

BORRADOR

Esta traducción es una versión preliminar. Si ve errores y desea contribuir, por favor contacte a nuestro equipo con una versión actualizada.

LIBRO BLANCO ZEN

Robert Viglione,
Rolf Versluis,
y Jane Lippencott.

Mayo 2017



ABSTRACT

Zen es un sistema encriptado de extremo a extremo con tecnología de conocimiento cero sobre comunicaciones, datos o valores que se pueden transmitir y almacenar de forma segura. Es una integración de tecnologías revolucionarias que producen un sistema de innovación acelerado combinando tres funciones que tradicionalmente están separados:

1) transacciones 2) comunicación, y 3) gobernabilidad competitiva. Esto se hace de forma segura y anónima, utilizando una cadena de bloques distribuida a nivel mundial con infraestructura informática. El sistema integra varias tecnologías de primera clase para formar una plataforma abierta para la innovación sin permisos que puede evolucionar con las preferencias del usuario.

* Los autores pueden ser contactados en rob@zensystem.io, rolf@zensystem.io, y jane@zensystem.io, respectivamente. También queremos agradecer a Jake Tarren por sus comentarios y sugerencias, así como por el Zclásico y Zen por ayudarnos a desarrollar estas ideas y hacer posible este movimiento.



CONTENIDO

1	Propósito	3
2	Historia	5
3	Especificaciones en el lanzamiento	6
4	Hoja de ruta	9
5	Elementos funcionales	11
5.1	T Transacciones	12
5.2	Z Transacciones	12
5.3	ZenTalk	15
5.4	ZenPub	16
5.5	ZenHide	16
5.6	Nodos seguros Zen	17
5.7	Nodos estándar Zen	21
5.8	Software de la carpeta ZenCash	21
5.9	Aplicaciones	21
6	Gobernanza	22
6.1	Descentralización óptima	23
6.2	Controles y saldos	24
7	DAO: Infraestructura, propuestas y votaciones	26
7.1	Infraestructura Zen Operado por DAO	27
7.2	Presentación y Votación de la Propuesta	28
7.3	Proceso de Votación	29
8	Comunidad Zen: fuerte y vibrante	33
8.1	La Ética del Código Abierto	33
8.2	Soporte Zen	33
8.3	Alcance Zen	34
9	Paisaje competitivo	38
10	El futuro del Zen	41



PROPÓSITO

“Crítica creando.” - Michelangelo Buonarroti

Vivimos en un mundo hiper-regulado y vigilado donde miles de millones de individuos son privados de los derechos humanos básicos, como la propiedad, la privacidad, la libre asociación y el acceso a la información. La tecnología ahora existe para resolver algunos de estos problemas, y la implementación temprana de Zen hará exactamente eso.

Zen es una colección de productos, servicios y negocios creado sobre tecnología que permite pruebas de cero conocimiento con un conjunto básico de creencias. Como un sistema de bloques distribuido aprovechando 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 después de Satoshi con una tecnología descentralizada, voluntario y pacífico de estructuras sociales para mejorar la vida de cualquiera que quiera participar. Creemos que esta es una idea cuyo momento ha llegado.

El marco de Zen es una infraestructura segura, orientada a la privacidad, con un sistema de gobierno estructurado para permitir a los participantes

ampliar la funcionalidad de forma colaborativa en muchas dimensiones. Las oportunidades incluyen alojamiento de los datos de identificación individual, la prueba selectiva de título para la propiedad, los servicios bancarios descentralizados, el intercambio de activos p2p / b2b que preserva la privacidad, las sociedades de ayuda mutua, seguro de p2p, los mecanismos descentralizados de ayuda humanitaria o el uso puramente como una señal anónima de valor.

Estas funciones pueden ser utilizadas para atender a las poblaciones marginadas actualmente excluidas de servicios vitales como la banca y la atención médica debido a la falta de identificación, dinero y canales seguros. También pueden ser apalancados por individuos que desean tomar la propiedad sobre y monetizar sus datos privados, o, por ejemplo, por comunidades emprendedoras que deseen desarrollar un sistema de licitación competitiva sobre la energía solar generada internamente. Las implementaciones únicas son ilimitadas, siendo el vínculo común la creencia de que la descentralización es el motor del progreso moral, y que las soluciones voluntarias son las más creativas y duraderas.



