Blockchain

ADR – UTN – FRBA -2020

Agenda

- Que es blockchain?
- Conceptos técnicos fundamentales
- Principios de blockchain
- Secuencia de pasos. ¿Cómo funciona Blockchain?
- Ventajas y desventajas
- Usos de blockchain
- BaaS - Blockchain as a service.

¿Qué es Blockchain?

Blockchain es una red peer-to-peer que no depende de ninguna entidad centralizada para llegar a un consenso. Es una tecnología de registro distribuido donde cada par tiene su propia copia del registro. Una vez que se realiza una transacción, se asigna a un bloque para su verificación a través del método de consenso utilizado por blockchain. El bloque de transacción se extrae o se valida a través de otros procesos. Si se confirma la transacción, ya no se puede alterar ni modificar de ninguna manera posible.

Más información relacionada:
https://bfa.ar/blockchain/blockchain
https://101blockchains.com/

Conceptos técnicos

- **P2P:** Protocolo de Red de comunicación entre pares. Ejemplos: Emule, torrent, etc.
- **Algoritmo de Hash:** Una función criptográfica hash usualmente conocida como “hash” es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.
- **Criptografía Asimétrica:** Consiste de la posesión de 2 claves, una pública y otra privada. Se pueden aplicar a contenidos (strings) una firma con la clave privada a través de una función de hash F y se puede validar con otra función F1 que solo el tenedor de la clave privada firmó ese contenido.

Conceptos técnicos

- **Proof of Work (PoW):** Conceptualmente es requerir un trabajo, que luego es verificado por la red. Normalmente el trabajo solicitado, consiste en realizar operaciones de cómputo que demuestran que alguien realizó un esfuerzo.

- **Consenso:** El consenso consiste en que toda la red está de acuerdo con el resultado de una prueba

Principios de Blockchain

Principios sobre los que se basa el diseño de Blockchain

- **Integridad en la red:** La integridad está cifrada en todas y cada una de las etapas del proceso y distribuida, y no depende de cada miembro individualmente. Comportarse sin integridad o es imposible, o cuesta mucho más tiempo, dinero, energía y reputación.
- **Poder distribuido:** El sistema distribuye poder por una red de iguales sin que haya ningún punto de control. Las partes no pueden apagar el sistema por sí solas. Si una autoridad central lograra inhabilitar o expulsar a un individuo o a un grupo, el sistema sobreviviría. Si la mitad de la red intentara dominar al conjunto, todo el mundo lo vería.

Más información relacionada:
Libro: Blockchain revolution

Principios de Blockchain

- **El valor como incentivo**: El sistema alinea los incentivos de todos los ‘stakeholders‘ y, por lo tanto, todos los intereses. El bitcoin o algún tipo de valor es parte esencial de esta alineación y correlativo a la reputación

- **Seguridad**: Las medidas de seguridad están integradas en toda la red sin puntos flojos y no solo garantizan la confidencialidad, sino también la autenticidad de todas las actividades y la imposibilidad de que sean negadas (no repudio)

Más información relacionada:
Libro: Blockchain revolution

Principios de Blockchain

- **Privacidad:** En una red blockchain, las personas pueden controlar sus propios datos y qué y cuándo quieren compartir con terceros. Al eliminarse la necesidad de confiar en los otros se elimina la necesidad de conocer la verdadera identidad de esos otros para interactuar con ellos.

- **Preservación de derechos:** Los derechos de propiedad son transparentes y legítimos. Las libertades individuales están reconocidas y son respetadas.
  Blockchain no sólo impide el doble gasto, sino que también confirma la propiedad de todas y cada una de las monedas en circulación, y cada transacción es inmutable e irreversible.

