privacidad se tratan haciendo énfasis en su uso dentro del espacio de las criptomonedas, y se presentan los conceptos de anonimato y pseudo-anonimato de las transacciones en una *blockchain*. Se considera la seguridad de las firmas digitales y los posibles planes de ataque, y se analiza en profundidad en un laboratorio un posible vector de ataque. La última parte del módulo trata el futuro de las firmas digitales, presentado algoritmos novedosos diseñados para resistir amenazas actuales y previstas relacionadas con el advenimiento de los computadores cuánticos.

Requisitos previos

Este módulo de aprendizaje tiene los siguientes requisitos previos:

- Técnicas de cifrado (LM2)

Objetivos del aprendizaje

- Explicar las propiedades básicas que debe satisfacer un algoritmo de firma digital.
- Presentar los algoritmos de firma digital más ampliamente utilizados por los sistemas basados en *blockchain.*
- Presentar los algoritmos de firma digital que protegen la privacidad.
- Tratar las características de anonimato y pseudo-anonimato de los sistemas *blockchain*.
- Presentar los ataques y problemas de seguridad relacionados con los algoritmos de firma digital.
- Presentar los últimos desarrollos relacionados con los algoritmos de firma digital.
- Presentar los casos de uso de las firmas digitales en los sistemas basados en *blockchain*.

Resultados esperados del aprendizaje

- **Comprender** las propiedades fundamentales de los algoritmos de firma digital.
- **Comprender** los detalles de los algoritmos de firma digital más utilizados.
- **Adquirir** habilidades técnicas relacionadas con el uso de las firmas digitales.
- **Comprender** el funcionamiento de los algoritmos de firma digital que protegen la privacidad.
- **Enumerar** los posibles ataques sobre los algoritmos de firma digital utilizados habitualmente.

Programa

1. Definiciones, propiedades y requisitos de las firmas
2. Preliminares
   2.1. Curvas elípticas

2.2. Laboratorio: la librería bitcoin-core/secp256k1

3. Algoritmos de firma digital
   3.1. Introducción
   3.2. DSA
   3.3. ECDSA
   3.4. Firmas de Schnorr
   3.5. Laboratorio: implementación y análisis de firmas de Schnorr
4. Firmas anulares
   4.1. Propiedades
   4.2. El papel de las firmas anulares en la *blockchain* de Monero
   4.3. Laboratorio: implementación de firmas anulares
5. Anonimato y pseudo-anonimato en las transacciones *blockchain*
6. Seguridad y ataques
   6.1. Perspectiva general de los problemas de seguridad y los ataques
   6.2. Laboratorio: un ataque específico sobre firmas de Schnorr
7. El futuro de las firmas digitales: retículas, firmas *hash*, y firmas umbral
8. Casos de uso

LM5: Contratos inteligentes

Descripción

El término “contratos inteligentes” se utiliza con dos interpretaciones distintas:

- “Un contrato inteligente es un conjunto de código (funciones) e información (estado) que reside en una dirección específica en la *blockchain*.”
- “Un contrato inteligente (contrato) es un protocolo informático que pretende facilitar, verificar o hacer cumplir digitalmente la negociación o la ejecución de un contrato.”

El módulo de aprendizaje 5 estudia los problemas de diseño de las aplicaciones (contratos inteligentes) basadas en *blockchain* que pueden ejecutar automáticamente los términos de un contrato, concentrándose en los aspectos tanto tecnológicos como comerciales del tema.

El módulo comienza con una introducción al concepto de contrato inteligente y una descripción de su evolución histórica. Se presenta una perspectiva general de los lenguajes de programación utilizados para el desarrollo de contratos inteligentes en sistemas *blockchain* y sus entornos de ejecución, seguida de una descripción detallada de la *Ethereum Virtual Machine* y un laboratorio temático sobre el desarrollo de contratos inteligentes en la plataforma Ethereum utilizando el lenguaje de programación Solidity. Se describen con detalle los “oráculos”, una categoría especial de contratos inteligentes que se comunican con entidades fiables. Se tratan los costes de computación y los problemas de seguridad de la programación de contratos inteligentes, y se presentan las buenas prácticas para mitigar sus problemas y riesgos. Finalmente, se identifican y describen los principales problemas regulatorios y legales que presenta el uso de los contratos inteligentes como contratos.