HISTORIA

Zen se basa en la herencia de los mejores “cryptocurrencies,” arquitectura de red y sistemas de intercambio de archivos distribuidos en la existencia mediante la incorporación tanto existentes como nuevas características para dar una base sólida diseñada para la viabilidad a largo plazo. Tan importante como nuestra pila de tecnología, estamos construyendo sobre las últimas ideas en consenso distribuido y gobernabilidad competitiva. Algunos de los fundamentos de nuestro proyecto provienen de Bitcoin, Dash, Decred y Seasteading.

Zcash extendió Bitcoin con transacciones protegidas totalmente anónimas, de modo que los usuarios podían elegir entre direcciones normales tipo Bitcoin (direcciones-T) o direcciones escudadas resistentes al análisis de correlación de tráfico (direcciones-Z). Entonces creamos Zclassic, un clon de Zcash que cambió algunos parámetros clave que nuestra comunidad consideró importantes: eliminamos la Recompensa de los Fundadores del 20% y el lento comienzo de la oferta monetaria. Desde el lanzamiento de Zclassic, hemos formado una comunidad vibrante de código abierto entusiasmado de mover la tecnología Zen en una dirección única. Algunos de los primeros logros incluyen el desarrollo de una aplicación de fuente de minería de código abierto para Zcash y Zclassic, también las carteras para Windows y Mac.

Nuestro equipo se dio cuenta de que Zclassic podría ampliarse como una red completamente cifrada con un modelo económico y de gobernanza innovativo que mejor se alinea con la visión original de Satoshi (inventor del Bitcoin) de una comunidad descentralizada global. Veemos Zclassic como un proyecto de código abierto de dinero críptico (cryptocurrency), mientras que Zen se extiende en una plataforma con fondos internos para facilitar un conjunto más amplio de comunicaciones, intercambio de archivos y ocupaciones.



ESPECÍFICOS EN EL LANZAMIENTO

El Zen es el sistema general sobre el cual se esparcen los tokens de ZenCash, similar a proyectos como Ethereum que tiene su token de Éter. ZenCash es una bifurca de Zclassic, y se extenderá con las siguientes características adicionales.

1. Fecha de lanzamiento: 8PM EDT, 23 de mayo de 2017 bifurcándose de Zclassic (0:00 UTC).
2. Equihash algoritmo de hash es un algoritmo de minería que es memoria intensa usando prueba de trabajo basado en el problema generalizado de cumpleaños y el algoritmo de Wagner para el.
3. Recompensa de bloque: 12.5 ZenCash.
4. Generación de bloques: 2.5 minutos.
5. Tamaño del bloque: 2 MB.
6. Dificultad ajustada algorítmicamente: Digishield V3, modificado para usar la siguiente ventana de dificultad media arrastrada:

$$\text{próxima dificultad} = \text{última dificultad} \times \sqrt{\frac{150 \text{ segundos}}{\text{Última hora de la solución}}}$$

7. División de cada recompensa de bloque PoW y honorarios de transacción entre mineros y otras partes interesadas:
 - (a) 88% a los mineros.
 - (b) 5% a uno o mas DAOs.
 - (c) 3.5% a operadores de nodos seguros.
 - (d) 3.5% al equipo central.
8. Oferta total de monedas: 21 millones.
9. La recompensa se reduce a la mitad cada ≈ 4 años, por Bitcoin.
10. Las transacciones blindados oscurecen el remitente, el receptor y la cantidad de la cadena de bloqueo.
11. Las transacciones transparentes publican el remitente, el receptor y la cantidad en blockchain.
12. Campo de mensaje seguro en la transacción z con 1024 bytes de caracteres:
 - (a) Publicación segura en ubicaciones de GUNet y / o IPFS.
 - (b) Mensajes cortos entre usuarios.
 - (c) Publique en los canales visibles por cualquier persona con la carpeta capaz de canal.
13. Los nodos seguros realizan funciones de infraestructura:
 - (a) Asegúrese de que todas las comunicaciones de red estén encriptadas entre los nodos.

- (b) Mantener la cadena de bloqueo completa de ZenCash.
 - (c) Proporcione conexiones de cifrado basadas en certificados para las aplicaciones de cartera ZenCash.
14. Los requisitos de reunión de los nodos seguros reciben premios de base de moneda.
 15. Servicio de fronting de dominios para transacciones z usando un CDN comercial.
 16. Gobierno por uno o más DAOs. (Ver sección Gobernabilidad).
 17. Zen DAOs responsable de las operaciones y mejora continua del sistema.

