UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Análisis de pertinencia de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano.
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación
Autor:
Andrés Ricardo Ramos Rodríguez
Tutor:
MSc. Pablo Recalde

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Msc. Pablo Recalde con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: Análisis de pertinencia de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano.

Elaborado por: Andrés Ricardo Ramos Rodríguez, de C.I: 1718453416, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Andrés Ricardo Ramos Rodríguez con C.I: 1718453416, autor/a del proyecto de titulación denominado: ANÁLISIS DE PERTINENCIA DE UNA SOLUCIÓN DE DISEÑO DE BLOQUES DE SEGURIDAD EN TRANSACCIONES DESCENTRALIZADAS PARA EL GOBIERNO ELECTRÓNICO ECUATORIANO. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
ANDRES RICARDO RAMOS RODRIGUEZ

Firma

Orcid: 0000-0002-0142-816X

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

La tecnología Blockchain crea una estructura de datos con características de seguridad únicas. Se basa en los principios de criptografía, descentralización y consenso, lo que garantiza confianza en las transacciones. En la mayoría de las tecnologías de cadena de bloques o libro mayor distribuido (DLT), los datos se organizan en bloques y cada bloque contiene una transacción o paquete de transacciones. Cada bloque nuevo está vinculado al anterior en la cadena criptográfica de una manera que es imposible de rastrear.

La gran mayoría de las de los eslabones (transacción) en la cadena de eslabones (bloques) se verifican y validan mediante un proceso de consenso para garantizar que todas las transacciones sean válidas y correctas (IBM, 2023).

Los sistemas de registro de transacciones públicas se basan en evidencia criptográfica en lugar de la confianza institucional; esto permite que el usuario civil, legal y el gobierno procesen transacciones directamente sin necesidad de una autoridad central de confianza, reduciendo costos para las partes. Estas transacciones no se pueden recuperar desde el punto de vista de cómputo, protegen a las partes del fraude y los mecanismos de protección de la retina.

El desarrollo de estas tecnologías ofrece una solución a los problemas financieros del gobierno y los ciudadanos mediante el uso de un servidor de registro distribuido en el tiempo para generar pruebas computacionales cronológicas de las transacciones, siempre que los nodos de confianza controlen más potencia de la CPU que cualquier combinación de nodos atacantes, en estas condiciones, el sistema es seguro (Nakamoto, 2009).

Problema de investigación

El deterioro de las instituciones públicas como entes reguladores de la información ciudadana ha provocado la dependencia de entidades de regulación que no han generado una ejecución eficiente en la operación de la información. Si bien, estos operan parcialmente para la gran cantidad de las transacciones, falla en un modelo basado en la confianza y el resguardo de la información.

En el ámbito gubernamental realizar transacciones completamente irreversibles no es tan real en procesos cambiantes y normativas regulatorias a largo plazo, ya que en cualquier

momento se pueden presentar disputas con afectaciones colaterales en las regulaciones o nuevas disposiciones del gobierno de turno.

El costo de la mediación a estas disputas aumenta costos operativos para el Estado y las entidades que participan en el proceso, limitando a generar transacciones de control o transaccionalidad ocasional que limita el realizar procesos irreversibles. Con la posibilidad o necesidad de revertir transacciones, esto debilita aún más la confianza en las entidades gubernamentales.

Los usuarios que utilizan los diferentes servicios públicos deben ser cautelosos para no entregar información indispensable y necesaria a las entidades públicas. Un porcentaje de transacciones inevitablemente generan fraude, sean transacciones en línea o de manera presencial.

¿Cómo una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano ayuda a las instituciones públicas a regular una ejecución en el manejo eficiente de la información?

Objetivo general

Proponer una solución que brinde transparencia y seguridad en los procesos y sistemas integrados a la transaccionalidad gubernamental.

Objetivos específicos

Examinar soluciones de tecnología Blockchain que actualmente se han implementado en: Estados Unidos, América del Sur, América Central, el Caribe, y la Unión de estados Europeos.

Analizar criterios de la tecnología Blockchain en la adopción en el estado ecuatoriano con el fin de establecer criterios que permitan cubrir los requerimientos de funcionalidades y cumplimiento normativo y legislativo en Ecuador.

Sugerir la implementación progresiva de la tecnología Blockchain en el gobierno electrónico en soluciones tecnológicas existentes.

Validar la tecnología Blockchain en los sistemas del ámbito público a través del análisis de especialistas.

Vinculación con la sociedad y beneficiarios directos:

Un modelo gubernamental basado en la confianza y el resguardo de la información, a través de transacciones completamente irreversibles en procesos cambiantes y normativas

regulatorias a largo plazo, busca brindar una guía para que a las instituciones públicas les permita optimizar los procesos de confidencialidad, trazabilidad, transparencia y seguridad.

Considerando los Objetivos de Desarrollo Sostenible, el análisis se centra en el objetivo número nueve que hace referencia a la Industria, Innovación e Infraestructuras. Ya que brinda asesoramiento sobre las tecnologías que pueden cubrir las necesidades de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano; ayuda a las instituciones públicas a regular una ejecución eficiente en el manejo de la información, garantizando que los usuarios puedan acceder de forma eficiente a toda la información y servicios ofrecidos por estas.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La estructura de datos ha sido un tema de investigación para las ciencias de la computación desde sus inicios, donde la gestión de la información es su enfoque principal. Blockchain es una tecnología que ha provocado una nueva revolución en las tecnologías existentes, dando paso a nuevos modelos y soluciones. Esta tecnología se ha expandido a varias soluciones, tanto gubernamentales como privadas; ofrece nuevos casos de aplicación que se han descubierto, mejorando así los beneficios que esta tecnología que tiene para ofrecer a largo plazo. (Salvatore, 2019).

