SKRUMBLE NETWORK

# BLOCKCHAIN PARA COMUNICACION CENTRICA Y SEGURA

## INFORME TECNICO OFICIAL

**Borrador abierto para la comunidad. Sujeto a cambios.**
**Si hay alguna discrepancia, por favor refiérase a la versión en Ingles**

*“La libertad de expresión lo es todo, , es todo el juego. La libertad de expresión es la vida misma.”*

Salman Rushdie

# TABLA DE CONTENIDOS

RESUMEN EJECUTIVO ..... 4

INTRODUCCIÓN ..... 7

EL PROBLEMA ..... 8

SOLUCIÓN ..... 11

SKRUMBLE NETWORK ..... 13

COMPONENTE TÉCNICO ..... 15

TOKEN UTILITARIO DE SKM ..... 26

USOS DE SKRUMBLE NETWORK Y AÑADIDOS A LA RED ..... 29

CONCLUSIÓN ..... 32

SOBRE SKRUMBLE TECHNOLOGIES INC ..... 33

REFERENCIAS ..... 36

# RESUMEN EJECUTIVO

## BASE Y VISIÓN

## BLOCKCHAIN DE REDES SOCIALES ENTRE PARES (P2P) PARA CONTACTAR Y CONTRATAR

Cuando estudiamos cómo y por qué las personas se juntan, podemos examinar qué nos depara el futuro de la conectividad. Hemos comenzado a explorar el nuevo paradigma de las conexiones que se están formando de manera descentralizada, y nos hemos dado cuenta de que una nueva evolución es necesaria. La humanidad está madurando, y mostrando un gran interés en ir más allá de la actual comunicación centralizada. El nuevo terreno de juego se está construyendo para lograr una comunicación accesible que permita a los usuarios conectarse libremente entre sí. Esto significa comunicación sin límites, sin control por parte del gobierno, sin filtraciones de informacion, sin terciarios vendiendo datos, y todo completamente en manos de la comunidad y los usuarios.

Pasadas plataformas centralizadas como Facebook, WhatsApp, WeChat y Telegram han ayudado ha avanzar a la sociedad, y continúan ayudando a conectar personas. Sin embargo, una nueva forma de pensar y un enfoque más seguro, global y orientado a la comunidad, se exige como el próximo paso al crecimiento. Este informe tecnico oficial describe el fuerte ímpetu global de moverse más allá del paradigma tradicional de intercambio de información centralizada hacia uno orientado al intercambio de valor de forma descentralizada, propiedad de la comunidad, de esta nueva revolución Blockchain que estamos experimentando.

Los seres humanos tienen una necesidad inherente de conectarse entre sí de forma libre y segura. Es por ello que es necesario un nivel diferente de blockchain. Una optimizada para comunicaciones, empoderando aplicaciones necesarias para una plataforma de comunicacion. Cientos de aplicaciones y usos únicos se pueden construir sobre esta base, y verdaderamente expandir la misión de todo el ecosistema blockchain de nuevas e innovadoras formas.

## LA SOLUCIÓN DE LA RED SKRUMBLE NETWORK

Skrumble Network es una red de comuncacion basada en la tecnologia blockchain la cual es segura, que cuenta con una aplicacion de comunicacion decentralizada, y la opcion para programadores de agregar la capa de comunicacion a cualquier otra aplicacion que la necesite. Todo ello con un fuerte énfasis en la comunicación. Sin intermediarios o servidores centralizados que puedan censurar, bloquear o manipular los datos, la red Skrumble Network permite una comunicación abierta y privada, impenetrable, en la que tanto los datos como las transacciones son propiedad única y exclusiva de la comunidad y del individuo.

Además de construir una blockchain segura, Skrumble construirá la primera aplicación de comunicación completamente descentralizada, que se abrirá paso entre los cortafuegos de software tradicionales, permitiendo la gestión de la reputación a la vez que asegurando el anonimato al usuario, garantizando el contenido y la privacidad de los datos a través de herramientas tales como mensajería, llamadas, videos, compartición archivos, y muchas más. La red blockchain y la aplicación descentralizada de Skrumble Network también creará oportunidades para que la gente pueda añadir elementos de comunicación descentralizada en cualquier ecosistema o plataforma.

Por el bien de la humanidad, es necesaria una herramienta para hablar libremente unos con otros, e intercambiar valor si fuera necesario. Por fin, las personas podrán conectarse globalmente en la red más segura posible. Esto llevará a Skrumble a ser la versión blockchain de plataformas como WeChat.

## TECNOLOGÍA: ¿CÓMO COMBINA LA RED SKRUMBLE COMUNICACIÓN Y BLOCKCHAIN?

Internet ha conseguido incrementar en gran medida el progreso por un intercambio de información global. Sin embargo, operan actualmente con un sistema centralizado de servidores, infraestructura de almacenamiento, y en definitiva, comunicación. La tecnología de Skrumble Network tiene como objetivo avanzar desde el intercambio puro de información hacia una creación de valor e intercambio y cooperación genuina.

Es ampliamente conocido que existen limitaciones técnicas significativas con blockchain en cuanto al almacenamiento de datos y la velocidad de conexión. Es por ello que es necesaria una metodología híbrida, que combine la seguridad de la infraestructura de blockchain con una comunicación distribuida y encriptada. Esto se conseguirá optimizando la blockchain de Skrumble para las necesidades modernas de comunicación, como riqueza de contenido multimedia, una velocidad rápida de transacción e intercambios financieros dentro de la propia aplicación. Estará construida para transportar una gran cantidad de información necesaria para establecer una comunicación entre pares (P2P) a la vez que transacciones en el libro contable digital. El objetivo principal de la blockchain de Skrumble será conseguir llegar al consenso lo más rápido posible. El número de transacciones es crítico. El diseño de Skrumble permitirá a la red escalar hasta las 1000 transacciones por segundo, desde las actuales 500.

Al conseguir un consenso rápido, el retraso asociado con las transacciones blockchain se eliminará de la experiencia del usuario. El resultado será una experiencia impecable y de calidad para el consumidor, que los usuarios esperan, con la seguridad y autenticación sin igual que proporciona la tecnología blockchain. Esto marcará el comienzo de una nueva generación de aplicaciones seguras y poderosas que cumplirán y superarán los estándares actuales de usabilidad.

La blockchain de Skrumble será una red con estructura entre pares, en la que los nodos se podrán comunicar entre ellos a través de un protocolo de mensajería en hash. En esta estructura, existirán dos tipos diferentes de nodos: nodos peer y nodos de validación. Un nodo peer puede transmitir, recibir y transferir transacciones o bloques, mientras que un nodo de validación puede crear bloques de datos.

## ESTRATEGIA COMUNITARIA:

La plataforma enfocada en comunicación de Skrumble es una blockchain pública. La Fundación, como sponsor del proyecto, trabajará para construir y mantener el ecosistema en vez de enfocarse en las ganancias corporativas, como las empresas tradicionales harían. La plataforma, que beneficiará a todos los que tengan el token, no pertenece a una única organización o individuo, y abarca a toda a toda la comunidad.  Usará los mecanismos del token y los recursos de la fundación para fomentar y promover a numerosas comunidades, como las técnicas, universitarias, usuarios, inversores, nodos, organizaciones centralizadas, proveedores de datos, etc. La visión de la comunidad de SN es crear una gran familia basada en la inclusión, que comparte la pasión y misión de hacer crecer a la red de Skrumble.

# INTRODUCCIÓN

La necesidad de medios de comunicación simples y seguros y la propiedad de nuestros datos nunca ha sido mayor. Comunicarse unos con otros es esencial para las personas, y es imperativo que esas personas puedan comunicarse de forma segura y tener la propiedad de sus datos. Skrumble Network innovará la comunicación descentralizada mediante una blockchain pública. Esta red será una blockchain centrada en la comunicación, poderosa y segura con una cantidad de transacciones por segundo que asegure unos tiempos de conexión rápidos. Esto permitirá una comunicación en tiempo real, a nivel comercial, con autenticación de identidad del usuario en la blockchain mediante la proporción de una clave segura que será derivada de forma completamente aleatoria desde la llave pública (public key) de cada participante. Solamente los propios participantes tendrán acceso a dichas comunicaciones. No hay ninguna entidad intermediaria que censure, bloquee o manipule ningún dato. Esto permitirá una comunicación abierta, global, privada verdaderamente en propiedad y operada por la comunidad. Esto brindará a las personas la oportunidad de añadir elementos descentralizados de comunicación a cualquier ecosistema blockchain, construir aplicaciones con comunicación descentralizada; finalmente, las personas pueden conectarse globalmente y hablar libremente en la red más segura posible.

Debido al auge de la tecnología blockchain y el nuevo paradigma global descentralizado, es esencial para Skrumbe Network innovar utilizado esta tecnología y demostrar cómo las redes descentralizadas tienen el poder de ser un catalizador para una comunicación más segura. Esto se conseguirá mediante la exclusiva seguridad blockchain híbrida de Skrumble Network, protocolo distribuido SSL patentado y medios ricos en tecnología de comunicación basada en WebRTC. En el presente whitepaper se van a tratar temas como los riesgos que conllevan servidores centralizados para el almacenamiento de datos, las amenazas a la información del usuario que involucran sistemas de comunicación basados en Internet y la dificultad de establecer conexiones significativas en línea. Estos problemas enfatizan la necesidad de una blockchain segura y de alta velocidad que permita una red segura y unificada que brinde una experiencia end-to-end única con total anonimato, y brindará la oportunidad para que una red de comunicación descentralizada experimente un crecimiento infinito.

Skrumble network tiene el potencial de verdaderamente democratizar la comunicación a escala global y marcar el comienzo de una nueva era de aplicaciones nunca hechas anteriormente, lo que lleva a formas avanzadas e incomparables de innovación y descubrimiento. Tendrá la capacidad de conectar a cualquier persona desde cualquier lugar del mundo de forma segura y sencilla. Utilizando tecnología blockchain y protocolos de redes descentralizados, Skrumble Network será el primero el construir un ecosistema completo y seguro de comunicación de medios completos que superará los firewalls tradicionales, asegurará el anonimato del usuario, garantizará el contenido y la privacidad de los datos. Ahora, cualquier aplicación tendrá la capacidad de implementar funciones principales de comunicación descentralizada, tales como mensajes grupales y de par a par (P2P), llamadas, video, transferencias de archivos y mucho más con un protocolo de red blockchain. Al igual que Blockchain interrumpió la industria financiera con una metodología de contabilidad distribuida debido a las disconformidades con los grandes establecimientos financieros centralizados, vemos grandes oportunidades para hacer lo mismo con la industria de las comunicaciones. Haremos esto devolviendo la propiedad y la seguridad de los datos a las personas, lejos de las grandes compañías de telecomunicaciones y proveedores de aplicaciones centralizadas (como Facebook, Telegram, WeChat y WhatsApp).

