



---

# WHITEPAPER V1

———— 27th June 2017 ————

## ÍNDICE

<b>INTRODUCCIÓN</b>	3
<b>LA RED INCENTIVIZEDNODE</b>	4
<b>¿CÓMO SON RECOMPENSADOS LOS INCENTIVIZEDNODES?</b>	4
<b>ORGANIZACIÓN DE LOS INCENTIVIZEDNODES</b>	5
<b>SISTEMA COLATERAL</b>	5
<b>MECANISMOS DE CONTROL Y EQUILIBRO DE LA RED</b>	5
<b>PROCEDIMIENTOS DE INCENTIVIZEDNODE</b>	6
<b>UBICACIÓN DE LOS INCENTIVIZEDNODES ACTIVOS</b>	6
<b>VELOCIDAD DE TRANSACCIÓN Y ESCALABILIDAD</b>	6
<b>MINADO</b>	7
<b>REMUNERACIÓN E IMPLEMENTACIÓN</b>	7
<b>GOBERNANZA Y FINANCIACIÓN</b>	7
<b>¿QUÉ ES EL AUTOGOBIERNO?</b>	8
<b>¿QUÉ ES LA AUTOFINANCIACIÓN?</b>	8
<b>PROBLEMAS DE FUNGIBILIDAD</b>	8
<b>LA SUPERIOR PRIVACIDAD DEL SISTEMA DE PRUEBA DE CONOCIMIENTO NULO</b>	9
<b>COMPRENDIENDO ZK-SNARKS</b>	9
<b>LAS CAPAS DE LA RED STASH</b>	10
<b>TRANSACCIONES INSTANTÁNEAS</b>	10
<b>TOKENS DE STASH Y OFERTA DE CRIPTOMONEDA STASH</b>	11
<b>OFERTA DE MINADO DE STASH</b>	11
<b>MAPA DE OBJETIVOS DE STASH</b>	11-13

 **STASH** LA PRÓXIMA GENERACIÓN EN CRIPTOMONEDAS

## INTRODUCCIÓN

Stash es una moneda criptográfica de software libre que combina muchas de las innovaciones de protocolo de Bitcoin, Dash y Zcash mientras que soluciona muchos de los problemas experimentados por las monedas digitales. Las distintas criptomonedas poseen atributos diversos y valiosos, pero a su vez enfrentan problemas particulares. Estos problemas incluyen velocidades de transacción demasiado lentas, costos de transacción altos, poca capacidad de escalar, un inicio lento, falta de privacidad, un sistema de gobernanza impráctico, la necesidad de financiamiento continuo y de brindar adecuados incentivos a los usuarios. El objetivo de Stash es lograr combinar muchas de estas tecnologías de última generación de las criptomonedas y construir sobre la base de la ya probada tecnología blockchain para poder solucionar o eliminar los problemas enfrentados. Esto a su vez permitirá crear una criptomoneda que es increíblemente útil y atractiva tanto para usuarios finales como para inversores de largo plazo.

Actualmente se ha planteado que nuevas características serán desarrolladas internamente y, a su vez, tercerizadas al resto de los miembros de la comunidad crypto, a medida que nuevas innovaciones se vuelven disponibles y que la red Stash decida que estas sean implementadas para mejorar la utilidad de Stash como dinero digital

En vez de ser una idea rígida e inmóvil, Stash es una moneda digital que evolucionará orgánicamente a través de la ayuda de su comunidad. Para tal fin Stash ha iniciado una venta de tokens para obtener recursos, aumentar su exposición y atraer talentosos desarrolladores de todo el mundo para ayudar a crecer e innovar.

Se ha progresado y los recursos obtenidos con la venta de los tokens han ayudado a incrementar y mejorar el desarrollo de la privacidad de la criptomoneda Stash, mediante el uso de redes de seguridad de prueba de conocimiento nulo (ZSL). El uso de ZSL en Stash será para establecer transacciones en la blockchain de un modo anónimo. Los dueños de los tokens de Stash podrán usar sus tokens para comprar la criptomoneda Stash a un cambio de 1 a 1 una vez que la integración ZSL haya finalizado. Todos los tokens Stash serán destruidos una vez que sean usados para adquirir la criptomoneda Stash.

