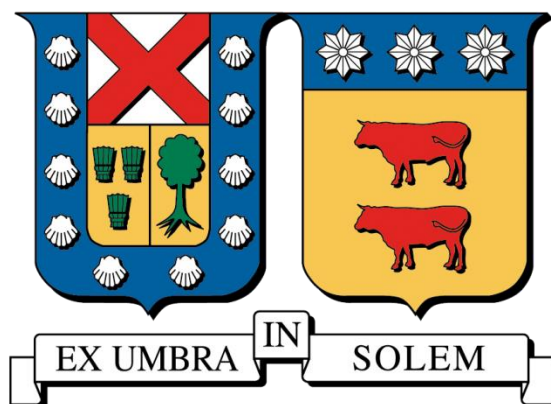


UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INGENIERÍA COMERCIAL
VALPARAÍSO-CHILE



**APLICACIÓN DE CADENAS DE BLOQUES Y CONTRATOS INTELIGENTES EN
INDUSTRIAS DEL ÁMBITO NACIONAL**

GONZALO JAVIER FLORES CASTRO

MEMORIA PARA OPTAR AL TÍTULO DE:
INGENIERO COMERCIAL

PROFESOR GUÍA: SR. JUAN TAPIA
PROFESOR CORREFERENTE: SR. LUIS ACOSTA

NOVIEMBRE 2019

RESUMEN

En el presente trabajo se intenta hacer un primer acercamiento investigativo de la población universitaria chilena con respecto a las tecnologías de cadenas de bloques, también nombrada en lo sucesivo como blockchain, y a las aplicaciones derivadas más conocidas de ésta, como son las criptomonedas y los contratos inteligentes. Además se describirán dos sectores específicos, como son la industria aseguradora y el sector gubernamental, puesto que éstos poseen a juicio de los expertos un enorme potencial para ser transformados por esta tecnología.

Para esto se realizará un análisis exploratorio que tenga en cuenta las opiniones de la población estudiada, y bibliográfico para describir y estudiar los casos en los que blockchain ya está transformando muchos países en el mundo. Se finalizará con conclusiones y recomendaciones asociadas a los resultados hallados.

ÍNDICE

1. Problema de Investigación	4
2. Objetivos	6
2.1 Objetivo General	6
2.2 Objetivos Específicos	6
3. Marco Teórico	7
3.1 Algunos antecedentes	7
3.1.1 Bitcoin	7
3.1.2 Ethereum	8
3.1.3 Ether	8
3.2 El funcionamiento y las Matemáticas del Blockchain	9
3.3. Los contratos inteligentes	11
3.4. La máquina virtual de Ethereum (EVM)	12
3.5. Oráculo	13
3.6. Raiden Network (RDN)	14
4. Metodología	15
4.1. La Encuesta	16
4.1.1 Formato Encuesta	17
4.1.2 Beneficios y Problemas de aplicar la encuesta	21

5. Resultados	23
5.1 Población y Blockchain	23
5.2 Áreas de Interés y Posibles Desarrollos	25
5.3 Sector Seguros	25
5.4 Sector Gubernamental	27
5.4.1 Estonia	27
5.4.2 Dubái	28
5.4.3 Otros Países	29
6. Conclusiones y Recomendaciones	30
7. Referencias	32

1 PROBLEMA DE INVESTIGACIÓN

Desde el nacimiento de la world wide web (www) en el año 1991 internet se ha masificado exponencialmente, las personas tienen acceso a esta a través de smartphones, tablets, computadores, en prácticamente todos los rincones del planeta, dando lugar a una transformación en casi la totalidad de los sectores industriales de la economía: retail, financiero, inmobiliario, educacional, instituciones gubernamentales, etc.

Dada la facilidad de acceso a Internet, a crear una página web, o a iniciar un negocio a través de esta, sería lógico pensar que Internet iba a ser un espacio democrático, con muchos competidores y negocios, donde individuos y empresas transaran eficazmente y todo fluyera a través de la libre competencia, pero con el pasar de los años nos encontramos con que unas pocas empresas dominan el mercado, Google, Apple, Amazon, Facebook y Microsoft, se han transformado en un oligopolio contra el que es prácticamente imposible entrar a competir dada la cantidad de recursos que estas empresas tecnológicas poseen (El País, 2018), además de los ecosistemas integrados de aplicaciones que tienen cada una de ellas, siendo Internet cada día mas parecido a un espacio cerrado y centralizado.

Por otro lado los sistemas de aplicaciones a través de nodos, sistemas y servidores cerrados y unidireccionales, esto es un equipo informático que brinda servicio a otros equipos (Pandorafms, 2019) en donde toda persona que desee entrar a una página web debe conectarse desde de su dispositivo a un servidor central, como por ejemplo para conectarse a bancos, instituciones financieras, educacionales, e información etc, han dado lugar a errores informáticos por parte de estas organizaciones proveedoras del servicio en cuestión, por ejemplo hackeos, filtración de datos personales, filtraciones de tarjetas de crédito, pérdidas de información sensible, o derechamente estafas, algunas recordadas como la filtración de 41 mil tarjetas de crédito y 13 instituciones afectadas en 2018 (Emol, 2019).

Otra clase de problemas de confiar en una institución y servidor central es que toda la confianza recae en los controladores. Digamos que dejamos nuestros ahorros en manos de

terceros, esto ha llevado a apropiaciones indebidas, posibles robos, malas elecciones de inversión e incluso estafas piramidales en la industria financiera. Recordados casos como el de 182 mil millones de Pesos y más de 10 mil clientes afectados (Tele13, 2019), demandas e imputados varios por la justicia chilena con el destape del caso AC Inversions, a los que luego se sumarían otros similares como Arcano, Investing Capital, Rodríguez & Asociados y una serie de empresas más. Hechos varios que provocan una irremediable falta de confianza en el sector, siendo actualmente vender productos financieros, especialmente administrar capitales de terceros, considerado por muchas empresas del rubro como vender “arena en el desierto” debido a la poca credibilidad y desconfianza por parte de los clientes y consumidores (Capitaria, 2019).

Otros temas como los ahorros previsionales y la desconfianza de los trabajadores en como estos son invertidos, la gran movilización nacional que se ha producido en los últimos años por parte una parte importante de la población con el movimiento de No + AFP, iniciativa popular en reclamo a las bajas pensiones acumuladas por las personas en Chile a lo largo de su vida (NomasAFP, 2019), y las comisiones cobradas por las AFPs correspondiente a un tramo entre el 10% y 15% aproximadamente por sobre el capital neto recaudado mensualmente de los trabajadores, también conocido como imposiciones obligatorias, porcentaje informado como “porcentaje de la remuneración o renta imponible” en promedio de 1,255% por la superintendencia de pensiones (superintendencia de pensiones, 2019).

Todos estos tipos de problemas observados por parte del consumidor en la industria que provee los bienes y servicios requeridos, y que podemos plantearlos como falta de confianza en la contraparte, además los encontramos en contratos de trabajo, compra venta y arriendos inmobiliarios, derechos de autor, industria agrícola y un largo etc. En otras palabras donde quiera que exista un acto mercantil entre partes desconocidas, existe la falta de confianza inherente dado los diferentes niveles de reputación de los individuos e instituciones. Así todas las industrias a día de hoy tienen en común que requieren la intervención humana, la cual provoca fraudes, ambición, conflictos de interés, luchas de ego, y más importante aún,

derechamente robos y estafas, afectando la confianza de los consumidores como las anteriormente vistas.

Acá nos encontramos con una posible solución, la tecnología de cadena de bloques (en adelante también llamada blockchain), una tecnología capaz de descentralizar aplicaciones y hacer la internet democrática, sin que las aplicaciones dependan de un organismo o servidor central, sino que cada uno de los usuarios es participante tanto como parte usuario como parte controladora, a través de donde este conectado, ya sea un ordenador, tablet, smartphone etc.

Blockchain tiene la capacidad de bajar al mínimo las comisiones transaccionales, eliminar todo tipo de intermediarios, además de brindar seguridad a las inversiones y ahorros de las personas. Lo mismo corre para contratos de trabajo, de arriendo, inmobiliarios, contratos industriales etc., los cuales deben ser fidedignos, confiables y supervisados.

Este trabajo abordará y dará una descripción detallada de cómo se pueden minimizar las altas comisiones monetarias, costos burocráticos y además qué industrias de servicios podrían ser transformadas, en distintos sectores del país, aumentando la transparencia, productividad, bajando los costos, reduciendo las tasas de espera, como por ejemplo en: altas tasas de interés financiero para la población, burocracia de contratos, de notarios públicos, de conservadores de bienes raíces, industrias con muchos intermediarios, acceso al crédito, corredores de propiedades, seguridad general etc. Además mediremos cuantitativamente cuál es el nivel de conocimiento de la población respecto a tecnologías de cadena de bloques y sus aplicaciones derivadas, como contratos inteligentes, criptomonedas, etc, a fin de hacer un diagnóstico de qué tan preparados están los profesionales del país respecto a las tecnologías que se empiezan a usar con mayor fuerza en el planeta.

En general se referirá a los sectores de bienes y servicios que podrían quedar obsoletos en el futuro bajo el supuesto de implementar tecnología blockchain y contratos inteligentes, y como los costos de estas industrias podrían en teoría ser prácticamente cero, con nula burocracia, sin comisiones de por medio y con total autonomía desde el instante inicial.

2 OBJETIVOS

2.1 Objetivo General

Explorar nivel de familiarización de la población respecto a tecnología de cadenas de bloques y describir sus utilización en industrias y países, a través de una investigación exploratoria con información disponible y recopilada, para reseñar industrias que podrían ser transformadas o creadas a nivel país.

.

2.2 Objetivos Específicos

1. Describir el nivel de conocimiento del segmento universitario y profesional de la población Chilena respecto al blockchain, a través de encuestas, para reseñar el nivel educativo de las personas respecto a esta tecnología en su posible implementación .
2. Explorar y describir el interés y atracción de la población encuestada, en tecnología blockchain y criptomonedas a través de la encuesta, para señalar posibles nuevas áreas de interés en este mercado en la actualidad.
3. Analizar percepciones actuales del sector industrial de aseguradoras y sector gubernamental en Chile, a través de encuestas y bibliografía, para describir cómo se benefician estos sectores con tecnología de cadenas de bloques.

