Libro Blanco Zen

“Zen White Paper”

Robert Viglione, Rolf Versluis y Jane Lippencott*

Mayo 2017

Resumen

Zen es un sistema encriptado entre iguales con tecnología de prueba de conocimiento nulo (zero-knowledge proof) en donde las comunicaciones, datos o valores se pueden transmitir y almacenar de forma segura. Es una integración de tecnologías revolucionarias que crean un sistema en donde la innovación se puede acelerar combinando tres funciones que tradicionalmente están separadas:
1) transacciones 2) comunicación y 3) gobernanza competitiva. Esto se hace de forma segura y anónima, utilizando una cadena de bloque distribuida a nivel mundial con infraestructura computacional. El sistema integra varias tecnologías de primera clase para formar una plataforma abierta para una innovación libre que puede evolucionar con las preferencias del usuario.

* Se puede contactar a los autores en rob@zensystem.io, rolf@zensystem.io, y jane@zensystem.io, respectivamente.

También quisiéramos agradecer a Jake Tarren por sus comentarios y sugerencias, así como a la amplia Comunidad de Zclassic y Zen por ayudarnos a desarrollar estas ideas y hacer posible este movimiento.

Contenido

1 PROPÓSITO

“Crítica creando.” - Michelangelo Buonarroti

Vivimos en un mundo extremadamente regulado y vigilado donde miles de millones de personas son privados de los derechos humanos básicos, como el derecho a una propiedad, la privacidad, la libre asociación y el acceso a la información. Existen tecnologías para resolver algunos de estos problemas y la temprana implementación de Zen hará exactamente eso.

Zen es una colección de productos, servicios y negocios construido sobre tecnologías que permiten pruebas de conocimiento nulo con un conjunto básico de creencias. Mediante tecnologías como un sistema de cadena de bloques (blockchain) distribuido, las últimas técnicas de evasión de censura, comunicaciones totalmente encriptadas y un modelo social y de gobernanza diseñado para la viabilidad a largo plazo, Zen contribuirá al derecho humano a la privacidad y proporcionará la infraestructura de red necesaria para que las personas colaboren y construyan valor de manera segura dentro de un ecosistema sin fronteras. Nuestra misión es integrar las últimas tecnologías disponibles post-Satoshi con un conjunto de estructuras sociales descentralizadas, voluntarias y pacíficas para mejorar la vida de cualquiera que desee participar. Creemos que esta es una idea cuyo momento ha llegado.

El marco de trabajo de Zen es seguro y orientado a la privacidad con un sistema de gobernanza estructurado para permitir a los participantes ampliar la funcionalidad de forma colaborativa en muchas maneras. Los usos de la plataforma incluyen: alojamiento de los datos de identificación, prueba selectiva de título de propiedad, servicios bancarios descentralizados, intercambio de activos p2p (par a par)/b2b (negocio a negocio) que preserva la privacidad, sociedades de ayuda mutua, seguro de p2p (par a par), los mecanismos descentralizados de ayuda humanitaria o su uso puramente como un activo anónimo de valor.

Estas funciones pueden ser utilizadas para atender a las poblaciones marginadas actualmente excluidas de servicios vitales tales como bancarios y atención médica debido a la falta de identificación personal, capital y canales seguros. También pueden ser aprovechadas por individuos que desean ser dueños y monetizar sus datos privados. Por ejemplo, comunidades emprendedoras que deseen desarrollar un sistema de licitación competitiva sobre la energía solar generada en un entorno interno. Las implementaciones son ilimitadas, el vínculo común de estas es la creencia de que la descentralización es el motor del progreso moral y que las soluciones voluntarias son las más creativas y duraderas.

2 HISTORIA

Zen se desarrolla sobre las mejores tecnologías existentes de las criptomonedas, arquitecturas de red y sistemas de intercambio de archivos distribuidos mediante la combinación de características ya existentes y nuevas para proveer una base sólida, misma que proporciona viabilidad al proyecto a largo plazo. Aunado a esto, estamos desarrollando sobre las últimas ideas en consenso distribuido y gobernanza competitiva. Algunos de los fundamentos de nuestro proyecto provienen de Bitcoin, Dash, Decred y Seasteading.

Zcash sobrepasó a Bitcoin con la implementación de transacciones protegidas totalmente anónimas, de modo que los usuarios podían elegir entre direcciones normales tipo Bitcoin (direcciones-T)

o direcciones privadas resistentes al análisis de correlación de tráfico (direcciones-Z). Después creamos Zclassic, un clon de Zcash, en donde se modificaron algunos parámetros que nuestra comunidad consideró importantes: eliminamos la Recompensa de los Fundadores del 20% para los primeros 4 años y el comienzo paulatino de la oferta monetaria. Desde el lanzamiento de Zclassic, hemos formado una gran comunidad de código abierto entusiasmada de mejorar la tecnología Zen. Algunos de los primeros logros incluyen el desarrollo de una aplicación de minería en conjunto (mining pool) de código abierto para Zcash y Zclassic, también las carteras digitales para Windows y Mac.

Nuestro equipo se percató que Zclassic podría mejorar mediante una red completamente encriptada con un modelo económico y de gobernanza innovador que se alinea más a la visión original de Satoshi (inventor de Bitcoin), la cual describe una comunidad descentralizada global. Nosotros vemos a Zclassic como un proyecto de criptomonedas puramente de código abierto y voluntario, mientras que Zen mejora esto al destinar fondos internos para facilitar un conjunto de comunicaciones, intercambio de archivos y actividades económicas más amplias.

3 ESPECIFICACIONES DEL LANZAMIENTO

Zen es el sistema dominante sobre el cual los token ZenCash se distribuyen. Similar a proyectos como Ethereum que tiene su token de Ether. ZenCash está diseñado como una bifurcación de Zclassic y tendrá las siguientes caracteristicas adicionales.

1. Fecha de lanzamiento: 8PM EDT, 23 de mayo de 2017 bifurcándose de Zclassic (0:00 UTC).
2. Algoritmo de cifrado Equihash, es un algoritmo de minería que usa la prueba de trabajo (Proof-of-Work) orientada en memoria. Basado en el problema generalizado de cumpleaños y el algoritmo de Wagner.
3. Recompensa de bloque: 12.5 ZenCash.
4. Generación de bloques: 2.5 minutos.
5. Tamaño del bloque: 2 MB.
6. Algoritmo de dificultad ajustada: Digishield V3, modificado para determinar el siguiente nivel de dificultad de la siguiente forma:

$$siguiente\ dificultad = dificultad\ pasada * \sqrt{\frac{150\ Segundos}{tiempo\ de\ respuesta\ pasado}}$$

7. Repartición de cada recompensa del bloque mediante prueba de trabajo (Proof-of-Work) y honorarios de transacción entre mineros y otras partes interesadas:
   (a) 88% a los mineros.
   (b) 5% a una o más Organizaciones Autónomas Descentralizadas (OAD).
   (c) 3.5% a operadores de nodos seguros.
   (d) 3.5% al equipo principal.
8. Oferta total de monedas: 21 millones.
9. La recompensa se reduce a la mitad cada ≈ 4 años, como en Bitcoin.
10. Las transacciones seguras ocultan el remitente, el receptor y la cantidad en la cadena de bloques (blockchain).
11. Las transacciones transparentes publican el remitente, el receptor y la cantidad en la cadena de bloques (blockchain).
12. Campo de mensaje seguro en la transacción Z con 1024 bytes de caracteres:

