



CERTIFICADO DE ESPECIALIDAD

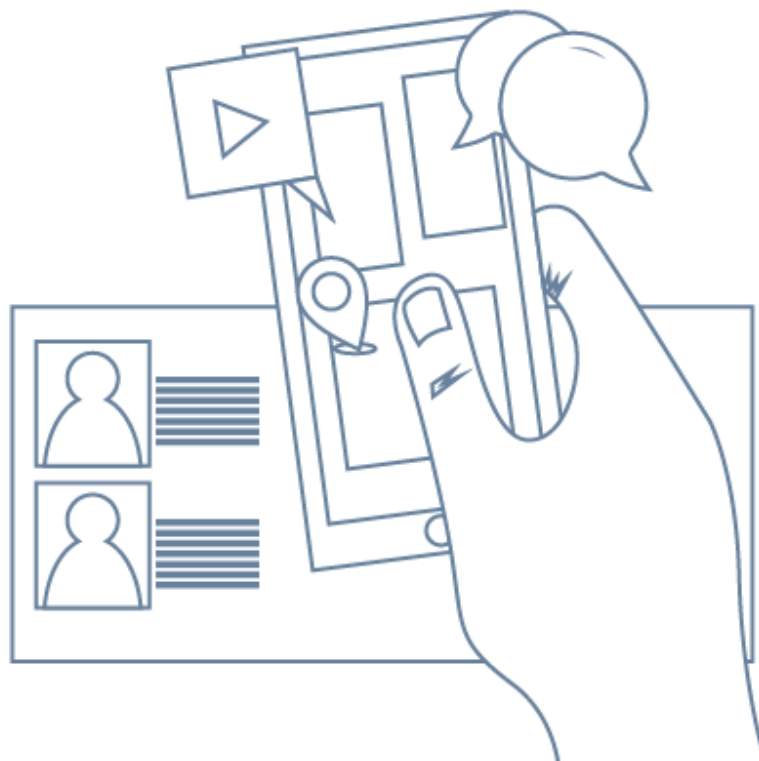
CIBERSEGURIDAD APLICADA I





CERTIFICADO DE ESPECIALIDAD

CIBERSEGURIDAD APLICADA I





ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director de Escuela / Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar / Julio Briones

Diseñador instruccional / Luisa García

VALIDACIÓN

Experto disciplinar / Andrés del Alcázar Cavallo

Jefa de diseño instruccional y multimedia / Alejandra San Juan Reyes


DISEÑO DOCUMENTO

Welearn



Contenido

APRENDIZAJE ESPERADO DE LA SEMANA.....	6
CONCEPTO MÁS IMPORTANTE	6
INTRODUCCIÓN	7
TIPOS DE VULNERABILIDADES EN UNA RED DE DATOS DIGITAL.....	8
Arquitectura Blockchain	8
Cadena de bloques pública.....	8
RIESGOS Y AMENAZAS QUE AFECTAN A LA INFORMACIÓN	9
Blockchain privado.....	9
Consortium Blockchain	9
INFORMACIÓN PROTEGIDA BAJO UNA ARQUITECTURA BLOCKCHAIN	11
Identificar el caso de uso	11
Identificar el Mecanismo de Consenso.....	11
ENCRIPTACIÓN DE INFORMACIÓN DIGITAL PARA RESGUARDO	13
Diseñar la arquitectura	13
Diseñar la cadena de bloques	13
Crear las API para su Blockchain.....	14
Diseño del front-end.....	14
PROPUESTAS DE VALOR PARA NEGOCIOS.....	15
Perspectivas futuras	15
Proyectos de cadena de bloques.....	15
ÁREAS DE APLICACIÓN DE BLOCKCHAIN.....	16
Usuarios de Blockchain	16
Mineros blockchain.....	16
Desarrolladores de Blockchain	17
REDES PÚBLICAS Y PRIVADAS: MÉTODOS DE ACCESO Y RESGUARDO DE LA INFORMACIÓN.....	18
Aplicaciones Blockchain.....	18
Blockchain.....	19
Superponer redes	19
Protocolos descentralizados	19
Sistema de soporte	20



Interfaz de usuario	20
BITCOIN	21
ETHEREUM	22
NEO	23
HYPERLEDGER	24
EOS	25
CORDA	26
QUORUM	27
MULTICHAIN	28
CONSUMO DE ENERGÍA	29
Escalabilidad	29
Percepción pública	29
Industrias actuales que utilizan Blockchain	30
Interrupciones emocionantes próximamente	31
IDEAS CLAVES	32
CONCLUSIONES	33
LINKS/MATERIAL MULTIMEDIA	34
BIBLIOGRAFÍA	35



APRENDIZAJE ESPERADO DE LA SEMANA

Relacionar estrategias y métodos de protección y seguridad de información asociados a Blockchain con propuestas de valor para negocios, considerando vulnerabilidades de la información en redes de datos y áreas de aplicación.

CONCEPTO MÁS IMPORTANTE

Un ataque cibernético en esta cadena de bloques es mucho más difícil dado que se debería ejecutar en todas las copias de la base de datos, algo que es físicamente difícil de lograr, por lo tanto, la seguridad de la información está garantizada. De llegar a sufrir cambios las discrepancias serán detectadas inmediatamente por la irreversibilidad del proceso del hash.

