

El Whitepaper de la Blockchain de Kii

Versión 2, Dic 2023

La primera blockchain layer 1 de América Latina marca el comienzo en la nueva era de tokenización de productos y commodities

Aviso legal: Este documento técnico y su contenido se proporcionan exclusivamente con fines informativos. No constituye una solicitud u oferta para la compra o venta de tokens o cualquier otro instrumento financiero y no debe interpretarse como tal. Se recomienda a los posibles poseedores de tokens que evalúen minuciosamente los riesgos potenciales y busquen orientación de sus asesores legales, financieros, fiscales y otros profesionales antes de realizar cualquier venta de tokens o cualquier inversión privada. Kii Global, junto con sus fundadores, miembros del equipo y partes afiliadas, declara explícitamente lo siguiente:

- Sin responsabilidad: No se asume ninguna responsabilidad por cualquier pérdida o daño resultante de la confianza en este whitepaper o el uso de los materiales contenidos en él.
- Incertidumbre regulatoria: el estado regulatorio de la tecnología blockchain de layer criptográfica 1 es incierto y puede sufrir cambios en diferentes jurisdicciones. Esta incertidumbre puede afectar los derechos de los poseedores de tokens; por lo tanto, tenga en cuenta las leyes de su jurisdicción.
- Información incompleta: a pesar de los esfuerzos por garantizar la precisión, el contenido de este whitepaper puede no ser exhaustivo y no implica elementos de una relación contractual.
- Sujeto a cambios: los detalles y estructuras descritos en este whitepaper están sujetos a cambios sin previo aviso, influenciados por desarrollos en curso, modificaciones regulatorias u otras razones relacionadas con el crecimiento de Kii Global.
- Sin garantías: no se brindan garantías con respecto a resultados específicos, el valor del token o el rendimiento futuro de los tokens nativos o activos subyacentes de la Kii Blockchain.
- Referencias de terceros: las referencias a datos, empresas o tecnologías de terceros no deben interpretarse como respaldos o recomendaciones.

Este descargo de responsabilidad recomienda encarecidamente a todos los participantes potenciales que realicen la debida diligencia, comprendan los detalles y riesgos específicos asociados con la blockchain de Kii Global y su token, y busquen asesoramiento profesional según sea necesario.

Abstract

Mucho ha sucedido desde el whitepaper de Satoshi que anunciaba la llegada de Bitcoin en 2008, ya que Bitcoin se ha convertido en el estándar de oro digital y se está posicionando como la moneda de reserva del mundo. En 2013, Ethereum se estableció como líder en infraestructura layer 1, iniciando el ciclo de crecimiento entre los negocios web2 y web3. Desde entonces, se han lanzado públicamente más de 10.000 tokens, cada una con su enfoque único.

El crecimiento de cada proyecto tiene un tema común dentro de la tecnología: la Comunicación. La infraestructura Blockchain conecta a los usuarios como nunca antes, eliminando una contraparte centralizada necesaria para facilitar esa conexión, y en su lugar propone cambios en la arquitectura que permiten la descentralización como el medio de comunicación preferido. Aunque este cambio ha impulsado la adopción por parte de los usuarios a nivel mundial, todavía existen brechas en la tecnología que se ajusta a las condiciones culturales y de mercado específicas de las economías emergentes.

En los países en desarrollo de América Latina, los usuarios no pueden adoptar acuerdos de blockchain donde las tarifas del gas son más costosas que el producto o servicio en sí, y muchos usuarios y empresas no comprenden los beneficios de construir sobre blockchains en el extranjero. Los actuales mecanismos de transferencia de valor que conectan a las economías emergentes con las economías desarrolladas son excesivamente centralizados, lentos y costosos. Se ha determinado que es la razón por la que las economías emergentes de los últimos 25 años aún no han “emergido” realmente. Estas redes de transferencia de valor no han logrado mejorar la globalización y el comercio local de manera eficiente, conectando a importantes contrapartes económicas para crear uniformidad en la forma en que se comunican.

Aunque económicamente son una industria muy grande, los mercados emergentes no prosperan sólo con las remesas de los usuarios en el extranjero. Sus economías normalmente se derivan de la producción local. Ya sean recursos naturales y materias primas, exportaciones de bienes, importaciones de materias primas para la producción de esos bienes; la necesidad de una red de liquidación B2B basada en productos y commodities deja en claro que el mercado B2B es 10 veces mayor que el tamaño de las remesas de los consumidores con un promedio más alto en volúmenes y

transacciones. Liquidaciones fiduciarias más rápidas, soluciones cambiarias más seguras y acceso a condiciones crediticias internacionales son sólo algunos de los puntos débiles actuales del mercado.

Kii Blockchain está firmemente comprometido en ofrecer soluciones blockchain de alto rendimiento, interconectadas y ultraseguras como motor del desarrollo económico en los mercados emergentes para mejorar la comunicación y la globalización. En el corazón de nuestra destreza tecnológica está el mecanismo Tendermint, una solución para los problemas que existen en la economía, particularmente en las economías emergentes y en América Latina. Sin embargo, más que una simple blockchain, Kii Global ha creado un ecosistema de soluciones que incluyen un exchange centralizado que agiliza la liquidez institucional a una variedad de soluciones de efectivo fiduciario de bajo costo y una sólida aplicación móvil DeFi que ofrece una variedad de soluciones de intercambio y custodia de bajo costo.

Introducción a Kii

La layer One Blockchain de Kii Global es un ecosistema pionero de tokenización y liquidación de pagos diseñado para América Latina y los mercados emergentes. Se combina perfectamente con las infraestructuras de pago predominantes, con el objetivo de aliviar los costos exorbitantes y reducir las barreras en las transacciones económicas.

Este sistema se basa en el Cosmos Tendermint BFT, un testimonio de su descentralización y compromiso para lograr transacciones ultrarrápidas y tarifas de red minúsculas. Principalmente, su diseño se adapta a las exigencias diarias de las economías emergentes, considerando los desequilibrios de riqueza que existen. El mecanismo Tendermint de Kii cuenta con validadores ultrarrápidos que producen bloques en segundos, lo que permite tiempos de transacción instantáneos y una tarifa en la red de menos de *un peso*.

El plan Kii experimentó una expansión dentro de su conjunto de productos y aplicaciones, incorporando billeteras móviles descentralizadas y un exchange centralizado (KIIEX) específicamente conceptualizado para asimilaciones de liquidación de pagos. El conjunto de productos proporciona infraestructura institucional y liquidez que conecta a los actores globales con los operadores locales. Kii Blockchain es personalizable y admitirá contratos inteligentes escritos e implementados con Solidity.

Reconociendo los costos exorbitantes asociados con los pagos locales y globales y la necesidad palpable de una solución más rápida y rentable, Danyel Arenas y Alex Cavallero forjaron el concepto Kii Blockchain. ¿Su visión colectiva? Esculpir un ámbito de

pagos sólido, seguro y escalable que marque el comienzo de la próxima generación de productos y commodities tokenizados, ofreciendo ahorros de primer nivel y accesibilidad para los principales impulsores económicos de la región.

Filosofía y Visión de Kii Global

Si bien el espacio de las criptomonedas está saturado con una gran variedad de opciones, Kii Global se distingue por su profundo compromiso con el mejoramiento social. Más allá de las maravillas técnicas y las perspectivas financieras, el espíritu de Kii se basa en fomentar un panorama financiero accesible e inclusivo, especialmente para la comunidad latina.

