Módulo I: INTRODUCCIÓN A LAS DLTs

El nuevo paradigma para las relaciones humanas

‹/codecrypto.academy›

Tabla de contenidos

Tabla de contenidos

01

Section A

Distributed Ledger Technology

‹/codecrypto.academy›

¿Qué son las DTLs?

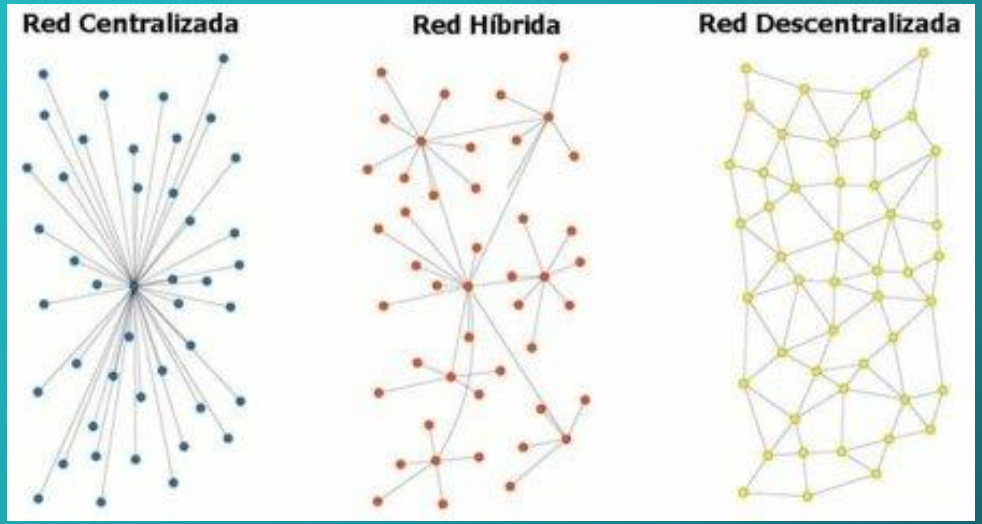
- Es el mundo de la **tecnología de libros contables distribuidos**.

- Por tanto, comprende todos aquellos sistemas distribuidos o descentralizados, que son aquellos en los que el sistema **no** depende únicamente de la gestión de una tercera parte o empresa, **siendo la propia red la encargada de decidir lo que se hace en ella**.

- Pregunta: ¿cómo funciona la red Bitcoin?

‹/codecrypto.academy›

Tipos de arquitectura de red



- Reflexión: realmente, incluso redes como Bitcoin o Ethereum (y casi la que quieras), tiene un cierto grado de centralización, ya que en estos casos, depende de que los mineros minen bloques o no, de que los desarrolladores hagan bien el código, así que como para comprar cryptos dependes de un exchange (normalmente CEX).

- En teoría, mayoritariamente las redes descentralizadas son más las privadas, y las redes distribuidas las públicas, pero hay que matizar bien lo que ocurre en cada una de manera práctica. Realmente, no existen redes 100% distribuidas o descentralizadas.