Ellos construirán y operarán:

- (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 central:
 - (a) Incluye fundadores del Zen.
 - (b) La misión es guiar el lanzamiento y 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.



HOJA DE RUTA

“Trial and error is freedom.” (Taleb, 2012)

Zen está lanzando como una integración de tecnologías revolucionarias para crear un sistema donde la innovación puede acelerar. Estamos estructurando la descentralización óptima y la competencia persistente para que el sistema evolucione constantemente y nunca llegue a una meseta de comodidad. La hoja de ruta inicial cubre una ventana de desarrollo de 12 a 18 meses para que el sistema funcione de forma autónoma. La clave de esto es establecer el conjunto básico de integraciones con nuestra propia red de nodos seguros, un sistema de almacenamiento de datos distribuido como GUNet y el ecosistema más amplio de intercambios, pools de minería y comunidades de usuarios. ZenCash necesita ser completamente operativo, fácilmente disponible y útil para una variedad diversa de partes interesadas. Nuestra hoja de ruta refleja el énfasis en ZenCash como nuestro primer y más importante producto inicial en la cartera Zen.

1. Desarrollar billeteras mejoradas.
 - (a) Windows para las transacciones t y z, mensajería, publicación GUNet.
 - (b) Linux para transacciones t y z, mensajería, publicación GUNet.
 - (c) Mac para las transacciones t y z, mensajería, publicación GUNet.
 - (d) Móvil (Android e iOS) para transacciones t y z.
 - (e) Hardware para transacciones t y z, mensajería, publicación GUNet.
 - (f) Carpeta Web para transacciones t y z, mensajería y publicación de GUNet.

2. Servicio de dominación de dominios para transacciones z usando un 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 Testigo Segregado.
6. Gestión de los resultados de investigación y desarrollo, incluido el sistema operacional plenamente probado (véase Gobernanza sección):
 - (a) Informe de investigación.
 - (b) Constitución.
 - (c) Sistema de votación probado e implementado.
 - (d) Primera elección de pie por lo menos un DAO, la transición del equipo central.



ELEMENTOS FUNCIONALES

Zen reúne muchos elementos diferentes para formar un todo de trabajo. En lugar de nodos regulares, Zen requiere Secure Nodes, 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 cifrada entre nodos, y entre nodos y billeteras, el zen protege contra los espionaje y los ataques de intermediario.

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 correladores de transacciones. ZenCash incorporará mensajería segura dentro de transacciones blindadas, 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 uno-a-muchos utilizando la cadena de bloques para almacenar mensajes permanentemente.

ZenPub - Una plataforma anónima de publicación de documentos utilizando GUNet o IPFS.

ZenHide - La habilidad para circunnavegar el bloqueo de criptocomercio usando fronting de dominio.

5.1 T transacciones

T son las transacciones tradicionales registradas en bloque de bloques controladas por una clave privada en una cartera. Estos son derivados de Bitcoin, y permiten una rápida compatibilidad con los intercambios, carteras y otras aplicaciones de ecosistemas derivadas de Bitcoin.

5.2 Transacciones Z

Se trata de transacciones enviadas a direcciones blindadas, heredadas de Zcash y Zclassic. Los saldos en direcciones blindadas son privados. Si pasa a una o más direcciones protegidas, el valor permanece privado, pero cualquier dirección transparente en el extremo receptor deshieldata el testigo y revelará el valor recibido en la cadena de bloques. Las direcciones blindadas de entrada y si el valor se envió desde uno o dos de éstos permanece confidencial cuando está desarmado. El protocolo Zcash describe este proceso en detalle:

El valor en Zcash es transparente o blindado. Las transferencias de valor transparente funcionan esencialmente como en Bitcoin y tienen las mismas propiedades de privacidad. El valor protegido 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 (para que haya una relación $1:1:1$ entre notas, compromisos de notas y anuladores). 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, pero el anulador no.