1.1. Contextualización general del estado del arte

El Centro Global de Capacitación de Seguridad Ciberseguridad (GCSCC) de la Universidad Norteamericana de Oxford ha desarrollado un modelo de Madurez de Funciones de Ciberseguridad para Países (CMM). Se habla de un modelo que intenta evaluar la madurez de las habilidades de ciberseguridad de una región mediante la asignación de fases específicas que corresponden a los niveles de logro del tema de ciberseguridad. Las cinco fases de madurez establecidas por la evaluación desde la más básica (inicial) hasta alcanzar el logro avanzada (dinámica). (BID; OEA, 2020).

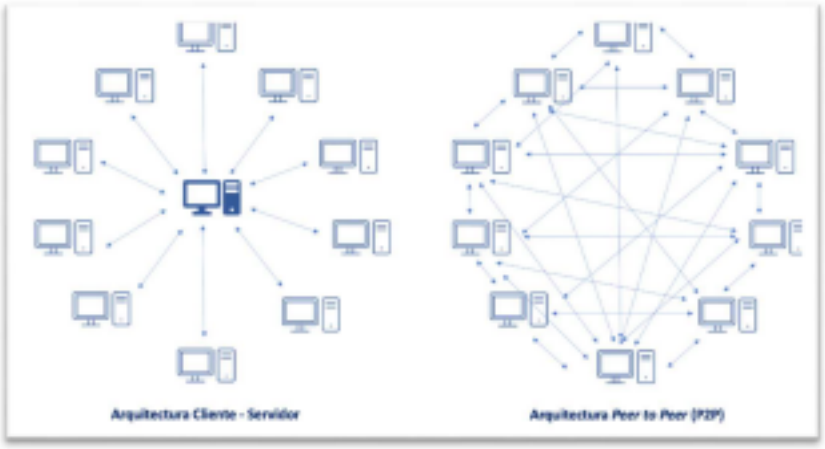
Cualquier sistema distribuido analizado tiene tres características básicas: número de equipos de cómputo (nodos), interconexión entre los mismos y estado compartido (Schroeder; Saltzer, 1972).

Un “sistema informático distribuido” puede definirse como un grupo de equipos de computacionales independientes, interconectadas a través de una red y lo suficiente mente capaces de cooperar entre sí y los demás equipos para realizar una tarea computacional (Coulouris; et al., 2012).

El modelo cliente-servidor presenta dos tipos de nodos: cliente y servidor. El cliente solicita un servicio y el servidor brinda el servicio más adecuado al cliente. La Figura 1 muestra la arquitectura básica del modelo cliente-servidor, aunque también es posible que un grupo de servidores interconectados sirvan a un grupo de equipos computacionales llamados clientes (López-Fuentes, 2015). La figura 1 también muestra la estructura general de un modelo peer-to-peer (P2P), que se puede definir como la asociación de nodos interconectados que pueden auto organizarse sin necesidad de intermediarios o asistencia de máquinas de autoridad mundial. De esta forma, cada nodo o miembro P2P puede ser en algún momento o al mismo tiempo dependiendo del trabajo a realizar servidor y cliente al mismo tiempo. Sin que exista una unidad

computacional de control central y todos los equipos que participan se comunican directamente entre sí.

Figura 1.
Arquitectura de nodos interconectados vs Arquitectura P2P



Nota. ***(López-Fuentes, 2015).***

La criptografía se puede definir como el uso de técnicas de alta comprensión matemática para salvaguardar la información de medios digitales de ataques no deseados (Kats et al., 2007). Sus elementos principales son: el remitente, el destinatario, el mensaje y la clave de cifrado, que permite alterar (cifrar) el mensaje digital original emitido para ser enviado por un canal indistintamente de su topología no confiable. Actualmente se ha desarrollado dos tipos de criptosistemas: clave simétrica o privada y clave asimétrica o pública.

Red pública de blockchain, según Preukschat (2017), se puede definir como una red computacional descentralizada de computadoras (nodos) que utilizan un protocolo de telecomunicación común asumido por todos los equipos computacionales y capaces de registrar transacciones. Con este tipo de blockchain, no hay límite en la cantidad de equipos de cómputo participantes que siempre pueden descargar en sus computadoras la tecnología necesaria para formar nodos que se unan a la red. Estos equipos computacionales clientes o servidores también participan en el proceso de consenso.

Cuantos más equipos computacionales interconectados (nodos) participen en una cadena de bloques, seránmás segura y menos vulnerable a posibles intentos de falsificación fraudulenta.

Las redes computacionales públicas actualmente más conocidas sin ningún orden en particular Cash, Ethereum, Bitcoin, Bitcoin y Litecoin. Dado que las cadenas de bloques de

estructuras Blockchain públicas están abiertas a todos los usuarios, se hizo necesario crear una cadena privada por motivos normativos o de privacidad.

Una red privada o proxy es una red en la que uno de sus procesos de consulta de información, validación y participación se limita a nodos específicos. Una autoridad Blockchain de gestión central que otorga derechos para comerciar, intercambiar información digital, ejecutar programas locales o remotos o acceder a información extraterritorial. Esto elimina la función de descentralización que era característica de la época en que se inventó la tecnología Blockchain. Además, el eficaz procesamiento y funcionamiento del Blockchain depende de la integridad de esta autoridad central.

El programa nacional de gobierno electrónico ofrece un modelo de gestión pública inclusivo, cercano a la ciudadanía, eficaz y eficiente, alineado con la política pública, orientado a una mayor participación e interacción entre la ciudadanía y el Estado (MINTEL, 2018-2021).

Las Normas de control interno desarrollados incluyen: normas generales y otros estándares específicos relacionados con la gestión financiera del gobierno, el personal, la UTICS tecnología de la información y la comunicación de la información, e incluyen el uso del Sistema Integral de Control Interno (COSO) emitido por el comité organizador que inició el Comité Treadway, que asegura que el proceso de gestión ofrece cinco componentes interrelacionados e integrados para ayudar a la empresa a alcanzar sus objetivos (CGE, 2009).