3 Marco Teórico

3.1 Algunos antecedentes

3.1.1 Bitcoin

Hace 10 años atrás, año 2009 nace el proyecto llamado bitcoin, una moneda o activo digital que usa décadas de estudios referentes a criptografía y se sustenta en la tecnología de blockchain o cadena de bloques, difícilmente falsificable y semejante a un gran libro contable, público y distribuido en el que queda reflejado el histórico de todas las transacciones (Investopedia, 2019).

Siendo la cadena de bloques, una estructura de datos en la que la información contenida se agrupa en conjuntos o bloques, a los que se les añade informaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en entorno distribuido de manera que la estructura de datos *blockchain* puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información (Economist, 2011).

Además, el bitcoin se caracteriza por ser descentralizado, es decir, no estar respaldado por ningún gobierno o entidad centralizada, como un banco central por ejemplo. Y utiliza un sistema de prueba de trabajo para impedir el doble gasto, esto es, que la moneda sea utilizada varias veces. A modo de ejemplo en un acto de mala fe, un usuario trata de enviar bitcoins a 2 direcciones destinatarias (billeteras) distintas con el fin de gastar la misma moneda 2 veces (Queesbitcoin, 2016), esto sería impedido por la prueba de trabajo que imposibilita esta práctica.

Bitcoin está concebida desde sus orígenes como una moneda digital, que permite realizar transacciones entre usuarios de nivel global a mínimos costos, por ejemplo la comisión de una transacción de envío de dinero, o de compra venta a través de bitcoin puede costar tan sólo 0,5 USD (bitcoinfees, 2019), a diferencia del 1,49% + IVA, valor máximo que cobra transbank por utilizar su servicio de compras con tarjeta de débito bancarias a la mayoría de PYMES del país (Transbank, 2019).

3.1.2 ETHEREUM

Por otro lado, Ethereum, organización fundada el año 2014, pretende ser una plataforma de desarrollo en sí misma, ésta representa una plataforma descentralizada que corre contratos inteligentes, los cuales son descritos como aplicaciones que funcionan y corren bajo un entorno computacional exactamente como fueron programadas, sin ninguna posibilidad de fraude, censura, o interferencia de terceras partes. Además Ethereum posee su propia criptomoneda en sí llamada Ether, la cual funciona como un Token, similar a un combustible, para recompensar a las partes que firman un contrato inteligente (Bitcoinist, 2019).

Ethereum fue concebida inicialmente por Vitalik Buterin, durante el año 2013, el cual definió a Ethereum como una “combinación de una red descentralizada de minería digital y una plataforma de desarrollo de software”, que facilita la creación de nuevos sistemas criptomonetarios que comparten una sola cadena de bloques (un registro público criptográfico de transacciones). (Futurethinkers, 2015)

Ethereum siguió los pasos de la tecnología previamente utilizada por Bitcoin y mejoró considerablemente sus capacidades. Se trata de una red que posee navegador de Internet, sistema de pago y lenguaje codificado, permitiendo a los usuarios la creación de sus propias aplicaciones descentralizadas de Ethereum en Blockchain.

Además, Ethereum se rige bajo un código de programación abierto, esto es el software de código abierto que es producto de la colaboración de infinidad de personas, es compartido libremente, se publica de manera transparente y se desarrolla para ser una comunidad en lugar de ser propiedad o negocio de una sola compañía o ente (bitcoin.es, 2019).

3.1.3 ETHER

El Ether consiste en un token cuya cadena de bloques es generada bajo la plataforma de Ethereum, el Ether puede ser transferido entre cuentas y usado para compensar a los nodos mineros participantes para los cálculos realizados, además es un símbolo fundamental para el funcionamiento de Ethereum, que por lo tanto proporciona un libro mayor público distribuido para las transacciones. El Ether es una unidad de cómputo utilizada en transacciones y otras transiciones de estado, y por error entre el público muchas veces se confunde el Ether con la misma red Ethereum,, siendo que esta última es la plataforma bajo la que corre el Ether (Tapscott, 2016) .

Algunas diferencias con Bitcoin es que el número máximo de éstos se sitúa en 21 millones de unidades de Bitcoins, que será alcanzado en un determinado momento y que bajo complejos algoritmos basados en criptografía controlan la oferta disponible (Investopedia, 2019), mientras que el suministro de Ether podría ser infinito. En materia de minería, los bloques de Bitcoin duran aproximadamente 10 minutos en ser minados y Ethereum ha marcado como objetivo máximo unos 12 segundos. Esto se traduce en que Ethereum tendrá validaciones más veloces que las de Bitcoin. Ethereum es de momento, la segunda moneda criptográfica más grande del mundo detrás de Bitcoin, ha sufrido un crecimiento mayor y mucho más rápido que éste, y se está utilizando cada vez más en el planeta (myethereum, 2019)

3.2 El funcionamiento y las Matemáticas del Blockchain

El primer elemento del blockchain son los llamados bloques y luego el hash. Los bloques son ficheros, normalmente de texto que contienen la información que se requiera guardar, forman una cadena ya que cada bloque tiene información sobre el bloque anterior, éste a su vez sobre el bloque anterior y así sucesivamente hasta el primer bloque, de ahí yace su nombre de “blockchain” o lo que en castellano es “cadena de bloques”.

El hash es la información que cada bloque tiene sobre el bloque anterior y es un código o número de serie matemático, y que además posee toda la información encriptada.

El segundo elemento del blockchain es la red de ordenadores, todos los ordenadores de la red guardan una copia exacta de la cadena de bloques, lo que quiere decir que no existe un solo servidor u ordenador que guarde por si solo toda la información como sucede con los servidores de bases de datos tradicionales. En este sentido, todo aquel que funcione como un nodo, es decir personas que ocupan sus ordenadores, tablets o teléfonos inteligentes, tienen una copia exacta de la información, lo que hace imposible que esta se pierda y hacen de la blockchain una red descentralizada, lo cual hasta ahora ha marcado su gran éxito.

Veamos como ejemplo el funcionamiento del bitcoin, criptomoneda pionera que usa la cadena de bloques desde su comienzo. El software de bitcoin es la red de ordenadores, tablets, smartphones etc que tienen este propio software instalado y por lo tanto descentralizado. Además es software libre, de código abierto, y la cadena de ficheros de bitcoin contiene todas y cada una de las transacciones de bitcoin de la historia. Así por ejemplo, leyendo esta cadena de bloques se puede saber cuántos bitcoin tiene cada usuario y de dónde han salido. Y cada bloque o fichero de la cadena de bitcoin contiene el hash de su bloque anterior seguido de una lista de transacciones.

El tercer elemento del blockchain es la prueba de trabajo, es una incógnita (se denominará “X”) y los llamados mineros. Como la información de los bloques está encriptada y sólo el que la creó la puede ver, a través de criptografía de clave pública y clave privada (eso es lo que hace que la información sea segura y anónima) sería lógico preguntarse cómo se añaden bloques y cómo se hace para que todos los nodos de la red tengan una copia exactamente igual

a los de la otra. Aquí es donde entran unos nodos especiales de la red de bloques que son los mineros y la incógnita “X”.

Cada vez que surge un nuevo bloque para añadir a la cadena, por ejemplo nuevas transacciones con bitcoin que añadir al historial, los mineros reciben un aviso. Para añadir el bloque a la red hace falta que alguien calcule una variable “X” y la añada al bloque. El primer minero que lo consiga avisa a todo el resto de mineros, luego todos los demás mineros comprueban que la “X” calculada sea correcta, y el minero que consiguió calcular la incógnita “X” se lleva un premio. Hallar esta variable X es extremadamente difícil y esta tiene que ver con los hash (código, número de serie) de cada bloque.

Como se ha explicado, un hash es un código o número de serie matemático. Y una función de hacer hashes es una función matemática convertida en algoritmo que recibe un fichero de texto, letras, números, o caracteres en general y le asigna un número único, de tal forma que el número único depende del texto. Si cambiáramos cualquier carácter el resultado ya no sería el mismo, además la forma de asignar el número es extremadamente complicada, o sea que si hipotéticamente se nos entregara el número final es imposible saber el texto del que proviene, y esto es lo que hacen en el blockchain los mineros, buscan la variable “X” del problema.

Para resumir los puntos anteriores, surge un bloque nuevo que añadir a la cadena, o sea por ejemplo nuevas transacciones con bitcoins que añadir al historial etc. Luego, se debe buscar una variable X para unirla a la información del bloque y que en el hash (número de serie) aparezca un número que comienza por 30 ceros usando el algoritmo de generación de hash, SHA 256.

Calcular este número en la práctica es imposible, incluso si se conoce el algoritmo. La única forma es probando al azar billones de combinaciones posibles hasta que salga lo que se requiere, y esto es lo que hacen los mineros de bitcoin.

Lo de los 30 ceros se llama dificultad de la prueba de trabajo y el protocolo bitcoin lo va ajustando para que cada bloque se tarda en minar más o menos 10 minutos. El algoritmo SHA 256 es extremadamente seguro, imposible de revertir, y se usa desde verificación de paquetes Linux, protocolos de seguridad en internet, y hasta en tribunales internacionales.

Al minero que consigue minar ese bloque se le dan 12,5 bitcoins (al momento de escribir estas palabras) y esta recompensa se reduce a la mitad por cada 210 mil bloques que se minan en la red. Además como todos los mineros tienen el mismo bloque para añadir a la cadena, esto hace que nadie pueda falsificar un bloque, y que además cuando alguien consigue la “X” del algoritmo todos los demás mineros la comprueban y la mayoría tiene que estar de acuerdo en que es correcto, sino no se añade.

Imagine por un momento que alguien intenta falsificar un bloque y cambia tan solo un caracter del fichero, un número o una letra. Como todos los mineros están tratando con el mismo problema matemático la incógnita X del falsificador no será verificada por los demás mineros y no funcionará a nadie más, por lo tanto no se añadirá el bloque y el falsificador no obtendrá su recompensa.

Minar consiste en probar billones de combinaciones al azar, por lo que obviamente al tener más capacidad de cómputo aumentan las posibilidades de conseguir el número y la recompensa, esto ha dado pie para que en países como China, Venezuela o Islandia, donde la electricidad es subvencionada por el estado o poseen un clima helado muy favorable (para evitar el sobrecalentamiento de los ordenadores), se hayan instalado las llamadas granjas de minado, lugares de cientos de metros cuadrados industrializados con ordenadores tratando de descifrar los algoritmos las 24 horas del día y así obtener la recompensa.