Una transacción puede contener entradas, salidas y secuencias 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 prover 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-privado” 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 había 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 entrada de nota 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 se basan en la mezcla de un número limitado de transacciones y que por lo tanto tienen conjuntos de trazabilidad de notas más pequeños

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 bloque. Hay un límite de 1024 caracteres para estos mensajes, y mejoran la capacidad de los usuarios para llevar a cabo el comercio seguro. En lugar de discutir la transacción en otros canales menos seguros que pueden no tener el mismo nivel de mejoras de privacidad que Zen, los usuarios pueden comunicarse a través de los mensajes ZenTalk con la otra parte o partes antes y después de la transferencia blindada tiene lugar con una transacción z muy pequeña. Gasta 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 nombre de canal, los usuarios pueden suscribirse al canal y leer cualquier cosa publicada por cualquiera en el canal.

5.4 ZenPub

Zen tiene la capacidad de publicar documentos en el IPFS o GUNet. Esto se hace publicando una dirección IPFS o GUNet en el campo de texto de una dirección z. El sistema de publicación de documentos preferido en

este momento es GUNet, 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 cripto-dineros como Bitcoin e incluso Zcash. Zen utiliza el dominio “fronting” para ampliar la capacidad de completar las transacciones entornos de red adversarial, como se explica en el bloqueo de la comunicación resistente a través del dominio frente a resumen:

Describimos el “fronting de dominio”, una técnica versátil de elusión 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 prohibido mientras parecen comunicarse con algún otro anfitrión, permitido por el censor. 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 censor bajo HTTPS encriptación.

Un censor, incapaz de distinguir el tráfico frontera y no 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 dominio frontal es fácil de implementar y usar y no requiere una coop-

eración 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 el Blockchain, aceptan transacciones de carteras, validan soluciones mineras y actúan como el sistema descentralizado de computación y comunicaciones para cripto-dineros. 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 blindadas.

Ampliación de RPC para permitir un perfecto apretón de manos secreto de secreto 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

en cola. 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) Asegúrese de que todas las comunicaciones de red estén encriptadas entre los nodos.
 - (b) Mantener bloqueo completo Zen.
 - (c) Proporcione 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 de moneda base de una manera que recompensa el tiempo de actividad con la funcionalidad completa:
 - (a) Utilice 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 Block de ZenCash en el sistema.
- (c) Proporcione un certificado SSL válido al software del nodo de ZenCash para utilizarlo para comunicarse con otros nodos y carteras.
- (d) Mantenga al menos 42 ZenCash en el servidor en una dirección t para apostar.

(e) Supervise 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) Responda al desafío con la información de identificación del nodo seguro.

(g) La respuesta al desafío será una combinación de dos cosas:

i. Enviar un mensaje protegido a “SecureNodeHQ” que contiene la dirección t pública y ubicación del documento GNUnet en el campo de mensaje.

ii. Publicar un documento en GNUnet firmado con la dirección t privada, incluyendo:

- A. Dirección pública de apostar Zen, que también se utilizará para el pago de recompensas.
- B. Certificado SSL y dirección IP.
- C. Bloquea la cabecera de blockchain.
- D. 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 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 ZenCash sistema para 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 un DAO 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 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 cifrado completa que un nodo seguro hace, todos los nodos ayudan al sistema a ejecutar la función eficientemente y permanecen resistentes al ataque.

5.8 Software de la carpeta ZenCash

El software ZenCash se puede utilizar como una cartera. La carpeta 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 para mejorar la experiencia del usuario y la seguridad de las fichas ZenCash. Las carpetas 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 muchas partes. Muchas de estas contribuciones probablemente vienen en forma voluntaria de código abierto, pero esperamos que una sólida comunidad de negocios también crezca alrededor de la plataforma. Además, el equipo central tiene un plan completo de desarrollo de aplicaciones que ya está en proceso. Esto incluye, pero no se limita a:

- Aplicación de nodos
- Piscinas Mineras de Equihash Open Source
- Aplicaciones de Gobierno
- Sistemas de Monitoreo y Reportes
- Carteras de todo tipo
- Sistema de monitoreo seguro de nodos
- Sistema de Pago de Nodos Seguros



GOBERNANCIA

“Así caen las ideologías: no por la violencia, sino por ejemplos que muestren 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 para evolucionar para adaptarse de manera óptima a nuestra comunidad. Fundamentalmente, nuestra filosofía de gobierno es 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 gobernabilidad como servicio (GaaS) y buscamos proveer valor eficientemente a nuestros grupos de interés directos, a la comunidad más amplia y al mundo.