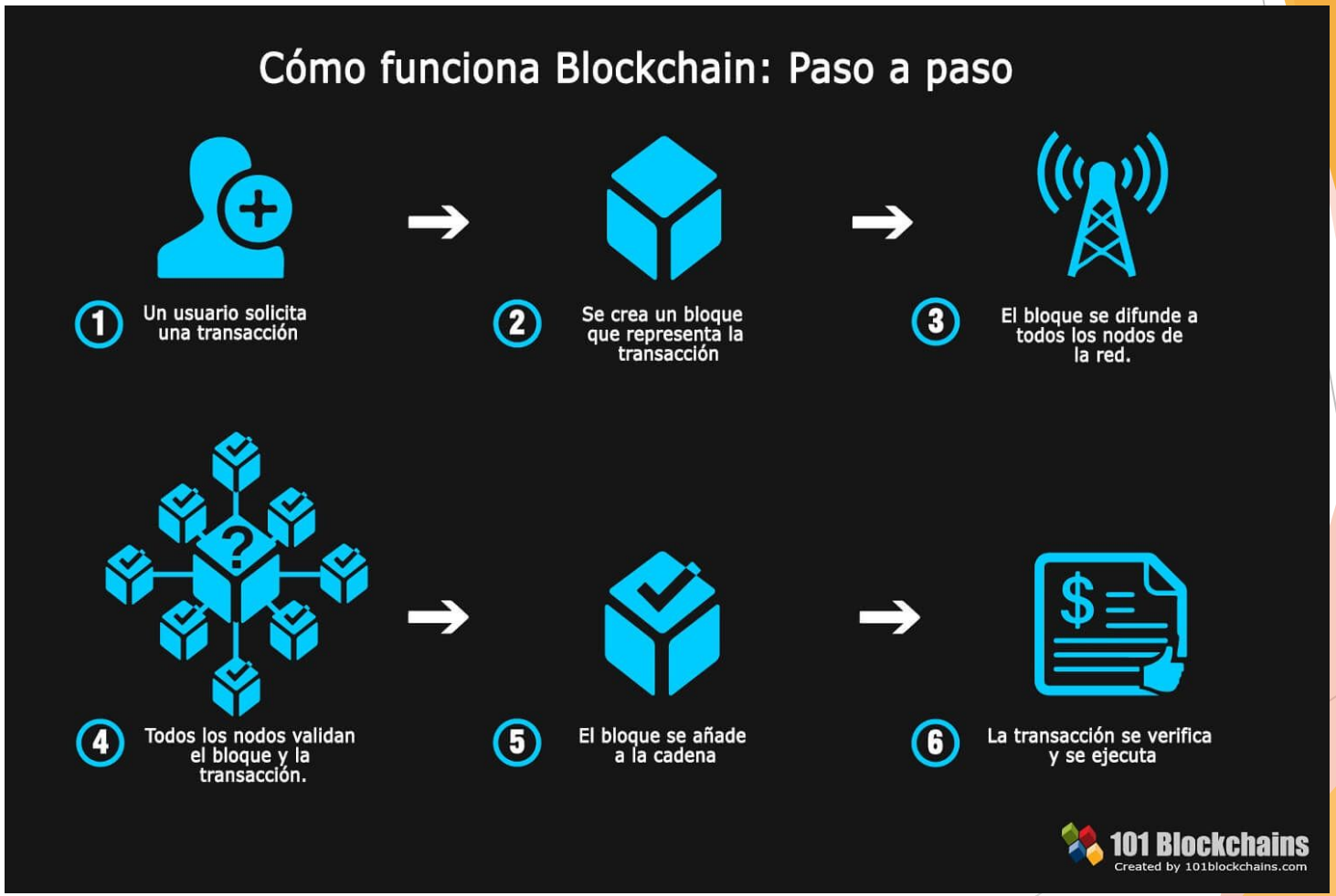
Más información relacionada:
Libro: Blockchain revolution

Principios de Blockchain

- **Inclusión:** La economía funciona mejor cuando funciona para todos. Eso significa eliminar obstáculos que dificulten la participación. Significa crear nuevas plataformas que hagan posible un capitalismo distribuido, no simplemente un capitalismo redistribuido

Más información relacionada:
Libro: Blockchain revolution

Secuencia de Pasos



Otros Usos de Blockchain

Dada la naturaleza de imposibilidad de alterar una red blockchain, es adecuada para: los contratos, libros contables, libros de registros, registros automotores, historias clínicas, escrituras de propiedades y todo tipo de proyectos donde se necesiten registrar datos y que sean confiables. Para todos estos casos, este tipo de red es ideal.