La propiedad en la cadena de bloques está determinada por dos claves criptográficas utilizadas para cifrar mensajes electrónicos: públicos y privados. Cuando alguien envía un mensaje cifrado, usa la clave pública, que está en el dominio público en la cadena de bloques. El destinatario, al abrir una carta, descifra el mensaje utilizando, a su vez, una clave privada a la que solo él puede acceder.



INTRODUCCIÓN

Conozca en profundidad los fundamentos de Blockchain, la arquitectura de Blockchain y varios casos de uso de Blockchain.

Blockchain.com (anteriormente Blockchain.info) es un servicio de exploración de bloques de Bitcoin, así como una billetera de criptomonedas y un intercambio de criptomonedas que admite Bitcoin, Bitcoin Cash y Ethereum. También proporcionan gráficos de datos de Bitcoin, estadísticas e información de mercado. Siguiendo con la semana 2, acá teniendo los conceptos claros de Bitcoin, revisaremos los tipos de vulnerabilidades, los riesgos y amenazas a la información, encriptación de Bitcoin y donde aplica el uso de las criptomonedas.

TIPOS DE VULNERABILIDADES EN UNA RED DE DATOS DIGITAL

Arquitectura Blockchain

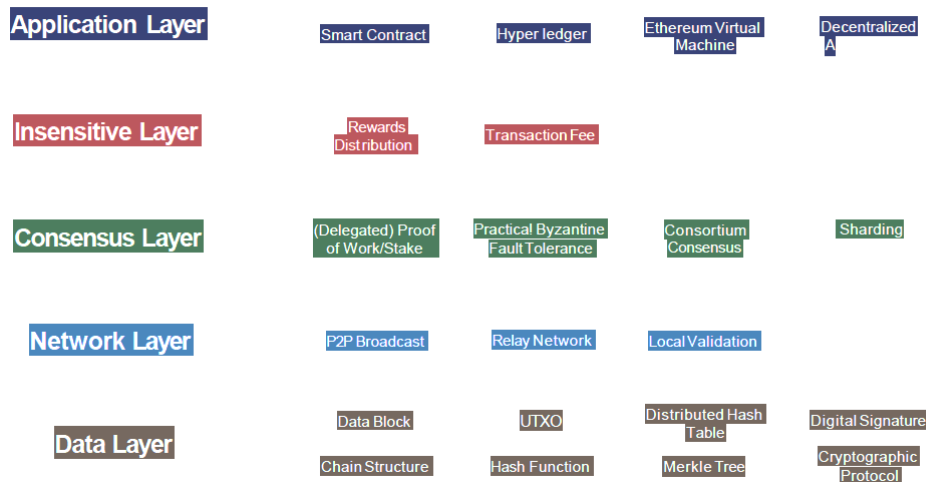


Imagen: Briones, J. (2020)

Cadena de bloques pública

- Una cadena de bloques pública como su nombre indica es la cadena de bloques que está disponible para todos, es decir, es una especie de blockchain que es 'para la gente, por la gente, y de la gente'.
- Nadie está a cargo de la red, y cualquiera puede participar en la lectura / escritura / auditoría de la cadena de bloques.
- Hay reglas más complejas para protegerla de los actores malintencionados.
- Todas las decisiones se toman utilizando el complejo algoritmo de consenso.
- Computacionalmente estas cadenas de bloques son caras para minar y cometer un bloque a través de la red.
- Ejemplo: Bitcoin Blockchain, Ethereum Blockchain, etc.



RIESGOS Y AMENAZAS QUE AFECTAN A LA INFORMACIÓN

Blockchain privado

- Un individuo o una organización opera de forma privada blockchain privada como su nombre lo sugiere.
- A diferencia de la cadena de bloques pública en cadenas de bloques privadas, hay un administrador/ancla que cuida de cosas esenciales como permisos e identidades.
- El consenso se logra sobre los caprichos de la central a cargo que puede proporcionar derechos mineros a cualquier persona o no dar en absoluto.
- En comparación con blockchain público es mucho más rápido y más barato porque uno no tiene que gastar una enorme cantidad de energía, tiempo y dinero para llegar a un consenso.
- Es menos seguro en comparación con la cadena de bloques pública.
- Ejemplos: Bankchain, Medichain, etc.

Consortium Blockchain

Este tipo de blockchain elimina la autonomía individual que se confiere en una sola entidad mediante el uso de cadenas de bloques privadas.

Aquí en lugar de uno a cargo, tenemos más de uno a cargo. Un grupo de empresas o representantes que se unen pueden tomar decisiones en beneficio de toda la red.

Como una forma de lograr las cosas mucho más rápido y también tener más de un único punto de fallas que protege todo el ecosistema.

En pocas palabras, es lo mejor de las cadenas de bloques privadas y públicas.

1. Ofrece opciones para la gestión de derechos y accesos mientras aprovecha la misma cadena de bloques, tecnología y cosechar sus beneficios.

Ejemplos: R3, EWF, etc.

Diferencia

Property	Public	Consortium	Private
Determinación del consenso	Todos los mineros	Algunos minerosseleccionados	Organizaciones participantes.
Permisos	Permisos de lectura para todos	Podría restringirse	Podría restringirse
Inmutabilidad	Casi imposible de manipular	Podría ser manipulado	Podría ser manipulado
Centralizada	No	Parcial	Sí
Eficiencia	Bajo	Alto	Alto
Proveedores de consenso	Sin permiso	Con permiso	Con permiso

Imagen: Briones, J. (2020).