Mientras que los fondos obtenidos de la venta de tokens proveerán el capital requerido para implementar el ZSL, el sistema de presupuesto y tesoro de Stash se asegurará que el proyecto continúe teniendo los fondos adecuados una vez que los fondos de la venta de tokens ya hayan sido utilizados. Para tal fin se financiará mediante recompensas de bloques mensuales.

Stash siempre se propondrá evolucionar y adaptar, siendo flexible, ágil y abierta a las nuevas oportunidades que surjan. Para esto el sistema de gobernanza de Stash ha sido establecido para poder adaptarse y aprovechar las nuevas oportunidades una vez que estas se han vuelto visibles. Por ende, el sistema de gobernanza no tendrá que lidiar con los problemas de decisiones que son claramente evidentes en otras criptomonedas.

El objetivo final de Stash es simple: ser la criptomoneda más útil y con la interfaz más amigable tanto para usuarios comunes como para transacciones internacionales.

## RED INCENTIVIZEDNODE

Los nodos completos son necesarios para que una criptomoneda pueda operar. Estos operan

en redes P2P y envían las actualizaciones de los eventos importantes de la red a los peers. Sin embargo, para poder ser efectivos, los nodos requieren de altos volúmenes de tráfico, así como recursos adicionales, por lo que conlleva a costos significativos.

Esto puede traer como consecuencia una disminución continua de los nodos completos, tal como se ha presenciado con la red Bitcoin. El resultado de esto es una notoria caída en el rendimiento, con tiempos de propagación de bloques que superan los 40 segundos.

Para evitar esta situación la criptomoneda Stash utiliza una red secundaria que funciona como una red de apoyo, lo que garantiza un mejor rendimiento por más tiempo. Esta es la red Incentivizednode de nodos que están ampliamente disponibles y que deben proveer un estándar mínimo de servicio para calificar al programa de recompensas e incentivos de Incentivizednode.

## ¿CÓMO SON RECOMPENSADOS LOS INCENTIVIZEDNODES?

El programa de recompensas de Incentivizednode sirve para promover la red, aumentando la cantidad de nodos completos que están en funcionamiento en todo momento. Sin tal programa, los usuarios de la red deberán pagar los costos de un nodo completo a medida que el tráfico aumenta y esto, a su vez, puede traer mayor inestabilidad.

La gran diferencia que posee la red Incentivizednode es que los nodos individuales están asociados a un nivel específico de servicio que está asegurado por un sistema colateral. Este sistema colateral permanece protegido mientras la red Incentivizednode se encuentre en funcionamiento, lo que promueve la estabilidad de toda la red y les da a los usuarios de Incentivizednode la oportunidad para ganar monedas digitales Stash adicionales.

Estos pagos son el producto de las recompensas acumuladas de la red, siendo alrededor del 45% de los dividendos pagos a los Incentivizednodes que cumplan con el nivel de servicio requerido. De todos modos, habrá una cierta fluctuación en la cantidad total disponible para pagos diariamente, debido a que los porcentajes destinados al sistema de recompensas de Incentivizednode serán fijos, pero el número de nodos será variable. (De la misma forma que se ajustan los porcentajes del Programa de Recompensas Incentivizednode). El pago por día de un Incentivizednode es entonces calculado de la siguiente manera

$$n * r * s / t$$

En donde

$n$  = Bloques por día

$r$  = Recompensa por bloque

$s$  = parte de Incentivizednode de cada recompensa de bloque

$t$  = número total de Incentivizednodes

Para calcular los pagos de recompensas de cada Incentivizednode se usa la siguiente formula  
Tasa de beneficio sobre inversión por Incentivizednode =  $(n * r * s) / t * 365.25 / 10,000$

Donde 10,000 = es la cantidad de Stash colateral para poder manejar un Incentivizednode

Debido a que hay una cantidad limitada de la criptomoneda Stash y hay un costo inherente en el manejo de un Incentivizednode, hay un límite de cuantos Incentivizednodes pueden estar en funcionamiento en un determinado momento. Este límite está basado en los 500 millones

de Stash generados en la venta de tokens y a esto se la agrega todos los Stash que se hayan minado desde el lanzamiento de la Blockchain de Stash.