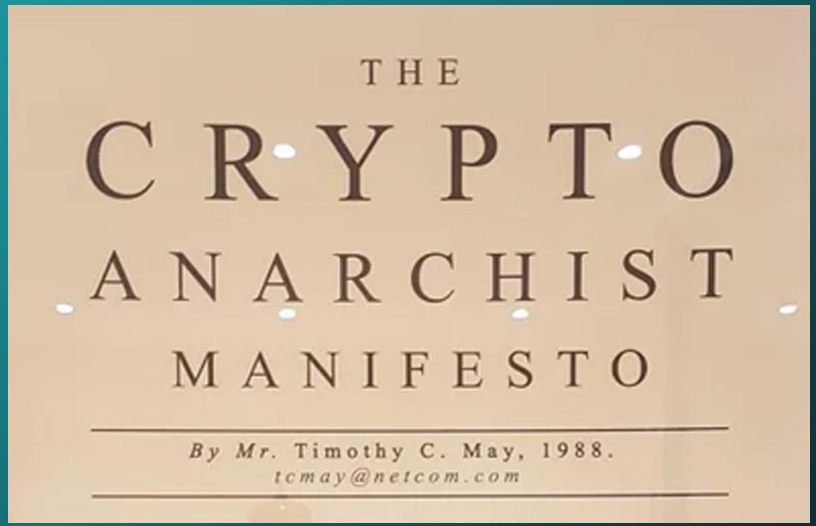
‹/codecrypto.academy›

Manifiesto CryptoAnarquista de Tomothy C May

- Escrito en 1988, ponía la primera piedra de lo que hoy conocemos como red Bitcoin.

- Y es que describía la necesidad de utilización de la criptografía para hacer efectiva la privacidad y libertad individual dentro de una red.

- Es un mecanismo para acorralar, desafiar y reducir el control de los Estados.



‹/codecrypto.academy›

¿Las DLTs son sólo un avance tecnológico?

- No, también es filosofía, ya que es la forma más justa conocida hasta el momento de mejorar las relaciones humanas. Tiene que ver con hacia donde queremos llevar el mundo

- Ejemplo: El Hardfork de Ethereum sucedió más que nada por una cuestión filosófica. Al haber ocurrido un robo de capital, se pensó en borrar ese registro, lo que supuso una división en la comunidad ETH. **La inmutabilidad de la red es inquebrantable, no se puede borrar nada de una red Blockchain por definición.**

- Pregunta: ¿Por qué nacen las redes DLT?

‹/codecrypto.academy›

Nixon deroga el patrón oro en 1971

- Desde esa fecha, **el dólar** no está respaldado por oro, perdiendo de esa forma todo su valor real. Es decir, se sigue usando simplemente por una cuestión de confianza en el sistema, pero no tiene ningún valor, **no esta respaldado por nada**.

- Pregunta: ¿Esta decisión tiene que ver algo con la inflación que vivimos?

‹/codecrypto.academy›

¿Por qué personas y organizaciones necesitamos entender cómo funciona Blockchain frente a los sistemas tradicionales?

- Lo que necesitamos entender, es que tenemos ante nuestros ojos, una nueva generación de sistemas mediantes los cuales no necesitamos depositar la confianza en la gestión a un tercero, véase gobierno o cualquier sistema centralizado que ponga sus propias reglas.

- La confianza está depositada en la red, y al ser este un concepto tan etéreo, se tiende a desconfiar. Es una cuestión de entendimiento y madurez tecnológica.

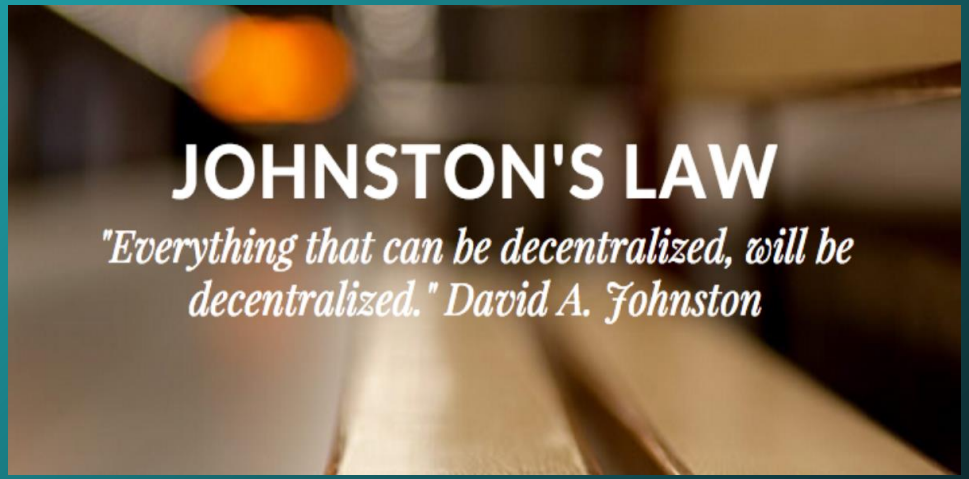
- Pregunta: ¿Cómo podríamos mejorar este proceso de adopción?