En Ecuador, donde el modelo que se ha venido implementado de software libre se convirtió de alguna manera en política tecnológica, el desarrollo de sistemas mediante el uso de software libre, el incentivo de uso de licencias de software libres, el uso de estándares de datos abiertos y el trabajo en comunidad promueven la inclusión social digital, la soberanía tecnológica y la innovación nacional. Optimizar el manejo del gasto público para el desarrollo local sostenible y promover la integración regional (E-Gobierno, 2023).

El Esquema de Seguridad de la Información del Gobierno (EGSI) busca proteger la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de procesos para la gestión de riesgos de seguridad de la información y la selección de controles para abordar los riesgos identificados (MINTEL, 2023).

FirmaEC es un sistema transversal desarrollado a través de contratación pública para la Subsecretaría de Gobierno Electrónico (MINTEL, 2023). FirmaEC brinda en su desarrollo implementado los elementos arquitectónicos de software para:

- Firmar documentos a través de certificados digitales obtenidos de manera local.

- Verificar la información de documentos firmados electrónicamente sin importar el origen o la entidad certificadora del certificado digital.
- Validar la autenticidad de certificados digitales emitidos por entes autorizados.
- Establecer la disponibilidad de servicios web para ser consumidos por sistemas gubernamentales desarrollados para que los ciudadanos o servidores públicos firmen electrónicamente.

La interoperabilidad del gobierno es una piedra angular del e-Gobierno ya que facilita, estandariza y regula el intercambio de datos electrónicos entre sistemas, y los estados necesitan automatizar los trámites para los procesos ciudadanos e institucionales (MINTEL, 2023).

1.2. Proceso investigativo metodológico

A continuación, se describe los procesos de investigación utilizados:

Investigación descriptiva

La investigación descriptiva ocurre cuando se quiere describir todos los componentes principales de la realidad. Se refiere al diseño de la investigación, la formulación de preguntas y el análisis de datos que se llevarán a cabo sobre el tema. A esto se le llama método de investigación observacional ya que de esta manera no se afecta ninguna de las variables que intervienen y que forman parte del estudio (Guevara, et al., 2020).

La investigación descriptiva se utiliza para recopilar información clave que respalda el desarrollo de este documento.

La investigación pretende entregar una guía la cual permita identificar las características comunes, diferencias y aplicabilidad de la solución Blockchain.

Investigación bibliográfica

Hay varias formas de acceder rápidamente a grandes cantidades de información, pero el mayor desafío es encontrar la información correcta. La investigación bibliográfica consiste en buscar y recopilar información que aporten de mejor manera con el tema de investigación. Uso de medios tradicionales y electrónicos (Gómez-Luna; et al., 2019).

El actual estudio utilizará el análisis cualitativo, identificará los elementos que se analizarán y recopilará información de diversas fuentes, como artículos, documentos científicos, informes de analistas de seguridad y documentos técnicos de soluciones.

Para un mayor análisis e investigación de soluciones seguras de cadena de bloques en intercambios descentralizados de gobierno electrónico, este paso verificará que los datos recopilados sean comprensibles y útiles para el propósito del estudio.

1.3. Análisis de resultados

Según Cordero, (2019), para realizar el análisis de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano, se han tomado las siguientes características:

Transparencia

Todos los gobiernos cuentan con reglas de transparencia, no solo como base para un gobierno de datos abiertos, sino también como parte un elemento básico de un estado en democracia en toda regla. Como los datos no solo deben estar a disposición de los ciudadanos, sino que de igual manera se debe regular el control de acceso y transparencia a esta información, han surgido leyes de protección de datos. Los mismos ciudadanos que quieren acceder a la información exigen al resguardo de sus datos personales.

Todavía no se ha logrado el equilibrio adecuado entre estos dos principios. Bajo estas leyes de transparencia han proliferado los sistemas web o escritorio de acceso a la información. Sin embargo, no se puede afirmar que de alguna manera se ha logrado erradicar los problemas como la corrupción o las irregularidades.

Colaboración

El gobierno democrático independiente y colaborativo involucra a los ciudadanos y otros agentes e involucra a los ciudadanos y otros agentes en el trabajo real del gobierno. Cooperación significa no solo trabajar con los ciudadanos, tambien ser apoyados con instituciones de ambiro privado, asociaciones y otros actores. De esta forma, se puede permitir el trabajo conjunto al interior del gobierno, entre sus empleados y los distintos poderes ejecutivos.

Participación

El compromiso cívico es una parte esencial de la buena gobernanza democrática, que fomenta una sociedad vibrante y ayuda a los gobiernos de cualquier línea ideológica a promover conjuntamente con sus ciudadanos el desarrollo productivo, social, intercultural y político.

Estos derechos ciudadanos enriquecen todos los procesos administrativos del sistema estatal, los hacen más competentes y crean relaciones respetuosas entre el ejecutivo y los ciudadanos.

Las aristas de participación ciudadana están estrechamente relacionadas con las nuevas tecnologías digitales que se introducen para estimular los caminos democráticos y los procesos institucionales y sociales compartidos (Shermin, 2017).

De esta manera, el objetivo es desarrollar herramientas de participación efectivas y fáciles de usar que mejoren la relación estratégica y comunicacional entre ambas partes. Una de las formas tradicionales de participación política son las elecciones. Encontrar soluciones seguras para el voto electrónico es un desafío para los gobiernos.

Digital por defecto, inclusión y accesibilidad

Garantiza que los ciudadanos y las empresas nacionales y extranjeras interactúen digitalmente con las administraciones gubernamentales de forma más conveniente, desarrollen sus habilidades digitales y promuevan servicios públicos digitales accesibles.

Principio de solo una vez

Evita que los ciudadanos tengan que proporcionar los mismos datos a diferentes autoridades. El objetivo impulsar el intercambio de información digital entre las diferentes administraciones a nivel comunitario, local, nacional e internacional.