Requisitos previos

Este módulo de aprendizaje tiene los siguientes requisitos previos:

- Mecanismos de consenso (LM3)
- Firmas digitales (LM4)

Objetivos del aprendizaje

- Definir y explicar las propiedades básicas de un contrato inteligente.
- Presentar los distintos lenguajes de programación que se utilizan para desarrollar contratos inteligentes y sus entornos de ejecución.
- Describir la *blockchain* de Ethereum y la *Ethereum Virtual Machine*.
- Explicar cómo utilizar el lenguaje Solidity para desarrollar un contrato inteligente en la *blockchain* de Ethereum.
- Presentar el concepto de “oráculos” y sus principios básicos de funcionamiento.
- Tratar los costes de computación de utilizar y ejecutar un contrato inteligente y el papel de *Gas* en la *blockchain* de Ethereum.
- Tratar los problemas de seguridad relacionados con el desarrollo y el uso de contratos inteligentes.
- Presentar los marcos regulatorios que afectan al uso de contratos inteligentes.
- Presentar los problemas legales relacionados con el uso de contratos inteligentes en un sistema basado en *blockchain*.

Resultados esperados del aprendizaje

- **Describir** los conceptos básicos de los contratos inteligentes.
- **Reconocer** los distintos lenguajes de programación de contratos inteligentes y sus entornos de ejecución.
- **Identificar** las características fundamentales de los distintos lenguajes de programación de contratos inteligentes.
- **Describir** la *blockchain* de Ethereum.
- **Explicar** cómo funciona la *Ethereum Virtual Machine*.
- **Implementar** contratos inteligentes en Ethereum utilizando Solidity.
- **Examinar** los costes de computación de utilizar un contrato inteligente en Ethereum.
- **Demostrar** los casos de uso de contratos inteligentes en múltiples dominios.
- **Comprender** las restricciones y limitaciones de la tecnología actual.
- **Identificar** los problemas relacionados con el desarrollo de contratos inteligentes.
- **Examinar** las ventajas y desventajas de utilizar un contrato inteligente.
- **Identificar** las preocupaciones sobre la seguridad, la estabilidad y el coste de un contrato inteligente.
- **Evaluar** si una solución basada en contratos inteligentes es adecuada para un problema específico.
- **Evaluar** cómo y cuando aplicar contratos inteligentes en situaciones reales.
- **Implementar** contratos inteligentes en situaciones reales.

Programa

1. Contratos inteligentes
   1.1. Historia, definición, casos de uso sencillos
   1.2. Introducción a los “contratos inteligentes” en *blockchain*
   1.3. El ciclo vital de un contrato inteligente (teoría)
2. Lenguajes de contratos inteligentes
   2.1. Alusión a los distintos entornos *blockchain* y explicación de sus características fundamentales: Ethereum, Hyperledger Fabric
   2.2. Evolución de los lenguajes de escritura de *blockchain*
   2.3. Perspectiva general de las características fundamentales de distintos lenguajes de programación de alto nivel para diferentes entornos *blockchain*
   2.4. Introducción a los entornos de ejecución de contratos inteligentes
   2.5. Análisis de la *Ethereum Virtual Machine* (EVM): Principales características, lenguajes de programación, límites
3. Laboratorio: Desarrollo en Ethereum con el lenguaje Solidity
   3.1. Tipos de datos básicos e instrucciones, tipos de datos específicos, estructuras de datos, modificadores de acceso y aplicaciones.
   3.2. Técnicas de diseño
   3.3. El ciclo de vida de un contrato inteligente en la práctica: compilación, utilización, interacción y destrucción
4. Oráculos
   4.1. Introducción a los oráculos
   4.2. Desarrollo de contratos que se comunican con entidades fiables en el mundo real

5. Costes de computación
   5.1. El papel de *gas* en Ethereum
   5.2. Análisis del coste de las transacciones
   5.3. Análisis del coste de un contrato inteligente
6. Seguridad
   6.1. Problemas: *hacks* conocidos y problemas
   6.2. Soluciones: librerías de seguridad, estándares abiertos conocidos, buenas prácticas, herramientas de análisis
   6.3. Problemas fundamentales y estrategias de solución
7. Marcos regulatorios
   7.1. Perspectiva general de las regulaciones existentes sobre contratos inteligentes
   7.2. Análisis de las leyes referentes a los contratos inteligentes
8. Cuestiones legales
   8.1. Clarificar las cuestiones legales referentes a los contratos inteligentes
   8.2. Aspectos políticos y ambientales

