UNIVERSIDAD PANAMERICANA

Facultad de Ingeniería y Ciencias Aplicadas

Licenciatura en Sistemas y Tecnologías de la Información y la Comunicación

Aplicación del modelo de tecnología Blockchain para transparentar el proceso de compras en el sistema Guatecompras del Gobierno de la República de Guatemala

(Tesis de Licenciatura)

Diego José Flores Gómez

Guatemala, noviembre de 2020

Aplicación del modelo de tecnología Blockchain para transparentar el proceso de compras en el sistema Guatecompras del Gobierno de la República de Guatemala

(Tesis de Licenciatura)

Diego José Flores Gómez

Ing. Carmen Fabiola Morales Pérez

Asesora y Revisora

Guatemala, septiembre de 2021

Autoridades de la Universidad Panamericana

M.Th Mynor Augusto Herrera Lemus

Rector

Dra. Hc. Alba Aracely de González

Vicerrectora Académica

M.A. César Augusto Custodio Cóbar

Vicerrector Administrativo

EMBA. Adolfo Noguera Bosque

Secretario General

Autoridades de la Facultad de Ingeniería y Ciencias Aplicadas

MSc. MBA. César Augusto Cuevas Guerra

Decano

M.A. Mónica Lissette Alcázar Serralde

Coordinadora

UNIVERSIDAD PANAMERICANA

"Sabiduría ante todo; adquiere sabiduría"

Guatemala, 25 de octubre de 2,021

Ref. FICA-63/2021

Facultad de Ingeniería y Ciencias Aplicadas

Campus Central, Guatemala

Por este medio hago constar que previo a la otorgársele el grado académico de Licenciado en Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación, el estudiante, ***Diego José Flores Gómez*** quien se identifica con ID ***000032818***, ha desarrollado el Proyecto de Egreso denominado **"Aplicación del Modelo de Tecnología Blockchain para Transparentar el Proceso de Compras en el Sistema Guatecompras del Gobierno de la República de Guatemala"**

Aunado a ello, posterior a la lectura del informe de Licenciatura, se hace constar que el trabajo realizado por el estudiante en mención reúne las cualidades necesarias de un trabajo profesional universitario de Licenciatura.

Por tanto,

En calidad de Decano de Facultad de Ingeniería y Ciencias Aplicadas se emite **DICTAMEN FAVORABLE** para que continúe con los trámites de rigor.

Ing. César Augusto Cuevas Guerra
Decano de Ingeniería y Ciencias Aplicadas

UNIVERSIDAD PANAMERICANA FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS DE GUATEMALA

M. Sc., MBA Ing. César Augusto Cuevas Guerra

Decano

Facultad de Ingeniería y Ciencias Aplicadas

UNIVERSIDAD PANAMERICANA

"Sabiduría ante todo; adquiere sabiduría"

Guatemala, 25 de octubre de 2021

Ref. FICA-PF-064/2021

Facultad de Ingeniería y Ciencias Aplicadas

Campus Central, Guatemala

De acuerdo con el dictamen rendido por la Ingeniera Carmen Fabiola Morales Pérez, revisora de la tesis denominada **Aplicación del Modelo de Tecnología Blockchain para Transparentar el Proceso de Compras en el Sistema Guatecompras del Gobierno de la República de Guatemala,** presentado por el estudiante Diego José Flores Gómez quien se identifica con ID 000032818 y, la aprobación de la Evaluación de Competencias Profesionales (ECP), según consta en el Acta No. 01 - 2021, de fecha 22 de marzo de 2021; por lo tanto, se **AUTORIZA LA IMPRESIÓN**, previo a conferirle el título de Licenciado en Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación.

Ing. César Augusto Cuevas Guerra
Decano de Ingeniería y Ciencias Aplicadas

UNIVERSIDAD PANAMERICANA FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS DE GUATEMALA

M. Sc., MBA Ing. César Augusto Cuevas Guerra
Decano
Facultad de Ingeniería y Ciencias Aplicadas

DICTAMEN DEL REVISOR DE TESIS DE LICENCIATURA

Nombre del estudiante: **DIEGO JOSÉ FLORES GÓMEZ**
Título de la tesis: **APLICACIÓN DEL MODELO DE TECNOLOGÍA BLOCKCHAIN PARA TRANSPARENTAR EL PROCESO DE COMPRAS EN EL SISTEMA GUATECOMPRAS DEL GOBIERNO DE LA REPÚBLICA DE GUATEMALA**

El Revisor de Tesis,

Considerando:

Primero: Que previo a otorgársele el grado académico de Licenciado(a) en *Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación, el estudiante ha desarrollado su tesis de licenciatura.*
Segundo: Que ha leído el informe de tesis, donde consta que el estudiante en mención realizó su tesis atendiendo a un método y técnicas propias de esta modalidad académica.
Tercero: Que ha realizado todas las correcciones de redacción y estilo que le fueron planteadas en su oportunidad.
Cuarto: Que dicho trabajo reúne las calidades necesarias de una tesis de licenciatura.

Por tanto,

En su calidad de Revisor de Tesis, emite **DICTAMEN FAVORABLE** para los trámites de rigor.

Guatemala, 25 de octubre de 2021.

"Sabiduría, ante todo, adquiere sabiduría"

Carta de Responsabilidad de Derechos de Autor

Guatemala

Dinorah del Carmen Castillo González
Revisor Metodológico de tesis

UNIVERSIDAD PANAMERICANA
"Sabiduría ante todo; adquiere sabiduría"

Guatemala, 25 de octubre de 2,021

Ref. FICA-PF-065/2021

DICTAMEN DEL REVISOR DE TESIS

Nombre del estudiante:	Flores Gómez, Diego José.
Título de la tesis:	Aplicación del Modelo de Tecnología Blockchain para Transparentar el Proceso de Compras en el Sistema Guatecompras del Gobierno de la República de Guatemala.
Revisora de la tesis:	Inga. Carmen Fabiola Morales Pérez

Considerando,

Primero: Que previo a la otorgársele el grado académico de Licenciado en Ingeniería en Sistemas y Tecnologías de la Información y la Comunicación, el estudiante, Diego José Flores Gómez quien se identifica con ID 000032818, ha desarrollado el trabajo de Tesis denominado **"Aplicación del Modelo de Tecnología Blockchain para Transparentar el Proceso de Compras en el Sistema Guatecompras del Gobierno de la República de Guatemala".**

Segundo: Que la profesional Inga. Carmen Fabiola Morales Pérez, ha leído el informe de tesis donde consta que el trabajo de tesis realizado por el estudiante en mención reúne las cualidades necesarias de un trabajo profesional universitario de Licenciatura.

Por tanto,

En su calidad de revisora del proyecto de tesis se emite **DICTAMEN FAVORABLE** para que continúe con los trámites de rigor.

Inga. Carmen Fabiola Morales Pérez
Revisora de Tesis

Ing. César Augusto Cuevas Guerra
Decano de Ingeniería y Ciencias Aplicadas

UNIVERSIDAD PANAMERICANA FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS GUATEMALA

M. Sc., MBA César Augusto Cuevas Guerra
Decano Facultad de Ingeniería y Ciencias Aplicadas

En la ciudad de Guatemala, en el departamento y municipio de Guatemala
a los 25 días del mes de noviembre de 2020

Por medio de la presente YO Diego José Flores Gómez y en lo sucesivo "LA PERSONA AUTORA" hago constar que soy el único titular intelectual de la obra denominada

" Aplicación del modelo de tecnología Blockchain para transparentar el proceso de compras en el sistema Guatecompras del Gobierno de la República de Guatemala. ",
en lo sucesivo "LA OBRA", en virtud de lo cual autorizo Universidad Panamericana de Guatemala, "EL ORGANISMO" para que efectué resguardo físico y/o electrónico mediante copia digital e impresa con la finalidad de garantizar su disponibilidad, divulgación, comunicación pública, distribución, transmisión, reproducción, así como digitalización de la misma sin fines de lucro y con el objetivo de divulgarla.

"LA PERSONA AUTORA" autoriza a "EL ORGANISMO" y/o a la Facultad de Ingenieria y Ciencias Aplicadas de la mencionada casa de estudios "LA OBRA" de forma exclusiva en los términos y condiciones aquí expresados, sin que ello implique que se le concede licencia o autorización alguna o algún tipo de derecho distinto al mencionado respecto a la "propiedad intelectual" de la misma obra; incluyendo todo tipo de derechos patrimoniales sobre obras y creaciones protegidas por derechos de autor y demás formas de propiedad industrial o intelectual reconocida o que lleguen a reconocer las leyes correspondientes.

Al reutilizar, reproducir, transmitir y/o distribuir "LA OBRA" se debe reconocer y dar crédito de autoría de la obra intelectual en los términos especificados por el autor, y el no hacerlo implica el término de uso de esta licencia para los fines estipulados. Nada en esta licencia menoscaba o restringe los derechos patrimoniales y morales de "LA PERSONA AUTORA".
De la misma manera, se hace manifiesto que el contenido artístico y/o intelectual de cualquier parte de "LA OBRA" son responsabilidad de "LA PERSONA AUTORA", por lo que se deslinda

a “EL ORGANISMO” por cualquier violación a los derechos de autora o autor, de acuerdo a lo establecido en la Ley Guatemalteca y/o tratados internacionales, así como cualquier responsabilidad relacionada con la misma frente a terceros.

Diego José Flores Gómez

NOMBRE Y FIRMA DE “LA PERSONA AUTORA”

Dedicatoria

A Dios: Con acciones de eterna gratitud por siempre guiarme con su mano protectora, por su infinita bondad y misericordia. A mi señor por darme el regalo de la vida dotado principalmente de sabiduría, inteligencia y amor.

A mis amados padres: Juan Martín Flores & Elizabeth Nohemí Gómez, siempre les estaré agradecido eternamente por darme una vida digna y crear para mi un futuro de bien, que este nuestro triunfo sea la recompensa de todo el apoyo, esfuerzo y amor brindado.

A mis amadas abuelas: Francisca Gómez & Graciela Argueta por siempre cuidar de mi desde niño y siempre guiar mi vida con valores de bien y temor a Dios, siempre las honrare y amare por su apoyo.

A mi querida hermana: Lourdes María Flores por siempre apoyarme y estar a mi lado, contigo comparto este logro nuestro, porque siempre has sido una compañera de vida para mí.

A mis tíos y tías: Sandra Flores, Patricia Flores, Carlos Duarte, Ángel Gómez, Edgar Gómez, Ruth Gómez, Josué Gómez & Aracely López. Porque cada uno de ustedes me ha mostrado el valor de la vida y me dan enseñado infinidad de cosas de ella, a ustedes mis más grandes respetos y honores, mis siempre maestros.

A mis primos: Luisa Duarte, Sara Jerez, Oscar Duarte & Pedro Jerez porque siempre han sido un apoyo y una grata compañía en mi vida. Este logro también es de ustedes.

A mis amigos: Samuel Soberanis & Rafael Pelaez a ustedes muchas gracias por su

amistad y camarería porque ustedes más que nadie sabe que este logro es nuestro y el camino ha sido alcanzable gracias a ustedes.

A mi amor: Jairo Manuel Yela por siempre apoyarme no importando los momentos, por siempre darme tu mano que me guía, por todo el amor que me profesas y por darme tu ayuda incondicional este logro es tuyo.

A mis tutores: Fabiola Morales & Roberto López por su ayuda y consejos, muchas gracias.

A mi alma mater: Universidad Panamericana, por ser el medio para formarme como profesional con valores íntegros y académicos.

Tabla de Contenidos

Lista de Tablas

Lista de Gráficos

Lista de Acrónimos

AAPP: Administración Pública
P2P: Peer-to-Peer (Par a Par)
EFF: Frontier Foundation
POW: Proof of Work
POS: Proof of Stone
PBFT: Practical Byzantine Faul Tolerance
DAPP: Aplicación descentralizada

UE: Unión Europea

GBA: Government Blockchain Association

OCDE: Organización para la Cooperación y el Desarrollo Económico

CEDN: Coordinación de Estrategia Digital Nacional

EVM: Maquina Virtual de Ethereum

ABI: Aplication Binary Interface

AAA: Advanced Aircraft Analysis

Guatecompras: Sistema de Contrataciones y Adquisiciones del Estado

Lista de Figuras

Resumen

El presente trabajo académico de tesis de grado, cuyo nombre se titula: “Aplicación del modelo de tecnología Blockchain para transparentar el proceso de compras en el sistema Guatecompras del Gobierno de la República de Guatemala”, consta de cinco grandes capítulos en que se describe, desarrollo y aplica la tecnología disruptiva de Blockchain al ámbito de compras del Estado de la República de Guatemala.

En el primer capítulo, titulado “Marco Contextual”, se detallan los antecedentes de Gobiernos que han adoptado esta tecnología en sus procesos de compras y así mismo el éxito de ella, tal es el caso puntual de Perú. De igual forma este capítulo delimita, se describe la interrogante del problema y se establecen los objetivos que dieron dirección a la tesis aplicativa.

En el segundo capítulo, titulado “Marco Teórico”, se desarrollaron los temas fundamentales de la tesis aplicativa, tales como que es Blockchain, tipos de Blockchain, es que un Smart Contract, la implementación del programa de Blockchain y su guía de trabajo, entre otros.

En el tercer capítulo, denominado “Marco Metodológico”, se aborda el método utilizado para la recopilación de la información, nivel y tipo de tesis, así como la técnica estadística para recolección de datos empíricos.

En el cuarto capítulo, denominado “Resultados de la Aplicación”, se presenta de forma ordenada y gráfica los resultados obtenidos durante la ampliación de la tecnología del Blockchain al proceso de compras del Estado de Guatemala. Así mismo en este capítulo es donde se muestra el resultado final de la implementación de la tecnología disruptiva. Y como último capítulo, titulado “Discusión y análisis de Resultados” se aborda la viabilidad de implementar el modelo Blockchain a la gestión pública en su proceso de compras.

Palabras clave:

Blockchain, administración pública, Guatecompras, Smart Contract, Ethereum, Solidity, Hash.

Abstract

The present academic thesis work, whose name is titled: "Application of the Blockchain technology model to make the purchasing process transparent in the Guatecompras system of the Government of the Republic of Guatemala", consists of five large chapters in which it is described, development and applies disruptive Blockchain technology to the procurement field of the State of the Republic of Guatemala.

In the first chapter, entitled “Contextual Framework”, the antecedents of governments that have adopted this technology in their purchasing processes and also its success are detailed, such is the specific case of Peru. Similarly, this chapter delimits, describes the question of the problem and establishes the objectives that gave direction to the applicative thesis.

In the second chapter, entitled "Theoretical Framework", the fundamental topics of the application thesis were developed, such as what is Blockchain, types of Blockchain, is a Smart Contract, the implementation of the Blockchain program and its work guide, among others.

In the third chapter, called "Methodological Framework", the method used to collect the information, level and type of thesis is addressed, as well as the statistical technique for collecting empirical data.

In the fourth chapter, called "Application Results", the results obtained during the expansion of Blockchain technology to the Guatemalan State purchase process are presented in an orderly and graphical way. Likewise, this chapter is where the final result of the implementation of disruptive technology is shown. And as the last chapter, entitled "Discussion and Analysis of Results" the feasibility of implementing the Blockchain model to public management in its purchasing process is addressed.

Keywords:
Blockchain, public administration, Guatecompras, Smart Contract, Ethereum, Solidity, Hash.

Introducción

Blockchain se ha convertido en la palabra de moda en los medios de comunicación e incluso en nuestra vida cotidiana. Sin embargo, no muchas personas conocen lo que este nuevo concepto realmente significa y sus implementaciones.

Según (Berryhill, J,2018) el Blockchain se define como un sistema de contabilidad distribuido digital que actúa como un registro abierto, compartido y de confianza que realiza transacciones entre las partes y no se almacena por una autoridad central y sigue manteniendo el enfoque tradicional.

Esta tecnología entra en debate público en distintos sectores e industrias por la amplitud de servicios, oportunidades y desafíos que puede ofrecer. La complejidad de esta tecnología es un tema que muchos Gobiernos están empezando a explorar para desarrollar posibles aplicaciones y plataformas que favorezcan el sistema de sus estados. Ya que el Blockchain plantea una amplia gama de soluciones potenciales en distintas áreas gubernamentales y que benefician principalmente al ciudadano, tal es el caso de la aplicación en la compra del Estado.

La sociedad actual cada día reclama una mayor transparencia, participación y cooperación ciudadana entre todas las partes en materia de actividades públicas que competen a las Administraciones Públicas y al Estado. La ciudadanía cada día está más despierta en los procesos administrativos y gubernamentales por la falta de transparencia y acceso a la información sobre los asuntos que ellos mismos son activos. Gracias a la falta de legislación actualmente vigente, como las leyes de transparencia, buen Gobierno, datos abiertos, administración electrónica y participación ciudadana, tanto centrales y departamentales, se está dejando atrás la concepción de una sociedad pasiva.

Lo que lleva a introducir el Blockchain en una nueva vertiente, presentar una nueva tecnología revolucionaria a los procesos de trabajo de las Administraciones Públicas (AAPP) centrales y departamentales. Esta tecnología gestiona la información, reduce el fraude, la corrupción, el

factor humano, el coste del uso del papel y garantiza la confianza de todas las partes implicadas en el sector público.

Capítulo I
Marco Contextual

En este primer apartado del documento académico se podrá encontrar la descripción detallada de la ubicación geográfica, el escenario físico, condiciones temporales y situación general del entorno del tópico aplicativo. Así mismo como el objetivo principal del tema y los antecedentes predecesores en una línea del tiempo cercana.

1.1 Antecedentes

Alrededor del mundo la tecnología ha sido parte fundamental del avance evolutivo de la humanidad. Y las tecnologías disruptivas, como lo es el Blockchain, no han sido la excepción a la norma. Desde los últimos años esta tecnología ha tenido un gran auge en las políticas de licitación y compras públicas de diferentes repúblicas y estados soberanos alrededor del mundo.

Para el desarrollo y aplicación de este documento académico se toma como referencias las siguientes aplicaciones y/o programas piloto internacionales gubernamentales de la tecnología de Blockchain, en el manejo y administración de compras públicas: En julio de 2018 el Gobierno de Chile hace el lanzamiento oficial de un programa piloto para el uso de la tecnología Blockchain en los procesos de compras públicas, esto sobre su plataforma de ChileCompras.

La iniciativa del plan piloto nace de la búsqueda de la actualización de la plataforma de compras, en donde más de 850 organismos del Estado realizan de manera autónoma sus licitaciones y compras. En este espacio aproximadamente se realizan actividades contractuales con más de 123 mil empresas proveedoras del Estado.

El objetivo de utilizar la tecnología Blockchain dentro del mercado público es proporcionar un mayor nivel de transparencia en los procesos de licitación y compras, procurando que la nueva

aplicación funcione como una especie de notario público virtual que certifique y conserve los documentos oficiales de forma que estos no puedan ser alterados y/o eliminados.

Las autoridades chilenas concluyen que la aplicación de este plan piloto destaca el gran potencial de la herramienta para reducir las tareas administrativas del Estado y evitar la corrupción, a lo cual agrega la posibilidad de hacer un seguimiento a las diferentes fases de los procesos de forma simultánea y en tiempo real.

Por parte de los especialistas tecnólogos que apoyan el plan piloto hacen énfasis en el hecho que los registros de las órdenes de compra que suben a la plataforma digital quedarán con un sello digital que nadie podría alterar, pues cualquier intento de alteración al registro quedará grabado en la red de Blockchain y podrá ser fiscalizado por todos los usuarios de la red, no solo por quienes administran el servicio de ChileCompras, sino por los contribuyentes.

Otra referencia contundente sobre esta tecnología se puede encontrar en las pruebas controladas realizadas por el Gobierno de los Estados Unidos Mexicanos. En el año 2018 durante la actividad Talent Land los participantes apreciaron cómo una unidad compradora puede realizar una convocatoria de licitación y cómo una empresa se postula para ofrecer sus productos y servicios al Gobierno federal, todo esto a través de la tecnología de Blockchain.

En conjunto el Gobierno mexicano y la Secretaria Estratégica Digital Nacional ponen a prueba el modelo de gobernanza que rige a la nueva red disruptiva. Misma que cuenta con tres tipos de nodos: públicos, administrativos y de servicios. Estos tres nodos garantizan la fiscalización pública fuera de las manos del Gobierno central, es decir, es una red mexicana, la seguridad de encriptación de los datos y la administración de los servicios.

Según los desarrolladores de la red mexicana de Blockchain, el Estado Mexicano generó un sistema de contrataciones basado en la utilización de esta tecnología y en el Estándar de Adjudicaciones Abiertas del Gobierno federal. Usa como base el sistema Ethereum y sirve para

gestionar las licitaciones gubernamentales a través de contratos inteligentes, sin tener que hacer uso de criptomoneda.

Si bien las dos anteriores recopilaciones del uso de la tecnología Blockchain eran planes piloto o pruebas contraladas. También se encuentran casos de implementaciones reales y documentales. Tal como es el caso de Perú, a mediados del año 2019 el Gobierno peruano ya contaba con más de 47 mil órdenes de compras soportadas por la tecnología del Blockchain.

Desde que la Central de Compras Pública, PerúCompras, implementó la tecnología de Blockchain como una forma de brindar transparencia en la contratación pública, se han registrado más de 47,152 órdenes de compras emitidas a través de la plataforma de Catálogo Electrónicos (plataforma Blockchain), esto a finales del año 2019.

Según el portal de PerúCompras, la tecnología Blockchain permite registrar cada orden de compra y sus respectivas ofertas en una red de servidores, denominados nodos, lo cual asegura que la información del sistema no ha sido adulterada de ninguna manera. De igual forma PerúCompras explica que han tenido dos problemas en la implementación de la tecnología:

La primera problemática es alertar si alguien que posee el acceso respectivo, modificó directamente los datos de la licitación (condiciones contractuales) a nivel de base de datos para inescrupulosamente beneficiar a un candidato. La segunda problemática es alertar si un postor ganador adulteró la orden de compra, modificando la cantidad o las condiciones de entrega y/o envío.

Según Zárate Sousa, gerente del proyecto de implementación, la solución para ambas problemáticas fue utilizar la herramienta de Stamping.io, con la finalidad de inmutar los datos de las ofertas y los documentos generados por medio de Hash entrelazados (Hashlink). Otro beneficio de esta herramienta es la visibilidad de la trazabilidad del proceso de la licitación en todas sus fases, según lo establece las normas legales de Perú.

1.2 Planteamiento del Problema

La situación actual que vive la gestión pública en licitación y/o compras por parte del Gobierno de la República de Guatemala, a ojos de sus gobernados e instituciones internacionales, es de incertidumbre y de desfalco de los recursos monetarios públicos. Lo anterior posiblemente por el historial en la falta de transparencia y/o adulteración de los elementos contractuales en el proceso de licitación en el portal de Guatecompras, por dicho ente gubernativo.

Dicho lo anterior el enfoque de este trabajo académico es otorgar una herramienta tecnológica capaz de mitigar la falta de transparencia y de manipulación de datos dentro del portal de licitación del Estado de la República de Guatemala, Guatecompras. En consecuencia, a la anterior sentencia nace la formulación de la pregunta de implementación: ¿Cómo la tecnología de Blockchain permitirá la descentralización de los procesos de compras del Estado de la República de Guatemala y ofrecerá a la ciudadanía una gestión transparente, trazable y segura?

1.3 Justificación

Uno de los objetivos primordiales de toda sociedad moderna es el correcto uso de los recursos disponibles que pueda poseer el Estado para la correcta gestión pública de los mismos. Esto garantiza la funcionalidad correcta de toda institución gubernamental cumpliendo con su mandato y garantizando la protección de la persona y la familia; el fin supremo es la realización del bien común.

Actualmente se vive en una sociedad que está gravemente influenciada por la falta de práctica de valores éticos y morales. Tal es el caso de los últimos años en la gestión pública, en el régimen de compras y contrataciones del Estado. Esto en los últimos años ha dado a grandes escándalos de corrupción y desfalcos millonarios de las arcas del Estado y en la falta fiscalización y transparencia del uso de los recursos monetarios.

Dado las premisas anteriores se ve en la necesidad de implementar nuevos mecanismos de protección a las acciones contractuales del estado y sus proveedores. Aquí es donde juega un papel importante la tecnología y la denominada Transformación Digital. El uso correcto de estas nuevas tecnologías ascendentes puede determinar la transparencia y seguridad de los recursos del Estado para que este cumpla su mandato supremo plasmado en la Constitución Política de la República de Guatemala.

El uso de Blockchain para fiscalizar y transparentar las compras del Estado radica en los siguientes beneficios: La aplicación de la tecnología descrita en la Administración Pública resuelve una de las grandes preocupaciones de la Sociedad Digital, la seguridad de los datos personales de los contribuyentes y la inviolabilidad en las bases de datos de la ciudadanía.

Blockchain por su naturaleza, apuesta por un modelo de transparencia abierto y participativo, pero a la vez seguro. La inviolabilidad de las transacciones y registros de Blockchain abren la puerta a una revolución en las relaciones de la ciudadanía con la Administración. Hablamos de la puesta en marcha de contratos inteligentes.

Mejora de todos los procesos de licitación y concursos públicos que gracias a la aplicación de Blockchain en la Administración Pública pueden resolver los constantes litigios y ganar significativamente en tiempos de tramitación.

En síntesis, el posible aporte más grande de Blockchain en la gestión pública de contratación es la invulnerabilidad de los datos, la trazabilidad de los acuerdos contractuales y la transparencia en todo momento de las licitaciones. Lo anterior desembocará en la mitigación de desfalcos económicos por funcionarios públicos con lo que se verá en la mejora operativa de los entes gubernativos y por ende a la potenciación del alcance del bien común.

Adicionalmente, este documento académico aporta una ventana de oportunidad para implementación de la tecnología en cualquier empresa en el ámbito privado, ya que la lógica no cambia, a lo que se refiere en contratos inteligentes.

1.4 Importancia de la Aplicación

Desde los inicios y evolución de la tecnología Blockchain han existido diversas ramas de investigación y aplicación, pero pocos indagan la posibilidad de materializar la idea de esta tecnología dentro de los servicios públicos, en concreto en los de licitación y compras en el Estado. Dentro de la documentación académica no se puede encontrar muchas investigaciones o tesis de implementación de proyectos sobre el Blockchain junto en las Administraciones Públicas (AAPP).

Adicionalmente en las bibliotecas científicas se encuentra poca literatura sobre el tema en cuestión, en la que pueda apoyar de forma confiable las afirmaciones que se está vertiendo sobre esta tecnología. A pesar de las dificultades y barreras que se obtenga en recopilar información y ponerla en práctica, existe información en canales electrónicos como videos, webinars y exposiciones académicas.

Dicho lo anterior, este documento académico toma importancia en ser un texto en el cual no solo se recopilará información relevante y confiable sobre esta tecnología disruptiva en auge, sino se pondrá en aplicación en el ámbito de la administración pública como modelo de referencia. De esa manera quedará registrado en la biblioteca de la Facultad de Ingeniería de esta casa de estudios superior, para su uso posterior de la comunidad académica interesada y adicional las empresas pioneras que deseen implementar Blockchain en sus procesos de licitación y compra.

Si bien, ya se mencionó la importancia del trabajo académico, cabe mencionar la relevancia que tiene la aplicación del Blockchain en este trabajo. Ya que la implementación que se realizará en esta faena es un piloto del uso de la tecnología en el portal de Guatecompras, para poder transparentar, trazar y fiscalizar las compras del Estado.

Dicho piloto tiene la potencial capacidad de ser un punto de partida, si bien así lo desee el órgano gubernamental competente, en implementar esta tecnología a todas las licitaciones del Gobierno

de la República de Guatemala. Con lo que beneficiaría a la población guatemalteca al momento de fiscalizar los fondos públicos y la transparencia de estos.