“Cualquier industria que ofrece un servicio pobre por un alto precio merece ser interrumpida” (Quirk, 2017), la gobernanza es un ejemplo consumado. En solidaridad con otros proyectos e ideas enraizados en todo el mundo, rechazamos la centralización forzada y abrazamos el voluntariado. En lugar de confiar a una minoría del pueblo con poder, creemos que todas las personas tienen el derecho a ser confiadas con libertad.

La filosofía central 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 estado y variable 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 DAOs competidores para compartir recursos o incluso subsumir completamente versiones menos eficientes o impopulares. No debe haber una estructura invariante de tamaño único para todo el entorno, la función, la cultura o el tiempo; Más bien, las estructuras deben ser fluidas, adecuadas a problemas específicos y flexibles a escala cuando se trabaja y se desvanecen cuando fallan en relación con las alternativas. Un sistema de sistemas de este tipo evolucionaría dinámicamente de tal manera que resultara antifragado a la retroalimentación competitiva

6.1 Descentralización óptima

“Un espectro está atormentando al mundo moderno, el espectro de la anarquía criptográfica”. -Crypto Manifiesto 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 lo máximo posible difusa, 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 a ciertos actores a tasas desiguales.

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 de la manada 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 DAOs está diseñado para alentar a grupos de expertos de área funcional de alto desempeño y profesionales a proponer su liderazgo en dominios especializados para que nuestra eficiencia en todo el sistema en la conversión de recursos a productos o servicios finales de mayor valor sea Evolucionando continuamente para satisfacer las necesidades y demandas de los usuarios.

6.2 Cheques y Saldos

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 equilibrios. El equilibrio 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 central en control del 3,5% de la financiación de recompensa en bloque, y un DAO 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 I + D y prueba 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 gobernabilidad estará finalmente sujeto a retroalimentación y cambio competitivo. Estamos adoptando un enfoque evolutivo que comienza con un modelo simple que crecerá con la comunidad.



DAO: Infraestructura, Propuestas y Votación

El sistema Zen tendrá por lo menos un DAO 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 de rigurosas I + D y pruebas, el objetivo es abrir el panorama de la gobernabilidad a la plena competencia; Esto significa que podríamos ver varios DAOs competitivos emerger con diferentes equipos trabajando en diferentes problemas. Cada DAO surgiría con su propia estructura, procesos y metas propuesto, lo que asegura que estos atributos evolucionan a través de la competencia y que las decisiones organizativas iniciales incorrectas no se perpetúan.

Nuestros DAOs serán responsables de construir, mantener y mejorar la infraestructura que mantiene 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 de la comunidad, tales como alcance comunitario, 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 DAO 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. Los DAOs 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 DAO con profesionales respetados que abarcan industrias relevantes. Cuando el plan de gobernanza esté listo para ser implementado, este DAO será una agrupación propuesta sujeto a la competencia del mercado para otros que deseen defender sus propias estructuras de gobierno; La comunidad amplia tomará esa decisión.

7.1 Zen Infrastructure Operado por DAO

El sistema DAO mantendrá servidores y servicios de aplicaciones, incluyendo:

- Servidor (es) de validación de nodos seguros.

- Servidor (es) del foro.

- Moderación moderada.

- Sitios web.

- Blogs.

- Sistema de propuestas.

- Sistema de votación.

- Repositorios binarios.

Los DAOs 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 una escalada de soporte.

Proporcionar una resolución rápida y final de la cuestión.

DAO distribuye ZenCash a los propietarios de propuestas después de una exitosa votación y vencimiento del período de veto.

Inicialmente habrá 3-5 oficiales de DAO, 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.

Habrà 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 y de jurado.

7.2 Presentación de Propuesta y Votación

Cada DAO tendrá su propia estructura, procesos y prioridades, pero un mecanismo consistente será un sistema de propuestas de propuesta libre y abierta para el trabajo y un proceso de evaluación y adjudicación. No hay razón para especificar cómo esto sucede, 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 nuestro DAO 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 día tras votación.

3. Veto - el equipo central puede vetar una propuesta dentro de los 7 días de una votación con un veto unánime del equipo central (esto casi nunca debería ser hecho).
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 fichas. 1440 fichas de votación distribuidas 1 mes antes de la votación.
6. La mayoría de las decisiones tomadas por mayoría de votos > 720 titulares simbólicos votan sí.
7. Algunas decisiones por mayoría superan el voto > 1080 titulares de fichas que votan sí.