INFORMACIÓN PROTEGIDA BAJO UNA ARQUITECTURA BLOCKCHAIN

Identificar el caso de uso


- La cadena de bloques no es una solución para todos los problemas.
- Hay un montón de bombo, pero es necesario mapear el bombo con el uso.
- Tener un caso de uso concreto es esencial para tejer la solución.
- Some of the widespread use cases are:
 - Payments
 - KYC
 - Smart asset
 - Land Records

Diseñar un flujo de trabajo para la integración de Blockchain

- Analice si necesita una cadena de bloques como solución o si hay otras maneras de resolver el problema existente.
- No empiece a renunciar a las especificaciones técnicas detalladas sin ninguna validación.
- Blockchain debe resolver un problema para los sistemas centralizados existentes, por ejemplo, la rentabilidad, la transparencia y la fiabilidad.
- Tener un diseño factible en la integración de la tecnología en su estrategia de desarrollo.

Identificar el Mecanismo de Consenso

- Dependiendo de su caso de uso, elija el Mecanismo de Consenso.
- Elija el mecanismo que es apto para el caso de uso.
- Por ejemplo, una solución privada de Blockchain puede no requerir un costoso consenso de POW.
- Algunos de los mecanismos de consenso populares son:
 - Proof-of-Work
 - Proof-of-Stake
 - Delegated-Proof-of-Stake

-
- 
- Proof-of-Authority
 - Proof-of-Weight

Identificar la plataforma

- Dependiendo del mecanismo de consenso de su elección, elija la plataforma que se adapte a sus necesidades y planes.
- Blockchain comenzó como código abierto, y hay muchas plataformas disponibles de uso gratuito.
- Algunas de las principales plataformas son:
 - Bitcoin
 - Ethereum
 - Multichain
 - Hyperledger
 - Corda
 - Quorum
 - BigChainDB
 - Stellar



ENCRIPCIÓN DE INFORMACIÓN DIGITAL PARA RESGUARDO

Diseñar la arquitectura

- La arquitectura incluye elementos como la infraestructura, el software y la configuración de hardware.
- La solución puede estar en la nube, local o un modelo híbrido en función de las necesidades de la organización.
- La arquitectura adicional se puede diseñar según permisos, con permiso, público, privado o híbrido.

Diseñar la cadena de bloques

- Debe planificar su instancia cuidadosamente.
- En plataformas específicas, es difícil configurar algunos parámetros una vez establecidos.
- Las cosas que se necesitan bajo configuración pueden ser las siguientes:
 - Permissions
 - Asset Issuance/ Reissuance
 - Atomic Exchanges
 - Key Management
 - Multi-Signature
 - Block Parameters
 - Limits
 - Network Protocols/ Handshaking
 - Key and Address Formats
 - Native Assets



Crear las API para su Blockchain

- Los desarrolladores y las aplicaciones requieren las API para interactuar con su Blockchain.
- Por lo general, las plataformas vienen con API y, si está creando desde cero, debe examinar cuidadosamente el diseño y los esquemas de las API.
- As per your requirements you need to see which APIs to expose for your Blockchain.
- Algunas de las API que puede necesitar:
 - Generating Key Pairs
 - Asset Issuance
 - Data Authentication
 - Checking Blockchain Parameters
 - Create and Read operations
 - Smart Contracts
 - Address Specifications

Diseño del front-end

- Necesita un front-end para sus usuarios y administradores.
- La mayoría de las plataformas funcionan en formato JSON que se puede colaborar con los principales lenguajes de programación.
- Algunas de las plataformas ofrecen SDK para integrar aplicaciones front-end existentes con Blockchain.
- Puede utilizar lenguajes como HTML5, CSS, PHP, C, Java, Javascript, Python, Ruby, Golang, Solidity, AngularJSNodejs.
- Además, también puede utilizar almacenamientos externos como Cloud Storage, NoSQL,
- RDBMS, etc.



PROPUESTAS DE VALOR PARA NEGOCIOS

Perspectivas futuras

- Una vez que tenga la aplicación estable en funcionamiento, puede buscar futuras integraciones con otras tecnologías.
- Puede mejorar el poder de su solución Blockchain integrando Inteligencia Artificial, Biometría, Internet de las cosas, Bots, Cloud, Servicios cognitivos, Contenedores, Análisis de Datos y Machine Learning.

Proyectos de cadena de bloques

El ecosistema Blockchain se está ejecutando actualmente con algunos proyectos importantes y más están en proceso. Algunos de los principales proyectos en Blockchain son:

- Bitcoin - Este proyecto introdujo al mundo a Blockchain.
- Ethereum - Este proyecto vino con el concepto de contratos inteligentes donde dos partes se adhieren a ciertas reglas y crean un fideicomiso. Esto abre el mundo a aplicaciones más descentralizadas.
- Neo - Este proyecto se posicionó como el "Chinese Ethereum" pero compró el Python como el idioma principal para la creación de Aplicaciones.
- Stellar - Este proyecto está tratando de hacer que las transacciones transfronterizas sean más simples. Stellar viene con amplias API que ayudan a los desarrolladores a crear aplicaciones rápidamente, reduciendo así el tiempo de comercialización de las aplicaciones.