## **ORGANIZACIÓN DE LOS INCENTIVIZEDNODES**

Un algoritmo basado en el hash del minado de bloques es usado para que Incentivizednodes funcionen de un modo semi-aleatorio y determinístico. La red de minado asegura esta funcionalidad mediante el uso del hash como prueba de trabajo para cada bloque.

## **SISTEMA COLATERAL**

Es vital para la seguridad del sistema que ningún individuo o entidad obtenga el control de la totalidad de la red de Incentivizednodes. Para evitar esto, el anteriormente mencionado sistema colateral ha sido implementado, para que obligue a quien quiera controlar un Incentivizednode activo a depositar 10.000 Stash.

La oferta limitada de Stash significa que el precio responde directa y rápidamente a la demanda. Para obtener un control significativo de la red Incentivizednode, un individuo tendría que adquirir una vasta cantidad de Stash en un libre mercado, lo que dispararía el precio y haría imposible continuar con la adquisición.

Esto permite a la red Stash utilizar la segunda capa de la red Incentivizednode para llevar a cabo tareas críticas. No se entrega toda la responsabilidad y confianza a un solo nodo o grupo de nodos, y nadie es capaz de controlar la red para sus propios fines debido a que los Incentivizednode son elegidos aleatoriamente para realizar la misma tarea al mismo tiempo.

## **MECANISMOS DE CONTROL Y EQUILIBRO DE LA RED**

El rol de un Incentivizednode no está solo limitado a transferir y validar transacciones. Hay otras tareas, de alta importancia y alto valor, que estos nodos pueden realizar. Por ende, es fundamental que la red pueda determinar qué Incentivizednodes se encuentra en línea, cuáles están respondiendo y cuáles se están comportando de acuerdo a los estándares establecidos.

Esto requiere una prueba de servicio. No es suficiente determinar cuáles Incentivizednodes están funcionando, sino que también un determinado nivel de servicio debe ser mantenido. Para lograr esto, Incentivizednode utiliza Quoroms; dos Quoroms son elegidos por cada bloque, por ejemplo, Quorum A analiza el nivel de servicio del Quorum B. Quorum A está compuesto de los nodos más cercanos al hash del bloque actual, mientras que Quorum B está compuesto de los bloques más lejos al hash del bloque actual.

De esta manera el sistema no necesita confianza, ya que los nodos son seleccionados aleatoriamente usando el sistema Quorum que logra hacer que la red se autoevalúe.

## **PROCEDIMIENTOS DE INCENTIVIZEDNODE**

La función básica de un Incentivizednode es simplemente transferir y validar las transacciones. Un nodo solo requiere de dos mensajes de protocolo para ser activo en la red Stash. Estos dos mensajes son el anuncio del Incentivizednode y el mensaje de ping del Incentivizednode.

El protocolo de anuncio del mensaje de es usado para anunciar la presencia del nodo a la red cuando este se activa. Siguiendo esto el mensaje de protocolo del ping será enviado cada 15 minutos como parte de la prueba de servicio. Si tales mensajes no son enviados a una tasa satisfactoria, el nodo será desactivado. Adicionalmente, el nodo debe tener sus puertos abiertos para recibir pings, de lo contrario, se lo considerará inactivo.

En la práctica, sin embargo, la función es más compleja y se sirve de protocolos adicionales, incluyendo PrivateSend e InstantSend, ambos usados para chequear la prueba de servicio.