Actualmente, el 50% de los ciudadanos de los países en desarrollo no están bancarizados. La razón principal: sus ingresos no son suficientes para pagar los costos mensuales asociados con los servicios financieros tradicionales. Como resultado, estos usuarios, y muchas pequeñas empresas asociadas, carecen de acceso a servicios financieros básicos y líneas de crédito.

A medida que el mundo gira rápidamente hacia un paradigma financiero descentralizado, Kii se visualiza a sí mismo a la vanguardia, no simplemente como un participante pasivo sino como un agente activo de cambio. Al iterar continuamente sus ofertas, forjar asociaciones significativas y mantenerse en sintonía con las necesidades del mundo real de sus usuarios, Kii no solo está construyendo una blockchain; está diseñando el futuro de las finanzas mediante el desarrollo de soluciones de costo fijo cero con soluciones que resuelven problemas de liquidación.

En el fondo de todo esto, Kii Global es más que una simple blockchain o una empresa de criptomonedas. Es un rayo de esperanza, una promesa de un futuro financiero más brillante y un testimonio de lo que es posible cuando la *innovación se une a la empatía*. Nuestro principal objetivo: *crear un cambio sistémico en la clase media*.

Gama de Productos del Ecosistema

Kii Global está construyendo un ecosistema para respaldar la próxima generación de tokenización en los mercados emergentes.

La Blockchain de Kii – una layer 1

La Blockchain de Kii es una layer 1 compatible con EVM y Rust diseñada para liquidación de pagos y tokenización de productos y commodities. Las transacciones en la blockchain se procesan más rápido de lo que tarda un dispositivo móvil en actualizar

una página web. Los costos de procesamiento y las tarifas gas serán una fracción de peso y no se inflarán más de una fracción de centavo.

Infraestructura de la Billetera

La Blockchain de Kii está integrada dentro del conjunto de opciones de Cosmos pero ha creado productos personalizados integrados con Keplr. Estas billeteras se pueden vincular a las billeteras web de Kii Blockchain, así como a la aplicación de Block Explorer. Además, disponible en iOS y Android, los usuarios pueden almacenar, enviar, recibir y stake su KII en la aplicación móvil Kii Wallet. Los usuarios pueden optar por administrar sus claves de forma privada o crear una cuenta centralizada. Al enviar y recibir KII, los usuarios pueden seleccionar su validador de preferencia.

KIIEX: Liquidez Centralizada para Pago Inmediato y APIs Abiertas.

Parte del ecosistema de Kii Global es KIIEX, una plataforma de intercambio (exchange) centralizada que brinda liquidez institucional y liquidación inmediata a los lugares que más lo necesitan. Además de operar como una plataforma comercial tradicional, KIIEX está poniendo a disposición en el mercado los instrumentos fiduciarios/criptográficos más populares de la región. Al integrar verticalmente la infraestructura de entrada y salida de efectivo, KIIEX está transformando la eficiencia de costos y los tiempos de liquidación en la región. Dentro de su conjunto de productos hay API abiertas donde las corporaciones y las aplicaciones de pago o DeFi pueden acceder a estas opciones de pago de liquidez.

La App DeFi de KIIEX

La billetera Kii está pasando a ser la billetera KIIEX DeFi, donde los usuarios pueden administrar sus propias claves y almacenar sus activos preferidos. Sin embargo, en lugar de tener solo la opción de intercambiar entre opciones DEX con altos costos de transacción y máximo bajo, la aplicación DeFi tendrá conectividad con KIIEX a través de conexiones API que permitirán intercambios instantáneos a costos significativamente más bajos que los DEX tradicionales.

Los Problemas Que Resuelve Kii

Sin lugar a duda, la infraestructura blockchain actual resuelve muchos problemas importantes dentro de una red de liquidación de transferencia de valor. Sin embargo, Kii está diseñado para resolver los problemas actuales de la industria dentro de su enfoque geográfico.

Las Mejores Liquidaciones en Efectivo en Latam

Los principales proveedores de remesas y pagos, atados a sistemas bancarios arcaicos como ACH y SWIFT, luchan contra ineficiencias, tardanzas y costos inflados. Sus contrapartes modernas, basadas en tecnología de contabilidad descentralizada, a menudo fallan en la "última milla", lo que hace que sus soluciones P2P sean antieconómicas.

El ecosistema de Kii Global ofrece una rampa de entrada y salida mucho mejor que cualquier otro proveedor en Latam. Los servicios típicos de entrada y salida tienen límites, retrasos y, en general, no son una forma confiable de incorporarse a cripto o de salir de las criptomonedas. Kii puede utilizar la infraestructura financiera local porque ha establecido relaciones con los bancos locales, lo que hace que sus servicios sean de bajo costo, confiables y sin grandes demoras. Una característica destacada del exchange es su énfasis en la "entrega de última milla", que aborda la importancia de los pares de liquidez profundos frente al dinero fiduciario local y la verticalización eficiente de sus vías de entrada y salida por menos del 1% de costo.

Escalabilidad de la Tarifa Gas para el Usuario Sensible a IBC

Existen problemas de escala en la infraestructura blockchain actual porque la cantidad de transacciones procesadas en segundos está limitada a la potencia de procesamiento total. Por ejemplo, Ethereum 2.0 apenas puede procesar aproximadamente 30 transacciones por segundo, por lo tanto, debe depender de fragmentación (sharding) y acumulaciones (rollups) para escalar horizontalmente y mantener el flujo de transacciones a costos mínimos. Las altas tarifas gas en Ethereum (\$5 - \$20 USD nominales) han impedido una adopción a gran escala entre los mercados emergentes. Hasta ahora, la mayor parte de la adopción se ha centrado en redes de gas más económicas como Tron. Sin embargo, estas redes están cada vez más congestionadas y la necesidad de una solución descentralizada estructurada y más sólida es evidente.

Cosmos BFT Tendermint puede procesar aproximadamente 10.000 transacciones por segundo y está prediseñada dentro del Inter-Blockchain Communication Pool (IBC). IBC trabaja en conjunto con otras layer 1 en la comunidad cosmos para procesar transacciones y mantener las tarifas gas mínimas *para siempre*.

Acceso a Liquidez y Crédito Institucional

El 50% de las personas en los mercados emergentes no cuentan con servicios bancarios suficientes y tienen un acceso extremadamente limitado a condiciones crediticias. El otro 50% lucha con altos costos bancarios y tasas de interés. Kii Global, por

medio de su layer 1 con infraestructura para opciones de préstamos DeFi combinado con pagos de liquidez de su exchange centralizado está resolviendo estos problemas.

Al reducir las disparidades de capital entre las economías desarrolladas y emergentes, el ecosistema Kii respaldará una amplia gama de protocolos de préstamos DeFi diseñados para los mercados emergentes en paralelo con liquidez abierta de KIIEX a aplicaciones centralizadas.

Tokenización Amigable

Las blockchains basadas en Cosmos están diseñadas para implementar contratos inteligentes escritos en Rust e implementados a través de CosmWasm. Aunque Rust es un lenguaje de código avanzado con sus beneficios, faltan desarrolladores del mundo real que comprendan Rust y empresas que busquen implementar sus contratos con ese lenguaje.

