Una introducción al Ecosistema Blockchain Para desarrolladores

Juan Antonio Lleó – BlockMAD
Codemotion 2018

INTRODUCCION: OBJETIVOS DEL WEBINAR

- Ofrecer un panorama del ecosistema blockchain, sobre todo fijar algunos conceptos y dar pistas que sean útiles para todos y principalmente aquellos que tengan un perfil técnico, sobre todo desarrolladores.

- Conviene tener en cuenta que se trata de un tema muy amplio y cuyo conocimiento en profunidad, incluso en ámbitos concretos, requiere un enorme esfuerzo y sobre todo tiempo.

- Se van a ver varios ejemplos, enlaces, herramientas web, etc.

INTRODUCCION: EL ECOSISTEMA BLOCKCHAIN

- Conviene recalcar la importancia del Software Libre en este proyecto. La gran mayoría de los desarrollos que tienen que ver con el blockchain hacen uso de programas de código abierto, en mayor o menor medida y cualquiera puede basarse en ellos para mejorar el código o desarrollar su propia solución.
- Hay un déficit enorme de desarrolladores en el ámbito del blockchain. Se encuentra aún en sus estados iniciales y es tremendamente cambiante.
- Una recomendación es que se parta de los conocimientos que ya se tienen y ver, en función de estos, en que ámbitos de desarrollo se puede aportar con mayor facilidad:
  - Por ejemplo, si se disponen de conocimientos en C/C++, Python, Java o de desarrollo web, o de sistemas, encriptación, ciberseguridad, etc. Lo mejor es partir de ello. Para cada caso hay distintas oportunidades.

INTRODUCCION: ¿POR QUÉ BLOCKCHAIN?

- El concepto y la primera implantación de Blockchain nace como parte de las necesidades tecnológicas para el desarrollo de la criptomoneda Bitcoin. Blockchain supone la combinación de tecnologías existentes, con el objetivo de intercambio electrónico de valor directamente, entre iguales.
- Bitcoin muy pronto va a hacer su décimo aniversario y aún se mantiene sin muchos cambios con respecto al proyecto inicial, aunque haya habido muchos otros proyectos que se basan en ella o en algunas de sus ideas, lo que implica que goza de cierto éxito.
- Aunque esto no quiere decir que vaya a durar muchos años más y que no vaya a ser sustituida, total o parcialmente por una o más tecnologías que consigan implantarse masivamente.

INTRODUCCION: ¿ES BLOCKCHAIN LA SOLUCION?

- Conviene analizar cada caso en concreto y ver qué es lo que aporta blockchain y a qué se renuncia, frente a otras tecnologías.
- Tanto la inmutabilidad como su aspecto público no siempre es deseable para cualquier proyecto, por ejemplo, puede haber conflicto con el RGPD.

BLOCKCHAIN COMO NEGOCIO

Aunque no es el objetivo principal del webinar, si que conviene tratar, aunque sea muy por encima los aspectos del blockchain y las criptomonedas como negocio, pues es algo en lo que se suele poner el foco y la verdad es que existe un enorme desconocimiento sobre ello.

- **RESERVA DE VALOR:**
  Las criptomonedas, tanto Bitcoin, como el resto de Altcoins, pueden verse como una manera de almacenar valor. Se puede apostar a que se van a revalorizar, pero no existe una garantía ni de que eso vaya a ocurrir, ni en que plazos, así como que en algún momento pierdan todo su valor. Una recomendación sería diversificar, con la esperanza de que algunas de ellas se revaloricen lo suficiente como para que compense la inversión total.

BLOCKCHAIN COMO NEGOCIO

- **MINADO Y STAKING:**
  El minado es el método por el cual, mediante la llamada prueba de trabajo, se crean los nuevos bloques y quien lo consigue, obtiene una suculenta recompensa. Aunque hace años, practicamente cualquiera tenía la capacidad suficiente con sus ordenadores para conseguirlo, en la actualidad es muy difícil competir con grupos y empresas dedicadas a ello, con fuertes inversiones y equipos de personas que lo mantienen en perfecto estado. Una opción sería la de montar uno propio o incorporarse a un equipo de minado (pool) que comparta las ganancias obtenidas en conjunto por todos los participantes que aporten potencia de cálculo.
  Existe otro método, con un algoritmo de consenso distinto, en este caso la prueba de pertenencia (PoS, proof of stake) en el que se consiguen recompensas simplemente si se mantienen ciertas cantidades de moneda un tiempo concreto.