Usos de Blockchain

BFA- Blockchain Federal Argentina

Es una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre blockchain.

Modelo

- **Sin criptomoneda**
- **Modelo liviano**
- **Permisionada**
- **Transacciones gratuitas**
- **Almacenamiento Off-Chain**
- **Software libre**

Más información relacionada:
https://bfa.ar/

Ventajas y Desventajas

Ventajas

- **Naturaleza Distribuida:** Cada nodo de la red es capaz de replicar y almacenar una copia de la base de datos y, como resultado de esto, no hay un “single point of failure” (punto único de fallo): un único nodo que se desconecta no afecta a la disponibilidad o seguridad de la red.

- **Estabilidad:** Es muy improbable que los bloques confirmados sean revertidos, lo que significa que una vez los datos han sido registrados en la blockchain, es extremadamente difícil eliminarlos o cambiarlos

Ventajas y Desventajas

Ventajas

- **Sistema "Trustless":** no requiere confiar en terceros. Evita el riesgo de tener que confiar en una organización individual, y reduce también los costes generales y comisiones por transacción al suprimir intermediarios y terceras partes
- **Incorruptible:** la alteración de la información contenida en los bloques se vuelve algo prácticamente imposible. Para empezar, siempre que se desee cambiar cualquier dato de un bloque, es necesario **cambiar todos los bloques de esa cadena**. Y eso significa también **rehacer todo el *proof-of-work*** asociado a los bloques.

Ventajas y Desventajas

Ventajas

- **Mayor Velocidad:** La ausencia de una autoridad central o intermediarios hace que la información esté al alcance de todos los participantes de la red in situ. La **simplificación del proceso de transmisión** de datos lleva inherente una mayor velocidad.
- **Transparencia:** Ofrece **una visión más clara de la procedencia de las transacciones.** Cualquiera puede consultar las transacciones en el registro, incluso verificarlas.

Ventajas y Desventajas

Ventajas

- **Trazabilidad:** Cada bloque de la cadena almacena información y los bloques se encuentran vinculados entre ellos. Gracias a ello, las organizaciones pueden **rastrear la información de forma más sencilla y procesar el historial de forma permanente.** Se crea así un mecanismo de trazabilidad que puede ayudar a las organizaciones a hacer un seguimiento único de cualquier transacción.
- **Libre de errores:** Como existe una red de nodos que comprueban los datos constantemente, y como la información es acordada por todos, los resultados son siempre **comprobados y correctos**. Y como existe una red de nodos, cada uno con una copia de la blockchain, la información contenida en ésta **difícilmente pueda perderse**.

Ventajas y Desventajas

Desventajas

- **Ataques del 51%:** Un ataque de este tipo puede tener lugar si una entidad logra hacerse con el control de más del 50% del hashing power (o tasa de hash) de la red, lo que eventualmente podría permitirle desorganizar la red mediante la exclusión o modificación intencionada del orden de las transacciones.
- **Modificación de datos:** una vez se han añadido datos a la blockchain, resulta muy difícil modificarlos. A pesar de que la estabilidad es una de las ventajas de las blockchains, ésta no siempre tiene por qué ser buena. El cambio de datos o código de una blockchain es habitualmente muy complicado y, a menudo, requiere de un hard fork -por el que una cadena es abandonada, y una nueva es retomada.