# LA PROBLEMA

| | | |
|---|---|---|
| 1. Seguridad: Los sistemas de comunicación con servidores centralizados plantean desafíos de seguridad de los datos. | 2. Privacidad y propiedad de los datos: las plataformas no son privadas, pueden ser bloqueadas o comprometidas y los usuarios no poseen sus datos. | 3. Acceso global: las comunidades marginadas buscan una discusión libre y conexiones confiables. |

## 1. Seguridad: Los sistemas de comunicación con servidores centralizados plantean desafíos de seguridad de los datos.

Internet ha revolucionado la forma en la que nos comunicamos y conectamos, es posible hacer llamadas de vídeo mediante un click, las empresas pueden operar y colaborar de forma internacional, los bancos facilitan transferencias internacionales que mueven trillones* (en la acepción anglosajona del concepto) de dólares cada día, y acercarse al presidente de un país está a solo un tweet de distancia. Con el e-commerce, un objeto puede estar manufacturado en Guangzhou, vendido por una empresa en Nueva York y comprado finalmente por una señora en Sidney. Las redes sociales han cambiado el aspecto de la comunicación, las noticias y el entretenimiento. Internet ha conseguido conectar casi a todas las personas en su red, pero también genera preocupaciones en cuanto a la privacidad y seguridad de los datos.

Los usuarios de Internet regularmente, y en ocasiones involuntariamente, aceptan términos y condiciones que dan a las compañías permiso y derecho para compartir sus datos personales con otras instituciones, desde anunciantes hasta gobiernos. Por ejemplo, Google consigue ofrecer sus principales servicios al consumidor de forma gratuita compartiendo datos de los usuarios tales como la actividad del navegador y el historial de búsqueda, mientras que Facebook vende los datos y actividades de los usuarios como los “me gusta” y comentarios a los anunciantes (Google, 2018, Facebook, 2018). Cuando se visitan redes sociales o sitios web de comercio electrónico, es común que en los anuncios se reflejen los datos mencionados anteriormente e incluso las conversaciones que se mantuvieron verbalmente sin conexión, lo que plantea preocupaciones específicas sobre el espionaje digital y la privacidad del usuario.

Las aplicaciones de comunicación administran cantidades masivas de tráfico de datos todos los días. La plataforma de mensajería WhatsApp maneja aproximadamente 55 mil millones de mensajes, 4 mil millones de fotos y mil millones de transferencias de video por día. Sin embargo, como la mayoría de las otras plataformas de comunicación basadas en Internet, todos estos datos se enrutan a través de un servidor centralizado con un punto de contacto principal. En este tipo de sistema centralizado, la violación de un punto de contacto es más fácil y podría dar a las partes malintencionadas acceso a una gran cantidad de datos de la red. Esto permitiría a los piratas informáticos robar y alterar la información. Debido a estos sucesos, en enero de 2018 los criptógrafos descubrieron una puerta trasera a través del sistema de seguridad de WhatsApp y pudieron infiltrarse en grupos de chats. Con una brecha de esta magnitud, la credibilidad de WhatsApp se volvió refutable y efectivamente se inutilizó la encriptación end-to-end de la herramienta de chat (Greenberg, 2018).

Es casi imposible usar Internet sin ceder a la privacidad o estar en riesgo de piratería. Existe una necesidad crítica de una red descentralizada e impenetrable a través de la cual los usuarios puedan comunicarse y conectarse de manera segura sin tener que preocuparse de que su información personal se vea comprometida. Esto es especialmente pertinente en el mundo de las criptomonedas, donde grandes sumas de dinero están en juego.

## 2. Privacidad y propiedad de los datos: las plataformas no son privadas, pueden ser bloqueadas o comprometidas y los usuarios no poseen sus datos.

Cuando se trata de comunicarse entre sí, generalmente las personas recurren a Internet como la principal fuente de transferencia de información. Sin embargo, con numerosas fuentes de información y foros de discusión disponibles en Internet hoy en día, las personas usan varias plataformas de comunicación diferentes para aprender y tener discusiones sobre blockchain y otros temas importantes. Esto lleva a una experiencia comunitaria muy fragmentada y desconectada.

El uso de varias plataformas como por ejemplo Facebook, WhatsApp, WeChat y otros para colaborar y compartir información hace que sea difícil tener un estándar global coherente y confiable. Incluso plataformas como Telegram, que se sabe que censuran y bloquean contenido, pueden ver sus datos recopilados, descifrados, también se puede bloquear el acceso a los datos mediante bloqueos a direcciones URL o direcciones IP VPN conocidas (Russell, 2017). De hecho, el 1 de febrero de 2018, Telegram fue retirado de la Apple App Store debido a "contenido inapropiado" y se les solicitó que se aseguraran de que tuvieran medidas de protección para filtrar su contenido (Warren, 2018). Algunas de estas plataformas están prohibidas o limitadas en ciertos países, lo que genera desigualdad en la información. Facebook y WhatsApp están prohibidos en China y recientemente se levantó la prohibición de Telegram en Irán, sin embargo Telegram está y ha sido prohibido en muchos otros países, como Indonesia (Toronto Star, 2018, Toor, 2017).

- Facebook, WhatsApp, y Google están baneadas en China continental (India Today, 2017).
- Se descubrió recientemente que WhatsApp tiene una puerta trasera que permite la infiltración en grupos de chats (Greenberg, 2018).
- WeChat censura las conversaciones de los usuarios y no tiene sincronización en múltiples dispositivos (WeChat, 2018).
- Telegram censura activamente contenido, fue prohibido previamente en Irán y prohibido recientemente en Rusia (Toronto Star, 2018).
- It was recently reported that over 87 million Facebook users had their data stolen and misused (Sherr, 2018)

Además, los foros específicos centrados en la discusión de nuevas tecnologías y otros temas pueden tener otras formas de censura. Un ejemplo de esto son los foros dedicados a la discusión sobre criptomonedas como Bitcointalk o hilos en Reddit. Una barrera crítica para la entrada de personas interesadas en criptomonedas es la falta de información sobre la legalidad del comercio de criptomonedas. Estos foros a menudo tienen ciertas limitaciones cuando se trata de precisión, credibilidad y confianza, ya que están compuestos principalmente por opiniones personales y no siempre están respaldados por hechos verificables.

Las personas también recurren a plataformas de intercambio de videos como YouTube para obtener información y educación sobre el ecosistema de criptomonedas y casi todo lo demás. Este contenido tiene el problema de ser unidireccional, de dudosa confianza y sesgada, ya que en su mayoría cubre las preferencias individuales, proporcionando sólo una visión superficial de cualquier tema. Además, dado que estas plataformas de comunicación usan redes centralizadas, se enfrentan todos los peligros previamente mencionados de hackeo, ingeniería social y otras vulnerabilidades de seguridad.

Después de estudiar las comunidades en línea actuales y las opciones de las plataformas de comunicación, las fallas y vulnerabilidades dentro de cada sistema son obvias. Las soluciones actuales están fragmentadas, desconectadas y no son confiables, lo que deja un margen de mejora para elevar la confianza y la conectividad en todo el mundo. A través de una solución como una comunidad en línea accesible a nivel mundial, la comunicación unificada y segura aumentaría y ampliaría las oportunidades para unir a las personas.

## 3. Acceso global: las comunidades marginadas buscan una discusión libre y conexiones confiables.

Con la constante aprehensión y la inseguridad de los datos, ¿cómo pueden las personas sentirse cómodas para crear comunidades en línea sostenibles y compartir información significativa en las conversaciones? Uno de los desafíos de la participación en línea es desarrollar relaciones mientras se protege su identidad, creando comodidad, seguridad y desarrollando actividades procesables. Las personas necesitan acceso sin ataduras a los foros y plataformas públicas para ejercer su derecho humano fundamental de libre expresión y no sentirse preocupados por los intermediarios y terceras personas desconocidas con acceso a su información privada.

Cosas tan simples como discusiones sobre intereses comunes, compartir historias y trabajar en red ayuda a unir a las personas. Cuando las personas están conectadas, se sienten desinhibidas y lo suficientemente cómodas como para compartir ideas genuinas y honestas, información personal y establecer relaciones significativas. Cuando las personas se sienten cómodas y conectadas, pueden suceder cosas increíbles e innovadoras.

A veces, para las comunidades marginadas que buscan foros para discutir libremente puede ser difícil encontrar un medio abierto y simplificado para compartir nuevas ideas. Un ejemplo de una comunidad que necesita conectividad y acceso global es la comunidad de criptomonedas. La percepción pública de una criptomoneda es uno de los factores decisivos más importantes detrás de su adopción y valor. Aunque solo tienen alrededor de nueve años, las criptomonedas se encuentran en una etapa de rápido crecimiento y expansión con miles de monedas y aplicaciones diferentes en la actualidad. En un entorno tan incipiente, es cada vez más difícil para las empresas de tecnología blockchain mostrar nuevas ideas y para que los usuarios potenciales se conecten y aprendan más sobre los últimos desarrollos de la comunidad. La mejor forma para que los defensores de blockchain interactúen con los usuarios potenciales y el público es a través de la comunicación directa.

Al no solo fomentar, sino también facilitar el establecimiento de conexiones significativas, una red de comunicaciones seguras podría proporcionar medios verdaderos esenciales para que cualquier persona, desde cualquier parte del mundo, pueda conectarse. Podrían simplemente hablar de forma libre, compartir información y transferir datos sin la preocupación de ser pirateados o que alguien más tenga acceso a su información personal. Una comunidad global de blockchain ayudaría a mejorar la comunicación en todo el mundo, ya sea entre los actuales usuarios de blockchain o cualquier persona que necesite conectarse con alguien que usa una red segura.

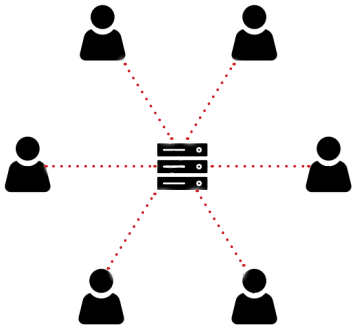
# REQUISITOS DE SOLUCIÓN

1. Seguridad: Mejorar la seguridad con tecnología de comunicación Skrumble

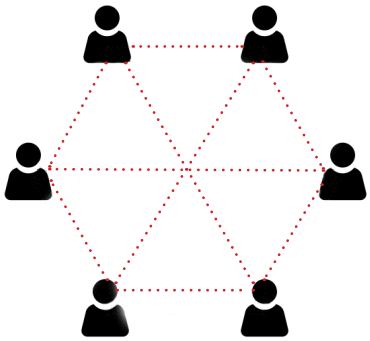
2. Descentralización: La tecnología contable distribuida de blockchain para conseguir transacciones basadas en comunicación.

