
BLOCKCHAIN Y ADMINISTRACIONES PÚBLICAS:

El objetivo es construir de forma colaborativa y rapida, un indice u hoja de ruta del documento que se construye para presentar, luego podemos subirlo a gitlab y consolidar el documento

Borrador **Indice**

Introduccion:

- - Bienes digitales y Monedas Digitales
- - Internet del valor : Salto Tecnologico y social
- - Cuestiones tecnológicas
- - Tipos de Blockchain: Público, Privado e Híbrido

Sistemas Blockhain Publicos:

- - Origen: criptoanarquía.Cryptopunk
- - Bitcoin: Descripción, Blockchain
- - Ethereum: supercomputacion descentralizada
- - Contratos Inteligentes (Smart Contract)
- - Certificaciones digitales de servicios y autocertificacion

.....

Qué puede aportar BlockChain a las Administraciones Públicas:

- Nuevo Modelo de las Administraciones Públicas
- Ámbitos
- Ventajas, valores añadidos
- Transparencia, auditorias continuas, antifraude:

auditoría sobre datos inmutables, datos que no pueden retocarse en fecha distinta. Poder evitar el fraude derivado es algo diferencial. Dato+timestamp+responsable inmutables.

Ejemplos de uso de Blockchain en administraciones del mundo:

- Lituania?? Estonia???

- Suiza: ciudad con blockchain
- Estados Unidos
- Argentina: fidelización de funcionarios, con recompensas mediante tokens (RSK)

Casos de uso y ayuntamiento de madrid:

- Identidad digital
- Votaciones Electronicas

- Registros: registro de documentos, catastro
- Linea Madrid: Gestion de tramites
- Impuestos, tributos, multas
- Historial de ayudas

Transparencia:

Contratos Publicos
Formacion
Ofertas Publicas

- Tecnologia e Infraestructura
- Desarrollo

- **Sistemas de fidelización:**
- - Tokens, recompensas, ventajas por uso de servicios públicos:
- - Transporte público, aparcamientos disuasorios, bicicletas compartidas, coches y motos eléctricos
-

Pruebas de Conceptos (POC):

- Ejemplo de blockchain sencillo
  - - En lenguaje Python
  - - En lenguaje Haskell
  - - Aplicación sobre sistema de Cita Previa (Línea Madrid)
  -
  - - Sistema de votación con blockchain, sobre Red Ethereum
  -
  - - Contratos inteligentes con blockchain, sobre Red Ethereum
  -
  -

-
-

BIBLIOGRAFIA Y RECURSOS:

-
-
-

Autor Borrador Introduccion: Pedro Romero

Introduccion:

Los negocios, el gobierno y la sociedad están basados en la confianza. Por eso muchas personas todavía se muestran escépticas al oír hablar de una tecnología que promete transformar el modo en que la logramos y aplicamos.

¿Que es la tecnologia Blockchain?

Blockchain no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada. También se puede definir como una base de datos compartida que funciona como un libro de registro de operaciones de compra y venta, como los libros contables.

Básicamente, el blockchain funciona como un libro de contabilidad muy complejo: proporciona una estructura de datos a prueba de falsificaciones que permite identificar la identidad en origen y destino durante una transacción, verificar que es auténtica y dar el visto bueno para que se realice, de forma que cada cadena de datos criptográficos que verifica una transacción sea imposible de replicar, y por tanto, de falsificar. Y lo más importante: la registra para la posteridad.

A día de hoy, las transacciones realizadas con Bitcoin están secuenciadas a través de blockchain utilizando sistemas de cifrado SHA-256, de forma que todas las trasacciones que se hacen a través de esta base de datos distribuida son firmadas mediante una clave privada a prueba de manipulaciones por terceros.

- Bienes digitales y Monedas Digitales

Para entender mejor lo que estamos exponiendo en este documento, necesitamos entender los dos conceptos:

El bien digital es un servicio de software, al que puede accederse remotamente, sin intervención humana, y cuyo contenido es universal (sonido, imagen, datos, hechos) transmitidos electrónicamente, que puede disfrutarse o utilizarse previo derecho de acceso u uso, oneroso o gratuito, que no tiene equivalencia o simetría con el bien material o físico que representa, salvo por aproximación.