Confianza y seguridad

Garantizar la oportuna de introducción y promoción de la normativa sobre identificación digital y servicios de acceso a la información de confianza para la realización de transacciones electrónicas en el mercado global. Garantiza que los derechos ciudadanos de privacidad se tengan en cuenta al diseñar servicios gubernamentales y soluciones basadas en tecnologías de la información (Cordero Valdavida, 2019).

Apertura y transparencia

Mejora del procesamiento de los datos personales recopilados por las autoridades administrativas estatales de ciudadanos y empresas (Cordero Valdavida, 2019).

Interoperabilidad por defecto

Promover la reutilización de soluciones técnicas compartidas y estandarizadas y el uso más amplio de soluciones y software abiertos en temas como la identidad digital, la firma electrónica ciudadana y jurídica o los contratos inteligentes (Cordero Valdavida, 2019).

Medidas políticas horizontales

Crear un conjunto de actividades para promover las habilidades de transformación digital de la organización, planificación, experimentación, intercambio de buenas prácticas, etc. (Cordero Valdavida, 2019).

2. CAPÍTULO II: PROPUESTA

Cuando se trata de la administración pública, existen antecedentes que facilitan de alguna manera el desarrollo o la implementación de proyectos de tecnologías, por mencionar algunos e-gobierno, o gobierno digital, y el llamado gobierno de datos abiertos.

2.1. Fundamentos teóricos aplicados

Blockchain

Según Preukschat (2017), una cadena de bloques no es más que una base de datos compartida entre numerosos usuarios, encriptada y organizada en bloques de transacciones que están relacionadas matemáticamente entre sí. Es una base de datos descentralizada segura, para decirlo de manera más sucinta. Su capacidad inherente para permitir que las partes que de alguna manera no confían plenamente entre sí mantengan un consenso sobre la existencia, el gobierno ecuatoriano y el desarrollo de una serie de factores es otro aspecto crucial para considerar.

Debido a que el consenso es la base para que todos los que usan un sistema de cadena de bloques puedan confiar en los datos que se registran en él, el consenso es precisamente la clave para un sistema de cadena de bloques. Este es un factor que tiene el poder de alterar drásticamente innumerables áreas importantes de la economía, sin mencionar la sociedad en la que vivimos, hasta el punto de que podría incluso alterar nuestra perspectiva del universo.

Técnicamente hablando, este sistema basado en la confianza y el consenso está compuesto por una vasta red informática que controla una base de datos considerable. Esto puede estar abierto a la participación de cualquiera (en cuyo caso hablamos de una "cadena de bloques pública") o restringido a un pequeño número de participantes (en cuyo caso hablamos de una "cadena de bloques privada"), pero nunca requiere una autoridad centralizada para supervisar o comprobar la eficacia de los procedimientos utilizados.

Redes Blockchain

La red pública de Blockchain se puede definir como una red única de computadoras (conexiones) que utilizan un protocolo de comunicación común que todos los equipos computacionales aceptan y les permite registrar transacciones, según Preukschat (2017). En este tipo de Blockchain, no hay límite en la cantidad de usuarios participantes que pueden descargar la tecnología requerida a sus computadoras en cualquier momento para crear un nodo que se conecte a la red.

Estos usuarios también intervienen en el proceso de sincronización. Cuantos más equipos computacionales (nodos) participen en la cadena de bloques, más segura será y menos vulnerable a los ataques cibernéticos fraudulentos de corromper o destruir.

Cadenas de bloques públicas

Dado que las cadenas de bloques públicas se comparten abiertamente entre todos los usuarios por motivos normativos o de privacidad, se sintió la necesidad de crear una cadena de bloques privada. Las redes privadas o autorizadas son redes donde la consulta, la autenticación y la participación están limitadas a ciertos nodos. Una autoridad central autoriza la comunicación, la ejecución del programa o el acceso a la información. Sin embargo, la descentralización como característica de la tecnología Blockchain debería desaparecer. Además, el correcto funcionamiento de estos dependerá de la precisión de estas autoridades centrales.

Cadenas de bloques privadas

Para limitar los problemas que existe en las redes públicas sin perder su infraestructura tecnológica (como las redes privadas), las instituciones financieras han propuesto soluciones complejas que no permiten que ningún usuario participe en la operación del acuerdo de autenticación, sino que están protegidos. Miembros de la organización. El grupo objetivo y las restricciones de acceso pueden ser ubicuos y limitados. Las agencias gubernamentales, al igual que las instituciones financieras, deben encontrar la mejor solución para sus necesidades.

Una de estas soluciones es conectar la Blockchain pública a los sistemas de información existentes, de modo que la información que queda en los sistemas de control y los rastros digitales de la transacción se almacenen en la Blockchain para que puedan aprovechar sus beneficios y reducir sus riesgos. Sin condenar las soluciones basadas en infraestructura privada, vale la pena considerar la declaración de Forde (2017) "La respuesta es pública: cadena de bloques pública, honesta" ("la respuesta es pública, cadena de bloques pública, honesta").

Limitaciones de la tecnología Blockchain

La cadena de bloques no tiene fronteras. Como señalaron Lander y Cooper (2017), la implementación gubernamental o privada de esta tecnología será lenta por varios motivos, uno de estos es la latencia propia del sistema: las ventajas de seguridad que ofrece el registro compartido limitado y redundante debido a su ineficiencia no solo en el tiempo de procesamiento sino también en los recursos informáticos en comparación con las bases de datos heredadas.

El uso de un gran número de fuentes de energía es una de las críticas más importantes a esta tecnología en auge. Además, antes de la implementación o lanzamiento de una nueva versión del sistema, es necesario transferir todos los datos para guardar el historial, lo que ralentizará el guardado. Todo esto se complica aún más por el tema de la privacidad, la solución es el cifrado, pero se requiere una garantía de seguridad. Adicionalmente, hay que analizar limitaciones o de alguna manera regulaciones legales como cuál es el valor de los contratos inteligentes.

¿Se puede usar el seguimiento de blockchain en los tribunales? Es evidente que se necesita un marco normativo común. Actualmente, el uso generalizado de blockchain puede resultar muy costoso para muchas transacciones.