Un Incentivizednode se vuelve activo cuando su usuario envía 10.000 unidades de Stash a una dirección de monedero designada en la red. Una vez que esta acción es confirmada el nodo podrá usar sus mensajes de anuncio y de ping para propagarse por la red.

La red incluye medidas de seguridad internas mediante el uso de un sistema físico para prever actividad maliciosa en el sistema. Por ejemplo, si un Incentivizednode envía una llave privada en un mensaje tras la activación y si este es usado por una segunda máquina, el sistema desactivará al primer nodo, protegiendo los 10.000 Stash de ser robados.

Las 10.000 criptomonedas Stash del sistema colateral no necesitarán ser depositadas en el monedero Incentivizednode pero en cambio serán depositadas en una ubicación remota y segura para proteger a las criptomonedas del sistema colateral de ser robadas.

## **UBICACIÓN DE LOS INCENTIVIZEDNODES ACTIVOS**

Si la red Stash desea ser exitosa, los nuevos usuarios deben poder entender de un modo fácil y rápido qué Incentivizednode está activo actualmente. Para lograr esto, los usuarios recibirán una lista de los Incentivizednodes y su estado cada vez que se unan a la red. Una vez recibida la lista, esta será almacenada en el cache del usuario para que cada vez que reinicie la red no tenga que solicitarla y pueda verla nuevamente.

## **VELOCIDAD DE TRANSACCIÓN Y ESCALABILIDAD**

Mediante la implementación de tiempos de bloque de 150 segundos y una capa secundaria de Incentivizednode, la red es capaz de manejar bloques de hasta 20 megabytes, Stash tiene 80 veces la capacidad de transacción de Bitcoin y como resultado las tarifas por transacción son de menor coste. Esto también significa que Stash no tendrá problemas de capacidad en el corto plazo lo que le permitirá al equipo de Stash continuar desarrollando e implementando mejoras a la red Stash con mayor tiempo.

## MINADO

En la red Stash, hay problemas criptográficos complejos que deben ser solucionados para asegurar un bloque en la Blockchain. Este procedimiento es conocido como minado y la red Stash recompensará a los usuarios que minen con criptomonedas Stash.

Para asegurar los bloques en la Stash Blockchain, proponemos que los mineros encuentren soluciones al algoritmo X11, esto puede ser logrado con distintos hardware, incluyendo los procesadores básicos encontrados en laptops y pc de escritorio.

Los procesadores modernos son bastante poderosos, pero están diseñados para fines diversos. Esta versatilidad de hecho es una desventaja al momento de minar, ya que el minado requiere de calcular un alto número de vectores al mismo tiempo.

Un procesador común (CPU) puede ser mejorado usando AES o AVX, haciéndolo más especializado para la minería. Las tarjetas de video (GPU) en cambio ofrecen un rendimiento superior debido a sus varios canales para los cálculos predecibles en la minería. Finalmente, los ASIC, que son especialmente diseñados para un alto rendimiento en un tipo particular de algoritmo son superiores tanto a los procesadores como tarjetas gráficas.

## REMUNERACIÓN E IMPLEMENTACIÓN

La red Stash está establecida para asegurar que cada Incentivizednode reciba su justa parte de la recompensa del bloque. Esto necesita que la red cumpla los pagos entre el bloque específico y el Incentivizednode correcto, a su vez esto necesita un comportamiento acorde del minero. Si el minero no puede cumplir con los estándares, los bloques que procesan serán rechazados por la red, esto servirá para evitar el fraude.

Pero esto debe ser llevado a cabo. Para lograrlo, los Incentivizednodes crean Quorums que emiten las decisiones al Incentivizednode correcto (al que se le debe pagar). El proceso es completamente descentralizado y sin confianza, así que no hay manera de que un Incentivizednode conspire con otro para defraudar al sistema. Una vez que un cierto número de mensajes ha sido recibido, se llega a un consenso mediante votos y el bloque es obligado a pagarle al Incentivizednode correcto.