(a) Publicación segura en ubicaciones de GNUnet y / o IPFS.
(b) Mensajes cortos entre usuarios.
(c) Publicaciones en los canales visibles para cualquier persona con la cartera digital que utiliza distintos canales

13. Los nodos seguros realizan las siguientes funciones de infraestructura de red:
    (a) Aseguran que todas las comunicaciones de red estén encriptadas entre los nodos.
    (b) Mantienen la cadena de bloques (blockchain) completa de ZenCash.
    (c) Proporcionan conexiones de cifrado basadas en certificados para las aplicaciones de cartera digital de ZenCash
14. Los nodos seguros que cumplan con los requisitos reciben premios en base a la moneda.
15. Servicio de fronting de dominios para transacciones Z usando un CDN comercial.
16. Gobernanza por una o más OADs. (Ver sección Gobernanza).
17. La OAD de Zen es responsable de las operaciones y mejora continua del sistema. Ellos construirán y administrarán lo siguiente:
    (a) Distribución de información Zen (Web, wiki, blog, medios de comunicación).
    (b) Sistema de Propuesta y Sistema de Votación.
    (c) Sistemas de informes y monitoreo.
18. Equipo principal:
    (a) Incluye fundadores del Zen.
    (b) La misión es guiar el lanzamiento, el crecimiento y desarrollo temprano.
    (c) Gastos del fondo importantes para el desarrollo y mantenimiento.
    (d) Operar en la interfaz de Zen y sistemas tradicionales.

4 PLAN DE TRABAJO

“El método prueba y error es libertad.” (Taleb, 2012)

Zen está desarrollando la integración de tecnologías revolucionarias para crear un sistema en donde la innovación se puede acelerar. Estamos estructurando la descentralización óptima y la competencia persistente para que el sistema evolucione constantemente y nunca llegue a un estado de confort. El plan de trabajo inicial cubre una ventana de desarrollo de 12 a 18 meses para que el sistema funcione de forma autónoma. La clave para realizar esto es, establecer el conjunto básico de integraciones con nuestra propia red de nodos seguros, un sistema de almacenamiento de datos distribuido como GNUnet y el ecosistema más amplio de intercambios, minería conjunta (pool mining) y comunidades de usuarios. ZenCash necesita ser completamente operativo, fácilmente disponible y útil para una variedad diversa de partes interesadas (stakeholders) al proyecto. Nuestro plan de trabajo refleja el énfasis en ZenCash como nuestro primer y más importante producto inicial del portafolio Zen.

1. Desarrollar carteras mejoradas en las siguientes plataformas:
    (a) Windows para las transacciones t y z, mensajería, publicación GNUnet.
    (b) Linux para transacciones t y z, mensajería, publicación GNUnet.
    (c) Mac para las transacciones t y z, mensajería, publicación GNUnet.
    (d) Móvil (Android & iOS) para transacciones t y z.

(e) Hardware para transacciones t y z, mensajería, publicación GNUnet.
(f) Cartera Web para transacciones t y z, mensajería y publicación de GNUnet.

2. Servicio de Domain Fronting para transacciones z usando una red (CDN) comercial.
3. Servidores de sistemas Zen en una configuración de centro multi-data resistente.
4. Pruebas de resistencia a la infraestructura, resultados y mejoras.
5. Implementar “Segregated Witness”.
6. Entregables del departamento de investigación y desarrollo de gobernanza, incluido el sistema operacional completamente probado (referirse a la sección de Gobernanza):
   (a) Reporte de investigación.
   (b) Constitución.
   (c) Sistema de votación probado e implementado.
   (d) Primera elección que se ejecute en por lo menos una OAD, la transición del equipo principal.

5 ELEMENTOS FUNCIONALES

Zen reúne múltiples elementos diferentes para formar un trabajo completo. En lugar de nodos básicos, Zen requiere nodos seguros, lo que garantiza que los nodos mantengan un estándar básico de seguridad y rendimiento para asegurar que el sistema permanezca distribuido, resiliente y seguro. Al reforzar la comunicación encriptada de nodos; y entre nodos y carteras, Zen se protege contra el espionaje y los ataques de intermediarios.

Zen también aborda la debilidad de los metadatos de otras criptomonedas. Por ejemplo, al comunicarse de una manera potencialmente comprometida y luego enviar Bitcoin, los participantes en una transacción Bitcoin están potencialmente expuestos a la identificación por agentes relacionados en las transacciones. ZenCash incorporará mensajería segura dentro de transacciones seguras, para que los usuarios puedan acordar la transacción, enviarla y luego verificar el recibo. Estos elementos funcionales se manifiestan en los siguientes sistemas:

- ZenTalk - Un nuevo tipo de red de comunicaciones seguras que permite la comunicación de uno-a-múltiples involucrados, utilizando la cadena de bloques para almacenar mensajes permanentemente.
- ZenPub - Una plataforma anónima de publicación de documentos utilizando GNUnet o IPFS.
- ZenHide - La habilidad para circunnavegar el bloqueo del cripto-comercio usando fronting de dominio .

5.1 Transacciones T

Las transacciones T , son transacciones tradicionales registradas en la cadena de bloques controladas por una clave privada en una cartera. Estas son derivados de Bitcoin y permiten una rápida compatibilidad con los centros cambiarios, carteras y otras aplicaciones de ecosistemas derivadas de Bitcoin.

5.2 Transacciones Z

Son transacciones enviadas a direcciones privadas, heredadas de Zcash y Zclassic. Los saldos en direcciones privados son invisibles. Si se hace una transacción a una o más direcciones privadas , el valor permanece privado, pero si la última dirección es transparente se revelará el valor recibido en la cadena de bloques. Las direcciones de entrada privadas y si el valor fue enviado a una o dos de éstas mismas, se mantiene confidencial cuando esta transacción se hace pública. El protocolo Zcash describe este proceso en detalle:

> El valor en Zcash es transparente o privado. Las transferencias de valor transparente funcionan esencialmente como en Bitcoin y tienen las mismas propiedades de privacidad. El valor "privado" (shielded) es transportado por notas, que especifican una cantidad y una clave de pago. La clave de pago forma parte de una dirección de pago, que es un destino al que se pueden enviar notas. Como en Bitcoin, esto se asocia con una clave privada que se puede utilizar para pasar notas enviadas a la dirección; En Zcash esto se llama una clave de gasto. A cada nota hay asociado criptográficamente un compromiso de nota y un anulador 1 (lo anterior con el fin de que exista una relación 1: 1: 1 entre notas, compromisos de notas y anuladores). Cabe recalcar que la computación del anulador requiere la clave de gasto privado asociada. Es imposible correlacionar el compromiso de nota con el anulador correspondiente sin conocer al menos esta clave de gasto. Una nota válida no utilizada, en un punto dado de la cadena de bloques, es aquella para la cual el compromiso de nota se ha revelado públicamente en la cadena de bloques antes de ese punto,sin que el anulador se haya revelado.
>
> Una transacción puede contener entradas, salidas y scripts de comandos transparentes, que funcionan como en Bitcoin [Bitcoin-Protocol]. También contiene una secuencia de cero o más descripciones JoinSplit. Cada uno de estos describe una transferencia JoinSplit que toma un valor transparente y hasta dos notas de entrada y produce un valor transparente y hasta dos notas de salida. Se revelan los anuladores de las notas de entrada (evitando que se vuelvan a gastar) y se revelan los compromisos de las notas de salida (permitiéndoles gastar en el futuro). Cada descripción de JoinSplit también incluye una prueba zk-SNARK computacionalmente sólida, Lo que demuestra que todas las siguientes se mantienen con una probabilidad insignificante:
>
> - El saldo de los valores de entrada y salida (individualmente para cada transferencia JoinSplit)
> - Para cada nota de entrada de valor distinto de cero, existe algún compromiso de nota revelada para esa nota.
> - El validador conocía las claves del gasto privado de las notas de entrada.
> - Los anuladores y compromisos de notas se calculan correctamente.
> - Las claves de gasto privadas de las notas de entrada están criptográficamente vinculadas a una firma sobre toda la transacción, de tal manera que la transacción no puede ser modificada por una parte que no conoce estas claves privadas.
> - Cada nota de salida se genera de tal manera que sea imposible hacer que su anulador choque con el anulador de cualquier otra nota.