Campos de aplicación de la tecnología blockchain

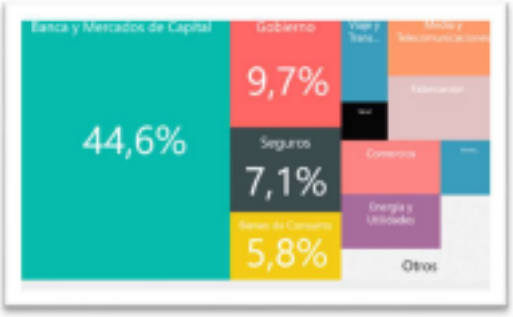
El Internet de la información se creó por primera vez en el ámbito militar y académico, luego se extendió a otras industrias. El sector financiero fue el primero en tomar acción, sin embargo, como antes el uso de esta tecnología no se limita a un solo sector, ya que otros sectores de la industria también están descubriendo todo su potencial.

Figura 2.
Cadenas de bloques blockchain

Nota: ***(Internet, 2023)***

Al revelarse que blockchain no solo se usará para intercambiar criptomonedas, sectores como gobierno, seguros y bienes de consumo participarán en el uso de esta tecnología, además de que su uso anterior solo en banca privada se encontró que va en aumento.

Figura 3.
Blockchain en la industria



Nota*: (Microsoft, 2020)*

Tabla 1.
Revisión del uso de la cadena de bloques en los diferentes países

País	Campo de Aplicación	Descripción
China	Salud	Alimentar datos de atención médica y mantener la logística
Canadá	Gobierno	Contribuciones y subvenciones, administración transparente de contratos gubernamentales
Estonia	Gobierno	e-Estonia, cada sector gubernamental se conectará en una sola plataforma.
Isla del Hombre	Privado	Regulaciones de protección del fraude en el sector de los juegos electrónicos entre otros.
Malta	Finanzas	Banco de cifrado y marco regulatorio para una mejor integración
Kenia	Vivienda	Implementación en proyecto de vivienda
Australia	Industria	Sostenibilidad de azúcar en polvo. Preservación de los derechos humanos, reducción ilegal de pesca, liquidez en bienes raíces
EEUU	Salud	Seguridad en datos de pacientes, aseguramiento de la información de cámaras fronterizas
Suecia	Inmobiliario	Manejo de títulos de propiedad descentralizada.
Dubái	Gobierno	Pagos, facturas, solicitudes de visa, renovaciones de licencias, registros ciudadanos
Chile	Gobierno	Manejo de pagos públicos.
Georgia	Gobierno	Registro de tierras.
Suiza	Gobierno	Pagos en criptomonedas, votación electrónica
Unión Europea	Gobierno	Gestión de propiedad intelectual
Singapur	Finanzas	Sistema interbancario
Reino Unido	Industria	Distribución de carne y garantizar la seguridad alimentaria
Gibraltar	Finanzas	Bolsa de valores y manejo de criptomonedas
Dinamarca	Gobierno	Sistema electoral y de votación
Venezuela	Gobierno	Emisión de moneda digital nacional
Corea del Sur	Gobierno	Intercambio de criptomonedas, tokens, soluciones empresariales
Tailandia	Gobierno	Moneda digital interbancaria entiempo real

Nota: Elaboración propia

Observatorio y Foro en Blockchain UE

En febrero de 2018, la Comisión Europea lanzó el Foro y Observatorio Blockchain de la UE para fortalecer el marco existente en Europa (y más allá), alentar a los actores europeos y fortalecer la integración europea con varias partes interesadas de blockchain. El registro está diseñado para realizar un seguimiento del progreso del desarrollo, solucionar problemas y encontrar información sobre blockchain. Las Reglas brindan una importante oportunidad de comunicación para que Europa exprese su visión a nivel internacional y busquen promover una acción conjunta basada en acciones prácticas en el interés europeo.

Blockchain Estados Unidos

El creciente interés en blockchain ha aumentado el número de empresas de este tipo en organizaciones públicas y privadas de millones de dólares en 2012 a miles de millones en 2017 y ahora está estableciendo a los Estados Unidos como líder en esta tecnología, más de $ 23.7 mil millones. (Smetanin et al., 2020)

Blockchain El Caribe y América Latina

Según el Banco Interamericano de Desarrollo (BID, 2018), en América Latina, el sector de pinzas de interfaz financiera permitió al departamento de distribución bajo la guía de sus modelos de negocios, sin embargo, la fuente de nuevos operadores y actividades inesperadas son utilizadas por las organizaciones responsables y el sistema. La velocidad y escala del cambio hace que los modelos de seguimiento tradicionales no sean suficientes, por lo que es necesario mencionar algunas fórmulas que ayuden y faciliten el funcionamiento de las empresas innovadoras en un entorno controlado y de bajo riesgo.

La regulación puede mejorar el proceso creativo en la medida en que elimina las asimetrías de información y genera confianza en los mercados y evita distorsiones al crear reglas de juego claras que garanticen el juego limpio. Los bancos de pruebas regulatorios brindan un entorno en el que las organizaciones pueden probar nuevos productos o servicios a pequeña escala antes de lanzarlos a gran escala, mientras que los reguladores pueden monitorear su desempeño. Es un enfoque flexible que permite soluciones individuales y ajustes o modificaciones, por lo que es la mejor herramienta para comprender la función de las partes afectadas dinámicamente. Un lugar importante para el aprendizaje, la colaboración y el diálogo con las empresas, donde los gerentes y representantes pueden analizar sus actividades y evaluar si necesitan monitorear nuevas actividades o cambiar instrucciones que podrían dificultar la

innovación. Todos estos países tienen una oportunidad única de beneficiarse del uso de las nuevas infraestructuras digitales para el desarrollo económico de la región.