Kii Blockchain ha codificado en el popular lenguaje Solidity para crear y lanzar contratos inteligentes, lo que hace que Kii Blockchain EVM sea compatible. Los usuarios pueden implementar fácilmente sus contratos inteligentes, ya escritos en Solidity, en la Kii Blockchain. Kii Global ha creado un equipo interno dedicado para ayudar a implementar contratos inteligentes de los usuarios dentro de la blockchain. Las empresas que buscan ayuda sobre cómo crear contratos inteligentes pueden confiar en los desarrolladores de Kii Global para obtener soporte y asistencia al escribir e implementar código.

Un Ecosistema Equitativo Construido para Latinoamérica

El token de Kii y Kii blockchain brinda a los locales de Latinoamérica la oportunidad de participar en un ecosistema creado solo para ellos y del que pueden poseer una parte. Los usuarios pueden obtener un rendimiento de su KII por medio de staking a través de nodos validadores, y las recompensas se reponen con el 5% del flujo de caja de Kii Global. Esto le brinda a cada latinoamericano la oportunidad de ser parte de una comunidad y una empresa con una visión de justicia equitativa para todos.

Un Ecosistema Compatible

KII no corre el riesgo de un contrapuesto con el gobierno y los bancos locales, porque el equipo de Kii ha realizado el arduo trabajo de educar y construir relaciones con los principales bancos y funcionarios gubernamentales de Latam. Si bien la mayoría de las instituciones financieras tradicionales tienen estigma y falta de conocimiento Crypto, Kii está allanando el camino al construir la infraestructura necesaria para ofrecer servicios de liquidación de efectivo sin fricciones. El equipo de Kii es un ejemplo brillante de lo que es lo correcto cuando se trata de cumplimiento.

Casos de Uso

Liquidación de Pagos y Remesas

Al bloque número 1, Kii Blockchain puede procesar 10.000 transacciones por segundo (TPS) y puede escalar dentro del ecosistema Cosmos con IBC. Actualmente, la comunidad Cosmos está sincronizada colectivamente para procesar ~500.000 TPS y, dependiendo de la inclusión de futuras layer 1, el procesamiento puede aumentar a un *número infinito*. Las tarifas de transacción en Kii Blockchain son una fracción de un peso y la liquidación es instantánea. Los usuarios pueden enviar fondos sin problemas a cualquier billetera del mundo.

Tokenización de Commodities

Los commodities se encuentran entre los bienes más valiosos y comercializados del mundo y las principales reservas se extraen y desarrollan en los países emergentes. Las empresas locales ahora pueden tokenizar sus commodities y contratos, valorándolos en KII o en un activo nativo de su proyecto y crear liquidez instantánea a escala global.

Tokenización de productos

Los bienes importados y exportados son uno de los principales impulsores del PIB en América Latina y las economías emergentes. Muchas empresas multinacionales de la región luchan por procesar fondos y gestionar las reservas de liquidez. Estos productos se pueden tokenizar y realizar transacciones en blockchain para que los usuarios realicen transacciones con estos bienes y para que las empresas administren mejor sus reservas.

Préstamos y Endeudamiento DeFi para un Sistema de Crédito Abierto

El crédito es un gran problema en los países en desarrollo con estrictas normas de suscripción, niveles tóxicos de tasas de interés y falta de capital disponible. Los préstamos DeFi proporcionarán formas seguras para que los usuarios de los países desarrollados extiendan condiciones de crédito seguras a los participantes en los mercados emergentes.

Yield Farming

Las oportunidades de alto rendimiento abundan en Latam y pueden ayudar a generar este rendimiento productivo para que los agregadores de yield farming lo ofrezcan a los prestamistas con liquidez.

Liquidación al Contado y a Plazo

El mercado de remesas B2B realiza transacciones por más de 600 mil millones de dólares. Estos importadores y exportadores ganan o pierden en acuerdos de contratos al contado o a plazo. Cuando cada contraparte publica liquidez a través de un contrato inteligente en la blockchain, los usuarios pueden eliminar pérdidas al participar en operaciones swing FX.

Protección Contra la Inflación

Kii blockchain tiene un suministro fijo de 1.800.000.000 KII sin *minting* o *burning* de monedas. Por lo tanto, el monto total nunca puede inflarse. De hecho, según el contrato, el 5% del flujo de caja de las operaciones de Kii Global se revertirá a la compra de KII y a la reposición del fondo de staking y recompensas.

Modelo de Negocio y Fuentes de Ingresos

La actividad de Kii Global se impulsará a través del conjunto de productos generadores de ingresos:

Tarifas de Negociación y Procesamiento de KIIEX

Al inaugurar nuestra propia plataforma de exchange centralizado, estamos revolucionando la experiencia de remesas y pagos para los usuarios. Este nexo del comercio de criptomonedas garantiza transacciones fluidas y al mismo tiempo fomenta un entorno de crecimiento y prosperidad financiera. KIIEX lidera el mercado de opciones de entrada y salida de efectivo en Latam.

Tarifas de Negociación Billetera DeFi

Nuestra billetera descentralizada multidivisa propia ofrece a los usuarios un refugio seguro para sus activos. Las tarifas nominales de negociación y transferencia no solo garantizan la asequibilidad para nuestros usuarios, sino que también sirven como una fuente de ingresos sostenible para el ecosistema Kii. Esta billetera, adaptada a las necesidades del usuario, ejemplifica la combinación de seguridad, funcionalidad y rentabilidad, convirtiéndose en una herramienta indispensable para todo entusiasta de las criptomonedas.

Comisiones DeFi

El 5% del suministro total se destina a liquidez para las operaciones DEX y, después de la venta pública, ese 5% se igualará en liquidez en el otro lado de la operación. Estas operaciones generarán ingresos para el holding.

Tarifas de Integraciones

Nuestra huella en el espacio blockchain no ha pasado desapercibida. Al integrar el sólido ecosistema de Kii en empresas de tecnología financiera convencionales, hemos forjado un modelo de ingresos en el que obtenemos una parte de cada transacción realizada a través de nuestras ofertas de infraestructura.

Conjunto Secundario de Productos

Además de las principales fuentes de ingresos, la hoja de ruta de Kii Global implica el lanzamiento de un conjunto de productos de banca como servicio, como tarjetas de procesamiento de almacenamiento frío, que generarán aún más ganancias para la empresa.

Características de Kii Blockchain

Introducción a Kii Blockchain: *Aprovechando la Superioridad de Tendermint en la Arquitectura Blockchain para el Desarrollo Económico en Mercados Emergentes.*

Información técnica proporcionada por Cosmos.

Cosmos es una red de blockchains paralelas independientes, cada una de las cuales funciona con algoritmos de consenso BFT clásicos como Tendermint 1. Kii Blockchain es su propia blockchain layer 1 independiente que se conectará al Cosmos Hub para aprovechar sus beneficios.

Cosmos Hub es la blockchain inaugural de esta red y sirve como un punto de conexión fundamental con varias otras cadenas de bloques (denominadas aquí como Zonas), incluida Kii Blockchain, a través del novedoso e innovador protocolo Inter-Blockchain Communication (IBC). Esta mantiene un registro de múltiples tipos de tokens y sus cantidades en todas las Zonas vinculadas. Gracias a este sistema, los tokens se pueden transferir de forma rápida y segura entre Zonas sin necesidad de un intercambio directo, ya que todas las transferencias entre zonas se canalizan a través del Cosmos Hub.