7.3 Proceso de Votación

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

1. 360 fichas para la venta - permite a los usuarios y titulares de ZenCash para 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 capacitar a los desarrolladores de software y sistemas.
3. 60 - Intercambios que llevan ZenCash.
(a) Los 6 primeros en volumen consiguen 10 cada uno.
4. 60 - Mineros propietarios de la piscina.
(a) 1 concedido cada 480 bloques a la piscina que encuentra el bloque.
5. 360 - Nodos seguros.
(a) 1 premiado cada 40 cuadras hasta que se otorguen 360 premios.
6. 120 - Oficiales de DAO, igualmente divididos entre oficiales.
7. 240 - Equipo Central, igualmente dividido entre los miembros del equipo central.



Comunidad Zen: Fuerte y Vibrante

Zen está evolucionando simbióticamente con el proyecto Zclassic, con nuestra comunidad combinada de alrededor de 1.000 miembros del foro, desarrolladores, mineros, comerciantes, inversores a largo plazo, organizaciones asociadas, intercambios, bloggers, etc. Como un proyecto completamente abierto e inclusivo, Contribuciones y apoyo han fluido hacia el Zen de todo el mundo, y este colectivo improvisado pero consistente es una de nuestras características definitorias 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 emergentes para prevenir o resolver problemas dispares.

8.1 La Ética del Código Abierto

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

8.2 Soporte Zen

Zen Support se refiere a una comunidad de desarrolladores Zen y otros profesionales de TI distribuidos comprometidos con el avance de la tecnología y ofreciendo asistencia básica a los usuarios. Esta red será financia-

da por el DAO, y servirá para que la tecnología de Zen sea la más intuitiva y fácil de relacionarse con el ecosistema. Zen Support 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 Support es un compromiso que el Zen está estructuralmente diseñado para fomentar la inclusión, la colaboración y la ayuda colectiva, y que los funcionarios ejecutivos, los Embajadores Zen, los Empresarios Verificados Zen o cualquier representante de la Comunidad Zen serán un recurso para que los contribuyentes dependan y colaborar con.

8.3 Zen Alcance

Nuestra Hoja de Ruta incluye emocionantes y sin precedentes programas de extensión que servirán para fortalecer nuestro colectivo y facilitar el compromiso con personas de todos los ámbitos de la vida. En resumen, el Zen no tiene un “mercado objetivo” singular; ¿Cómo podríamos, cuando los casos de uso práctico y las implementaciones de nuestra tecnología son vastos y diversos? No pretendemos limitar la utilización del 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. Nuestro DAO 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 Los miembros apasionados de la comunidad tendrán la oportunidad de representar el 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 mentor de los Capítulos Zen para representar el Zen en la prensa.

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 DAO construidas en la plataforma Zen a las loterías que asignan recursos para cubrir los gastos de educación de Zen Youths. Estos jóvenes pioneros también serán movilizados para reclutar a sus compañeros y comprometer a sus comunidades. Los empresarios que gestionan proyectos financiados por DAO serán los Empresarios

Verificados Zen y obtendrán acceso a los beneficios relevantes del acelerador de arranque, como el acceso a mentores de negocios exitosos, canales de comercialización y adquisición de usuarios, participación abierta de desarrolladores, canales directos a inversores y empresas de capital riesgo , Y 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 capítu-

los zen que proselijen la tecnología Zen, la ética y / o el gobierno y desarrollen proyectos en todo el mundo. Estos Capítulos 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 van desde:

Contenido comercial y educativo que detalla los orígenes, especificidades, diferenciaciones y objetivos del Zen.

Plantillas e ideas para grupos que desean crear eventos promocionales o educativos patrocinados por Zen, conferencias y cursos.

Módulos, discusiones y webinars sobre los principios zen y temas relevantes para que los Capítulos participen y contribuyan, tales como Codificación, Emprendimiento, Ética de la Descentralización, Fundamentos de Blockchain, etc.

Base de datos de planes de negocios, documentos legales, modelos de ingresos, tácticas de adquisición de usuarios, etc. para promover los objetivos de Capítulos de emprender una iniciativa de desarrollo empresarial o un esfuerzo de mejora de la comunidad.

Acceso a colaboradores y desarrolladores de Zen para apoyo, asesoramiento, orientación y asistencia vía canales Zen.