‹/codecrypto.academy›

Ley de Johnston

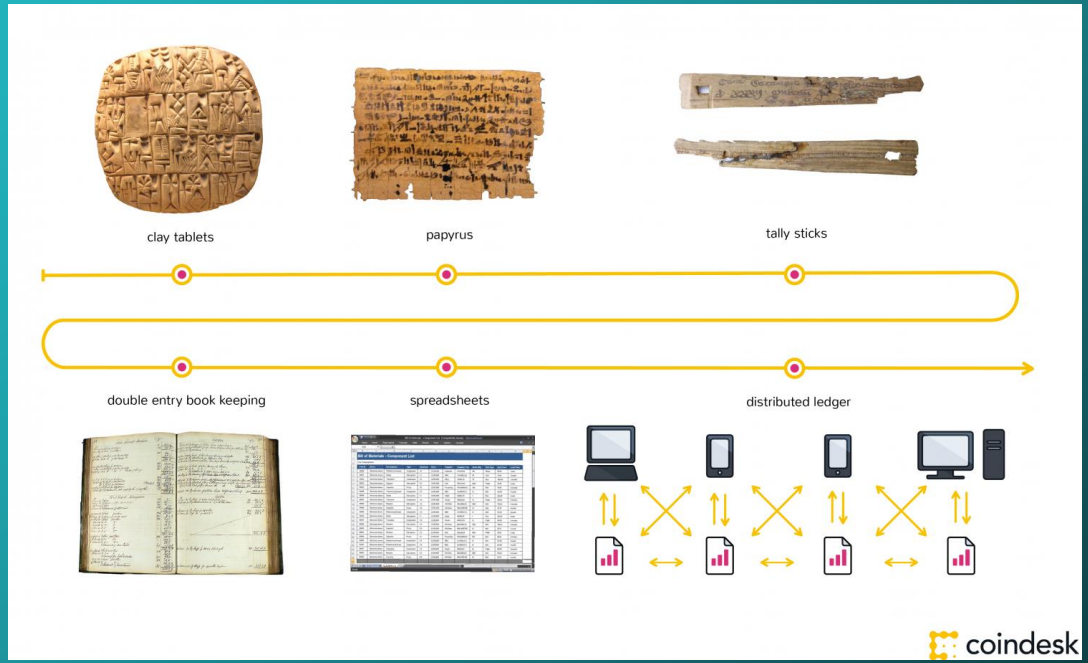
- **Vamos a enumerar diferentes sectores donde existe intermediador**: energía (Estado), transporte (Uber), turismo (Booking), casas de apuesta (Codere), periodismo (los periodistas dependen de su empresa), sanidad (expedientes médicos desparramados), finanzas (bancos y estado manejan tus fondos), etc.

Pregunta: ¿Cómo sería el caso de un Uber descentralizado?



Análogos Blockchain vs sistemas tradicionales

¿Pero todo esto de las DLTs es nuevo?



¿Es Blockchain el único tipo de DLT que existe?

- **¡NO! Blockchain, es solo un tipo de DLT**.

- Por ejemplo, hay DLTs que no tienen ni cadenas ni bloques, como pasa en redes como IOTA (que usa DAG) o Hedera (que usa Hashgraph).

- *Las tecnologías DLT, se usan para tener redes en las cuales los datos sean confiables, inalterables y que no necesite un tercero, y a partir de ahí, según las necesidades, se usa una tecnología u otra dentro de las DLTs.*

Regla Golden Hammer: ¿Valen las DLTs para todo?

- A menudo, cuando surge una tecnología tan disruptiva, se tiende a querer utilizarla para resolver todos los problemas, cumpliéndose lo que se llama la regla Golder Hammer (o martillo de oro).

- Es como si de repente miraras en la caja de herramientas, y solo encontraras un martillo, ¿o es que en la vida, arreglamos todas las cosas a martillazos? (¡algunos si que lo hacen!)