Este diseño aborda varios desafíos que enfrenta actualmente el sector blockchain, incluida la interoperabilidad de aplicaciones, la escalabilidad y la fácil actualización. Cosmos Hub es compatible con diversos sistemas blockchain como Bitcoin, Go-Ethereum, CryptoNote y BNB, lo que facilita una escalabilidad infinita para satisfacer las demandas de transacciones en todo el mundo. Además, su arquitectura es adecuada para usos intersectoriales como exchanges descentralizados.

Cosmos se extiende más allá de un libro de contabilidad distribuida solitaria, y Cosmos Hub no es un ecosistema aislado ni su punto focal. Más bien, es parte de una visión más amplia para crear una red abierta de libros de contabilidad distribuidos, sentando las

bases para nuevos sistemas financieros basados en criptografía, principios económicos sólidos, teoría del consenso, transparencia y responsabilidad.

Aspectos Técnicos Clave

Velocidad de Transacción Inigualable

Olvídense de la agonizante espera de las lentas confirmaciones de transacciones. El algoritmo de consenso Byzantine Fault Tolerant (BFT) de Tendermint produce resultados rápidos. La velocidad es una prioridad y Tendermint no decepciona.

Seguridad Sólida

¿Cuál es el beneficio de tener velocidad si se está comprometiendo la seguridad? Con Tendermint, no es necesario hacer ese intercambio. Sus propiedades BFT garantizan que, a menos que más de un tercio de la red se vea comprometida, sus datos serán impenetrables. Es una promesa firme de confiabilidad, y se alinea perfectamente con el compromiso que Kii Blockchain tiene con una seguridad sólida.

Interacciones Fluidas Entre Cadenas

En el panorama digitalizado actual, trabajar en silos es una fórmula para el estancamiento. La arquitectura de Tendermint se nutre de la interoperabilidad, lo que permite interacciones fluidas entre blockchains dispares. Kii Blockchain aprovecha esta característica para allanar el camino para operaciones ilimitadas entre cadenas.

Sostenibilidad en el foco

A medida que se intensifica la conciencia global sobre el cambio climático, Tendermint ofrece una alternativa ecológica a los mecanismos de consenso que consumen mucha energía. Esto se alinea perfectamente con los objetivos propios de sostenibilidad de Kii Blockchain. En pocas palabras, Tendermint no es sólo un mecanismo; es un modelo para el futuro de la tecnología blockchain. Al integrar Tendermint en nuestra arquitectura, Kii Blockchain no solo sigue el ritmo de los avances; nosotros estamos marcando el ritmo.

Fundamentos Técnicos de Tendermint: Un Algoritmo de Consenso Avanzado Distinguido en Eficacia

La eficacia de una arquitectura blockchain depende, en gran medida, de la solidez de su algoritmo de consenso subyacente. Tendermint se distingue como un ejemplo en este campo y es instructivo profundizar en sus complejidades operativas para comprender su superioridad.

Rondas de Consenso Secuenciales: Un Paradigma Tripartito

El modelo de consenso de Tendermint opera a través de una secuencia tripartita que comprende las fases de Prevote, Precommit y Commit. Esta construcción algorítmica genera un enfoque organizado y determinista para la toma de decisiones.

Prevote: En esta fase, los validadores participan en una ronda de votación preliminar para sopesar la validez de un bloque propuesto.

Precommit: condicionado a la obtención de un quórum de votos previos afirmativos (específicamente una mayoría de dos tercios), el algoritmo pasa a un commit más formalizado con el bloque propuesto.

Commit: Una afirmación posterior en esta fase culmina con la aceptación irrevocable del bloque en la blockchain. Esta disposición secuencial garantiza la integridad del procedimiento y minimiza el potencial de inserciones erróneas o maliciosas.

Finalidad Determinista: Un Punto de Referencia en la Integridad de las Transacciones

Mientras que varias plataformas blockchain emplean finalidad probabilística, Tendermint asegura finalidad determinista. Una vez que una transacción obtiene la aprobación por consenso, queda irrevocablemente comprometida con el libro de contabilidad público, eliminando así cualquier ambigüedad o vulnerabilidad posterior.

Byzantine Fault Tolerance: Mitigación de Riesgos Sistémicos

Una de las características más destacadas de Tendermint es su capacidad para mitigar el problema de los Generales Bizantinos, un dilema clásico en la informática distribuida. La tolerancia a fallas bizantinas de Tendermint garantiza que la red mantenga su integridad funcional incluso cuando hasta un tercio de sus nodos están comprometidos o no funcionan correctamente.

Economía Proof-of-Stake: Un Enfoque Ecológico

En yuxtaposición a los algoritmos Proof-of-Work que consumen mucha energía, Tendermint emplea un modelo Proof-of-Stake. Esto hace que el proceso de consenso no sólo sea más eficiente sino también congruente con los protocolos de utilización de energía sostenible.

Tendermint BFT Implica Negocios

Lanzado en 2014, el proyecto de código abierto Tendermint tenía como objetivo superar las limitaciones del algoritmo de consenso proof-of-work de Bitcoin, particularmente en términos de velocidad, escalabilidad e impacto ambiental. Aprovechando y mejorando los algoritmos de Byzantine Fault Tolerance (BFT) desarrollados originalmente en MIT en 1988, el equipo de Tendermint fue pionero en el desarrollo conceptual de una criptomoneda proof-of-stake. Esta innovación abordó con éxito el problema de

"nothing-at-stake" ("nada en juego"), un problema frecuente en las primeras criptomonedas proof-of-stake como NXT y BitShares1.0.

Hoy en día, la mayoría de las billeteras móviles de Bitcoin dependen de servidores confiables para la verificación de transacciones debido a la necesidad de múltiples confirmaciones proof-of-work para garantizar que una transacción se confirme de manera irreversible. Esto ha llevado a exitosos ataques de doble gasto en plataformas como Coinbase.

Por el contrario, el sistema de consenso blockchain de Tendermint permite una verificación segura e inmediata de los pagos de clientes móviles. Diseñado para evitar la bifurcación por completo, Tendermint permite que las billeteras móviles confirmen transacciones al instante, facilitando pagos prácticos y de poca confianza en teléfonos inteligentes; lo que también es beneficioso para las aplicaciones de Internet de las Cosas.

Los validadores de Kii funcionan de manera similar a los mineros de Bitcoin, pero utilizan firmas criptográficas para votar. Estos validadores, que operan en máquinas seguras y dedicadas, son responsables del commit del bloque. Los no validadores pueden delegar sus KII tokens a los validadores, ganando una parte de las tarifas de bloque y las recompensas de Kii (Kii Rewards). Sin embargo, existe el riesgo de recibir una penalización (slashing) si el validador elegido se ve comprometido o infringe las reglas del protocolo. La confiabilidad comprobada del consenso BFT de Tendermint y los depósitos de garantía tanto de los validadores como de los delegados brindan un nivel de seguridad mensurable y confiable para todos los nodos de la red y clientes light.

Gobernanza

Cada libro de contabilidad público distribuido debería incluir una constitución y un mecanismo de gobernanza. Bitcoin, por ejemplo, depende de la Fundación Bitcoin y su comunidad minera para gestionar las actualizaciones, un proceso que tiende a ser lento. Ethereum experimentó una división en ETH y ETC luego de un *hard-fork* para rectificar el hackeo de TheDAO, principalmente debido a la ausencia de un contrato social establecido o un proceso de toma de decisiones.