Los mineros que usan software de pool pueden obtener información de cómo conseguir un bloque a través del uso de RPC API. Cuando se accede al API, el usuario extiende la forma y agrega un recipiente secundario en GetBlockTemplate. Si el bloque es minado exitosamente, el pago es dividido entre los mineros y los Incentivizednodes.

## GOBERNANZA Y FINANCIACIÓN

El dilema de la gobernabilidad es complejo para los desarrolladores de una red de criptomoneda. Por un lado, la red debe ser efectiva, con decisiones que se tomen rápida y efectivamente para asegurar un desarrollo positivo a corto y largo plazo. Por otro lado, la naturaleza descentralizada de la criptomoneda debe ser protegida.

Esto requiere un sistema estructurado de gobernanza; algo que Stash implementa mediante el autogobierno.

## ¿QUÉ ES EL AUTOGOBIERNO?

El autogobierno es la solución de gobernanza que Stash utiliza para la toma de decisiones rápidas en una red descentralizada. En vez de debatir opciones, posibilidades y decisiones el autogobierno provee una serie de reglas que permiten resoluciones rápidas. Tomando Bitcoin como ejemplo, un debate en la red sobre el tamaño de un bloque individual ha tomado años en ser resuelto, mientras que en Stash, tal debate sería votado y solucionado en cuestión de horas. El resultado es una red mucho más eficiente.

El autogobierno requiere que las propuestas sean promovidas por la red, y después votadas. En la práctica, esto significa que los Incentivizednodes pueden votar los importantes cambios del sistema o de la red, y, como nadie puede asumir el control de demasiados Incentivizednodes, obtener el control de los votos es imposible.

## ¿QUÉ ES LA AUTOFINANCIACIÓN?

Incluido en el sistema de autogobierno está la manera en la cual las recompensas de bloques son utilizadas para promover la financiación continua de la red. Por cada bloque minado, el minero recibe el 45% de la recompensa, mientras que el Incentivizednode otro 45%, lo que deja un 10% sobrante. Ese 10% no es creado hasta el final del mes. Durante el mes, cualquiera puede hacer una propuesta de presupuesto, la cual será votada por la red. Al final del mes los bloques de tesoro son creados y si ninguna propuesta fue aprobada o ese 10% es superior a lo necesitado para resolver las propuestas la recompensa es enviada al tesoro para ser usada en futuras propuestas. Este sistema le permite a la red autofinanciarse y le permite la oportunidad de construir activos en la forma de la moneda Stash que luego puede ser usada para propuestas aún mayores.

## PROBLEMAS DE FUNGIBILIDAD

Bitcoin ha hecho evidente que las transacciones no son del todo privadas. Esto ha llevado al problema de la fungibilidad. Fungibilidad significa que mis Bitcoins no valen lo mismo que las tuyas pero que son sustitutos perfectos. Analizando los registros públicos terceras partes pueden vincular las transacciones de Bitcoins con las identidades de las personas. Esto puede llevar a que las Bitcoins sean manchadas por un historial negativo. Stash en cambio integrará un sistema de prueba de conocimiento nulo en la capa de seguridad (ZSL) para proveer a los usuarios con mayor privacidad y solucionar los problemas de fungibilidad.

La capa de seguridad de prueba de conocimiento nulo está basada en zk-SNARKS, una forma de criptografía de conocimiento nulo que brinda privacidad de transacción a los usuarios de la red. La privacidad es lograda permitiendo encriptación completa en las transacciones de la blockchain, pero permitiendo verificabilidad por consenso de la red. Esta sección explica cómo esto es posible, y los beneficios que brinda tanto a usuarios como a la red.



## LA PRIVACIDAD SUPERIOR DEL SISTEMA DE PRUEBA DE CONOCIMIENTO NULO

A diferencia de otros métodos de privacidad para criptomonedas que dependen de oscurecer el vínculo entre las transacciones, Stash encripta las transacciones en la blockchain. Esto permite que el monto, origen y destino del pago permanezca oculto pero igualmente verificando la transacción de fondos bajo las reglas de consenso de red de zk-SNARK usando las pruebas del mismo.

