Módulo 4: Describiendo Redes Blockchain

Las redes públicas no lo son todo

‹/codecrypto.academy›

Tabla de contenidos

‹/codecrypto.academy›

01

Section A

Ethereum, Enterprise Ethereum Alliance & Quorum

codecrypto.academy

Ethereum, Enterprise Ethereum Alliance & Quorum

- Ethereum es un proyecto lanzado en 2014 con una primera entrada en producción durante 2015. Luego, el proyecto evolucionó mucho y una parte importante de su código fue reutilizada por empresas emergentes y otros proyectos.

- En 2016 sufrió el famoso hackeo The DAO, mediante el cual se vieron comprometidos 150M$, dando lugar al conocido Hardfork ETH & ETC

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

- La nueva rama creada (ETH) ha sido explotada posteriormente en tres categorías:
  - **Ethereum**: blockchain publica.
  - **Enterprise Ethereum Alliance**: blockchain permisionada de la blockchain con muchas mejoras específicas para empresas.
  - **Quorum**: forma permisionada empaquetada por JPMorgan de la versión original de Ethereum.

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

- Ethereum es ante todo un protocolo, una criptomoneda y una infraestructura. Este protocolo es una innovación que permite representar todo tipo de bienes de manera digital y descentralizada.

- Uno de los usos más extendidos es la creación de ICOS para la creación de nuevas redes Blockchain. (El padre le ofrece al hijo la posibilidad de nacer)

/codecrypto.academy

Ethereum, Enterprise Ethereum Alliance & Quorum

Ventaja: Permite al desarrollador la posibilidad de programar lógica de aplicaciones en modo serverless → Es decir, el programador no se ocupa de la infraestructura, solo del desarrollo.

Inconveniente: Como developer, no es fácil estimar la cantidad de tokens que la ejecución de tu software costará. Lo bueno, es que a día de hoy ya existen soluciones en la nube para prever dichos costes antes de que la operación se ejecute en mainnet.

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

Ventaja: El sistema incluye un modelo de implementación y de uso de código muy sencillo, por ejemplo, a la hora de descargar el módulo Parity (cliente Ethereum)

Inconveniente: Para que funcione todo correctamente, el código debe ser desarrollado de una simplicidad absurda, por ejemplo usando los bucles de manera muy justificada.

/codecrypto.academy

Ethereum, Enterprise Ethereum Alliance & Quorum

Ventaja: Se ha convertido en un estándar sobre el cual se desarrolla todo lo relativo a sistemas descentralizados

Inconveniente: No es posible desarrollar programas complejos. El bucle más pequeño (mirar elementos de una lista) consume mucho GAS, por lo que la mayoría de SCs se limitan a condiciones con objetos muy simples

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

Ventaja: Se ha convertido en un estándar sobre el cual se desarrolla todo lo relativo a sistemas descentralizados

Inconveniente: No es posible desarrollar programas complejos. El bucle más pequeño (mirar elementos de una lista) consume mucho GAS, por lo que la mayoría de SCs se limitan a condiciones con objetos muy simples

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

Ventaja: La información es alojada en la cadena de una forma inmutable y segura.

Inconveniente: Según la cotización del Ether, almacenar datos costará más o menos, pero haciendo una comparativa, almacenar 1 GB de información en esta cadena valdría alrededor de las varias decenas de millones de euros, mientras que en una BBDD tradicional cloud vale unos pocos céntimos de euro.

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

Ventaja: La información esta descentralizada.

Inconveniente: El consumo del protocolo en términos de potencia, comparado con uno tradicional, es colosalmente mayor.

/codecrypto.academy

Ethereum, Enterprise Ethereum Alliance & Quorum

- En vista de todas estas problemáticas Ethereum ha visto poco a poco una disminución en sus fondos para financiar el proyecto, creándose de esa forma la fundación Enterprise Ethereum Alliance (EEA).

- EEA se trata de una solución de software que ofrece una blockchain al mundo empresarial.