En Kii Blockchain, tanto los validadores como los delegados tienen el poder de votar respecto de propuestas. Estas propuestas pueden modificar automáticamente la configuración del sistema (como el límite gas del bloque), facilitar actualizaciones o modificar la constitución legible por humanos de la blockchain, que dicta sus políticas. Esta constitución proporciona un marco para que las partes interesadas aborden de forma rápida y eficaz problemas como robos o errores, similar al incidente de TheDAO.

La red Kii Blockchain, con su compromiso con la interoperabilidad entre diferentes zonas políticas, ofrece a los usuarios una libertad incomparable y oportunidades para la experimentación sin restricciones. Está previsto introducir la gobernanza abierta en Kii Blockchain dentro de los 12 a 24 meses posteriores al lanzamiento.

Validadores

En los algoritmos bizantinos clásicos tolerantes a fallas (BFT), cada nodo tiene el mismo peso. En Tendermint, los nodos tienen una cantidad no negativa de poder de voto, y los nodos que tienen poder de voto positivo se denominan validadores. Los validadores participan en el protocolo de consenso transmitiendo firmas criptográficas o votos para acordar el siguiente bloque.

Los poderes de voto de los validadores se determinan en la génesis o la blockchain los cambia de manera determinista, según la aplicación. Por ejemplo, en una aplicación proof-of-stake como Kii Blockchain, el poder de voto puede estar determinado por la cantidad de tokens de staking vinculadas como garantía.

NOTA: Fracciones como $\frac{2}{3}$ y $\frac{1}{3}$ se refieren a fracciones del poder de voto total, nunca al número total de validadores, a menos que todos los validadores tengan el mismo peso. $>\frac{2}{3}$ significa “más de $\frac{2}{3}$ ”, $\geq\frac{1}{3}$ significa “al menos $\frac{1}{3}$ ”.

Consenso

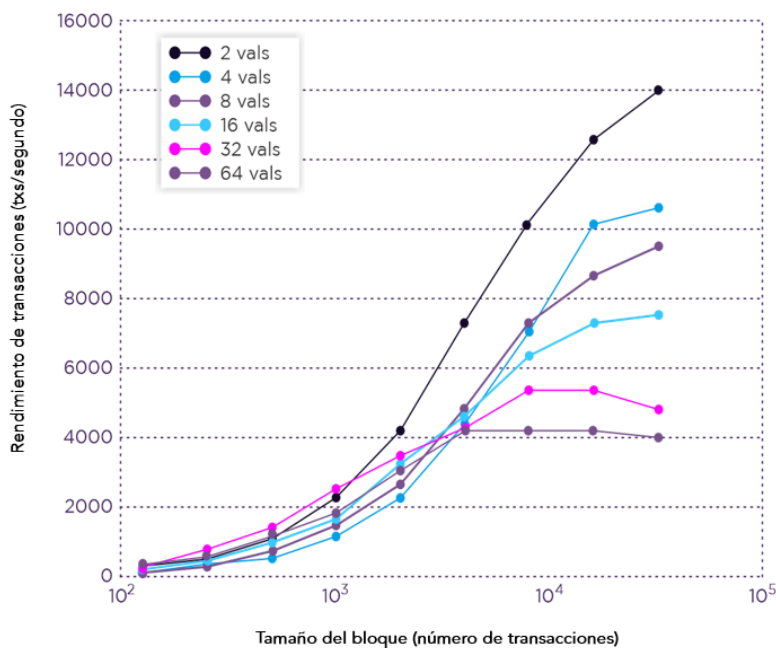
Tendermint es un protocolo de consenso BFT parcialmente sincrónico derivado del algoritmo de consenso DLS [20]. Tendermint se destaca por su simplicidad, rendimiento y responsabilidad en la bifurcación. El protocolo requiere un conjunto fijo conocido de validadores, donde cada validador se identifica por su clave pública. Los validadores intentan llegar a un consenso sobre un bloque a la vez, donde un bloque es una lista de transacciones. La votación por consenso sobre un bloque se realiza en rondas. Cada ronda tiene un líder de ronda, o proponente, que propone un bloque. Luego, los validadores votan, por etapas, sobre si aceptan el bloque propuesto o pasan a la siguiente ronda. El proponente de una ronda se elige de forma determinista de la lista ordenada de validadores, en proporción a su poder de voto.

La seguridad de Tendermint se deriva de su uso de una tolerancia bizantina óptima a fallos mediante votación supermayoría ($>\frac{2}{3}$) y un mecanismo de bloqueo. Juntos, aseguran que:

- $\geq\frac{1}{3}$ del poder de voto debe ser Bizantino para causar una violación de la seguridad, cuando se cometen más de dos valores.

- Si algún conjunto de validadores alguna vez logra violar la seguridad, o incluso intenta hacerlo, el protocolo puede identificarlos. Esto incluye tanto votar por bloques en conflicto como difundir votos injustificados.

A pesar de sus sólidas garantías, Tendermint ofrece un rendimiento excepcional. En pruebas comparativas de 64 nodos distribuidos en 7 centros de datos en 5 continentes, en instancias de nube de productos básicos, el consenso de Tendermint puede procesar miles de transacciones por segundo, con latencias de confirmación del orden de uno a dos segundos. En particular, el rendimiento de más de mil transacciones por segundo se mantiene incluso en condiciones adversas, con validadores que fallan o transmiten votos elaborados con fines malintencionados. Consulte la figura a continuación para obtener más detalles.



Cientes Light

Un beneficio importante del algoritmo de consenso de Tendermint es la seguridad simplificada del cliente light, lo que lo convierte en un candidato ideal para casos de uso móviles y de Internet de las Cosas. Mientras que un cliente light de Bitcoin debe sincronizar cadenas de encabezados de bloques y encontrar el que tenga mayor proof of work, los clientes light de Tendermint solo necesitan mantenerse al día con los cambios en el conjunto de validadores y luego verificar $>2/3$ Precommits en el último bloque para determinar el último estado.

Las pruebas sucintas de los clientes light también permiten Inter-Blockchain Communication (comunicación entre blockchains).

Prevención de Ataques

Tendermint tiene medidas de protección para prevenir ciertos ataques notables, como la censura y el doble gasto de largo alcance sin nada en juego (long-range-nothing-at-stake double spends).

ABCI

El algoritmo de consenso de Tendermint se implementa en un programa llamado Tendermint Core. Tendermint BFT es un "motor de consenso" independiente de la aplicación que puede convertir cualquier aplicación determinista de blackbox en una blockchain replicada distribuida. Tendermint BFT se conecta a aplicaciones blockchain a través de la Interfaz Blockchain de Aplicaciones (Application Blockchain Interface, por sus siglas en Ingles ABCI). ABCI es una interfaz que define el límite entre el motor de replicación (la blockchain) y la máquina de estados (la aplicación). Al utilizar un protocolo de socket, permitimos que un motor de consenso que se ejecuta en un proceso administre el estado de una aplicación que se ejecuta en otro. Por lo tanto, ABCI permite programar aplicaciones blockchain en cualquier lenguaje, no solo el lenguaje de programación en el que está escrito el motor de consenso. Además, ABCI permite intercambiar fácilmente la capa (layer) de consenso de cualquier pila blockchain existente.