1.5 Objetivos

En este apartado del documento académico, se va a presentar los objetivos, tanto el principal como los específicos, que se han considerado esenciales para el trabajo de aplicación, estructuración y desarrollo del trabajo.

1.5.1 Objetivo principal

Aplicar la tecnología de Blockchain en el proceso de licitación y/o compras del Estado de la República de Guatemala, en su portal Guatecompras, para favorecer la transparencia, trazabilidad y acceso de la información a toda la ciudadanía guatemalteca y a toda persona o entidad interesada.

1.5.2 Objetivos específicos

1. Analizar la legislación guatemalteca e internacional ratificada por el Gobierno de Guatemala relevante que puede encontrarse relacionada con el acceso a la información y compras del Estado.

2. Estudiar la bibliografía relacionada con la temática y los casos de éxito relacionados con los problemas que presentan la sociedad y las instituciones guatemaltecas actualmente, referente a la licitación y compras del Estado.

3. Identificar las plataformas aplicables a la implementación piloto y posibles tecnologías Blockchain al contexto guatemalteco, y a la plataforma Guatecompras.

4. Mostrar una aplicación con Blockchain sobre el caso de uso de licitación del Estado de Guatemala, en su plataforma Guatecompras.

1.6 Alcances y Límites

El alcance de la tesis de aplicación contempla la investigación e implementación de un programa piloto de la tecnología Blockchain en el entorno de licitaciones y/o compras del Estado de Guatemala en su portal de Guatecompras. Entender el modelo de negocio de las compras del Estado, de tal manera comprender sus beneficios y áreas en áreas en las que se puede innovar utilizando esta tecnología como herramienta.

Así mismo el alcance de esta tesis de aplicación es buscar el mejor software Open source y lenguaje de programación que de adapte a la necesidad del negocio para su evolución a la tecnología del Blockchain.

La temporalidad de este trabajo aplicativo conllevará en su totalidad 123 días en los cuales se llevará a cabo la elaboración de cada uno de los capítulos de este documento académico y la aplicación de la tecnología en un programa piloto. A lo que se refiere a su alcance geográfico, este trabajo reflejara únicamente sus esfuerzos en la República de Guatemala.

Cabe mencionar que, como límite del trabajo académico, este no abordará el tema de las criptomonedas y ningún otro elemento fuera de la tecnología en sí del fichero.

Concretamente este trabajo de tesis aplicativo ayudará a que las compras y licitaciones cargadas en el portal de Guatecompras sean transparentes en toda la fase del proceso, así como trazables y fiscalizadas por cualquier persona interesada, ya sea por parte del Gobierno, del proveedor o de la ciudadanía misma.

Capítulo 2
Marco teórico

2.1 Antecedentes

La tecnología Blockchain es una innovación revolucionaria en varios campos de la informática, con la capacidad de mutar muchos sistemas tradicionales existentes en sistemas más seguros, distribuidos, transparentes y colaborativos, mientras que empodera a sus usuarios. La tecnología Blockchain, a pesar de que en concreto no se conoce a su creador, fue noticia por primera vez en el año 2009 con la llegada de la primera criptomoneda, “Bitcoin”.

Para el 2020, la red de servicios basados en Blockchain abarca más de solo criptomonedas, la tecnología abarcó varios campos del sector privado, así como del sector público tal y como es la administración de compras y licitaciones del Estado. Lo que se busca con esta nueva tecnología es reducir o eliminar muchos puntos de fricción para una variedad de transacciones comerciales; las personas y las empresas podrán intercambiar una amplia gama de activos y valores digitalizados y para la gestión pública se podrá otorgar mejor transparencia en el manejo de los fondos públicos.

Según (Zhao, Fan, & Yan, 2016) Blockchain se ha convertido en una nueva frontera de capitales de riesgo que ha atraído la atención de bancos, Gobiernos y otras corporaciones comerciales. Blockchain está a punto de convertirse en la invención más emocionante después de Internet; mientras que el segundo conecta el mundo a habilitar nuevos modelos comerciales basados en procesos en línea, el primero ayuda a resolver el problema de confianza de manera más eficiente a través de la computación en red.

Un claro caso de éxito de la aplicación de esta tecnología al proceso de compras y licitación del Estado es, PerúCompras. En el año 2019 el Gobierno de Perú implementó la tecnología Blockchain como una forma de brindar transparencia en la contratación pública, desde sus inicios

hasta mediados de agosto de 2019, se han registrado más de 47,152 órdenes de compra emitidas a través de la plataforma de Catálogos Electrónicos a nivel nacional.
La tecnología Blockchain permite a PerúCompras registrar cada orden de compra y sus respectivas ofertas en una red de servidores, denominados también nodos, lo cual asegura que la información del sistema no ha sido manipulada de ninguna manera.

Del total de órdenes de compra registradas en la tecnología Blockchain, el 73 por ciento corresponde a proveedores del interior del país, entre los cuales destacan Cusco con 10.4 por ciento, Arequipa con 5 por ciento, La Libertad con 4.4 por ciento y Junín con 4.2 por ciento. También figuran Huancavelica con 3.9 por ciento, Puno con 3.8 por ciento, Apurímac con 3.7 por ciento, Ayacucho con 3.5 por ciento, Cajamarca con 3.4 por ciento y San Martín con 3 por ciento.

2.2 Blockchain

La tecnología de Blockchain o por su traducción al español “Cadena de Bloques” es mayormente conocido como el monedero de la criptomoneda de Bitcoin creada por el reconocido Satoshi Nakamoto. Sin embargo, la funcionalidad de esta tecnología no se limita únicamente a ser utilizado por Bitcoin o cualquier otra criptomoneda.

2.2.1 Definición de Blockchain

Seguramente alguna vez a escuchado hablar sobre la tecnología Blockchain o sobre el dinero electrónico y como estos han evolucionado de manera exponencial en nuestra era digital. Aunque esta palabra sea muy mencionada en ámbitos de economía, tecnología, gobernanza entre otros su significado y utilidad, no son del todo clara.

Según (Berryhill, Bourgery y Hanson,2018) es un sistema de contabilidad distribuido digital que actúa como un registro abierto, compartido y de confianza que realiza transacciones entre las partes y no se almacena por una autoridad central y sigue manteniendo el enfoque tradicional.

La tecnología de Blockchain surge en la década de los años 90 con el fundamento de crear un espacio de trabajo colaborativo económico en una red pública. La concepción de esta idea se remonta hasta la década del 70 en dónde se hablada de crear divisas electrónicas descentralizas sin límites de jurisdicción

Teniendo un panorama previo de cuál es la idea principal de Blockchain, a continuación, se expondrán definiciones con un nivel mayor de concepción técnica en lo que se refiere al ámbito tecnológico y económico.

Yahon (2018) afirma

> Blockchain es un ledger distribuido creado por bloques que contienen detalles de transacciones conectados en orden cronológico para formar una serie de cadena. Es un libro mayor distribuido en el cual los participantes de la red peer-to-peer (P2P) de Blockchain, y no el administrador central, genera bloques. Las posibilidades de uso de Blockchain son reconocidas en muchos campos diferentes, lo que resulta en muchos desarrollos y estudios que se llevan a cabo, y las inversiones están sucediendo activamente. Blockchain es una tecnología para asegurar la integridad y confiabilidad de los registros de transacciones sin tercero como proveedor de servicios de confianza, haciendo que todos los participantes de la red creen, graben, almacenen y verifiquen la información de la transacción conjuntamente, y tiene la estructura para realizar diversos servicios de aplicaciones basados en infraestructura de red distribuida, utilizando tecnologías de seguridad incluyendo Hash, firma digital y criptografía. (p. 22)

A lo que se refiere en un ámbito latinoamericano sin traducción o distorsión del idioma nativo, la literatura de define Lérida & Pérez (2016) Blockchain es un sistema que permite escribir movimientos de tokens en un gran libro virtual que funciona a modo de libro de contabilidad para una moneda. Este libro ha demostrado ser intocable, gracias a estar completamente distribuido y constantemente actualizado con las nuevas entradas contables que se producen. Las entradas contables se agrupan por bloques antes de ser escritas en gran libro de contabilidad que es el Blockchain. De esta manera Blockchain pasa a ser un gran libro de contabilidad que puede ser escrito por cualquier entidad, pero una vez escrito no puede ser modificado, aunque cualquiera puede leerlo.

2.2.2 Estado del arte de Blockchain

Como se mencionó en el apartado anterior la tecnología de Blockchain no vio sus inicios en los últimos años de la humanidad ni mucho menos de la década del 2010. La tecnología o la concepción de la idea de Blockchain nace a finales de la década de los 70 y esta es consecuencia de más de 40 años de investigaciones.

A lo largo de la primera mitad del siglo XX, distintas iniciativas la mayoría vinculadas al ámbito militar, sentaron las bases técnicas de la criptografía, una disciplina que durante un largo tiempo fue dominio de los Gobiernos. Años más tarde, a partir de estos avances matemáticos se desarrollaron una serie de algoritmos que permitieron la creación de la 'criptografía de clave pública', un precedente imprescindible para el desarrollo de 'Blockchain' y bitcoin.

Pero no fue hasta la década de los 90, en el denominado ciberpunk, cuando otro conjunto de proyectos informáticos, vinculados a la libertad de información y la búsqueda de un sistema descentralizado, hicieron posible la publicación de Bitcoin P2P e-cash, el primer hito hacia la creación de la criptomoneda.

Con las bases técnicas cimentadas, en los años 90 se da un nuevo aire a las tendencias que concretan el Blockchain de la mano del Bitcoin. Comienzan a destacar el PGP de Phil Zimmermann en 1991, el primer software de encriptación ampliamente utilizado en el mercado y la Electronic Frontier Foundation (EFF, creada en 1990), de donde se fundamenta el manifiesto cripto-anarquista de Tim May, uno de los textos referentes en toda esta historia de Blockchain.

El camino del Blockchain estaba trazado y perfilado, pero antes de ello hubo pioneros como Nick Szabo con sus desarrollos de Digicash, Hashcash y Bitgold (que esbozó el concepto de contratos inteligentes) que estableció la señalización del camino de Blockchain.

Pero no fue hasta el 31 de octubre de 2008 que Satoshi Nakamoto publica su icónico documento de investigación "The White Paper" en el que establece todo un sistema de dinero electrónico

"peer-to-peer", independiente de intermediarios. Todo el sistema de Nakamoto se base en la tecnología de Blockchain. Y en menos de un año más tarde Nakamoto genera el primer bloque de la cadena de bloques de Bitcoin, denominado el bloque "Génesis", que marcó el inicio de Blockchain que hoy conocemos en día.

2.2.3 Características y atributos del Blockchain

Blockchain se caracteriza por ser una cadena de bloques que tiene la responsabilidad de generar un mecanismo para la encriptación y cifrado seguro de las reglas del protocolo que rigen su sistema. Este sistema de criptografía es fundamental en Blockchain para la manipulación de los datos almacenados en ella por medio del "Nonce" y el "Hash". Dicho sistema garantiza que no exista manipulación, hurto o eliminación de los datos por los distintos miembros que partición en la red.

A continuación, se describirá de manera detallada las principales características de la tecnología detrás de Blockchain:

La primera característica que dicta Blockchain es el registro de la información distribuida. A diferencia de las tecnologías de bases de datos centralizada (información almacenada en un solo lugar físico y controlada por una sola entidad) la cadena de bloques almacena toda la información en distintos equipos de cómputo interconectados (nodos) y estos en conjunto controlan la red de Blockchain. Todos los participantes o usuarios tienen una copia de todos los bloques en cadena de la red y ningún participante puede añadir, modificar o eliminar información sin el consenso y autorización del resto.

La inmutabilidad es un aspecto fundamental de la cadena de bloques, ya que en ningún caso se puede editar o borrar información que haya sido validada y añadida en Blockchain. Si algún nodo es comprometido (ataque cibernético, falla de hardware, falla de software, entre otros) inmediatamente todos los otros nodos mantendrán la base de datos integra y suplantaran al nodo comprometido. A su vez, si se llegara a modificar información en la Blockchain por algún nodo

este sería rechazado por el resto de los nodos ya que alteraría la cadena subsecuente a la misma cambiando su encriptación la cual sería diferente a la cadena de los demás nodos, con lo que los nodos de la red rechazan el cambio.

Si por algún motivo se necesita modificar la información de alguna transacción en algún bloque de la cadena de bloques, esta modificación se debe hacer agregándola en otro bloque para que cronológicamente tenga validez sobre la transacción origen.

Siguiendo con la próxima característica de Blockchain se encuentra el protocolo de consenso el cual permite que la información contenida en un bloque sea considerada valida por todos los nodos y esta pueda ser desplegada a la red de Blockchain. El protocolo de consenso permite que los distintos nodos no tengan por qué confiar unos en otros y aun así puedan compartir un registro de información confiable. No hace falta una persona o entidad centralizadora que legitime la información guardada en la cadena, ya que es segura por naturaleza (según el tipo de red). Está garantizada por la matemática, por la criptografía.

La trazabilidad y transparencia son dos de las características resaltantes de la tecnología de Blockchain, esto a raíz del encadenamiento sucesivo de los bloques basado en la criptografía de este (Hash). Dichas características brindan a la tecnología un orden cronológico de los eventos, de modo que las cada una de las transacciones está dotada de trazabilidad y transparencia. Toda información almacenada en la cadena es susceptible de ser consultada y auditada.

Como ultima característica fundamental de Blockchain se encuentra la criptografía, que es el corazón de esta. Gran parte de la seguridad de la información en Blockchain se debe al uso de métodos criptográficos para encriptarla, una de las principales herramientas para hacerlo son los denominados Hash.

2.2.4 Elementos de Blockchain

Antes de poder entrar en materia sobre el funcionamiento de Blockchain en este apartado del documento, se debe aclarar que dentro del entorno de la tecnología existen conceptos que se deben abordar para poder tener un panorama holístico de la misma. A continuación, se describen dichos conceptos claves.

2.2.4.1 Red Peer-to-Peer

La red de Blockchain está conformada por una serie de nodos que tienen una comunicación de esquema descentralizado, con lo que no existe un nodo y/o elemento administrador. Comprende una red de pares, o red entre iguales, en donde todos los nodos que hacen la red se compartan exactamente iguales entre ellos, interactuando a la vez como servidores y clientes del resto de nodos en la red.

El principal beneficio de la red peer-to-peer es su solidez frente a contingencias, ya que cada nodo funciona de madera totalmente independiente. De manera que si un nodo presenta algún tipo de compromiso este será remplazado por sus nodos semejantes para que la red siga funcionando de manera correcta.

2.2.4.2 Encriptación de clave pública

El manejo de la encriptación en la tecnología de Blockchain tiene dos propósitos. El primero busca otorgar direcciones seguras al emisor y receptor de una transacción. Este primer propósito en realidad es la encriptación de la conocida IP publica en la comunicación de internet, en Blockchain a esto se le conoce como llave pública.

Cualquier usuario que necesite realizar una transacción en la red de Blockchain necesita un par clave pública/privada para poder realizar cualquier transacción de envió y/o recibo de información. De la sentencia anterior nace el segundo propósito de emplear encriptación, misma

que es que todas las transacciones van firmadas digitalmente por el emisor, para garantizar la autoría de esta.

2.2.4.3 Algoritmo de Consenso

Para poder realizar un cambio en el libro mayor de Blockchain, la red misma debe llegar a un consenso para realizar dicha modificación. Para ello se realiza mediante un algoritmo informático.

Según (Álvarez Luis,2018) generar un consenso significa que varios servidores en la red distribuida están de acuerdo con el estado de verdad actual del sistema, o en el caso básico de Blockchain, los valores en el libro mayor distribuido. Una vez que las computadoras de la red llegan a una decisión sobre un valor, esa decisión es definitiva. En el contexto informático clásico, los algoritmos de consenso se utilizan para acordar los comandos en los registros de los servidores distribuidos.

El principal inconveniente de las redes descentralizadas es mantener la integridad de la información durante el proceso de actualización de la información que gestionan. La solución a esta problemática es la utilización del algoritmo de consenso, que no es más que todos los nodos estén de acuerdo con el cambio a realizar.

Según (Bermúdez, 2016) en la red de Blockchain se utiliza la prueba de trabajo Proof of Work (POW) que obliga al nodo a realizar un esfuerzo computacional para crear un bloque. El primer nodo que cumpla con la prueba de trabajo lo anuncia en la red con el fin de que el resto de los nodos conozcan quien es el ganador, validen la información y por lo tanto el nodo que podrá modificar la información.

Según (Melanie Swan, 2018) en las redes Blockchain, los tres tipos principales de algoritmos de consenso para llegar a un acuerdo de manera distribuida son Prueba de Trabajo (POW), Prueba de Participación (POS) y Práctica de la tolerancia a falta bizantina (PBFT). La principal

innovación del protocolo Blockchain es la estructura de datos sobre un algoritmo de consenso, que permite construir una red distribuida abierta en la que todas las partes pueden llegar a un acuerdo.

La prueba de trabajo Proof of Work (POW) por sus siglas en inglés, es un método cuya principal función es evitar comportamientos maliciosos en un sistema informático. Para llevar a cabo este algoritmo los mineros deben realizar un trabajo que sea muy costoso para ellos, pero fácil de verificar para el resto de la red. Dicho trabajo es computacional y para llevarlo a cabo el coste es elevado en procesamiento, que se traduce a tiempo, electricidad y hardware.

"Los algoritmos que operan el sistema distribuido recompensan a los mineros que resuelven problemas matemáticos. El incentivo financiero para cada minero es ser el primero en crear el nuevo bloque de transacciones que las otras máquinas tomarán como el nuevo estado de verdad de la red. El lucrativo registro de transacciones ha generado operaciones dedicadas exclusivamente a la minería." (Melanie Swan ,2018, p.36)

Otro algoritmo de consenso que se encuentra disponible para su aplicación en la red de Blockchain es el de Prueba de Transacción (POS) Proof of Stale de sus siglas en ingles. El algoritmo de consenso se basa en la participación de la red. En los sistemas POS, el autor de un nuevo bloque se elige de manera determinista, dependiendo de su participación o grado de compromiso (riqueza) dentro de la red. Este método a menudo no se toma en cuenta por su poco beneficio a la red.

El tercer algoritmo de consenso aplicado a las redes de Blockchain es la Práctica de la tolerancia a falta bizantina Practical Byzantine Faul Tolerance (PBFT) por sus siglas en inglés.

"Básicamente, mediante el envío de mensajes entre los nodos 'validadores' se intenta averiguar si existe alguno que falla o perturba a la red para aislarlo del sistema. Es la capacidad de un sistema informático distribuido para operar independientemente de los nodos defectuosos

(malintencionados o no). PBFT confía en que haya una diversidad de participantes en el sistema distribuido (unos pocos cientos). Para cada bloque en el caso de las transacciones, los algoritmos seleccionan al azar un grupo pequeño y único de usuarios de manera segura y justa. Para protegerlos de los atacantes, las identidades de estos usuarios generalmente se ocultan hasta que se confirma el bloqueo. El tamaño de este grupo generalmente permanece constante a medida que la red crece." (Melanie Swan ,2018, p.42)

Sin embargo, en este último método descrito se pierde descentralización ya que los nodos validadores que están a cargo de la votación son elegidos por una autoridad central, es decir una unidad centralizadora.

2.2.5 Los Mineros

Existen tres tipos de nodos dentro de la red de Blockchain, entre ellos están los usuarios, los desarrolladores y por ultimo los mineros. No todos los nodos de la red de Blockchain participan en resolver los retos matemáticos de pruebas de trabajo, únicamente aquellos nodos que sí participan en dicha competición se les denomina "mineros". La denominación minero es una analogía de un trabajador en busca de un metal precioso, en este caso ese metal es una criptomoneda.

Según (Lérida & Pérez, 2016) los mineros son computadores que aportan poder computacional a la red, además estos son los encargados de crear los nuevos bloques, a los que incorporan las transacciones que validan, y a su vez tratan de añadirlos a la Blockchain. En las redes Blockchain, cada vez que un minero consigue resolver el reto recibe una recompensa por su esfuerzo, ya que al ser redes descentralizadas es la propia red la que debe pagar de alguna forma a los nodos para que estos trabajen para la red.

"Reciben dos tipos de incentivos: las nuevas monedas creadas en el bloque y todas las comisiones de las transacciones incluidas en el bloque." (Caballero, 2018, p.69).

“A sí mismo la minería sirve para asegurar el sistema contra transacciones fraudulentas o transacciones que gastan la misma cantidad de criptomonedas más de una vez, por lo tanto, si un usuario intenta reutilizar monedas que él mismo ya gastó, la red lo detectará y rechazará la transacción”. (Santiago, 2016, p.32)

2.2.6 Transacción

Las transacciones en el entorno de Blockchain, son un elemento central, mediante la cual una dirección de la red envía un mensaje a otra dirección de la red. El objetivo principal de una transacción es realizar de forma segura movimientos de unidades monetarias o tokens entre usuarios. En el protocolo de Blockchain una transacción se compone de dos partes principales.

La primera parte de una transacción es su salida, que es la transferencia de fondos o tokens. Indica la cantidad de fondos a transferir y el destinatario de estos. La segunda parte de una transferencia son sus entradas, que no son más que los fondos a utilizar en la transacción.

2.2.7 Bloque de la cadena

Se trata de un contenedor de un conjunto de transacciones que los mineros agrupan para poder resolver el reto matemático. Los mineros son los encargados de generar un bloque con una frecuencia única, cabe mencionar que esta varía dependiendo de la Blockchain. El bloque se componer de una cabecera, que contiene los metadatos, seguido de una larga lista de operaciones que componen la mayor parte de su tamaño.

2.2.7.1 Cabecera del bloque de la cadena

Este elemento se compone de tres subconjuntos de metadatos. En primera posición, se contempla una referencia al Hash del bloque anterior, que conecta este bloque al anterior dentro de la cadena de bloques; en segunda posición se encuentra los metadatos que están relacionados con la competencia en la minería; la última pieza de metadatos es la raíz del árbol merkle, una estructura de datos utilizada para resumir, de manera concisa, todas las transacciones en el bloque.

2.3 Funcionamiento de Blockchain

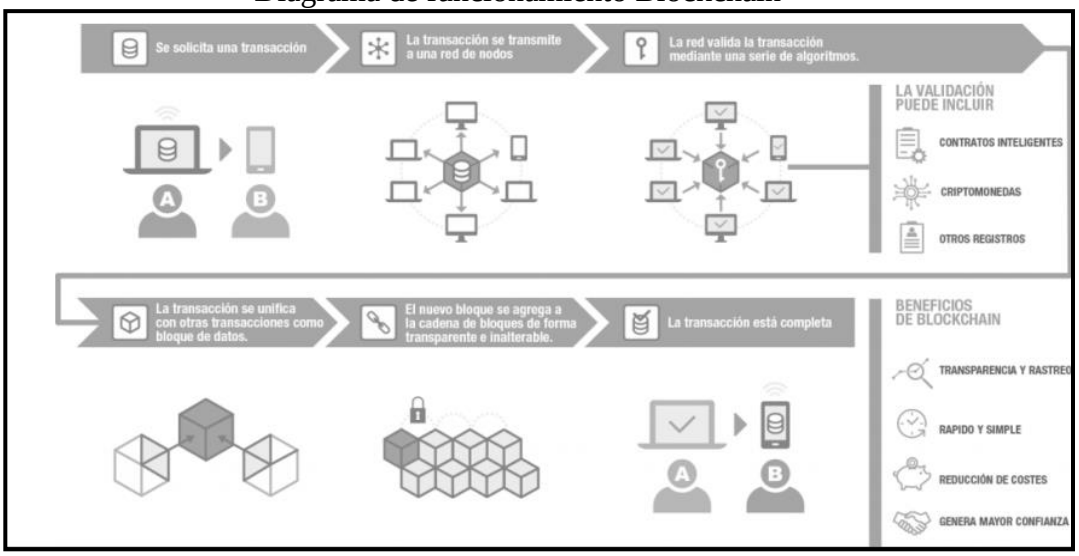
Según lo dictado en las páginas anteriores la tecnología de Blockchain se base en tres fundamentos esenciales que son: el registro compartido de las transacciones, el consenso para verificar las transacciones realizadas y por último la criptografía que fundamenta todo. Dicho todo lo anterior a continuación se dicta el funcionamiento de Blockchain y como cada uno de sus elementos se integran para conformar un bloque. En Blockchain, las transacciones se producen entre usuarios anónimos (su identidad no consta en ningún lugar) mediante criptografía de clave pública, es decir, cada usuario posee una clave privada, que solo él conoce, y una clave pública, que es la que comparte con los demás nodos.

Según (Dwyer, 2014) todas las transacciones se comunican a todos los nodos de la red. Los nodos verifican las transacciones y las van agrupando en bloques. Cada bloque se identifica por medio de un Hash: un valor único calculado criptográficamente a partir del contenido del bloque, e incluye una referencia al Hash del bloque anterior, de modo que los bloques quedan enlazados. Esta cadena de bloques es pues un registro de transacciones o libro contable (ledger) público, compartido por todos los nodos de la red.

Siguiendo este procedimiento, todos los nodos pueden verificar que las claves utilizadas son correctas y que las transacciones realizadas proceden de uno de otros bloques evitando el gasto doble. Sin embargo, una transacción se considera procesada cuando forma parte de un bloque añadido a la cadena de bloques. Para añadir un bloque hace falta minarlo, o lo que es lo mismo, calcular su Hash, lo cual requiere resolver un problema matemático único de gran dificultad que consume unos recursos informáticos muy considerables, máxime cuando sabemos que la dificultad de resolución del Hash se reajusta periódicamente para adaptarse a la capacidad de proceso de la red: a medida que aumenta la potencia de los ordenadores conectados, la dificultad del problema crece.

Figura No. 1

Diagrama de funcionamiento Blockchain



Fuente: (Dwyer, 2014)

2.4 Seguridad en Blockchain

En el siguiente apartado del documento se dictará las problemáticas de seguridad que la tecnología Blockchain se encarga de cubrir mediante sus procedimientos y bases criptográficas. Cabe mencionar que la tecnología Blockchain dispone de los tres pilares de la seguridad informática.

A lo que se refiere en confidencialidad de los datos, Blockchain, aunque originalmente fue creada sin controles de acceso específico (debido a su naturaleza pública), existen implementaciones en el mercado que comienzan a controlar el acceso a la misma proporcionando encriptación de datos de bloques y capacidades AAA.

La encriptación completa de los datos de la cadena de bloques garantiza que las partes no autorizadas no puedan acceder a los datos mientras estos datos se encuentren en tránsito (especialmente si los datos fluyen a través de redes no confiables).

Uno de los puntos más fuertes y seguros de Blockchain es el pilar de la integridad de los datos, esto debido a la inmutabilidad de estos. La tecnología Blockchain puede considerarse como una tecnología segura, desde el punto de vista que permite a los usuarios confiar en que las transacciones almacenadas en el libro de contabilidad contra manipulaciones maliciosas. La combinación de Hashing y criptografía secuencial, a lo largo de una estructura descentralizada, hace que sea muy difícil para cualquier parte manipular la información a comparación de una base de datos estándar. Esto proporciona a las organizaciones el usar las tecnologías con seguridad sobre la integridad y la veracidad de la información.

A lo que refiere en el tercer pilar de la seguridad informática, disponibilidad, la definición que usa Blockchain es "no existe un único punto de falla." La tecnología Blockchain no tiene un único punto de falla, lo que reduce considerablemente las posibilidades de que un ataque cibernético, como tal podría ser un ataque DDoS basado en IP que interrumpa el funcionamiento normal.
Si se quita un nodo, los datos siguen siendo accesibles a través de otros nodos dentro de la red, ya que todos ellos mantienen una copia completa del bloque mayor en todo momento. La naturaleza distribuida de la tecnología resuelve el problema de falso consenso.