Fuera del zk-SNARK, también se comprueba que los anuladores de las notas de entrada no se habían revelado (es decir, no se habían gastado).

Una dirección de pago incluye dos claves públicas: una clave de pago que coincide con la de las notas enviadas a la dirección y una clave de transmisión para un esquema de cifrado asimétrico privado-clave. "Clave-privada" significa que los textos cifrados no revelan información sobre la clave en la que se cifraron, excepto a un titular de la clave privada correspondiente, que en este contexto se denomina clave de visualización. Esta facilidad se utiliza para comunicar notas de salida cifradas en la cadena de bloque a su destinatario, que puede utilizar la clave de visualización para explorar las cadenas de bloques para las notas dirigidas a ellas y luego descifrar esas notas.

La base de las propiedades de privacidad de Zcash es que cuando una nota se gasta, el gastador sólo demuestra que se ha revelado cierto compromiso por ello, sin revelar cuál. Esto implica que una nota gastada no se puede vincular a la transacción en la que se creó. Es decir, desde el punto de vista de un adversario, el conjunto de posibilidades para una nota de entrada dada a una transacción, su conjunto de trazabilidad de notas, incluye todas las notas anteriores que el adversario no controla o sabe que se han gastado. Esto contrasta con otras propuestas de sistemas de pago privados como CoinJoin o CryptoNote, que están basados en mezclar un número limitado de transacciones y que por lo tanto tienen un conjunto de trazabilidad de notas menor.

Los anuladores son necesarios para evitar el doble gasto: cada nota sólo tiene un anulador válido, por lo que intentar pasar una nota dos veces revelaría el anulador dos veces, lo que haría que la segunda transacción fuera rechazada.

5.3 ZenTalk

Las transacciones Z en ZenCash tienen la capacidad de incorporar mensajes basados en texto, que se cifran y se incluyen en la cadena de bloques. Hay un límite de 1024 caracteres para estos mensajes. Estos mensajes permiten mejorar la capacidad de los usuarios para llevar a cabo el comercio seguro. En lugar de efectuar la transacción en otros canales menos seguros que pueden no tener el mismo nivel de privacidad que Zen, los usuarios pueden comunicarse a través de los mensajes ZenTalk con la otra persona o personas antes y después de la transferencia privada con un gasto muy pequeño de la transacción z. Estos mensajes se pueden enviar directamente de una dirección z a otra y también se pueden enviar a un canal. Al generar una dirección-z desde el hash de un canal, los usuarios pueden suscribirse al canal y leer cualquier cosa publicada por cualquiera en el canal.

Por ejemplo, los anuncios del canal #ZenCash-announcements tendrían un hash a zXXXXXXXXXXXX, permitiendo a cualquier usuario enviar un mensaje anónimo al canal. Cada mensaje costaría una cantidad de ZenCash para enviar, ya que está contenido en una transacción Z, por lo tanto reduciendo la cantidad de mensajes no útiles en canales comunes. Los anuncios oficiales estarían firmados por claves privadas y solo se mostrarían a los usuarios si se consideran válidos. Además, los mensajes grupales privados se pueden publicar usando transacciones Z creando primero un nombre de canal complejo y luego encriptar el contenido del mensaje solo con claves que los destinatarios deseados tienen. Los mensajes ZenTalk se cifran con algoritmos como AES-256 con Perfect Forward Secrecy (PFS) que coincide con los estándares actuales de encriptación para una comunicación segura.

5.4 ZenPub

Zen tiene la capacidad de publicar documentos en el IPFS (Interplanetary File System) o GNUnet. Esto se hace publicando una dirección IPFS o GNUnet en el campo de texto de una dirección Z. El sistema de publicación de documentos preferido en este momento es GNUnet, ya que proporciona la infraestructura necesaria para la publicación anónima y mantiene una base de datos activa de documentos. El sistema es similarmente extensible a IPFS o a cualquier otro sistema de archivo de distribución futuro. Al crear una capa de mensajería anónima junto con una capa de publicación anónima, ZenPub permite la creación de publicaciones verdaderamente anónimas que se pueden distribuir rápidamente a los lectores interesados.

5.5 ZenHide

Es posible que los reguladores en los países hostiles al cripto-comercio bloqueen los criptomonedas como Bitcoin e incluso Zcash. Zen utiliza el fronting de dominio para ampliar la capacidad de completar las transacciones en entornos de red adversarial, como se explica en el bloqueo de la comunicación resistente a través del fronting de dominio en el siguiente resumen:

> Describimos el "fronting de dominio" como una técnica versátil de la censura que oculta el punto final remoto de una comunicación. El fronting de dominio funciona en la capa de aplicación, mediante HTTPS, para comunicarse con un host (anfitrión) prohibido mientras parecen comunicarse con algún otro host, permitido por el sensor. La idea clave es el uso de diferentes nombres de dominio en diferentes capas de comunicación. Un dominio aparece en el "exterior" de una solicitud HTTPS-en el DNS y TLS Server Name Indication, mientras que otro dominio aparece en el "interior" -en el encabezado HTTP Host, invisible para el sensor encriptado debajo de HTTPS.
>
> Un sensor, incapaz de distinguir el tráfico con frontera y sin frontera de un dominio, debe elegir entre permitir el tráfico de evitación y bloquear el dominio por completo, lo que resulta en costosos daños colaterales.
>
> El fronting de dominio es fácil de implementar y usar y no requiere una cooperación especial por parte de los intermediarios de red. Identificamos una serie de servicios web difíciles de bloquear, como redes de distribución de contenido, que admiten conexiones con dominio y son útiles para la elusión de la censura.

La implementación específica de fronting de dominio utilizada por Zen en el lanzamiento es con una red de distribución de contenido comercial, pero como con todos los aspectos de nuestra arquitectura, la flexibilidad está diseñada desde el principio y el sistema puede extenderse en muchas direcciones a medida que la tecnología evoluciona.

5.6 Nodos Seguros Zen

Los nodos son los sistemas clave que mantienen la cadena de bloques, aceptan transacciones de carteras digitales, validan soluciones de minería y actúan como el sistema descentralizado de computación y comunicaciones para criptomonedas. En Zen, toda la información transmitida desde y hacia los Nodos

seguros está encriptada con certificados válidos usando TLS versión 1.3 y protegida con Perfect Forward Secrecy (PFS). Como parte de la capacidad de Secure Node, la aplicación ZenCash mejora la funcionalidad mediante:

- Ampliación de RPC para permitir que los datos cifrados AES residan en transacciones privadas.
- Ampliación de RPC para permitir una PFS (Perfect Forward Secrecy) entre claves públicas.