Hacemos una analogía con la conocida criptomoneda Bitcoin. Bitcoin es una blockchain de criptomonedas donde cada nodo mantiene una base de datos de salida de transacciones no gastadas (Unspent Transaction Output, por sus siglas en Ingles UTXO) completamente auditada. Si uno quisiera crear un sistema similar a Bitcoin además de ABCI, Tendermint BFT sería responsable de

- Compartir bloques y transacciones entre nodos
- Establecer un orden canónico/inmutable de transacciones (la blockchain)

Mientras tanto, la aplicación ABCI sería responsable de

- Mantener la base de datos UTXO
- Validar firmas criptográficas de transacciones.
- Evitar que las transacciones gasten fondos inexistentes

- Permitir que los clientes consulten la base de datos UTXO

Tendermint puede descomponer el diseño de blockchain ofreciendo una API muy simple entre el proceso de aplicación y el proceso de consenso.

ABCI consta de tres tipos de mensajes principales que se envían desde el núcleo a la aplicación. La aplicación responde con los mensajes de respuesta correspondientes.

El mensaje *AppendTx* es el caballo de batalla de la aplicación. Cada transacción en la blockchain se entrega con este mensaje. La aplicación debe validar cada transacción recibida con el mensaje *AppendTx* con el estado actual, el protocolo de la aplicación y las credenciales criptográficas de la transacción. Luego, una transacción validada necesita actualizar el estado de la aplicación, vinculando un valor en un almacén de valores clave o actualizando la base de datos UTXO.

El mensaje *CheckTx* es similar a *AppendTx*, pero solo sirve para validar transacciones. El mempool de Tendermint BFT primero verifica la validez de una transacción con *CheckTx* y solo transmite transacciones válidas a sus pares. Las aplicaciones pueden verificar un nonce incremental en la transacción y devolver un error en *CheckTx* si el nonce es antiguo.

El mensaje de confirmación se utiliza para computar un commit criptográfico con el estado actual de la aplicación, que se colocará en el siguiente encabezado del bloque. Esto tiene algunas propiedades útiles. Las inconsistencias en la actualización de ese estado ahora aparecerán como bifurcaciones de blockchain que captan toda una clase de errores de programación. Esto también simplifica el desarrollo de clientes light seguros, ya que las pruebas Merkle-hash se pueden verificar comparándolas con el hash del bloque, y el hash del bloque está firmado por un quórum de validadores (por poder de voto).

Los mensajes ABCI adicionales permiten a la aplicación realizar un seguimiento y cambiar el conjunto de validadores, y que la aplicación reciba la información del bloque, como el número del bloque emitido (height) y los votos de confirmación.

Las solicitudes/respuestas ABCI son mensajes simples de Protobuf. Consulte el archivo de esquema.

AppendTx

- Arguments:
 - Data ([]byte): The request transaction bytes
- Returns:

- Code (uint32): Response code
 - Data ([]byte): Result bytes, if any
 - Log (string): Debug or error message
- Usage:
Append and run a transaction. If the transaction is valid, returns CodeType.OK

CheckTx

- Arguments:
 - Data ([]byte): The request transaction bytes
- Returns:
 - Code (uint32): Response code
 - Data ([]byte): Result bytes, if any
 - Log (string): Debug or error message
- Usage:
Validate a transaction. This message should not mutate the state. Transactions are first run through CheckTx before broadcast to peers in the mempool layer. You can make CheckTx semi-stateful and clear the state upon Commit or BeginBlock, to allow for dependent sequences of transactions in the same block.

Commit

- Returns:
 - Data ([]byte): The Merkle root hash
 - Log (string): Debug or error message
- Usage:
Return a Merkle root hash of the application state.

Query

- Arguments:
 - Data ([]byte): The query request bytes
- Returns:
 - Code (uint32): Response code

- Data ([]byte): The query response bytes
- Log (string): Debug or error message

Flush

- Usage:
Flush the response queue. Applications that implement types.Application need not implement this message – it's handled by the project.

Info

- Returns:
 - Data ([]byte): The info bytes
- Usage:
Return information about the application state. Application specific.

SetOption

- Arguments:
 - Key (string): Key to set
 - Value (string): Value to set for key
- Returns:
 - Log (string): Debug or error message
- Usage:
Set application options. E.g. Key="mode", Value="mempool" for a mempool connection, or Key="mode", Value="consensus" for a consensus connection. Other options are application specific.

InitChain

- Arguments:
 - Validators ([]Validator): Initial genesis-validators

- Usage:
Called once upon genesis

BeginBlock

- Arguments:
 - Height (uint64): The block height that is starting
- Usage:
Signals the beginning of a new block. Called prior to any AppendTx.

EndBlock

- Arguments:
 - Height (uint64): The block height that ended
- Returns:
 - Validators ([]Validator): Changed validators with new voting powers (0 to remove)
- Usage:
Signals the end of a block. Called prior to each Commit after all transactions

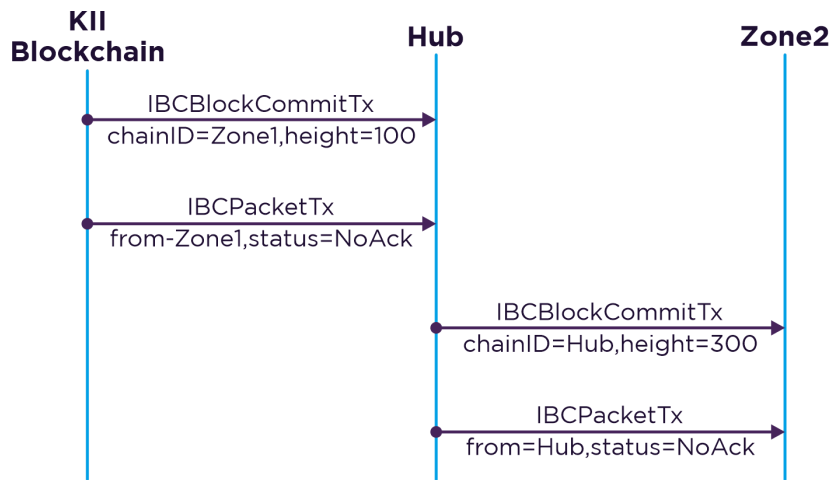
IBC: Inter-Blockchain Communication

Ahora veremos cómo se comunican el Hub y las zonas entre sí. Por ejemplo, si hay tres blockchains, "Zona1", "Zona2" y "Hub", y deseamos que "Zona1" produzca un paquete destinado a "Zona2" que pase por "Hub". Para mover un paquete de una blockchain a otra, se publica una prueba en la cadena receptora. La prueba afirma que la cadena de envío publicó un paquete para el supuesto destino. Para que la cadena receptora verifique esta prueba, debe poder mantenerse al día con los encabezados de bloque del remitente. Este mecanismo es similar al utilizado por sidechains, que requieren que dos cadenas que interactúan se conozcan entre sí a través de un flujo bidireccional de datagramas proof-of-existence (transacciones). Así es como Kii Blockchain se conecta al Cosmos Hub.

Naturalmente, el protocolo IBC se puede definir utilizando dos tipos de transacciones: una transacción IBCBlockCommitTx, que permite a una blockchain demostrarle a cualquier observador su hash de bloque más reciente, y una transacción IBCPacketTx,

que permite a una blockchain demostrarle a cualquier observador que, de hecho, el paquete dado fue publicado por la aplicación del remitente, a través de una prueba Merkle al hash de bloque reciente.

Al dividir la mecánica de IBC en dos transacciones separadas, permitimos que el mecanismo de mercado de tarifas nativo de la cadena receptora determine qué paquetes se confirman (es decir, se reconocen), al tiempo que se permite total libertad en la cadena de envío en cuanto a cuántos paquetes salientes se permiten.