### ¿COMPRENDIENDO ZK-SNARKS?

zk-SNARK o “zero knowledge succinct non-interactive argument of knowledge” (argumento de lógica sucinto no interactivo de conocimiento nulo) y su sistema de pruebas han estado disponibles desde hace tiempo, pero fue usado por primera vez de forma masiva con la criptomoneda ZCash.

Mediante zk-SNARK un individuo, puede probar que tiene cierta información sin revelar tal información, y sin ninguna interacción con otro usuario; definidos como el probador y el verificador.

Con la prueba de conocimiento nulo el probador puede convencer al verificador que cierta afirmación es verdadera simplemente revelando información que prueba la validez de la afirmación y no la afirmación misma. Por ejemplo, se puede probar que un hash de un número aleatorio existe sin revelar tal número.

La prueba de conocimiento nulo lleva esto aún más allá. El probador convence al verificador no solo de que tal número existe sino de que conoce el número sin revelar nada de información del mismo.

Es posible confirmar las pruebas de conocimiento nulo sucintas con unos pocos cientos de bytes y dentro de milisegundos incluso para las afirmaciones más grandes. Mientras que los primeros sistemas de pruebas de conocimiento nulo requerían varias rondas de comunicación, los sistemas no interactivos requieren un solo mensaje entre probador y verificador. En este punto las pruebas de conocimiento nulo son tan cortas que pueden ser publicadas en una blockchain que consiste en una fase de establecimiento que crea referencias mutuas en una serie que luego es compartida entre probador y verificador. Esta serie puede ser referida como parámetros públicos.

Si alguien pudiera acceder a la aleatoriedad secreta usada para crear parámetros públicos, solo podrían producir pruebas falsas y, a su vez, monedas Stash falsas que serían indistinguibles de las reales. Sin embargo, para evitar actividades fraudulentas, la manera en la que los parámetros son creados es un evento sofisticado entre varios usuarios, tal evento es conocido como la ceremonia. Cada usuario en la ceremonia es obligado a destruir su minúscula pieza de los parámetros. Incluso si un solo usuario destruye su pieza, los parámetros son inútiles, haciendo extremadamente improbable que tales parámetros pudieran existir y caer en las manos equivocadas.

Stash proveerá más información sobre la ceremonia en nuestro sitio web.

## LAS CAPAS DE LA RED STASH

Para que una red de criptomoneda pueda funcionar correctamente, debe poseer una estructura; una transacción debe pasar por ciertas pruebas para poder ser verificada.

En el caso de la Bitcoin una transacción será validada después de tres pruebas:

1. Que los Bitcoin usados no hayan sido gastados anteriormente por el usuario que realiza el envío. El usuario no debe realizar acciones adicionales ya que esto es comprobado por el libro de registros.
2. Que el usuario que realiza el envío tenga la autoridad suficiente para enviar las monedas por la cantidad establecida para la transacción. Esto se verifica mediante la firma de la transacción con una llave secreta que está vinculada a la dirección donde las monedas son enviadas.
3. Que la transacción sea balanceada en cantidad de monedas enviadas y monedas recibidas. Esto debería ser evidente por la transacción, debido a que el monto es conocido por todas las partes.

Stash usará una forma de prueba de conocimiento nulo conocida como zk-SNARKs para probar todos los puntos anteriores sin revelar ninguna información adicional. Cuando cada transacción es válida, también un zk-SNARK usado para mostrar que las monedas Stash existen y que no han sido gastadas, que el usuario que realiza el envío tenga la autoridad para enviarlas y que la cantidad de monedas enviadas corresponde la cantidad recibida.

Durante este proceso, la información requerida para usar las monedas Stash está adjunta a la transacción mediante la creación de un nuevo zk-SNARK que es encriptado usando la llave pública de los recipientes que solo puede ser usada por el usuario que recibe la transacción.

Los resultados son entonces distribuidos en el nuevo libro de registro que ha sido llamado la capa de seguridad del sistema de prueba de conocimiento nulo.