La infraestructura de Blockchain evidentemente proporciona un nivel adicional de accesibilidad a los datos, dado que los datos son accesibles a través de cualquiera de los nodos de la red, incluso en el caso de que un ataque DDoS interrumpa algunos de los nodos.

2.4.1 El problema del 51%

Lérida & Pérez (2016) definen

> Todo el mecanismo que tiene una aplicación descentralizada (Dapp) para su funcionamiento tiene un punto débil que se conoce de antemano y de difícil resolución: el problema del 51%. Cuando más del 51% de la tasa de Hash está controlada por un solo nodo (un minero o grupo de mineros), la cadena de bloques se puede distorsionar maliciosamente. El ataque del 51%

también resulta en una bifurcación, que es donde hay dos bloques conflictivos compitiendo para la adición a la cadena de bloques. (p. 22)

Sanz (2017) define

> Si se modifica un bloque en medio del Blockchain, los enlaces Hash no coincidirán y deberán crear nuevamente. Para hacer esto, los bloques posteriores deben ser re-minados para incluir los nuevos Hashes que se deben volver a calcular. En el caso entonces que un atacante quisiera modificar un valor por su beneficio e intente reconstruir la cadena modificada calculando los Hashes, debería tener el control de al menos el 51% del recurso que utilice el protocolo de consenso, para que pueda reconstruir la cadena a una velocidad superior a la que ésta se genera. Esta vulnerabilidad afecta principalmente a las plataformas que utilizan prueba de trabajo o prueba de participación, pero aun así es una situación difícilmente realizable, dado que significaría tener el 51% de la potencia computacional o el 51% de las criptomonedas de toda la red. (p. 36)

2.4.2 El doble gasto

Satoshi Nakamoto en su famoso documento “The White Paper” aborda la problemática del doble gasto y como esta ha sido el mayor freno a la comercialización de divisas electrónica. “La tecnología Blockchain resuelve un importante problema informático que había sido una barrera para tener un sistema monetario digital funcional durante años: el problema del doble gasto” (Satoshi Nakamoto, 2008).

“El problema del doble gasto es que el dinero solo debe gastarse una vez, a diferencia de un archivo, que puede ser copiado arbitrariamente muchas veces” (Melanie Swan, 2018).

Efanov & Roschin (2018) determinan

> El doble gasto ocurre cuando alguien hace más de un pago usando un cuerpo de fondos. Esto es posible en una red peer-to-peer porque puede haber retrasos de propagación cuando los pagos pendientes se transmiten a la red o a las redes y los nodos reciben transacciones no confirmadas en diferentes momentos. Blockchain aborda este problema requiriendo que los nodos mineros resuelvan un problema matemático complejo para verificar la transacción. La complejidad del cálculo se ajusta de modo que, en promedio, se necesita 10 minutos para resolver un problema utilizando los poderes de procesamiento de los mineros. Porque solo bloques con respuestas correctas al problema matemático se pueden agregar a la cadena, solo uno entre los pagos múltiples es aceptado y registrado en la Blockchain, por lo que es casi imposible para las partes gastar fondos doblemente. Los sistemas centralizados de almacenamiento y administración de datos son susceptibles de piratería, intrusión e incumplimientos, pero el mecanismo de consenso distribuido Blockchain evita el hackeo. Cada transacción debe ser verificada por la comunidad de mineros, dejando transacciones fraudulentas que no pueden pasar la verificación colectiva y validación porque Blockchain es constantemente monitoreada por toda la red de nodos, cada uno de los cuales mantiene una copia de la cadena de bloques, los usuarios maliciosos no tienen forma de insertar bloques fraudulentos en el libro de contabilidad público sin ser notado inmediatamente por otros. Por lo tanto, es imposible comprometer la integridad de los registros en el Blockchain. (p.48)

2.5 Tipos de Blockchain

“Los tipos de Blockchain se pueden clasificar en función del acceso a los datos, la distinción entre los tipos de Blockchain es el esquema del libro distribuido y quién puede participar en el sistema” (Viriyasitavat & Hoonsopon, 2018).

De acuerdo con la premisa de Viriyasitavat & Hoonsopon existen tres tipos de Blockchain las cuales son públicas, privadas e hibridas.

2.5.1 Blockchain públicas

Oh & Shong (2017) definen

> Son de tipo abierto, en el que cualquiera puede participar. Todos los participantes pueden acceder libremente a datos y realizar transacciones, pero dado que numerosos usuarios no verificados están participando, se necesita cifrado y verificaciones avanzadas, por lo tanto, la expansión de la red se torna lenta y difícil. Además, el Blockchain público forma una perfecta estructura distribuida, y los participantes de la red son pseudoanónimos, por lo tanto, no es apropiado para los servicios financieros y gubernamentales que necesitan ser controlados por la información centralizada del sistema de gestión. (p.123)

2.5.2 Blockchain privada

“En ella el propietario genera y maneja el Blockchain. Esto es apropiado si el propietario desea administrar la Blockchain como el sistema centralizado” (Oh & Shong, 2017).

Viriyasitavat & Hoonsopon (2018) definen

> Los libros contables son compartidos y validados por un grupo predefinido de nodos. El sistema requiere iniciación o validación a los nodos que desean ser parte del sistema. Los

nodos autorizados son responsables de mantener el consenso. Blockchain privadas son adecuadas para sistemas cerrados, donde todos los nodos son completamente confiables. En definitiva, es el propietario quien tiene la máxima autoridad para controlar el acceso a nodos autorizados. (p.89)

2.5.3 Blockchain Hibridas

Oh & Shong (2017) definen

> Es el tipo intermedio de Blockchain pública y privada. A diferencia de Blockchain Privadas en el que el propietario tiene la autoridad, son los nodos preestablecidos quienes tienen la autoridad en este tipo de Blockchain. Por lo tanto, Blockchain Hibridas mantienen una estructura distribuida al mismo tiempo que fortalece la seguridad mediante una participación limitada, y resuelve el problema de la lenta velocidad de transacción y los problemas de escalabilidad de la red planteados en Blockchain Pública. (p.90)

Viriyasitavat & Hoonsopon (2018) aclaran

> La Blockchain hibrida es adecuada para sistemas semicerrados compuestos por unas pocas empresas, a menudo organizadas en forma de consorcio. El grado de apertura de los datos varía, por lo general con controles de acceso, definidos por el consorcio, para controlar el acceso en ambos participantes y la información dentro de Blockchain. A pesar de que el sistema no está
>
> completamente abierto, los beneficios de la descentralización se pueden obtener parcialmente. Hyperledger Fabric, Ripple y Stellar son ejemplos de implementaciones de Blockchain Hibridas. (p. 66)

Tabla No 1. Características según tipo de Blockchain

Tipo de Blockchain	Blockchain pública	Blockchain híbrida	Blockchain privada
Nodo gestor	Todos los nodos de la red (descentralizada)	Nodos participantes del consorcio	Un nodo centralizado contiene toda autoridad
Gobernanza	Es casi imposible cambiar las reglas del negocio.	Las reglas del negocio se pueden cambiar si los participantes del consorcio están de acuerdo.	Las reglas del negocio se pueden cambiar con facilidad a criterio del nodo centralizador.
Velocidad de Transacción	La velocidad de transacción es lenta y es difícil su expansión.	Es sencillo expandir la red y la transferencia de datos es rápida.	Es sencillo expandir la red y la transferencia de datos es rápida.
Acceso a los datos	Cualquier nodo puede acceder a los datos.	Solo los usuarios autorizados pueden acceder a los datos identificándose.	Solo los usuarios autorizados pueden acceder a los datos identificándose.
Identificabilidad	Seudo-anónimo	Es identificable el usuario.	Es identificable el usuario.
Prueba de Transacción	La entidad para la prueba de la transacción se decide mediante algoritmos como PoW y PoS.	La verificación de la transacción y generación de bloques se realizan de acuerdo con las reglas acordadas de antemano.	La prueba de transacción es realizada por la institución central.

Fuente: Oh, J., & Shong, I. (2017).

2.6 Contratos inteligentes

El término contrato inteligente o más conocidos como Smart contract en su traducción a las inglés, hacer referencia a cualquier contrato que se ejecute por sí mismo automáticamente sin necesidad de mediador o un tercero entre participantes individuales. El contrato se escribe por medio de programas informáticos, como lo es solidity, este puede definir las reglas del negocio y consecuencias estrictas.

El concepto lo define el criptógrafo Nick Szabo en 1994, sin embargo, no es hasta los últimos cinco años que en concepto se vuelve una realidad tangible gracias a los protocolos de cifrado y a la tecnología de Blockchain.

Sin importar el tipo de Blockchain, uno de los principales usos potenciales de la tecnología es la posibilidad de escribir algoritmos (procesos, condiciones, acciones) en un bloque, los cuales se ejecutarán cuando se cumpla(n) alguna(s) condiciones preestablecidas. A estos algoritmos se los llama contratos inteligentes. Desde la realización de transferencias financieras periódicas hasta pagos una vez confirmado un envío, el potencial de los contratos inteligentes es alto. Una vez escrito el código y firmado digitalmente a la hora de agregarlo a la cadena de bloques, su ejecución (cuando se cumpla alguna condición establecida o se realice la activación de este a través de un pago) es realizada y corroborada por todos los participantes de la red.

Si bien puede haber un alto potencial detrás del uso de contratos inteligentes existen algunos puntos a considerar. El primero es que, efectivamente, una vez escritos los contratos en Blockchain, estos quedarán inscritos en la cadena de bloques como cualquier otra información. Es decir: no podrá cambiarse ni podrá terminarse, a menos que el contrato mismo incluya alguna condición para hacerlo.

En segundo lugar, cualquier pago o transferencia vinculados a esta transacción se podrán realizar dentro del mismo ámbito de la cadena. Es decir, para las redes permisionadas basadas en criptomonedas, la mayoría de los pagos y transferencias será en la criptomoneda que la cadena de

bloques soporte. En el caso de las redes no permisionadas a fin de disponer dinero virtual para realizar transacciones, este se debe tokenizar; este dinero tokenizado permite poder comprar y vender activos. Finalmente, es importante mencionar que cualquier falla en el código del contrato puede tener consecuencias no anticipadas, desde la posibilidad de fraude por parte de programadores que explotan alguna debilidad en el código hasta el estancamiento de dinero por alguna falla en el código que, por ejemplo, reduzca el balance de una cuenta, pero no aumente el de ninguna otra.

En resumen, los contratos inteligentes son scripts modulares, repetibles y autónomos que normalmente se ejecutan en un Blockchain y representan promesas unilaterales de proporcionar una tarea informática determinada. Estos scripts se almacenan en el Blockchain, en una dirección específica que se determina cuando se implementan los contratos en el Blockchain. Cuando se produce un evento contemplado en el contrato, se envía una transacción a esa dirección y la máquina virtual distribuida ejecuta los códigos de operación del script (o cláusulas) utilizando los datos enviados con la transacción.

Los contratos inteligentes pueden estar codificados de modo que reflejen cualquier tipo de lógica empresarial basada en los datos: desde acciones tan sencillas como votar por una publicación en un foro hasta acciones con un mayor nivel de complejidad, como garantías de préstamos y contratos de futuros, así como acciones sumamente complejas como la fijación de prioridades de pago en una nota estructurada.

Figura No. 2

Diagrama de funcionamiento Tokenización

Fuente: Oh, J., & Shong, I. (2017).

2.7 Tokenización de Activos

Hasta ahora se han mencionado las transacciones monetarias escritas y transferidas en la Blockchain. Las sumas y restas de las billeteras tenían la misma unidad de medida y lo importante es la verificación del saldo final. Sin embargo, se podría reemplazar la moneda por distintas fichas (tokens), cada una de las cuales representa un activo distinto (una parte o la totalidad de un activo, físico o virtual, por ejemplo). Así, lo importante ya no será el saldo al final de todas las transacciones sino cada transacción de manera individual, ya que cada una es una representación en Blockchain de un cambio (transferencia de propiedad, por ejemplo) de algún activo.

2.8 Time Stamping

Cuando se valida una transacción y se agrega a un bloque en la cadena, esta validación incluirá la hora exacta de la transacción y la firma digital de quien la haya enviado. Esta verificación de la fecha y hora de una transacción, llamada time stamping, puede a veces ser muy valiosa en sí misma porque puede servir para demostrar el momento en que una acción específica ocurrió. La consistencia en la información entre todos los nodos participantes minimiza la

probabilidad de manipulación y otorga un alto grado de certeza respecto del momento en el que se realizó la transacción.

2.9 Beneficios de Blockchain

Es importante notar que, como se ha explicado, el uso de una Blockchain privada afecta el alcance de algunos atributos, los cuales dependerán en estos casos del protocolo de consenso que se utilice, del número de nodos que sean parte de la red y del grado de independencia de los nodos. Finalmente, también es importante mencionar que la inmutabilidad de la información en Blockchain es producto de varios atributos: la distribución en tiempo casi real, el encadenamiento y el mecanismo de consenso. Sin embargo, cabe destacar que el grado de inmutabilidad de la información es directamente proporcional al número de nodos independientes que existan en la red.

Tabla No 2. Beneficios de Blockchain

Atributo	Beneficio	Descripción	Consideraciones
Distribución en tiempo Semi real	Constancia en la información entre todos los nodos.	La información es copiada automáticamente en múltiples nodos en tiempo semi real como parte del protocolo de consenso.	En redes públicas el consenso demora alrededor de 10 minutos, puede llegar a tardar una hora dependiendo el número de confirmaciones.
Lectura	Transparencia	Todos los nodos participantes pueden acceder a la información de la red Blockchain.	En redes privadas se puede restringir el acceso a cierto tipo de usuarios.
Escritura	Acceso extendido	Todos los nodos pueden agregar información a Blockchain.	En redes privadas se puede restringir el acceso a cierto tipo de usuarios. (distinto al que tiene el acceso de lectura).
Encadenamiento	Seguridad en la	No se puede editar ni borrar un	Dependiendo del

	trazabilidad.	bloque, solo se puede agregar uno nuevo.	protocolo de consenso, los bloques se pueden cambiar si el 50%+1 de los nodos unidos. En redes privadas, dependiendo del número de nodos, esto puede ser más sencillo.
Protocolo de consenso	Prescindir del intermediario de confianza	Proceso para agregar nuevos bloques de cadena sin necesidad de un intermediario o entidad de validación.	El POW retrasa el registro de transacciones y con- sume mucha energía. En redes privadas se puede tener más flexibilidad para validar transacciones, incluyendo a uno o varios intermediarios
Firma digital y encriptación	Seguridad de la información, time stamping	La información que se agrega a la cadena es firmada digitalmente y encriptada	Cada usuario tiene credenciales para escribir en la cadena. En redes privadas es posible que se necesiten credenciales para leer también.
Contratos inteligentes	Certidumbre y reglas claras	Algoritmos incluidos en la Blockchain con reglas que se activan cuando cumplen ciertos criterios predefinidos.	En general, el código deber ser auditado minuciosamente, en particular en aquellos contratos que incluyan condiciones complejas o involucren grandes cantidades de dinero. La interfaz con el mundo externo en muchos casos igual requiere de un tercero de confianza.

Fuente: Florencia Setale,Christoph Redl & Arturo Muente-Kunigami, (2019).

2.10 Blockchain en el mundo

Como se dictó en el paso apartado del documento Blockchain es una base de datos de transacciones que se guarda en varias computadoras (nodos) y que crece constantemente a medida que se le agregan nuevas transacciones o las ya conocidas "bloques", que permite la transferencia de datos digitales con una codificación muy sofisticada y que, en sus orígenes, generaba más confianza que los propios intermediarios en materia de seguridad, formando una cadena de datos pública.

Aunque esta cadena de bloques ha estado vinculada normalmente a las criptomonedas, este sistema tiene futuro más allá de la economía. Cualquier área podría ser transformada por esta tecnología por su versatilidad cambiando así la manera que tenemos de entender los negocios y la sociedad.

Términos como “bitcoin” o “Blockchain” se extienden cada vez más en el mundo digital con proyectos que buscan evolucionar a la nueva era. Estas tecnologías todavía tienen mucho que avanzar, pero, su crecimiento va avanzando exponencialmente, con la motivación de buscar nuevos espacios de aplicación más allá de las clásicas transacciones.

2.10.1 Importancia en un mundo globalizado

Actualmente se encuentra en la era en donde todo empieza a evolucionar y se empieza a dejar los estándares antiguos y se adopta la mentalidad de transformación digital. Es imperativo mantener una constante capacitación informativa acerca de cómo se trabajan y en qué consiste la utilización de las monedas digitales para un futuro financiero al alcance de la mano.

El registro de las transacciones financieras apoya a la organización, ordenamiento y determinación del flujo de efectivo que se posee, así como la capacidad adquisitiva, y los haberes existentes. Si el registro es robado, borrado o desaparecido, no se podría conocer el estado de cuentas o dónde está alojada los bienes adquiridos.

Blockchain aún está en creciendo, pero, no impide que muchos inversores pongan sus esperanzas en el crecimiento de este. Muchas empresas han invertido millones en el proyecto, haciendo que las monedas digitales sean más famosas, incluso Mark Zuckerberg creador en Facebook está dispuesto a entrar en el negocio Blockchain, para mejorar la experiencia del usuario y dar un valor agregado a dicha plataforma social.

En el ámbito social, el Blockchain permite un mayor nivel de transparencia en organismos como ONG, donde las donaciones están en la actualidad gestionadas por intermediarios que en muchos casos no hacen una distribución justa del dinero aportado por los donantes. Cualquier sector que centralice en una base de datos la información de la que disponen a través de diferentes fuentes, puede poner en marcha el sistema de bloques, lo que traerá numerosos beneficios tanto para las entidades como para sus clientes.

Radoslav Dragov, el líder de tecnología Blockchain de la International Data Corporation, explicó que hay una serie de factores que pueden crear condiciones favorables para la adopción, que van desde la inversión hasta el talento, comentando lo siguiente:

Radoslav Dragov (2019) define

> Más allá de estos factores, la inversión en la Blockchain está muy influenciada por la regulación actual y futura, y la actitud general del Gobierno hacia esta tecnología. En algunos casos, falta la regulación y esa incertidumbre puede asustar a muchos inversores. Al adoptar una reglamentación favorable a las empresas, algunos países europeos como Suiza, Estonia y Malta se han convertido en terreno fértil para muchas empresas Blockchain. (p. 36)

El Medio Oriente es un centro de tecnología floreciente. Muchos países, especialmente los pequeños estados productores de petróleo tienen sus propias zonas económicas libres dedicadas a fomentar el desarrollo tecnológico y la innovación. Sólo los Emiratos Árabes Unidos tienen 45 y tanto Arabia Saudita como Omán están desarrollando rápidamente las suyas propias. Saba Kifle, de Miami Devcon, dijo a Cointelegraph que los Gobiernos de Oriente Medio y África.

Saba Kifle (2018) afirma

> En última instancia, los organismos gubernamentales de cada una de estas regiones han invertido fuertemente en la comprensión de cómo la Blockchain y las monedas digitales pueden mejorar las perspectivas económicas de sus regiones. Y lo que es más importante, han tomado medidas inteligentes y cautelosas para hacer frente a las arenas reglamentarias para probar cómo estas tecnologías afectarán a esa población. (p.99)

Europa es uno de los principales puntos financieros del mundo. El entorno reglamentario de Europa está bien desarrollado y la tecnología emergente goza de un fuerte apoyo tanto académico como político. Además, la Unión Europea está interesada en la Blockchain. La Comisión Europea, el órgano ejecutivo de la Unión Europea (UE), está explorando activamente las formas de aplicar la tecnología. El director ejecutivo de INATBA, Marc Tavener, expuso a Cointelegraph su opinión de que Europa tiene una ventaja.

Afirma (Marc Tavener, 2018) estamos viendo continuas inversiones (públicas y privadas) que dan a Europa una ventaja competitiva en cuanto a cómo se está implementando la tecnología en los Gobiernos, empresas e instituciones.

2.11 Blockchain en Latinoamérica

IBM ha anunciado que invertirá 5,5 millones de dólares hasta 2020 en el primer centro de soluciones dedicadas a “Blockchain”, o cadena de bloques en América Latina, que estará ubicado en la ciudad brasileña de Sao Paulo. La noticia llega en un momento especialmente relevante para el desarrollo y expansión de Blockchain en toda la región, que es contemplado por los especialistas como una oportunidad para que la economía de muchos países del cono sur reciba nuevos impulsos al margen de la economía tradicional.

El nuevo “hub” que acaba de anunciar el gigante informático está diseñado para ayudar “a los clientes a construir una nueva generación de aplicaciones de ‘Blockchain’ en la plataforma IBM Cloud, con los niveles más altos de seguridad”, según ha destacado la compañía. El centro “permitirá a los clientes en toda América Latina abordar nuevas formas de transacciones empresariales”, explicó Ana Paula Assis, gerente general de IBM Latinoamérica, citada en la nota.

Con esta infraestructura, que comenzará a operar en el segundo trimestre de 2018, Brasil se une al grupo de cinco países -Reino Unido, EE.UU., Canadá, Japón y Alemania-, que poseen infraestructura de IBM Cloud con capacidades de “Blockchain”. Esta inversión, además, ofrecerá a los clientes en Latinoamérica de la firma estadounidense “un lugar único para desarrollar todo el ciclo de vida de las soluciones comerciales de ‘Blockchain’, desde el inicio, en IBM Cloud”, añadió la compañía.

Lo que permite aligerar la carga de trabajo de confirmación y pago. Cada vez son más las iniciativas Blockchain en América Latina, así como la organización de eventos que buscan informar sobre los nuevos pasos de esta tecnología disruptiva a la que aún muchos no tienen acceso.

Según Everis(2020) afirma

> La tecnología Blockchain puede ofrecer muchas posibilidades para los bancos de América Latina, ya que pueden realizarse transacciones de una forma más rápida, menos costosa y con menor margen de error. De hecho, algunos bancos globales de los que operan en México ya están en periodo de pruebas. Tal es el caso del español BBVA, que en noviembre pasado realizó un piloto de una transacción a través de Blockchain, al presentar de forma electrónica en una operación de importación-exportación entre España y México. (p.36)

En abril, se celebrará simultáneamente en Colombia y Argentina el Congreso Internacional Blockchain Argentina -Colombia- Rusia que tendrá como escenario tres ciudades diferentes: Córdoba y Buenos Aires (Argentina) y Bogotá (Colombia).

Su objetivo del congreso es abrir diálogos entre Latinoamérica y la comunidad cripto Internacional para enseñar a las personas acerca de las oportunidades de las criptomonedas para que cada persona tenga muchos beneficios de estas. También para atraer mayores inversiones extranjera y adaptar prácticas avanzadas económicas digitales basada en Blockchain.

En Brasil, el startup de pagos móviles Ubank recientemente ha lanzado una venta de tokens para Ubcoin Market, un ecosistema que permitirá a los usuarios convertirse en inversionistas de la criptomoneda por el simple hecho de la venta de bienes reales y recibir las criptomonedas en su cambio.

Ubcoin Market cubre la brecha entre la criptomoneda y el mundo real. Por otro lado, aquellos que no tienen gran conocimiento sobre Blockchain podrán convertirse en inversores de manera fácil y segura, y, por otro lado, miembros experimentados del universo descentralizado tendrán el poder de gastar su dinero sin convertir a monedas fiduciarias.

Ubcoin Market ofrece una solución para dos oportunidades claras y objetivas. La primera oportunidad viene de casi 2.000 millones de ciudadanos digitales, muchos de los cuales, como ocurre en América Latina, están muy interesados en criptomonedas, pero tienen dificultades de acceso debido a barreras tecnológicas y legales. La segunda cuestión es la que enfrenta a más de 23 millones de propietarios de criptomonedas que no son capaces de gastar fácilmente sus inversiones debido a restricciones impuestas por las organizaciones gubernamentales y financieras.

Y es que en América Latina el 49% de los adultos no tiene acceso a una cuenta bancaria. Este escenario hace que el principal motor para acelerar este mercado provenga de las empresas de tecnología financiera o fintech, que están ofreciendo alternativas al mercado bancario tradicional.

En los próximos meses los modelos de negocios de bancos y aseguradores deberán tener componentes basados en tecnologías sustentadas en el Internet de las Cosas, machine learning, big data, Blockchain, criptomonedas y realidad virtual.

Los expertos se muestran convencidos de que solo de esta manera se dará respuesta a una nueva complejidad de las industrias para prever el comportamiento de los consumidores.

Marcelo Spaziani, vicepresidente de ventas de IBM América Latina, explicó:

> El Blockchain ha tenido en el último tiempo un papel fundamental para los negocios, a medida que los líderes de las distintas industrias, como finanzas, seguros o cadena de suministros, exploran cómo se puede usar Blockchain para re-imaginar la forma en que intercambian valor e información. (p.1)

Por otra parte, México se ha convertido en el primer país latinoamericano en aprobar una ley para la industria Fintech, que permite la fijación de estándares de operación para las plataformas en apoyo a los nuevos modelos financieros, así como generar una sociedad de confianza para el sector involucrado. El entorno igualitario generará mayor competencia en el medio financiero, lo que permitirá reducir los costos de gestión crediticia y el desarrollo de nuevos productos según sus promotores. Para terminar, se espera que ayude a integrar a una mayor población y empresas al ámbito financiero beneficiado así su desarrollo y la productividad del país.

Eduardo Guraieb (2018), director general de Fintech México

> Considera que la nueva ley Potenciará la atracción de inversiones en empresas de tecnología financiera, convirtiendo a México en el epicentro de innovación financiera y Fintech en América Latina, y en un agente que estimulará la inversión en el sector de Blockchain. (p. 1)

2.12 Blockchain en Guatemala

Como ya se ha dictado anteriormente en este trabajo las criptomonedas, se presentan como un candidato para cambiar el sector financiero ya que su método de libro de transacciones que se compromete a proteger los datos de sus usuarios ya que reduce los costos de transacción y fraude, algo que podría aprovechar el sector financiero.

Olav Dirkmaat,(2017) profesor de Economía de la Universidad Francisco Marroquín (UMF) resalta

> La característica que tiene Blockchain, de proteger a sus usuarios de agresiones de piratas cibernéticos ya que ayudaría a los bancos a proteger a sus clientes, como su dinero. Olav resaltó que casos como el de México, ya se están haciendo pruebas para usar la tecnología de las remesas ya que el uso de este reduce los costos, comparando con la forma tradicional como los migrantes envían fondos. (p.2)

2.12.1 Caso: Subasta Ana Café Guatemala

En Guatemala el 19 de junio de 2020, se implementó la tecnología Blockchain en una subasta de café, en un evento que buscó asegurar la trazabilidad del producto. Dicha propuesta nace de las eventualidades y coyunturas sociales debido a la pandemia COVID-19 que merma al mundo. El 17 de mayo del año 2019, se propuso implementar la tecnología del Blockchain en dicha subasta de café, en un evento en línea que buscó la adquisición del producto guatemalteco a nivel mundial.

Con un registro de 90 compradores internacionales aproximadamente, la Asociación Nacional del Café (Anacafé) realizó su primera subasta con la metodología Blockchain, con la que se recaudó ingresos por USD 250 mil. Con la idea del Blockchain, se buscó poner al café como un producto diferenciado por los demás, ya que con esta iniciativa buscó garantizar mejores precios para los productores en un espacio con precios por debajo de USD 1 por libra en la bolsa de valores.

2.12.2 Caso: Conteo de Votos

El 31 de enero del 2020, el joven guatemalteco Carlos Toriello tuvo la oportunidad de presentar la iniciativa llamada Fiscal Digital en el Capitolio de Estados Unidos en Washington DC durante el evento organizado por Government Blockchain Association (GBA) llamado el "El Futuro del Dinero, la Gobernanza y la Ley" (FoMGL) que fue auspiciado por el Comité de Trabajo de Blockchain del Congreso de Estados Unidos, entre otros. Toriello tuvo el honor de recibir en nombre del equipo de Fiscal Digital el premio anual por Valentía.