Los nodos seguros que cumplan con todos los requisitos serán recompensados con la porción de los nodos seguros de la minería de una manera secuencial. Los nodos seguros necesitan supervisar el canal del nodo #secure. El sistema de pago de nodos seguros está diseñado para ser operado de manera auditable con estándares claros para maximizar la operatividad y minimizar los problemas.

1. Funciones básicas de infraestructura realizadas por Nodos Seguros:
    (a) Asegurar que todas las comunicaciones de red estén encriptadas entre los nodos.
    (b) Mantener completa la cadena de bloques de Zen.
    (c) Proporcionar conexiones de cifrado basadas en certificados para las aplicaciones de cartera ZenCash.
2. Los nodos seguros que cumplan los requisitos descritos a continuación reciben el 3.5% de la recompensa base, de tal manera que recompensa el tiempo de actividad con la funcionalidad completa:
    (a) Utilizar el software de nodo en un sistema capaz según lo especificado por los requisitos de la infraestructura.
        - La memoria recomendada es de más de 4 GB.
    (b) Mantener toda la cadena de bloques de ZenCash en el sistema.
    (c) Proporcionar un certificado SSL válido al software del nodo de ZenCash para utilizarlo y comunicarse con otros nodos y carteras.
    (d) Mantener al menos 42 ZenCash en el servidor en una dirección T como fondo base.
    (e) Supervisar el canal de Nodo Seguro para los mensajes de desafío de “SecureNodeHQ” Aproximadamente cada 10 minutos (en un campo de mensaje de transacción Z).
    (f) Responder al desafío con la información de identificación del nodo seguro.
    (g) La respuesta al desafío será una combinación de dos cosas:
        - Enviar un mensaje privado a “SecureNodeHQ” que contiene la dirección T pública y ubicación del documento GNUnet en el campo de mensaje.
        - Publicar un documento en GNUnet firmado con la dirección T privada, incluyendo:
            1. Dirección pública de fondos Zen, que también se utilizará para el pago de recompensas.
            2. Certificado SSL y dirección IP.
            3. Encabezado de bloqueo de la cadena de bloques.
            4. Otra información que puede ser necesaria para asegurarse de que es un servidor único.

(h) Cada nodo seguro de Zen también debe ser un igual (peer) en los sistemas de GNUnet para publicar la respuesta de desafío anónimamente y apoyar las publicaciones anónimas de otros elementos del sistema.
(i) Otros requisitos potenciales que pueden surgir en el futuro para permitir que el sistema de ZenCash pueda usar los nodos seguros para el consenso y la energía de cómputo.

3. Sistema de pago de Nodo Seguro Zen (Z-SNPS):
   (a) Z-SNPS operado por una OAD Zen.
   (b) Z-SNPS realizará un seguimiento de las respuestas de desafío de cada nodo seguro.
   (c) Los nodos seguros serán rastreados y publicados por sus direcciones T.
   (d) El bloque minado pagará la recompensa del 3.5% al sistema ZC-SNPS, el cual distribuirá periódicamente el ZenCash a los Nodos Seguros basado en su tiempo de actividad en el período de tiempo definido.

Debido a que Zen tendrá esta red de computación distribuida en forma de Nodos Seguros compensados, estos nodos pueden ser requeridos para proporcionar otros servicios de computación para la red dependiendo de la evolución del consenso de la comunidad.

5.7 Nodos Estándar Zen

La aplicación ZenCash se puede utilizar en cualquier servidor linux, Mac o PC. El cliente actúa como un nodo y una cartera. Aunque no tiene la capacidad de encriptación completa que un nodo seguro tiene, todos los nodos ayudan al sistema a ejecutar la función eficientemente y permanecen resistentes al ataque.

5.8 Software de la cartera ZenCash

El software ZenCash se puede utilizar como una cartera. La cartera de línea de comandos es el formulario básico, pero ya existen versiones basadas en interfaz gráfica de usuario (GUI) para el escritorio. Mobile, Web, Raspberry Pi y otras carteras de hardware son de alta prioridad para desarrollar de inmediato y con esto mejorar la experiencia del usuario y la seguridad de los tokens ZenCash. Las carteras se pueden configurar para usar cualquier nodo disponible de ZenCash para la comunicación o pueden ser fijadas para conectar solamente con los nodos seguros para mantener niveles altos de seguridad de la información.

5.9 Aplicaciones

Zen es lo que consideramos un proyecto de código abierto óptimamente descentralizado, por lo que esperamos que las aplicaciones sean construidas y contribuyan al ecosistema por múltiples partes o personas. Muchas de estas contribuciones probablemente vendrán en código abierto de forma voluntaria, pero esperamos que una sólida comunidad de negocios también crezca alrededor de la plataforma. Además, el equipo principal tiene un plan completo de desarrollo de aplicaciones que ya está en proceso. Esto incluye, pero no está limitado a:

- Aplicación de nodos
- Conjuntos de Minería Equihash de Código Abierto
- Aplicaciones para el Sistema de Gobernanza

- Sistemas y Reportes de Monitoreo
- Carteras digitales de todo tipo
- Sistema de monitoreo seguro de nodos
- Sistema de Pago de Nodos Seguros

6 GOBERNANZA

“Así caen las ideologías: no por la violencia, sino por ejemplos que muestran una mejor manera” -Joe Quirk, Seasteading Institute

Zen está diseñado con un modelo de gobierno descentralizado que incorpora el empoderamiento de múltiples actores y la flexibilidad de evolucionar para adaptarse de manera óptima a nuestra comunidad. Fundamentalmente, nuestra filosofía de gobernanza está basada en que no conocemos a priori el mejor enfoque, pero tenemos algunas ideas sobre cómo inicializar el sistema y permitirle evolucionar con las necesidades de la comunidad. Creemos en la gobernanza como servicio (GaaS) y buscamos eficientemente proveer valor a nuestros grupos de interés directos, a la comunidad y al mundo.

“Cualquier industria que ofrece un servicio pobre por un alto precio merece ser interrumpida” (Quirk, 2017), los sistemas de gobierno tradicional siendo un ejemplo de lo anterior. En solidaridad con otros proyectos e ideas en todo el mundo, rechazamos la centralización forzada y fomentamos el voluntariado. En lugar de confiar a una minoría del pueblo con poder, creemos que todas las personas tienen el derecho a ser confiadas libremente.

La filosofía principal de nuestro modelo de gobierno es que la descentralización del poder maximiza la inclusión y la creatividad. Las implementaciones prácticas deben reconocer que la puesta en común de recursos y esfuerzo proporciona sinergias que deben ser equilibradas de manera óptima contra la descentralización total; puntos óptimos que son estáticos y variables en el tiempo, mejor determinado a través de la participación voluntaria y la secesión.

Es importante destacar que estamos implementando un sistema en el que pueden surgir OADs (Organizaciones Autónomas Descentralizadas) competitivas para compartir recursos o incluso reprimir completamente versiones menos eficientes o impopulares. No debe haber una estructura invariante de tamaño único para el entorno, la función, la cultura o el tiempo; Más bien, las estructuras deben ser fluidas, adecuadas a problemas específicos y flexibles a escala y mismas que se desvanecen cuando fallan en relación con las alternativas de trabajo. Un sistema de sistemas de este tipo evolucionaría dinámicamente de tal manera que resultará fuerte a la retroalimentación competitiva.