Por último, se puede hacer la analogía de que la gran mayoría de criptomonedas y aplicaciones funcionando bajo blockchain poseen una lógica y forma de funcionar similar a la descrita anteriormente.

Para concluir este punto 3.2, quisiera agradecer a don Eduardo Sáenz de Cabezón, Doctor en Matemáticas de la Universidad de la Rioja, España, por ser el autor intelectual de gran parte de las ideas en que se basó este capítulo.

3.3 Los contratos inteligentes

La mejor analogía para definir un contrato inteligente es pensar en un clásico contrato de toda la vida, por ejemplo de arrendamiento, inmobiliario, de trabajo, de prestación de servicio etc, y llevarlo al ámbito digital. La diferencia es que acá el contrato debe ser codificado y programado por una persona que se maneje en lenguaje de programación y contará con ciertas reglas y algoritmos donde se liberan los pagos involucrados automáticamente a medida que las condiciones del contrato se van cumpliendo.

Por ejemplo imagine un contrato de trabajo, donde el empleador y empleado firman un clásico contrato de trabajo, la diferencia es que acá utilizan la tecnología de contrato inteligente y lo codifican. En este caso el contrato inteligente liberará los pagos desde la cuenta del empleador al empleado en el día pactado, pagará las imposiciones correspondientes y realizará otros trámites, y si no existe dinero disponible en la cuenta del empleador el día correspondiente, puede dar aviso automáticamente a la inspección del trabajo, e incluso iniciar un juicio en caso de ser necesario, bajo la internet de las cosas (IoT), tecnología posiblemente ya totalmente desarrollada durante la próxima década bajo el umbral 5G, velocidades inalámbricas de internet prácticamente instantáneas y que precisamente este año 2019 hará su debut en EEUU (Verizon, 2018).

Para nombrar otros ejemplos prácticos de los contratos inteligentes y la desburocratización de actividades en potencia que poseen podemos imaginar el reemplazo de corredores de bolsa, de propiedades, notarios públicos, conservadores de bienes raíces, corredores de apuestas, etc. Actividades que pueden ser codificadas secuencialmente y que ayudarían a reducir enormes costos y sobre todo tiempo. Muchos servicios que hoy en día funcionan de forma manual, teniendo el potencial para poder funcionar de forma automática.

3.4 La máquina virtual de Ethereum (EVM)

La Máquina Virtual de Ethereum (o EVM, Ethereum Virtual Machine) es considerada la principal creación de Ethereum. Se trata de un software completo de Turing con el que se puede resolver casi cualquier problema computacional y que es ejecutado dentro de la misma red de Ethereum. Su diseño tiene como principal objetivo poner en marcha códigos algorítmicos complejos y facilitar el proceso de creación de aplicaciones a través de lenguajes de programación mucho más amigables, como es el caso de JavaScript, evitando la construcción de una cadena de bloques completamente nueva para cada una de las aplicaciones. Ethereum permite que cada una de las aplicaciones se desarrollen dentro de una misma plataforma.

A su vez, Ethereum Virtual Machine se encuentra separada del resto de la red, lo que permite que cualquier persona o empresa pueda aprender a crear un contrato inteligente más grande y con mayor fuerza usando la EVM, sin necesidad de afectar a otras transacciones que tengan lugar en la cadena de bloques (Libertex, 2019).

La máquina virtual Ethereum se enfoca en brindar seguridad y ejecutar código no confiable en computadoras de todo el mundo. Para ser más específico, este proyecto se enfoca en prevenir los ataques de denegación de servicio, que se han vuelto comunes en el mundo de las criptomonedas. Además, EVM garantiza que los programas no tengan acceso al estado del otro, lo que garantiza que la comunicación se puede establecer sin ninguna interferencia potencial.

Para poner esto en un lenguaje que todos puedan entender, Ethereum Virtual Machine está diseñada para servir como un entorno de ejecución para contratos inteligentes basados en Ethereum.

Dado que la Máquina Virtual Ethereum está completamente aislada del resto de la red principal, es un entorno de prueba perfecto, cualquier empresa que busque crear un contrato inteligente puede hacerlo utilizando la EVM, sin que esto afecte las operaciones principales de la cadena de bloques. La prueba de esta tecnología es de suma importancia, ya que un código defectuoso puede significar la desaparición de incluso los contratos inteligentes más grandes. Además, se podría considerar al EVM como un "entorno de aprendizaje" para construir contratos inteligentes más grandes, mejores y más robustos.

También vale la pena mencionar que cada nodo Ethereum en la red ejecuta su propia implementación de EVM y es capaz de ejecutar las mismas instrucciones, además es una puerta de entrada para construir contratos inteligentes adecuados, tanto para los principiantes como para los programadores experimentados que buscan obtener un enfoque práctico con Solidity, un lenguaje de alto nivel orientado a objetos para implementar contratos inteligentes (Solidity, 2019). Además, el EVM se ha implementado en lenguajes de programación más tradicionales, tales como Python, Ruby, C ++ y algunos otros lenguajes de codificación. (Themerkle, 2019)

3.5 Oráculo

Suenan como algo de la mitología griega y de alguna manera funcionan de forma similar, cuenta la leyenda que en el mundo antiguo las personas no tenían suficiente información para tomar decisiones y recurrieron a oráculos para indagar más allá de los límites de su propia comprensión.

De la misma manera, las cadenas de bloques como las de Bitcoin y Ethereum, no tienen acceso fácil a la información fuera de la cadena, por lo que no existe una forma directa de validar las condiciones en que se basan los contratos inteligentes. Un oráculo es, simplemente, un traductor para la información proporcionada por una plataforma externa. Los oráculos dentro del blockchain son fuentes de información externas y que permiten a los contratos inteligentes ejecutar órdenes con información imparcial, pública y no manipulada.

Los oráculos proporcionan los datos necesarios para que se ejecuten contratos inteligentes cuando se cumplan los términos originales del contrato. Estas condiciones podrían ser cualquier cosa asociada con el contrato inteligente: temperatura, finalización del pago, cambios de precio, etc. Estos oráculos son la única forma de que los contratos inteligentes interactúen con datos fuera del entorno de Blockchain. (Cointelegraph, 2019).

Es importante entender que los contratos inteligentes no pueden funcionar sin una fuente externa de datos fiable, si esto no pasara perderían su potencial enormemente.

3.6 Raiden Network (RDN)

Raiden network es una red para transacciones instantáneas, opera bajo la plataforma de Ethereum y es análoga a Lightning Network de bitcoin, siendo ésta un protocolo en capas de la parte superior de la cadena de bloques de bitcoin (Bitcoinlightning, 2019) que permite transacciones rápidas entre nodos participantes y se ha promocionado como una solución al problema de escalabilidad del bitcoin.

Cuenta con un sistema de igual a igual para realizar micro pagos de criptomoneda a través de una red de canales de pago bidireccionales sin delegar la custodia de los fondos. La implementación de Lightning Network también simplifica los intercambios inmediatos (Poon, 2016). De igual manera Raiden Network permite la transferencia segura de tokens (Ether) entre los participantes sin la necesidad de un consenso global. Esto se logra mediante transferencias firmadas digitalmente y con bloqueo hash, también llamadas pruebas de saldo, totalmente garantizadas por depósitos en la cadena previamente configurados. Este concepto, se conoce como tecnología de canal de pago. Los canales de pago permiten transferencias bidireccionales prácticamente ilimitadas entre dos participantes, siempre que la suma neta de sus transferencias no exceda los tokens depositados. Estas transferencias se pueden realizar de forma instantánea y sin ninguna participación de la propia cadena de bloques real, excepto por una creación inicial única en la cadena y un eventual cierre del canal (Raiden, 2019).

Las limitaciones de Ethereum y otras cadenas de bloques han sido un tema de discusión dentro de la comunidad de desarrolladores por un tiempo. Como cualquier otra cadena de bloques, Ethereum tiene la intención de dar soporte a tantos usuarios como sea posible. En la actualidad, Ethereum puede soportar sólo 13 transacciones por segundo. Para dar una perspectiva de las cosas, Visa procesa un promedio de 4,000 transacciones por segundo, mientras que Facebook maneja alrededor de 170,000 solicitudes por segundo. Esto demuestra que la adopción generalizada de Ethereum todavía está lejos. Sin embargo es por esto que la red Raiden es una solución de escalamiento fuera de la cadena para realizar transferencias de token compatibles con la cadena de bloques Ethereum, y el símil es que permitirá pagos casi instantáneos, de bajo costo, escalables y que preservan la privacidad (Quora, 2019).

4. Metodología

Con la aparición de internet masivamente en el planeta, a mediados de los años 90s, el mundo vive una verdadera revolución en cuanto a la obtención de información. Acceso prácticamente inmediato a cualquier fuente, trabajo, dato o resultado que se requiera obtener y conocer.

Entre toda la información actual en internet, alrededor de más de 10 Zettabytes, (1 Zettabyte=1.099.511.627.776 gigas, o 10^{21} bytes) (Xataka, 2016), disponibles de datos en la actualidad en la nube, también ha aparecido otro problema, el cual es la obtención de información de poca utilidad, fiabilidad y confiabilidad, problema conocido como “información basura” disponible a la que accedemos.

A fin de analizar ciertos problemas con mayor precisión sin manipular ningún tipo de variables, en esta memoria se usa una metodología de investigación exploratoria y descriptiva. Como su nombre lo indica, el objetivo de la investigación exploratoria es explorar o examinar un problema o situación para brindar conocimientos y comprensión.

Se funda en la descripción de fenómenos en cuestión para realizar análisis y los datos medidos se obtienen de la manera en que se presentan. Además la investigación es de tipo transversal puesto que en el diseño se obtienen los datos en un único momento en el tiempo.

La investigación exploratoria, por lo general va seguida en el futuro de mayor investigación exploratoria o una investigación concluyente y en este trabajo tiene por objetivos obtener las ideas para desarrollar un enfoque del problema y establecer prioridades para la investigación posterior.

La técnica de muestreo será no probabilísticos, de tipo “por conveniencia” para realizar encuestas y de tipo revisión bibliográfica para obtener y añadir información sobre los temas. La revisión bibliográfica es observacional, vale decir sin intervención del investigador y las soluciones y mejoras de sectores industriales y servicios donde se encuentre que sea aprovechable el uso tecnología de cadenas de bloques y contratos inteligentes.