/codecrypto.academy

Ethereum, Enterprise Ethereum Alliance & Quorum

- **Seguridad**: su gestión en EEA es más avanzada, existiendo una integración en el directorio de empresas para los participantes (una cierta certificación de entrada)

- **Consenso**: su algoritmo se puede modificar de manera relativamente sencilla, de manera que la red ofrece cierta flexibilidad de diseño en función de los intereses de las empresas.

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

- **Datos**: es posible intercambiar datos privados entre terceros con una gestión de la confidencialidad inexistente en la versión publica.

- **Tokens**: es posible excluir la lógica de uso de tokens, de manera que el intercambio de información carezca de gastos de GAS.

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

- Del mismo modo que para Java, surgió Java Enterprise Edition, Ethereum saca su versión para empresas

- **https://entethalliance.org/**

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

- **Quorum,** es una solución basada en Ethereum a caballo entre la solución publica y EEA. La iniciativa fue lanzada por JPMorgan Chase. Ofrece una solución de empresa con componentes técnicos desarrollados internamente. Por ejemplo, ofrece módulos que permiten ocultar al emisor de una transacción y los importes intercambiados.

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

- **Código:** es de uso gratuito y esta disponible en internet. El problema es que el proceso de descarga, compilación y containerización es algo tedioso.

- **Alastria**: La primera de las redes actuales de nodos de socios de Alastria (Red T) está construida sobre tecnolo gía Quorum.

‹/codecrypto.academy›

Ethereum, Enterprise Ethereum Alliance & Quorum

- Usa consenso de tipo **Raft**, que consiste en que un nodo se convierte en líder y mina hasta que deja de serlo. En el proceso de minado, el líder envía la transacción a todos sus followers, que lo guardan en su local, avisando éstos al líder, de que finalmente genera el nuevo bloque; y se repite el proceso, eligiendo a un nuevo líder.

- Se utilizan series de Montecarlo para que no sean consecutivos.