## TRANSACCIONES INSTANTÁNEAS

Las transacciones de la red Stash deben ser seguras y privadas, pero también veloces. Los usuarios de los Incentivizednodes Quorums son utilizados para enviar y recibir transacciones irreversibles instantáneamente.

Cuando un Quorum es formado, lo ingresado de la transacción es bloqueado. Este bloqueo lleva 4 segundos para ser completado. Si la red Incentivizednode llega a un acuerdo mayoritario, cualquier transacción o bloque controversial será rechazado de antemano.

Solo coincidencias exactas del ID de la transacción serán aceptadas.

La idea de esto es conectar la criptomoneda Stash con su uso del mundo real por ejemplo mediante de una aplicación móvil para ventas. Si un usuario puede realizar transacciones

comerciales usando dinero digital encriptado y que no tenga tiempos de espera, entonces la criptomoneda Stash puede convertirse en un rival importante para el uso del dinero tradicional, tanto en papel físico como para las tarjetas de débito y crédito.

## **TOKENS DE STASH Y OFERTA DE CRIPTOMONEDA STASH**

Un total de 500 millones de tokens de Stash serán entregados durante la venta de Tokens. Los ingresos obtenidos serán utilizados para establecer la criptografía de prueba de conocimiento nulo dentro de la criptomoneda Stash y para crear el monedero virtual de Stash. Una vez que estas características de privacidad hayan sido puestas en funcionamiento los dueños de los tokens de Stash podrán usarlos para comprar criptomonedas Stash a un cambio de a 1 a 1. Un máximo de 997.8 millones de monedas Stash serán creadas esto incluyendo tanto las monedas compradas con tokens Stash como las que serán creadas producto de la minería durante los próximos 100 años.

## **OFERTA DE MINADO DE STASH**

El minado de la criptomoneda Stash creará nuevas unidades de la moneda, y por ende resultará en inflación. Como medida antiinflacionaria, la oferta nueva será reducida año tras año a una tasa del 7.1% anual.

Sumándose a esta medida, Stash también implementará una conexión directa entre la oferta para cada bloque y el número de mineros activos en la red. Si el número de mineros disminuye las recompensas de cada bloque aumentan y viceversa.

Se espera que la producción de la criptomoneda continúe hasta mediados del próximo siglo, momento en el cual la recompensa por bloque llegará a cero y los mineros e Incentivizednodes serán recompensando mediante comisiones por transacciones.

# **MAPA DE OBJETIVOS DE STASH**

## **INTEGRACION DE ZSL Y MONEDERO STASH Q2, 2018**

Stash usará los ingresos de la venta inicial para integrar ZSL, una capa de seguridad de conocimiento nulo diseñada para establecer transacciones en la blockchain de un modo anónimo y seguro, al mismo tiempo que mantiene el origen, monto y destino del pago privado. Stash también desarrollará un monedero con interfaz GUI para almacenar las criptomonedas Stash.

## **LANZAMIENTO DE LA CRIPTOMONEDA STASH Q2 2018**

Una vez que ZSL haya sido integrado, los dueños de tokens de Stash (STT) podrán usar sus tokens para comprar Stash a un cambio de 1 a 1, la criptomoneda también se abrirá al minado. Los dueños de la criptomoneda Stash podrán manejar sus propios Incentivizednodes y a cambio de brindarle recursos a la red recibir criptomonedas Stash como parte de las recompensas de los bloques.

## **SISTEMA DE FINANCIAMIENTO Y GOBIERNO DE STASH Q3 2018**

Stash estará abierta a la comunidad para recibir fondos y propuestas de gobierno lo que le permitirá a Stash implementar nuevas características que sean votadas por los Incentivizednodes. El sistema de gobernanza y financiación de Stash ayudará a mantener la red abierta, autónoma y descentralizada (ODAN) para un funcionamiento eficiente y la exploración de propuestas de un modo orgánico, para evolucionar usando la inteligencia colectiva de los miembros de la comunidad Stash.