4.1 La Encuesta

Para alcanzar los objetivos de este trabajo se realizará un muestreo no probabilístico, dado que a diferencia de un muestreo probabilístico, no requiere y tampoco se tiene el acceso a toda una lista completa de los individuos que forman parte de la población en estudio, definiendo a ésta como “todos los individuos de cualquier sexo que poseen al menos estudios universitarios de pregrado completos en Chile”.

Además el muestreo será por conveniencia puesto que la muestra seleccionada de la población se escogió por ser accesible para el investigador y no por un criterio estadístico, obteniendo como ventajas el ahorro en costos, en tiempo, y el poder identificar tendencias.

Para la primera parte de los objetivos se utilizará la técnica de encuesta cuyo procedimiento de obtener información se basa en el interrogatorio de los individuos, a quienes se les plantea una variedad de preguntas con respecto a su comportamiento, intenciones, actitudes, conocimiento, motivaciones, así como características demográficas y de su estilo de vida (Naresh, 2008).

Se ha definido la encuesta de tal manera que las preguntas 1 a 4 van dirigidas a definir si el encuestado posee el grado mínimo de conocimiento respecto al blockchain, criptomonedas y contratos inteligentes. Las preguntas 5, 6 y 7 van dirigidas a medir si el encuestado se encuentra interesado en estas tecnologías y si se encontraría dispuesto a invertir en ella. Las preguntas 8 a 12 se han hecho con el propósito de ver el nivel de conformidad actual del encuestado respecto a servicios estatales y de compañías de seguros que podrían verse beneficiados con tecnología blockchain. Por último las preguntas 13 y 14 se hacen con la intención de definir si el encuestado forma parte de la población estudiada y poder realizar una mayor segmentación respecto a las repuestas por diferencia de sexo y nivel educacional.

La muestra, seleccionada por conveniencia para generar el máximo de información, es pequeña y no representativa. Los datos primarios son de naturaleza cualitativa y se analizan de acuerdo con ello. Dadas esas características del proceso de investigación, los hallazgos de la investigación exploratoria de adoptar tecnología de cadenas de bloques en las industrias chilenas deberían considerarse como tentativas o como aportaciones que se deben seguir investigando en profundidad de ahí que se trate de un estudio sólo a nivel exploratorio.

4.1.1 Formato Encuesta

A continuación se deja la encuesta tipo utilizada para obtener la información:

APLICACIÓN DE CADENAS DE BLOQUES Y CONTRATOS INTELIGENTES

Contestar esta breve encuesta te tomará aproximadamente 3 minutos. Muchas gracias por tu tiempo

1- ¿Has escuchado o leído alguna vez acerca de las tecnologías de cadenas de bloques o blockchain?

- ☐ Sí
- ☐ No

2- ¿Has escuchado o leído alguna vez acerca del Bitcoin?

- ☐ SI
- ☐ No

3- ¿Has escuchado o leído acerca de los contratos inteligentes o smart contracts?

- ☐ Sí
- ☐ No

4- Además de la criptomoneda Bitcoin ¿conoces algunas otras criptomonedas que pudieses nombrar? ¿Cuántas?

- ☐ No conozco Bitcoin ni ninguna otra criptomoneda
- ☐ Sólo conozco Bitcoin
- ☐ Conozco Bitcoin y sólo una criptomoneda más
- ☐ Conozco Bitcoin y dos o más criptomonedas

5- En general el mercado e industria de las criptomonedas y/o blockchain te provocan:

- ☐ Interés
- ☐ Desconfianza
- ☐ Indiferencia
- ☐ Otros

6- Si quisieras hipotéticamente, comprar o vender bitcoins u otras criptomonedas, ¿sabes donde hacerlo?

- ☐ Sí, sé donde comprar o vender criptomonedas
- ☐ No, no sé donde comprar o vender criptomonedas

7- Teniendo en cuenta que algunas criptomonedas han multiplicado por 100 y hasta 10.000 veces su valor en los últimos años, mientras que otras han desaparecido. ¿Estarías dispuesto a invertir una pequeña parte de tus ahorros en un portafolio o cartera de criptomonedas?

- ☐ Sí, invertiría el 10% o más de mis ahorros
- ☐ Sí, invertiría un número entre el 1% y menos del 10% de mis ahorros
- ☐ No invertiría nada
- ☐ No lo sé

8- ¿Crees que tu dinero, ahorros y/o inversiones en bancos y otras instituciones financieras tradicionales se encuentran seguros y sin riesgo de fraudes? Pon una nota, donde 7 representa máxima seguridad y 1 la mínima seguridad.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ 6
- ☐ 7

9- ¿Has contratado alguna vez algún seguro a tu nombre?

- ☐ Sí
- ☐ No
- ☐ No lo sé

10- ¿Has estado en la situación de que te ha tocado activar o hacer uso de dicho seguro?

- ☐ Sí
- ☐ No
- ☐ No lo sé

11- Si ocupaste, activaste o hiciste uso del seguro alguna vez, consideras que este trámite fue:

- ☐ Nunca he contratado o activado un seguro

- ☐ Muy rápido y expedito
- ☐ Más bien rápido y expedito
- ☐ Más bien lento y engorroso
- ☐ Muy lento y engorroso
- ☐ No sabe/No contesta

12- En general, qué nivel de burocracia crees que existe en las instituciones del estado que usualmente interactúan con el público. Por ejemplo: Justicia y Poder Judicial, Impuestos Internos, Registro Civil, Juzgados de Policía Local etc

- ☐ Mucha burocracia
- ☐ Más bien algo de burocracia
- ☐ Poca burocracia
- ☐ Nada de burocracia
- ☐ No sabe/No contesta

13- Cuéntanos un poco sobre ti. Tu máximo nivel educacional es:

- ☐ Postgrado (completo o en curso)
- ☐ Universitario Completo
- ☐ Universitario Incompleto
- ☐ Educación media completa o equivalente, o un grado inferior a esta

14- Cuéntanos tu género

- ☐ Hombre
- ☐ Mujer
- ☐ Me identifico con otro género

4.1.2 Beneficios y problemas de aplicar la encuesta

Debido a que se puede obtener una gran variedad de datos, los proporcionados por las encuestas tienen diversos usos. Se pueden utilizar para segmentar mercados, como sucede con los datos psicográficos y del estilo de vida, y para establecer perfiles de consumidores, determinar la imagen, la medida y el posicionamiento del producto, y para conducir análisis de la percepción de precios.

Las encuestas son el medio más flexible para obtener datos de las personas, para obtener información sobre los motivos, las actitudes y las preferencias de los consumidores.

Si se analizan adecuadamente, los datos de una encuesta pueden manipularse de varias maneras para que el investigador observe diferencias dentro de un grupo, examine los efectos de variables independientes como la edad o el ingreso, o incluso predecir el comportamiento futuro. (Naresh, 2007)

Por otro lado desde el punto de vista de los problemas, el mayor desafío que presenta el muestreo no probabilístico es la recreación del mismo tipo de resultados sin sesgo que brinda el muestreo probabilístico. Así teniendo en cuenta que al aplicar el muestreo no probabilístico por conveniencia a través de la encuesta se pueden presentar estos sesgos debido a la naturaleza de la misma muestra, los participantes podrían contestar más de una vez, negar características poco atractivas y solo responder características socialmente aceptadas, dar respuestas extremas dentro de escalas numéricas, existe brecha entre lo que las personas dicen y realmente hacen, etc.

Si bien estamos trabajando con una investigación exploratoria, de todas formas para evitar este tipo de sesgos se ha realizado la encuesta desarrollando las preguntas a través de una lógica secuencial, con un cuestionario prediseñado, con control de duplicados, predefiniendo las características de la población encuestada para ajustarla con la población objetivo, y se ha

desarrollado una encuesta breve para evitar la fatiga de respuesta dejando claro al encuestado el tiempo que le llevará responder desde un principio.

5. Resultados

5.1 Población y Blockchain

Para explorar el nivel de familiarización de la población universitaria estudiada, se han dirigido cuatro preguntas en la encuesta que apuntan a conocer nivel cultural de los profesionales en Chile respecto a las tecnologías de cadenas de bloques, criptomonedas y contratos inteligentes.

No se sabe, ya que hasta día de hoy es imposible conocer el futuro, si la tecnología de cadenas de bloques se acabará imponiendo, sin embargo existe cierto consenso entre los autores y profesionales del sector informático de que si estamos ante un avance que podría ser potencialmente revolucionario y tiene la capacidad de ser disruptivo dentro de la próxima década, además de cambiar de forma radical y automatizar muchos procesos que hacemos hoy en día de forma manual o de los cuales requerimos la presencia humana.

Al aproximarse a los resultados, se encuentra que del total de encuestados un 47% nunca ha escuchado o leído acerca de la tecnología de cadenas de bloques o blockchain y un 70% afirma que tampoco sabe ni ha escuchado nombrar lo que es un contrato inteligente. A pesar de esto todos los encuestados (100%) sí habían escuchado o leído alguna vez acerca del Bitcoin, criptomoneda más famosa. Sin embargo tan solo el 27% podía nombrar al menos 3 criptomonedas de las 4.836 listadas a día de hoy en Coinmarketcap.com (sitio web líder en cuanto a información de capitalizaciones de criptomonedas), mientras que el 54% de los encuestados sólo conocía bitcoin.

A pesar de no ser un estudio concluyente pero si exploratorio y de indagación, podemos corroborar algunos problemas citados por la comunidad de blockchain y criptomonedas en general como resultado de la encuesta. Uno de los principales problemas del blockchain y criptomonedas es que gran parte de la población estudiada, correspondiente a personas profesionales con estudios universitarios completos y que son potenciales usuarios y/o clientes, no sabe ni conoce lo que es esta tecnología, lo cual es uno de los principales problemas para su escalabilidad y masificación actual, corroborando lo que dicen algunas encuestas en distintas partes del mundo. Por ejemplo en España tras realizar una encuesta a más de 200 jefes de Recursos Humanos de

distintas empresas, el 63% de los directores desconocía totalmente el concepto de la blockchain (Cryptoguía, 2019). Otro estudio muestra que un 68% de las empresas de la región Asia-Pacífico no tienen conocimiento de blockchain y en términos de los grandes obstáculos para la adopción de la tecnología en ésta región, la falta de entendimiento respecto a blockchain debería ser una de los más significativos (Tokenpost, 2019). Otra encuesta publicada el 2017 en el Reino Unido mostraba que el 40% de los clientes del banco HSBC había escuchado sobre blockchain, pero apenas un 20% de éstos (8% del total de encuestados), podían explicar con palabras de lo que se trataba (Coindesk, 2017)

Una solución a este problema de escalabilidad puede ser crear organizaciones destinadas al marketing y difusión del universo blockchain y criptomonedas. La capitalización total de criptomonedas este año 2019 ha fluctuado entre los 180 mil y 350 mil millones de USD, y la capitalización de Bitcoin y Ethereum es de unos aproximados 148 mil y 19 mil millones de USD respectivamente, a noviembre 2019 y dejando en claro que estos montos son extremadamente volátiles. A modo de referencia y siempre teniendo en cuenta que se trata de criptomonedas distribuidas entre millones de individuos, bitcoin cuenta con la misma capitalización de McDonald's a día de hoy, pero aún muy lejos de Apple, Microsoft, Google y Amazon que se acercan al trillón (un millón de millones) de USD.