## 1. SEGURIDAD: MEJORAR LA SEGURIDAD CON TECNOLOGÍA DE COMUNICACIÓN SKRUMBLE

Tradicionalmente, las plataformas de comunicación dependen de servidores centralizados para transmitir información y almacenar los datos enviados entre los usuarios. Al contrario del método tradicional, en una red descentralizada, como blockchain, no hay ningún tipo de información que se almacene en una única localización, lo que hace los ataques de cibercriminales casi virtualmente imposibles. Hackers y otros cibercriminales se infiltran regularmente en sistemas de seguridad informática y en redes, desde cualquier parte del mundo, en cuestión de horas. Sin embargo, una vez que la información se registra en la blockchain, no se puede borrar, cambiar, mover o modificar de ninguna manera. Atacar un servidor central deja de ser una opción para conseguir el control total del sistema. Esta inmutabilidad, basada en diversos protocolos, en una red descentralizada, crea un marco de referencia transparente y seguro, con una trascendencia inmensa.



Servidor centralizado



Red descentralizada

En el sector bancario es imprescindible un método que asegure las transacciones digitales, y la tecnología blockchain usada en las criptomonedas es una de las mejores opciones. Los economistas que se dedican a estudiar las criptomonedas han confirmado que el dinero se está volviendo cada vez más digital, y que gobiernos en países tales como Canadá, India y Rusia han empezado a explorar la manera de incorporar el uso de las criptomonedas en su economía (Sabbin, 2018). La inmutabilidad propia de Blockchain reduce el coste de verificar transacciones y su naturaleza descentralizada ofrece la posibilidad de eliminar a los intermediarios en los intercambios de valor.

Lo mismo se puede decir sobre las soluciones que puede aportar una red descentralizada sobre comunicación y gestión de la identidad. Dado el gran alcance de las posibles aplicaciones de la tecnología blockchain, y la transparencia y seguridad que pueden aportar, los servicios y plataformas que ofrezcan todas estas ventajas de manera accesible al público, tendrán la oportunidad de conseguir un crecimiento significativo.

## 2. DESCENTRALIZACIÓN: LA TECNOLOGÍA CONTABLE DISTRIBUIDA DE BLOCKCHAIN PARA CONSEGUIR TRANSACCIONES BASADAS EN COMUNICACIÓN.

En 1998, Nick Szabo, criptógrafo y pionero de los contratos inteligentes, declaró que "hacer negocios en Internet requiere dar un salto de fé". La confianza siempre ha sido la moneda de cambio tanto en la comunicación como en el comercio. Cada segundo, nuevas transacciones en línea ocurren entre extraños alrededor del mundo, normalmente a través de una tercera parte, permitiendo el intercambio de información, y la confianza tiene que establecerse entre el usuario y esa tercera parte para llevar a cabo la operación. Ya sea un mensaje o un pago lo que se envía, el que lo hace no tiene más remedio que confiar en que el intermediario transmitirá la transacción al receptor de forma segura.

Con el libro digital de contabilidad distribuido de blockchain (ledger), los usuarios pueden conectarse de manera segura y directa unos con otros, ejecutando transacciones sin tener que depender de un intermediario ni preocuparse por la protección de su privacidad. Blockchain y las redes descentralizadas ofrecen una manera de operar en un ambiente en el que la confianza no es necesaria, usando el registro contable distribuido para crear registros de transacciones inalterables, basados en la transparencia y el consenso. Cada nuevo bloque de transacciones es verificado por la red al completo, y se vincula de manera inmutable al resto de la cadena, para conseguir una seguridad y registro incomparables.

Además, existe una creciente necesidad de mejorar los sistemas de identificación a lo largo de la web. La necesidad de verificar la identidad propia de cada individuo es ahora mismo esencial para una gran cantidad de cuentas y transacciones en línea, incluyendo datos tales como dirección, información de contacto, información financiera, y muchos más. En 2017, en los Estados Unidos, se alcanzó un número récord de 15.4 millones de americanos que sufrieron fraude financiero y robo de la información de su cuenta (Pascual, 2017).

Los libros de contabilidad distribuidos ofrecen mejores métodos para verificar la identidad de los usuarios, sin necesidad de compartir información de contacto, además de ofrecer la posibilidad de digitalizar la información personal. El mecanismo de encriptado en una blockchain a través de clave pública y privada permite a las aplicaciones verificar digitalmente la identidad de las personas que las usan, eliminando el riesgo de suplantación de identidad y de alteración o robo de datos personales.

Usando la tecnología blockchain, que conecta a los usuarios directamente, eliminando la necesidad de confiar en un intermediario o una tercera parte desconocida, se pueden solucionar muchos de los problemas en seguridad y transparencia que existen actualmente en las redes distribuidas. Una red de comunicación distribuida significa que los usuarios puedan conectarse de manera directa y segura, e intercambiar información entre sí, sin necesidad de preocuparse por su privacidad.

# SKRUMBLE NETWORK: Blockchain de redes sociales entre pares (P2P) para contactar y contratar

Existe una necesidad innegable de una blockchain centrada en comunicación, segura, optimizada y estandarizada, sobre la que sea fácil construir, y que permita una comunicación con un alto grado de descentralización, de manera segura, llegando perfectamente al nivel comercial. Con un marco robusto, designado especialmente para el ecosistema blockchain, y una gran experiencia en el terreno de las comunicaciones, Skrumble Network se establece como la mejor equipada para satisfacer esta necesidad.

El primer ecosistema completo de comunicación en una red descentralizada de autenticación basada en blockchain será construido por Skrumble Technologies Inc. Este ecosistema único, basado en la sencillez de uso y en la seguridad, logrará conectar personas en cualquier lugar del mundo a través de una comunicación abierta e imparable. Con una comunicación unificada, los miembros de la comunidad de Skrumble Network y los desarrolladores asociados podrán por fin establecer conexiones significativas, en un entorno descentralizado, democrático, global e incuestionablemente seguro.

Usando un algoritmo basado en el consenso, y medidas de identificación pseudónimas, en las que las personas pueden establecer sus nombres de usuario, estas contarán con la completa propiedad de su información, datos, y las transacciones realizadas. Los usuarios tendrán la oportunidad de establecer comunidades en línea con una gran cantidad de personas o realizar conversaciones más personales con otros usuarios, todo ello manteniendo toda su información privada y segura. Esta red permitirá a los usuarios interactuar entre sí usando mensajes, llamadas, vídeos, transferencias de archivos y muchas opciones más, y mejorar el acceso a la comunicación, la gestión de la identidad, y a las transacciones seguras. Skrumble Network tiene la intención de aprovechar su tecnología de seguridad única y novedosa para resolver los riesgos de seguridad de los actuales sistemas de comunicación basados en Internet, a través de su autenticación distribuida basada en blockchain y SSL patentado, además enriquecer los protocolos de comunicación actuales.

Debido al crecimiento de la tecnología blockchain, y al nuevo paradigma global descentralizado, es esencial para la comunidad de Skrumble Network innovar todos juntos, utilizando esta tecnología y demostrar cómo las redes descentralizadas tienen el poder de ser el catalizador de una comunicación más segura.

En el mundo actual, basado en la no-confianza, la reputación será una materia esencial, para no tener que usar los métodos tradicionales de construir relaciones y realizar transacciones. Por ejemplo, en el pasado, si querías construir una relación de confianza, e intercambiar con otra persona, tendrías que ir a cenar fuera, quizá tomarte unas copas, leer el carácter de la otra persona, etc. En el actual mundo de la no-confianza, no necesitas ni siquiera saber el nombre de la otra persona para establecer una relación, solamente su reputación de los tratos anteriores, y un contrato inteligente obvia la necesidad de todo lo demás.

En Skrumble, al contrario que en otras plataformas centralizadas que requieren de un número de teléfono, un identificativo o un correo electrónico, únicamente necesitas una clave segura a la que solo tú y tus pares en la conversación tienen acceso. Las personas serán ahora capaces de unirse a la economía blockchain con sencillez y verdadera posesión de sus datos.

Skrumble Technologies Inc reconoce la necesidad inherente de un ecosistema seguro de comunicaciones, utilizando la inmutabilidad basada en el consenso de protocolos de red descentralizados  Skrumble Network se basa en la pericia y la experiencia del equipo irremplazable detrás de Skrumble, para ofrecer esta funcionalidad única e innovadora. Mediante el uso de kits de desarrollo de software (SDK) de código abierto, el ecosistema completo de comunicación se construirá para que sea fácilmente adaptable para que terceros puedan integrar y desarrollar una multitud de aplicaciones que requieren comunicaciones seguras, privadas y anónimas.

Uno de los primeros de su especie, Skrumble Network operará al margen de la comunicación centralizada tradicional, en la que se suelen usar algunos de los protocolos que hay detrás de blockchain, para conseguir un nuevo estándar global de comunicación, autenticación y sobre cómo la tecnología blockchain puede ser usada en aplicaciones alrededor del mundo.

## LAS CARACTERÍSTICAS DE COMUNICACIÓN DE LA BLOCKCHAIN DE SKRUMBLE NETWORK

- Mensajería
- Llamadas de audio
- Videollamadas
- Transferencia de archivos
- Conferencias grupales
- Pantalla compartida
- Almacenamiento controlado por el usuario
- Notificaciones de capturas de pantalla
- Identificación pseudo anónima
- Encriptado de datos
- La mayoría de las funcionalidades admitidas en cualquier navegador moderno
- Cartera para transferencias internas de dinero

# COMPONENTE TÉCNICO: LA TECNOLOGÍA QUE IMPULSA LA RED SKRUMBLE

## INTRODUCCIÓN: COMUNICACIONES SEGURAS EN UNA RED DESCENTRALIZADA

Las redes de comunicación tradicionales se basan en servidores centralizados. Independientemente de los protocolos de comunicación que se utilizan, esencialmente todos funcionan de la misma manera. Esto es, mediante un paquete de información que contiene el coloquio y el intercambio de meta información para establecer la corriente de medios de comunicación. Skrumble Network revolucionará la forma en que ocurre la comunicación al eliminar por completo el servidor centralizado.

## VISIÓN GENERAL DE LA RED BLOCKCHAIN DE SKRUMBLE NETWORK

La blockchain de Skrumble Network está optimizada para satisfacer las necesidades de las comunicaciones modernas, necesidades como abundante multimedia, tiempos de transacción rápidos, seguridad e intercambios financieros dentro de la aplicación. Está diseñada para transportar una carga útil de información que se requiere para establecer una comunicación P2P, así como datos contables de transacciones financieras. El objetivo principal de la blockchain de Skrumble es lograr el consenso lo más rápido posible. Aunque las TPS sin críticas, el diseño permitirá a la red Skrumble escalar hasta 1000 TPS en el futuro desde el nivel operativo actual de 500 TPS.