LM6: Privacidad y derechos de propiedad

Descripción

La informática no opera en un vacío, sino que afecta a la sociedad y es afectada por ella. Además, en la mayoría de los casos la tecnología va por delante de la sociedad y su legislación, que necesitan ponerse al día y adaptarse a la nueva situación definida por la tecnología. Sin embargo, en casos excepcionales, la tecnología sale en ayuda de la legislación y la sociedad y permite que determinadas operaciones se realicen de forma más rápida y transparente de lo que permiten las prácticas actuales.

El módulo de aprendizaje 6 trata de cómo la tecnología *blockchain* puede ayudar a la legislación sobre los derechos de propiedad tangible e intangible y describe problemas relacionados con la privacidad en *blockchain*. Se presenta la legislación europea sobre los derechos de propiedad y las licencias y cómo las tencologías *blockchain* podrían ayudar a diseñar un sistema de remuneración justo. A continuación se trata el Reglamento General de Protección de Datos (RGPD) y problemas relacionados con la privacidad, junto con las implicaciones para los derechos garantizados bajo el RGPD (como el "derecho al olvido") relacionadas con la inmutabilidad de la *blockchain.* Finalmente, se presentan las tecnologías que refuerzan la privacidad de los sistemas basados en *blockchain* y se tratan en detalle los problemas relacionados con ellas.

Requisitos previos

Este módulo de aprendizaje tiene los siguientes requisitos previos:

- Contratos inteligentes (LM5)

Objetivos del aprendizaje

- Presentar el marco legislativo europeo actual en relación con los derechos de propiedad.
- Describir los tipos de licencias de *software* existentes.
- Explicar las leyes de *copyright* internacionales.
- Tratar la coordinación de licencias y el papel de los registros.
- Tratar problemas relacionados con los derechos de propiedad que surgen cuando se utilizan DLTs.
- Presentar el RGPD europeo y sus implicaciones para la privacidad y la libertad de información.
- Tratar problemas relacionados con el RGPD que surgen cuando se utilizan DLTs.
- Presentar un conjunto de técnicas de cifrado que protegen la privacidad.
- Tratar problemas relacionados con la privacidad que surgen en sistemas basados en DLT.

Resultados esperados del aprendizaje

- **Comprender** el RGPD y sus implicaciones para las tecnologías *blockchain*.
- **Comprender** cómo evitar conflictos legales al utilizar la tecnología *blockchain*.
- **Describir** los derechos de propiedad que puden protegerse utilizando *blockchain*.
- **Comprender** cómo los individuos pueden mantener el control sobre sus datos personales gracias a la tecnología *blockchain.*
- **Describir** cómo los inversores pueden valorar las empresas relacionadas con *blockchain*.
- **Enumerar** el papel de los derechos de propiedad intelectual para fomentar la innovación y la creatividad y cómo la *blockchain* puede adaptarse/facilitar los derechos de propiedad intelectual.

- **Comprender** cómo pueden protegerse los derechos de propiedad utilizando la tecnología *blockchain.*
- **Revisar** los factores de seguridad y privacidad en el almacenamiento integrado.

Programa

1. Derechos de propiedad
   1.1. La legislación sobre derechos de propiedad intelectual (*Copyright, Designs and Patents Act* – CPDA, 1988)
   1.2. Qué es una licencia de *software*
   1.3. Tipos de licencias
   1.4. Derecho internacional sobre *copyright*
   1.5. ¿*Tokens* como licencia?
   1.6. Pedidos privados
   1.7. Fragmentación
   1.8. Coordinación de licencias
   1.9. Registros
   1.10. Formalidades
   1.11. Las obras "huérfanas" y el dominio público
   1.12. Información sobre la gestión de derechos
   1.13. La remuneración justa
2. Problemas de las DLT relacionados con los derechos de propiedad
3. El RGDP – Los problemas de privacidad y libertad de información
4. Problemas de las DLT relacionados con el RGDP
5. Técnicas de cifrado aplicadas a las privacidad
   5.1. Funciones *hash* "camaleónicas"
   5.2. Direcciones indetectables
   5.3. Transacciones confidenciales mediante firmas anulares
   5.4. Implementando privacidad a través de ZKP
   5.5. Contratos inteligentes privados – Enigma
   5.6. Almacenamiento *off-chain*
6. Los problemas de privacidad de las DLT