BLOCKCHAIN COMO NEGOCIO

- **ESPECULACION Y TRADING:**
  Las mismas técnicas que usan los gestores financieros (traders) pueden aplicarse, prácticamente sin cambios, a las criptomonedas. Pero las constantes fluctuaciones de sus valores hace que sea muy arriesgado, sobre todo si no se cuentan con los conocimientos adecuados, además de una dedicación exhaustiva.
- **ICO/ITO:** Tanto las ofertas iniciales de monedas ICO (o tokens ITO, en ese caso) son una manera interesante para muchos proyectos de conseguir financiación de inversores en cualquier parte del mundo, en relativamente poco tiempo. A pesar de que se trata de un modelo en mi opinión muy válido, ha habido por un lado gran cantidad de ejemplos en los que ya sea por inconsciencia y/o falta de experiencia en el desarrollo, o sencillamente por una intencionalidad de defraudar, en los cuales no se han cumplido las espectativas que prometían.

BLOCKCHAIN COMO NEGOCIO

- **MASTERNODOS:**
  - Otra opción que está adquiriendo cierta importancia como alternativa de financiación para proyectos en los cuales se necesiten criptomonedas o tokens propios es la red de masternodos.
  - Asociado al PoS, los poseedores de un masternodo válido reciben recompensas de un modo aleatorio, pero equitativo, cada vez que resuelven el bloque que les asigna el sistema.
  - Para disponer de un masternodo hay que comprar una cierta cantidad de la criptomoneda correspondiente al masternodo, por ejemplo 1000 unidades y mantenerlas reservadas, sin tocar.

RECOMENDACIONES Y PRECAUCIONES

- **MUCHO SCAM Y PROYECTOS POCO CONSISTENTES:**
  Conviene ser tremendamente cauteloso a la hora de seleccionar un proyecto en el cual invertir y siempre pensando en la posibilidad de que se puede perder la totalidad de dicha inversión. Es por tanto imprescindible tratar de informarse por diversos medios, comprender lo que se está haciendo, contrastar la información en foros, etc. Es bastante habitual, por desgracia, que bastantes sitios sean simplemente falsos y que inviertir en ellos sea una forma de perder el dinero.
- **PENDIENTE DE LEGISLAR:**
  Por otro lado también hay que tener en cuenta que, en muchos casos aún no existe legislación sobre gran cantida de estos temas y, aunque la prohibición absoluta sea inviable, si que es cierto que una legislación restrictiva puede dificultar las cosas.

BLOCKCHAIN: DISCIPLINAS CERCANAS

- **CRIPTOGRAFIA**
- **LENGUAJES DE PROGRAMACION**
- **CIBERSEGURIDAD**
- **INTEGRACION:**
  - **Aplicaciones**
  - **Web y web apps**
  - **App para móviles**

INTRODUCCION: RECURSOS BASICOS

Existen infinidad de sitios que ofrecen recursos de todo tipo relacionados con el ecosistema blockchain. Un buen punto de partida puede ser:

- **Wikipedia**
- **Sitios oficiales de los proyectos**
- **BIT2ME:** https://bit2me.com/
  - Bit2Me Academy:
  - https://academy.bit2me.com
- **Comunidad:** Blockchain España, Criptoinvest, Blockmad...
- **Cursos gratuitos**
- **Meetups, grupos de Telegram y otras mensajerías**
- **Articulos:** Por ejemplo: https://medium.com/the-mission/the-top-10-cryptocurrency-resources-for-non-technical-people-3efb42eb7be6

INTRODUCCION: EXPLORADORES Y LIBRERÍAS

- **QUE SON Y PARA QUE SIRVEN:**
  - Los exploradores de blockchain permiten analizar las cadenas de bloques desde un navegador web.
  - Estos servicios se ofrecen gratuitamente, aunque con limitaciones y están disponibles para distintas criptomonedas.
  - Los sitios que los brindan suelen ser los del propio proyecto de la criptomoneda, o empresas interesadas en ello por distintos motivos, por ejemplo: casas de cambio (exchanges), empresas de desarrollo, etc
  - Uno de los más conocidos es el de Blockchain.com: https://www.blockchain.com/explorer

INTRODUCCION: WALLETS (CARTERAS)

- Para poder conservar las criptomonedas se necesita disponer de una cartera (wallet).
- También se ocupan de facilitar los pagos y el seguimiento de nuestra actividad.
- Hay de distintos tipos y cada una de ellos tiene sus propias ventajas e inconvenientes.