Según (Toriello, 2020) las elecciones son la experiencia cívica más enriquecedora para sus ciudadanos, porque el Estado somos todos, y el Gobierno son los mandatarios, por lo tanto, el voto es el momento en que elegimos por un tiempo definido a nuestros representantes.

Toriello participó en múltiples procesos electorales hasta el último que fue en 2019, cuando los guatemaltecos eligieron a Alejandro Giammattei como presidente de la República de Guatemala. Fue en esas últimas elecciones donde Toriello llegó a la conclusión de que se debía hacer algo para cambiar la forma de auditar los votos, ya que hubo una controversia que surgió por fallas de la página de resultados preliminares del TSE. En ese momento, fue cuando Toriello pensó en la idea de Fiscal Digital donde explicó que una certificación Blockchain es la herramienta que permitirá hacer que el voto en Guatemala sea más seguro y fiable.

Fiscal Digital nació gracias al apoyo de la Fundación Herencia Cultural Guatemalteca y otros 27 patrocinadores locales e internacionales para auditar las elecciones. Se implementó un equipo de desarrolladores jóvenes guatemaltecos y profesionales extranjeros involucrados a más de 1,500 personas, quienes para enero de 2020 generaron más de 145 mil digitaciones en base a los duplicados de informática entregados el 21 de junio del 2019 logrando validar más de 18 mil actas de las 126 mil duplicadas, entregadas por el Departamento de Informática del TSE a la fecha.

2.12.3 Ley de Contrataciones del Estado

ARTÍCULO 1. Objeto de la ley y ámbito de aplicación. *

Esta Ley tiene por objeto normar las compras, ventas, contrataciones, arrendamientos o cualquier otra modalidad de adquisición pública, que realicen:

a) Los Organismos del Estado;

b) Las entidades descentralizadas y autónomas, incluyendo las municipalidades;

c) Las entidades o empresas, cualquiera sea su forma de organización, cuyo capital mayoritariamente esté conformado con aportaciones del Estado;

d) Las Organizaciones No Gubernamentales y cualquier entidad sin fin de lucro, que reciba, administre o ejecute fondos públicos. Se exceptúan las Organizaciones de Padres de Familia - OPF-Comités, Consejos Educativos y Juntas Escolares del Ministerio de Educación para los programas de apoyo escolar; y las subvenciones y subsidios otorgados a los centros educativos privados gratuitos;

e) Todas las entidades de cualquier naturaleza que tengan como fuente de ingresos, ya sea total o parcialmente, recursos, subsidios o aportes del Estado, respecto a los mismos;

f) Los fideicomisos constituidos con fondos públicos y los fondos sociales;

g) Las demás instituciones que conforman el sector público.

Las entidades anteriores se sujetan a la presente Ley, su reglamento y a los procedimientos establecidos por la Dirección General de Adquisiciones del Estado del Ministerio de Finanzas Públicas, dentro del ámbito de su competencia, en lo relativo al uso de fondos públicos. El reglamento establecerá los procedimientos aplicables para el caso de las entidades incluidas en las literales d), e) y f).

Las adquisiciones cuya fuente de financiamiento sean recursos del crédito público, incluyendo la deuda pública de mediano o largo plazo, o fondos de contrapartida de donaciones que hagan personas, entidades, asociaciones u otros Estados a favor del Estado de Guatemala, sus dependencias, instituciones o municipalidades, se regirán por esta Ley.

Sin embargo, en el caso de los contratos, convenios o tratados internacionales de los cuales la República de Guatemala sea parte, podrán someterse a las disposiciones de tales entidades. En estos casos, las adquisiciones siempre deberán cumplir con un proceso de concurso público.

ARTÍCULO 4. Programación de negociaciones. Para la eficaz aplicación de la presente ley, las entidades públicas, antes del inicio del ejercicio fiscal, deberán programar las compras, suministros y contrataciones que tengan que hacerse durante el mismo.

ARTÍCULO 4 Bis. * Sistema de información de Contrataciones y Adquisiciones del Estado. El Sistema de información de Contrataciones y Adquisiciones del Estado denominado GUATECOMPRAS, es un sistema para la transparencia y la eficiencia de las adquisiciones públicas. Su consulta será pública, irrestricta y gratuita, y proveerá información en formatos electrónicos y de datos abiertos sobre los mecanismos y las disposiciones normadas en esta Ley y su reglamento.

El sistema será desarrollado, administrado y normado por el Ministerio de Finanzas Públicas, el cual es el órgano rector del sistema, y será utilizado por todos los sujetos obligados por esta Ley, para las compras, ventas, contrataciones, arrendamientos o cualquier otra modalidad de adquisición pública. En él se debe publicar la información relativa a todas las fases del proceso de adquisición pública, así como las codificaciones o catálogos que se establezcan para las adquisiciones públicas.

El sistema GUATECOMPRAS proveerá las herramientas necesarias para que la información sea publicada y suministrada en forma completa y oportuna, según lo establezca el órgano rector, incorporando de manera continua y dinámica las herramientas y formularios electrónicos necesarios para cada fase de los procesos de adquisición pública, incluyendo la contratación, ejecución y liquidación. La información electrónica y digital que deberá publicarse en el sistema incluirá, pero no se limitará a: los llamados a presentar ofertas, la recepción de las ofertas, aclaraciones, inconformidades, respuestas, modificaciones, ofertas, adjudicaciones, contratos y sus modificaciones, variaciones o ampliaciones, seguros de caución y todo aquel documento que respalde el expediente de la adquisición hasta la finalización del proceso de adquisición. Ningún funcionario público limitará, alterará o restringirá la información pública que debe contener el sistema GUATECOMPRAS.

Los sujetos obligados de conformidad con la presente Ley publicarán en el sistema GUATECOMPRAS la información que la normativa vigente establezca como requisitos obligatorios, en los plazos establecidos en las normas, disposiciones reglamentarias y las resoluciones respectivas.

Es obligatorio el uso de formularios electrónicos en todos los procesos de adquisición pública.

Las programaciones de las adquisiciones públicas y sus modificaciones deberán publicarse en GUATECOMPRAS, pudiendo ser ajustados cuando sea necesario por la autoridad superior, mediante resolución debidamente justificada.

El sistema GUATECOMPRAS permitirá acceder a otros registros y sistemas relacionados con las adquisiciones públicas.

El incumplimiento por parte de los usuarios de GUATECOMPRAS de lo establecido en este artículo se sancionará según lo previsto en el artículo 83 de la presente Ley.

ARTÍCULO 15. * Dirección General de Adquisiciones del Estado.

La Dirección General de Adquisiciones del Estado es el ente rector de las adquisiciones públicas, responsable de facilitar procesos, proponer o aprobar la normativa en el ámbito de su competencia. El objeto de la Dirección General de Adquisiciones del Estado es procurar que las adquisiciones públicas se desarrollen en un marco general de transparencia, certeza, eficiencia y competencia en las adquisiciones públicas. Entre sus funciones se encuentra:

a) Ser el órgano rector de las adquisiciones públicas y del Sistema de Información de Contrataciones y Adquisiciones del Estado GUATECOMPRAS;

b) Diseñar, administrar, normar e implementar políticas destinadas para el desarrollo de GUATECOMPRAS;

c) Establecer procedimientos para la adecuada aplicación de la legislación en materia de adquisiciones públicas;

d) Coordinar la modalidad de compra por contrato abierto;

e) Decidir el destino de los fondos privativos de la dirección, para el fortalecimiento, desarrollo y modernización de los sistemas, procesos y procedimientos de adquisiciones públicas;

f) Capacitar periódicamente a las entidades del sector público en materia de procedimientos para las adquisiciones públicas;

g) Certificar a los funcionarios o empleados, públicos responsables de las adquisiciones, en las entidades sujetas a la presente Ley;

h) Requerir a todas las entidades del sector público, por medio del sistema GUATECOMPRAS, su programación anual de compras, para su optimización y elaboración de estadísticas y sus modificaciones;

i) Estandarizar los procesos de contrataciones de las entidades públicas;

j) Generar y mantener actualizadas estadísticas, las cuales serán de acceso público; y,

k) Otras que establezca el reglamento, la ley y el despacho ministerial, en el ámbito de su competencia.

ARTÍCULO 22. *

Entrega de bases. La entidad requirente debe publicar las bases de los eventos en GUATECOMPRAS, de donde las personas interesadas las podrán obtener de forma gratuita. En el caso que las obras, bienes o servicios requieran documentos que no puedan ser incluidos en GUATECOMPRAS, tales como planos no elaborados por medios electrónicos o cualquier otro que por su naturaleza no lo permita, se deberá indicar en el portal de GUATECOMPRAS el lugar donde se pondrán a disposición los documentos.

El pago correspondiente por los documentos anexos que no puedan ser elaborados por medios electrónicos, podrán cobrarse al costo de su reproducción, fondos que serán considerados privativos, utilizados exclusivamente para la modernización institucional de la entidad.

ARTÍCULO 23. Publicaciones. *

Las convocatorias a licitar se deben publicar en el Sistema de Información de Contrataciones y Adquisiciones del Estado, denominado GUATECOMPRAS, y una vez en el diario oficial. Entre ambas publicaciones debe mediar un plazo no mayor de cinco (5) días calendario. Entre la publicación en GUATECOMPRAS y al día fijado para la presentación y recepción de ofertas deben transcurrir por lo menos cuarenta (40) días calendario.

En los procesos de cotización y de licitación, la entidad contratante debe publicar en GUATECOMPRAS, como mínimo, la siguiente información: bases de cotización o licitación, especificaciones técnicas, criterios de evaluación, preguntas, respuestas, listado de oferentes, actas de adjudicación y los contratos de las contrataciones y adquisiciones.

En lo relativo a lo dispuesto en convenios y tratados internacionales de los cuales la República de Guatemala, sea parte, las disposiciones contenidas en los mismos se aplicarán en forma complementaria, siempre y cuando no contradigan el contenido del presente artículo.

ARTÍCULO 24 Bis. * Presentación de ofertas electrónicas.

Para cualquier modalidad de compra regulada en esta Ley, en la que se soliciten ofertas de forma electrónica, deberán acatarse las disposiciones establecidas en el reglamento y las normas de uso del sistema GUATECOMPRAS.

ARTÍCULO 35. * Notificación electrónica e inconformidades.

Las notificaciones que provengan de actos en los que se aplique la presente Ley, serán efectuadas por vía electrónica a través de GUATECOMPRAS, y surtirán sus efectos al día siguiente de su publicación en dicho sistema.

Las personas inconformes por cualquier acto que contravenga los procedimientos regulados por la presente Ley, su reglamento o los reglamentos de los registros, pueden presentar a través de GUATECOMPRAS sus inconformidades.

Las inconformidades relacionadas con la adjudicación de la Junta sólo pueden presentarse dentro del plazo de cinco (5) días calendario, posteriores a la publicación de la adjudicación en GUATECOMPRAS.

Tanto la Junta como la entidad contratante que reciba una inconformidad, debe responderla a través de GUATECOMPRAS, en un plazo no mayor de cinco (5) días calendario a partir de su presentación.

A consecuencia de una inconformidad, la Junta podrá modificar su decisión, únicamente dentro del plazo señalado. Contra esta decisión por no ser un acto definitivo, no cabrá recurso alguno.

Contra la resolución definitiva emitida por la entidad contratante podrá interponerse, en la fase respectiva, una inconformidad. El reglamento regulará lo respectivo a esta materia.

2.12.4 Ley de Acceso a la Información Pública

ARTÍCULO 7. Actualización de información.

Los sujetos obligados deberán actualizar su información en un plazo no mayor de treinta días, después de producirse un cambio.

ARTÍCULO 10. Información pública de oficio.

Los Sujetos Obligados deberán mantener, actualizada y disponible, en todo momento, de acuerdo con sus funciones y a disposición de cualquier interesado, como mínimo, la siguiente información, que podrá ser consultada de manera directa o a través de los portales electrónicos de cada sujeto obligado:

11. La información sobre contrataciones de todos los bienes y servicios que son utilizados por los sujetos obligados, identificando los montos, precios unitarios, costos, los renglones presupuestarios correspondientes, las características de los proveedores, los detalles de los procesos de adjudicación y el contenido de los contratos;

14. información sobre los contratos de mantenimiento de equipo, vehículos, inmuebles, plantas e instalaciones de todos los sujetos obligados, incluyendo monto y plazo del contrato e información del proveedor;

16. La información relacionada a los contratos, licencias o concesiones para el usufructo o explotación de bienes del Estado;

17. Los listados de las empresas precalificadas para la ejecución de obras públicas, de venta de bienes y de prestación de servicios de cualquier naturaleza, incluyendo la información relacionada a la razón social, capital autorizado y la información que corresponda al renglón para el que fueron precalificadas;

19. Los contratos de arrendamiento de inmuebles, equipo, maquinaria o cualquier otro bien o servicio, especificando las características de los mismos, motivos del arrendamiento, datos generales del arrendatario, monto y plazo de los contratos;

20. Información sobre todas las contrataciones que se realicen a través de los procesos de cotización y licitación y sus contratos respectivos, identificando el número de operación correspondiente a los sistemas electrónicos de registro de contrataciones de bienes o servicios,

fecha de adjudicación, nombre del proveedor, monto adjudicado, plazo del contrato y fecha de aprobación del contrato respectivo;

21. Destino total del ejercicio de los recursos de los fideicomisos constituidos con fondos públicos, incluyendo la información relacionada a las cotizaciones o licitaciones realizadas para la ejecución de dichos recursos y gastos administrativos y operativos del fideicomiso;

22. El listado de las compras directas realizadas por las dependencias de los sujetos obligados;

ARTÍCULO 38. Procedimiento de acceso a la información pública.

El procedimiento para el acceso a la información pública se inicia mediante solicitud verbal, escrita o vía electrónica que deberá formular el interesado al sujeto obligado, a través de la Unidad de Información. El modelo de solicitud de información tendrá el propósito de facilitar el acceso a la información pública, pero no constituirá un requisito de procedencia para ejercer el derecho de acceso a la información pública.

La persona de la Unidad de Información que reciba la solicitud no podrá alegar incompetencia o falta de autorización para recibirla, debiendo obligadamente, bajo su responsabilidad, remitirla inmediatamente a quien corresponda.

El procedimiento de acceso a la información no perjudicará, limitará o sustituirá el derecho a presenciar u observar los actos de los sujetos obligados, ni limitará el derecho a solicitar información a los sujetos obligados en la forma contemplada en otras leyes, ni la realización de solicitudes de información que pudieran hacerse ante entes cuya naturaleza es de publicidad frente a terceros en donde por principio de especialidad se deberá acudir a través de los trámites correspondientes.

ARTÍCULO 39. Sistemas de información electrónicos.

Los sujetos obligados establecerán como vía de acceso a la información pública, entre otros, sistemas de información electrónicos.

Bajo responsabilidad de la autoridad máxima garantizará que la información publicada sea fidedigna y legitima.

La información publicada en los sistemas de información electrónicos, entre otros, deberá coincidir exactamente con los sistemas de administración financiera, contable y de auditoria y esta deberá ser actualizada en los plazos establecidos en esta ley.

ARTÍCULO 40. Respuesta en sistemas de información electrónicos.

Los sujetos obligados adoptarán las medidas de seguridad que permitan dotar de certeza a los informes enviados por mensajes de datos. En cualquier casó conservarán constancia de las resoluciones originales.

2.13 Blockchain generador de valor

2.13.1 Generación de valor agregado para el sector público

En los pasados apartados de este documento se dictaron las iniciativas que están siendo exploradas en el sector público en la región latinoamericana y en función de los atributos de las tecnologías de estas naciones. Se identifican cuatro grandes categorías en donde la tecnología Blockchain embonaría y daría un valor agregado. Estas cuatro grandes categorías son: desintermediación de la información, tokenización de activos, automatización de procesos e interoperabilidad.

2.13.2 Desintermediación de la información

En muchas instancias la generación de información en el sector público se basa en una cadena de procesos compuesta por distintas personas o entidades. A través de la tecnología, la información puede registrarse de manera segura y confiable, convirtiendo a la red en una especie de notariado digital de datos y transacciones. Potencialmente, el incluir estos procesos en una cadena de Blockchain permitirá prescindir de algunos de estos intermediarios, aumentar la trazabilidad de cada etapa del proceso de manera confiable y reducir costos tanto en tiempo como en recursos.

2.13.3 Tokenización de activos

El uso de la tecnología puede permitir expresar distintos activos como fichas (tokens), de manera que se los pueda representar de manera digital y así contar con un registro confiable

de los cambios de propiedad (o de localización, en el caso de cadenas de producción o de distribución). Esta característica también permite la posibilidad de atomizar la propiedad de un solo activo entre muchos propietarios.

2.13.4 Automatización de procesos

Una ventaja de la inscripción de contratos inteligentes en un registro distribuido es la posibilidad de automatizar procesos a través del establecimiento de reglas que deberán cumplirse para que se realice cierta acción (ejecución del contrato) de manera automática sin intermediarios de confianza. El pago automático de transferencias condicionadas cuando se cumplen condicionalidades predefinidas, el cobro de bienes y servicios después de haber sido entregados o el hacer cumplir diversas regulaciones pueden traducirse en reglas incluidas en contratos inteligentes.

2.13.5 Interoperabilidad

Uno de los principales retos para la prestación integrada de servicios de Gobierno es la necesidad de conectar los distintos sistemas de las entidades públicas y privadas de forma segura y confiable. El uso de Blockchain para la certificación de información ciudadana puede permitir que sean los mismos ciudadanos los que ayuden a que los distintos sistemas operen entre sí sin la necesidad de que estén integrados, otorgando en tiempo real los permisos necesarios para que su información personal pueda ser accedida por distintas entidades. Este enfoque tiene además la ventaja de permitir una mayor trazabilidad en el acceso de información personal del ciudadano.

2.14 Incremento de la transparencia de los procesos de compras del estado

Blockchain tiene el potencial de facilitar el registro y la publicación de datos y procesos públicos, prescindiendo de intermediarios que puedan manipular o retrasar el procedimiento y fomentando su monitoreo por parte de la ciudadanía. Los elementos intrínsecos de la tecnología que facilitan

este objetivo son la distribución de la información, la disponibilidad de los datos en múltiples nodos que pueden estar fuera de la administración pública y la posibilidad de verificación de la integridad de la información por parte de cada uno de ellos.

Por ejemplo, a través de la implementación de contratos inteligentes pueden concretar la licitación de una compra del estado de maneta transparente y eficiente. En el momento en que alguien comienza a realizar transacciones en el sistema se origina un historial de todas las interacciones y transacciones que está disponible para todos los participantes, lo cual genera un alto nivel de transparencia, trazabilidad y confianza en la integridad de la red. Adicionalmente, la tecnología habilita la notarización de la información, es decir, puede certificar que determinada información no ha sido alterada. Si bien una red privada distribuida puede agregar restricciones sobre quién puede escribir o leer transacciones, conserva la característica de acceso común a su conjunto de transacciones. Por otro lado, cuanto más distribuidos se encuentren los nodos, no solo dentro de las organizaciones de la administración pública con competencia en el proceso o con roles de auditoría sino en organizaciones fuera de la administración pública, la solución tendrá mayor probabilidad de incrementar la transparencia e integridad de la información.

2.15 Facilitación de la auditoría de la información

La tecnología Blockchain (principalmente las Blockchain públicas no permisionadas) facilita la auditoría de la información al asegurar el registro de todas las transacciones, las cuales generan una cadena de bloques que no se puede borrar o modificar sin dejar una huella. Esta característica además permite auditar procesos confiando en la información de la cadena y sin la necesidad de que terceros brinden la información, lo que quita los incentivos a manipularla con fines particulares.

2.15.1 Licitaciones públicas inteligentes: Caso de estudio México

Un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre México identificó que para 2015 aproximadamente un 21% del presupuesto asignado a

la Administración Pública Federal se destinaba a contrataciones públicas (OCDE, 2018), las cuales se realizan de manera electrónica a través del sistema CompraNet. Un sistema de contratación electrónica puede ayudar a incrementar la transparencia y la eficiencia en la asignación de recursos al reducir las interacciones entre funcionarios encargados de las contrataciones y los oferentes.

En este contexto, la OCDE realizó un diagnóstico y una serie de recomendaciones a CompraNet para mejorar la publicación de la información relativa a todo el ciclo de contratación, el funcionamiento del sistema, el procesamiento de denuncias y su integridad. Actualmente, los ciudadanos no pueden participar en la auditoría de los procesos de contratación pública, sino que existe la figura de testigo social, que es un representante de la sociedad civil que participa en el proceso y revisa su legalidad y transparencia.

En este marco la solución de contratos inteligentes basada en la tecnología Blockchain tiene como objetivo incrementar la confianza ciudadana en los procesos de contratación pública, permitiendo que aquellos que se hayan registrado puedan participar del monitoreo social de las adquisiciones. También permite a los evaluadores certificados votar y calificar las propuestas de manera anónima, otorgando más transparencia al proceso y eliminando intermediarios para proveer la información sujeta a auditoría.

El piloto de contrataciones inteligentes fue lanzado en 2018 y tuvo como objetivo diseñar un sistema de contrataciones basado en Blockchain y un estándar de contrataciones abiertas que fomente la transparencia de los procesos y su auditoría social. Dentro de las innovaciones previstas para esta solución, se plantea la introducción de la figura de los evaluadores independientes, lo que otorga voz y voto a los ciudadanos para evaluar propuestas, a diferencia de la figura del testigo social. Por otra parte, el estándar de contrataciones abiertas le brinda una mayor integridad a la información del proceso de contratación. La solución plantea una infraestructura híbrida montada sobre la Red Federal mencionada en la primera parte, la cual utiliza una instancia de Ethereum.

Este caso es particularmente valioso por dos razones. En primer lugar, intenta resolver el problema de falta de transparencia e integridad de la información en los procesos de licitación pública, dado que automatiza aquellos pasos que están expuestos a mayor corrupción el más relevante de ellos es la evaluación técnica y económica de pro puestas y busca maneras de fomentar la participación ciudadana a través de la evaluación de propuestas y el monitoreo de las contrataciones.

Si bien el piloto ha probado que puede generarse una infraestructura para estandarizar y mejorar el proceso de contratación pública, a fin de democratizar el uso de la solución se requiere conocer a los potenciales usuarios de la plataforma y analizar si tienen las capacidades técnicas para poder hacerlo.

En segundo lugar, este piloto sirve como caso de uso para la generación del ecosistema en el marco de la Red Federal impulsada desde la Coordinación de Estrategia Digital Nacional (CEDN). Se espera que la evaluación de este aplicativo genere incentivos para el desarrollo de esta red, el diseño de nuevos casos de uso por parte de los actores de este incipiente ecosistema y el fortalecimiento de su gobernanza.

2.16 Aseguramiento de la integridad de los datos

Blockchain permite mejorar y proteger la integridad de los datos al hacer muy difícil la posibilidad de manipularlos sin dejar una huella. Por su diseño intrínseco la tecnología impide la posterior manipulación de datos almacenados en los bloques de la cadena sin que lo perciba el resto de los participantes. La consistencia en los datos entre todos los nodos genera seguridad sobre su integridad, lo cual incentiva la eliminación de intermediarios.

Una función importante del Gobierno es mantener información confiable sobre individuos, organizaciones, activos y actividades. La gestión de estos registros suele ser complicada principalmente porque la mayoría de esta información se encuentra en papel. Las agencias de

Gobierno tienden a construir sus propios silos de datos y protocolos de gestión de la información, lo que impide que otras partes del Gobierno los utilicen.

Pisa y Juden (2017) definen

> Almacenar un registro de la propiedad en una red distribuida mejora en gran medida su seguridad al eliminar el riesgo de un punto único de falla y hacer más difícil su manipulación. Con esto también se puede aumentar la transparencia y mantener la integridad de los registros permitiendo a los agentes certificados (incluidos, potencialmente, auditores u organizaciones sin fines de lucro) monitorear los cambios realizados en el registro casi en tiempo real y mejorar la eficiencia al reducir el tiempo y dinero asociados con el registro de la propiedad. (p.36)

2.17 Ethereum

Como se ha hecho mención durante todo este documenta académico, la tecnología de Blockchain ha tenido en los últimos años un gran crecimiento y popularidad en el mundo. Ethereum no es la excepción a la regla, Ethereum es la segunda plataforma de Blockchain más usada y conocida del mundo, posterior a la de Bitcoin.

Ethereum fue creada por el afamado progamador y escritor ruso Vitalik Buterin, conocido también por ser el CO-CEO de la revista Bitcoin. La tecnología fue lanzada públicamente a finales de 2014. El objetivo de la red de Blockchain es integrar una plataforma que permite y facilita a programadores la creación de aplicaciones descentralizadas por medio de “Smart contracts”.

2.17.1 Definición y funcionamiento de Ethereum

Jaime Raúl (2018) define

> Ethereum es una Blockchain o Tecnología de Contabilidad Distribuida (DTL) con un lenguaje de programación Turing completo integrado, una computadora Blockchain, que permite que cualquiera pueda escribir contratos inteligentes y aplicaciones descentralizadas simplemente escribiendo la lógica en unas pocas líneas de código. El protocolo Ethereum fue concebido originalmente como una versión mejorada de la criptomoneda Bitcoin, para superar las limitaciones de su lenguaje de programación, proporcionando características avanzadas tales como custodia sobre la Blockchain, límites de retiro, contratos financieros, mercado de juegos de azar, entre otros. (p. 5)

Ethereum presta las características y la tecnología de Blockchain para basar su infraestructura y evolución de las aplicaciones y servicios centralizados a un concepto descentralizado. Ethereum al igual que la Blockchain de Bitcoin utiliza el protocolo de consenso de Proof-of-Work para la elaboración de nuevos bloques para su cadena.

2.17.2 Ethereum Virtual Machine (EVM)

Se debe tener claro que Ethereum nace con el objetivo principal de facilitar la creación de aplicaciones que usen la tecnología de Blockchain de manera “open source”, al mismo tiempo que sirve como plataforma mundial segura, de donde se alimentan dichas aplicaciones. Por lo anterior la comunidad de Blockchain de Ethereum “la gran computadora mundial” y todo debido al uso de la Ethereum Virtual Machine (EVM), la máquina virtual de Ethereum.

La máquina virtual de Ethereum (EVM) es un interpretador virtual potente, en espacio aislado, incrustado dentro de cada nodo completo de Ethereum. Este es responsable de ejecutar o interpretar tanto los entornos de desarrollo de los Smart contract como el lenguaje en que se

escriben (Solidity) a códigos de bytes del contrato. Los contratos generalmente se escriben en lenguajes de alto nivel, y luego se compilan en el código de bytes EVM.

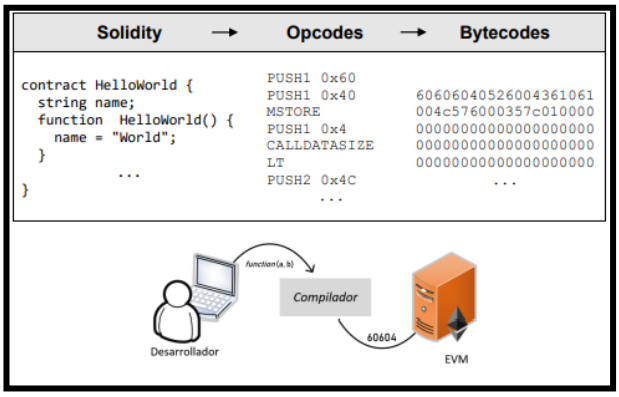
Lo anterior significa que el código de la máquina virtual está completamente aislado de la red de Ethereum, el sistema de archivos o cualquier proceso de la computadora host, o servidor de aplicación Ethereum. Cada nodo de la red Ethereum ejecuta una instancia de EVM que les permite acordar la ejecución de las mismas instrucciones. La EVM es una máquina de Turing por completo, que se hace referencia a que esta puede llevar a cabo cualquier tipo de proceso lógico funcional computacional.