Al lograr el consenso rápidamente, la experiencia de retraso típicamente asociado a las transacciones de blockchain se elimina para los usuarios. El efecto neto es una experiencia impecable y de calidad para el consumidor tal y como los usuarios esperan, con la seguridad y autenticación sin igual que proporciona la tecnología blockchain. Esto marcará el comienzo de una nueva generación de aplicaciones seguras y potentes que cumplen y superan las expectativas de los estándares actuales de usabilidad.

Skrumble Blockchain es una estructura de red P2P, en la que los nodos se pueden comunicar entre sí a través de un protocolo de mensajería hash. En esta estructura, hay dos tipos diferentes de nodos: nodos “peer” y nodos de validación. Un nodo “peer” puede transmitir, recibir y transferir transacciones o bloques, mientras que un nodo de validación puede crear bloques de datos.

El protocolo blockchain es similar al de Bitcoin, sin embargo, la estructura de datos como bloques o transacciones es significativamente diferente porque contiene no solo datos financieros sino también instrucciones de comunicación e información de cifrado.

Un ejemplo de los requisitos adicionales de carga útil son los campos de datos que permiten que se establezcan las comunicaciones de igual a igual. Esto incluye campos que identifican la ID de la sesión (SID). Este campo es obligatorio y se vincula al nombre de usuario de la rama “b”. Esto se usa no solo para identificar la sesión actual, sino que también permite al usuario ver el historial completo de conversación entre las partes.

La ofuscación de la información transversal IP y NAT se logra mediante el uso de un algoritmo hash que se incrementa. El incremento del algoritmo se logra a través de dos campos de identificación. El primero es el VID (ID de versión) que le dice a los otros usuarios qué versión de la aplicación está siendo utilizada. El segundo es el IID (ID de incremento) que alerta a las otras ramas de la comunicación qué algoritmo de hashing usar. Los algoritmos hash se actualizarán con cada nueva versión de software. Las versiones de software que tienen más de dos versiones separadas generarán un error. Esto se hace para garantizar que los usuarios tengan el último software de aplicación.

También se incluye un enlace de descarga hash para usuarios en ubicaciones geográficas que quizás no tengan acceso a tiendas de aplicaciones tradicionales. Este enlace cambiará constantemente para garantizar el acceso de las poblaciones marginadas. Este enlace será pasado por un proceso hash utilizando la misma técnica de datos VID e IID para confundir aún más cualquier intento por parte de las autoridades de conocer el destino del enlace. Además, las direcciones de validación de nodos se correlacionarán de la misma manera, es decir, utilizando el VID

## SEGURIDAD DE RED BASADA EN IDENTIDAD

La blockchain de Skrumble Network emplea un enfoque novedoso para la gestión de identidades de usuarios en los servicios de blockchain. Implementamos seguridad de extremo a extremo basada en identidad que se extiende desde el cliente al tejido blockchain. Este enfoque permite la segmentación de la red basada en la identidad y la separación del tráfico, lo que permite que múltiples usuarios compartan de forma segura la misma infraestructura de blockchain, reduce el riesgo de ataques DDoS y permite auditorías de cumplimiento reglamentario automatizadas. Nuestra solución se basa en la tecnología Skrumble Network Transport Access Control (SKTAC), implementadas mediante los puntos finales de la biblioteca de aplicaciones de software Skrumble Network. Este enfoque puede generalizarse fácilmente para proteger muchos tipos diferentes de aplicaciones comerciales.
Las características de SKTAC incluyen control de permisos y confidencialidad, privacidad de identidad no enlazable para participantes de blockchain, un protocolo de consenso modular fácilmente auditable y escalabilidad mejorada. SKTAC **amplía el blockchain de varias maneras importantes.**

- Un nuevo método para la seguridad de la red basada en la identidad, que se extiende de extremo a extremo desde el cliente al tejido blockchain. Esto se realiza autenticando el primer paquete de una solicitud de conexión de red utilizando tokens de identidad criptográfica, que se insertan en el encabezado del paquete mediante la aplicación Skrumble Network en el cliente, y luego se autentican mediante un nodo de validación. Todo el tráfico no autorizado (incluidos los escaneos de puertos) se elimina en el nivel de transporte, por lo que la fuente de tráfico no recibe ningún reconocimiento o retroalimentación que pueda utilizarse para el reconocimiento o la enumeración como el primer paso en un ciberataque. De esta manera, aislamos y protegemos los servicios de blockchain del acceso no autorizado; esto ayuda a prevenir los ciberataques, habilita los servicios de blockchain y forma la base de una red blockchain de confianza cero.

- SKTAC introduce segmentación de red basada en identidad y separación de tráfico, lo que reduce el riesgo de ciberataques. Al utilizar la autenticación de primer paquete descrita anteriormente, separamos el tráfico interno entre pares y nodos de validación utilizadas en la blockchain de Skrumble. Los registros de auditoría para todos los intentos de conexión autorizados y no autorizados a la cadena de bloques se mantienen y se pueden auditar fácilmente mediante el uso de software para analizar el contenido del registro.

Sin autenticación, cualquier usuario no autorizado recibirá el mensaje de que no se puede acceder a este sitio, y que no hay más información disponible.

## ASEGURANDO LA CONVERSACIÓN

Quizá el componente más único y crítico de la blockchain de Skrumble es el sistema de encriptación. Este se usa para cifrar todos los aspectos de la comunicación, incluyendo video, audio, e incluso los archivos que se intercambien y almacenen.

Skrumble Network deriva su esquema de cifrado de los datos que se comercializan anómalamente a través de blockchain. Esto garantiza el más alto nivel de encriptación, privacidad y propiedadde los datos del usuario.

Skrumble Network ha desarrollado un protocolo llamado SKRTP (Skrumble Secured Real Time Protocol). El documento oficial para este protocolo se publicará en el momento del lanzamiento.

## EL PROTOCOLO DE TRANSPORTE SEGURO EN TIEMPO REAL DE SKRUMBLE (SKRTP)

Skrumble Network empleará el protocolo de transporte seguro en tiempo real (SKRTP), un perfil del protocolo de transporte en tiempo real (RTP), que proporciona confidencialidad, autenticación de mensajes y protección de reproducción para el tráfico RTP y para el tráfico de control para RTP. el protocolo de control de transporte en tiempo real (RTCP).

El protocolo de transporte seguro en tiempo real (SKRTP), un perfil del protocolo de transporte en tiempo real (RTP), que puede proporcionar confidencialidad, autenticación de mensajes y protección de reproducción para el tráfico RTP y para el tráfico de control para RTP, RTCP (el Protocolo de control de transporte en tiempo real).

SKRTP proporciona un marco para el cifrado y la autenticación de mensajes de flujos RTP y RTCP. SKRTP define un conjunto de transformaciones criptográficas y permite la introducción de nuevas transformaciones en el futuro. Con una gestión de claves adecuada, SKRTP es seguro para aplicaciones RTP de unidifusión y multidifusión.

SKRTP puede lograr un alto rendimiento y una baja expansión de paquetes. SKRTP demuestra ser una protección adecuada para entornos heterogéneos (combinación de redes con cable e inalámbricas). Para obtener tales características, se describen transformaciones predeterminadas, basadas en un cifrado de flujo aditivo para encriptación, una función basada en hash con clave para la autenticación de mensajes y un índice “implícito” para la secuencia / sincronización basada en el número de secuencia RTP para SKRTP y un índice número para Secure RTCP (SRTCP).

## CARACTERÍSTICAS

Los objetivos de seguridad para SKRTP son garantizar:
• La confidencialidad de las cargas útiles RTP y RTCP, y
• La integridad de todos los paquetes RTP y RTCP, junto con la protección contra paquetes repetidos.

Estos servicios de seguridad son opcionales e independientes entre sí, excepto que la protección de integridad SRTCP es obligatoria (la alteración maliciosa o errónea de los mensajes RTCP podría interrumpir el procesamiento de la transmisión RTP).

Otras características del el protocolo son:
• Bajo costo de ancho de banda, es decir, un marco que preserva la eficiencia de compresión del encabezado RTP y, afirmado por las transformaciones predefinidas:
• Un bajo costo computacional,
• Una huella pequeña (es decir, tamaño de código pequeño y memoria de datos para introducir información y listas de reproducción),
• Expansión de paquete limitada para soportar el objetivo de economía de banda ancha,
• Independencia del transporte subyacente, red y capas físicas utilizadas por RTP, alta tolerancia a la pérdida de paquetes y reordenamiento.

Todas estas propiedades aseguran que SKRTP es un esquema de protección adecuado para RTP / RTCP en escenarios tanto cableados como inalámbricos.

SKRTP proporciona algunas características adicionales que se han introducido para aligerar la carga en la administración de claves y incrementar aún más el nivel de seguridad. Incluyendo:
• Una única “clave maestra” puede proporcionar claves secretas de formato, longitud e importe para la protección de la confidencialidad y la integridad, tanto para la transmisión SKRTP como para la transmisión SRTCP correspondiente. Esto se logra con una función de derivación de clave, que proporciona “claves de sesión” para la respectiva clave primitiva, derivada de forma segura de la clave maestra.
• Además, la derivación de la clave se puede configurar para actualizar periódicamente las claves de sesión, lo que limita la cantidad de texto cifrado producido por una clave fija, disponible para que un adversario pueda realizar un criptoanálisis.
• El salteado de claves se usa para proteger contra los ataques de precomputación y compensación de tiempo-memoria.

## CIFRADO

El encriptado definido en el SKRTP traza la ruta para la indexación de paquetes y claves secretas en un segmento de flujo de claves pseudo aleatorio. Cada segmento de flujo de claves encripta un solo paquete RTP. El proceso de encriptación de un paquete consiste en generar el segmento de flujo de claves correspondiente al paquete y, a continuación, excluir bit a bit ese segmento de flujo de claves en la carga útil del paquete RTP para producir la Porción encriptada del paquete SKRTP. En caso de que el tamaño de la carga útil no sea un múltiplo entero de n_b bits, los bits en exceso (menos significativos) de la cadena de claves simplemente se descartan. El descifrado se realiza de la misma manera, excepto al cambiar las funciones del texto sin formato y el texto cifrado.

La definición de cómo se genera el flujo de claves, dado el índice, depende del cifrado y su modo de operación. A continuación, se definen dos generadores de flujo de claves. También se define el cifrado NULL, que se utilizará cuando no se requiera el cifrado de RTP.