‹/codecrypto.academy›

¿Y al haber tantas, con cual me quedo? (I)

- Hay cientos de soluciones DLT que compiten por solucionar los problemas de la mejor manera, pero, cada problema necesita probablemente una solución específica y diferente; por eso surgen tantas. Por dar un ejemplo, existen unos 1000 forks de la red de Bitcoin (Litecoin es uno de ellos)

- **Hay que tener en cuenta, que al ser redes jóvenes, la mayoría de ellas aun no están maduras**. Volviendo al ejemplo del Hardfork de Ethereum, el fallo se produjo ya que el lenguaje usado en la red (Solidity) tiene aún 8 años de vida, faltándole muchas mejoras y desarrollo.

‹/codecrypto.academy›

¿Y al haber tantas, con cual me quedo? (II)

- Lo que hay que preguntarse es, **¿tiene esta red sus patrones lo suficientemente definidos en términos de robustez, para desarrollar lo que me están demandando?**

- Por este motivo, Hyperledger le gana a Ethereum en el entorno empresarial, donde siempre se requiere de mayor seguridad.

- **Hyperledger es el líder para el mundo privado (consorcios y empresas) y Ethereum para el mundo público (dApps de uso extendido)**

‹/codecrypto.academy›

02

Section B

Teoría de Juegos

codecrypto.academy

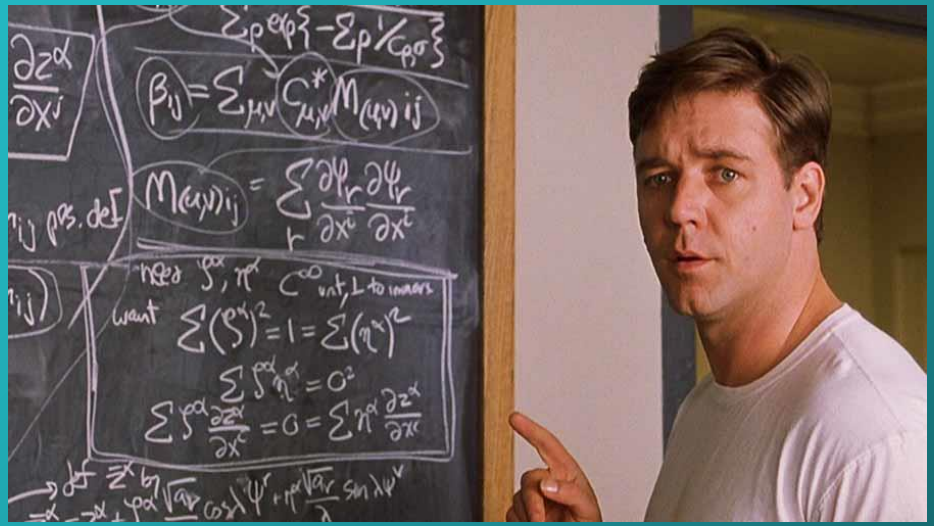
¿Qué es la Teoría de Juegos? (Teoría matemática)

- La **Teoría de Juegos**, es la parte de las matemáticas que hace que todo sistema DLT tenga sentido.

- La idea principal, es que todas las partes implicadas sacan su beneficio si cumplen las reglas; de manera que a todas las partes les interesa seguir jugando.

Pregunta: ¿Por qué en la red de Bitcoin nadie miente?

Equilibrio de John Nash o Equilibrio del Miedo



- El **Equilibrio de Nash** o **Equilibrio del Miedo**, es la idea que mejor representa los sistemas DLT.

- Cuando un jugador A toma una decisión, el jugador B no necesita cambiar su estrategia, puesto que esa **decisión ya es beneficiosa para ambos**.

- Todas las partes sacan su parte, y todos conocen las **reglas** establecidas, las cuales son **inquebrantables por definición.**

‹/codecrypto.academy›

Entonces, ¿cuándo es necesaria una DTL? (I)

Como respuesta corta:
Cuando pueda existir un problema de **CONFIANZA** entre los participantes de la red.