Los bancos de pruebas regulares pueden ser una forma eficaz y asequible de comprender cómo funciona la industria FinTech y tomar las medidas regulatorias más adecuadas para utilizar todo su potencial en un entorno controlado que garantice la estabilidad del sistema y la protección de los intereses de todos los intermediarios.

En este contexto, desde febrero de 2018 se desarrolla sandbox una prueba de concepto denominada CADENA con el objetivo de compartir información sobre empresas bajo el Programa Económico Autorizado (OEA) entre diferentes regiones de Latinoamérica.

Esta prueba está siendo desarrollada por el BID y Microsoft con la participación del Servicio Nacional de Aduanas de Chile, el Servicio Nacional de Impuestos y Aduanas de Colombia, la Dirección General de Aduanas de Costa Rica, el Servicio de Administración Tributaria de México y el Ministerio de la Nación del Departamento de Aduanas e Impuestos Especiales del Perú.

De acuerdo con este plan, cuatro países (Chile, Colombia, México y Perú) que forman parte de la Unión del Pacífico firmaron en 2018 un Acuerdo de reconocimiento mutuo, que se espera que sea integren los países centroamericanos, así como la Comunidad Andina y MERCOSUR (BID, 2020).

2.2. Descripción de la propuesta

El Gobierno Electrónico del Ecuador en el marco de la gestión tecnológica para promover el desarrollo y el uso efectivo de la tecnología gubernamental blockchain desde una perspectiva de la atención descentralizada en la sociedad ecuatoriana. La solución de firma electrónica de FirmaEC se apoya en el sistema de administración pública Quipux; esto permitirá desarrollar un proyecto para evaluar la factibilidad y los beneficios de utilizar un sistema de registro electrónico basado en tecnología blockchain, con software que utiliza Blockchain (tecnología de contabilidad distribuida) para registrar, identificar y rastrear documentos y cualquier dato digital.

El registro de FirmaEc podrá actuar como un servicio en demanda notarial que permite:

a. el registro y publicación de documentos a través del registro de huellas digitales y sus metadatos,
b. visualización de documentos y otros datos digitales, y
c. transferencia de datos bidireccionales.

Con otros sistemas, se incluyen:

1. para acceso en línea a documentos,
2. para demostrar el uso práctico de la tecnología blockchain en análisis,
3. para usar sistemas de arquitectura web, interfaz responsiva y fácil de usar para facilitar el uso al registrarse confiando en privacidad de la información,
4. basado sobre la universalidad. La plataforma blockchain
5. permite la comunicación entre estas plataformas blockchain públicas y los sistemas informáticos internos.

Esto permitirá a los actores involucrados almacenar documentos digitales en una cadena de bloques pública, el poder verificar su autenticidad y crear un registro de auditoría seguro y compartido.

La figura 4 proporciona una propuesta de arquitectura de registro de FirmaEc Registry el cual brindara un servicio de cálculo de una huella digital de los diferentes documentos o datos registrados, y con esta se registran todos los datos de las transacciones en la blockchain pública.

Tanto las redes públicas o privadas, cualquiera de estas soluciones a ser desarrolladas permitirá almacenar este rastro digital en cadenas de bloque digitales almacenando los diferentes documentos en recursos privados de almacenamiento, esto será gestionado a través de Registro FirmaEc Registry, esto brindará un servicio público en beneficio de todos los actores de esta solución.

De esto, esta solución no incurre en el de la ley de protección de datos. Así como, el volumen de información escrita es viable su almacenamiento, lo que reduce los costos gubernamentales destinados para el proyecto. El sistema tiene como objetivo principal el registro de estas cadenas públicas descentralizadas brindando siempre una reducción en la latencia de respuesta para que el usuario no experimente retrasos en el sistema.

Para minimizar el riesgo inherente a la falta de disponibilidad de la infraestructura, el registro se realiza en las plataformas gubernamentales y en algunos casos con el apoyo de empresas privadas existentes. En el caso de una auditoría nacional o internacional en el cierre de ciclos periódicos de gestión gubernamental, el principio es registrar la evidencia tal como la presentó el beneficiario. Sin embargo, todos los demás participantes en el proceso, como planificadores, organizaciones locales y otros órganos administrativos, necesitan acceso al registro solo para registrar nueva información o para buscar y encontrar información en el registro.

a. Estructura general

Figura 4.
Propuesta FirmaEc Registry

Nota: ***Desarrollo propio basado en (MINTEL, 2020)***

b. Explicación del aporte

El registro de FirmaEc puede integrarse con el sistema de información existente en Gobierno Electrónico y otros organismos reguladores y puede procesar evidencia confiable, introduciendo el concepto de gestión por diseño; esto puede llevar a una reducción significativa en los costos de auditoría, ayudando a las organizaciones de auditoría y a los auditados en todos los diferentes gobiernos establecidos en Ecuador (nacional, regional o local) a proporcionar y lograr un valor agregado regulatorio estratégico. El proceso genera confianza, reduce el fraude y aumenta la transparencia.

Además, Gobierno Ecuatoriano Electrónico demostrará su liderazgo en innovación tecnológica en el proceso de calificación de la gestión gubernamental. En cuanto al uso de la contratación pública, la propuesta permitirá el uso de registros informáticos para garantizar la precisión de los documentos generados en las transacciones de bloque y el cumplimiento de los plazos para la ejecución de los procesos y la gestión pública.

c. Estrategias

Muchos países de nuestro entorno han creado una red nacional para dar a conocer esta tecnología, especialmente en el sector público; establecer enlace de expertos con diversas funciones administrativas; Facilitar la cooperación entre los gerentes; y ayuda a crear una cultura de esfuerzo sostenido. Estas redes han desarrollado programas y en muchos casos han recibido financiamiento nacional o internacional para poner en marcha programas piloto. Lo mismo ocurre en Finlandia, Italia o España, entre otros. Según Chen, et at. (2017), las organizaciones gubernamentales podrían adoptar un modelo de incubación de proyectos para competir y prosperar en este mundo globalizado de cadenas de bloques.