Por ejemplo, un Capítulo Zen en Filipinas, donde sólo alrededor del 30% de la población tiene acceso a servicios financieros, podría comprometerse prácticamente con el colectivo internacional para desarrollar un proyecto

FinTech que satisfaga las necesidades particulares de los filipinos y especificaciones de la cultura y 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 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 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 de un proyecto de criptotoxicidad. Esperamos ser tanto de un movimiento social como somos un proyecto de tecnología, el objetivo final puro para ayudar a hacer la vida más libre y más satisfactoria para tantas personas como podamos.



PAISAJE COMPETITIVO

“Hemos creído que 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 ser un poco incómodo para mantenerse relevante.” -Larry Page, Alphabet

La competencia se infunde en el Zen en 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 el panorama más amplio de la criptografía para ZenCash, y para nuestro sistema en el ecosistema de plataformas blockchain.

ZenCash compite directamente con ZCash, Zclassic, Dash, Monero, ZCoin, Bytecoin, ShadowCash, Boolberry y otras cripto-dineros mejoradas en privacidad. La competencia se extiende a través de múltiples dimensiones, pero desde una perspectiva tecnológica, competimos directamente con las otras monedas de conocimiento cero 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 mezcladores más simples. Todas estas monedas sirven a un nicho particular orientado a la privacidad en la curva de demanda de cripto-dinero.

Nuestra proposición de valor es que incorporamos elementos que consideramos que son los mejores, que comienzan con heredar la implementación de ZCash de cero-conocimiento de blindaje a través de zk-SNARKs, pero tomamos esto un paso crucial más allá y ofuscar a toda nuestra red con finalidad - enruta el cifrado y habilita la mensajería dentro de la infraestructura más segura del espacio. 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 subyacente, sino para nosotros mismos los innovadores del espacio.

Zen está construyendo una arquitectura de sistema con ZenCash como su símbolo de valor, o combustible de transacción. Como tal, también competimos con proyectos de tipo plataforma más amplios, 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 de una amplia gama de vectores de ataque, pero también limita los grados de libertad útiles para ejecuciones de código complejas posibles para plataformas con guiones Turing completos mejorados. Ethereum y Ethereum Classic. Nuestra ventaja en este escenario competitivo es que los dApps pueden ser contruidos sobre la red de criptocurrencia más segura del mundo y que somos lo suficientemente flexibles para operar a través de cadenas en alianzas estratégicas.

Nuestra innovación única para la comunidad de la criptoconversión es nuestra 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 la

comunidad integrada; Cada uno de ellos ha contribuido positivamente a la evolución del consenso descentralizado, pero el Zen lo lleva al siguiente nivel relajando 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 en cómo los sistemas descentralizados se organizan para resolver problemas específicos. En este sentido, creemos que el Zen es innovador en la tecnología social, pionero en un sistema que nunca se ha intentado a escala.

Desde una perspectiva más amplia, Zen compite con las monedas y los sistemas bancarios existentes, así como con las nuevas empresas emergentes de FinTech, con una ventaja particular en la prestación de servicios a los privados de 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 saludables de crecimiento 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 desprovisto de progreso. Esperamos que el Zen agregue positivamente al bienestar humano integrando grandes tecnologías y comunidades, transformando la gobernabilidad en un servicio competitivo y permitiendo que cualquier persona en el mundo participe en nuestro sistema de innovación sin permisos, colaborativa y descentralizada. También vemos a los titulares ya las futuras startups en este espacio como potenciales socios y aliados en lugar de competidores ganadores



EL FUTURO DEL ZEN

La predicción es un ejercicio desafiante, pero vemos un futuro brillante para el Zen y el ecosistema pacífico y productivo que estamos construyendo. Creemos que la organización descentralizada, totalmente inclusiva, voluntaria y flexible que estamos creando será vista como obviamente superior en el futuro en comparación con las versiones estáticas, centralizadas y uniformes de todas las versiones perpetuadas en el siglo XX. El advenimiento de la criptografía, la filosofía del voluntariado y la tecnología de bloque 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.

Los próximos de uno a dos años verán que esta visión se materializa en nuestra organización inicial ejecutando nuestra Hoja de Ruta. 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 solamente porque son tan numerosos y las contribuciones tan fundacionales.



REFERENCES

- [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 anónimos 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) Protocolo Zcash Especificación Versión 2017.0-beta-2.5.
- [6] May, T. (1992). El manifiesto criptoanárquico. Mediodía alta en la frontera 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.