‹/codecrypto.academy›

Entonces, ¿cuándo es necesaria una DTL? (II)

- **Ejemplo1: Proyecto para la recompensa de los empleados en una empresa.**

Normalmente, el departamento de RRHH es visto a menudo como poco transparente en sus acciones (favoritismos). Para solucionarlo se crea un token, mediante el cual, los propios empleados se distribuyen los méritos entregando más tokens a quien creen que lo merece (habiéndose establecido una serie de reglas previamente). Posteriormente, estos tokens se pueden intercambiar por días libres.

‹/codecrypto.academy›

Entonces, ¿cuándo es necesaria una DTL? (III)

- **Ejemplo2: Consorcio de empresas que quieren hacer negocios, pero no se fían las unas de las otras.**

- No quieren que entidades externas a ellos participen, por lo que una DLT privada tiene sentido. Veamos un consorcio entre hotel, agencia de viajes, alquiler de coches y aseguradora. Les interesa tener un consorcio de turismo, en la que la DLT esté manejando todos los nodos (cada una de las empresas tendrán los suyos). De esta forma, todos los documentos serán inalterables e imborrables, ofreciéndose confianza unos a otros. Así, se evitan comprobaciones innecesarias que entorpecen los procesos, ahorrando todos en tiempo y esfuerzo.

‹/codecrypto.academy›

03

Section C

Blockchain pública, de consorcio y privada

‹/codecrypto.academy›

Tipos de redes blockchain

‹/codecrypto.academy›

Blockchain privada (con permisos)

HYPERLEDGER
FABRIC

- Una Blockchain privada es una aplicación de la tecnología donde una persona debe dar la autorización para acceder. La gestión de la infraestructura, sus normas de gestión y su funcionamiento están completamente centralizados. Permite realizar intercambios de información entre distintos socios. La información inscrita se fecha y se firma. Esto permite garantizar que la información se ha intercambiado correctamente en una fecha y hora determinadas, y se puede identificar a su autor.

‹/codecrypto.academy›

Blockchain privada (con permisos)

- En la práctica, no se habla forzosamente de una blockchain, sino más bien de un registro distribuido. Cuando todos los emisores de información son conocidos fiables, no es necesario tener un componente técnico que controle la veracidad de la información, solo que se ha realizado una operación.

‹/codecrypto.academy›

Algunos ejemplos de redes privadas

- Es la principal red privada de España, y esta impulsada por las principales empresas que operan en el IBEX35 (y recientemente muchas más) como son: Repsol, Iberdrola, BBVA, Caixa, etc.

r3·corda

- Es una de las principales redes privadas a nivel global, formada por empresas como: Accenture, NTT Data, AWS, Capgemini, etc.

‹/codecrypto.academy›

Blockchain de consorcio (permisionada)

- En esencia, una blockchain permisionada es comparable a una blockchain privada. Se agrega una cantidad de actores mayor procedentes de razones sociales distintas y en los que no es obligatorio confiar completamente.

‹/codecrypto.academy›

Blockchain de consorcio (permisionada)

- El acceso a esta blockchain es menos centralizado, porque la autorización del acceso se hace habitualmente mediante el intermediario de una autoridad para cada empresa participante. La función de esta autoridad es administrar los accesos de manera delegada. Por lo tanto, los actores son conocidos y es muy recomendable utilizar una lógica de alias para identificarlos.

- Para asegurar la fiabilidad de la información, se debe utilizar un algoritmo de consenso, siendo el más extendido para este tipo de redes el PoW

Blockchain pública (no permisionada)

- Una blockchain pública es un registro distribuido donde todos pueden leer y escribir sin pasar por una autoridad reguladora central. Por eso se habla también de solución sin permisos. Hay muchas blockchains públicas y todo el mundo tiene derecho a crear la suya. Como sustitutas de las redes centralizadas, estas blockchains tienen un funcionamiento basado en principios criptoeconómicos definidos por Vitalik Buterin: "*La combinación de incitaciones económicas y los mecanismos de verificación que utilizan la criptografía como una prueba de trabajo o prueba de la participación*" → Es decir, se anima a todos a participar en la verificación de las transacciones mediante ventajas económicas.