- **Los tipos principales son:**

- APLICACIONES: web, para móviles, portátiles, sobremesa, etc
- HARDWARE: dispositivos que se conectan a un ordenador y que disponen de la información de la cartera, convenientemente protegida
- EN PAPEL: Aunque pueda sorprender, el escribir la clave privada en un papel (y protegerlo adecuadamente) es una opción válida y a veces recomendable.

  Hay que tener en cuenta que si perdemos o alguien nos roba o conoce nuestra clave privada podemos perder parte o todo el valor asociado a la misma.

- EJEMPLO: Escoje tu monedero Bitcoin: https://bitcoin.org/es/elige-tu-monedero

INTRODUCCION: EXCHANGES

EXCHANGES:

- Los exchanges (casas de cambio) son empresas en las cuales podemos tanto convertir dinero Fiat en criptomonedas o viceversa, como cambiar una criptomoneda por otra.
- Pueden ser sitios web o disponer de locales, ya sea propios o asociados a su red.
- Dentro de los más usados y reconocidos destacan:

- Y aparte hay muchos otros que tratan de abrirse camino, aportando distintas propuestas que los diferencian, por ejemplo, Crex24, que ofrece faucets (grifos de monedas gratis), simplemente abriendo una cuenta con ellos y pulsando un botón cada cierto tiempo.
  - **CREX24:** https://crex24.com

ALGORITMOS DE CONSENSO Y MINADO

Algoritmos de consenso y minado:

- **Prueba de trabajo (Proof of Work)**
  - Mineria
    - Equipos hardware de minado:
      - CPU
      - GPU + rigs
      - Asic
      - USB

- **Minado en grupo:**
  - Nicehash: https://www.nicehash.com/

El BLOCKCHAIN DE BITCOIN

- **Sitio oficial:** https://bitcoin.org/es/
- **White Paper:** https://bitcoin.org/bitcoin.pdf
- **Github:** https://github.com/bitcoin/bitcoin
- **Otros Recursos:**
  - **Libro De Satoshi (en español):** http://libroblockchain.com/satoshi/

ALTCOINS: ALTERNATIVAS A BITCOIN

- A las criptomonedas alternativas desarrolladas con posterioridad a Bitcoin y basadas en mayor o menor medida en ese proyecto, se las suele conocer como Altcoins.

- La principal es Ethereum, aunque existen muchísimas más.

- Para hacernos una idea de las principales, podemos visitar el sitio Coin Market Cap:
  - https://coinmarketcap.com/

ETHEREUM

La propia Ethereum Foundation ofrece muchos recursos de varios tipos, algunos relacionados con el desarrollo.

- **Herramientas de linea de comandos:** https://www.ethereum.org/cli
- Tambien te permite crear una red de test privada (private test net) para probar a hacer transacciones o contratos inteligentes.
- **Ejemplo de creacion de contrato inteligente con la linea de comandos:** https://www.ethereum.org/greeter
- **Incluso Crear Un Mínimo Token Viable:** https://www.ethereum.org/token
- **Exploradores Ethereum:** https://etherscan.io/
- **Ethereum Developer APIs:** (gratis, limitada a 5 pet./sg) https://etherscan.io/apis
  - Permite hacer consultas mediante links, por ejemplo, Para conseguir el balance de una única dirección (Get Ether Balance for a single Address): **https://api.etherscan.io/api?module=account&action=balance&address=0xddbd2b932c763ba5b1b7ae3b362eac3e8d40121a&tag=latest&apikey=YourApiKeyToken**

- **Proyectos que permiten acceder al sitio de Etherscan:** https://etherscan.io/apis#misc
  - **Libreria con Node JS:** https://github.com/sebs/etherscan-api
  - **Libreria con Python:** https://github.com/corpetty/py-etherscan-api
  - **Estadisticas de Ethereum:** https://ethstats.net/

CONTRATOS INTELIGENTES

Los contratos inteligentes, o Smart Contracts permiten ejecutar automáticamente una acción siempre que se cumplan unas condiciones acordadas entre dos o más partes.