La moneda digital es más que un bien digital en sentido estricto: un bien de información intangible fundado en protocolos especificos de software libre, representativo de un bien fisico o material(por ejemplo, dinero) y , detalle significativo, en el que la creación de moneda da lugar a contraprestación por el trabajo realizado por determinado usuario o partícipe (miner) en la comunidad en red.

Internet de la Informacion vs Internet del Valor

Blockchain, dicen los expertos, va a posibilitar dar el salto del llamado *internet de la información* al *internet del valor*. Durante los últimos 23 años hemos convivido con el primero, un ecosistema que ha penetrado hasta las profundidades de nuestro día a día y que ha hecho que florezcan empresas como Google, Facebook o Twitter. Estos nombres han cambiado modelos de negocio de industrias enteras como los medios de comunicación, las telecomunicaciones o el turismo.

Se le llama internet de la información porque hasta ahora lo que se ha compartido ha sido fundamentalmente información. Ahora, estamos dando el salto hacia el *internet del valor.* Y esta ola es mucho mayor que la primera

Realmente el Internet del valor, es una infraestructura que te permite construir sobre internet, y crear otra capa sobre la que las personas van a poder intercambiar valor entre ellas". Eso afecta a todos los sectores: ya tocó a la banca, pero va a afectar también al sector de las energías, a las telecomunicaciones, a las cadenas de valor de logística, etc. etc.

Internet del valor : Salto Tecnologico y social

El mundo cambió de repente, de forma repentina, sin que muchos vieran el impacto real que iba a tener en el futuro y que tendrá, fue con la aparición de

los bits, no hablemos técnicamente de lo que son los bits, sino intentar transmitir el concepto de digitalización. Hoy en día, todo se puede almacenar, todo deja huellas digitales, hay suficiente capacidad como para almacenar toda la información generada por el hombre durante los últimos 40.000 años.

"mientras los sistemas sociales cambian incrementalmente, la tecnología lo hace de forma exponencial, creándose así una brecha que posibilita los cambios discontinuos y revolucionarios".

Estamos viviendo una época interesante, las antiguas estructuras esclerotizadas, pueden provocar la aparición de fuerzas de transformación y de regeneración que cambian el paradigma de ciertos sectores de una forma tan radical que cuesta imaginarlo.

Hasta ahora, las organizaciones han tenido que adaptarse y adoptar los beneficios que ha creado la era digital, han tenido que rediseñar sus diferentes sistemas de comunicación internos para introducir ordenadores y software necesarios para facilitar tareas y operaciones que se llevan a cabo dentro de ellas o mínimo en sus principales áreas.

Pero con blockchain las posibilidades de transmitir informacion de bienes digitales y que todo el mundo pueda intercambiar y compartir valor de igual a igual(P2P) mediante criptomonedas propias, nos deja claro que el poder no va a estar tan centralizado. Eso cambia la operativa de las empresas, pero también la operativa de las personas, cómo interactuamos ahora entre nosotros. Y esto es realmente fascinante, tratar de imaginar cómo va a ser el futuro en 20, 30 sobre todo a nivel social.

Lo cierto, es que hasta ahora aunque no de forma completa, las TIC habian resultado imprescindibles en aspectos de tanta repercusión social, como son la igualdad de oportunidades, la democratización en el acceso a la información, o la eliminación de los riesgos de las brechas socioeconómicos y culturales por motivos geográficos, de edad, de género, de origen, etc…

Blockchain puede provocar cambios profundos en todos estos casos, dentro de muy poco tiempo. Quizás uno de los efectos más interesantes de la economía descentralizada basada en protocolos abiertos: la redistribución del valor en esta transición.