El EVM es esencial para el Protocolo Ethereum y es fundamental para el motor de consenso del sistema Ethereum. Permite a cualquier persona ejecutar código en un ecosistema sin confianza en el que se puede garantizar el resultado de una ejecución y es totalmente determinista (es decir, ejecutar Smart contracts).

La forma en que la EVM trabaja cuando un contrato está diseñado con Solidity y es compilado, esta lo convierte en una secuencia de código de operaciones (operation codes) también conocidas como opcodes, que están referenciados por nombres mnemotécnicos como lo pueden ser ADD (para sumas) o MUL (para multiplicaciones). Los bytecodes son similares a los opcodes, pero representan números hexadecimales que la EVM es capaz de procesar.

Figura No. 3

Diagrama de funcionamiento EVM



Fuente: Ethereum (2019).

2.17.3 El Gas de Ethereum

El término “Gas” en Ethereum hace referencia a la energía necesaria para llevar a cabo la ejecución de transacciones en Ethereum. Este término engloba tanto transacciones de ether, criptomoneda nativa de Ethereum, de una cuenta a otra, como la ejecución de un Smart contract.

Cada operación u opcode que se haga en el código tiene una cantidad de gas asignada. Por ejemplo, un “ADD” cuesta 3 gas, calcular un Hash “SHA 30” gas y enviar una transacción de ether 21,000 gas. Operaciones con más dificultad computacional requerirán más gas. El parámetro que la EVM necesita para ejecutar las transacciones es el STARTGAS, también conocido como transaction gaslimit (límite de gas). La transaction gaslimit es la cantidad de gas que se decide enviar en una transacción (parámetro modificable por el usuario). En el caso de querer transferir a otro usuario ether si se indica cómo transaction gaslimit un total de 30000 gas, sabiendo que la transacción de ether cuesta 21000, se devolverá al usuario el gas no gastado, 9000 gas (30.000 - 21.0000).

El gas también sirve como mecanismo para pagar a los mineros. En cada transacción se debe de especificar una cantidad de transaction gaslimit que está dispuesto a pagar, en el caso de una transacción de ether, se conoce que son 21,000 gas, pero normalmente el usuario no puede conocer cuánto gas le va a costar, por ello especifica una cantidad límite. A parte se ha de indicar cuánto se
está dispuesto a pagar por cada gas. El gas solo existe dentro de la máquina virtual Ethereum. Cuando se trata de pagar por el gas consumido, la tarifa se cobra con la equivalencia en ether. A este otro término se le conoce como gasprice (precio del gas) definido como Gwei/gas (1 Gwei es 10^9 ether).

Al inicio de una ejecución de una transacción, el transaction gaslimit * gasprice se restará de la cuenta de usuario. Si la transacción se completa y se ha consumido menos gas del que se ha especificado como límite, el gas restante (gasrem) multiplicado por el gasprice será devuelto al

que envió la transacción. En Ethereum el gas usado realmente (transaction gaslimit - gasrem) * gasprice, se le dará como premio al minero del bloque.

En el caso de que la transacción supere el transaction gaslimit, conocido como “Runs out of gas”, la transacción se revertirá, y el minero recibirá por su esfuerzo todo el gas (transaction gaslimit*gasprice). El bloque se incluye en la Blockchain, pero como fallido. Adicionalmente, se debe conocer que los propios bloques tienen un campo también de límite de gas llamado block gaslimit (en Ethereum hablar de gas limit, se sobre entiende que se habla del límite de gas de un bloque).

2.17.4 Desarrollo de Smart Contract

Dictado los apartados anteriores de este documento académico se procede a plantear los siguientes cuestionamientos, donde y como se desarrollan los Smart contract de Ethereum. Para ello cabe recordar, que los Smart contracts son pequeños programas informáticos que se ejecutan en un entorno Blockchain y como programa, necesitan para su construcción un lenguaje de programación de alto nivel.

Existen unas cuantas opciones diferentes de lenguajes de programación para la creación de Smart contract, entre ellos se puede encontrar el lenguaje Serpent (basado en Python), LLL, Bamboo y Solidity (estos últimos tres basados en Java Script). Mayoritariamente, el lenguaje más utilizado y conocido es el de Solidity, un lenguaje de programación de alto nivel creado específicamente por y para Ethereum. Es por este motivo que es el escogido para el desarrollo de los contratos inteligentes en este trabajo académico, que posteriormente se dictará todo un subcapítulo de este y se expondrá en el desarrollo del aplicativo a realizar.

Sin embargo, antes de entrar en materia sobre el desarrollo de Smart contract, es imperativo dictar sobre el entorno de trabajo para poder programar y testear los contratos programados. Para ello en esta tesis de grado se utilizó de primera instancia el entorno de trabajo de Remix.

2.17.5 Entorno de trabajo Remix

Remix, antes conocido como Browser Solidity, es un entorno de desarrollo online basado en navegador con entorno de pruebas y de depuración integrado. Se instala en un ordenador de forma nativa, pero de igual forma se puede utilizar en su versión online para su comodidad.

Remix es una potente herramienta de desarrollo de código abierto, cuyo objetivo es facilitar la escritura de contratos inteligentes en Solidity. Esta herramienta está escrita en JavaScript y hace uso de las librerías de Node JS para la ejecución de comandos. Remix también admite pruebas, depuración e implantación de contratos inteligentes de manera nativa.

Para la ejecución de los contratos en esta plataforma se debe tomar en cuenta que existen varias variables a considerar como es el entorno de desarrollo, las listas asociadas, el gas limit y el valor de la transacción, todas ellas configurables desde Remix de una forma rápida y sencilla.

A lo que se refiere en entorno de desarrollo se debe decidir en qué entorno se ejecutaran los conectarnos. Se tiene las opciones del entorno de JavaScript VM, donde en local ejecuta y crea una Blockchain de test. Injected Web3 entorno de ejecución que conecta con algún proveedor que proporciona conectividad con la Blockchain de Ethereum como pueden ser Metamask o Mist (sismos que se dictaran en apartados más adelante del documento). Por última opción Web3 Provider que permite conectar a un nodo remoto.

Esta herramienta de igual forma proporciona un compilador integrado que proporciona datos muy importantes del Smart contract como son algunos metadatos. Los metadatos del contrato incluyen la versión de compilación que se estará usando. El bytecode ejecutado durante le creación del contrato, estimaciones de gas y el ABI o ABI array (Aplication Binary Interface), el cual describe completamente las interfaces del contrato.

2.17.6 Entorno de trabajo Ganache y Truffle

Otro entorno utilizado durante el desarrollo del aplicativo de este trabajo académico es Ganache desarrollado por la compañía Truffle suite. Ganache es una cadena de bloques personal para el desarrollo rápido de aplicaciones distribuidas de Ethereum y Corda. Se puede implementar Ganache durante todo el ciclo de desarrollo; lo que le permite desarrollar, implementar y probar las dApps en un entorno seguro y determinista.

Se puede utilizar Ganache como Testnet para desplegar, y probar Smart Contracts, ejecutar test, ejecutar comandos, e inspeccionar el estado de la cadena de bloques mientras se controla como la cadena opera. Se conecta con Remix a través del entorno Web3 Provider indicando la ruta del Web3 Provider Endpoint (servidor nativo) que indica Ganache como “RPC Server”.

2.18 Lenguaje de programación Solidity

Solidity es un lenguaje de alto nivel orientado a contratos. Su sintaxis es similar a la de JavaScript y está enfocado específicamente a la Máquina Virtual de Ethereum (EVM). Solidity está tipado de manera estática y acepta, entre otras cosas, herencias, librerías y tipos complejos definidos por el usuario.

La extensión para los ficheros es “.sol”. Un contrato de Solidity no es más que una colección de código (funciones y variables) que residen en una dirección especifica de la Blockchain de Ethereum. Cada contrato incluirá variables de estado, funciones, modificadores, eventos, estructuras y herencias de otros contratos.

2.18.1 Diseño de ficheros

2.18.1.1 Versionamiento

Todos los contratos y sin excepción inicializarán con la instrucción reservada “pragma solidity” acompañado de la versión del leguaje. Lo anterior para especificar la versión del compilador va a ser usada. Como ejemplo, se podría utilizar la versión 0.4.0 o mayor “^” (indicado con el acento circunflejo).

2.18.1.2 Importación de ficheros

La sintaxis que se utilizara a nivel global para poder realizar una importación de ficheros es: “import filename.sol”, siempre colocando la extensión del fichero de tipo solidity. Esta instrucción importa todas las características definidas en "filename.sol" (variables y funciones) al ámbito global actual del contrato.

En lo apartado de sintaxis, el nombre de archivo, si se trata de una ruta, se accede con (/), como separador de directorios, (.) para el directorio actual y (..) para subir un directorio. Todos los nombres de rutas se tratan como rutas absolutas a menos que comiencen por (.) o (..).

2.18.2 Tipos de datos

Solidity es un lenguaje de tipo estático, lo que quiere decir, que el tipo de variable tendrá que estar definido antes de la compilación. Para este lenguaje de alto novel se encuentran los siguientes tipos de datos:

- Address: Una “Address” ocupa un valor de 20 bytes. Es una variable específica para guardar las direcciones de contratos o de usuarios de Ethereum.
- Integer: Un “int / uint”, guardan valores numéricos con signo y sin signo respectivamente.
- String: El “string” contiene una cadena de caracteres.
- Booleano: Un “bool”, puede tener dos posibles valores (true o false).
- Bytes: Los Bytes1 hasta bytes32, que son arrays de bytes fijos o bytes con tamaño

variable.

- Enumeración: Los “enum” se pueden usar para crear tipos de datos personalizados con un finito conjunto de valores.
- Estructura: “Struct” permite construir objetos con múltiples tipos de atributos.
- Array de datos: Los arrays pueden tener un tamaño fijo o pueden ser dinámicos. Una array de tamaño fijo y elemento tipo T se escribe como T[k], una matriz de tamaño dinámico como T[].
- Mapeador: El “mapping” básicamente permite usar un tipo de variable como índice de un array. Son declarados como mapping (“KeyType => ValueType”). Donde “KeyType” es el tipo de dato excepto mapping y el “ValueType” puede ser cualquier tipo.

2.18.2.1 Visibilidad de datos

Todos los datos pueden tener diferentes tipos de visibilidad para acceder a las variables. El tipo “public” accesible, se puede obtener el dato guardado en la variable en cualquier momento. El dato “constant” variable que no se podrá modificar una vez inicializada. Y la última configuración es la variable tipo “prívate” la cual no es accesible en ningún momento fuera de su estructura.

2.18.3 Unidades y variables especiales disponibles

2.18.3.1 Unidades de Ether

Un número literal puede tomar un sufijo de “wei”, “szabo”, “finney” o “ether” para convertir el número en una su denominación de ether. Sí el número va sin prefijo se asumen wei, la unidad más pequeña. Algunas conversiones más usadas:

También se pueden hacer comparaciones entre diferentes unidades, como 2 ether == 2000 finney y se evalúa como true.

2.18.3.2 Unidades de Temporales

Los sufijos como “seconds”, “minutes”, “hours”, “days”, “weeks” and “years” se pueden usar para convertir numerales en unidades de tiempo, donde los segundos son la unidad base.

2.18.4 Estructura interna de Smart Contract

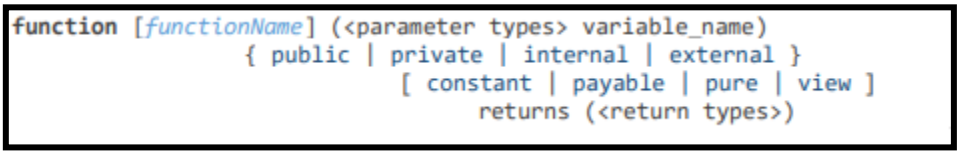
El contrato es el objeto más grande que existe en el Blockchain de Ethereum. Todas las acciones que se peritan hacer con un Smart contract estarán predefinidas en el “contract”. Los contratos en Solidity son similares a las clases en lenguajes orientados a objetos. Contienen datos persistentes en variables de estado y funciones que pueden modificar estas variables. Algunas de las opciones y funciones más significativas que se diseñan en los contratos son las siguientes:

2.18.4.1 Funciones

Las funciones son las unidades básicas que ejecutarán la parte lógica del código dentro de un contrato. Las funciones que se pueden representar vienen creadas siguiendo la regla siguiente:

Figura No. 4

Estructura de función en Ethereum



Fuente: Ethereum (2019).

Donde parameter types, son los parámetros de entrada que acepta y los return types, son los parámetros que devolverá. En ambos casos hay indicar el tipo de variable. Las funciones pueden ser de diferentes tipos y se especifican como external, public, internal o private.

Las dos funciones principales son las “get” y “set”, mismas para obtener el valor de una variable o modificar el valor en las mismas.

2.18.4.2 Métodos de variables y funciones especiales

Existen variables y funciones especiales que siempre existen en el espacio de nombres global y se utilizan principalmente para proporcionar información sobre la Blockchain. Estas son las siguientes:

A. Propiedades de bloques y transacciones

a. block.blockHash (uint block number) returns (bytes32): Hash del bloque dado. Sólo funciona para los 256 bloques más recientes, excluyendo el bloque actual.
b. block.coinbase (address): La dirección del actual del minero del bloque.
c. block.difficulty (uint): Dificultad del bloque.
d. block.gaslimit (uint): Límite de gas actual.
e. block.number (uint): Número del bloque actual.
f. block.timestamp (uint): Marca de tiempo del bloque actual.
g. msg.gas (uint): Gas restante.
h. msg.sender (address): Remitente del mensaje actual.
i. msg.value (uint): Cantidad de Ether (en wei) enviado.
j. now (uint): Alias block.timestamp (uint)
k. tx.gasprice (uint): Precio del gas de la transacción.

B. Relacionado con las direcciones

a. Balance y transfer: Es posible consultar el saldo de una dirección usando la propiedad de balance y enviar ether (en unidades de wei) a una dirección usando transfer.
b. Send: El valor send indicará si se ha ejecutado o no la transacción. Si la ejecución falla, send devolverá false.

C. Relacionado al contrato:

a. This: El contrato actual.
b. Selfdestruct (address) o suicide (address): Destruye el contrato actual enviando los fondos a la dirección dada como parámetro de Desarrollando Smart contract

entrada. Esto es útil cuando se ha terminado con un contrato, ya que el uso de gas es menor que usando <address>.send(this.balance).

2.18.4.3 Constructor

Se asimila a un constructor en programación orientada a objetos. Es una subrutina cuya misión será inicializar un objeto. El constructor ha de tener el mismo nombre que el contrato y será la primera en ser ejecutada. El constructor es opcional y acepta parámetros de entrada. Muy útil para inicializar variables.

2.18.4.4 Modificadores

Los modificadores se pueden utilizar para cambiar fácilmente el comportamiento de las funciones. Por ejemplo, pueden comprobar automáticamente una condición antes de ejecutar la función.

2.18.4.5 Herencia

El concepto de herencia en Solidity, significa básicamente que se pueden crear diferentes contratos donde un contrato tiene como herencia las funcionalidades del anterior. Cuando un contrato hereda de contratos múltiples, sólo se crea un contrato único en la cadena de bloque, y el código de todos los contratos base se copia en el contrato creado. Se usa el “is” para derivar de otro contrato.

2.18.4.6 Eventos Ethereum

Desde la interfaz de usuario de la Dapp, se puede registrar a un evento que sucede en la Blockchain. Dentro de los contratos existe sintaxis como lo es “evento”, para declarar registros dentro de funciones. Estos registros pueden aceptar parámetros.

2.18.4.7 Funciones abstractas

La función abstracta es una función que no tiene implementación real y para heredarla a un contrato es necesario implementarla completamente en el subcontrato o contracto hijo.

2.19 Guatecompras

2.19.1 Definición de Guatecompras

Guatecompras es el nombre designado al Sistema Informático de Contrataciones y Adquisiciones del Estado de la República de Guatemala y en un mercado electrónico, operado a través de la red de la Internet. Este sistema está a cargo del departamento de informática del Ministerio de Finanzas.

2.19.2 Función de Guatecompras

El Estado de la República de Guatemala utiliza el sistema informático de Guatecompras para comprar y contratar bienes y servicios y dar cumplimiento a las disposiciones del Decreto 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado y su Reglamento.

2.19.3 Objetivos de Guatecompras

Los principales objetivos base que se logran con una buena gestión de forma transparente e integra del sistema informático de Guatecompras son:

2.19.3.1 Transparencia

Permite que las etapas del proceso de adquisiciones estén a la vista de todos. De esta manera los empresarios conocen las oportunidades de negocios, los organismos públicos compradores conocen tempranamente todas las ofertas disponibles, la ciudadanía vigila los procesos y conoce los precios pagados para cada adquisición. Esto aumenta la competencia y reduce la corrupción.

2.19.3.2 Eficiencia

Estimula la competencia, por lo tanto, pretende lograr importantes reducciones en los costos, en los plazos de los procesos de adquisición, en los precios de los bienes y servicios adquiridos y en el número de las impugnaciones. De este modo, el gasto público es más eficiente.

2.19.4 Promoción del Desarrollo

Es un instrumento esencial para la modernización del Estado, la buena gestión política, el fortalecimiento de las instituciones y la construcción de la democracia. Con frecuencia las adquisiciones gubernamentales son vistas simplemente como un problema de logística y provisión de suministros. En realidad, constituyen un aspecto esencial de la gestión del desarrollo.

Los avances electrónicos, permiten aumentar sustancialmente el impacto de las adquisiciones del sector público para convertirlas en un soporte decisivo de la transformación de las instituciones, el mejoramiento del bienestar colectivo, la promoción del crecimiento económico y la construcción de la democracia. Guatecompras permite que las adquisiciones del Gobierno sean utilizadas como un instrumento para promover el sector privado y el desarrollo equilibrado, porque facilita la protección contra el monopolio, fomenta el crecimiento gradual de la productividad y posibilita la expansión de las economías locales y de las pequeñas y medianas empresas.

2.19.5 Integración regional

Se vislumbra que los procedimientos de compras gubernamentales por medio de internet, representan un enorme potencial para lograr dos grandes objetivos de la integración: por una parte, facilitar los intercambios comerciales en los mercados regionales y subregionales, gracias a la eficiencia de las comunicaciones electrónicas y al uso de estándares comunes; por otra parte, garantizar transparencia y posibilidad de vigilancia y control de prácticas de competencia desleal de empresas o países.

2.20 Beneficios ofrecidos por Guatecompras

Guatecompras ofrece beneficios a las tres grandes partes interesadas en la licitación y adquisición de bienes y servicios del Estado de la República de Guatemala. Estos tres son, el sector público, el sector privado y la ciudadanía.

El sector público dispone de:

- Procedimientos de trabajo estandarizados al contar con la información en medios electrónicos y en formatos y tiempos iguales.
- Agilidad y transparencia en los procesos de licitación pública. La consulta en medios electrónicos es más rápida y se encuentra a disposición de quien la requiera en todo momento.
- Mecanismos expeditos de control y seguimiento en las contrataciones.
- Mayor cantidad de proveedores en las licitaciones al ser más fácil y menos costoso el procedimiento.
- Mejores condiciones de calidad y precios en las propuestas de empresas al no repercutir en sus ofertas los gastos de viaje y desplazamiento.
- Economías significativas de recursos a través de la deducción de desperdicios y negociación de los mejores precios, sin perjuicio de la calidad y de acuerdo con las necesidades del aparato administrativo.

Por parte de las empresas o el sector privado, el sistema de Guatecompras ofrece:

- Mayores posibilidades de participar en licitaciones públicas.
- Mecanismos más rápidos y fáciles para obtener información y dar seguimiento a los procesos de contratación del Gobierno.
- Ahorros en el costo de las bases de licitaciones.
- Acceso más amplio a la oferta de bienes y servicios de las pequeñas y medianas empresas, antes limitadas por las condiciones restrictivas de los procesos de licitación.

Capítulo 3

Marco Metodológico

Según (Balestrini, 2000) señala que el marco metodológico es el conjunto de procedimientos a seguir con la finalidad de lograr los objetivos de la información de forma válida y con una alta precisión.

En otras palabras, es el apartado sistemático para la recolección, ordenamiento y análisis de la información, que permite la interpretación de los resultados en función de la solución a implementar.

3.1 Tipo de Investigación

Este trabajo académico de tesis será dictado bajo el diseño del planteamiento metodológico del enfoque cuantitativo, debido a que éste es el mejor enfoque el cual se adapta a las características y necesidades del trabajo académico.

El enfoque cuantitativo utiliza como base la recolección, el ordenamiento y el análisis de los datos obtenidos para dilucidar el comportamiento natural de las tecnologías disruptivas y descentralizadas. “La medición numérica, el conteo y frecuentemente el uso de la estadística para establecer con exactitud patrones de comportamientos en una población.” (Hernández, Fernández & Baptista, 2003)

De los beneficios del enfoque cuantitativo se tomará la técnica de encuestas para poder, por medio de método estadístico, identificar y establecer patrones de comportamiento en la muestra estudiada que servirán como ejes centrales para la búsqueda de una solución efectiva.

3.2 Sujetos de Investigación

La población o sujetos de la investigación se definen como “un conjunto de todos los elementos que se están estudiando, acerca de los cuales se intentan hallar conjeturas.” (Levin y Rubin, 1996).

En el presente documento académico, la población o sujetos de investigación están conformados por empleados profesionales de la “Dirección de Sistemas Informáticos del Ministerio de Finanzas Públicas”, así como empleados profesionales del sector privado del área informática de una institución del sistema financiero guatemalteco.

3.3. Procedimiento

El procedimiento utilizado en esta tesis consta de una serie de pasos esquematizados y documentales los cuales son los siguientes:

1. Elección premeditada del grupo de profesionales a quienes se les aplicó la encuesta.
2. Determinación de la herramienta de software utilizada para la realización y tabulación de las encuestas a los profesionales tecnológicos, esta fue a través de QuestionPro.
3. El tercer paso refiere la interpretación y análisis de los datos obtenidos y tabulados.
4. Se determinó un marco de trabajo de desarrollo para crear el aplicativo en base a los resultados.

3.4 Universo / Población

La población seleccionada se conforma de 25 empleados del sector privado del área informática de una institución del sistema financiero guatemalteco.

Se utilizó una población finita, la cual la conforma profesionales de la tecnología del sector público y privado de la Ciudad de Guatemala.

3.5 Muestra

La muestra es definida como “un subconjunto de una población o grupo de sujetos que formar parte de una misma población.” (Fortin, 1999). En esta línea, señala que es “un subconjunto de la población en que se llevará a cabo la investigación con el fin posterior de generalizar los hallazgos del todo.” (Pineda, Alvarado y Hernández, 1994)

En este trabajo se utilizó el método de muestro no probabilístico, en el cual, de acuerdo con “se toman los casos o unidades que estén disponibles en un momento dato” (Pineda, Alvarado y Canales, 1994), puesto que se solicitó a los empleados que laboran en la Dirección de Sistemas Informáticos del Ministerio de Finanzas Públicas y del área informática de una institución del sistema financiero guatemalteco que formen parte del estudio.

3.6 Plan de recolección de datos

Se refieren a la técnica de recolección de datos como “el procedimiento o forma particular de obtener datos o información (..) la aplicación de una técnica conduce a la obtención de información, la cual debe ser resguardada mediante un instrumento de recolección de datos.” (Falcon y Herrera, 2005).

La técnica y/o instrumento de recolección de datos que se utilizó en el presente trabajo académico es la encuesta de tipo mixta. La cual sus sujetos de aplicación fueron profesionales de las ciencias computacionales del sector privado y público de la Ciudad de Guatemala, tal y como se establece anteriormente.

3.7 Validez y confiabilidad

Para el presente trabajo se es aceptable un porcentaje de confianza que este dentro del rango del 80% al 90%.

3.8 Metodología de desarrollo del Aplicativo

Debido a la naturaleza experimental de Ethereum (ya que está en continuo desarrollo y si tener la primera versión estable fue en 2016), el plan de trabajo consistió en investigar semanalmente cómo evolucionaba el lenguaje de programación de Ethereum. A medida que se aprendió a desarrollar aplicaciones, el desarrollador de la tesis programó cada dos semanas para lograr un avance significativo. También se realizaron reuniones con los tutores virtuales o cursos en línea sobre el desarrollo de Smart Contract en Ethereum. Cada vez que se conseguía algún avance, este era documentado y registrado en el Project del proyecto.

Con lo que la metodología de software mejor adecuada es la iterativo, ya que por medio de un prototipo permite desarrollar modelos de aplicaciones de software que permiten ver la funcionalidad básica de la misma.

3.9 Definición de Requerimientos del Producto

Los requerimientos del producto, en este caso en concreto, de un software específico. No es más que la propiedad o restricción, determinada con precisión, que un producto de software debe satisfacer intrínsecamente.

Los requerimientos del usuario son declaraciones, en lenguaje natural y en diagramas, de los servicios que se espera que el sistema provea y de las restricciones bajo las cuales debe operar. Mientras los requerimientos del sistema establecen con detalle los servicios y restricciones del sistema. El documento de requerimientos del sistema, algunas veces denominado especificación funcional, debe ser preciso. Éste sirve como un contrato entre el comprador del sistema y el desarrollador de software.

3.9.1 Requerimientos Funcionales

Los requerimientos funcionales para este software, el cual usara la tecnología de Blockchain es el almacenamiento seguro de un proceso de licitación el cual se puede consultar en cualquier momento. En este contrato inteligente se tendrán que ver plasmado los siguientes datos del contrato:

1. NOG: Es el número de contrato interno del portal de Guatecompras, más bien no será el identificador del bloque dentro de la cadena de bloques de Ethereum.
2. Descripción: El código del contratante o licitante.
3. Categoría: Rubro perteneciente de la compra (Ejemplo: salud e insumos hospitalarios).
4. Tipo de concurso: Si es de tipo público, privado, entre otros.
5. Entidad: Institución gubernamental quien está solicitando la compra.
6. Tipo de entidad: Descentralizada, autónoma, entre otros.
7. Unidad de compra: Unidad de la institución gubernamental quien compra.
8. Tipo de recepción de ofertas: Si es de forma electrónica o en físico.
9. Fecha de publicación.
10. Fecha de cierre de recepción de ofertas.
11. Tipo de Proceso: Si es de adquisición de servicios, productos, entre otros.
12. Fecha de presentación de ofertas.
13. Monto de cierre de la licitación.
14. Estatus.
15. Empresa o entidad ganadora de la licitación.

En síntesis, los requerimientos funcionales del aplicativo son dos, el primero el ingreso de los datos por el usuario para su almacenamiento y la segunda la lectura de estos datos incorruptibles.

3.9.2 Requerimientos No Funcionales

A lo que se refiere de los requerimientos no funcionales estos esta intrínsicamente relacionado con la tecnología de Blockchain y a la red de Ethereum, entre los aspectos más significativos a resaltar de la tecnología del software están:

1. Entorno Operativo: El Hardware utilizado es toda aquella maquina nodo que se encuentre enlazada a la red de Ethereum, esto brinda al aplicativo de disponibilidad 24/7.
2. Espacio de almacenamiento: El espacio de almacenamiento es tan grande como la red de Ethereum la cual crece día a día, con lo que el software será escalable.
3. La fiabilidad de los datos está intrínseca en la operación, gracias a que estos son inmutables.
4. En lo que se refiere a seguridad, el software cuenta con los tres pilares de la seguridad informática gracias al beneficio de la Blockchain.
5. El beneficio del Smart Contract a desarrollar puede aportar sus métodos y funciones a otro, con lo que el software es reusable en una buena parte.
6. El software no sufre de compatibilidad según el sistema operativo o navegador web que se utilice.