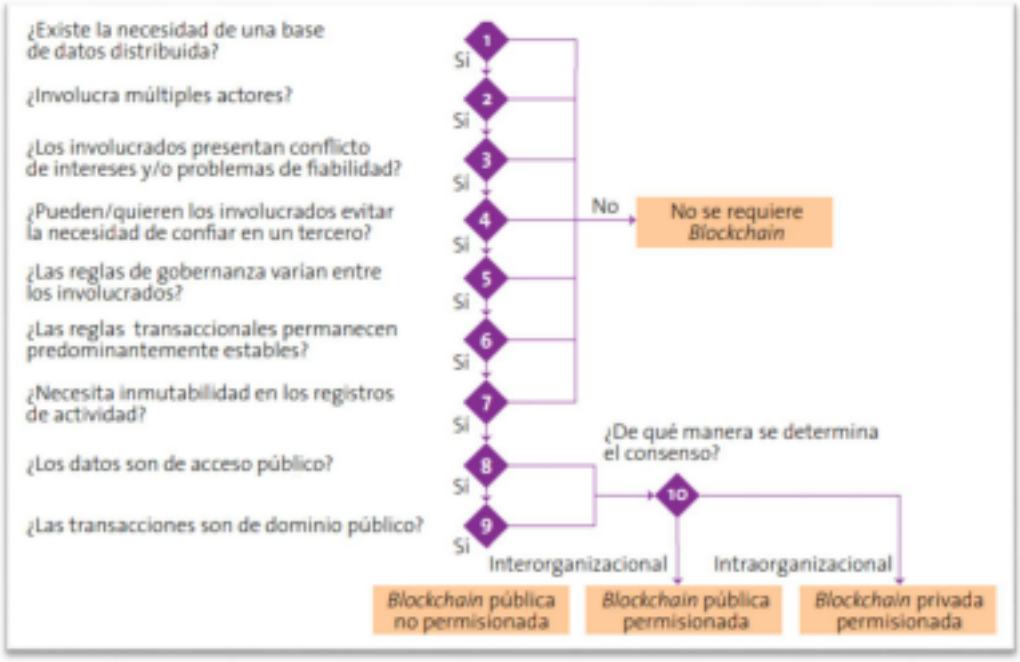
El estado ecuatoriano puede formar un grupo reducido para comenzar a intercambiar ideas y mostrar áreas en las que esta tecnología puede ayudar. Una vez hecho esto, se deben identificar los programas que pueden brindar el mayor beneficio. El equipo destinado para el análisis de estos proyectos o estas propuestas podrá crear las suficientes pruebas de concepto para validar la idea presentada. Las buenas ideas se pueden exportar y entregar a empresas profesionales para su implementación en colaboración.

El primer prototipo deberá ser discutido y transferido con otros actores del país para lograr una aplicación internacional. Una vez hecho esto, podría considerar extender el concepto a un contexto global. Los gobiernos pueden y deben cambiar las prácticas, incluidas las asociaciones internacionales, el intercambio de tecnología y la promoción de estándares internacionales.

2.3. Validación de la propuesta

Una primera mirada se realiza a través de un manejo de preguntas y respuestas condicionantes para a factibilidad de la solución a ser implementada.

Figura 4.
Esquema condicionante de Factibilidad



Nota: (Internet, 2023)

Marco Normativo Vigente

No se define expresamente dentro de la normativa vigente en la Ley Ecuatoriana E-Commerce el termino Blockchain para definir en un marco jurídico su implementación. Sin embargo, si se encuentra normado el uso de documentos electrónicos, en el artículo cuarenta y cuatro de la ley ecuatoriana de E-commerce.

(...)"Cualquier actividad, transacción mercantil, financiera o deservicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.", (E-commerce ecuatoriano, 2023).

De igual manera, el artículo 45 y 46 manifiesta el uso de documentos electrónicos para celebrar actos jurídicos, aceptando los mismos de manera legal. A partir de esto conforme al artículo 14 de la ley ecuatoriana de E-commerce, reconoce la validez que las firmas manuscritas como lo expresa un criterio jurídico por parte de MINTEL.

La firma electrónica es el conjunto de datos en forma electrónica consignados en un mensaje de datos y que pueden ser utilizados para identificar al titular de la firma e indicar que este aprueba y reconoce la información constante en el mensaje de datos. Esta Ley, además, confiere a la firma electrónico la misma validez y la generación de los mismos efectos que una firma

manuscrita. Sin embargo, para la verificación de una firma electrónica y su validez en un mensaje de datos, este debe permanecer en su forma original, en la que fue creado, (MINTEL, 2021).

2.4. Matriz de articulación de la propuesta

Tabla 2.
Matriz de articulación de la propuesta

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Criptografía	El uso de técnicas basados en algoritmos matemáticos desarrolladas para proteger la información de ataques cibernéticos no deseados (Kats et al., 2007).		Identificar la priorización de la información gubernamental.	El gobierno mejora los procesos de manejo de información.	Algoritmos matemáticos
Sistema informático distribuido	Grupo de computadoras independientes, interconectadas a través de una red y capaces de cooperar entre sí para realizar un procesamiento computacional		Número de equipos computacionales (nodos), interconectados y en un permanente estado compartido.	modelo peer-to-peer (P2P)	
Blockchain	Estructura de datos con características de seguridad únicas. Se basa en los principios de criptografía, descentralización y consenso, lo				

	que garantiza confianza en las transacciones.		
Gobierno electrónico	Modelo de gestión pública inclusivo, cercano a la ciudadanía, eficaz y eficiente, alineado con la política pública, orientado a una mayor participación e interacción entre la ciudadanía y el Estado.	modelo de gestión pública inclusivo	participación e interacción entre la ciudadanía y el Estado
FirmaEC	Sistema de origen transversal desarrollado para la Subsecretaría de Gobierno Electrónico.	Firmar documentos mediante el uso de certificados digitales. Verificar la información de los mismos. Validar certificados digitales adquiridos en las diferentes entidades autorizadas.	Establecer servicios API WEB de consumo.