Origen de de la tecnologia Blockchain: Criptoanarquía (Cipherpunk)

Los movimientos *cyberpunk*, *cypherpunk* y *hacktivista* sentaron las bases que permitirían crear la primera criptomoneda del mundo, el *bitcoin*; pero, más relevante aun, facilitaron idear el protocolo de cadenas de bloques, basado en la criptografia de clave publica, que habia nacido años antes, rompiendo la hegemonia de la NSA americana, basada en criptografia de clave privada simetrica

David Chaum es uno de los iniciadores de la criptografía aplicada a los pagos, firmas ciegas para pagos ilocalizables, imposibles de rastrear. Un sistema que, por un lado, no permite a terceras partes la determinación del perceptor, el tiempo o el importe de los pagos hechos por otra persona; importante en términos de intimidad y privacidad; por otra, la capacidad de los individuos para proveer una prueba del pago o informar de la identidad del perceptor bajo circunstancias excepcionales.

Entre 1992 y 1994 se difunde la criptografía como manifestación de un movimiento denominado criptoanarquÍa: un medio para tutelar la privacidad y la libertad individual en la red: "...*una criptografía potente puede causar la declinación del poder del estado y quizá aún colapsarlo. Creemos que la expansión en el ciberespacio con comunicaciones seguras, anonimato y seudónimos y otras interacciones criptomediales cambiaran profundamente la naturaleza de las interacciones económicas y sociales*.

"*La informática está al borde de proporcionar la capacidad a individuos y grupos de comunicarse e interactuar entre ellos de forma totalmente anónima. Dos personas pueden intercambiar mensajes, hacer negocios y negociar contratos electrónicos, sin saber nunca el Nombre Auténtico, o la identidad legal, de la otra. Las interacciones sobre las redes serán intrazables, gracias al uso extendido de re-enrutado de paquetes encriptados en máquinas a prueba de manipulacion que implementen protocolos Criptograficos, con garantias casi perfectas, contra cualquier intento de alteracion.*
Las reputaciones tendrán una importancia crucial, mucho más importante en los tratos que las calificaciones crediticias de hoy en dia. Estos progresos alterarán completamente la naturaleza de la regulación del gobierno, la capacidad de gravar y de controlar las interacciones económicas, la capacidad de mantener la información secreta, e incluso alterarán la naturaleza de la confianza y de la reputación"

Timothy C.May Cifernomicron. Manifiesto

Tipos de Blockchain: Público, Privado e Híbrido

Existen tres tipos:

-Públicas

-Privadas

-Híbridas.

Blockchains públicas

Los ejemplos más conocidos de Blockchains públicas son **Bitcoin y Ethereum.** Una Blockchain pública es accesible a cualquier usuario en el mundo. Lo único

que se necesita es un ordenador y una conexión a Internet.

Ejemplo: Bitcoin

La Blockchain pública de Bitcoin se compone del *protocolo Bitcoin* (con B mayúscula), la unidad de cuenta o token bitcoin (con b minúscula) y la red blockchain (la base de datos en la que se registran las transacciones). Bitcoin ha sido el inventor del concepto Blockchain, inspirándose en otras soluciones y combinándolas de tal forma que se pudiera crear un sistema descentralizado que resolvía el problema del "doble gasto". El problema del "doble gasto", que se llevaba investigando por científicos en todo el mundo desde hace más de 30 años, decía que en un sistema descentralizado era imposible evitar que un activo o bien digital se gastará dos o más veces.

En un sistema centralizado evitar el problema del "doble gasto" es muy sencillo, pero en un sistema descentralizado en el que todos los ordenadores tienen una copia de todas las transacciones (la blockchain) la cuestión de cómo se ponen de acuerdo todos los nodos para definir cuál es la realidad de esa base de datos de forma descentralizada para llegar a un consenso y funcionar es un problema altamente complejo que nadie consiguió resolver hasta que apareció Bitcoin. Bitcoin resuelve este problema con las matemáticas, la criptografía y la comunidad Bitcoin (los usuarios, mineros, casas de cambio y desarrolladores del ecosistema Bitcoin).

Blockchains privadas

Una Blockchain privada**,** a diferencia de una Blockchain pública, no está abierta al público, sino que solo se puede acceder a ella por invitación. Las Blockchains privadas son más nuevas que las Blockchains públicas y pueden ser muy diferentes las unas a las otras y en algunos casos es incluso cuestionable que se pueda hablar de Blockchain para algunas de las soluciones que se conocen en el mercado. Algunas de las más famosas son Hyperledger (de la Fundación Linux), R3 (un consorcio de bancos internacionales para desarrollar soluciones bancarias de blockchain privada) o Ripple (un protocolo para facilitar las transferencias internacionales de dinero).