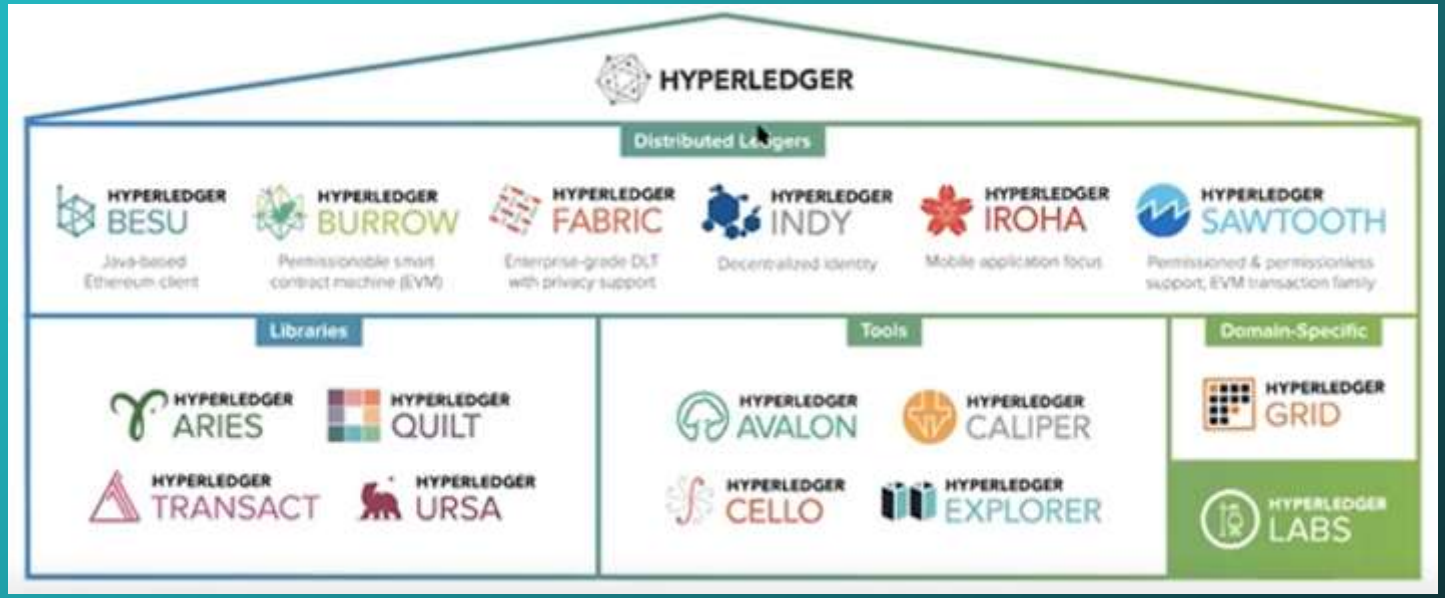
‹/codecrypto.academy›

02 Section B

Hyperledger

codecrypto.academy

Hyperledger



‹/codecrypto.academy›

Hyperledger

- **Besu**: Hyperledger Besu es un cliente Ethereum de código abierto escrito en Java bajo licencia Apache 2.0. Está diseñado para su utilización tanto en la red principal de Ethereum como para la creación de redes privadas de propósito empresarial basadas en la misma tecnología.
- **Burrow**: Es una cadena de bloques privada basada en el código de Ethereum. Permite el desarrollo de contratos inteligentes desarrollados en Solidity.

/codecrypto.academy

Hyperledger

- **Fabric**: Es Hyperledger Fabric, un proyecto de código abierto de Linux Foundation, es la infraestructura modular de blockchain y el estándar de facto para plataformas blockchain empresariales. Diseñada como base para desarrollar aplicaciones de nivel empresarial y soluciones sectoriales, la arquitectura modular y abierta utiliza componentes plug-and-play para acomodar una amplia gama de casos de uso.

Con la participación de más de 120 000 organizaciones y la colaboración de más de 15 000 ingenieros, Hyperledger Fabric ofrece un enfoque único para el consenso que permite el rendimiento a escala, al mismo tiempo que se respeta la demanda de privacidad de datos de las empresas.

/codecrypto.academy

Hyperledger

- **Indy:** Hyperledger Indy es un libro mayor distribuido, diseñado específicamente para la identidad descentralizada. Proporciona herramientas, bibliotecas y componentes reutilizables para crear y utilizar identidades digitales independientes enraizadas en cadenas de bloques u otros registros distribuidos.

‹/codecrypto.academy›

Hyperledger

- **Iroha:** Tecnología blockchain permisionada con un diseño guiado por dominio en C++ y pensada para el desarrollo de aplicaciones móviles con bibliotecas de cliente para Android, iOS y JavaScript. Tuvo mucho impulso en Japón, con empresas como Soramitsu, Hitachi, NTT Data y Colu. Su protocolo de consenso se denomina Sumeragi, y logra transacciones en menos de 2s

/codecrypto.academy

Hyperledger

- **Sawtooth**: es una plataforma BaaS empresarial de código abierto que puede ejecutar contratos inteligentes personalizados sin necesidad de conocer el diseño subyacente del sistema central (por parte de las empresas que usen sus servicios). Está muy indicada para cadena de suministros (trazabilidad seafood) e intercambio de assets (tokenización)

/codecrypto.academy

03

Section C

Ripple

codecrypto.academy

Ripple

- Ripple es una red y protocolo de pago digital basado en blockchain con su propia criptomoneda, XRP. En lugar de utilizar la minería de cadenas de bloques, Ripple utiliza un mecanismo de consenso, a través de un grupo de servidores de propiedad del banco, para confirmar las transacciones.

/codecrypto.academy

Ripple

- Es usado por muchos bancos para realizar envíos de una parte del mundo a otra para evitar utilizar el sistema tradicional Swift.

- Aunque la realidad, es que Ripple fue diseñada para el uso entre personas en 2004 (creada por Jed McCaleb).