‹/codecrypto.academy›

Blockchain pública (no permisionada)

- La parte que puede tomar cada uno en el proceso de consenso se define en función de los recursos que puede poner a disposición. Pero el riesgo con este modo de funcionamiento es que los más poderosos se hagan con la mayor parte de las validaciones.

‹/codecrypto.academy›

Casos de uso Blockchain Pública

- **Transacciones financieras:** cuando se recibe una factura, un smart contract puede verificar las condiciones y activar el pago.

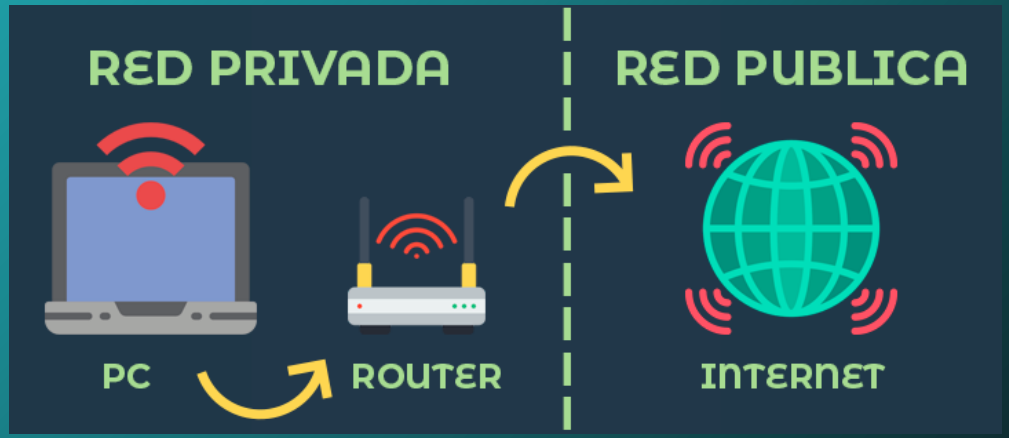
- **SAP** puede hacer este tipo de operación y actúan como bancos en sustitución de tokens virtuales. Sin embargo, es una solución muy costosa.

- **Bitcoin** es un actor histórico y tiene un rendimiento muy bueno por su comunidad de usuarios.
- **Ripple**, se ha especializado en los intercambios transfronterizos con grandes bancos.
- **Stellar** se ha posicionado en los micropagos, pero va a atacar a Ripple.
- **IOTA**, busca desarrollar su actividad de pago entre máquinas, por ejemplo, en el segmento to X, o VtoX, en el sector de la automoción.