Blockchains híbridas

Las Blockchain híbridas son una combinación de las públicas y privadas. En una Blockchain híbrida los nodos participantes son invitados, pero todas las transacciones son públicas. Eso quiere decir que los nodos participan en el

mantenimiento y seguridad de esta blockchain, pero que todas las transacciones son visibles para usuarios en todo el mundo y que no tienen que conocer el contenido de la blockchain, a diferencia de las blockchains privadas en la cual las transacciones son privadas también. Algunos ejemplos de blockchains híbridas son BigchainDB (un proveedor de tecnología Blockchain) o Evernym, una blockchain híbrida que quiere facilitar la gestión de la Identidad Digital Soberana (ltSelf Sovereign Identity).

Sistemas Blockchain Publicos:

Bitcoin con mas detalle:

Ya hemos explicado en parte Bitcoin anteriormente, como el gran ejemplo actual de Blockchain Publica.

Bitcoin es realmente, un conjunto de conceptos y tecnologías que conforman un ecosistema de dinero digital. El almacenamiento y transmisión de valor entre los participantes de la red bitcoin se consigue mediante la utilización de las unidades monetarias llamadas bitcoins. Los usuarios de bitcoin se comunican entre ellos usando el protocolo Bitcoin, principalmente a través de Internet, aunque también se pueden utilizar otras redes de transporte. La pila de protocolos bitcoin, disponible como software open source, puede ejecutarse sobre una amplia variedad de dispositivos, incluyendo Portatiles y smartphones, lo que hace que la tecnología sea fácilmente accesible.

Los usuarios pueden transferir bitcoins a través de la red para hacer prácticamente cualquier cosa realizable con monedas convencionales, incluyendo comprar y vender bienes, enviar dinero a personas y organizaciones, o extender créditos. Los bitcoins pueden comprarse, venderse e intercambiarse por otras monedas en casas de cambio especializadas. En cierta forma bitcoin es la forma de dinero perfecta para Internet, ya que es rápido, seguro y carente de fronteras.

Bitcoin es un sistema entre pares (peer-to-peer) distribuido. Como tal no existe ningún servidor o punto de control "central". Los bitcoins se crean mediante un proceso llamado "minería," que se basa en una competencia por encontrar soluciones a un problema matemático a la vez que se procesan transacciones bitcoin. Cualquier participante de la red bitcoin (léase, cualquier persona utilizando un dispositivo con la pila de protocolos bitcoin completa) puede operar como minero, utilizando el poder de computacion de su computador para verificar y registrar transacciones.

Cada 10 minutos en promedio alguien consigue validar las transacciones de los

últimos 10 minutos y es recompensado con nuevos bitcoins.
En esencia, la minería de bitcoins descentraliza la función de emisión de moneda y la autorización de un banco central, y reemplaza la necesidad de un banco central con esta competencia global.

El protocolo bitcoin incluye algoritmos que regulan la función de minería en toda la red. La dificultad de la tarea de procesamiento que los mineros deben ejecutar (para registrar con éxito un bloque de transacciones para la red bitcoin) se ajusta dinámicamente de forma que, en promedio, alguien tendrá exito cada 10 minutos sin importar cuántos mineros (y CPUs) hayan trabajado en la tarea en cada momento. Cada cuatro años, el protocolo también reduce a la mitad la tasa a la que se crean nuevos bitcoins, asegurando se seguirán creando bitcoins hasta un valor límite de 21 millones de monedas.

El resultado es que el número de bitcoins en circulación sigue de cerca una curva fácilmente predecible que alcanza los 21 millones en el año 2140. Debido a la decreciente tasa de emisión, bitcoin es deflacionario en el largo plazo. Además bitcoin no puede ser inflado a través de la "impresión" de nuevo dinero por encima de la tasa de emisión esperada.

Lo relevante: Revolucion en Computación Distribuida

Bitcoin da una solución a un Problema de Computación Distribuida, La invención de Satoshi Nakamoto es también una solución a un problema previamente sin solución en computación distribuida, conocido como el "Problema de los Generales Bizantinos."