‹/codecrypto.academy›

Ripple

- Hace años, se produjo un robo de BTC en un exchange llamado MTGox, y el software del sistema lo había programado Jeb (programa que inicialmente se usó para cambiar cartas de Magic). El caso es que posteriormente, el dueño de MTGox, vio la posibilidad de usar este software para realizar intercambios de XRP
- Puedes encontrar la Wallet de XRP en gatehub.net

/codecrypto.academy

04 Section D

Corda

codecrypto.academy

Corda

- **Corda no es una Blockchain**. Se trata de un sistema que propone registros compartidos entre pares con una lógica de firma electrónica para garantizar la seguridad de las transacciones. Cae en la categoría de registros distribuidos de uso exclusivamente permisionado, no teniendo variante pública.

- No dispone de criptomoneda (aunque existe un SDK que arregla este factor)

‹/codecrypto.academy›

Corda

- Inicialmente fue desarrollada para el entorno bancario, pero encontró caminos finalmente en sectores muy variados. En concreto, Accenture coloca a esta tecnología como un estándar dentro del universo Blockchain.

- **Ventaja**: atención a la gestión de la Confidencialidad de los participantes, ya que ninguna de las tecnologías cercanas lo ofrecen. Se pueden crear redes nuevas a partir de solo dos actores. Cuando se quiere intercambiar datos entre varios actores, no es necesario pasar por *canales* como en Hyperledger.

‹/codecrypto.academy›

Corda

- **Inconveniente**: está entorno a las 1.800 tps, lo cual está muy lejos de la velocidad de las soluciones de banca de inversión, y es un 30% más lenta que Hyperledger.

- **Ventaja**: La solución responde a problemas reales documentales laboriosos que consumen mucho tiempo e implican muchos gastos.

- **Ventaja**: Añadir un nuevo actor a la red no exige romper y reconstruir la blockchain cada vez (como ocurre en Hyperledger)

‹/codecrypto.academy›

Corda

- Bitcoin se hace famoso ante el mundo realmente cuando sale en los medios de comunicación debido al desmantelamiento de SilkRoad (mercado negro en línea en el que se aceptaba Bitcoin como moneda de pago). Entonces, a partir de ese momento, la gente se preguntó, ¿van a ser los criminales tan ingenuos de aceptar una moneda que no tiene valor? → Y es que es a partir de este punto donde Bitcoin comienza a tener valor y surgen nuevas redes

- Y es así como nace **Corda**, que no es más que un consorcio de empresas del mundo financiero

/codecrypto.academy

Corda

- Otras de las partes importantes de Corda es la de **Identidad Digital**, ya que como banco, les interesa saber quien está realizando esas operaciones financieras

Ver proyecto **Uport** sobre Identidad Digital y la soberanía de datos de usuario.
De él, han emergido dos nuevos proyectos como son **Serto** y **Veramo**

‹/codecrypto.academy›

Alastria

- 100% española. Están todas las grandes corporaciones tecnológicas españolas (Santander, BBVA, Sabadell, Bankia, Iberdrola, Gas Natural, Cepsa)
- https://www.alastria.io/

/codecrypto.academy

Alastria

- Los socios de Alastria tienen dos redes operativas (Red T y Red B) sobre las que pueden desplegarse nodos (bien nodos regulares o bien nodos críticos validadores y permisionadores).

- La primera de las redes actuales de nodos de socios de Alastria (Red T) está construida sobre tecnología **Quorum**.

/codecrypto.academy

Alastria

- La segunda de las redes (Red B) está construida sobre **Hyperledger Besu**.
- Los socios de Alastria han definido que seamos una plataforma blockchain “agnostic” (no confiamos nuestro desarrollo a una sola plataforma), por ello se han iniciado trabajos de creación de otro tipo más de red basada en **Hyperledger Fabric** (de The Linux Foundation) y en cómo interconectar las tres redes y con otras redes en el futuro.

/codecrypto.academy

Reflexión Importante: ¡puede matar un proyecto!

- En general, hay que evaluar sobre qué red desarrollar qué soluciones, atendiendo a las necesidades y al rendimiento del cliente SW que vayamos a usar. Sobre todo, ahora, al estar empezando, **las librerías están incompletas y están en constante cambio, por lo que hay que estar muy al loro para ver que va saliendo nuevo. Mucha atención con esto, que puede matar un proyecto.**

/codecrypto.academy

FIN

¡MUCHAS GRACIAS!

codecrypto.academy