Nuestra gobernanza objetiva equilibrará la descentralización, la implementación eficiente, separación de poderes, amplio empoderamiento de las partes interesadas y flexibilidad evolutiva. Este estado inicial será el resultado de un esfuerzo por parte del equipo de Investigación y Desarrollo de por lo menos 12 a 18 meses en temas como la teoría de juegos, ciencia política y la investigación económica en mecanismos de votación óptimos junto con retroalimentación de múltiples implementaciones en testnet. El proyecto será uno de nuestros primeros esfuerzos con entregables finales incluyendo un informe de investigación integral y de código operativo integrado en la red Zen. Dentro de los 6 meses de la implementación del gobierno, esperamos tener equipos de liderazgo en operación desde nuestra primera elección completa y abierta.

6.1 Descentralización óptima

“Un espectro está atormentando al mundo moderno, el espectro de la anarquía criptográfica”. -Manifiesto Cripto Anarquista

Por descentralización queremos decir que todos tienen la misma oportunidad de participar, que somos plenamente inclusivos y que la autoridad para tomar decisiones es máximamente expandible, de tal manera que el sistema es resistente a la captura. La máxima descentralización teórica significa que cada individuo conserva la autoridad para influir igualmente en la toma de decisiones; Esto es difícil de implementar en la práctica al unir recursos para colaborar en un sistema común. Incluso si se implementan de una manera tan pura, las decisiones individuales se acumulan naturalmente para la eficiencia de la colaboración y los recursos se acumulan de manera desigual.

No podemos detener estas fuerzas naturales, ni hay razones para considerarlas categóricamente perjudiciales en todos los casos. Lo que podemos hacer es diseñar el sistema de manera tal que toda participación sea voluntaria, que el poder de decisión sobre la asignación de recursos esté equilibrado en una amplia gama de tipos de actores y que exista un mecanismo creíble para evolucionar con la retroalimentación. Una estructura infundida con flexibilidad es más importante que el diseño inicial del mejor sistema para adaptarse a todas las circunstancias, especialmente desde que estamos creando un movimiento tan expansivo que predecir todos los desarrollos es esencialmente imposible.

La eficiencia de la implementación es también una gran preocupación para las organizaciones descentralizadas. La descentralización pura podría sufrir parálisis de toma de decisiones, apatía de los votantes o delirios del conjunto en los extremos. Esta es la razón por la que inicialmente nos alejamos de un sistema de democracia pura para toda toma de decisiones y nos tomamos el tiempo para investigar modelos competitivos y probarlos bajo diferentes condiciones de estrés. Nuestro sistema propuesto de competencia libre y abierta para OADs (Organizaciones Autónomas Descentralizadas) está diseñado para alentar a grupos de expertos de área funcional de alto desempeño y profesionales para proponer su liderazgo en dominios especializados con el fin de que nuestra eficiencia en la conversión de recursos a productos o servicios evolucione para satisfacer las necesidades y demandas de los usuarios.

6.2 Controles y Contrapesos

Una lección clave aprendida de la historia de la humanidad es que los poderes se separan mejor y los grupos de poder competidores deben proporcionar algún estado de equilibrio de los controles y contrapesos. El equilibrio o contrapeso debe ser resistente a un crecimiento sin control en cualquier grupo de energía simple de tal manera que todo el sistema sucumbe a la captura. Para prevenir inicialmente esta condición, Zen está lanzando con un equipo principal (core team) en control del 3,5% de la financiación de recompensa en bloque, y una OAD inicial compuesto por líderes de la industria controlando el 5% de los recursos. Además, nuestro estado objetivo que se implementará después de la fase de Investigación y Desarrollo en un periodo de 12 a 18 meses incluirá un tipo híbrido de votación de múltiples interesados para que una amplia muestra de la comunidad conserve el poder de influir en las decisiones y la asignación de recursos. Cada aspecto de nuestra estructura de gobernanza estará finalmente sujeto a retroalimentación y cambio competitivo. Estamos adoptando un enfoque evolutivo que comienza con un modelo simple que crecerá con la comunidad.

7 OAD: Infraestructura, Propuestas y Votación

El sistema Zen tendrá por lo menos un OAD financiado por una parte de las recompensas mineras, y gobernado por un sistema de votación que reúne a las partes interesadas. Este sistema de gobernanza ayuda a asegurar que la implementación de cambios, mejoras e integraciones minimice la contención y reduce la posibilidad de que un desacuerdo conduzca a una bifurcación en el proyecto. A medida que desarrollemos nuestro plan más amplio de gobernanza derivado del equipo de Investigación y Desarrollo, el objetivo es abrir el panorama de la gobernanza a la plena competencia; Esto significa que podríamos ver diferentes OADs competitivas emerger con diferentes equipos trabajando en diferentes problemas. Cada OAD surgiría con su propia estructura, procesos y metas propuestas, lo que asegura que estos atributos evolucionan a través de la competencia y que las decisiones organizativas iniciales incorrectas no se vuelvan perpetuas.

Nuestras OADs serán responsables de construir, mantener y mejorar la infraestructura que mantendrá el sistema en marcha. También es responsable de implementar cambios en las aplicaciones de software Zen y es lo suficientemente flexible como para acomodarse a otras prioridades tales como: marketing, capacitación, etc.

A medida que el sistema Zen crece en popularidad, las estructuras de apoyo para usuarios, mineros, operadores de nodos seguros y socios de ecosistemas necesitarán crecer y escalar también. Las estructuras de la OAD contarán con fondos, asignados a través de proyectos y propuestas, con los que contribuirán al crecimiento y apoyo.

Se anima a la comunidad a participar en la contribución al Zen de diferentes maneras. Las OADs son responsables de coordinar las contribuciones de la comunidad y tienen fondos para ayudar a compensar los gastos incurridos por la comunidad. Uno de los propósitos de las propuestas es pagar a los miembros de la comunidad por sus gastos en el apoyo al sistema.

En el lanzamiento, Zen tendrá una OAD con profesionales respetados que abarcan industrias relevantes. Cuando el plan de gobernanza esté listo para ser implementado, esta OAD será una agrupación propuesta sujeto a la competencia del mercado para otros que deseen defender sus propias estructuras de gobierno; la comunidad tomará esa decisión.

7.1 Infraestructura Zen Operado por la OAD

El sistema de la OAD mantendrá servidores y servicios de aplicaciones, incluyendo:

- Servidor (es) de validación de nodos seguros.
- Servidor (es) del foro.
- Moderaciones pertinentes.
- Sitios web.
- Blogs.
- Sistema de propuestas.
- Sistema de votación.
- Repositorios binarios.

Las OADs son responsables del siguiente soporte:

- Ayudar a las personas a usar ZenCash u otras funciones del sistema.
- Ayuda a los operadores de nodos seguros.
- Solucionar problemas de recompensa de nodos.
- Solucionar problemas del sistema de votación.
- Proporcionar soporte a manera que va creciendo.
- Proporcionar una resolución rápida y final de alguna cuestión.

La OAD distribuye ZenCash a los propietarios de propuestas después de una exitosa votación y vencimiento del período de rechazo.

Inicialmente habrá 3-5 oficiales en la OAD, pero esto en última instancia será ilimitado. Los oficiales pueden ser anónimos, pero eso no es un requisito. De hecho, la declaración abierta de la identidad viene con la ventaja de que los logros profesionales previos y la fuerza del carácter se heredan naturalmente en el sistema Zen.