Nacen en el sistema Ethereum y se suelen programar en el lenguaje solidity, aunque no es el único y se ejecutan en la EVM: la máquina virtual de ethereum:

- **Precauciones de los contratos:**
  - Implica conocimientos combinados en desarrollo y cuestiones legales
  - Una vez lanzados no se pueden alterar, aunque si renovarlos con un nuevo acuerdo

DAPPS

- **DAPPS:** Las DAPPS son herramientas que permiten la interacción directa entre los usuarios finales y los proveedores. Ethereum lo facilita con la posibilidad de los contratos inteligentes,

  - **Herramientas para desarrollo de contratos y transacciones:**
    http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html#dapps

- **Introducción al desarrollo con Ethereum:**
  https://dappsforbeginners.wordpress.com/tutorials/introduction-to-development-on-ethereum/

BLOCKCHAIN PERMISIONADO E HIBRIDO

- **HYPERLEDGER:**

  Una de las opciones que cuenta con un mayor apoyo en cuanto a grandes empresas es el proyecto Hyperledger.
  Auspiciado por la Linux Foundation provee un sistema para la creación de blockchain permisionados e híbridos.

- **Web oficial del proyecto:**
  https://www.hyperledger.org/

- **Curso de introducción**
  https://www.edx.org/es/course/blockchain-for-business-an-introduction-to-hyperledger-technologies

ALTERNATIVAS A BLOCKCHAIN

- **ALTERNATIVAS A BLOCKCHAIN:**
  - **HEDERA HASHGRAPH:**
    Esta plataforma ofrece una nueva forma de consenso distribuido que no depende de costosas pruebas de trabajo.

    https://www.hedera.com/platform

    https://www.hedera.com/whitepaper

CONCLUSIONES

CONCLUSIONES:

- **Una gran oportunidad para los desarrolladores**
- **Magnífico complemento a los conocimientos que ya se tienen**
- **Mucha demanda de desarrollo, la mayoría no se satisface**
- **Muchas opciones distintas en cuanto a desarrollo**
- **Proyectos globales**

MATERIALES:

MATERIALES:

http://blockmad.lleo.net/

INTRODUCCION: ¿Qué es Blockchain?

¡Muchas Gracias!

Juan Antonio Lleó:
juan.a.lleo@gmail.com

BlockMAD
Grupo de Blockchain orientado al desarrollo:
https://www.meetup.com/es-ES/BlockMAD/

INTRODUCCION: ¿Qué es Blockchain?

¡Muchas Gracias!

Juan Antonio Lleó:
juan.a.lleo@gmail.com

BlockMAD
Grupo de Blockchain orientado al desarrollo:
https://www.meetup.com/es-ES/BlockMAD/

FIN

FIN

ANEXO: ¿Qué es Blockchain?