ÁREAS DE APLICACIÓN DE BLOCKCHAIN

Usuarios de Blockchain

- Los usuarios de Blockchain son personas normales como tú y yo, que hacen uso de la cadena de bloques o criptomoneda para lograr algunos resultados. También pueden ser inversores que compran criptomonedas para vender en una fecha posterior.
- Para crear una base de usuarios Blockchain la tecnología o criptomoneda debe tener alguna utilidad relacionada con el problema que se está abordando.

Por ejemplo:


- Bitcoin sirve a la principal utilidad de pago de bienes y servicios. Actualmente hay más de 50.000 comerciantes registrados en Bitcoin incluyendo - Microsoft, PayPal y Subway.
- Bitcoin fue el primer impulsor en Blockchain y su alta utilidad como sistema de pago se aseguró de que una gran parte de su ecosistema se basa en los usuarios.

Intercambios de cadenas de bloques

- Cada proyecto Blockchain tiene un ecosistema robusto que trabaja bajo él, y siempre incluye un intercambio descentralizado. Estos son desarrollados por el equipo de Blockchain o la comunidad de otros desarrolladores.
- Un intercambio típico está diseñado para encontrar los tipos de cambio más baratos entre dos criptomonedas, por lo que es más asequible para el comercio de tokens/criptomonedas.
- Los intercambios utilizados para el comercio también pueden integrarse con carteras de hardware, o los usuarios pueden crear su propia cartera en el sitio web de intercambio.

Mineros blockchain

- Para funcionar una cadena de bloques y mantener su integridad, necesita una gran red de nodos independientes en todo el mundo para mantenerla continuamente. En cadenas de bloques privadas, una organización central tiene la autoridad sobre cada nodo de la red. En el caso de las cadenas de bloques públicas, por otro lado, cualquier persona puede configurar su equipo para que actúe como un nodo. Los dueños de estas computadoras se llaman mineros.
- Dado que la integridad de la cadena de bloques está directamente relacionada con el número de nodos independientes en la red, también debe haber algún incentivo para la minería. Diferentes cadenas de bloques utilizan diferentes sistemas de minería, sin embargo, la mayoría de ellos contienen alguna forma de:

-
- 
- An incentive system
 - A consensus algorithm

Desarrolladores de Blockchain

- La tecnología Blockchain se construye por el potencial de los desarrolladores que trabajan detrás de ella. Un equipo sólido de desarrolladores puede conducir a un proyecto Blockchain exitoso. Actualmente existen dos tipos de desarrolladores en el ecosistema blockchain:
 - a. Blockchain developers
 - b. dApp developers
- Los desarrolladores de Blockchain construyen nuevas cadenas de bloques con diferentes niveles de funcionalidades y algoritmos de consenso.
- dApp los desarrolladores trabajan con aplicaciones descentralizadas que se pueden ejecutar en cadenas de bloques proporcionando así una funcionalidad similar como Google Play Store a través de la tecnología Blockchain.
- El desarrollo de contratos inteligentes sobre el Blockchain tiene abierta la posibilidad de que los desarrolladores creen amplias aplicaciones y casos de uso para las industrias.

REDES PÚBLICAS Y PRIVADAS: MÉTODOS DE ACCESO Y RESGUARDO DE LA INFORMACIÓN

Aplicaciones Blockchain

Aparte de los intercambios, plataformas y usuarios, otro aspecto importante del ecosistema Blockchain son las aplicaciones que las industrias, desarrolladores y comunidades construyen para servir a un propósito específico.

Hay varios ejemplos de aplicaciones que se basan en Blockchain, algunas de las principales aplicaciones de trabajo son:

- CryptPad - A decentralized document creation application.
- Humaniq - A fintech startup which connects unbanked people with global economy.
- Augur - A peer to peer oracle and prediction market place.
- Filament - Building the IoT applications over the Blockchain.