LM7: Aplicaciones descentralizadas basadas en *blockchain*

Descripción

Las aplicaciones descentralizadas son diferentes a sus alternativas centralizadas, puesto que operan sobre una red P2P. La necesidad de que las partes de una transacción se comuniquen sin necesidad de una autoridad central es un tema habitual de discusión y evaluación entre los entusiastas de la tecnología. Estas aplicaciones descentralizadas, o dApps, presentan el potencial de alterar diversos sectores, que suelen presentarse ante la audiencia como casos de uso, por ejemplo las finanzas, la academia, las cadenas de aprovisionamiento, el sector energético, y otros.

El módulo de aprendizaje 7 analiza las dApps en todos sus aspectos y está dirigido tanto a audiencias técnicas como no técnicas, manteniendo siempre el interés por el tema. El principal objetivo del módulo es el de permitir a los participantes evaluar qué sectores están preparados para adoptar la tecnología *blockchain* y hasta que punto lo están. La descentralización y la desintermediación son conceptos novedosos y difíciles de comprender por completo. Deben considerarse muchos elementos, como los grados de seguridad, privacidad e interoperabilidad. Cada red DLT satisface estos elementos en distinta medida. Evaluar las buenas prácticas y las limitaciones potenciales de esta tecnología es de crucial importancia para los creadores de contenido. La estructura básica y los principales patrones de diseño de dApps se presentan como una introducción a los elementos esenciales del desarrollo de dApps. Los casos de uso de dApps avanzadas en diversos sectores se presentan acompañados de su relación con otras tecnologías perturbadoras dentro del marco de la 4ª Revolución Industrial.

Requisitos previos

Este módulo de aprendizaje tiene los siguientes requisitos previos:

- Contratos inteligentes (LM5)

Objetivos del aprendizaje

- Presentar una comparación de las condiciones bajo las que pueden utilizarse los modelos centralizados tradicionales y las dApps.
- Asociar las características fundamentales de las dApps con las propiedades fundamentales de las *blockchains.*
- Explicar el significado de requisitos funcionales y no funcionales en el contexto de las dApps.
- Presentar una comparación entre distintas blockchains como candidatas para el desarrollo de dApps.
- Ilustrar cómo fluye la información en las dApps a nivel arquitectónico.
- Presentar el conjunto tecnológico de las dApps.
- Presentar varios casos de uso indicativos construídos alrededor de dApps.
- Explicar las posibles sinergias de las dApps con otras tecnologías emergentes.
- Tratar las posibles implicaciones legales de las dApps.

Resultados esperados del aprendizaje

- **Evaluar** si se necesita una dApp en lugar del modelo centralizado tradicional.
- **Analizar** las características fundamentales de las dApps con las propiedades fundamentales de las *blockchains*.

- **Identificar** y **analizar** los requisitos funcionales y no funcionales de las dApps.
- **Evaluar** la idoneidad de distintas *blockchains* para las dApps.
- **Diseñar** las arquitecturas de flujos de información para las dApps.
- **Identificar** y analizar las principales capas tecnológicas de las dApps.
- **Examinar** cómo se utilizan las dApps en casos de uso específicos.
- **Relacionar** las dApps con otras tecnologías emergentes.
- **Identificar** cualquier requisito que pueda plantear problemas legales.

Programa

1. Anatomía de alto nivel de una dApp
   1.1. Perspectiva general del conjunto de aplicaciones *blockchain*
   1.2. Ejemplos *backend*
   1.3. Ejemplos *frontend*
2. Pautas de diseño de dApps
   2.1. Pautas de interacción con el mundo exterior
   2.2. Pautas de gestión de dato
   2.3. Pautas de seguridad
   2.4. Pautas estructurales de contrato
3. Desarrollo básico de dApps
   3.1. Programación de *blockchains* públicas
   3.2. Programación de *blockchains* privadas/autorizadas
   3.3. El ciclo de vida de las dApps
4. Casos de uso de dApps avanzadas
   4.1. Mercados cambiarios descentralizados
   4.2. Mercados de información descentralizados
   4.3. Certificados verificables en una *blockchain* e identidades auto-soberanas
   4.4. Temas emergentes en el marco (amplio) de las dApps
5. De las dApps a la 4ª revolución industrial
   5.1. La relación entre la “internet de las cosas”, la inteligencia artificial y las tecnologías *blockchain*