Ventajas y Desventajas

Desventajas

- **Claves Privadas:** El Blockchain utiliza criptografía asimétrica para otorgar a los usuarios la propiedad de los datos. Cada cuenta de la blockchain (o dirección) dispone de dos claves correspondientes: una clave pública (que puede ser compartida) y una clave privada (que debe ser mantenida en secreto). Los usuarios necesitan sus claves privadas para acceder a los datos. Si un usuario pierde su clave privada, perderá también sus datos (en el caso de BTC dinero), y no hay nada que pueda hacerse al respecto.
- **Ineficiente**:Las blockchains, especialmente aquellas que usan Proof of Work, son altamente ineficientes. Se ha producido en los últimos años un incremento notable de los recursos empleados por la red Bitcoin -hasta el punto que ésta, en la actualidad, consume más energía que muchos países como Dinamarca, Irlanda o Nigeria.

Ventajas y Desventajas

Desventajas

- **Almacenamiento:** Los libros contables (ledgers) blockchain pueden crecer mucho con el paso del tiempo. La blockchain de Bitcoin requiere actualmente en torno a 200 GB de almacenamiento

- **Apertura:** Al ser una red abierta, cualquier ente puede consultar los datos presentes e históricos de cualquier otro.

Ventajas y Desventajas

Conclusión:

Como en casi todos los aspectos del análisis de un producto, servicio, una situación o problema, gran parte del mismo debe realizarse teniendo presente las variables del contexto.
La clasificación de las características anteriores dentro de las categorías de ventaja - desventaja, pueden variar dependiendo del problema que se busca solucionar.
Por ejemplo: la característica de anonimidad puede resultar una desventaja si se evalúa desde el punto de vista o lo zapatos de una entidad fiscalizadora (por ejemplo, el estado). Pero puede tornarse una ventaja si se analiza desde el punto de vista de un usuario final el cual puede sentir mayor seguridad en el resguardo de su información personal. El mismo concepto puede aplicarse al resto de las características enunciadas anteriormente.

Lo importante de la tecnología Blockchain es que presenta características que la hacen **única**, y esto le adjudica un diferencial respecto a otras herramientas del mercado.

Más información relacionada:

https://academy.binance.com/es/blockchain/positives-and-negatives-of-blockchain
https://www.izertis.com/es/-/blog/cinco-beneficios-de-blockchain-en-las-empresas
https://www.emprendices.co/blockchain-cuales-ventajas-desventajas/
https://mersanlaw.com/la-revolucion-de-la-blockchain-y-los-smart-contracts/
https://www.santalucia.es/blog/cadena-de-bloques-o-blockchain/

Posibles ataques

Doble Gasto: El doble gasto es un defecto potencial del dinero digital por el que una misma moneda digital (a la que también se llama token) puede gastarse más de una vez. Esto es posible porque cada moneda consta de un archivo digital que puede duplicarse o falsificarse

Redes Fantasma: Red impostora donde con operaciones falsas.

Nota: El protocolo de blockchain resuelve ambos problemas.

Más información relacionada:

https://academy.binance.com/es/security/double-spending-explained
https://es.cointelegraph.com/explained/double-spend-or-double-spend-attack-in-bitcoin-myth-or-reality

Blockchain as a Service

¿Qué es BaaS?

Blockchain-as-a-Service (BaaS) es la creación y gestión de redes basadas en la nube por parte de terceros para empresas en el negocio de la creación de aplicaciones blockchain. Estos servicios de terceros son un desarrollo relativamente nuevo en el creciente campo de la tecnología blockchain. El negocio de la tecnología blockchain ha ido mucho más allá de su uso más conocido en transacciones de criptomonedas y se ha ampliado para abordar transacciones seguras de todo tipo. Como resultado, existe una demanda de servicios de alojamiento.

Blockchain as a Service

¿Cómo Funciona?

Un proveedor de BaaS configura y administra la tecnología y la infraestructura blockchain para un cliente. El cliente paga una tarifas al proveedor de BaaS por el uso del servicio.
Es responsabilidad del prestador del servicio mantener en funcionamiento la infraestructura de blockchain.
Se rige bajo las normas generales de cualquier prestación de servicio. Puede implementarse un SLA.