Mobile/Web Applications

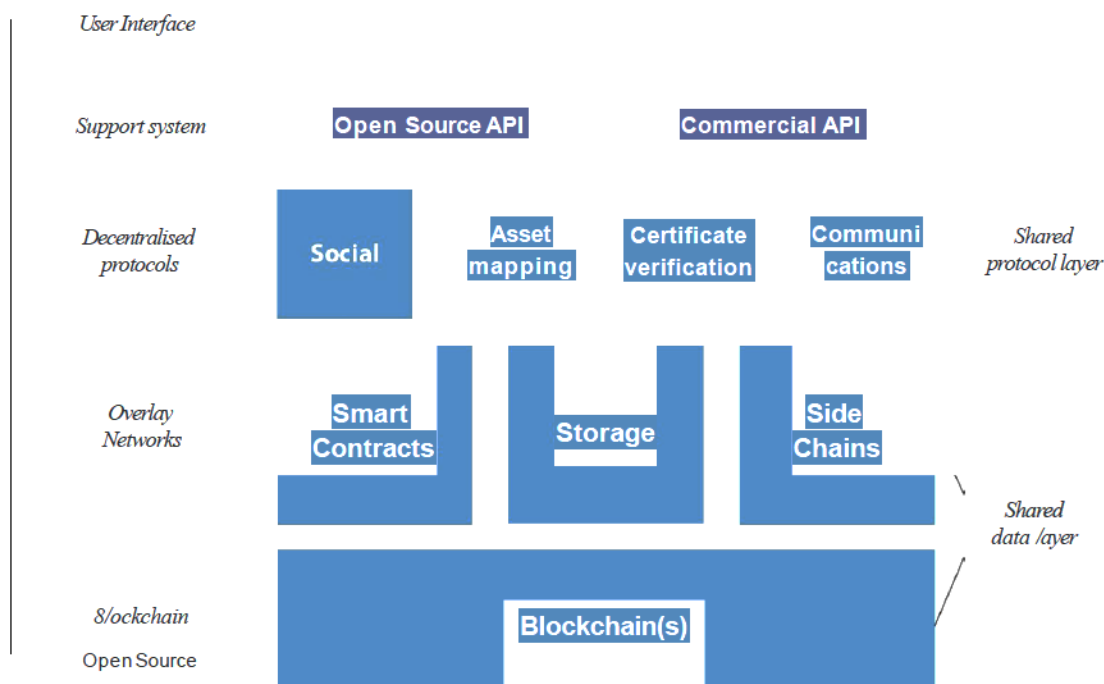


Imagen: Briones, J. (2020)



ESTRATEGIAS Y MÉTODOS PARA LA PROTECCIÓN DE LA INFORMACIÓN EN UN MEDIO DIGITAL

Blockchain

- Esta es la base de todas las aplicaciones basadas en Blockchain.
- Es una red de nodos repartidos por todo el mundo que ejecutan algoritmos para verificar y confirmar transacciones a través de la cadena de bloques.
- Esta es una red descentralizada y en su mayoría basados en algoritmos de criptografía de código abierto.
- Esto se puede crear como público, privado o consorcio.
- Esto también puede incluir autoridades de certificación y servicios de membresía para el gobierno y las empresas.

Superponer redes

- Esta es una red que logra funcionalidad adicional sin arrancar los protocolos originales.
- Se benefician de los efectos de la red y se basan en eso.
- Algunas de las funcionalidades adicionales que logra son:
 - Contratos inteligentes - acuerdos criptográficos entre dos partes
 - Almacenamiento - red de alquiler
 - Sidechains: transfiera tokens de una cadena de bloques a una cadena de bloques
 - diferente.

Protocolos descentralizados

- La suya es la parte esencial de la pila de tecnología Blockchain, ya que se asegura de que la capa Blockchain y las redes de superposición no dependan de una sola entidad para la validación y las transacciones.
- Ayuda a crear conjuntos de datos descentralizados punto a punto.
- Los protocolos descentralizados pueden basarse en la asignación de activos, las identidades sociales, los algoritmos de verificación o los canales de comunicación.



Sistema de soporte

- Para crear aplicaciones de Blockchain, necesita que las API interactúen con la tecnología underneath.
- Puede crear directamente una solución con las API existentes, sin depender y trabajar en el libro mayor.
- Más APIs responder al formato JSON, por lo que se puede integrar fácilmente con las tecnologías front-end existentes.
- Puede utilizar las API de código abierto como Bitcoin y Ethereum, o puede elegir entre LAS API comerciales como block.io o blockcypher para más funcionalidades en caja.

Interfaz de usuario

- Por último, se requiere una interfaz de usuario para que los usuarios se conecten a su Blockchain.
- La interfaz de usuario se puede construir con mecanismos front-end existentes y puede emplear fácilmente el poder de Blockchain mediante el uso de APIs.
- Algunas plataformas como Hyperledger también proporcionan generadores para producir una interfaz de usuario de caja para las aplicaciones creadas para abrirlas.
- La mayoría de las plataformas Blockchain también proporcionan servicios de conexión para vincular Aplicaciones a Blockchain.

BITCOIN

- Es un sistema de pago digital y criptomoneda mundialmente conocido.
- Primera moneda digital descentralizada cuyo libro mayor es mantenido por Blockchain abiertamente y nos dio el sabor de la cadena de bloques.
- Fue fundada por una persona desconocida o grupo de personas y lanzado como software de código abierto en 2009.
- Punto a punto.
- Las transacciones tienen lugar entre usuarios directamente, sin intermediarios.
- Los nodos de red comprueban estas transacciones y las registran en un libro mayor distribuido público denominado Blockchain.



Imagen: Freepik, "Bitcoin", consultada en diciembre del 2020, disponible en: https://www.freepik.es/vector-gratis/moneda-oro-palabra-bitcoin_2094980.htm#page=2&query=bitcoin&position=23

Características que diferencian Bitcoin de las monedas fiduciarias:

- Sistema descentralizado: El control de Bitcoin no está centralizado. Los nodos/ordenadores trabajan juntos para extraer la moneda y procesar las transacciones que forman la red, sin necesidad de una autoridad central.
- Proceso de configuración simple: Los bancos regulares le hacen pasar por una gran cantidad de procesos para abrir una cuenta. Sin embargo, el proceso de configuración de criptomoneda es sencillo y gratuito.
- Uso anónimo y transparente: Los usuarios pueden tener muchas direcciones Bitcoin sin un enlace a ninguna información de identificación personal. Sin embargo, registra cada transacción en un libro de contabilidad gigante llamado Blockchain.
- Tarifa de transacción escasa: Bitcoin cobra una tarifa mínima por las transferencias internacionales.
- Proceso de red rápido: El proceso de pago es rápido en la red Bitcoin.
- No reembolsable: Una vez enviado, bitcoins no pueden ser reembolsados.