LM8: Organizaciones autónomas descentralizadas

Descripción

Las organizaciones autónomas descentralizadas (*Decentralized Autonomous Organization* - DAO) son organizaciones autónomas que pueden tomar decisiones descentralizadas utilizando una determinada tecnología, como por ejemplo una tecnología *blockchain*, una tecnología basada en grafos dirigidos acíclicos (*Directed Acyclic Graph* – DAG), el algoritmo *Hashgraph*, etc. Una DAO suele ser una organización que funciona a través de protocolos codificados como diversos tipos de programas informáticos llamados contratos inteligentes.

En ocasiones se hace referencia a las DAOs como "corporaciones autónomas descentralizadas" (*Decentralized Autonomous Corporation* - DAC). Sus transacciones financieras y sus registros programáticos de los protocolos se guardan en *blockchains* o tecnologías similares. Aunque estos tipos de organizaciones son similares a cualquier otra del mundo real, en el mundo digital sus reglas (es decir, las reglas de una compañía) no se pueden hacer cumplir digitalmente. Son digitales y están ahí por suy propia naturaleza. Las DAO son como una democracia criptográfica para una organización, donde cada participante puede votar para añadir nuevos protocolos, alterar los existentes o incluir y excluir miembros, entre otros tipos de derechos.

El módulo de aprendizaje 8 trata de las principales características de las DAO, sus ventajas y sus inconvenientes. Se prestará una atención especial a las implicaciones legales, culturales y políticas del uso de este paradigma perturbador. Se analiza en detalle un estudio de caso de una DAO y se explicará finalmente cómo implementar DAO en la infraestructura Ethereum a través de una sesión de laboratorio específica.

Requisitos previos

Este módulo de aprendizaje tiene los siguientes requisitos previos:

- Contratos inteligentes (LM5)
- Privacidad y derechos de propiedad (LM6)

Objetivos del aprendizaje

- Introducir el concepto de DAO como una extensión de una dApp.
- Presentar la estructura y los mecanismos de gobernanza dentro de una DAO.
- Tratar las ventajas y desventajas de utilizar una DAO para gestionar una organización.
- Presentar los problemas de seguridad y responsabilidad legal, así como los riesgos de las DAO.
- Tratar las implicaciones culturales y políticas de las DAO.
- Analizar en profundidad un caso de uso específico de DAO.
- Presentar posible desarrollos futuros de las DAO.
- Demostrar cómo implementar una DAO en la *blockchain* de Ethereum utilizando Solidity.

Resultados esperados del aprendizaje

- **Comprender** el concepto básico de DAO.
- **Comprender** las ventajas y deventajas de utilizar DAO.
- **Enumerar** los riesgos legales y de seguridad de las DAO.

- **Describir** los casos de estudio más importantes que utilizan DAO.
- **Implementar** una DAO en Solidity.

Programa

1. Introducción a las organizaciones autónomas descentralizadas (*Decentralized Autonomous Organization* (DAO)
   1.1. Definición de DAO
   1.2. De las dApp a las DAO
   1.3. Estructura de las DAO
   1.4. La democracia en las DAO
2. Ventajas y desventajas
   2.1. Ventajas de las DAO
   2.2. Desventajas de las DAO
   2.3. Los retos de las DAO
   2.4. La efectividad de las DAO
3. La seguridad, la responsabilidad legal y los riesgos
   3.1. La seguridad de las DAO
   3.2. La responsabilidad legal de las DAO
   3.3. Riegos relacionados con las DAO
4. Las implicaciones culturales y políticas
   4.1. Las diferencias e implicaciones culturales de las DAO
   4.2. Los sistemas políticos y las implementaciones de las DAO
5. Un caso de estudio de DAO
   5.1. Explorando un caso de DAO
   5.2. Lecciones extraídas del caso
6. El futuro de las DAO
7. Laboratorio: Implementar una DAO en Solidity