Con contratos inteligentes y blockchain las posibilidades son tan amplias como se tenga imaginación y de que se trate de proyectos que sean rentables (aunque esto último no sea un requerimiento en sí mismo). Por ejemplo una empresa dedicada exclusivamente a promocionar bitcoin y/o Ethereum financiada a través de un porcentaje fijo o flexible de la minería podría solucionar el problema de la llegada al público masivo, esto llevaría el aliciente de que los mineros verían sacrificada una pequeña parte de su ingreso en pos de una mayor masificación de bitcoin, Ethereum (u otra criptomoneda) y por consiguiente un aumento de la demanda que conlleva a un mayor valor de mercado de ésta. El hecho de que esta organización pudiese existir en teoría y que fuera confiable se podría regular asimismo bajo un contrato inteligente, en

donde todos los movimientos, ingresos, egresos, gastos, sueldos, balance, estados de resultados etc quedarían automáticamente controlados y supervisados, siendo detectado cualquier tipo de fraude, robo o desvío de fondos por el contrato inteligente y que es justamente en teoría lo revolucionario que este mismo promete.

5.2 Áreas de Interés y Posibles Desarrollos

Se observa en los resultados preliminares que sí existe un segmento importante de los profesionales universitarios del país, y por tanto personas con mayores ingresos a la media de la población, que están interesados en la tecnología de cadenas de bloque.

Si bien un 53% de los encuestados se decanta por la opción de “desconfianza” al ser preguntado sobre cuál es el sentimiento que le provoca la industria del blockchain y/o criptomonedas, muy probablemente relacionada con la poca difusión actual en nuestro país de la tecnología en cuestión, por el contrario existe un 27% encuestado que declara sentirse interesado en ella y un 17% adicional con una dubitativa indiferencia.

Además, un 30% del universo encuestado dijo que estaría dispuesto a invertir una parte de sus ahorros en una cartera de criptomonedas y un 33% adicional a este, dijo que no lo sabía con seguridad, pero sólo un 16% sabía donde comprar o vender criptomonedas o invertir en proyectos que tuvieran que ver con blockchain.

Como conclusión, se observa que hay un mercado potencial que presenta interesantes oportunidades de negocio a futuro, en donde existe una demanda por parte de un segmento de la población que no está cubierta por la oferta existente actual en nuestro país, tanto de brokers financieros como de educación respecto a blockchain, debido fundamentalmente a la etapa del ciclo de vida en que se encuentra esta tecnología, que a pesar de haber hecho su debut más

importante con el bitcoin el año 2009 aún se encuentra entre las etapas de introducción y crecimiento.

5.3 Sector Seguros

Se ha analizado el sector de seguros ya que presenta un amplísimo potencial de estar en el top 5 de las industrias que pueden ser transformadas y beneficiadas con blockchain.

Respecto al sector de empresas aseguradoras, explorando algunos de los datos preliminares obtenidos, el 77% de los encuestados ha contratado por lo menos algún seguro a su nombre. El 50% del universo encuestado declaraba haber activado alguna vez un seguro y la mitad de estos dijeron que el proceso les había parecido más bien lento y engorroso, mientras la otra mitad les había parecido más bien un proceso rápido. No podemos concluir, pero sí inferir que a pesar de que un número importante de individuos que se encuentran contentos con la gestión durante la activación de un seguro, aún hay mucho margen de mejora y aquí blockchain con sus automatismos es donde tiene la capacidad de jugar un rol importante.

No es un misterio que la industria de seguros es altamente lucrativa, en Chile presenta una rentabilidad sobre patrimonio (ROE) de 8,1% en promedio (SVS, 2019) y además de las 7 compañías existentes de AFPs en Chile, 5 de ellas son propiedad de compañías de seguros, así como Metlife es controladora de AFP Provida, Sura lo es de Capital, Assicurazioni Generali de PlanVital, Principal Financial de Cuprum, y Prudential Financial de Hábitat.

Con estos datos tan solo empíricamente se puede hacer una idea del capital y dinero que las industrias de seguros controlan y poseen, y sin embargo a pesar de manejar

estos capitales de varios billones de dólares, es una industria que no ha variado mucho su forma de operar en las últimas décadas.

Una alternativa interesante a esta situación son las llamadas Insurtech, startups completamente digitales y especializadas , que se espera en los próximos años se desarrollen, colaboren y compitan con el sector de seguros establecido. Estas startups utilizan la última tecnología, como el Big Data, el internet de las cosas o la inteligencia cognitiva, para diseñar productos y servicios adaptados a las necesidades del sector (Blockchain: La revolución industrial, 2017) en donde blockchain juega un papel primordial.

Un informe de PWC señala que el 90% de aseguradoras teme perder parte de su negocio a empresas tecnológicas, 3 de cada 4 predicen revoluciones en su industria en los próximos 5 años pero menos del 33% está explorando asociarse con empresas tecnológicas, y sólo un 14% tiene una activa participación invirtiendo y/o apoyando a incubadoras tecnológicas (PWC, 2016). Un 60 % de las Insurtech se localizan en EEUU y dadas las dificultades y la complejidad de administrar un negocio de seguros, la mayoría de las startups han decidido concentrarse en algunas partes de la cadena de valor y asociarse con aseguradoras y reaseguradoras. Hay muchas excepciones a esto, pero a excepción de Zhong An, la Insurtech China valorada en 8,000 millones de USD, la mayoría de estas empresas son todavía jóvenes y su éxito es demasiado pronto para medir (Marsh, 2019).

5.4 Sector Gubernamental

Otro de los sectores que teóricamente presenta un mayor potencial para ser parte de la transformación al blockchain es el sector gubernamental y de instituciones del Estado.

Al momento de indagar en la población encuestada cuál era el nivel de burocracia percibido sobre instituciones del Estado, tales como Justicia y Poder Judicial, Impuestos Internos, Registro Civil, Juzgados de Policía Local etc, sí existió un amplio consenso casi unánime del 96% de declarar estas instituciones como más bien burocráticas o muy burócratas.

Se puede intuir y observar que hay una gran parte de la población que percibe a las instituciones del sector gubernamental como ampliamente mejorables y desburocratizables, con lo que se recomienda y sería interesante la evaluación de proyectos más profundos correspondientes en estas área utilizando blockchain.

A modo de propuestas se verá a continuación algunos casos que están ocurriendo actualmente en el planeta y podrían ser replicados en Chile utilizando la tecnología de cadenas de bloques:

5.4.1 Estonia

Uno de los casos más interesantes es sin duda el de Estonia, este pequeño país báltico emplea esta tecnología en sus registros fiscales y empresariales, y de ahí la ha extendido a los registros sanitarios electrónicos de sus ciudadanos para protegerlos (Fernández Hergueta, 2017). Estonia es un caso extremadamente llamativo y que ha sido elogiado como “el país más digitalizado del mundo” por Forbes, o incluso ha sido objeto de bromas por el mismo Barack Obama aduciendo que “debí llamar a los Estonios cuando tuve problemas con el lanzamiento web de nuestro programa de salud”, refiriéndose al Obamacare, durante 2014.

Actualmente en 2019, el 99% de los servicios públicos en Estonia están disponibles en formato digital excepto casamientos, divorcios y transacciones de bienes raíces.

Reportes indican que se ahorran más de 1400 años de tiempo de trabajo y un 2% del PIB al digitalizar servicios públicos.

También fue la primera nación en desplegar sistemas de producción bajo tecnología de cadenas de bloques en 2012. La tecnología elegida fue KSI blockchain, la misma del departamento de justicia de EE.UU. Los datos nunca salen del sistema, solo se envía el hash al servicio blockchain. Como no hay datos almacenados en la Blockchain, estos pueden escalar para proporcionar inmutabilidad a petabytes (10^{15} bytes) de datos cada segundo. La lección aprendida por Estonia es que la velocidad es esencial para una buena experiencia ciudadana.

Ser una sociedad digital significa estar expuesto a constantes ciberamenazas, hoy lleva siete meses en promedio descubrir violaciones de datos, con la cadena de bloques KSI de Estonia la tecnología puede detectar estas infracciones instantáneamente. Con importantes inversiones en infraestructura de ciberseguridad, Estonia ha desarrollado amplia experiencia en esta área, convirtiéndose en uno de los más reconocidos y valorados internacionales expertos en ciberseguridad (PWC, 2019).

5.4.2 Dubái

Este conocido Emirato y su capital homónima, uno de los 7 pertenecientes a Emiratos Árabes Unidos (EAU), que en el futuro próximo planea tener policías robóticos, taxis voladores, vehículos autónomos, e incluso ha determinado un Ministro especialmente a cargo de un departamento de inteligencia artificial, es otra que se ha propuesto grandes metas tecnológicas tales como “ser el primer gobierno en el mundo motorizado por Blockchain”.

Para 2020 el Emirato quiere que todas las aplicaciones para visas, pagos de facturas, renovaciones de licencias etc, documentos que representan sobre las 100 millones de unidades al año, sean realizadas digitalmente usando Blockchain, y con la adopción de ésta, la estrategia podría salvar 25.1 millones de horas hombre, o 1500 millones de USD al año (Forbes, 2018). Además para 2021, el conjunto total de EAU se propone registrar más del 50% de las transacciones gubernamentales utilizando la tecnología de cadenas de bloques (Tynmagazine, 2019).