ETHEREUM

- Ethereum es una plataforma de software de código abierto que se basa en la tecnología Blockchain que permite a los desarrolladores crear e implementar aplicaciones descentralizadas como contratos inteligentes.
- Ofrece una máquina virtual descentralizada también conocida como máquina virtual Ethereum que puede ejecutar scripts utilizando una red distribuida globalmente de nodos públicos.
- Lanzado por Vitalik Buterin a finales de 2013.
- El desarrollo para ethereum fue financiado por una venta masiva pública en línea durante julio-agosto de 2014, mediante la compra del token Ethereum (Ether).

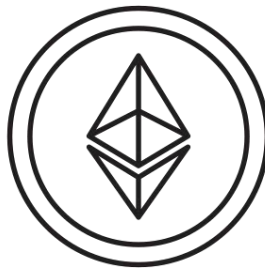


Imagen: Briones, J. (2020)

- La primera red de versiones preliminares beta públicas conocida como "Olímpico". La red olímpica proporciona a los usuarios una recompensa por error de 25.000 éteres para probar los límites de Ethereum Blockchain.
- El Blockchain en vivo de Ethereum llamado "Frontier" fue lanzado el 30 de julio de 2015.
- El hito actual se llama "Homestead" y se considera estable. Como ha llevado a varias mejoras como el procesamiento de transacciones, los precios del gas y la seguridad.
- Hay al menos otras dos mejoras de protocolo planeadas para el futuro, es decir, Metrópolis y Serenity (Prueba de estaca).

NEO

- NEO es una economía inteligente para la red distribuida.
- NEO fue elegido como el nombre porque "NEO" en griego significa, "novedad, novedad y juventud".
- NEO inicialmente se llamó AntShares (ANS) que fue lanzado en 2014, fundada por Da Hongfei y Erik Zhang.
- Antshares anunció el 22 de junio de 2017, que planeaba cambiar su nombre como NEO.
- El primero ICO en la cadena de bloques NEO, Red Pulse Token (RPX) fue anunciado poco después de que el cambio de marca terminó.
- Aparte de la criptomoneda NEO en sí, la plataforma NEO tiene otro crypto-token llamado "GAS" que anteriormente se llamaba "ANC-Antcoins."



Imagen: Briones, J. (2020)

HYPERLEDGER

- Hyperledger es un código abierto creado para avanzar en las tecnologías blockchain entre industrias.
- Es una colaboración global, organizada por The Linux Foundation, incluyendo líderes en finanzas, banca, Internet de las cosas, cadenas de suministro, fabricación y tecnología.
- Hyperledger actúa como un sistema operativo para mercados, redes de intercambio de datos, microdivisas y comunidades digitales descentralizadas. Tiene el potencial de reducir enormemente los gastos y complicaciones para hacer las cosas en el mundo real.



HYPERLEDGER

Imagen: Briones, J. (2020)

EOS

- EOS es un sistema operativo para mercados, redes de intercambio de datos, micro-monedas y comunidades digitales descentralizadas. Tiene el potencial de reducir enormemente los gastos y complicaciones para hacer las cosas en el mundo real.
- EOS Blockchain tiene como objetivo convertirse en un sistema operativo descentralizado que puede soportar aplicaciones descentralizadas a escala industrial.
- EOS está planeando eliminar las tarifas de transacción. EOS afirma tener la capacidad de realizar millones de transacciones porsegundo.
- EOS se ejecuta en el algoritmo de consenso DPOS



Imagen: Briones, J. (2020)



CORDA

- Corda es una cadena de bloques de código abierto con el objetivo de cumplir con los requisitos para el uso de blockchain en las empresas.
- Corda ofrece una solución en la que se puede iniciar un libro mayor compartido entre las partes en virtud del contrato.
- Las comunicaciones de Corda son punto a punto, lo que significa que solo los participantes de una transacción pueden verla.
- Con la arquitectura punto a punto de Corda, los participantes solo tienen copias de las transacciones a las que son participantes u observadores. Esto significa que es probable que cada nodo de una red corda tenga un libro mayor único. Esto se denomina libro mayor multilateral.



Imagen: Briones, J. (2020)

QUORUM

- Quorum es la creación de J.P. Morgan trayendo en la versión centrada en la empresa de Ethereum.
- Quorum proporciona ejecución de contratos inteligentes privados y rendimiento de nivel empresarial.
- Quorum utiliza la criptografía zk-Snarks que permite la verificación de la corrección del cálculo sin siquiera aprender lo que se ejecutó.
- Quorum utiliza un diseño de privacidad híbrido.





MULTICHAIN

- Multichain fue creado por Gideon para poner a disposición una solución blockchain para que las organizaciones construyan y desarrollen rápidamente.
- Multichain se basa en Bitcoin Blockchain, pero ofrece la funcionalidad de Permisos, Transmisiones y Activos
- Multichain también proporciona otras herramientas como exploradores para interactuar con el subrayado Blockchain sin problemas.
- Bankchain está usando Multichain ya que es base.