3.10 Equipos de trabajo y roles

En la metodología iterativa o incremental, metodología que se suele utilizar en microempresas o freelances. Durante las distintas iteraciones se va suministrando al cliente funcionalidad adicional, construyendo así un entorno adecuado para el cumplimiento de los requerimientos.

A lo que se requiere de la conformación del equipo de trabajo, este es conformado por únicamente una persona, el cual su rol se enfoca desde el análisis del requerimiento, la planeación, la ejecución, y la puesta en producción.

3.11 Metodología Iterativa

La primera fase que se encuentra en esta metodología es la fase de preparación. la cual inicia con el Staffing y planificación. Aceptación proyecto, asignación fecha inicio y fecha en que arranca el proyecto.

Recursos del proyecto: cliente y desarrollador. Identificación de los principales recursos humanos del equipo de desarrollo (autor de esta tesis) y de los recursos del cliente (responsable/s de proyecto, en este caso el autor de esta tesis). Áreas clave y designación key users. Áreas para cubrir por el proyecto y usuarios clave afectados.

Planificación y calendario reuniones con responsables proyecto. Cronograma reuniones de primer nivel (entiéndase primer nivel por funcionalidades principales, sin detalle). Identificación requerimientos a cubrir. Requerimientos de primer nivel que debe cubrir el proyecto.

Reunión kick-off. Reunión formal de inicio de proyecto, inicio del proyecto. Reunión formal de inicio de proyecto Presentación equipo de trabajo, en este caso es de una única persona. Comunicación objetivos y alcance proyecto. Comunicación de los objetivos a conseguir con la implantación del proyecto, repercusión y mejoras ofrecidas por el nuevo sistema. Definición calendario trabajo. Cronograma de actividades y tareas.

La segunda fase de la metodología interactiva es la fase de prototipado iterativo. Instalación entorno desarrollo. Preparación entorno desarrollos y/o pruebas. Construcción iterativa y configuración y parametrización módulos y extensiones Instalación módulos necesarios y extensiones. Configuración y parametrización. Diseño y desarrollo funcionalidad adicional. Desarrollos adicionales al core de la herramienta. Integración sobre el estándar o como customización.

Desarrollo interfaces con otras herramientas, entornos de integración con herramientas ajenas al core. Realización de pruebas y feedback con implantador. Pruebas unitarias y retroalimentación con implantadores y/o desarrollador. Vuelta al principio y nueva iteración hasta su validación.

Instalación entorno de producción. Instalación modificaciones en entorno de producción de aquellos desarrollos validados.

3.12 Producto

El prototipo final del software será un Smart Contract costumizado con la necesidad del negocio tomando en cuenta los datos de entrada que este requiere para su almacenamiento en la red de Ethereum.

Dicho software contara con una interfaz gráfica sencilla la cual se desplegará a nivel Web para que el usuario final pueda ingresar los datos de la licitación y estos se integren a la red de Ethereum.

Capítulo IV

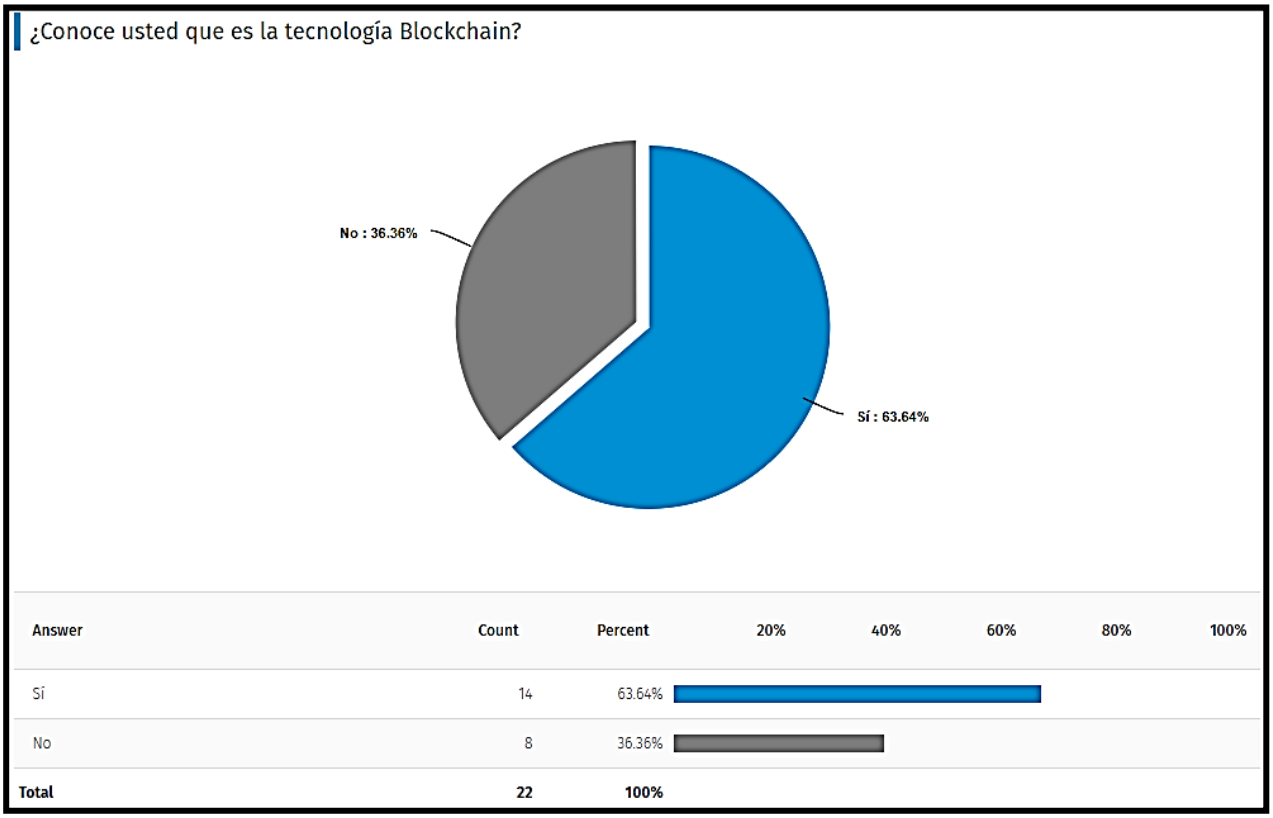
Resultados de la Investigación

4.1 Presentación de Resultados

Los resultados mostrados a continuación es un conteo parcial de las encuestas realizadas a 50 profesionales de las tecnologías de la información y la comunicación. Este conteo es parcial (21 respuestas) debido a que los profesionales del sector público aun a la fecha no han aceptado mi solicitud de encuesta. Los resultados a continuación son recabados en el mes de octubre del año 2020 de forma digital y a tiempo real.

Gráfico No. 1

Conocimiento de la tecnología Blockchain

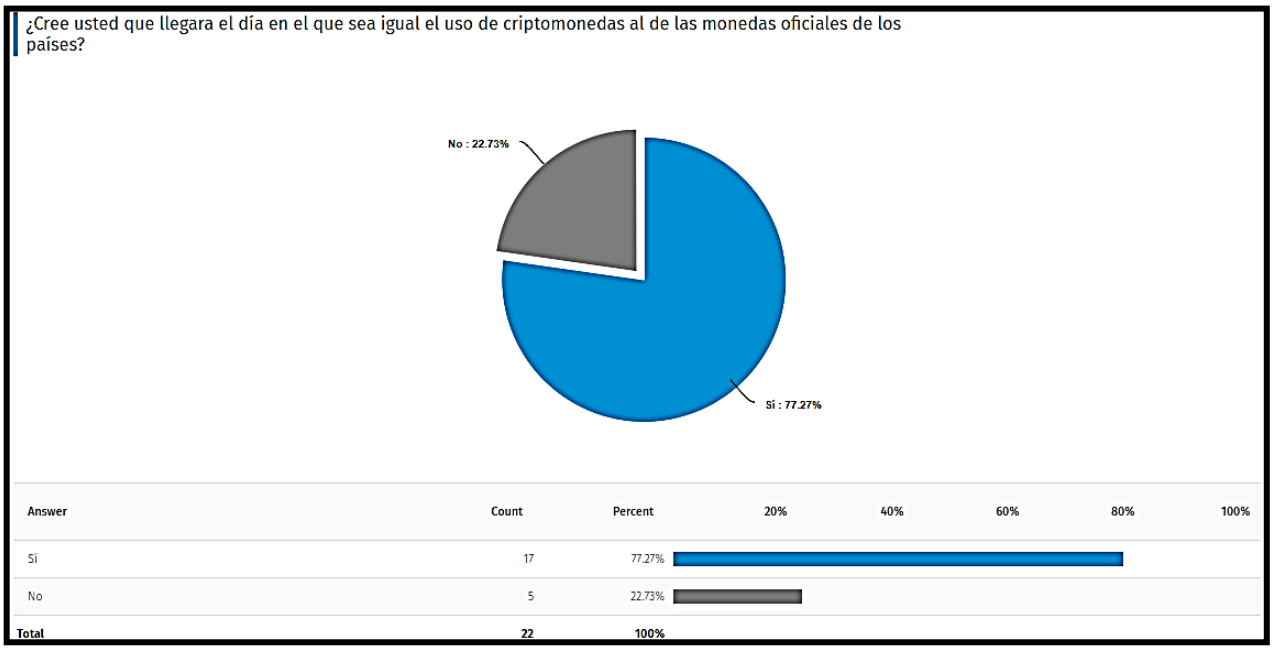


Answer	Count	Percent	20%	40%	60%	80%	100%
Sí	14	63.64%					
No	8	36.36%					
Total	**22**	**100%**					

Fuente: Elaboración propia

Gráfico No. 2

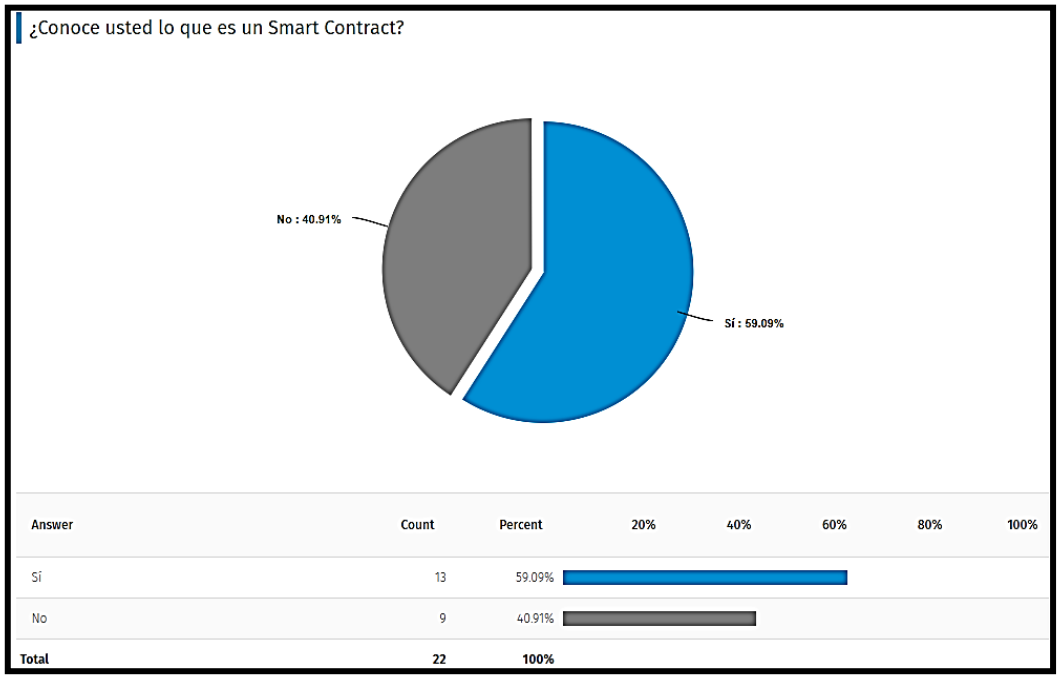
Uso de criptomonedas como moneda oficial



Fuente: Elaboración propia

Gráfico No. 3

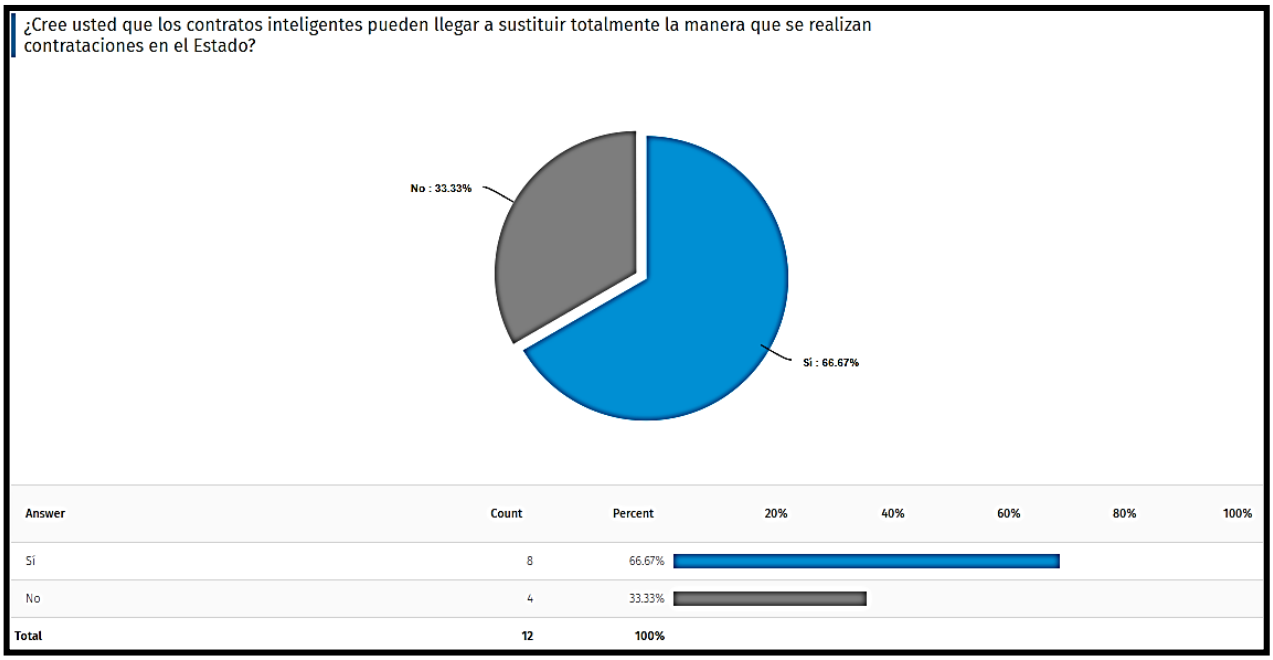
Conocimiento de Smart Contract



Fuente: Elaboración propia

Gráfico No. 4

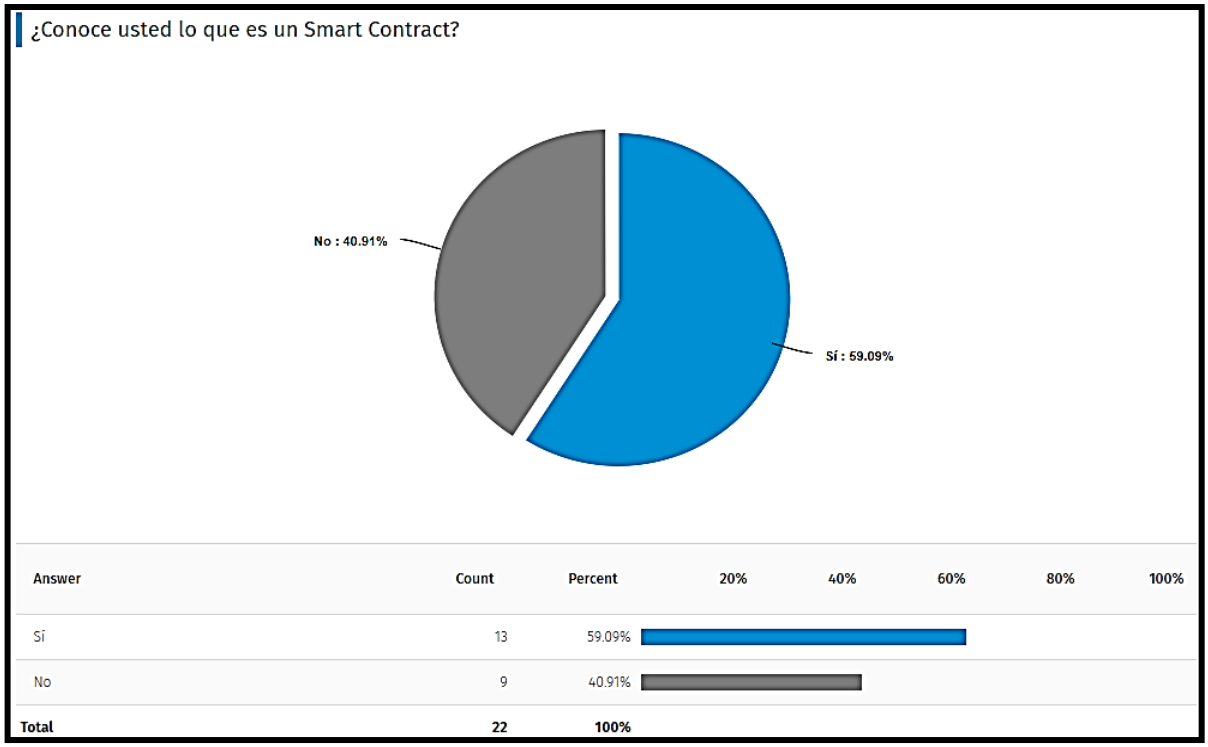
Sustitución de contrataciones del Estado