Los octetos iniciales de cada segmento de flujo de claves pueden reservarse para su uso en un código de autenticación de mensaje, en cuyo caso el flujo de claves utilizado para el cifrado comienza inmediatamente después del último octeto reservado. Los octetos reservados inicialmente se denominan “prefijo keystream”, y los octetos restantes se llaman “sufijo keystream”.

El número de octetos en el prefijo de flujo de claves se denota como SKRTP_PREFIX_LENGTH. El prefijo keystream se indica mediante un valor positivo distinto de cero de SKRTP_PREFIX_LENGTH. Esto significa que, incluso si no se debe proporcionar confidencialidad, la salida del generador de flujo de claves aún puede necesitar computarse para la autenticación de paquetes, en cuyo caso se utilizará el generador (modo) de flujo de claves predeterminado.

El cifrado es el Estándar de cifrado avanzado (AES), el Modo de contador de enteros segmentados AES. Deje que E (k, x) sea AES aplicado a la clave k y el bloque de entrada x. Conceptualmente, AES consiste en encriptar enteros sucesivos. La definición real es algo más complicada, aleatorizar el punto de partida de la secuencia entera. Cada paquete se cifra con un segmento de flujo de claves distinto, que se calcula de la siguiente manera.

Un segmento de flujo de claves es la concatenación de los bloques de salida de 128 bits del cifrado AES en la dirección de cifrado, utilizando la clave k = k_e, en la cual los índices de bloques siguen un orden creciente. Escrito con símbolos, cada segmento keystream se ve así:

E(k, IV) || E(k, IV + 1 mod 2^128) || E(k, IV + 2 mod 2^128) ...

Donde el valor entero IV de 128 bits está definido por el SSRC, el índice de paquete SKRTP i, y la clave sal de sesión SKRTP k_s, como a continuación:

IV = (k_s * 2^16) XOR (SSRC * 2^64) XOR (i * 2^16)

Cada uno de los tres términos en la suma XOR anterior se rellena con tantos ceros a la izquierda como sea necesario para que la operación esté bien definida, considerada como un valor de 128 bits.

La inclusión del SSRC permite el uso de la misma clave para proteger flujos SKRTP distintos dentro de la misma sesión RTP.

En el caso de SRTCP, es OBLIGATORIO utilizar el SSRC del primer encabezado del paquete compuesto, i DEBE ser el índice SRTCP de 31 bits y k_e, k_s se reemplaza por la clave de sesión de cifrado SRTCP y sal.

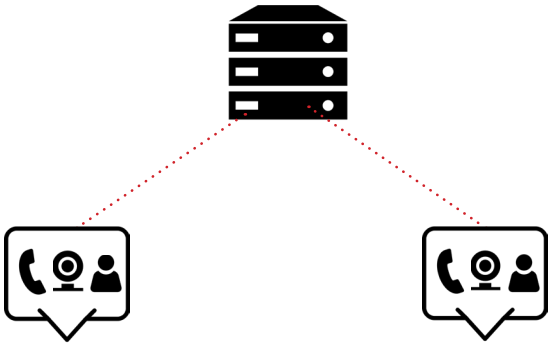
Hay que tener en cuenta que el valor inicial, IV, es fijo para cada paquete y se forma al “reservar” 16 ceros en los bits menos significativos para el propósito del contador. El número de bloques de flujo de claves generado para cualquier valor fijo de IV no debe exceder de 2^16 para evitar la reutilización de la secuencia clave, ver a continuación. El AES tiene un tamaño de bloque de 128 bits, por lo que 2^16 bloques de salida son suficientes para generar los 2^23 bits del flujo de claves necesarios para encriptar el paquete RTP más grande posible. Esta restricción en el tamaño máximo de bits del paquete que se puede encriptar garantiza la seguridad del método de cifrado al limitar la efectividad de los ataques probabilísticos.

## DERIVACIÓN DE CLAVES

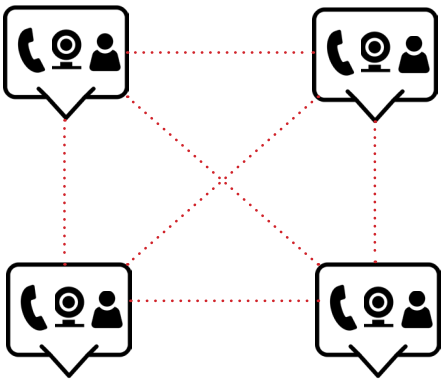
La derivación de claves reduce la carga en el establecimiento de la clave. Se necesitan hasta seis claves diferentes por contexto criptográfico (claves sal y claves de cifrado SKRTP y SRTCP, claves de autenticación SKRTP y SRTCP), pero se derivan de una sola clave maestra de una manera criptográficamente segura. Por lo tanto, el protocolo de administración de claves necesita intercambiar solo una clave maestra (más sal maestra cuando sea necesario), y luego el SKRTP mismo deriva todas las claves de sesión necesarias.

Múltiples aplicaciones de la función de derivación de claves brindarán beneficios de seguridad cuando estén habilitadas. Impiden que un atacante obtenga grandes cantidades de texto cifrado producido por una sola clave de sesión fija. En caso de que el atacante logre recopilar una gran cantidad de texto cifrado para una determinada clave de sesión, podría recibir ayuda al organizar ciertos ataques.

Las múltiples aplicaciones de la función de derivación de clave proporcionan seguridad tanto hacia adelante y hacia atrás en el sentido de que una clave de sesión comprometida no pone en peligro otras claves de sesión derivadas de la misma clave maestra. Esto significa que el atacante que pueda recuperar una determinada clave de sesión, de todos modos, no podrá tener acceso a los mensajes asegurados en claves de sesión anteriores y posteriores (derivadas de la misma clave maestra). (Tenga en cuenta que, por supuesto, una clave maestra filtrada revela todas las claves de sesión derivadas de ella.) Los documentos detallados y el código fuente se publicarán coincidiendo con el lanzamiento público de la cadena Skrumble Network.



Redes tradicionales con servidores centralizados



Decentralized network with no central server. Skrumble Network: Red descentralizada sin servidor central

## IDENTIFICACIÓN DE SESIÓN ÚNICA Y GESTIÓN DE DATOS UTILIZANDO LOS PROTOCOLOS DE LA RED DE SKRUMBLE

Skrumble Network será un ecosistema tecnológico habilitado por blockchain único en su especie que permite un ecosistema de comunicación completamente descentralizado y anónimo. Aprovechará los protocolos de comunicación en tiempo real sobre las conexiones entre pares utilizando cualquier navegador web moderno o las aplicaciones nativas de Skrumble Network (iOS, Android, PC y Mac).

Los protocolos de seguridad únicos de Skrumble Network se entregarán a través de un algoritmo derivado de clave patentado que utiliza la blockchain de Skrumble Network. Al unirse a la red, se les pedirá a los usuarios que ingresen la clave pública de la cartera donde guardan sus tokens de Skrumble Network. Además, se les pedirá que ingresen una contraseña segura y un seudónimo (nombre de usuario privado). Se usará una derivada de estos elementos para generar su ID de usuario única de Skrumble Network privada y una ID pública. Se generará un código QR y un enlace para compartir fácilmente la ID de red de Skrumble Network público de los usuarios.

Con una seguridad sin igual, las conversaciones se cifrarán usando una derivada de las claves de identificación de usuario privadas de Skrumble Network de cada participante como la clave inicial para el cifrado. El algoritmo derivado seleccionará aleatoriamente de las claves de red Skrumble Network asociadas en la sesión en función de los participantes involucrados, por lo tanto, no habrá dos claves iguales. Esto garantiza una capa adicional de seguridad, ya que no hay dos conversaciones que utilicen la misma clave, lo que hace que las conversaciones de Skrumble Network sean prácticamente imposibles de descifrar utilizando metodologías basadas en patrones. Por ejemplo, una combinación aleatoria de la clave privada ID de usuario Skrumble Network del usuario A y la clave ID de usuario privada Skrumble Network del usuario B se combinarán para formar la clave inicial de conversación y la ID de conversación.

Cuando se establece una comunicación entre los usuarios, la blockchain de Skrumble Network reemplazará el protocolo de enlace que ocurre en una red de comunicación tradicional. En la Red Skrumble Network, los mensajes del Protocolo de Descripción de Sesión (SDP) usarán la blockchain para establecer cada sesión, actuando como el saludo y la señal para que comience la comunicación, y el flujo del Protocolo de Transporte en Tiempo Real (RTP) para los multimedia (voz, video, mensaje, etc.) para comenzar la transmisión.

Una vez que se establece una conexión entre pares, las direcciones IP de los usuarios solo serán reveladas entre ellos y se establecerá una conexión websocket segura para abrir una sesión de comunicación interactiva entre los dispositivos de los usuarios para intercambiar datos en tiempo real de mensajes. transferencias de archivos y notificaciones. Esto permite que los datos se distribuyan de forma instantánea, lo que da como resultado una conexión de baja latencia.

Las comunicaciones en Skrumble Network serán P2P (Peer-to-Peer) y tendrán la capacidad de acceder a un puente de comunicación ad-hoc de alta capacidad para conferencias de voz y video para un mayor número de participantes.

Skrumble Network se construirá para operar en cualquier navegador moderno, además de funcionar como una aplicación independiente para la mayoría de los dispositivos móviles y tabletas (iOS y Android) y computadoras (Mac y PC). Las versiones de la aplicación independiente ofrecerán funcionalidades adicionales sobre la versión basada en el navegador.

## Skrumble Network AUTONICACIÓN DE LA LOS PROTOCOLOS DE COMUNICACIÓN BLOCKCHAIN

Skrumble Network desarrollará su propia blockchain que establece sesiones de comunicación ad-hoc únicas y seguras. La blockchain de Skrumble Network se utilizará en varios aspectos de la aplicación:

- Establecer la sesión de comunicación inicial.
- Sincronizar los seudónimos del usuario con la identificación de usuario de Skrumble Network.

Ambas funciones requerirán esfuerzos de minería para llegar a la validación y autenticación de consenso. Skrumble Network desarrollará un sólido programa de recompensa y extensión para incentivar a los anfitriones del servidor del nodo maestro, así como a su comunidad minera y socios para apoyar activamente el proyecto. Estas asociaciones ayudarán a garantizar que los tiempos de resolución de consenso de Skrumble Network estén optimizados.