Habrá disputas y por lo tanto los mecanismos de resolución deben ser desarrollados para adjudicar estos de manera eficiente y justa. Una idea que se explorará en el proyecto de investigación y desarrollo de la Gobernanza será establecer un sistema judicial pertinente.

7.2 Presentación de Propuesta y Votación

Cada OAD tendrá su propia estructura, procesos y prioridades pero un mecanismo consistente será un sistema de propuestas de manera libre y abierta para el trabajo y un proceso de evaluación y adjudicación. No hay razón para especificar cómo sucede esto, sólo que debe suceder. Esta es una comunidad abierta a toda la humanidad, por lo que no debe haber barreras a la participación. Un método propuesto para nuestra OAD inicial es el siguiente:

1. Votar cada dos meses. Fecha límite para la presentación de propuestas dos semanas antes de la votación. Fechas de votación: 31 de enero, 31 de marzo, 31 de mayo, 31 de julio, 31 de septiembre, 31 de noviembre.
2. La presentación de la propuesta se abre un día tras votación.
3. Rechazo - el equipo principal puede vetar una propuesta dentro de los 7 días de una votación con un veto unánime del equipo principal (esto casi nunca debería de ocurrir).
4. Las propuestas pueden ser financiadas en el equivalente de ZenCash de la moneda fiat local en la fecha de la votación (evitar la cuestión de Dash de rápido aumento que conduce al rechazo del proyecto).
5. Votación hecha con acciones (tokens). 1440 tokens de votación distribuidas 1 mes antes de la votación.
6. La mayoría de las decisiones tomadas por mayoría de votos > 720 titulares de tokens que votan sí.
7. Algunas decisiones por mayoría superan el voto> 1080 titulares de tokens que votan sí.

7.3 Proceso de Votación

Plan de Distribución de Token - hecho para cada período de votación, 1440 tokens:

1. 360 tokens para la venta - permite a los usuarios y titulares de ZenCash comprar votos.

   (a) 1-30: 1 ZenCash
   (b) 31-60: 2 ZenCash
   (c) 61-90: 3 ZenCash
   (d) Etc hasta 12 ZenCash por token para el último grupo de 30
2. 240 - Desarrolladores de proyectos ZenCash.
   - Se otorga por compromisos, solicitudes de reclutamiento u otra medida razonable de contribución.
   - El objetivo es empoderar a los desarrolladores de software.
3. 60 - Centros cambiarios (exchanges) que incluyen ZenCash.
   (a) Los 6 primeros en volumen consiguen 10 cada uno.
4. 60 - Mineros propietarios de minerías en conjunto.
   (a) 1 premio cada 480 bloques al conjunto que encuentra el bloque.
5. 360 - Nodos seguros.
   (a) 1 premiado cada 40 bloques hasta que se otorguen 360 premios.
6. 120 - Oficiales de la OAD, igualmente divididos entre sí mismos.
7. 240 - Equipo principal, igualmente dividido entre los miembros del equipo.

8 NÚCLEO ZEN: Fundación y Liderazgo

El equipo principal inicialmente consiste en los tres primeros fundadores del proyecto, Joshua Yabut, Rob Viglione y Rolf Versluis. Cada fundador es un líder dentro de su respectivo dominio profesional y tiene una sólida trayectoria de experiencia en criptomonedas.

Josh es un desarrollador que trabajó anteriormente en industria aeroespacial. Él tiene una pasión para desarrollar redes resistentes a la adversidad y desea redefinir el status quo. Posee una certificación de Experto Certificado en Seguridad Ofensiva (OSCE), una maestría de la Universidad de DePaul en Gestión de proyectos de TI, y tiene amplio conocimiento en la explotación de redes gubernamentales y corporativas. Josh tiene una extensa experiencia en desarrollo de criptomonedas liderando el equipo central de Zclassic, desarrollando el z-nomp mining pool protocol, que admite la comunidad de desarrollo ZCash y consistentemente entrega software de calidad.

Rob fue anteriormente un físico, matemático y oficial militar con experiencia en radares satelitales, vehículos de lanzamiento espacial e inteligencia de apoyo de combate. Contribuciones dentro del espacio criptográfico incluye haber sido parte del equipo principal de Zclassic, apoyar al proyecto Bitshares, haber encabezado el programa de embajadores de BlockPay en EUA. y Canadá y proveer consultoría para Bitgate. Actualmente es candidato a un doctorado en finanzas en la Universidad de South Carolina investigando en temas de cripto-finanzas y enseñando "Aplicaciones de Bitcoin y Blockchain en Finanzas". Rob tiene una maestría en Finanzas y Marketing y la certificación PMP. Él es un libertario apasionado que defiende la paz, la libertad y el respeto por la vida individual.

Rolf es un propietario de negocios con experiencia en la industria de TI y posee centros mineros de tamaño mediano de Bitcoin y Zclassic (ZenCash) en Alpharetta, Georgia. Con experiencia previa en los sistemas de Cisco, la industria de los semiconductores y como oficial de formación nuclear en los EUA. en el departamento de fuerza submarina, Rolf aporta liderazgo, gestión y experiencia operativa técnica a la organización de ZenCash.

La motivación para formar una entidad como equipo principal con autoridad para tomar decisiones y un presupuesto independiente era desplegar rápidamente el sistema y ejecutar de manera eficiente un amplio rango de las primeras tareas de desarrollo que van a culminar en una red plenamente

operativa descrita en nuestro plan de trabajo; el resultado final será una transición a la estructura de gobernanza más amplia resultado del equipo de I + D y pruebas de resistencia . Nuestro objetivo es liberarnos de nuestros trabajos después de cumplir con el plan de trabajo inicial y defender nuestra primera OAD elegida por el plan de gobernanza propuesto.

9 COMUNIDAD ZEN: Grande y Fuerte

Zen está evolucionando simbióticamente con el proyecto Zclassic, con nuestra comunidad combinada de alrededor de 1.000 miembros en foros, desarrolladores, mineros, comerciantes, inversionistas a largo plazo, organizaciones asociadas, centros intercambiarios, bloggers, etc. Como un proyecto completamente abierto e inclusivo, las contribuciones y el apoyo han fluido hacia Zen de todo el mundo y este colectivo improvisado pero consistente es una de nuestras características distintivas como sistema. Nuestra comunidad ya tiene una historia duradera no sólo de relaciones positivas y de interacciones amistosas, sino también de apoyo y compromiso espontáneo emergente para prevenir o resolver problemas.

9.1 La Ética del Código Abierto

Los proyectos de código abierto pueden asumir un conjunto evolutivo y fluido de ética, sin embargo los fundadores esperan mantener a la comunidad centrada en los principios de zen, de ahí nuestro nombre. Estamos desarrollando un sistema que esperamos sea utilizado para la colaboración pacífica, la innovación libre y la máxima inclusión. Esperamos que nuestro legado sea una adición masiva positiva para la sociedad y personalmente rechazamos trabajar con cualquier persona que intente hacer daño, ya sea físico o por medio de fraude.

9.2 Soporte Zen

Soporte Zen se refiere a una comunidad de desarrolladores Zen y otros profesionales de tecnologías de la información distribuidos comprometidos con el avance de la tecnología y ofreciendo asistencia básica a los usuarios. Esta red será financiada por la OAD y servirá para que la tecnología de Zen sea la más intuitiva y fácil de relacionarse con el ecosistema.