Fuente: Elaboración propia

Gráfico No. 5

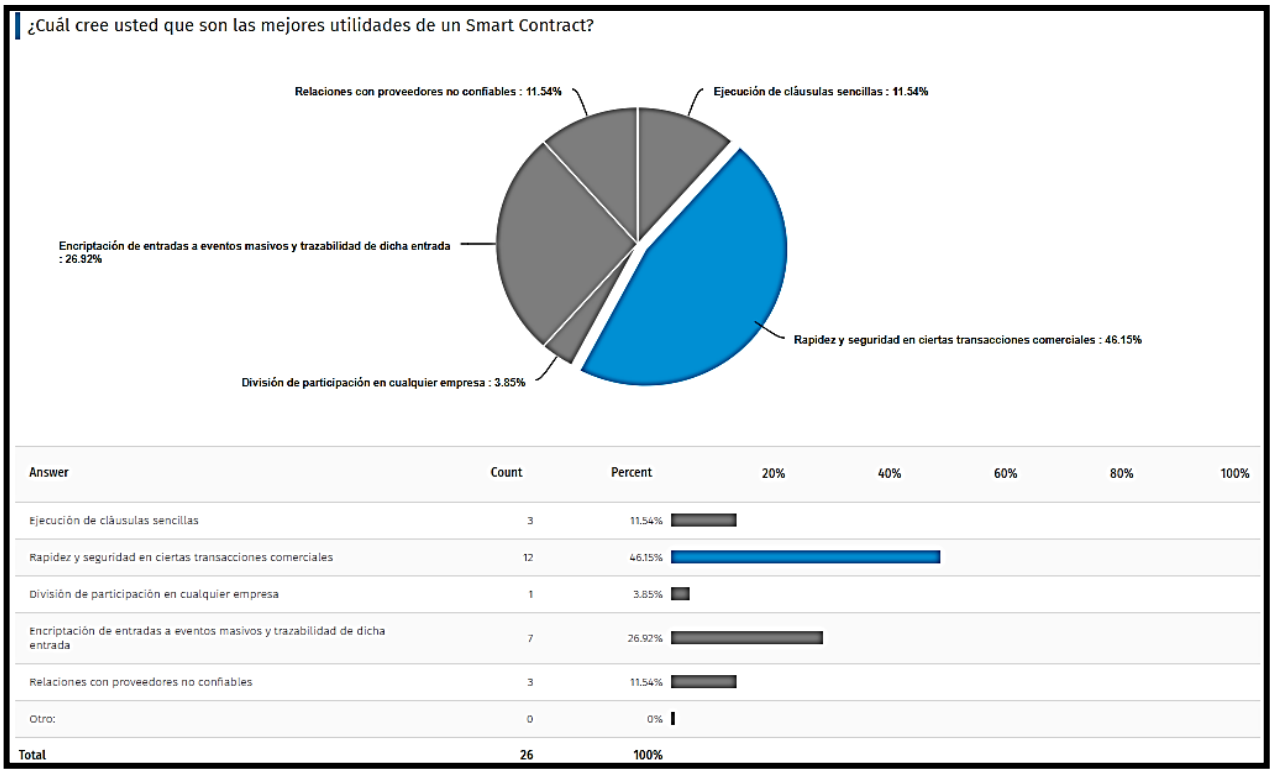
Utilidades de un Smart Contract



Fuente: Elaboración propia

Gráfico No. 6

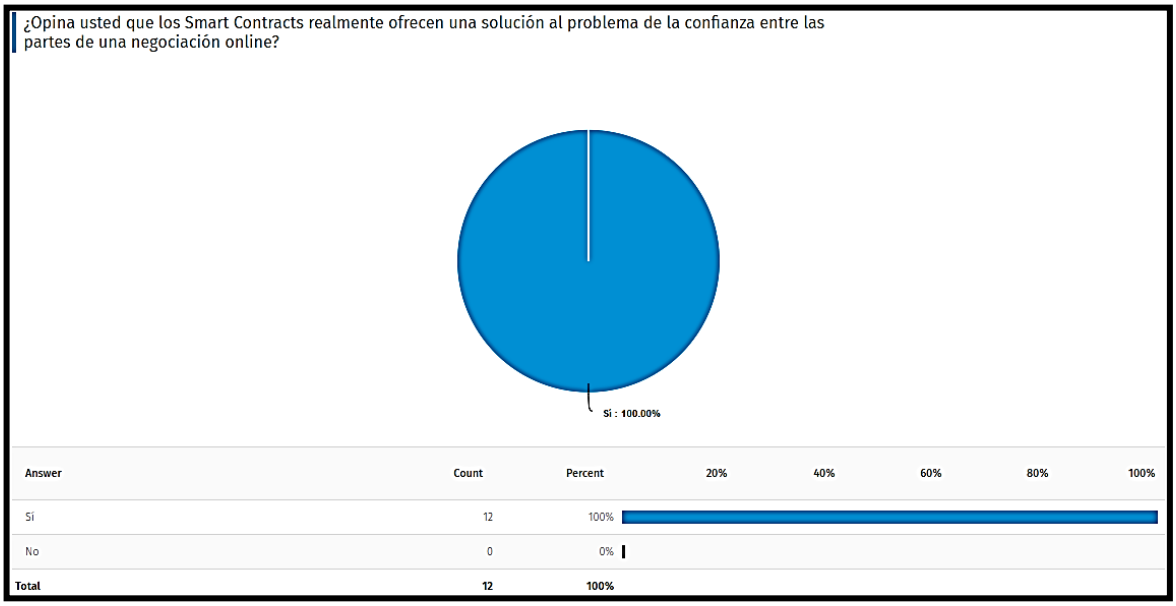
Utilidades de un Smart Contract



Fuente: Elaboración propia

Gráfico No. 7

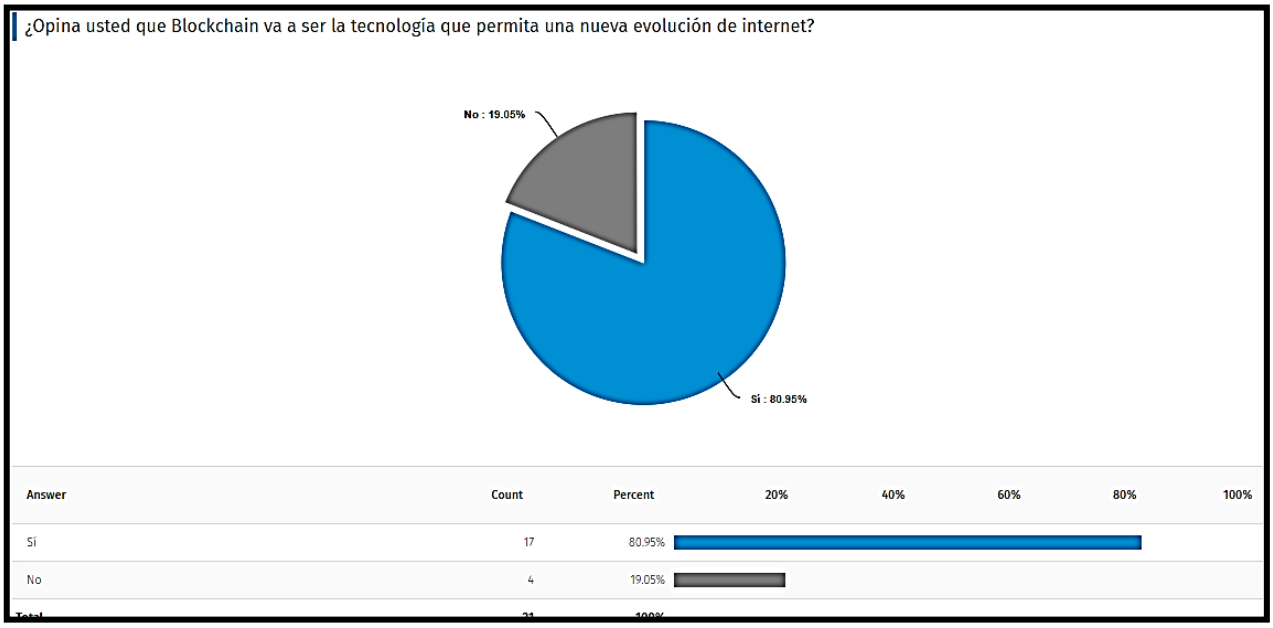
Solución de confianza



Fuente: Elaboración propia

Gráfico No. 8

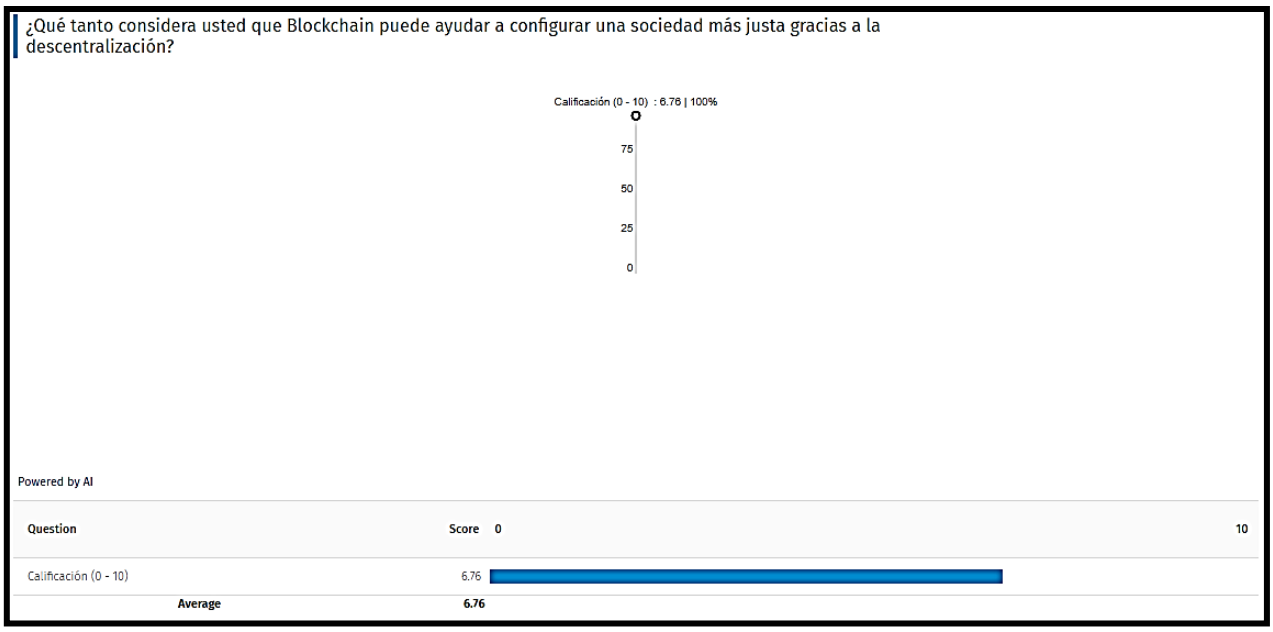
Revolución del Internet



Fuente: Elaboración propia

Gráfico No. 9

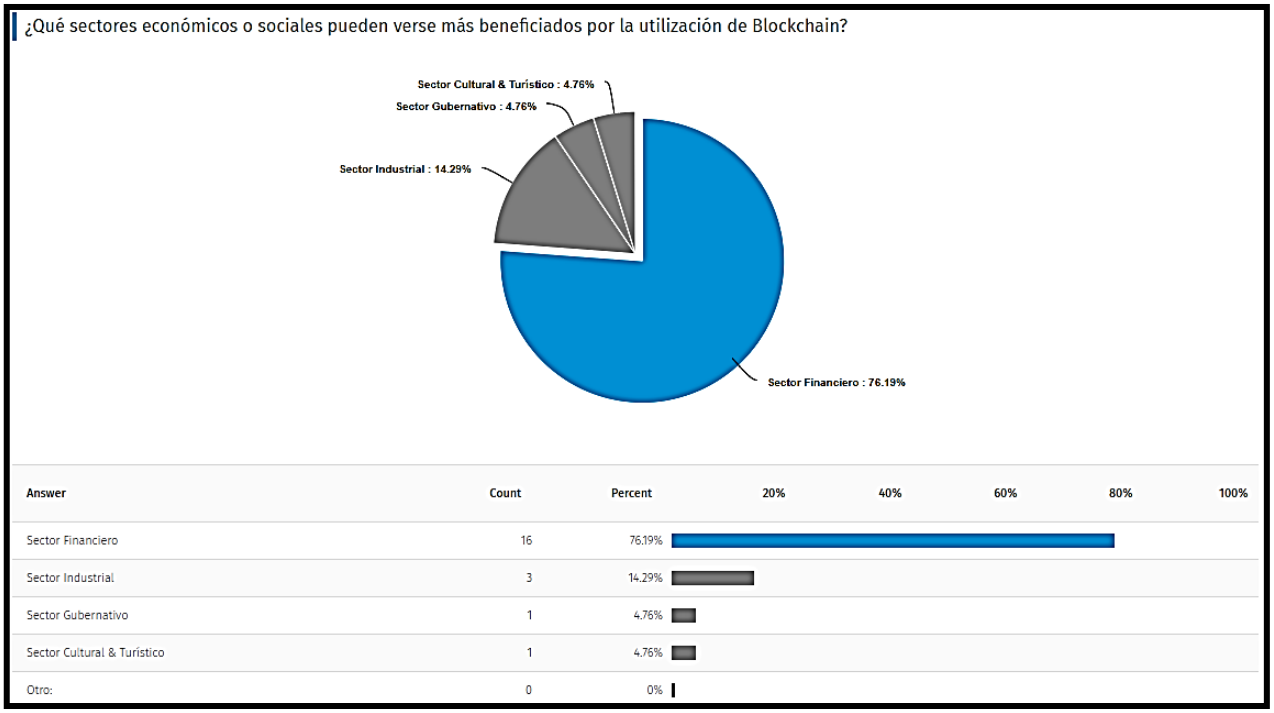
Configuración de la sociedad justa



Fuente: Elaboración propia

Gráfico No. 10

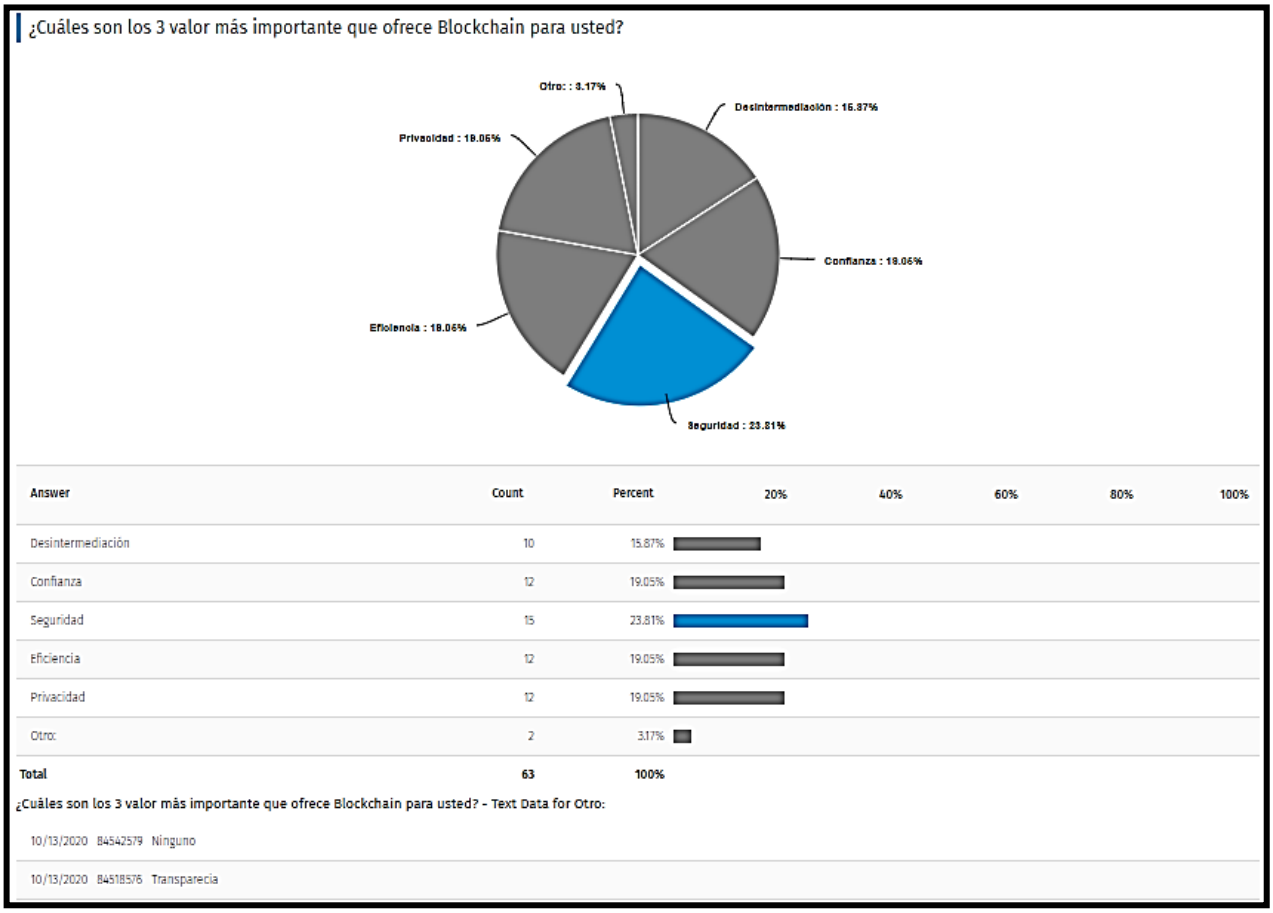
Factores de beneficio en Blockchain



Fuente: Elaboración propia

Gráfico No. 11

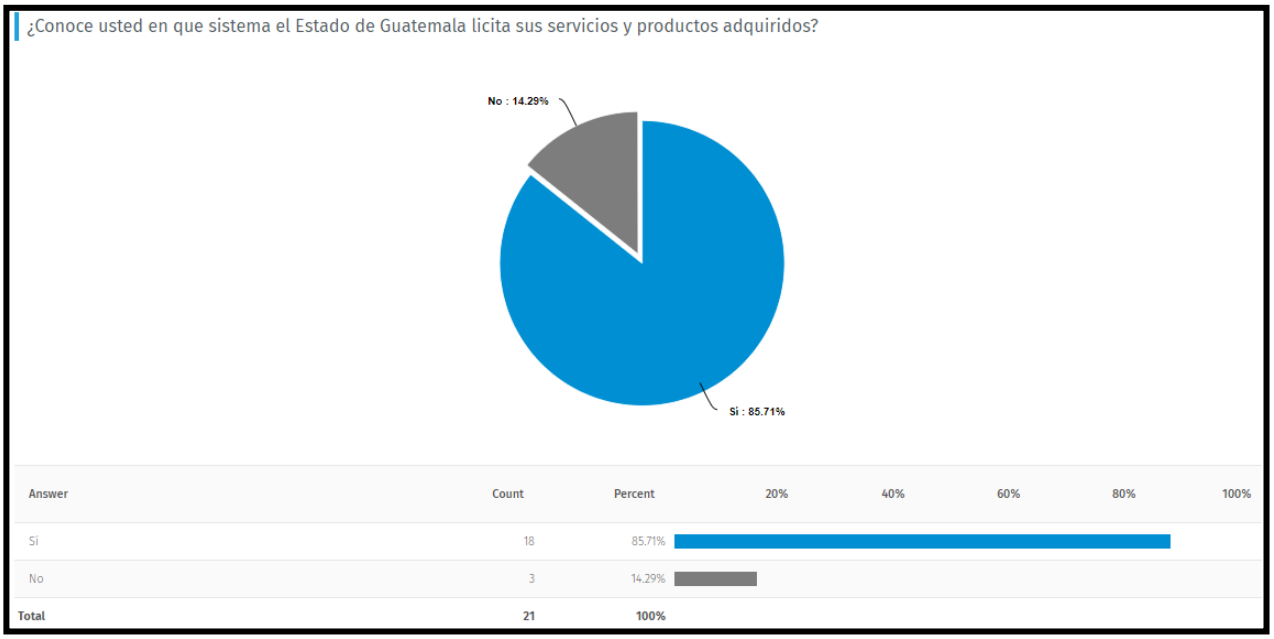
Valores de Blockchain



Fuente: Elaboración propia

Gráfico No. 12

Sistema de licitación del Estado de Guatemala



Fuente: Elaboración propia

4.2 Desarrollo de la Aplicación

En este apartado del documento académico se describen las herramientas y lenguajes que se utilizan y ejecutan en la parte técnica de la investigación llevada a cabo para mostrar el resultado de los objetivos detallados en la metodología. Para ello, ha sido necesaria una revisión de estos como autoaprendizaje, disponible en la documentación accesible de la página web de Ethereum.

4.2.2 Fases del Desarrollo

Las fases del desarrollo utilizado durante este documento académico competen a los de la metodología de desarrollo utilizada en este. Dicha metodología fue descrita en el apartado anterior de este documento. El desarrollo del aplicativo fue basado en tres grandes etapas estas son: fase de preparación y/o análisis, Fase de Prototipado y/o Desarrollo y por último la fase de Instalación y/o pruebas e Implementación.

4.2.3 Análisis

En la primera fase de análisis se dio a la tarea de realizar una investigación previa de modelos de negocios similares al portal de Guatecompras, mismos que han sido migrados a tecnologías disruptivas como lo es Blockchain.

Durante la investigación de estos modelos de negocios similares se determinan funcionalidades similares a lo que hoy proporciona el portal de Guatecompras, con lo que se tomaron como requerimientos bases del software a implementar. Los requerimientos son particulares y de índole transaccional, con lo que el análisis hecho presenta los resultados de usar la tecnología de los Smart contracts, mismos que sus requerimientos funcionales son los siguientes:

- Registros de información contractual.
- Registro de entes contractuales.
- Almacenamiento de datos en la red de Ethereum.
- Interfaz gráfica de usuario amigable e intuitiva.

4.2.4 Situación Actual

Actualmente, el Gobierno de la República de Guatemala cuenta con el sistema Web de Guatecompras, mismo en el cual se maneja toda la gestión de licitación de compras y servicios de todas las unidades gubernamentales que existen en el país. Actualmente el software de Guatecompras se encuentra en un esquema de arquitectura cliente servidor, el cual son servidores físicos resguardados por el Gobierno.

Históricamente Guatemala se ha envuelto en casos de corrupción masivos por licitaciones inmorales favoreciendo a empresas afines a funcionarios públicos, esto por medio de tratos ilegales con los mismos para obtener contratos millonarios. Con lo anterior la ciudadanía actualmente tiene un sentimiento de desconfianza en la mayoría de las licitaciones que realiza el Estado inclusive que el Gobierno de la República de Guatemala cuenta con un software en cual se fiscalice este tipo de actividades.

Adicional a lo anterior, actualmente en temas de legalidad y trasfondos políticos en uso de tecnologías informáticas para el beneficio del Estado y la ciudadanía guatemalteca, se tiene un gran vacío legal y ninguna política de Estado. Dicho lo anterior dificulta mucho la implementación de nuevas tecnologías, tal como lo es Blockchain, por parte de las unidades tecnológicas de los distintos ministerios del Estado de Guatemala.

4.2.5 Situación optimizada

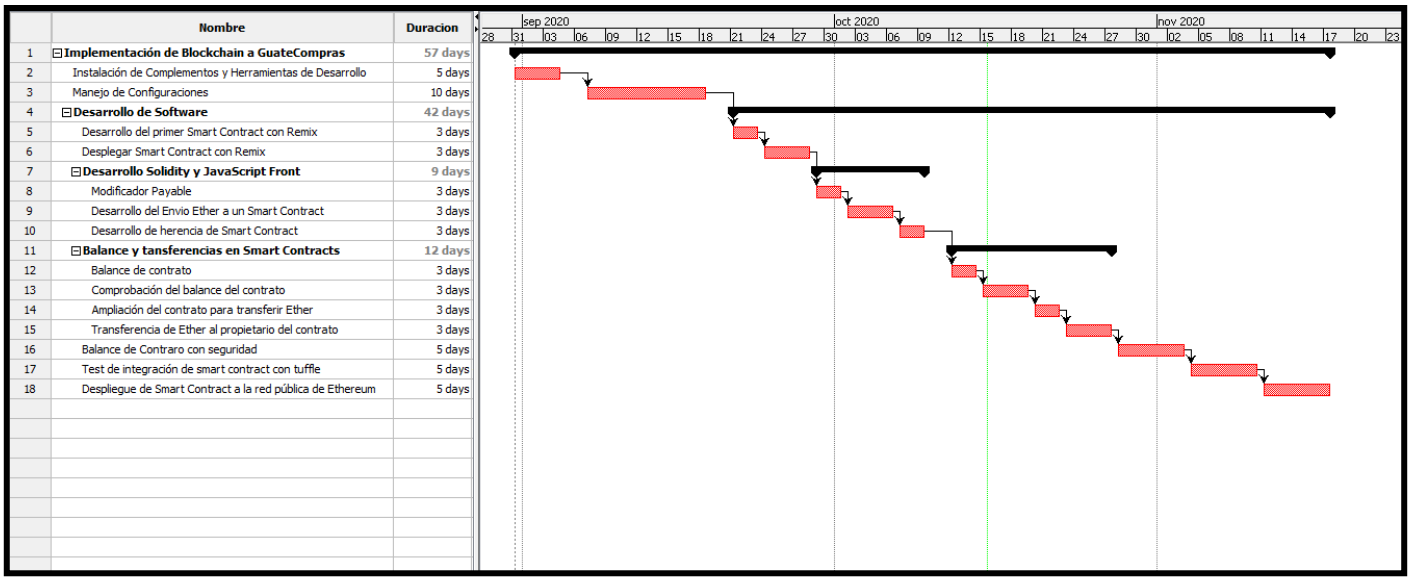
La administración, control, almacenamiento y fiscalización se optimiza mediante un aplicativo web descentralizado, o más conocida como Dapp o Contratos Inteligentes. El beneficio brindado por este aplicativo propuesto es proveer a la ciudadanía una herramienta de fiscalización continua y trazable de todo el proceso de licitación, la cual cualquier ciudadano guatemalteco, o entidad internacional pueda observar y fiscalizar la compra de bienes y servicios por parte del Estado de Guatemala.

En temas tecnológicos, esta tecnología disruptiva brinda una de las redes más grandes e importantes del mundo, Ethereum. La que está presente en millones de computadoras o nodos, que son escalables y están disponibles en todo momento. Con lo que asegura que la información almacenada en las cadenas de bloques siempre se pueda consultar de forma segura y que esta data no sea manipulable por ningún motivo.

4.3 Planificación

La planificación para el desarrollo del aplicativo web fue estimado a 57 días iniciando el 31 de agosto y finalizando el 17 de noviembre de 2020. Durante el desarrollo se visualiza la demo y/o prototipo del software mediante los hitos de:

- Desarrollo de Software.
- Desarrollo Solidity y Front End.
- Balance y transferencias en Smart Contracts.
- Pruebas de Satisfacción



	Nombre	Duracion
1	**Implementación de Blockchain a GuateCompras**	57 days
2	Instalación de Complementos y Herramientas de Desarrollo	5 days
3	Manejo de Configuraciones	10 days
4	**Desarrollo de Software**	42 days
5	Desarrollo del primer Smart Contract con Remix	3 days
6	Desplegar Smart Contract con Remix	3 days
7	**Desarrollo Solidity y JavaScript Front**	9 days
8	Modificador Payable	3 days
9	Desarrollo del Envio Ether a un Smart Contract	3 days
10	Desarrollo de herencia de Smart Contract	3 days
11	**Balance y tansferencias en Smart Contracts**	12 days
12	Balance de contrato	3 days
13	Comprobación del balance del contrato	3 days
14	Ampliación del contrato para transferir Ether	3 days
15	Transferencia de Ether al propietario del contrato	3 days
16	Balance de Contraro con seguridad	5 days
17	Test de integración de smart contract con tuffle	5 days
18	Despliegue de Smart Contract a la red pública de Ethereum	5 days

4.4 Desarrollo

El sistema de licitación propuesto para el uso de Guatecompras se ha realizado mediante una aplicación descentralizada, o más conocida como Dapp. Una Dapp es una aplicación que no depende de un tercero, es decir, un sistema descentralizado que depende de una comunidad de usuarios que la utilizan. Se puede como una aplicación web (Ethereum, 2016). Para el presente trabajo se utiliza como aplicación web e interactúa con un Smart contract de Ethereum.

La diferencia principal entre las aplicaciones tradicionales que todos conocemos frente las Dapps es la parte del servidor o backend. Las Dapps interactúan con el backend si el cliente o frontend cumple las funciones estipuladas en el Smart contract de Ethereum, mientras que las aplicaciones tradicionales el backend se compone de una base de datos o sistema de almacenamiento que la aplicación no puede guardar.

La razón por la que se construye la Dapp sobre Ethereum es precisamente porque la plataforma sirve para la creación de aplicaciones descentralizadas y para ello es principal la seguridad y la interoperabilidad. La seguridad que proporciona Ethereum con PoW es que cuantos más nodos en la red se tenga más segura es el Dapp ante los posibles hackers. La interoperabilidad, favorece al sistema para procesar los datos por igual y evitar fallos, de igual modo que las Dapps funcionan con Blockchain y operan con otras redes independientes, que no sería posible si no hubiera un consenso en el proceso de las transacciones. Por lo tanto, si las Dapps se basan en Ethereum deben estar escritas en el mismo lenguaje para que los programadores puedan interactuar, es decir, en Solidity.

Solidity es un lenguaje informático específico para crear cadena de bloques públicos de Ethereum con una sintaxis similar a Javasript (Ethereum, 2016). Este lenguaje se diseña y compila en bytes (bytecode) para crear y desarrollar los Smart contracts que se ejecutan en una máquina virtual, Ethereum Virtual Machine (EVM). Solidity es un lenguaje de alto nivel, es decir, Turing Complete, aplicado para la tecnología Blockchain y los Smart contracts.

Para implementar la herramienta se requiere definir los programas para crear los nodos, el cliente y las librerías que ayuden a desarrollar la herramienta de participación ciudadana:

Node.js es un entorno de ejecución del nodo que incluye un programa de elaboración en JavaScript para ayudar a que los sitios web sean interactivos. En el trabajo se utiliza el lenguaje Python admitido para Node.js desde terminal. Se escoge está opción ya que es de código abierto, gratuito y se ejecuta para varias plataformas.

Para conseguir un emulador de Blockchain Ethereum ofrece una herramienta de código abierto llamada Ganache. Este programa crea una cadena de bloques virtual y genera diez cuentas falsas que se utilizarán durante el desarrollo del sistema para conseguir hacer transferencias licitaciones sin mucho peso de trabajo.

Web3js es una colección de librerías que permite interactuar con los clientes, ya sea de forma local (teniendo el cliente en nuestro propio ordenador) o de forma remota (estando el cliente instalado en otro ordenador) usando los protocolos Http o Ipc. Web3 nos permite compilar, desplegar e interactuar con nuestros propios contratos inteligentes (Ethereum, 2016).

4.4.1 Arquitectura de hardware

Las operaciones y procesos que la arquitectura contempla son: gestión de claves, emisión, distribución, revocación, renovación y validación. Al igual que la arquitectura PKI vigente, este proceso se encarga de aceptar la petición de emisión de certificados digitales de los diferentes usuarios.

En consiguiente, una vez generado el par de claves, el portador de las mismas expone la clave pública en formato Base58 Check en el servidor web, en la dirección “URL-RAÍZ/emit/pk”, por ejemplo: “www.prueba-clave-publica.com/emit/pk”. Es decir, si un usuario realiza una petición web GET de ese recurso, obtendría la clave pública expuesta anteriormente en formato Base58 Check.

Ya generado esto, se crea una transacción de emisión de certificados que lleva dentro:

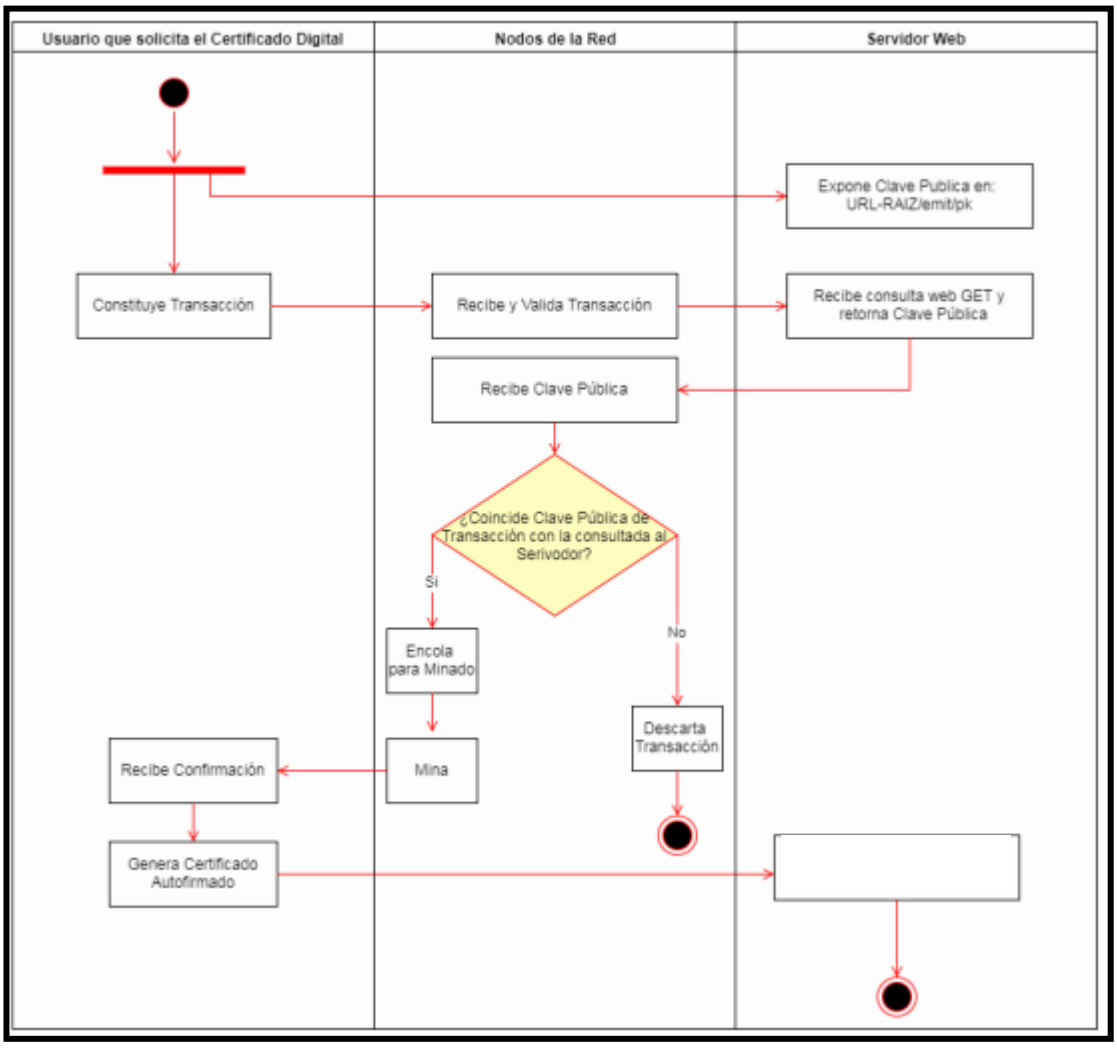
- Como dirección: el Hash de la misma.
- La clave pública del servidor (clave pública a dar de alta).
- El dominio portador de la clave pública (URL-RAÍZ).
- La ruta donde buscarla (/emit/pk).

Luego se disemina esta transacción por la red peer to peer y el portador de la clave pública guarda su confirmación. Todos los nodos que reciban dicha transacción verificarán su integridad y realizarán una petición web GET hacia el recurso expuesto en la misma. Ya recibida la respuesta de la petición, se compara el resultado con la clave pública del servidor contenida dentro de la transacción y en caso afirmativo se retransmite a los demás nodos y se encola para realizar el proceso de minado, en su defecto la misma se descarta.

Una vez minada y confirmada la transacción (al igual que en Bitcoin, para la confirmación se aconsejan 10 bloques por delante del bloque en donde se encuentra la transacción), el creador de la transacción debe generar un certificado x.509 autofirmado o firmado por una Autoridad Certificante propia, desconocida por los demás o incluso conocida. Este certificado contendrá los diferentes campos correspondientes al estándar y a la configuración que se desee, salvo la particularidad de que en el campo opcional issuerUniqueID se dejará asentado el identificador de la transacción confirmada. Ya a esta altura el usuario se encuentra en condiciones de agregarlo a la 69 configuración HTTPS del servidor con su dominio en cuestión y/o firmar otros certificados digitales.

Figura No. 5

Diagrama de flujo Ethereum



Fuente: Elaboración propia.