La estrategia Blockchain en Dubái introducirá un sistema para permitir a los ciudadanos y socios crear nuevas empresas utilizando la tecnología. Bajo la nueva estrategia, Blockchain permitirá miles de oportunidades de negocios en el sector privado. Las industrias que se beneficiarán de la tecnología Blockchain incluyen: bienes raíces, tecnología financiera y banca, atención médica, transporte, planificación urbana, energía inteligente, comercio digital y turismo.

Por último la estrategia Blockchain de Dubái apunta hacia el liderazgo internacional. En línea con este pilar, abrirá su plataforma Blockchain a contrapartes globales para mejorar la seguridad y conveniencia de los viajeros internacionales al Emirato. Bajo la nueva estrategia, los viajeros internacionales se beneficiarán de una entrada más rápida con pasaporte pre aprobado y autorización de seguridad y visas; movilidad más fácil dentro de la ciudad debido a licencias de conducir aprobadas y alquiler de autos (Futureblockchainsummit, 2019).

5.4.3 Otros Países

Si bien los casos de Estonia y Dubái aparecen en el papel como los más interesantes en cuanto a utilización de tecnología de cadenas de bloques, también tenemos muchos otros proyectos destacables que se están llevando a cabo alrededor del mundo tanto en pleno desarrollo como recién empezando.

En Uganda el gobierno está trabajando con la startup de blockchain Mediconnect, para intentar seguir cada paso de la cadena de suministro de remedios y medicamentos, a modo de prevenir falsificaciones. El gobierno estima que en estos momentos mas del 10% de los medicamentos que llegan a la población actualmente son falsos.

En Zug, Suiza, ya se aceptan pago en criptomonedas para servicios públicos. Se han digitalizados las identificaciones de los ciudadanos usando blockchain, y

recientemente se han asociado a la Universidad de Lucerna para crear un sistema de votación digitalizado usando blockchain, el cual ya ha pasado sus primeras pruebas.

En Georgia, el gobierno ha experimentado con blockchain, en un proyecto de registro de propiedad, en donde un sello de estampado digital permite verificar y firmar documentos que contienen toda la información esencial de los ciudadanos, y pruebas de registros inmobiliarios. La importancia y enorme potencial de este proyecto radica en hacer de los registros de tierras y propiedades en general, disponibles para miles de millones de personas que en estos momentos son incapaces de registrar sus propiedades legalmente alrededor del planeta. De ahí que el proyecto no solo afecte a Georgia, sino que posea escalabilidad mundial (Computerworld, 2019).

En Singapur, el gobierno está trabajando en el denominado proyecto Ubin, proyecto colaborativo con la industria para explorar el uso de Blockchain y la Tecnología de libro mayor distribuido (DLT) para la compensación y liquidación de pagos y valores. El Proyecto Ubin es un proyecto de múltiples fases y varios años, con cada fase dirigida a resolver los desafíos apremiantes que enfrenta la industria financiera y el ecosistema blockchain. El proyecto se encuentra ahora en su quinta fase destinada a buscar la viabilidad comercial de pagos y transferencias basados en una red de blockchain y actualmente está siendo sometida a pruebas de la industria para determinar su capacidad de integrarse con aplicaciones comerciales basadas en esta tecnología (Mas.gov, 2019).

6 Conclusiones y Recomendaciones

Al contemplar los proyectos que se están desarrollando con tecnología de cadenas de bloques a través del mundo, no es difícil inferir que en el caso de nuestro país, éste

se encuentra evidentemente por detrás en cuanto a cultura, difusión y/o proyectos respecto a otras naciones, no existen mayores innovaciones en el ámbito gubernamental bajo esta tecnología ni tampoco en el mundo privado.

Aunque están existiendo algunos esfuerzos por educar a los profesionales, de hecho dos reconocidas universidades del ámbito nacional que siempre lideran los rankings internacionales, para el próximo año 2020 lanzarán las primeras versiones de sus diplomados en blockchain (curiosamente en sus mallas curriculares se puede observar todo lo que se ha tratado en esta memoria) y también hay esfuerzos de la ACTI (Asociación chilena de empresas de tecnologías de la información) por llevar conocimiento a la población, aún estamos lejos de otros países.

Si bien no sería justo compararnos con casos como el de Emiratos Árabes, que prácticamente nos triplica en ingreso (25.891USD contra 70.262USD al año 2018), si aparecen otros países con casos muy interesantes más cercanos a la realidad nacional aplicando tecnología blockchain.

El caso de Estonia sería un caso digno de ser estudiado y quizás imitado, el país cuenta con un PIB per cápita 30% más grande que el de Chile (a pesar que en la década de los 90' se encontraba muy por detrás), y una población de apenas 1.324.000 personas aproximadamente, algo por detrás de las poblaciones que se encuentran en la Región de Valparaíso o del Biobío, donde podrían realizarse mayores incubadoras experimentales en vías de llevar a cabo la transformación digital que nuestro país merece y todos los beneficios que ello conlleva.

Además se puede apreciar que a pesar de no existir en Chile aún una cultura en cuanto a cadenas de bloques y criptomonedas y sus aplicaciones, si existe una demanda por mayor conocimiento por parte de la población profesional, lo que brinda buenas posibilidades de negocios a futuro que merecen ser estudiadas y evaluadas con mayor detalle, de una tendencia llamada blockchain de la cual existe un consenso prácticamente unánime que tiene la capacidad de transformar nuestras vidas y el mundo que nos rodea.

7. Referencias

Emol (2019) emol.com

ElPais (2018) elpais.com

PandoraFMS (2019) pandorafms

Capitaria (2019). www.capitaria.com

Tele13 (2016). www.t13.cl/noticia/negocios/estafas-piramidales

No más AFP (2019). <http://www.nomasafp.cl/inicio/>

Superintendencia de pensiones (2019). www.spensiones.cl/apps/estcom/estcom.php

Steemit (2018). steemit.com

Ethereum (2019). www.ethereum.org

Investopedia (2019). <https://www.investopedia.com/terms/b/blockchain.asp>

Miethereum (2019). www.miethereum.com/ether/bitcoin-vs-ethereum

Economist (2011). <https://www.economist.com/babbage/2011/06/13/bits-and-bob>

Bitcoin.es (2019). <https://bitcoin.es/actualidad/codigo-abierto-criptos-y-blockchain/>

Queesbitcoin (2016). <https://www.queesbitcoin.info/el-doble-gasto-de-bitcoin-explicado/>

Bitcoinfees (2019). <https://bitcoinfees.net>

Transbank (2019). <https://www.transbank.cl/web/servicios-y-tarifas/comercios/tarifas-aceptacion-tarjetas-debito>

Bitcoinist (2019). <https://bitcoinist.com/bitcoin-vs-ethereum/>

Tapscott (2016); Tapscott, Alex (7 Mayo 2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.*

Investopedia (2019). <https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/>

Futurethinkers (2015). <https://futurethinkers.org/vitalik-buterin-ethereum-decentralized-future/>

Verizon (2018). <https://www.verizon.com/about/our-company/5g>

Libertex (2019). <https://libertex.com/es/blog/que-es-ethereum-y-como-funciona-guia-completa-para-principiantes>

Solidity (2019). <https://solidity.readthedocs.io/en/v0.5.6/>

Themerkle (2019). <https://themerkle.com/what-is-the-ethereum-virtual-machine>

Cointelegraph (2019). <https://cointelegraph.com/explained/blockchain-oracles-explained>

Bitcoinlightning (2019). <https://www.bitcoinlightning.com/what-is-bitcoin-lightning>

Poon (2016). <https://lightning.network/lightning-network-paper.pdf>

Raiden (2019). <https://raiden.network/101.html>

Quora (2019). <https://www.quora.com/Why-did-Ethereum-choose-Raiden-Network-and-not-lightning-network>

Xataka (2016). <https://www.xataka.com/tecnologiaz/en/sabemos-cuanto-ocupa-todo-el-contenido-que-hay-en-internet-en-este-momento>

Svs (2019), https://www.svs.cl/portal/estadisticas/606/articles-27372_recurso_1.pdf

PWC (2019) <https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf>

Scribbr (2019) <https://www.scribbr.es/category/revision-bibliografica/>

Cryptoguia (2019) <https://kryptoguia.com/tech/empresas-espanolas-no-conocen-blockchain/>

Tokenpost (2019) <https://tokenpost.com/70-of-Asia-Pacific-Companies-Lack-Blockchain-Education-2657>

Coindesk (2017) <https://www.coindesk.com/whats-blockchain-hsbc-survey-finds-59-consumers-dont-know>

Marsh (2019) <https://www.marsh.com/uy/es/insights/research/-que-es-insurtech-y-como-esta-impactando-el-modelo-de-negocio-as.html>

PWC (2016) <https://www.pwc.com/gx/en/financial-services/assets/fintech-insurance-report.pdf>

Forbes (2018) <https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#3774a562454b>

Futureblockchainsummit (2019) <https://www.futureblockchainsummit.com/smart-dubai-blockchain-strategy-2020>

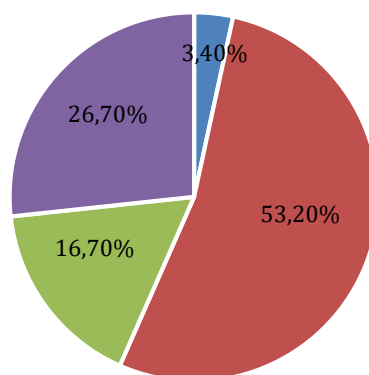
Tynmagazine (2019) <https://www.tynmagazine.com/smart-dubai-global-blockchain-challenge-eligio-a-sus-ganadores/>

Computerworld (2019) <https://www.computerworld.com/article/3412304/how-governments-around-the-world-are-using-blockchain.html#slide1>