Soporte Zen también consistirá en una red de colaboradores de diversas industrias que están comprometidos a servir como embajadores, mentores y apoyo a los colaboradores Zen. (Vea más en las subsiguientes secciones de la Comunidad Zen). Zen Soporte es un compromiso en el que Zen está estructuralmente diseñado para fomentar la inclusión, la colaboración, la ayuda colectiva y que los funcionarios ejecutivos, los Embajadores, los Empresarios Verificados o cualquier representante de la Comunidad Zen serán un recurso para que los contribuyentes puedan apoyarse y colaborar.

9.3 Alcance Zen

Nuestro plan de trabajo incluye emocionantes programas de extensión sin precedentes, que servirán para fortalecer colectivamente y facilitar el compromiso con personas de todos los ámbitos de la vida. En resumen, Zen no tiene un "mercado objetivo" en particular; ¿Cómo podríamos, Sobre todo cuando los casos de uso práctico y las implementaciones de nuestra tecnología son vastos y diversos? No pretendemos limitar la utilización de Zen a las visiones personales de nuestros miembros del equipo básico, por lo que alternativamente lanzaremos programas en el inicio diseñados para maximizar el compromiso con el Zen y permitir a los miembros de la comunidad adaptar nuestra misión e iniciativas a medida que el Zen evolucione. Nuestra OAD inicial está reservando recursos para financiar programas experimentales y recompensar contribuciones activas a nuestra comunidad. A continuación se explican algunas de las ideas propuestas para el programa.

Una vez más, el Zen es inclusivo y agnóstico, y nuestra presencia global reflejará estos valores fundamentales. Incluiremos grupos de interés tales como empresarios, activistas, desarrolladores, universidades, corporaciones y personas desinformadas pero curiosas, todas con diferentes registros de participación en el espacio de la criptografía.

A través de nuestro Programa Embajador Zen , usuarios experimentados, líderes y los miembros apasionados de la comunidad tendrán la oportunidad de representar Zen, propagando nuestra visión a la gente en los rincones del mundo sin acceso a los recursos, capital y tecnología necesarios para descubrir y unirse a nuestra comunidad por iniciativa individual. Los líderes en este programa pueden servir a muchos propósitos, desde asesorar a las startups Zen hasta realizar mentoría y capacitación Zen para representar a Zen en diversos medios informativos.

Al participar en nuestro Programa Juventud Zen , se ofrecerá a los menores codificación y desarrollo de negocios y oportunidades únicas para el compromiso con el colectivo Zen. Esta iniciativa será multifacética, con ofertas que van desde competencias globales de jóvenes para las startups financiadas por la OAD construidas en la plataforma Zen hasta loterías que asignan recursos para cubrir los gastos de educación del programa Juventud Zen. Estos jóvenes pioneros también serán movilizados para reclutar a sus compañeros y comprometer a sus comunidades. Los empresarios que gestionan proyectos financiados por la OAD serán los empresarios verificados Zen y obtendrán acceso a los beneficios relevantes de aceleración, como el acceso a mentores de negocios exitosos, canales de comercialización y adquisición de usuarios, participación abierta de desarrolladores, canales directos a inversionistas y empresas de capital de riesgo, así como eventos, asociaciones y seminarios diseñados para resolver de manera colaborativa y fomentar la innovación.

Los contribuyentes individuales tendrán acceso a contenidos plug and play diseñados para ayudar a generar movimientos de base en forma de divisiones Zen que construyan la tecnología Zen, la ética y / o el gobierno y desarrollen proyectos en todo el mundo. Estas divisiones Zen serán localizables y personalizables, con un énfasis fluido dependiendo de las necesidades de la región y la comunidad. Zen ofrecerá una plataforma en línea fundamental de recursos materiales, que incluyen:

- Contenido comercial y educativo que detalla los orígenes, especificaciones, diferenciaciones y objetivos de Zen.
- Plantillas e ideas para grupos que desean crear eventos promocionales o educativos patrocinados por Zen, conferencias y concursos.
- Módulos, discusiones y webinars sobre los principios de Zen y temas relevantes para que participen y contribuyan en las diferentes divisiones, tales como Codificación, Emprendimiento, Ética de la Descentralización, Fundamentos de Cadena de Bloques, etc.
- Plantillas para planes de negocios, documentos legales, modelos de ingresos, tácticas de adquisición de usuarios, etc; mismos que pueden promover los objetivos de las diferentes divisiones y emprender una iniciativa de desarrollo empresarial o un esfuerzo de mejora de la comunidad.
- Acceso a colaboradores y desarrolladores de Zen para apoyo, asesoría, orientación y asistencia a través de los canales de comunicación de Zen.

Por ejemplo, si se crea una división Zen en Filipinas, en donde sólo alrededor del 30% de la población tiene acceso a servicios financieros, podría comprometerse para desarrollar un proyecto FinTech que satisfaga las necesidades particulares de los filipinos y especificaciones de la cultura e infraestructura. Tal compromiso escalable podría reducir drásticamente la fricción que históricamente ha impedido a las comunidades estimular de manera autónoma sus propias economías de pequeña escala y aumentar su capacidad para competir.

La interacción virtual y la comunicación son un desarrollo inestimable del siglo XXI y serán el canal principal para conectar a miles de personas a miles de kilómetros de distancia para fomentar de manera cooperativa la innovación y el desarrollo de Zen. Dicho esto, nosotros en Zen reconocemos que hay algo sensacional en la interacción cara a cara con aquellos igualmente dedicados y movilizados alrededor de un conjunto de principios y visión común. La "Universidad Zen" es un programa de recompensa que se llevará a cabo anualmente para recompensar y comprometer a los contribuyentes más activos y de valor añadido de Zen, jóvenes en ascenso y empresarios destacados. También habrá una lotería que distribuya los boletos al azar a nodos Zen especialmente obedientes y seguros. El tema, el contenido y la intención de este evento variarán según las preferencias de la Comunidad Zen.

Nuestros recursos están destinados a nuestra Comunidad Zen que abarca muchas más categorías de participantes e iniciativas y ofrece mucho más valor que las partes interesadas tradicionales en un proyecto de criptografía. Esperamos ser tanto de un movimiento social como somos un proyecto de tecnología, el objetivo final siendo para ayudar a hacer la vida más libre y más satisfactoria para tantas personas como podamos.

10 ESCENARIO COMPETITIVO

"Hemos creído con el tiempo las empresas tienden a sentirse cómodas haciendo lo mismo, simplemente haciendo cambios incrementales. Pero en la industria de la tecnología, donde las ideas revolucionarias impulsan las próximas áreas de crecimiento, es necesario sentirse incómodo para mantenerse relevante."
-Larry Page, Alphabet

La competencia se infunde en Zen desde su esencia; por su naturaleza, es una necesidad de descentralización óptima y un principio que creemos permite una evolución beneficiosa. Este proceso también incluye la competencia en un panorama más amplio de las criptomonedas para ZenCash y para nuestro sistema en el ecosistema de plataformas de cadena de bloques.

ZenCash compite directamente con otras criptomonedas tales como: ZCash, Zclassic, Dash, Monero, ZCoin, Bytecoin, ShadowCash, Boolberry y otras criptomonedas mejoradas en aspectos de privacidad. La competencia se extiende a través de múltiples dimensiones, pero desde una perspectiva tecnológica, competimos directamente con las otras monedas con pruebas de trabajo nulo usando zk-SNARKs. ZCash fue el pionero en este campo y nuestra tecnología se beneficia directamente de sus innovadoras contribuciones. La privacidad como característica también significa que ZenCash compite con otras implementaciones, como el protocolo Zerocoin, CryptoNote, RingCT y otras más simples. Todas estas monedas sirven a un nicho en particular orientado a la privacidad dentro de la curva de demanda de las criptomonedas.