4.4.2 Arquitectura de Software

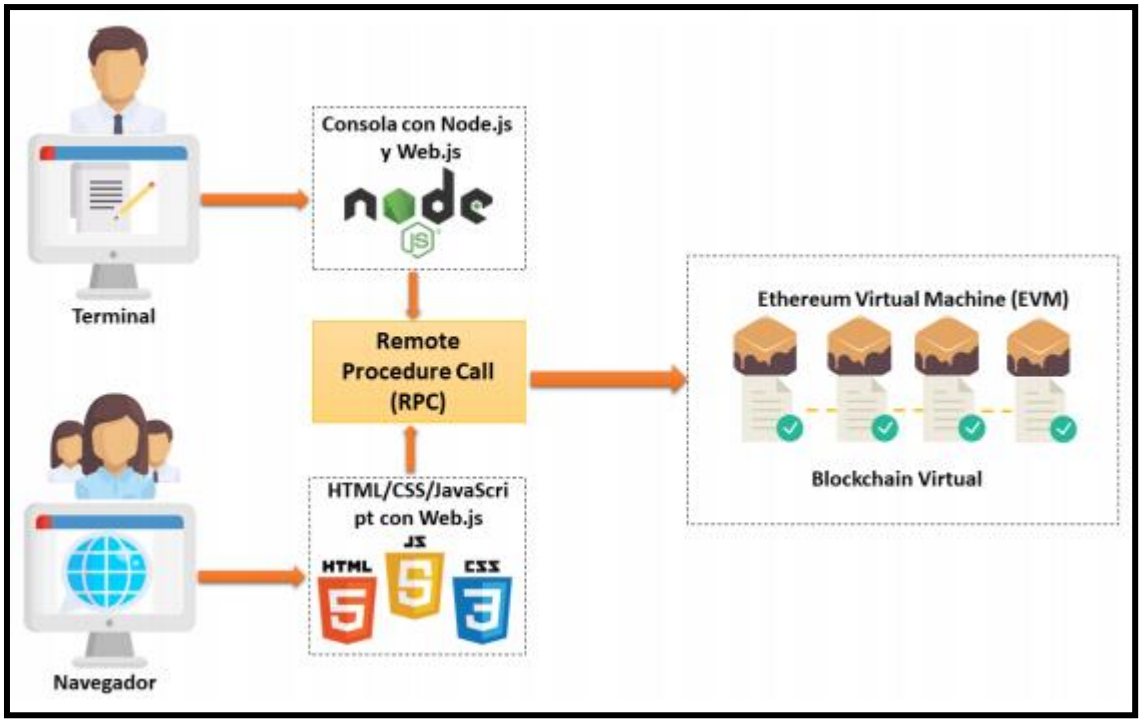
Teniendo en cuenta todas las herramientas necesarias para instalar y ejecutar, se procede a explicar el desarrollo de la herramienta de participación ciudadana a través del sistema de licitación propuesto para este trabajo académico.

A través de la Dapp se estructura el sistema de trabajo para la implementación de la herramienta desde dos partes, desde terminal y desde la web. Desde terminal se ejecuta el node.js junto a la

librería web3js, mientras que para la segunda parte se trabaja con JavaScript y también con web3js, para visualizar el resultado de las votaciones en el navegador web. Ambas partes del trabajo se realiza en computación distribuida, llamada al procedimiento remoto, o Remote Procedure Call (RPC) cuyo fin es ejecutar el código en otra máquina remota sin tener que preocuparse de las comunicaciones entre cliente-servidor. Con la librería web3js se permite interactuar con la máquina virtual del Blockchain ejecutándolo en EVM y RPC para proceder a desplegar el contrato inteligente de la licitación.

Figura No. 6

Diagrama de arquitectura Ethereum



Fuente: Elaboración propia.

Capítulo V
Discusión y análisis de resultados

5.1. Discusión de Resultados

Al paso de los años y las nuevas actualizaciones en tecnología, parece más claro que las tres tecnologías que más potencial tienen para influir en cómo será el futuro de la humanidad son: la Inteligencia Artificial, la Biotecnología y Blockchain. Sin menospreciar otras tecnologías como la ingeniería aeroespacial que puede llevarnos a convertirnos en una sociedad interplanetaria o la realidad virtual que podría llevarnos a un nuevo modelo de vida mixto entre lo real y lo virtual.

El dato anterior es obtenido del libro de Javier Martín Robles denominado “Futrurizable”. Mismo que dedica sus esfuerzos a desentrañar la innovación en tecnología y sus principales corrientes exponenciales que tendrán gran impacto en l sociedad en los años venideros de la humanidad.

De las tres más importantes que se indican, la que puede generar cambios más drásticos para la humanidad es la inteligencia artificial, ya que tiene la capacidad de utilizarse con el resto de las tecnologías para potenciarlas. En el caso de la biotecnología la evolución va a ser más gradual, ya que en la mayoría de los casos se realiza en el ámbito de la investigación científica, donde se requiere mucho tiempo para que las innovaciones lleguen a las personas. Por último, Blockchain se muestra como la tecnología con más rápido evolución y en la que se están llevando a cabo más iniciativas por todo el mundo, sobre todo por el gran interés que despiertan las criptomonedas y por las aplicaciones tan claras que tiene esta tecnología para mejorar la eficiencia en multitud de sectores de la economía como los aplicativos Dapps.

A continuación, se presente el análisis de los datos obtenidos de la encuesta realizada con anterioridad a 25 profesionales de la tecnología que son especialistas en el área financiera en el sector privado.

- La primera interrogante del cuestionario disgrega a los profesionales de la tecnología que han escuchado o conocen de la terminología de Blockchain. Los datos son bastante alentadores teniendo una afirmativa del 63.64% de los participantes. A pesar de ser una tecnología bastante joven en Guatemala y prácticamente inexplorada más del 50% del foro de encuestado afirman tener conocimiento o al menos haber tenido una mínima interacción con la tecnología.

- La segunda interrogante planteada en el cuestionario trata de indagar entre el foro el asertividad del uso de criptomonedas, según los datos el 77.2% del foro afirma que el uso de dichas criptomonedas igualara al uso de la moneda oficial guatemalteca. Esto concuerda con datos obtenidos en otros países latinoamericanos, con lo que los integrantes de las sociedades latinoamericanas están de acuerdo con el uso de divisa digital para transacciones cambiarias, esto se asevera en la pregunta número 3 y 4 de este cuestionario.

- La tercera pregunta trata de indagar que tanto se conoce de Blockchain preguntando sobre el conocimiento de una aplicación especifica de la tecnología, “Smart Contract”. El foro ya anteriormente disgregado, responde de manera mayoritaria afirmando de su conocimiento con el 66.67 %. Con lo que el uso de estos softwares será bien recibido por la comunidad tecnológica, dicha sentencia se afirma con la siguiente pregunta.

- La cuarta pregunta interroga al foro sobre cuáles son los beneficios que ven sobre los Smart Contract. En su mayoría el foro responde con un 46% que el beneficio de estos programas informáticos es su rapidez y seguridad al momento de realizar transacciones, claves para generar confianza en compras de bienes y servicios. Adicional el segundo rubro más votado con un 26.9% es la trazabilidad clara en las operaciones transaccionales, lo que brinda un alto grado de auditabilidad y confianza en dichas acciones cambiarias.

- La quinta interrogante es una aseveración al análisis realizado de la cuarta interrogante. En esta quinta pregunta se trata de conocer que tanta confianza genera un Smart contract

en la compra de bienes y servicios online a el foro. La respuesta a esta interrogante es una masiva afirmación del 100%, con lo que a todos los profesionales del foro les genera confianza este tipo de aplicaciones al momento de realizar transacciones cambiarias.

- La séptima pregunta realizada al foro de profesionales trata de indagar si a sus juicios la tecnología de Blockchain generara una revolución significativa dentro de la vida cotidiana de la ciudadanía. Y los resultados muestran que a juicio de los profesionales la revolución de esta tecnología si afectara el modo cotidiano de la ciudadanía para bien con un 80.95%

- La novena pregunta del cuestionario indaga sobre en qué sectores el foro ve más viable el uso de esta nueva tecnología de "Blockchain". Mayoritariamente el foro con un 76% ve el uso de esta tecnología en el sector financiero, esto debido a que el foro en su mayoría está conformado por profesionales de la tecnología del área financiera. Sin embargo, hubo un 4.76% del foro que afirma que esta tecnología podría utilizarse en el sector gubernamental.

- La décima pregunta del cuestionario indaga a grandes rasgos cuales son los mayores beneficios de Blockchain para el foro de profesionales de la tecnología. Nuevamente el rubro con mayor votación es la seguridad con un 23.81% de los votos escrutados, la segunda posición la comparten los rubros de confianza y eficiencia. Con lo que, esta tecnología es bien aceptada por la comunidad de tecnología ya que asevera dos de los tres grandes beneficios dictados por Blockchain y este documento de investigación.

- Como décima primera pregunta se le hace la interrogante a todo el foro sin discrutinio alguno si conoce el sistema gubernamental de licitación de bienes y servicios del estado de Guatemala. El foro responde de forma asertiva con un 85.71% con lo que el foro conoce las bases de este documento académico y por ende encontrara de gran beneficio la unión de ambas.

5.2 Utilidad de la Aplicación

Finalmente, después del análisis realizado de los datos obtenidos, las investigaciones previas en los capítulos iniciales, así como el análisis jurídico que se llevó a cabo para saber si la tecnología de Blockchain es aplicable en el marco legar y público.

Dicho lo anterior, la utilidad del aplicativo realizado durante este trabajo de grado no es aplicable al sector público preestablecido ya que actualmente no se cuenta con sustento legal válido para la implementación de dicha tecnología.

Sin embargo, la funcionalidad del aplicativo en sí, demostró ser correcta para el ámbito predefinido, y cuenta con las capacidades necesarias para dar satisfacción a las necesidades del negocio. Las transaccionalidades del aplicativo realizado cuenta con todas las bases de la tecnología Blockchain con lo que cada una de las transacciones son seguras, incorruptibles y sobre todo trazables en el tiempo espacio.

Los resultados efectivos de dicha aplicación son sustentados por las pruebas y demostraciones realizadas del mismo. Así también son respaldadas por los resultados de las encuestas realizadas a los profesionales. Ya que demuestra en la práctica lo plasmado por los resultados en la encuesta.

Talvez en este momento no se puede llevar una implementación de esta tecnología al sector público deseado por falta de argumentos legales, sin embargo, esta aplicación fue dotada de una característica de heredación con lo cual puede mutar a otra necesidad de negocio similar, siempre conservando su característica de transaccionalidad. Una de esas necesidades que puede atender esta tecnología y específicamente el aplicativo realizado es la compra de boletos aéreos online. Puede registrar las compras de los boletos aéreos almacenarlos en la red de Blockchain y registrar toda la trazabilidad de vuelo. Así como también puede otorgar un sistema de lealtad. En donde por cada compra de un boleto aéreo, al cliente se le devuelve un porcentaje en divisa electrónica.

Conclusiones

Finalmente, tras haber desarrollado todo el documento de cierre de grado, a continuación, se desarrollan una serie de conclusiones relacionadas principalmente con los objetivos preestablecidos al comienzo del trabajo y con la aplicación de Blockchain que se ha podido desarrollar durante el mismo.

A lo largo de este trabajo se pretendió entender, conocer y aplicar con mayor profundidad las características básicas de Blockchain que permitieran generar valor y una idea de cuál es su potencial para el ámbito público guatemalteco.

Según los resultados encontrados de acuerdo la elaboración del anterior modelo, con base al objetivo de este proyecto que es evaluar el posible uso y aplicación de la tecnología Blockchain como una solución para la gestión de licitaciones públicas en Guatemala, con el fin de superar los problemas actuales de corrupción, confianza, competencia y transparencia en el sector público y siendo probado bajo un caso de estudio de licitación ya ejecutado, podemos concluir lo siguiente:

- Tras el análisis relacionado con la legislación en el ámbito nacional y local se ha podido conocer la nula evolución de la normativa dentro del marco del sector público. Este estudio ha servido para conocer todos los conceptos legales claves que pueden estar estrechamente ligados con el Blockchain, ya que todavía no existe ninguna normativa regulada sobre esta tecnología.

- Sobre el Blockchain existen muchas referencias actuales, pero pocas de ellas la introducen en la vertiente de las entidades públicas. A pesar de las limitaciones que ha supuesto la recogida de la información relacionada con el Blockchain y las AAPP, se ha podido analizar varias fuentes de datos. De esta manera, se ha conocido los conceptos clave de esta tecnología y sus diversas implementaciones que garantizan una mayor calidad de vida a las instituciones y a la ciudadanía.

- Blockchain tiene la posibilidad de apoyar a los Gobiernos a descentralizar la información y
  generar mayor fiabilidad y confianza entre sus ciudadanos creando bases de datos transparentes que ayuden a minimizar la corrupción.

- La tecnología Blockchain permite compartir la información con diferentes nodos a nivel global, para que pueda ser analizada y fiscalizada por cualquier usuario de la red.

- El modelo propuesto permite que exista una contratación trasparente cumpliendo con los requisitos legales, sin generar sobrecostos y atendiendo las necesidades de los ciudadanos.

- Como último punto respondiendo a la pregunta del planteamiento inicial de este trabajo académico: "¿Cómo la tecnología de Blockchain permitirá la descentralización de los procesos de compras del Estado de la República de Guatemala y ofrecerá a la ciudadanía una gestión transparente, trazable y segura?", la respuesta a esta interrogante es la implementación de una red de Blockchain hibrida entre el sector público, académico y privado tal como el modelo de otros países latinoamericanos que se han sumado a esta tecnología. O bien implementado Smart Contract en una red como la es Ethereum para poder postular y licitar de una forma más transversal a todos los sectores guatemaltecos interesados, tal y como lo dicta el modelo propuesto en este trabajo. Sin embargo, debido a la falta de legislación actualmente en el país sobre este tema actualmente es imposible una implementación de dicha tecnología al ámbito de licitaciones y compras del Estado de la República de Guatemala. Con lo que la respuesta a la pregunta planteada lastimosamente es negativa, ya que actualmente Blockchain no puede ofrecer a la ciudadanía guatemalteca una gestión transparente, trazable y segura de las compras del Estado debido al vacío legal existente.

Trabajo Futuro

Dado a que actualmente la implementación de la tecnología de Blockchain, en el sistema que gestiona las Licitaciones y Compras del Estado de Guatemala, es imposible en la actualidad por un vacío legal. Se expone el acontecimiento dicho y una nueva propuesta de implementación en este apartado especial del trabajo académico.

Después de las investigaciones y análisis del ámbito legal y normativo guatemalteco en conjunto con especialistas legales y tecnológicos, sobre el uso de tecnologías disruptivas en aplicativos que gestiona los poderes el Estado de Guatemala, y el análisis de la Ley de Contrataciones del Estado de Guatemala.

Se determina que existe un vacío legal en el marco de la Ley ya que en ninguno de los artículos de la Ley de Contrataciones del Estado de Guatemala y en las leyes orgánicas del Ministerio de Finanzas norma la forma y tecnologías que se pueden aplicar al resguardo y manejo de la data utilizada en el proceso de licitaciones y compras del Estado de Guatemala, con lo que al momento de aplicar la tecnología de Blockchain no existe base legal alguna con lo que la entidad gubernativa contralora determina que este tipo de tecnología no es propicia sin ley y sin presupuesto establecido con anticipación.

A grandes rasgos los tres grandes vacíos legales que se encuentran en las leyes mencionadas son las siguientes:

- La inexistente ley y/o artículos que norme la manera y forma de crear un aplicativo que resguarde y gestione la data implicada en la licitación y compras del Estado de Guatemala. Así como el uso explícito de tecnologías que se puedan implementar y el uso que se pueda dar de ellas a favor de la ciudadanía guatemalteca.

- La inexistente ley y/o artículos que normen la sanción por la forma en que se lleve la administración e implementación (arquitectura) del aplicativo de licitaciones y contrataciones del Estado de Guatemala.

- Al momento de querer implementar una tecnología como lo es Blockchain al sistema de licitaciones del Estado de la República de Guatemala, este por su naturaleza no contempla un gasto fijo para el Estado ya que por cada transacción realizada se debe pagar un monto no determinado, es decir fluctuante (determinado por oferta y demanda de los mercados internacionales) con lo que no se puede determinar dato exacto de ese gasto. Dicho lo anterior, la Contraloría General de Cuentas de la Nación de Guatemala niega este tipo de procedimientos y sanciona a criterio subjetivo sin base legal.

Dada la explicación del motivo por la cual no se puede llevar a etapa de implementación el proyecto de software de esta tesis y únicamente llego a etapa de prototipo, se procede a realizar un planteamiento nuevo sobre algún otro rol de negocio en donde se pueda implementar dicha tecnología a un futuro.

Nuevo Planteamiento – La aerolínea

Pueden comenzar por dejar atrás las percepciones erróneas comunes. No es sorprendente que los no iniciados confundan Blockchain con Bitcoin. La realidad, sin embargo, es que Blockchain es la tecnología de Bitcoin, sin la moneda.

La tecnología Blockchain transfiere y tokeniza valor con elegancia. Ampliar la definición de valor muestra de cuántas formas se puede aplicar la cadena de bloques. Existe el intercambio de valor financiero directo. Sin embargo, también existe el intercambio de valor financiero indirecto: el valor comercial, operativo y de experiencia del cliente que proviene de mover datos a través de una empresa o ecosistema.

Las características de la industria de las aerolíneas, y también la industria de viajes en general, se alinean muy bien con las capacidades de Blockchain. El intercambio de datos entre múltiples actores y puntos de contacto impulsa el viaje. Desde la reserva hasta la llegada, los involucrados pueden incluir aerolíneas, plataformas de viajes en línea, proveedores de tarjetas, aeropuertos, inmigración, Gobierno, hoteles, agencias de alquiler de automóviles y más.

Cada actor requiere, recopila, almacena y, a menudo, comparte información operativa y de viajeros. De hecho, una red de conciliación de datos compleja y aparentemente interminable está ocurriendo detrás de escena de cada punto de contacto del viaje de cada viajero.

Con tantos sistemas en juego (las aerolíneas por sí solas almacenan datos en muchos sistemas aislados, desde el servicio de pasajeros hasta la gestión de la tripulación), el intercambio de datos no siempre es fluido. Y en la industria de las aerolíneas, no solo están en juego la integridad operativa y la generación de ingresos cuando algo sale mal, sino también la seguridad y la protección.

Es fácil ver por qué el uso de la tecnología Blockchain para mejorar la reconciliación y el intercambio de datos es una propuesta de valor convincente para esta industria. Las posibilidades más creativas y disruptivas van más allá de las meras transacciones financieras. Considera lo siguiente:

- Venta de pasajes aéreos: Un boleto electrónico es, en esencia, una entrada de base de datos, información que se habría impreso en un boleto de papel desmaterializado, almacenado y recuperado de una base de datos masiva. La cadena de bloques puede tokenizar este activo y desmaterializarlo aún más. Mediante el uso de contratos inteligentes asociados con el activo, las aerolíneas pueden agregar lógica comercial y términos y condiciones sobre cómo se vende y usa el boleto. Esto abre la puerta para que los boletos sean vendidos por diferentes socios, y en tiempo real, desde cualquier parte del mundo.

- Planes de Lealtad: La lealtad es un gran negocio en los viajes aéreos. En los esquemas tradicionales de puntos de fidelidad, los viajeros a menudo tienen que esperar hasta que los puntos se liquiden y se acumulan para usarlos, y están limitados en cuanto a dónde pueden gastarlos. Al tokenizar los puntos de fidelidad en la cadena de bloques, los viajeros pueden obtener un valor instantáneo canjeándolos en el acto. También pueden utilizarlos de manera más amplia a través de una comunidad de usuarios específica de socios. Piense en ello como un mercado o modelo de intercambio. Con los puntos aceptados como "moneda" entre más proveedores, los viajeros obtienen un programa más fácil y rápido de usar que es más relevante para sus preferencias personales.

- Seguridad informática y de identidad: La protección de la privacidad de los datos es un tema claro cuando se trata de registros de pasajeros, manifiestos de vuelo e información de la tripulación. Sin mencionar las implicaciones de seguridad que están en juego en el mundo actual si estos datos no están protegidos adecuadamente. La tecnología Blockchain con un envoltorio de seguridad crea una forma muy diferente y menos riesgosa de administrar y compartir esta información mediante el uso de requisitos de acceso autorizados.

- Mantenimiento y escalabilidad: La tecnología Blockchain puede transformar los registros de mantenimiento, que en el mejor de los casos se encuentran en engorrosas bases de datos y, en el peor de los casos, en carpetas de papel. La cadena de bloques puede ayudar a la industria a garantizar que las piezas adquiridas sean legítimas y pueda ofrecer un registro inmutable de "copia virtual" de la procedencia de cada pieza en el avión, cada vez que ha sido manipulada y por quién, desde el comienzo de la existencia de la aeronave. Esta visibilidad es profunda y puede llevar la práctica del mantenimiento, la seguridad y la protección de las aeronaves a nuevos niveles.

El entusiasmo por la tecnología Blockchain está justificado en las aerolíneas. Aun así, las aerolíneas deben abordar la evolución de la cadena de bloques con criterio. La gestión de datos no puede convertirse de marea simple. La mejor manera de evaluar la viabilidad de la cadena de

bloques para las necesidades de gestión de datos es preguntando y respondiendo afirmativamente a las siguientes preguntas: ¿Hay muchos puntos de validación y control?, ¿Hay varios actores consumiendo los datos?, ¿Es necesario conciliar los datos?, ¿La visibilidad de la cadena de custodia completa no es negociable? y ¿Se debe realizar un seguimiento de la calidad y el linaje de los datos desde el primer día?

Recomendaciones

Dentro de este apartado se establecen una serie de recomendaciones a los involucrados claves para la implementación de Blockchain como tecnología clave para la transformación digital inteligente del proceso de Licitaciones y Contrataciones del Estado de Guatemala, las recomendaciones están dirigidas a los siguientes involucrados:

- Facultad de Ingenieria y Ciencias Aplicadas: Crear dos cursos dentro del pensum actual de la carrera en donde se pueda capacitar a los nuevos profesionales de la tecnología sobre Blockchain, las tecnologías disruptivas y descentralizadas.

- A los actuales profesionales de la tecnología: Buscar cursos de capacitación en línea sobre la tecnología de Blockchain y como esta es uno de los tres pilares informáticos del futuro próximo.

- Al Gobierno de la República de Guatemala: Llevar a cabo una propuesta de ley y su debida aprobación para poder legislar una ley en la que se pueda implementar la tecnología del Blockchain, no solo al ámbito de licitaciones y compras del Estado, sino a todo ámbito de gestión pública. Este tipo de legislación favorecen al pueblo de Guatemala, así como a la administración gubernativa.

- Al pueblo en general de Guatemala: Informase sobre esta nueva tecnología y los beneficios para una sociedad más justa e igualitaria. Empoderarse y solicitar a los legisladores en turno crear leyes favorables a dicha tecnología para poder tener una fiscalización transversal, segura y continua de la administración pública.

- A las organizaciones internacionales y países aliados: Crear tratados internacionales en donde se incluya al Estado de Guatemala como firmante activo y reconocido sobre la creación de aplicativos basados en Blockchain y tecnologías descentralizadas para la administración pública.

Referencias

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. International Journal of Research in Engineering and Technology, 5, 1-10.

Academy by Bit2me. Smart Contracts: ¿Qué son? cómo funcionan y qué aportan? s.f.https://academy.bit2me.com/que-son-los-smart-contracts/

ALEIXANDRE-BENAVENT, R.; CASTELLÓ, L; FERRER-SAPENA, A.; PESET, F. (2018). Tendencias de investigación en los artículos recientes sobre las aplicaciones de la tecnología Blockchain en ciencias de la salud. XVIII Jornadas Nacionales de Documentación Médica, 13-15 de junio 2018, Santander http://www.jornadasdocumentacion2018.com/wpcontent/uploads/2018/06/P04.pdf

ALEIXANDRE-BENAVENT, R.; FERRER-SAPENA, A.; PESET, F.; SÁNCHEZ-PÉREZ, EA.; CALABUIG JM.; BEJARANO BAILEN, J.; FALCIANI, H. (2018). Hacia nuevos modelos de comunicación científica. Propuesta para la revalorización del trabajo científico basada en tecnología Blockchain -Scie-Chain. XVIII Jornadas Nacionales de Documentación Médica, 13-15 de junio 2018, Santander http://www.jornadasdocumentacion2018.com/wpcontent/uploads/2018/06/P14.pdf

Allende López, Marcos. «Blockchain: Cómo desarrollar confianza en entornos complejos para generar valor de impacto social.» Junio de 2018. https://publications.iadb.org/es/publicacion/17379/Blockchain-como-desarrollarconfianza-en-entornos-complejos-para-generar-valor-de

BERRYHILL, J., BOURGERY, T. & HANSON, A. (2018), "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", OECD Working Papers on Public Governance, n. 28. https://doi.org/10.1787/3c32c429-en

CABALLERO GIMENO, J. A. (2018). Estudio de tecnologías Bitcloin y Blockchain. Trabajo Fin de Máster. Barcelona: Universitat Oberta de Catalunya, http://hdl.handle.net/10609/81268

Chen, & Yan. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. Business Horizons, Volume 61, Issue 4, 567-575.

Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and

innovation. Business Horizons, Volume 61, Issue 4, 567-575.

ETHEREUM (2016). Ethereum Homestead Documentation. http://ethdocs.org/en/latest/index.html

Ethereum. El "Gas" en Ethereum. 2018. https://www.miethereum.com/ether/gas/

Guatecompras, portal de licitaciones y compras del estado de Guatemala 2020. https://www.Guatecompras.gt/

Maldonado, Jose. Votaciones Blockchain: mitos, realidades y retos futuros. 28 de Mayo de 2019. https://www.bitcobie.com/votaciones-Blockchain-mitos-realidades-y-retosfuturos/

miethereum. (8 de Octubre de 2020). Obtenido de https://miethereum.com/mineria/

miethereum. (2020). Ethereum. Obtenido de https://miethereum.com/smartcontracts/dapps/#toc1

OROYFINANAZAS (2015). “Diferencias entre las cadenas de bloques (Blockchain) públicas y cadenas de bloques privadas”, 15 de octubre. https://www.oroyfinanzas.com/2015/10/diferencias-cadenas-bloquesBlockchain-publicas-privadas/

Anexos

Anexo I

1. ¿Conoce usted que es Blockchain?

Si

No

2. ¿Cree usted que llegara el día en el que se igual el uso de criptomonedas al de las monedas oficiales de los países?

Si

No

3. ¿Cree usted que los contratos inteligentes pueden llegar a sustituir totalmente la manera que se realizan contrataciones en el Estado?

Si

No

4. ¿Opina usted que Blockchain va a ser la tecnología que permita una nueva evolución de internet?

Si

No

5. ¿Qué tanto considera usted que Blockchain puede ayudar a configurar una sociedad más justa gracias a la descentralización?

0 a 10 (siendo 10 la calificación más alta)

6. ¿Qué sectores económicos o sociales pueden verse más beneficiados por la utilización de Blockchain?

Finanzas

Industria

Gobierno

Cultura

Otros

7. ¿Cuáles son los 3 valor más importante que ofrece Blockchain para usted?

Desintermediación

Confianza

Seguridad

Eficiencia

Privacidad

Otros:_____

8. ¿Conoce usted lo que es un Smart Contract?

Si

No

9. ¿Cuál cree usted que es la mejor utilidad de un Smart Contract?

Ejecución de cláusulas sencillas

Rapidez y seguridad en ciertas transacciones comerciales

División de participación en cualquier empresa

Encriptación de entradas a eventos masivos y trazabilidad de dicha entrada

Relaciones con proveedores no confiables

Otros (Especifique)

10. ¿Opina usted que los Smart Contracts realmente ofrecen una solución al problema de la confianza entre las partes de una negociación online?

Si

No

11. ¿Conoce usted en que sistema el Estado de Guatemala licita sus servicios y productos adquiridos?

Si

No.

12. Para usted en 10 años en dónde ve esta tecnología de Blockchain?

_____

13. Cree usted que el uso de la Blockchain en sistemas de licitación del Estado tiene algún beneficio a la ciudadanía y porque?