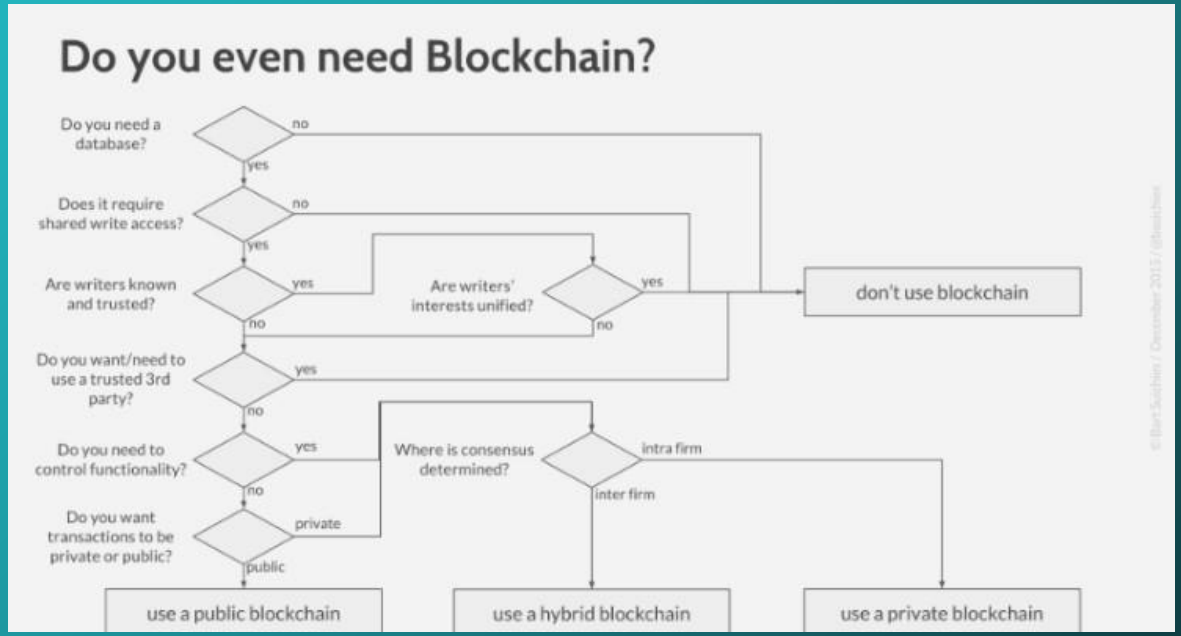
‹/codecrypto.academy›

Un poco de visión hacia el futuro

- Donde nos vamos a mover en **el futuro es en las redes mixtas**. Por ejemplo, usar Hyperledger **(red privada) para el día a día y con cierta frecuencia usar una DLT pública**, donde los datos sean imborrables definitivamente. Piensa, que quien maneja una red privada son empresas, y si se ponen de acuerdo, podrían borrar o modificar datos a su antojo.

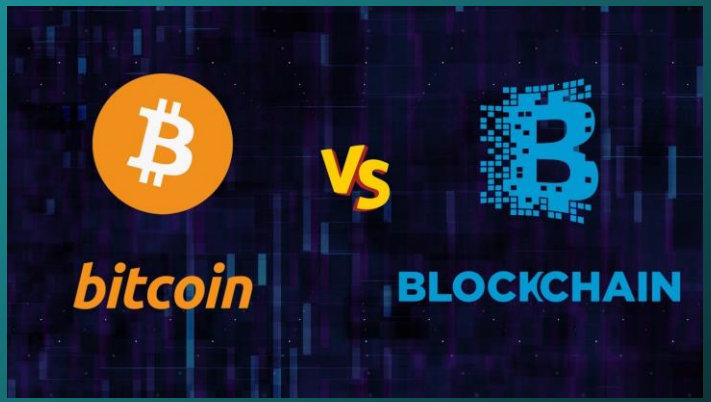


Decision Path Blockchain



Dilema: ¿Es Bitcoin o Blockchain lo importante?

- Es decir, ¿es a través de Bitcoin mediante lo cual, utilizando Blockchain, llegaremos a un nuevo modelo económico, o por el contrario, será desarrollando diferentes Blockchains (o DLTs en general) para los diferentes sectores?



‹/codecrypto.academy›

04

Section D

La gobernanza

codecrypto.academy

La gobernanza en la blockchain

- El grado de gobernanza depende del tipo de blockchain. Cuanto más abierta es, menos puede influir un actor concreto en la gobernanza.

- En una blockchain pública, los nodos de red se encargan de validar las opciones analizadas e iniciadas por los desarrolladores decidiendo aprobar o no las modificaciones propuestas (EIPs de Ethereum). La única norma de funcionamiento la define la tecnología (El código es la ley). Este planteamiento implica numerosos fallos y la experiencia de estos diez últimos años ha aportado muchas enseñanzas.