Nuestra propuesta de valor es que incorporamos elementos que consideramos que son los mejores, que comienzan con heredar la implementación de ZCash de la prueba de conocimiento nulo de blindaje a través de zk-SNARKs, pero tomamos esto un paso más allá y fortaleciendo a toda nuestra red con encriptación enruta de punto a punto, en donde el cifrado habilita la mensajería dentro de una infraestructura más segura. Es importante destacar que no tenemos la intención de ser desplazados, porque estamos estructuralmente preparados para no sólo actualizar y rejuvenecer nuestros sistemas a medida que avanza la tecnología subsecuente, sino para nosotros mismos convertirnos en los innovadores del espacio.

Zen está construyendo una arquitectura de sistema con ZenCash como su símbolo o token de valor y combustible de transacción. Como tal, también competimos con proyectos de plataforma más amplia como: Ethereum, Ethereum Classic, NEM, Lisk y Synereo sobre los cuales se pueden construir aplicaciones descentralizadas (dApps). En este dominio, el lenguaje de scripting simple de Zen, heredado de Bitcoin y ZCash, conserva alta seguridad y resiliencia para vectores de ataque, pero también limita los grados de libertad útiles para ejecuciones de código complejas, mismas que son posibles para plataformas con guiones del tipo “Turing” similares a las de Ethereum y Ethereum Classic. Nuestra ventaja en este escenario competitivo es que las dApps (aplicaciones descentralizadas) pueden ser construidas sobre la red de criptografía más segura del mundo y que somos lo suficientemente flexibles para operar a través de cadenas de alianzas estratégicas.

Nuestra innovación única para la comunidad de las criptomonedas es nuestro modelo de gobernanza evolutiva para potenciar un amplio espectro de partes interesadas en un entorno de descentralización óptima. Bitcoin creó el avance original en el consenso distribuido, pero otros proyectos han tomado esto desde entonces con varios mecanismos de votación.

Estos proyectos van desde Dash con su propuesta simple de presentación y modelo de votación comunitaria hasta Decred con su gobernanza de comunidad integrada; Cada uno de ellos ha contribuido positivamente a la evolución del consenso descentralizado, pero en Zen lo llevamos al siguiente nivel disminuyendo restricciones adicionales para que nuestro sistema evolucione con el tiempo a través de una competencia perpetua entre los proveedores de servicios de gobernanza dentro del ecosistema.

Estamos implementando un sistema autónomo que cambiará con retroalimentación e innovaciones de prueba y error de cómo los sistemas descentralizados se organizan para resolver problemas específicos. En este sentido, creemos que Zen es innovador en la tecnología social, pionero en un sistema que nunca se ha intentado escalar.

Desde una perspectiva más amplia, Zen compite con las monedas tradicionales y los sistemas bancarios existentes, así como con las nuevas empresas emergentes de fintech (tecnología financiera), con una ventaja particular en la prestación de servicios a las personas privadas de sus derechos. Elegimos hacer nuestra contribución a este espacio innovador y orientado al bienestar social proporcionando mayor privacidad y seguridad. Como sistema seguro de mensajería y distribución de datos, competimos con otros servicios, como Signal, Telegram y el Tor Project. También hay un número infinito de proyectos potenciales que se pueden construir en la plataforma Zen, aumentando exponencialmente nuestra competitividad.

Consideramos la competencia como un facilitador de procesos de crecimiento saludables y por lo tanto acogemos con satisfacción la máxima competencia. Preferimos vivir en un mundo con competidores feroces que nos obligan a acelerar nuestras propias innovaciones que un mundo estático sin progreso. Esperamos que Zen complemente positivamente al bienestar humano integrando grandes tecnologías y comunidades, transformando la gobernanza en un servicio competitivo y permitiendo que cualquier persona en el mundo participe en nuestro sistema de innovación libre, colaborativo y descentralizado. También vemos a las empresas existentes y a las futuras startups en este espacio como potenciales socios y aliados en lugar de competidores que se apoderan de todo el mercado.

11 EL FUTURO DE ZEN

La predicción es un ejercicio desafiante, pero vemos un futuro brillante para Zen y el ecosistema pacífico y productivo que estamos construyendo. Creemos que la organización descentralizada, totalmente inclusiva, voluntaria y flexible será vista de manera obvia como superior en el futuro en comparación con las versiones estáticas, centralizadas y uniformes de todas las versiones perpetuas en el siglo XX. El advenimiento de la criptografía, la filosofía del voluntariado y la tecnología de la cadena de bloques hacen posible tal cosa y creemos que muchas personas ya comparten nuestra visión de un mundo mejor; sobre todo cuando ven cómo podemos acelerar la innovación y mejorar el bienestar humano al permitir que todos expresen sus valores.

En los próximos dos años esta visión se va a materializar en nuestra organización inicial ejecutando nuestro plan de trabajo. Ciertamente habrá desafíos a lo largo del camino, pero la flexibilidad y la cooperación pacífica superan constantemente los problemas aparentemente insuperables.

Somos afortunados de vivir en una época de increíble innovación tanto en tecnología como en ideas. Estamos construyendo sobre los hombros de los gigantes proverbiales, algunos de ellos enumerados abajo, pero muchos otros van sin nombre debido a que son numerosos y fundamentales.

12 GLOSARIO

Inglés	Español
Blockchain	Cadena de bloques
Checks and Balances	Controles y Contrapesos
DAO (Decentralized Autonomous Organization)	OAD (Organización Autónoma Descentralizada)
Dapps	Aplicaciones Descentralizadas
Exchange	Centro Cambiario
Fintech	Tecnología Financiera
Governance	Gobernanza
Mining Pool	Minería en Conjunto
Proof -of- work	Prueba de Trabajo
Roadmap	Plan de Trabajo
Stakeholders	Partes interesadas
Zero-Knowledge Proof	Pruebas de Conocimiento Nulo

13 REFERENCIAS BIBLIOGRÁFICAS

[1] Juan Benet. (2014) IPFS - Contenido dirigido, versionado, Sistema de archivos P2P.

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer y Madars Virza. (2014) Zerocash: Pagos anóni-mos descentralizados de Bitcoin.

[3] Evan Duffield, Kyle Hagan. (2014) Darkcoin: Moneda de Cripto Par-a-Punto con Transacciones anónimas Blockchain y un sistema mejorado de prueba de trabajo.

[4] David Fifield, Chang Lan, Rod Hynes, Percy Wegmann y Vern Paxson. (2015) Comunicación resistente al bloqueo a través del dominio.

[5] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) Pro-tocolo Zcash Especificación Versión 2017.0-beta-2.5.

[6] May, T. (1992). El manifiesto criptoanárquico. Mediodía alta en la fron-tera electrónica: Cuestiones Conceptuales en el Ciberespacio.

[7] Nakamoto S. (2008): Bitcoin: Un sistema de dinero electrónico punto a punto.

[8] Quirk, Joe y Patri Friedman. (2017) Seasteading: Cómo las naciones flotantes restaurarán Enriquecer a los pobres, curar a los enfermos y liberar a la Políticos. Prensa Libre.

[9] Taleb, N. N. (2012). Antifragile: Cosas que ganan del desorden (Vol. 3). Aleatorio Casa.