Brevemente, el problema consiste en tratar de llegar a un consenso al respecto de un plan de acción intercambiando información a través de una red poco fiable y potencialmente comprometida.

La solución de Satoshi Nakamoto, que utiliza el concepto de prueba de trabajo para alcanzar un consenso sin requerir confianza en una autoridad central, representa un avance en computación distribuida y posee amplias aplicaciones más allá de las monedas. Puede ser utilizada para alcanzar consenso en redes distribuidas para probar la legitimidad de elecciones, loterías, registros de activos, autorizaciones bajo notario digitales, y más.

Ethereum: supercomputacion descentralizada

Imagina que toda la humanidad podría tener acceso a una sola super-computadora. Pero eso, de hecho, fue hecho de una combinación de cientos de miles de ordenadores, dispersas por el mundo, trabajando en la misma red, de manera descentralizada y procesando la misma información. Esta es básicamente la propuesta detrás de la plataforma

Ethereum.

Ethereum es una plataforma digital cuya principal misión es la implementación de aplicaciones descentralizadas (dapps) y contratos inteligentes. “Dapps” son programas informáticos que eliminan la necesidad de intermediarios en virtualmente cualquier servicio centralizado existente al permitir que cualquiera confíe en una contraparte desconocida para realizar los más variados tipos de acuerdos y acuerdos de una manera 100% digital.

En Ethereum, los desarrolladores también pueden escribir lógica de negocio y acuerdos en forma de contratos inteligentes, los cuales se ejecutan automáticamente cuando sus condiciones son satisfechas por ambas partes e informadas a la red.

Estos contratos pueden almacenar datos, enviar y recibir transacciones e incluso interactuar con otros contratos, independientemente de cualquier control.

Inicialmente, el término "contrato inteligente" se utilizó para describir el uso de sistemas informáticos (u otros medios automatizados) que tenían por objeto realizar ciertos acuerdos.

Como ejemplo de un contrato mecánico inteligente, podemos mencionar una máquina que vende refrescos o chocolates. Cuando colocas un billete o moneda en estas máquinas, un sistema informático programado para identificar la cantidad recibida y el producto elegido hace cumplir un acuerdo entre el consumidor y el propietario de la máquina, realizando una venta automática.

Los dapps y los contratos inteligentes trabajan en el blockchain Ethereum, que tuvo su arquitectura inicial concebida por un joven genio ruso a la edad de 19 años, llamado Vitalik Buterin, quien eligió el siguiente título para su libro blanco: "*Ethereum: A Platform of Smart contracts and next generation decentralized applications*."

Una aplicación futura de Ethereum son DAOs o Organizaciones Autónomas Descentralizadas.

Un DAO se compone de uno o más contratos y podría ser financiado por un grupo de personas con ideas similares. Un DAO opera completamente transparente e independiente de cualquier intervención humana, incluyendo a sus creadores originales. Un DAO permanecerá en la red mientras cubra sus costos de supervivencia y proporcione un servicio útil a su base de clientes.

Contratos inteligentes (Smart Contracts)

Realmente, se trata de meros programas de software que recogen los términos de un contrato entre las partes y se almacenan en la *blockchain*, con la peculiaridad de que se autoejecutan cuando se cumplen una serie de condiciones especificadas en el propio contrato.

De este modo se evitan los intermediarios, aligerando costes y retrasos burocráticos; así como cualquier tipo de interferencia por parte de un tercero.
Las posibilidades de esta funcionalidad combinada con otras nuevas tecnologías como el Internet de las cosas y las tecnologías financieras son enormes

Son contratos con las siguientes características:

- No requiere de intermediarios que lo validen o que garanticen su cumplimiento.
- No son interpretables, por o que evitas que alguno de los firmantes evite cumplir su parte del acuerdo en base a una interpretación subjetiva.
- Se cumple por sí mismo y se ejecuta cuando se cumplen las condiciones pactadas.
- Puede ser firmado por personas (físicas o jurídicas) o por máquinas autónomas.
- y tiene todas las características inherentes a *Blockchain*: público, descentralizado, transparente e inmutables.