Blockchain as a Service

Factores determinantes para elección de plataforma BaaS:

- **Integración con contratos inteligentes:** Dado que las plataformas BaaS son inmutables, las pruebas y la implementación de contratos inteligentes son bastante complicadas para los desarrolladores. Es crucial tener en cuenta que blockchain como empresa de servicios le proporciona la integración de contrato inteligente con la implementación.
- **IAM(Identity Access Management) Platforms:** Una red autorizada permite a los usuarios acceder a información o capas específicas. La integración de una plataforma de gestión de identidades hará que la red blockchain sea totalmente segura y podrá otorgar permisos a las personas.

Blockchain as a Service

Factores determinantes para elección de plataforma BaaS:

- **Runtimes y Frameworks diferentes:** Algunos proveedores de BaaS solo admiten un tipo de implementación de blockchain empresarial. Elegir un BaaS que admita una amplia gama de entornos de ejecución y marcos ayudará a aportar flexibilidad y portabilidad.
- **Mecanismos de consenso basados en la identidad:** la prueba de trabajo no ofrece la escalabilidad suficiente que necesita la solución de nivel empresarial. Por lo tanto, ante un escenario de gran escalabilidad, se debe tener en cuenta que los proveedores de blockchain como servicio trabajen en un mecanismo de consenso que no dependa del cálculo, sino de un algoritmo de consenso basado en identidad.

Blockchain as a Service

Análisis de Costos: oferta de BaaS frente a blockchain on premise

Cuando se trata de analizar el costo de la aplicación Blockchain on premise, se espera que el costo total de propiedad (TCO) sea alto debido a los costos de inicio (infraestructura, personal, software, licencias, hardware, consultoría y más), costos de retiro (desmantelamiento de racks de servidores) y costos operativos (monitoreo, costo por transacciones, gastos de ancho de banda). Además, el costo de construir e implementar un solo contrato inteligente bajo el modelo anterior puede costar hasta cien mil dólares.
Una aplicación blockchain alojada en la nube como parte de la oferta de BaaS se puede comprar por alrededor de USD 0.29 por hora de CPU asignada. Significa que tendrá que pagar sobre la marcha, es decir, deberá pagar solo por las unidades de servicios utilizados.

Blockchain as a Service

Análisis de Costos: oferta de BaaS frente a blockchain on premise

Los costos reales en el modelo BaaS dependen de factores como la tasa de transacción, el número máximo de transacciones simultáneas, el tamaño de la carga útil de las transacciones, etc.
Por ejemplo, el precio del servicio Amazon AWS Managed Blockchain depende de factores como los nodos de pares, los datos escritos en la red, la pertenencia a la red, la transferencia de datos y el almacenamiento de los nodos de pares.

Más información relacionada:
https://aws.amazon.com/es/managed-blockchain/pricing/

Grandes Jugadores

Microsoft

Microsoft es uno de los primeros proveedores en proporcionar BaaS cuando fundó Azure Blockchain Service en 2015. Se unieron a Consensys para desarrollar Microsoft Azure, que se basa en Ethereum Blockchain. El servicio tiene como objetivo permitir a los desarrolladores y clientes empresariales experimentar con la tecnología blockchain con un "entorno de desarrollo de blockchain basado en la nube con un solo clic".
Blockchain-as-a-Service de Microsoft Azure también permite a sus usuarios construir entornos de blockchain públicos, privados y de consorcio con marcos de nivel industrial y llevar sus aplicaciones de blockchain al mercado. Al integrar el sistema de asistencia virtual basado en IA, Cortana, Azure ayuda a sus usuarios a comprender e implementar la tecnología de contabilidad distribuida.