En el ejemplo anterior, para actualizar el hash de bloque de "Zona1" en "Hub" (o de "Hub" en "Zona2"), se debe publicar una transacción `IBCBlockCommitTx` en "Hub" con el hash de bloque de "Zona1" (o en "Zona2" con el hash de bloque de "Hub").

Tipos de Transacciones: Cómo Interactúa Kii con Cosmos Hub

En la implementación estándar, las transacciones se transmiten a la aplicación Cosmos Hub a través de ABCI (Application Blockchain Interface).

Cosmos Hub aceptará una serie de tipos de transacciones principales de Kii Blockchain, incluidos `SendTx`, `BondTx`, `UnbondTx`, `ReportHackTx`, `SlashTx`, `ProposalCreateTx` y `ProposalVoteTx`, que se explican por sí mismos y se documentarán en una revisión futura de este documento. Aquí documentamos los dos tipos de transacciones principales para IBC: `IBCBlockCommitTx` e `IBCPacketTx`.

IBCBlockCommitTx

Una transacción `IBCBlockCommitTx` se compone de:

- ChainID (string): El ID de la blockchain
- BlockHash ([]byte): los bytes del hash del bloque, la raíz de Merkle que incluye el hash de la aplicación
- BlockPartsHeader (PartSetHeader): los bytes del encabezado del conjunto parcial del bloque, solo necesarios para verificar las firmas de voto
- BlockHeight (int): la altura de la confirmación
- BlockRound (int): la ronda de la confirmación
- Commit ([]Voto): $>\frac{2}{3}$ votos de Precommit de Tendermint que componen un commit en bloque.
- ValidatorsHash ([]byte): un hash raíz del árbol Merkle del nuevo conjunto de validadores
- ValidatorsHashProof (SimpleProof): una prueba de SimpleTree Merkle para probar el ValidatorsHash contra BlockHash
- AppHash ([]byte): un hash raíz del árbol IAVLTree Merkle del estado de la aplicación
- AppHashProof (SimpleProof): una prueba de SimpleTree Merkle para probar AppHash frente a BlockHash

IBCPacketTx

Un IBCPacket se compone de:

- Header (IBCPacketHeader): el encabezado del paquete
- Payload ([]byte): los bytes de la carga útil (payload) del paquete. *Opcional*
- PayloadHash ([]byte): el hash de los bytes del paquete. *Opcional*

Debe estar presente Payload o PayloadHash. El hash de un IBCPacket es una raíz Merkle simple de los dos elementos, Header y Payload. Un IBCPacket sin Payload completo se denomina *paquete abreviado* (abbreviated packet).

Un IBCPacketHeader se compone de:

- SrcChainID (string): el ID de la blockchain de origen.

- DstChainID (string): el ID de la blockchain de destino.
- Number (int): un número único para todos los paquetes.
- Status (enum): puede ser uno de AckPending, AckSent, AckReceived, NoAck o Timeout.
- Type (string): Los tipos dependen de la aplicación. Cosmos se reserva el tipo de paquete "coin"
- MaxHeight (int): si el estatus no es NoAckWanted o AckReceived por este bloque emitido, el status pasa a ser Timeout. *Opcional*

Una transacción *IBCPacketTx* se compone de:

- FromChainID (string): el ID de la blockchain que proporciona este paquete; no necesariamente la fuente
- FromBlockHeight (int): el número de bloque emitido de la blockchain en la que se incluye el siguiente paquete (merkleizado) en el hash de bloque de la cadena de origen
- Packet (IBCPacket): un paquete de datos, cuyo status puede ser AckPending, AckSent, AckReceived, NoAck o Timeout
- PacketProof (IAVLProof): Prueba IAVLTree Merkle para probar el hash del paquete contra el AppHash de la cadena de origen a un bloque emitido (height) determinado

La secuencia para enviar un paquete desde la "Zona1" a la "Zona2" a través del "Hub" se muestra en la {Figura X}. Primero, un IBCPacketTx le demuestra al "Hub" que el paquete está incluido en el estado de la aplicación de "Zona1". Luego, otro IBCPacketTx le demuestra a "Zona2" que el paquete está incluido en el estado de aplicación de "Hub". Durante este procedimiento, los campos de IBCPacket son idénticos: SrcChainID siempre es "Zona1" y DstChainID siempre es "Zona2".

PacketProof debe tener la ruta correcta a prueba de Merkle, de la siguiente manera:

IBC/<SrcChainID>/<DstChainID>/<Number>

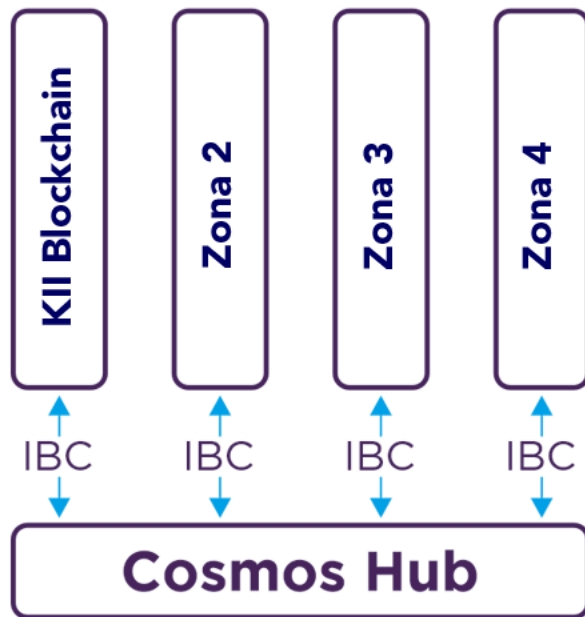
Cuando "Zona1" quiere enviar un paquete a "Zona2" a través de "Hub", los datos de IBCPacket son idénticos ya sea que el paquete esté Merkleizado en "Zona1", el "Hub" o "Zona2". El único campo mutable es status para el seguimiento de la entrega.

El Hub y Zonas: Cómo Kii Blockchain se Conecta al Cosmos Hub

El Hub y las Zonas, alimentadas por IBC, es un modelo innovador para el crecimiento y la escalabilidad en el mundo del libro de contabilidad público descentralizado de blockchain. Como hemos comentado antes, Cosmos es una red de múltiples blockchains impulsadas por Tendermint, y Kii Blockchain es una de esas blockchains. Si bien las propuestas existentes apuntan a crear una "blockchain independiente" con procesamiento de transacciones dependiente de su propia red, o layers 2 que se construyen debajo de ellas, Cosmos permite que muchas blockchain layer 1 se ejecuten simultáneamente entre sí manteniendo la interoperabilidad.

En esencia, Cosmos Hub gestiona muchas blockchains independientes llamadas "Zonas" (a veces denominadas "shards", en referencia a la técnica de escalado de bases de datos conocida como "sharding"). En Cosmos Hub se publica un flujo constante de información de bloques recientes (Commits) de Zonas, lo que permite que Cosmos Hub se mantenga al día con el status de cada Zona. Del mismo modo, cada Zona se mantiene al día con el status del Hub (sin embargo, las Zonas no se mantienen al día entre sí excepto indirectamente a través del Hub). Luego, los "paquetes" de información se comunican de una zona a otra mediante la publicación de pruebas Merkle como evidencia de que la información fue enviada y recibida. Este mecanismo se llama inter-blockchain communication (comunicación entre blockchains), o IBC para abreviar.