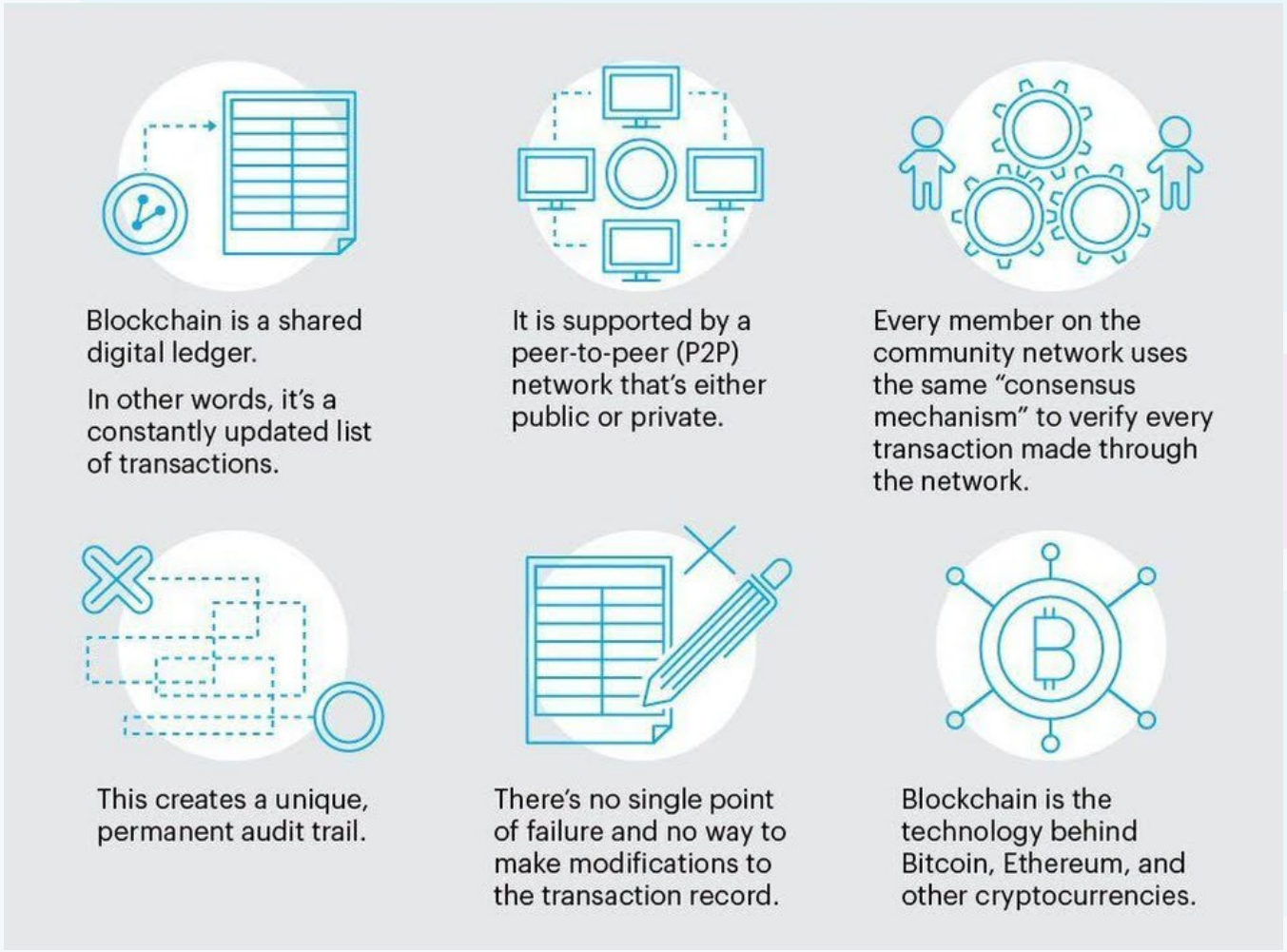
ANEXO: ¿Qué es Blockchain?

INTRODUCCION: ¿Qué es Blockchain?

- Puede traducirse literalmente como “Cadena de Bloques”
- Basicamente, es una base de datos, distribuida, inmutable
- Supone una nueva revolución tecnológica
- La aplicación más conocida es el Bitcoin y las criptomonedas
- La Red Ethereum ofrece, además, contratos inteligentes
- DAO: Organizaciones Autónomas Descentralizadas
- Una forma de financiación de startups y proyectos:
  - ICO’s e ITO’s (Hemos vivido una burbuja, actualmente)

INTRODUCCION: ¿Qué es Blockchain?

Es una base de datos distribuida, pero con ciertas características:



INTRODUCCION: ¿Qué es Blockchain?

- Blockchain es una solución tecnológica que nace como respuesta a las necesidades del proyecto Bitcoin.
  Pero esta tecnología transciende ampliamente su uso inicial.

- La verdadera identidad de su creador o creadores, que se presentan bajo el nombre de Satoshi Nakamoto, permanece aún desconocida y suele asociarse a entornos cercanos al cypherpunk.

- A pesar de encontrarse en una etapa incipiente de su desarrollo y posibilidades, se están creando una gran multitud de proyectos y propuestas de muy diverso tipo.

  - Un blockchain puede ser público, privado o híbrido.

INTRODUCCION: ¿Qué es Blockchain?