CONSUMO DE ENERGÍA

- Algunas cadenas de bloques públicas importantes utilizan algoritmos de prueba de trabajo.
- PoW implica el uso del poder computacional de una máquina para resolver un rompecabezas matemático complejo para verificar una transacción y agregarla a un bloque.
- El consumo actual de energía Bitcoin es casi igual al consumo de Irlanda.
- Para 2020 se estima que Bitcoin utilizará más consumo de energía que el mundo entero utiliza actualmente.
- Una solución probable para esto ha surgido en forma de diferentes mecanismos de consenso como la prueba de estaca, la prueba de dec.

Escalabilidad

- La escalabilidad ha aparecido como un problema significativo para las redes Blockchain como Bitcoin y Ethereum.
- Las cadenas de bloques están teniendo problemas para dar soporte efectivo a un gran número de usuarios en la red.
- Además, el tamaño de las cadenas de bloques públicas sigue aumentando. Actualmente, el tamaño del libro mayor de Bitcoin es superior a 100 GB.
- Una posible solución que ha surgido es almacenar un hash de datos a través de la red.

Percepción pública

- En la actualidad, la tecnología blockchain es casi sinónimo de Bitcoin.
- La mayoría del público sigue siendo ajeno a la existencia y los usos potenciales de la tecnología Blockchain.
- Como Bitcoin es anónimo y se utiliza para los negocios sombríos de lavado de dinero, comercio del mercado negro, y otras actividades ilegales. La cadena de bloques también está recibiendo una mala reputación debido a la misma.
- La adopción principal es necesaria para eliminarlos matices a veces negativos de Bitcoin.

Normas y Reglamentos de Blockchain


-
- 
- Las cadenas de bloques están en continua evolución, pero aún así, los países son escépticos al respecto, ya que no existe una definición adecuada para las normas y regulaciones.
 - Las empresas y los gobiernos requieren regulaciones para proteger a sus clientes.
 - Para abordar este problema, algunos países están tratando de lanzar sus regulaciones sobre la tecnología.
 - La adopción masiva también podría estandarizar la cadena de bloques.



Imagen: Briones, J. (2020)

Industrias actuales que utilizan Blockchain

- Productos farmacéuticos - DHL trabajó con Accenture para establecer un sistema de seguimiento y seguimiento basado en blockchain en seis áreas en todo el mundo. Actualmente, el sistema tiene 7 mil millones de números de serie farmacéuticos únicos y maneja más de 1.500 transacciones por segundo.
- Moda - CGS ha desarrollado un sistema de seguimiento de prendas y cumplimientos de materias primas para muchos clientes de ropa y moda.
- Pagos transfronterizos - IBM ha desarrollado una nueva solución de banca blockchain que permite a las instituciones financieras moverse de forma rápida y rentable procesando pagos a nivel mundial.
- Seguridad Alimentaria - IBM se ha asociado con Dole, Nestlé y Walmart para establecer una cadena de bloques para una mejor regulación de los alimentos.
- Naciones Unidas - Las Naciones Unidas utilizan actualmente Blockchain para 16 organismos, incluidos la trata de personas y el Programa Mundial de Alimentos.
- Joyería - Brilliant Earth se ha asociado con Everledger para usar blockchain en el seguimiento y seguimiento de la procedencia de diamantes y otras piedras preciosas. Esto también garantizará que estén libres de conflictos.