Mas.gov (2019) <https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin>

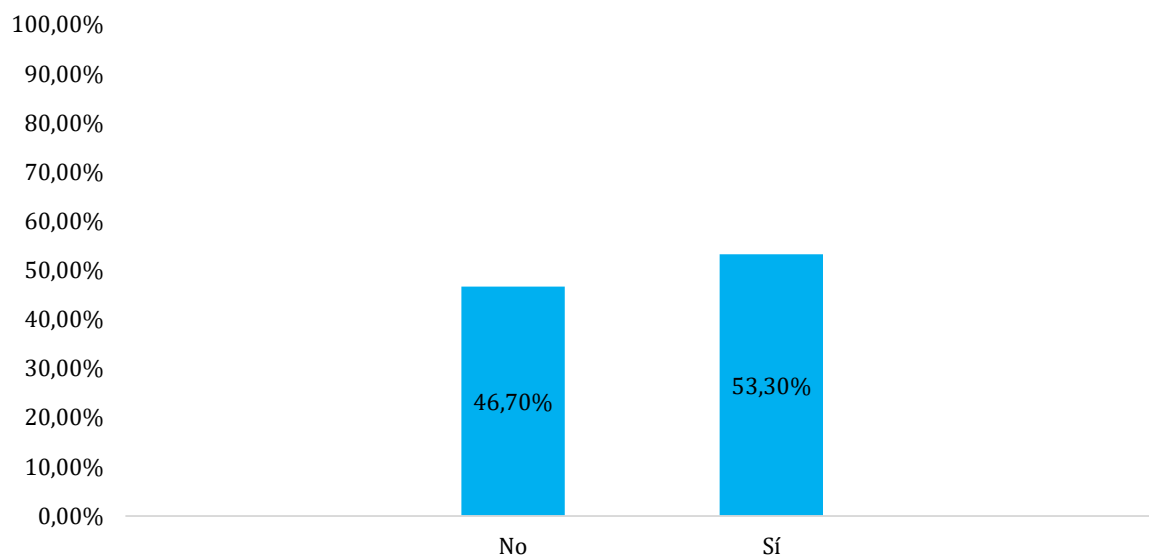
Pandasecurity (2017) <https://www.pandasecurity.com/spain/mediacenter/seguridad/blockchain-ciberserquidad/>

Además de la criptomoneda bitcoin, ¿conoces alguna otra criptomoneda que pudieses nombrar? ¿Cuántas?

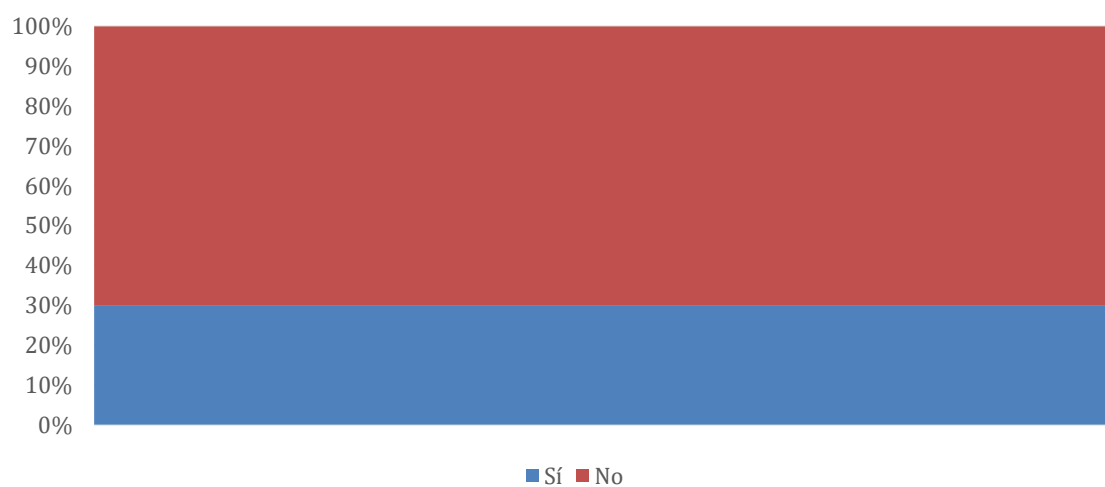


- No, no conozco bitcoin ni ninguna otra criptomoneda
- Sólo conozco bitcoin
- Conozco bitcoin y 1 criptomoneda más
- Conozco bitcoin y 2 o más criptomonedas

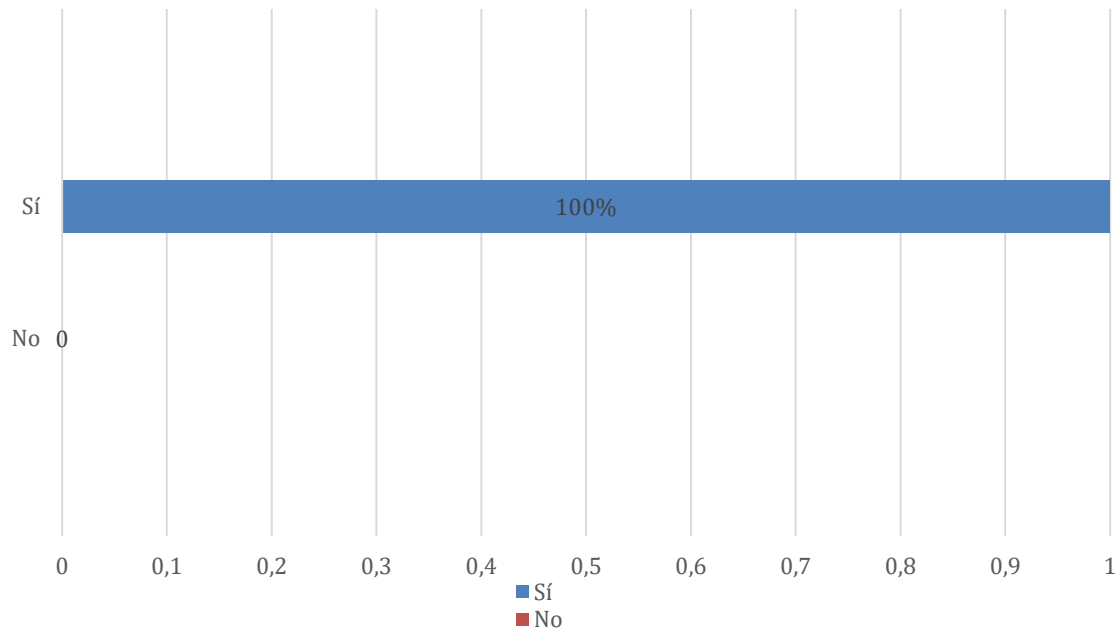
¿Has escuchado o leído alguna vez acerca de las tecnologías de cadenas de bloques o blockchain?



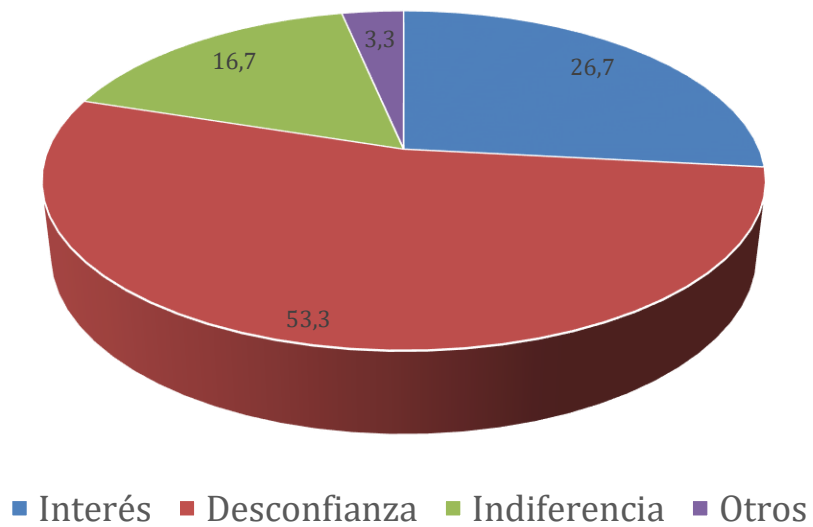
¿Has escuchado o leído acerca de los contratos inteligentes o smart contracts?



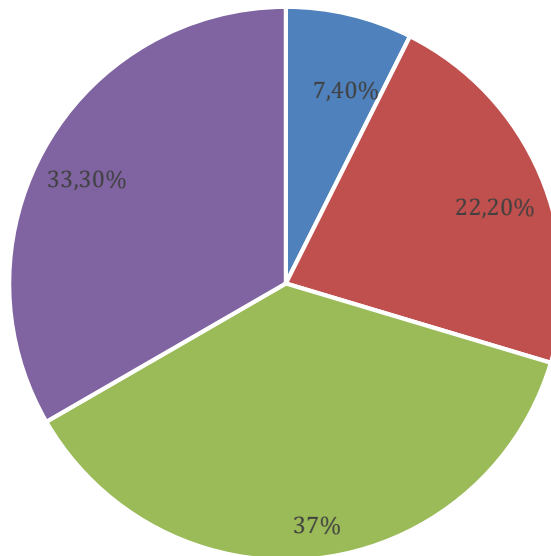
¿Has escuchado o leído alguna vez acerca del Bitcoin?.



En general el mercado e industria de las criptomonedas y/o blockchain te provocan:

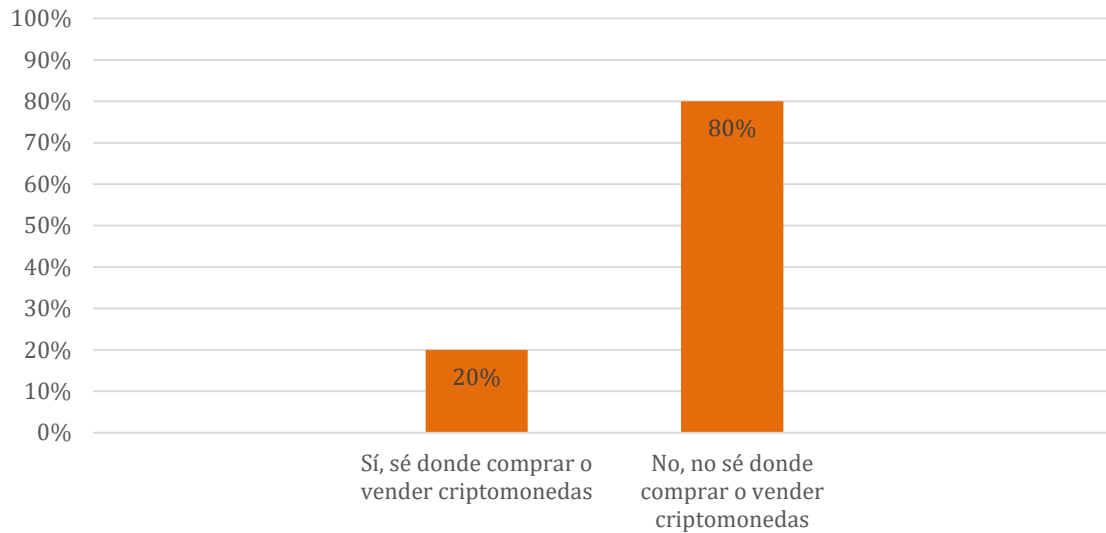


Teniendo en cuenta que algunas criptomonedas han multiplicado por 100 y hasta 10.000 veces su valor en los últimos años, mientras que otras han desaparecido. ¿Estarías dispuesto a invertir una pequeña parte de tus ahorros en un portafolio o cartera de cri