## CAPACIDAD Y VELOCIDAD DE DATOS SIN IGUAL

Actualmente, cuando los usuarios realizan actividades utilizando aplicaciones existentes basadas en blockchain, se guardan y almacenan nuevas transacciones y datos. Cuantas más transacciones se guarden, menor será el tiempo de carga. Por ejemplo, una transacción financiera estándar en Ethereum generalmente necesita unos veinte segundos en llegar al consenso (Yannik, 2017). Con un aumento en el volumen de transacciones de comunicación, la necesidad de Skrumble Network de que cada mensaje, llamada, videollamada y transferencia de archivos se consideren como otra transacción reduciría el rendimiento de cada usuario. Por lo tanto, para aliviar este punto crucial, Skrumble Network utilizará el algoritmo de consenso Practical Byzantine Fault Tolerance (PBFT), para ofrecer un equilibrio entre el rendimiento y la escalabilidad. Para que las transacciones se resuelvan en tiempo real, Skrumble Network intentará lograr la configuración de la comunicación en menos de diez segundos, respaldado por esfuerzos de minería incentivados.

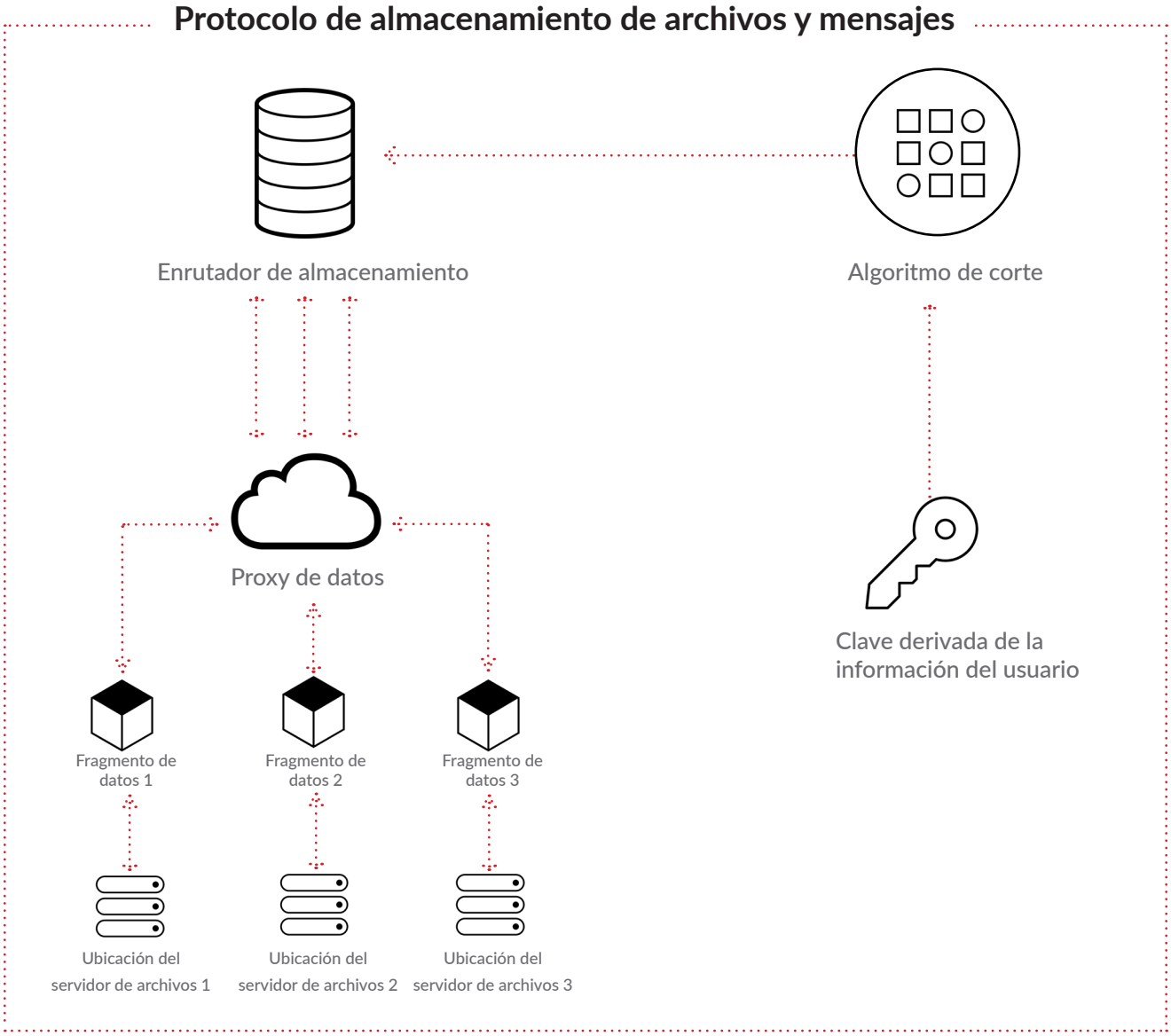
Para garantizar que Skrumble Network haya optimizado los tiempos de carga, estos protocolos se desarrollarán utilizando la tecnología de sharding. Mediante el uso de tecnología de sharding, Skrumble Network podrá dividir bases de datos muy grandes en partes más pequeñas, más rápidas y más fáciles de administrar. Cuando se necesitan datos, en lugar de cargar un solo registro a la vez, Skrumble Network se cargará como una base de datos en capas al extraer la información en piezas desde cada fragmento.

El equipo de Skrumble Network estará constantemente investigando y evaluando métodos nuevos y más rápidos de reducción de tiempos de carga de consenso y blockchain. El equipo se comprometerá a mejorar la red de forma continua para garantizar que la experiencia del usuario sea siempre sin interrupciones y sea consistente en la red Skrumble.

## LLAVES CIFRADAS EXCLUSIVAS PARA ALMACENAMIENTO DE ARCHIVOS EN RED DESCENTRALIZADA

Skrumble Network logrará un almacenamiento de archivos verdaderamente descentralizado utilizando un algoritmo que utiliza una identificación de sesión única y datos clave aleatorizados por usuario para garantizar que la información del archivo esté encriptada. Con este algoritmo, Skrumble Network puede garantizar la transferencia directa de archivos entre los usuarios y solo los usuarios que han participado en las conversaciones tendrán acceso permitido.

Skrumble Network empleará un novedoso método de estrategia de almacenamiento híbrido aún pendiente de patente . Este método fue creado y desarrollado por Skrumble Technologies Inc en 2015. Usando este enfoque híbrido, los archivos se cifrarán utilizando un algoritmo que se derivará de la ID de sesión única y su clave inicial. Una vez cifrados, los archivos individuales se dividirán en varios fragmentos, se distribuirán y almacenarán en servidores diferentes. Estos archivos solo se pueden volver a ensamblar con la clave adecuada. Por lo tanto, si se compromete cualquier servidor de archivos, los datos obtenidos serán ininteligibles, proporcionando además un almacenamiento de datos seguro para todos los usuarios.



Además, las características como el tiempo de almacenamiento y los tamaños de archivo permitidos vendrán determinados por el nivel de uso que el usuario haya desbloqueado en función de la cantidad de tokens de red Skrumble en su wallet.

## PUENTE DE COMUNICACIÓN DE ALTA CAPACIDAD

Para las conferencias de voz y video que contienen más de 6 participantes, se establecerán sesiones anónimas ad-hoc a través de puentes dedicados que se ubicarán en áreas estratégicas a nivel mundial y se autenticarán a través de la ID única de la sesión y la clave derivada. Skrumble Network utilizará un esquema de túnel IP a una dirección, cambiando aleatoriamente de un grupo muy grande, que solo se revela durante la conexión de socket segura entre los usuarios una vez que están conectados. Según el protocolo que se utiliza para conectarse al puente, los usuarios verificarán la conexión. Si no se establece, el usuario probará la siguiente dirección acordada. Estos protocolos permitirán una mayor escala en llamadas de voz, videoconferencias , mensajes, pantalla compartida, transferencias de archivos y notificaciones. El desbloqueo de funciones como la posibilidad de agregar un mayor número de participantes o el tiempo permitido, se determinará según el nivel de uso que el usuario haya obtenido, en función de la cantidad de tokens en su cartera.

## CARACTERÍSTICAS PRINCIAPELS Y ALMACENAMIENTO CONTROLADO POR EL USUARIO

Uno de los principales diferenciadores de Skrumble Network es la opción de guardar y almacenar mensajes grupales y entre pares. Los registros de conversación se almacenarán usando servidores en la nube. Solo los usuarios con la clave de conversación única (los que participaron en la conversación original) podrán acceder a la información guardada.

Cuando se crea un mensaje de grupo, el administrador de esa conversación tendrá la opción de guardar los registros. La funcionalidad de selección se desbloqueará basándose en el número de tokens en posesión. Cuando otros participantes intenten entrar en la conversación, serán notificados en primer lugar si el administrador ha optado por guardar la conversación, a lo que los participantes podrán negarse. En situaciones de conversación entre dos participantes, habrá un consentimiento mútuo. Cada participante necesitará aceptar el guardar la conversación para que el registro se guarde.

Además, Skrumble Network también presentará otras funcionalidades exclusivas, como un algoritmo único que crea claves de encriptación basadas en los participantes en una discusión, y otros factores, para diferenciar cada conversación. Con la intención de conectar a cualquiera en cualquier parte del mundo, los usuarios podrán crear fácilmente grandes comunidades de personas. Para mantener el protocolo de anonimato de Skrumble Network, los usuarios se registrarán usando un sistema de identificación pseudo anónima Los usuarios recibirán notificaciones cuando otros usuarios realicen capturas de pantalla en pantalla compartida o videollamada. Los usuarios tendrán acceso a grupos con chat de video en vivo, y a transferencias de datos y archivos encriptados, de forma descentralizada. Mediante la publicación de SDK de código abierto, Skrumble Network incentivará a los desarrolladores de terceros a construir nuevas tecnologías y aplicaciones utilizando las capacidades del ecosistema de comunicación segura, privada y anónima de la Blockchain de Skrumble.

## SKRUMBLE NETWORK: COMUNICACIONES GLOBALES, SIN FIREWALLS

Entre los numerosos beneficios de utilizar la plataforma de comunicación descentralizada, segura y anónima de Skrumble Network, también existen tres ventajas notables sobre las que merece la pena detenerse:

1. Skrumble Network no puede ser bloqueado por cortafuegos convencionales.
2. Skrumble Network tiene almacenamiento controlado por el usuario, y una vez borrado, los datos no pueden ser almacenados en ningún servidor.
3. Alto grado de encriptación en cada conversación, mensaje y archivo.

No habrá un punto a través del que se pueda bloquear, usando un firewall, porque cada usuario y conversación es distintiva y diferente. Esto asegura una anonimidad completa, y un acceso ilimitado a Skrumble Network desde cualquier parte del mundo. Las jurisdicciones sin acceso a Internet serán las únicas que no puedan participar.