‹/codecrypto.academy›

La gobernanza en la blockchain

- En un contexto de privada o de consenso, las normas de gobernanza son extrañamente diversas. En un grupo de e presas, el ejercicio puede volverse sensible con rapidez y se necesitan métodos de trabajo especializados con un personal cualificado. No se trata solo de ponerse de acuerdo sobre los actores susceptibles de leer o escribir en la blockchain. Las normas de negocio, las responsabilidades y la visibilidad de algunos exigen un gran rigor en la negociación e implementación

‹/codecrypto.academy›

05

Section E

Propiedades de las DLTs

codecrypto.academy

Propiedades de las DLTs

Programadores éticos

- De acuerdo con los aspectos filosóficos que los sistemas DLTs proveen, existe un tema importante a tener en cuenta. Y es que, **estamos a merced de lo que los programadores de software hagan**. “**Son las nuevas estrellas del rock**”. Realmente, son los que deciden cómo se hacen las cosas del nuevo mundo en el que vivimos y hacia el que vamos.
- Por eso, surge la necesidad de tener programadores de software con ética, en el sentido de que nuestro futuro está siendo dirigido por ellos.

‹/codecrypto.academy›

Inciso: Responsabilidad

- Ben Parker (el tío de Spiderman) decía: **todo poder lleva consigo una gran responsabilidad**.
- Nos gusta poco el riesgo, por lo que contratamos seguros. Siempre estamos tratando de cargar nuestra responsabilidad a alguien. Es decir, si tu gestionas tus datos (**soberanía digital**), tu eres el responsable de si pierdes por ejemplo tu contraseña, perdiendo así tus fondos, cosa que no pasa con un banco central… **Entonces, ¿bancos y entidades centrales siempre tendrán sus clientes?**

‹/codecrypto.academy›

Competición de Implementaciones Blockchain

- Vivimos una constante competición por ser la red Blockchain del futuro. ¿Quién ganará? Hay opiniones de todo tipo

- Hablaremos de algunas de las más populares, como son: Hyperledger, Ripple, Corda, Lisk, Alastria, Enterprise Ethereum Alliance, IOTA, Hashgraph

‹/codecrypto.academy›

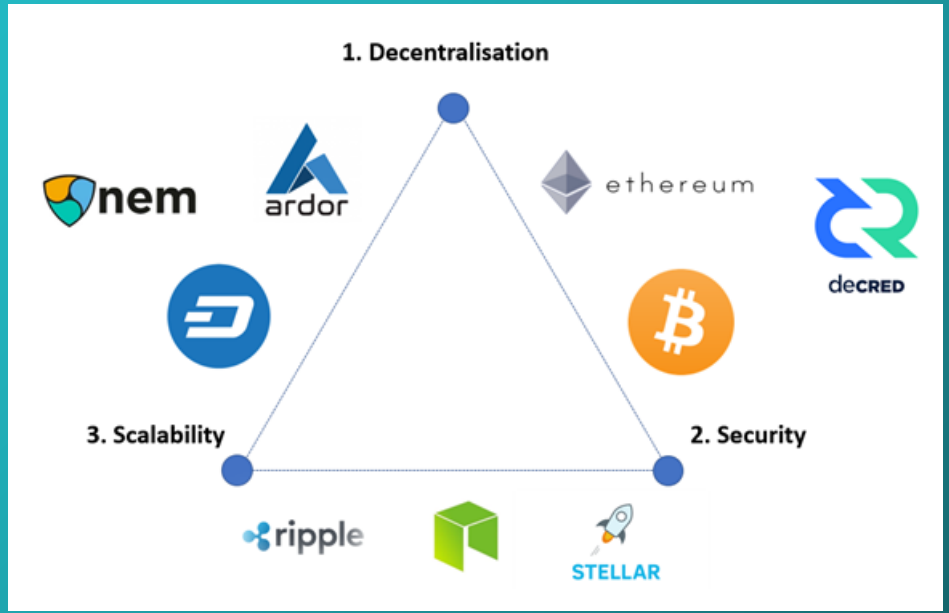
06

Section F

Gestión del Trilema

codecrypto.academy

Gestión del trilema (nunca se pueden cumplir los tres principios básicos de las redes Blockchain)



1. **Descentralización**: interés por evitar la censura y los errores de seguridad de entes centralizados.

2. **Escalabilidad**: interés por incrementar el número de transacciones por segundo que se ejecutan en la red.

3. **Seguridad**: interés por salvaguardar ataques del 51% o similares

FIN

¡MUCHAS GRACIAS!

‹/codecrypto.academy›