Supone una auténtica revolución en muchos aspectos de nuestra actual sociedad, por ejemplo:

- Economía: moneda, medios de pago, inmediatez y universalidad de las transacciones
- Internet del valor
- Transparencia, anonimato
- Marketing personalizado y recompensable

Incluso TODO podría estar en cuestión y necesitara renovarse: aspectos tales como la propia organización de la sociedad, gobierno, impuestos, empresas, trabajo, etc.

INTRODUCCION: ¿Qué es Blockchain?

Actualmente, sobre todo Bitcoin está prácticamente a diario en las noticias, con variaciones de precio exponenciales.

Pero hay diversos factores que pueden hacer que esa valoración cambie:

- Legislaciones en contra
- Cuestiones tecnológicas: depende de la tecnología internet
- Sustitución por una opción mejor
- Existe una enorme carencia de desarrolladores de estas tecnologías.

INTRODUCCION: ¿Qué es Blockchain?

Inversión en:

- Compra de criptodivisas o trading
- ICO's, ITO's y Masternodos
- Minado: en la nube, con equipos propios, grupos (pool) de minado, monedas menos conocidas.
- **Peligros:**
- Volatilidad, sitios falsos, hackers, pérdida de los datos de la criptodivisa, obsolescencia o ruina de los proyectos.
- Hay que ser muy cuidadoso, puede ser muy arriesgado.
- Conviene pensar en una especie de lotería mas que como algo seguro.

INTRODUCCION: ¿Qué es Blockchain?

Blockchain, previsiones:

- La tecnología Blockchain puede suponer que cambien muchas de las actividades tal cual las conocemos y no sólo en cuanto a las tecnológicas: buscadores, redes sociales, sistemas de pago...
- ...Sino también en el mundo físico, por ejemplo, con lo que se conoce como tokenización de activos.
- Como suele ocurrir con cualquier tecnología nueva, es imposible prever todas las aplicaciones e implicaciones que pueden tener en un futuro.

INTRODUCCION: ¿Qué es Blockchain?

EJEMPLOS DATAMAD 2017

Pruebas de concepto: Blockchain sencilla, con Python

Blockchain sencilla, con Python:

Teniendo como base una implementación de un sistema sencillo de blockchain sobre Python, que simula una serie de transacciones aleatorias entre dos (o más) individuos, se trató de adaptarlo al sistema de Cita Previa, del Servicio de Atención al Ciudadano del Ayuntamiento: **Linea Madrid**.

La Prueba de Concepto (POC) presentada se implementó en un Jupyter Notebook.

Se partió del dataset original, publicado en la web de datos abiertos del Ayuntamiento.

Pruebas de concepto: Blockchain avanzada, con Python

Blockchain avanzada, con Python:

- Consta de dos programas:
  - PROGRAMA PRINCIPAL: taller.py
  - LIBRERIA, genera cada bloque y los encadena: blockchain.py
- Permite simular una cadena de bloques en red
- También implementa un sistema de consenso, mediante el método de Prueba de Trabajo, similar al que usa Bitcoin

Pruebas de concepto: Blockchain avanzada con Haskell

Blockchain avanzada con Haskell:

Basado en el proyecto de implementación de una criptomoneda en Haskell, Haskoin:

Rolling your Own Blockchain in Haskell - Michael Burge

http://www.michaelburge.us/2017/08/17/rolling-your-own-blockchain.html

La adaptación, a cargo de Lorenzo López, incluyó una modificación del código, para facilitar su comprensión.

Pruebas de concepto: Sistema de Votación con Ethereum

Sistema de votación mediante contratos inteligentes con Ethereum:

La POC del sistema de votación con Ethereum se presentó como un documento en formato pdf, con los detalles de la implementación, a cargo de Daniel Mery:

Una introducción al blockchain de Ethereum;
- DocBlockchain-Intro01.pdf

Y la POC, paso a paso:
- POC_Ethereum.pdf

AGRADECIMIENTOS:

¡Muchas Gracias!

Juan Antonio Lleó:
juan.a.lleo@gmail.com

Grupo de Data Science
Haskell MAD - Madrid Haskell Users Group:
https://www.meetup.com/es-ES/Haskell-MAD/

FIN

FIN