Características de Microsoft Azure:

Admite múltiples marcos de blockchain, incluidos Quorum, Corda, Hyperledger Fabric y Ethereum.
Implementación sencilla con la CLI de Azure, Azure Portal o Visual Studio Code con Azure Blockchain Extension.
Gestión de consorcio incorporada para gestionar miembros de la red.
Monitoreo y registro completo

Grandes Jugadores

Amazon

Al igual que otras grandes organizaciones, Amazon también ha presentado su oferta de BaaS llamada "Amazon Managed Blockchain". Amazon Managed Blockchain es un servicio completamente administrado que permite a sus usuarios configurar y manejar una red de blockchain escalable con solo unos pocos clics.

Amazon Managed Blockchain admite dos marcos de desarrollo populares de blockchain, Ethereum e Hyperledger Fabric, lo que facilita a los clientes la administración de redes blockchain públicas y autorizadas a través de un único servicio administrado. Al proporcionar una variedad de tipos de instancias que incluyen diferentes combinaciones de memoria y CPU, la oferta de BaaS de Amazon le brinda la flexibilidad de seleccionar los recursos adecuados para su carga de trabajo.

Características de Amazon Managed Blockchain:

- Totalmente administrado.
- Admite Hyperledger Fabric y Ethereum.
- AWS Key Management Service para proteger la CA (autoridad certificadora) de Hyperledger Fabric.
- Utiliza la tecnología de Amazon QLDB para administrar el servicio de pedidos aumentado.

Grandes Jugadores

R3

ChainStack, una plataforma blockchain como servicio, lanzó su servicio de corda R3 administrado que brinda a las empresas acceso a la implementación con un solo clic de los nodos Corda basados en la nube.
La plataforma Corda R3 administrada reduce el tiempo de implementación de los nodos de blockchain a unos pocos minutos, lo que permite a las empresas, los socios de R3 y los gobiernos alojar la red Corda con solo tres clics.
Basado en la última versión de Corda 4.1, los desarrolladores pueden desarrollar sus redes privadas para entornos de prueba e instalar CorDapps en los nodos de la red privada. Conduce a esfuerzos y recursos reducidos y ofrece escalabilidad en un período más corto. Los desarrolladores ya no necesitan centrarse en el mantenimiento de las redes.

Características del servicio R3 Corda:

- Implementación sencilla basada en la nube y configuración rápida de nodos con Docker.
- Firewall de aplicaciones blockchain incorporado para proporcionar seguridad adicional.
- La función de interoperabilidad de R3 permite a los desarrolladores operar con más de una aplicación a la vez.

Grandes Jugadores

SAP Cloud Platform Blockchain

También llamado "Leonardo", SAP Blockchain-as-a-service reside en SAP Cloud Service y no requiere ningún software o hardware en las instalaciones. Al eliminar la necesidad de una gran inversión de capital inicial, Leonardo de SAP permite utilizar estándares abiertos para desarrollar redes de cadenas de bloques privadas y de consorcio.
La plataforma Blockchain-as-a-service de SAP funciona como un servicio blockchain en la nube, un servicio de aprendizaje automático y brinda soporte a IoT dentro de un único ecosistema.

Características de Leonardo de SAP:

- Cloud Deployment.
- Monitoreo de datos de blockchain en tiempo real.
- SAP Cloud Platform para Blockchain permite prototipar, construir y probar contratos inteligentes y blockchain.
- Dado que encontrará muchas plataformas de blockchain como servicio en el mercado, debe considerar algunos factores en función de los cuales puede seleccionar el proveedor BaaS ideal para su caso de uso de blockchain.

BaaS

Referencias

https://www.trustradius.com/blockchain-as-a-service-baas

https://medium.com/hackernoon/what-is-blockchain-as-a-service-28667754d6dc

https://news.bitcoin.com/7-of-the-worlds-largest-blockchain-as-a-service-enterprises/

https://www.bbva.com/es/blockchain-as-service-puede-interesar-negocio/

https://www.investopedia.com/terms/b/blockchainasaservice-baas.asp