## **APP PARA CELULARES STASH Q3, 2018**

Stash desarrollará una aplicación móvil que permitirá a los usuarios de Stash, guardar, enviar y recibir criptomonedas Stash. La aplicación móvil de Stash permitirá usar el celular fácilmente para las transacciones diarias, también permitirá monitorear tus recompensas criptomonedas Stash por el manejo de Incentivizednodes.

## **MENSAJERÍA PRIVADA Q4, 2018**

StashChat será un sistema de p2p de mensajes privados que permitirá a los usuarios de Stash enviar mensajes protegidos usando criptografía de conocimiento nulo. StashChat brindará comunicaciones completamente anónimas sin intermediarios lo que permitirá a los usuarios comunicarse privadamente tanto individual como grupalmente.

## **API DESCENTRALIZADA Q1, 2019**

Stash lanzará una API descentralizada que usará grupos aleatorios de Incentivizednodes, lo que eliminará la necesidad de los desarrolladores de software de almacenar, validar y descargar la blockchain de Stash entera, pero aun así brindando la seguridad y privacidad de un Incentivizednode.

## **TARJETA DE DÉBITO STASH Q2 2019**

Creando una tarjeta de débito STASH que permitirá a los dueños de Stash almacenar de una manera segura sus pagos con Stash en persona, online o por el teléfono con cualquier vendedor que acepta monedas fiat. Como resultado los usuarios de Stash podrán comprar cualquier producto o servicio que deseen con STASH y aumentando la utilidad de la criptomoneda Stash.

## **CONVERSIÓN DIRECTA A MONEDAS FIAT Q3 2019**

Creando un método de pago directo que permita a los usuarios cambiar su STASH por dinero fiat y viceversa. La puerta de conversión STASH estará integrada al monedero STASH y la aplicación para celular. Esto permitirá a los usuarios libre y fácilmente transferir entre dólares, euros, yuanes, dólares australianos y STASH en vez de tener que acudir a cambios o intermediarios.

## **IMPLICACIONES LEGALES DEL LANZAMIENTO DE LOS TOKENS**

Los tokens de STASH no son seguridades. Los tokens de STASH no tienen reembolso. Los tokens de STASH no son para inversiones especulativas. Toda la documentación de Stash, sus diseños y fuentes en investigación, desarrollo y etapa conceptual pueden cambiar. No hay promesas de rendimiento futuro ni de valor hechas con respecto a Los tokens de STASH o la criptomoneda STASH, incluyendo ninguna promesa de valor inherente, ninguna promesa de continuación en los pagos, y ninguna garantía de Los tokens de STASH o la criptomoneda Stash poseerán algún valor. Los tokens de STASH y la criptomoneda STASH no son participaciones en la empresa y Los tokens de STASH y la criptomoneda STASH no brindan ningún derecho frente a tal empresa. Los tokens de STASH son vendidos como un producto funcional y todas las ganancias son recibidas por la empresa y usadas por la empresa de un modo libre sin ningún tipo de condición. Los tokens de STASH y la criptomoneda Stash son para expertos que manejan tokens criptográficos y sistemas de software basados en la blockchain.

STASH Tokens are not securities. STASH Tokens are non-refundable. STASH Tokens are not for speculative investment. All Stash documentation, designs and sources are in the research, development and conceptual phase and subject to change. No promises of future performance or value are or will be made with respect to STASH Tokens or Stash Cryptocurrency, including no promise of inherent value, no promise of continuing payments, and no guarantee that STASH Tokens or Stash Cryptocurrency will hold any particular value. STASH Tokens and Stash Cryptocurrency are not participation in the Company and STASH Tokens and Stash Cryptocurrency hold no rights in said company. STASH Tokens are sold as a functional good and all proceeds received by Company may be spent freely by Company absent any conditions. STASH Tokens and Stash Cryptocurrency are intended for experts in dealing with cryptographic tokens and blockchain-based software systems.