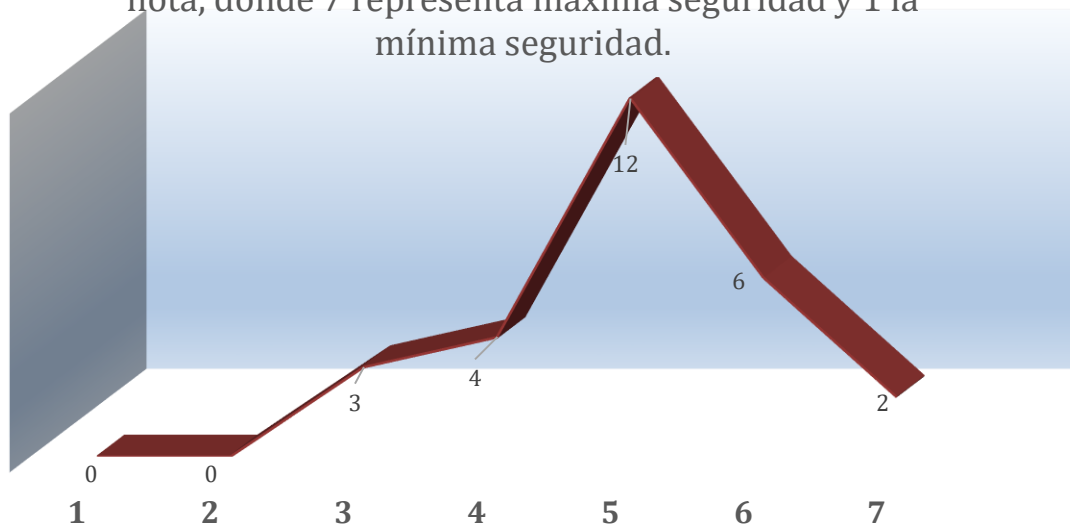


- Sí, invertiría el 10% o más de mis ahorros
- Sí, invertiría un número entre el 1% y menos del 10% de mis ahorros
- No invertiría nada
- No lo sé

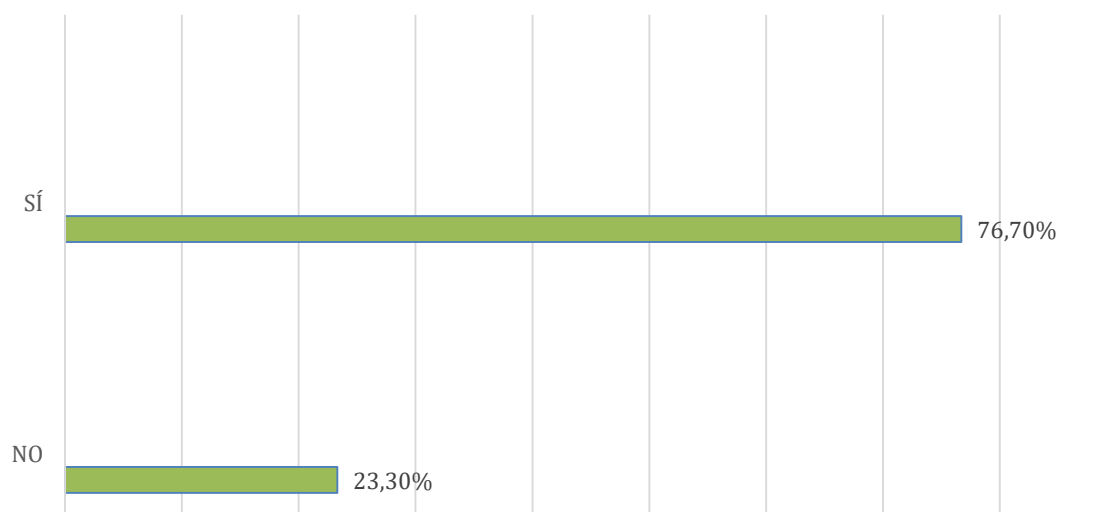
Si quisieras hipotéticamente, comprar o vender bitcoins u otras criptomonedas, ¿sabes donde hacerlo?



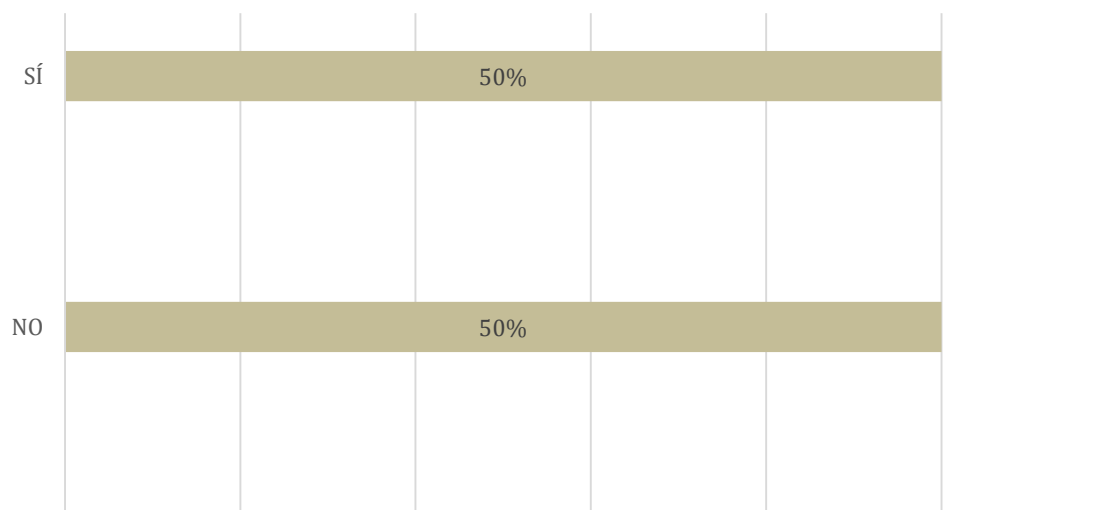
¿Crees que tu dinero, ahorros y/o inversiones en bancos y otras instituciones financieras tradicionales se encuentran seguros y sin riesgo de fraudes? Pon una nota, donde 7 representa máxima seguridad y 1 la mínima seguridad.



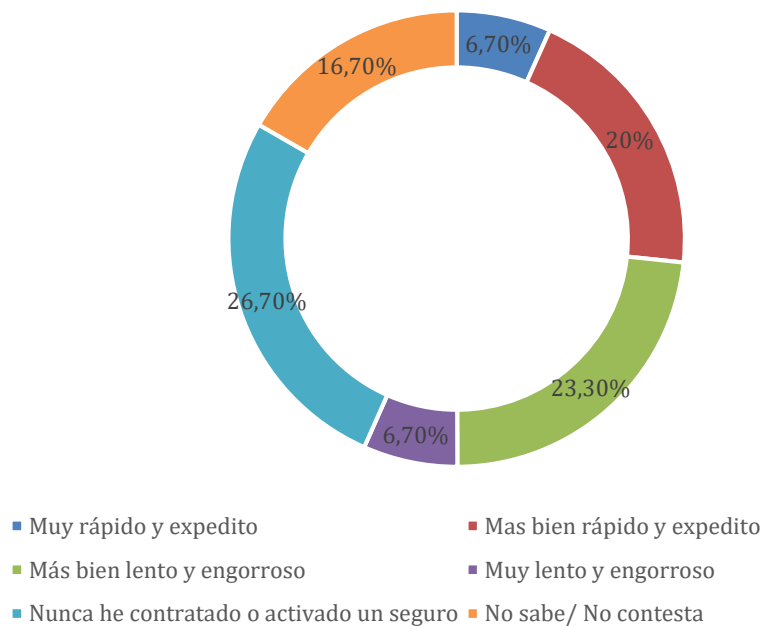
¿Has contratado alguna vez un seguro a tu nombre?



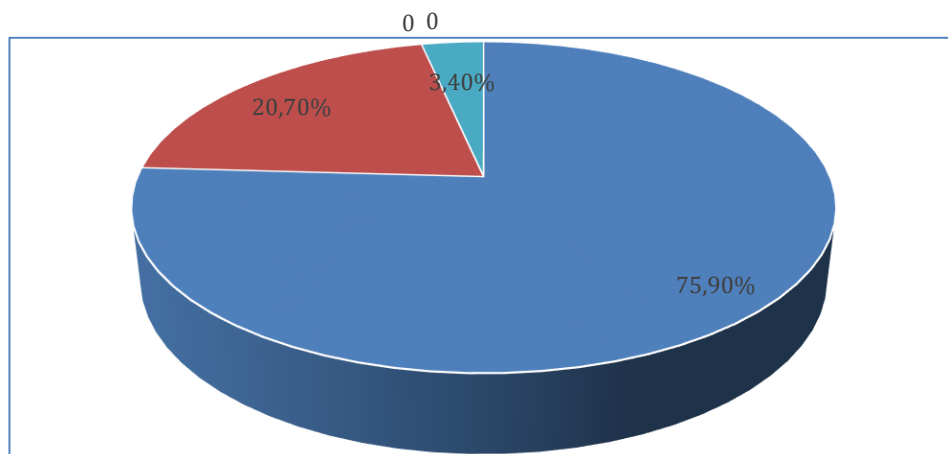
¿Has estado en la situación en la que has debido activar o hacer uso de dicho seguro?



Si ocupaste, activaste o hiciste uso del seguro alguna vez, consideras que este trámite fue:



En general, ¿qué nivel de burocracia crees que existe en las instituciones del estado que usualmente interactúan con el público. Por ejemplo: Justicia y Poder Judicial, Impuestos Internos, Registro Civil, Juzgados de Policía Local etc



- Mucha burocracia
- Más bien algo de burocracia
- Poca burocracia
- Nada de burocracia
- No sabe/No contesta