# AFILIACIÓN DEL TOKEN UTILITARIO DE SKM: IMPULSANDO LAS COMUNICACIONES DE SKRUMBLE NETWORK

SKM es un token de utilidad que ofrecerá un cierto tipo de afiliación según el número de tokens que el usuario posea. Estos privilegios de afiliado permitirán el acceso a distintas características y acciones en el ecosistema de Skrumble Network. El uso inicial será gratuito, y el token servirá como medio de acceso para desbloquear características premium, niveles de afiliación o utilizar varias funcionalidades adicionales.

**Ejemplos de uso del token de utilidad SKM**

l usuario A en Canadá quiere comenzar una videollamada con el usuario B en Tailandia. La llamada de vídeo podría ser una función premium. El usuario A y el usuario B necesitarían tener en posesión el número establecido de tokens de utilidad SKM para realizar la llamada de video solicitada.

El usuario A en Francia quiere enviar un archivo al usuario B en Brasil. El archivo excede los requisitos iniciales de tamaño de archivo permitido. El usuario A debe poseer una determinada cantidad de tokens para enviar un archivo de mayor tamaño del que permite su acceso actual.

Usuario A en Colombia que desea seleccionar guardar una conversación que está a punto de tener con el usuario B en Australia. El almacenamiento de registros controlados por el usuario podría ser una función premium. El usuario B ha confirmado que participarán en una conversación guardada. Ambos usuarios pueden necesitar un token para el almacenamiento.

El usuario A en Alemania quiere enviar un archivo al usuario B en los Estados Unidos, pero el usuario A no quiere que el usuario B comparta el archivo con nadie. El usuario A posee una cierta cantidad de token y recibirá una notificación si se transfiere el archivo.

El usuario A en Finlandia quiere enviar un archivo al usuario B en Escocia usando una clave de acceso restringido para que solo el usuario B pueda acceder al archivo. El usuario A posee una cierta cantidad de tokens, el usuario B envía el archivo en pedazos y solo la clave de acceso dada al usuario B del usuario A puede desbloquear el archivo.

## Recompensas de usuario: Sorpresa y deleite

• Los miembros activos de la comunidad recibirán recompensas de tokens sorpresa de acuerdo con ciertos criterios. Por ejemplo, un miembro que ha inicializado una cierta cantidad de conversaciones recibirá una cantidad adicional de tokens.
• Habrá recompensas en forma de airdrop al azar para que los grupos promuevan a los contribuyentes de la comunidad.
• Aquellos que ayudan a minar, autentificar y promover la comunidad de la red también tendrán oportunidades de recibir recompensas.

## CONSTRUYENDO UN ECOSISTEMA AUTOSUFICIENTE

Al ofrecer nuestros SDK de código libre y documentación de productos con diversas funciones (API abierta), muchas industrias y entornos diferentes, como empresarios, desarrolladores y miembros de la comunidad, pueden aprovechar la tecnología de comunicación descentralizada única de Skrumble Network para brindar servicios a la vertical que elijan.

FASE 1: INICIATIVAS DE LABORATORIO: INCUBADORA

Durante la fase inicial del proceso del ecosistema, Skrumble reunirá a entre 2 y 3 socios estratégicos iniciales para mantener una incubadora. Los participantes realizarán una lluvia de ideas y crearán adiciones sobre Skrumble Network, como Freelance Marketplace y Showrooms virtuales, para crear un ecosistema autosostenible.

FASE 2: SDKS de CÓDIGO LIBRE & API

La segunda fase incluirá la publicación de los SDK de código abierto y la API con acceso abierto para que cualquiera pueda utilizar la documentación para crear su propio producto o servicio sobre la red Skrumble.

El token de SKM será utilizado por todos los usuarios a través de las diferentes aplicaciones dentro del ecosistema de Skrumble Network y aquellas aplicaciones construidas por separado. Estas diversas aplicaciones también serán incentivadas por sus ofertas a través de tokens SKM. Por lo tanto, el ecosistema se volverá sostenible a través de un sistema innovador de desarrollo de plataforma, coste y recompensa.

# SKRUMBLE NETWORK FOUNDATION ROADMAP

**2014**

Fundación de Skrumble

**2015**

Registro de patentes a nivel global

**2016**

Q1: Lanzamiento en beta del producto UC

**2017**

Q2: Lanzamiento del producto UC

Q4: Lanzamiento de un mercado con una API abierta

**2018**

Lanzamiento de los tokens de Skrumble Network

Lanzamiento del MVP - Mayo

Q4: Lanzamiento de la versión beta de la red Skrumble

**2019**

Q1: Lanzamiento de la versión 1 de la red

Q3: Primeros gran grupo de asociados del ecosistema

Q4: Lanzamiento del ecosistema blockchain de Skrumble

# BENEFICIOS DE USAR SKRUMBLE NETWORK

- Privacidad
- Servidores descentralizados
- Almacenamiento c ontrolado por el usuario
- API abierta
- Seguridad
- Encriptado
- Transferencia segura de archivos
- Sin rastreo
- Anonimato
- Conexión global
- Notificaciones de capturas de pantalla
- Sin posibilidad de ser bloqueada

# USOS DE SKRUMBLE NETWORK

## 1. GUARDAR Y BORRAR MENSAJES

Aunque los usuarios utilizarán Skrumble Network para tener conversaciones privadas, seguras y anónimas, es necesario que exista la posibilidad de guardar y almacenar el historial de conversaciones. Esto puede incluir mensajes, historial de llamadas, y almacenamiento de archivos. Durante conversaciones entre pares, los usuarios necesitarán del consentimiento mútuo para aprobar que las conversaciones sean guardadas. En conversaciones grupales, el administrador elegirá si quiere guardar o no los mensajes, y los otros participantes podrán entonces aceptar o rechazar el almacenamiento de los datos. Si la elección es no guardar nada, ningún dato será almacenado en la red descentralizada. Si por el contrario, se elige guardar, la información será almacenada en el sistema en la nube patentado por Skrumble, y los datos serán accesibles únicamente para los participantes en la conversación.

## 2. TRANSFERENCIAS SEGURAS DE ARCHIVOS

Skrumble Network tiene como objetivo proporcionar a los usuarios de espacio para compartir sus propios datos y enviar archivos de forma segura y encriptada. Los usuarios podrán enviar archivos usando una clave de acceso restringido, lo que significa que los archivos se enviarán en trozos de un usuario a otro. Al usuario que recibe el archivo se le dará un código de acceso secreto para desbloquear el contenido y volver a unir el archivo en una sola pieza. Los usuarios también podrán poner notificaciones en los archivos que envíen. Esto es para asegurar que si el archivo que no quieren que otros descarguen o transfieran a otra conversación es enviado o descargado, puedan recibir una alerta inmediatamente.

# AÑADIDOS AL ECOSISTEMA SKRUMBLE NETWORK

Los tokens SKM serán consumidos y usados por los usuarios en diferentes aplicaciones vía la red de Skrumble Network. Las variadas aplicaciones también serán incentivadas por lo que ofrece los tokens SKM. Por lo tanto, El ecosistema será autosustentable por la innovación y el desarrollo de la plataforma, el costo y el sistema de premiación.

Las siguientes aplicaciones iniciales están siendo planeadas para ser lanzadas vía Skrumble, Skrumble Labs Incubation Program y otras plataformas terciarias:

## 1. PASARELAS DE PAGO SEGURAS Y EN CONTEXTO

La mayoría de las pasarelas de pago son complicadas, requieren de un alto grado de pericia técnica para ser montadas, e implican una aplicación o formato separado y no relacionado con lo demás. Skrumble Network incluirá un sistema de pago dentro de la propia aplicación, con encriptación de extremo a extremo, ya sea a través de transferencias de dinero entre pares dentro de una conversación, pagos de comercio electrónico sin salir de la página o simplemente métodos de comunicación como mensajes privados, llamadas y archivos.

## 2. MERCADO DE FREELANCERS

En los últimos años, se ha incrementado el número de plataformas de Internet centradas en la idea de contratos temporales a freelancers, por un tiempo limitado de trabajo y un salario fijado. Skrumble Network tiene las funcionalidades necesarias en cuanto a comunicación y transacciones para construir un mercado de freelancers a través de los contratos inteligentes. Las partes interesadas pueden elegir un freelancer, establecer los parámetros del trabajo, y esa persona será pagada si cumple con los requisitos establecidos en el contrato.

## 3. CONTRATOS INTELIGENTES DENTRO DE LA CONVERSACIÓN

Los contratos inteligentes son vitales para realizar transacciones y cerrar negocios de forma remota. Skrumble Network está preparada para albergar plantillas de contratos inteligentes para que los usuarios rellenen y firmen durante sus conversaciones y transacciones. , ya sea para aceptar los términos de servicio para abogados y clientes, documentar las expectativas del proyecto para trabajadores remotos, contratar a un freelancer del mercado independiente mencionado anteriormente, o cualquier tipo de transacción que requiera la aprobación de las partes interesadas. Se establecen los términos, el contrato inteligente se firma en la conversación y cuando se completa la asociación, cada parte recibe lo que se prometió en el contrato.

## 4. SALAS VIRTUALES

Utilizando capacidades de video, mensajería y presentación, Skrumble Network puede personalizar fácilmente esta funcionalidad para incluir puntos P2P simples o de interacción grupal. Estos puntos de contacto servirán para proporcionar a los usuarios una plataforma para transmitir videos en vivo, compartir talentos y recibir pagos por su contenido dentro de la conversación.

## 5. ASOCIACIONES TECNOLÓGICAS

Para mejorar aún más la funcionalidad y las ofertas del ecosistema de Skrumble Network, Skrumble se asociará con líderes clave en las industrias de blockchain y criptomonedas. Alinearse con proyectos y personas influyentes de la industria, como el ecosistema de Aion Network y sus soluciones de pago, puede enriquecer las oportunidades para los usuarios de la red Skrumble e incentivar aún más a los propietarios del utility token.

# CONCLUSIÓN: REVELAR UN LADO MÁS HUMANO Y CONECTADO AL BLOCKCHAIN

La tecnología blockchain resuelve un montón de problemas serios. Las criptomonedas promueven las instituciones financieras transfronterizas y el comercio sin fuertes comisiones bancarias, y los contratos inteligentes garantizan que a los profesionales sean pagados por los servicios prestados y que se pueda acceder a los datos en tiempo real para rastrear la transferencia y propiedad de los bienes. Debido a indiscutibles cualidades como altas medidas de seguridad, gestión de datos y oportunidades de comunicación, una red descentralizada es un catalizador esencial para una comunicación más segura.