Revolución de la cadena de bloques

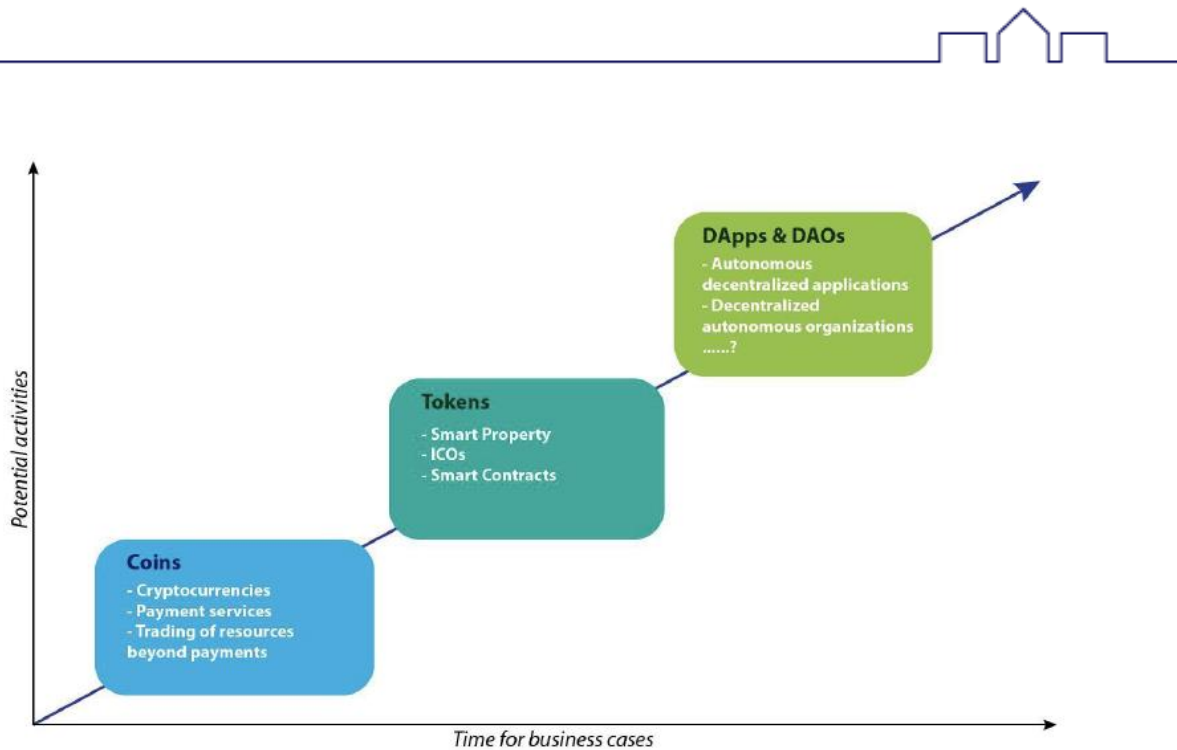


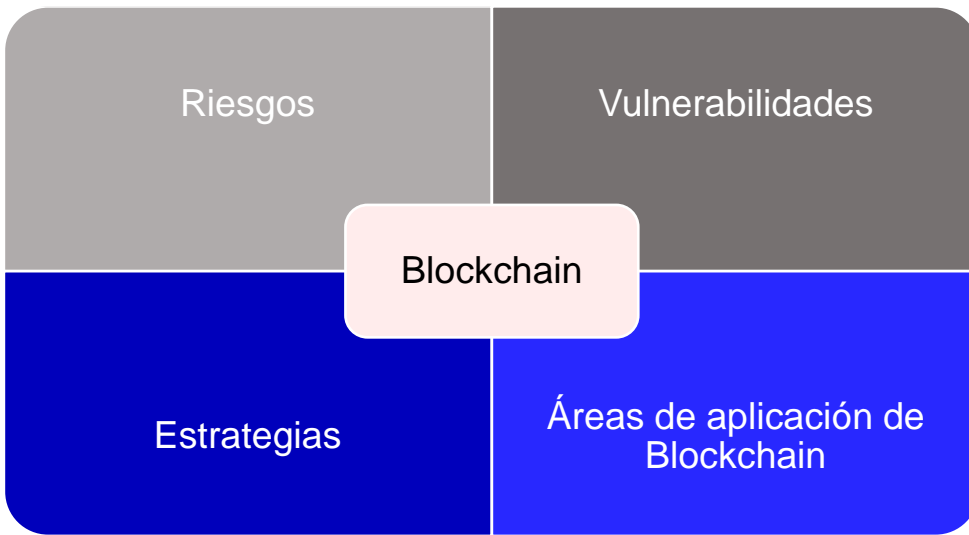
Imagen: Briones, J. (2020).

Interrupciones emocionantes próximamente

- Entertainment Industry - Movie Braid fue la primera película en ser producida por hacer un ICO.
- Alquiler de propiedades - Rentberry tiene como objetivo abordar los escollos comunes y dolores de cabeza del modelo de alquiler tradicional.
- Política - Sierra Leona llevó a cabo sus elecciones en Blockchain.
- Educación - Sócrates Coin está haciendo grandes movimientos para cambiar el enfoque tradicional a un "3DInternet".
- Publicidad digital - Basic Attention Token está tomando una grieta para resolver los problemas con los anuncios digitales.
- Internet de las cosas - Waltonchain, un galardonado proyecto chino que busca integrar la tecnología IoT y blockchain a una escala sin precedentes.



IDEAS CLAVES






CONCLUSIONES

Blockchain es una cadena continua de bloques que contiene información con una secuencia estricta de su creación: un nuevo bloque siempre llega exclusivamente al final de un enlace. Alineándose de esta manera cronológica y criptográficamente en una especie de cadena inextricable, regularmente cubierta de nuevos contenidos.

LINKS/MATERIAL MULTIMEDIA

MÓDULO: Ciberseguridad Aplicada I		Unidad: 2
Recurso	Descripción	
 Video	EALDE bussines school (2018), <i>La irrupción de Blockchain en la gestión de Riesgos globales</i> , consultado en diciembre del 2020, disponible en: https://www.youtube.com/watch?v=BldgAemznY8	



BIBLIOGRAFÍA

- Gómez, B & Blanco, D. (2018), *Blockchain, así es la nueva revolución de internet*, consultado en diciembre, disponible en: <https://www.paradigmadigital.com/techbiz/blockchain-asi-es-la-nueva-revolucion-de-internet/?prs=1BLOCKCHAIN> <http://paradig.ma/blockchain>
- Ministerio de Economía, Fomento y Turismo (s.f), *Blockchain: un camino a la 4ta revolución industrial*, consultado en diciembre, disponible en: <https://www.economia.gob.cl/wp-content/uploads/2019/03/libroblockchain-VB-31AGO-v3.pdf>
- Kuchkovsky, C; Fernández, R & Molero, I. (2017), *Blockchain: la revolución industrial de internet. Cap.1-2*, PAIDOS EMPRESA.
- Piscini, E & Kehoe, L (2018), *Blockchain-Ciberseguridad*, consultado en diciembre, disponible en: [https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain&%20CiberseguridadESP%20\(1\).pdf](https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain&%20CiberseguridadESP%20(1).pdf)