Nota: Elaboración propia

CONCLUSIONES

El potencial de Blockchain para contribuir a la transformación digital del sector público ecuatoriano es innegable. La capacidad gubernamental ecuatoriano en analizar, diseñar y construir un sistema integrando entidades públicas o privadas que brinde suficiente evidencia para creer en la tecnología, con la mayor transparencia que puede brindar para incrementar en gran medida la confianza de los ciudadanos hacia el estado e instituciones privadas, podrá funcionar notoriamente bien en ausencia de desarrollo digital, democracia digital y protección de datos. Sin embargo, hay algunas cosas a considerar.

- Todos los actores públicos y privados se esforzarán mucho para que la tecnología tenga éxito, lo que demuestra que esto no se hace de forma tácita, como con la expansión de Internet, sino al implementado una política pública.
- Falta de un marco regulatorio y normativo vigente que esperamos se resuelva pronto, especialmente a nivel ecuatoriano y regional, no debemos pensar que otras tecnologías de cadena también interfieren con la infraestructura de Blockchain y representan un riesgo, como la computación cuántica, que puede repensar todos los sistemas basados en criptografía.

La acogida de esta tecnología a nivel internacional y su implementación en diferentes industrias evidencia la importancia de generar inversiones estatales para incluir estas tecnologías a un nivel estratégico y productivo.

El estado dentro de su modelo de gestión pública inclusivo, cercano a la ciudadanía, eficaz y eficiente, alineado con la política pública, orientado a una mayor participación e interacción entre la ciudadanía y el Estado; el crecimiento de proyecto de interoperabilidad del gobierno que es la piedra angular del e-Gobierno, protegiendo la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de procesos para la gestión de riesgos de seguridad de la información; a través del Esquema de Seguridad de la Información de Gobierno (EGSI).

La viabilidad de una integración a través del sistema FirmaEC; permitirá apoyar en el sistema de administración pública QUIPUX, desarrollando un proyecto para evaluar la factibilidad y los beneficios de utilizar un sistema de resguardo digital basado en tecnología Blockchain.

RECOMENDACIONES

Para la implementación del análisis de pertinencia de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano, para ello, necesitamos reducir la brecha competitiva frente a los países en desarrollo, que ya van un paso por delante, impulsando el desarrollo de este conocimiento en diversos sectores. De lo contrario, se abre la puerta para que los patrocinadores de tecnología extranjeros se aprovechen de nuestro conocimiento limitado en este campo y se pierdan las oportunidades que esta tecnología puede brindar.

Es importante equilibrar los beneficios de Blockchain para que las limitaciones sean menos importantes, esto es importante para que podamos encontrarnos a la vanguardia del desarrollo de esta nueva fase de Revolución Industrial 4.

Es una inversión que hace el estado ecuatoriano, los beneficios que Blockchain y los Smart Contracts pueden traer al sector gubernamental son amplios, abarcan diferentes áreas, hacen que las mejoras y los procesos sean más eficientes y crean problemas complejos que pueden resolver la posición de los diferentes actores en el sistema.

Invertir en el levantamiento de información de relevancia gubernamental, la gestión, y el intercambio de información interinstitucional mediante el uso de cadenas de bloques, el acceso a los datos públicos.

Implementar sistemas administrativos de cadenas de bloques que permitan a todas las instituciones públicas el uso regular de estos y el reconocimiento en sus programas de gestión gubernamental y en la implementación.

Colaborar con la academia e investigadores, así como observadores mundiales que lideran esta tecnología; que fomenten el uso del rastro digital en las políticas públicas. La academia e investigadores que tienen experiencia en generar, sintetizar y aplicar la información recolectada pueden ser socios estratégicos para su comprensión y los esfuerzos del gobierno ecuatoriano en el uso datos públicos y evidencia de manera sistemática la implementación de estas tecnologías en aras de la ejecución eficiente en el manejo de la información.

BIBLIOGRAFÍA

Alban, G. P., Arguello, A. E., & Molina, N. E. (01 de 07 de 2020). *Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción).* Obtenido de recimundo.com: http://recimundo.com/index.php/es/article/view/860

Amo, D. F.-P. (2020). *Privacidad, seguridad y legalidad en soluciones educativas basadas en Blockchain: Una Revisión Sistemática de la Literatura .* Obtenido de Revista Iberoamericana de Educación a Distancia: https://revistas.uned.es/index.php/ried/article/view/26388

CEPAL. (21 de 07 de 2021). *Oportunidades y desafíos para la implementación de blockchain en el ámbito logístico de América Latina y el Caribe.* Obtenido de https://repositorio.cepal.org/handle/11362/47098

Gómez-Luna, E., Fernando-Navas, D., Aponte-Mayor, G., & Betancourt-Buitrago, L. A. (1 de abril de 2019). *Metodología para la revisión bibliográfica y la gestión de.* Obtenido de dyna: https://www.redalyc.org/pdf/496/49630405022.pdf

Nakamoto, S. (2008). A Peer-to-Peer Electronic Cash System. *bitcoin.org*, 9.

Retamal, C. D., Roig, J. B., & Tapia, J. L. (2017). *La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6207510

Salvador, J. D. (28 de Marzo de 2019). *Estudio de blockchain desde la prespectiva de estructuras de datos.* Obtenido de USAC: http://www.repositorio.usac.edu.gt/13940/1/Josué%20David%20Itzep%20Salvador.pdf

Sánchez, C. R. (15 de 7 de 2022). *Blockchain: Funcionamiento y pertinencia en sectores públicos y privados.* Obtenido de https://is.uv.mx/index.php/IS/article/view/2734/4638

Serale, F., Redl, C., & Muente, A. (10 de 2019). *Blockchain en la administración pública: ¿Mucho ruido y pocos bloques?* Obtenido de http://dx.doi.org/10.18235/0001951