Blockchain combina la seguridad de la criptografía y el almacenamiento y transmisión de datos únicos, con redes peer-to-peer para crear una base de datos descentralizada y confiable. Las principales preocupaciones sobre ciberseguridad, almacenamiento de datos y amenazas a la información del usuario que involucran sistemas de comunicación basados en Internet se vuelven prácticamente irrelevantes con el uso de un libro contable distribuido. Más allá de resolver estos problemas, el blockchain representa una oportunidad incomparable para la innovación. Desde descubrir nuevos métodos de pago dentro de las aplicaciones hasta crear nuevas formas de establecer conexiones para que personas de todo el mundo puedan comunicarse.

La descentralización presenta infinitas posibilidades de innovación y ofrece una solución para una red unificada y segura que proporciona cifrado de extremo a extremo, completo anonimato y nuevas oportunidades de comunicación para permitir que el mundo se conecte, comparta y crezca.

La red de Skrumble Network tendrá la habilidad de conectar a cualquiera desde cualquier parte del mundo, de un modo seguro y simple, con el potencial de democratizar completamente los sistemas de comunicación a escala global. Usar la blockchain para establecer comunicaciones de esa manera nunca se ha hecho antes. Skrumble Network transformará el uso de la tecnología blockchain de las transacciones financieras a la capacidad de ser un componente integral de cualquier aplicación. Con una comunicación descentralizada confiable y de fácil acceso, las personas de todo el mundo tendrán la oportunidad de recuperar la propiedad de los datos, no volver a preocuparse por su seguridad y participar activamente en las diferentes comunidades en un entorno basado en el consenso, y en una tecnología que puede revolucionar el mundo.

# SOBRE SKRUMBLE TECHNOLOGIES INC

Lanzado en 2014, Skrumble Technologies Inc se ha convertido en una empresa de comunicación en la nube bien establecida en la industria. Con más de 30 patentes globales, Skrumble aprovecha su tecnología exclusiva para crear soluciones confiables para compañías de Fortune 500, firmas de consultoría en TIC, centros de llamadas, servicios profesionales, fuerzas policiales, compañías de seguridad, gobiernos, empresas remotas, desarrolladores y muchos más. Más de 400,000 usuarios han aprovechado las diversas soluciones tecnológicas y de comunicación de Skrumble. La misión de Skrumble es innovar en los métodos de comunicación y crear oportunidades para que las personas se conecten globalmente en las plataformas más seguras posibles. Skrumble tiene cuatro soluciones principales de comunicación. Una plataforma de comunicación unificada lanzada en la primavera de 2017, documentación del producto publicada y una potente API abierta para que los desarrolladores programen funciones de comunicación en cualquier aplicación, una solución de comunicación personalizada de marca blanca para que las empresas de asistencia sanitaria, derecho, consultoría y más tengan sus propias plataformas de telecomunicaciones, y un nuevo widget recientemente lanzado para que los desarrolladores incorporen chat, voz y video directamente en cualquier sitio web o plataforma.

El equipo Skrumble continúa levantando las barreras de comunicación e innova soluciones para que las empresas de todo el mundo se unan y crezcan. Skrumble Technologies Inc proporcionará desarrollo, experiencia en blockchain y licencias tecnológicas para impulsar Skrumble Network. Skrumble Network se centrará en tecnologías de comunicación descentralizadas y en la construcción y el fomento de la comunidad de redes. Skrumble cree que con una verdadera autonomía y propiedad de los datos, se puede generar confianza y desbloquear las enormes oportunidades de una verdadera red global.

# NUESTRAS OFICINAS

Oficina de Desarrollo de Negocios de Toronto

Oficina de Operaciones en Tecnología de Toronto

Oficina de ventas de América Latina

# CONOCE A LOS MIEMBROS CLAVE DE LA COMUNIDAD

David Lifson
CEO y Presidente

Tamir Wolfson
Vice presidente ejecutivo

Vivi Herlick
Vice presidente de operaciones

Eric Lifson
Cofundador, Marketing

Christine Guo
Vice presidente de desarrollo corporativo

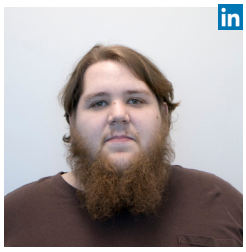
Johnathan Dwek
CFO - CFA

Aleksandra Mihajlovic
Director de producto

Michael Dabydeen
Lead Developer

Mikhail Khoroshun
Desarrollador Front-End

Mikhail Berezovskiy
Desarrollador Front-End



Daniel Audino
Desarrollador Full Stack

Danyi Lin
Desarrollador Full Stack

Mauricio Bertanha
Desarrollador Full Stack

Matt Mollon
Desarrollador Full Stack

Leah Williams
Desarrollador Full Stack

Chantale Barnard
Desarrollador Full Stack

Eric Eddy
Desarrollador en móviles

Akash Patel
Desarrollador en móviles

Gabriel Hernandez
Desarrollador en móviles

Arnaud Ladoucetter
Desarrollador en móviles

Siv Sathiyaseelan
Analista de calidad

Avenson Navalta
Diseñador de interfaz y experiencia

Shelby Pearce
Coordinadora de marketing

Wendy Lu
Coordinadora de marketing digital

Wei Chen
Representante del desarrollo del negocio

LEA ESTA SECCIÓN DE AVISO LEGAL DETENIDAMENTE. SI TIENE ALGUNA DUDA EN CUANTO A LA ACCIÓN QUE DEBERÍA TOMAR, DEBE CONSULTAR A SUS ASESORES LEGALES, FINANCIEROS, DE IMPUESTOS U OTROS PROFESIONALES.

La información presentada en este documento puede no ser exhaustiva, y no implica ningún elemento de una relación contractual. Toda la información está sujeta a futuros cambios o actualizaciones sin previa notificación, y de ninguna manera constituye asesoramiento profesional. Skrumble Technologies Inc., sus subsidiarias y afiliadas, no garantizan ni aceptan ninguna responsabilidad legal que surja de, o esté relacionada con, la precisión, fiabilidad, vigencia o integridad de cualquier material contenido en este documento.

Los tokens de SKM no están destinados a constituir securities en ninguna jurisdicción, pero pueden ser considerados como tal por los reguladores en ciertas jurisdicciones. Este documento no constituye una oferta de venta - o una solicitud de una oferta de compra- de tokens de SKM en ninguna jurisdicción en la que sea ilegal realizar dicha oferta o solicitud. Los residentes de Canadá y los residentes o titulares de la tarjeta verde en los Estados Unidos están excluidos de la compra de tokens SKM, salvo en conformidad con las exenciones aplicables a dichos requisitos de la ley de valores. Cualquier oferta o solicitud relacionada con los tokens de SKM se realizará solo a través de un memorando de oferta confidencial y de acuerdo con los términos de los valores aplicables y otras leyes. Skrumble Technologies Inc., sus subsidiarias y afiliadas no brindan ninguna opinión con respecto a la compra, venta u otra distribución de los tokens de SKM, y los lectores de este documento no deberían usarlo para formar la base o confiar en él antes de ingresar en cualquier contrato o tomar una decisión de inversión.

# REFERENCIAS


Cendrowski, Scott (April 14, 2017). Fortune Magazine. China's WeChat is a censorship juggernaut. Retrieved on January 26, 2018 from http://fortune.com/2017/04/14/china-wechat-tencent-censorship-709-crackdown/

Coin Market Cap (2018). Cryptocurrency Market Capitalizations. Retrieved on January 21, 2018 from https://coinmarketcap.com/all/views/all/

CyberScout (December 27, 2017). Identity Theft Resource Center. Data Breach Reports. Retrieved on January 24, 2017 from https://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

Facebook (2018). Making ads better and giving your more control. Retrieved on January 26, 2018 from https://www.facebook.com/help/585318558251813?ref=notif&notif_t=oba

Google (2018). How Ads Work. Retrieved on January 26, 2018 from https://privacy.google.com/how-ads-work.html

Greenberg, Andy (January 10, 2018). Wired. WhatsApp security flaws could allow snoops to slide into group chats. Retrieved on January 25, 2018 from https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/

Hollerith, David (November 6, 2017). Bitcoin Magazine. Survey polls American awareness of cryptocurrencies and ICOs. Retrieved on January 20, 2018 from https://bitcoinmagazine.com/articles/survey-polls-american-awareness-cryptocurrencies-and-icos/

Martin, Ellen (October 2017). The Next Web. Why more people will use blockchain-based payment platforms over banks in the future. Retrieved on January 18, 2018 from https://thenextweb.com/contributors/2017/09/07/blockchain-vs-banks/

Pascual, Al, Marchini, Kyle & Miller, Sarah (February 1, 2017). 2017 Identity Fraud: Securing the Connected Life. Retrieved on January 20, 2018 from https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

Perlroth, Nicole & Haag, Matthew (April 29, 2017). The New York Times. Hacker leaks episodes from Netflix show and threatens other networks. Retrieved on January 24, 2018 from https://www.nytimes.com/2017/04/29/business/media/netflix-hack-orange-is-the-new-black.html

Pullen, John Patrick (November 21, 2017). Fortune Magazine. Jennifer Lawrence reveals why she didn't sue Apple over her nude photo leak. Retrieved on January 24, 2017 from http://fortune.com/2017/11/21/jennifer-lawrence-apple-lawsuit-nude-photo-leak/

Sabin, Dyani (January 3, 2018). Futurism. Everything you need to know about cryptocurrency and why it's the future of money. Retrieved on January 17, 2018 from https://futurism.com/cryptocurrency-future-money-bitcoin/

Sethi, Rahul (September 26, 2017). After Google and Facebook, WhatsApp banned in China. Retrieved on January 26, 2018 from https://www.indiatoday.in/technology/news/story/after-google-and-facebook-whatsapp-banned-in-china-1052534-2017-09-26

Sherr, Ian (March 23, 2018). CNET. Facebook, Cambridge Analytics and data mining: What you need to know. Retrieved on March 26, 2018 from https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/

Toronto Star (January 13, 2018). World News. As protests wane, Iran lifts ban on messaging app Telegram. Retrieved on January 24, 2018 from https://www.thestar.com/news/world/2018/01/13/as-protests-wane-iran-lifts-ban-on-messaging-app-telegram.html

WeChat (2018). WeChat Help Center. Why doesn't my prior chat log appear when I log in to WeChat from a new device? Retrieved on January 26, 2018 from https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?t=help_center/topic_detail&opcode=2&id=1208117b2mai1410242meeYj&lang=en&plat=android&Channel=helpcenter

Yannik (June 26, 2017). Updated January 9, 2018. How long do Ethereum transactions take? Retrieved on February 1, 2018 from https://support.metalpay.com/hc/en-us/articles/115000373814-How-long-do-Ethereum-transactions-take-