Cualquiera de las zonas puede ser en sí misma hubs para formar un gráfico acíclico, pero en aras de la claridad solo describiremos la configuración simple en la que solo hay un hub y muchas zonas que no son hubs.



El Hub

Cosmos Hub es una blockchain que alberga un libro de contabilidad público distribuido de múltiples activos, donde los usuarios individuales o las zonas pueden tener tokens. Estos tokens se pueden mover de una zona a otra en un paquete IBC especial llamado “paquete de monedas” (“coin packet”); así es como se comunica la información entre la zona y el hub. El hub es responsable de preservar la invariancia global de la cantidad total de cada token en las zonas. Las transacciones de paquetes de monedas IBC deben ser confirmadas por las blockchains del remitente, el hub y el receptor.

Dado que Cosmos Hub actúa como el libro de contabilidad público central de todo el sistema, la seguridad del Hub es de suma importancia. Si bien cada zona puede ser una blockchain Tendermint que está protegida por tan solo 4 validadores (o incluso menos si no se necesita el consenso de BFT), el Hub debe estar protegido por un conjunto globalmente descentralizado de validadores que puedan resistir los escenarios de ataque más severos, como una partición de la red continental o un ataque patrocinado por un estado-nación.

Las Zonas

Una zona Cosmos es una blockchain independiente que intercambia mensajes IBC con el Hub y en este caso particular, la zona es Kii Blockchain. Desde la perspectiva del Hub, Kii Blockchain es una cuenta multifirma de membresía dinámica de múltiples activos que puede enviar y recibir tokens utilizando paquetes IBC. Al igual que una cuenta de

criptomonedas, Kii Blockchain no puede transferir más tokens de los que tiene, pero puede recibir tokens de otras personas que los tengan.

Los validadores pueden realizar stake en Kii Blockchain mientras está conectado al Hub. Si bien los ataques de doble gasto en estas zonas resultarían en la reducción (slashing) de KII con la responsabilidad bifurcada de Tendermint, una zona donde más de dos tercios del poder de voto son bizantinos puede commit un estado no válido. Cosmos Hub no verifica ni ejecuta transacciones comprometidas en Kii Blockchain, por lo que es responsabilidad de los usuarios enviar tokens a zonas en las que confían.

Habilitando Contratos Inteligentes

El módulo Cosmos EVM permite que contratos inteligentes compatibles con Ethereum se ejecuten en una blockchain Cosmos, emulando el entorno EVM. Este módulo garantiza la compatibilidad con las herramientas y dApps de Ethereum existentes, lo que permite a los desarrolladores implementar contratos inteligentes de Ethereum en las blockchains Cosmos sin modificaciones significativas.

El módulo procesa y ejecuta contratos inteligentes escritos en Solidity de manera similar a como se ejecutarían en la blockchain de Ethereum. Las transacciones destinadas al módulo EVM se identifican y procesan. Estos pueden incluir implementación de contratos, interacción de contratos u otras operaciones específicas de EVM. Un beneficio del módulo Cosmos EVM es que está integrado dentro del SDK de Cosmos, por lo tanto, el módulo puede coexistir con otros módulos, brindando flexibilidad y funcionalidad a la blockchain.

Al respaldar los contratos inteligentes de Ethereum, Kii Blockchain puede aprovechar el vasto ecosistema de desarrolladores de Ethereum y dApps existentes, fomentando una mayor colaboración e innovación. El módulo EVM opera dentro de su propio entorno de ejecución, lo que garantiza que los problemas dentro del EVM no afecten a otras partes de la blockchain y abre la puerta para que estos contratos interactúen con otras blockchains habilitadas para IBC dentro de la red Cosmos. Este nivel de interoperabilidad es un avance significativo en el espacio blockchain. El módulo gestiona el estado de Ethereum por separado del estado de Cosmos. Esta segregación garantiza que las transiciones de estado y los modelos de cuenta de EVM no entren en conflicto con el estado de la cadena Cosmos.

Al integrar el módulo EVM, los desarrolladores pueden configurarlo para adaptarlo a sus necesidades específicas. Esto incluye establecer los precios del gas, habilitar funcionalidades EVM específicas o definir cómo se manejan las transacciones de Ethereum y los contratos inteligentes dentro de Kii Blockchain. El módulo expone API y Endpoint RPC que son compatibles con Ethereum, lo que permite que las herramientas y aplicaciones creadas para Ethereum (como billeteras y dApps) interactúen con la

cadena Kii Blockchain sin modificaciones significativas. Los desarrolladores pueden utilizar herramientas de desarrollo estándar como aplicaciones Node.js y entornos como Truffle o Hardhat son populares para el desarrollo de Solidity.

Kii Coin

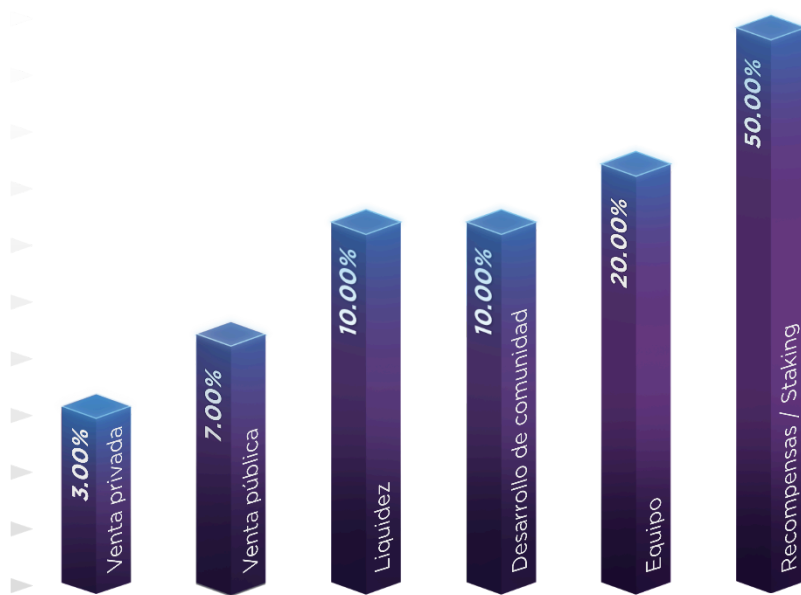
Si bien Kii Blockchain opera dentro de Cosmos Hub, ejecuta su activo nativo, KII, como una criptomoneda no inflacionaria. La economía del token es vital para determinar cómo interactuará el ecosistema con la blockchain y detallará el uso del token nativo, KII. En este caso, el valor del token está diseñado para derivar de su utilidad y uso, en lugar de una inversión especulativa. El objetivo es crear un modelo sostenible que cree una comunidad profunda, compense a los validadores y delegadores por su trabajo a largo plazo y diseñe una estructura que extraiga la máxima utilidad para KII. El objetivo de esta sección es explicar ese valor dentro del ecosistema, la distribución del tokenomics, las expectativas de liberación y circulación, y su utilidad general.

Tokenomics

El límite máximo de Kii Blockchain se establece en 1.800.000.000 KII. En el bloque génesis, los 1.800.000.000 tokens se liberan en cuentas específicas, cada una con su propósito en el ecosistema. KII tiene un suministro fijo, lo que significa que no pueden ser *minted* ni creadas monedas adicionales.

La distribución inicial de tokens y validadores Kii en Genesis se distribuirá en las siguientes categorías:





Categoría	% Suministro total	Cantidad de tokens	Comentarios
Preventa	3%	56.000.000	La preventa se vendió en tres rondas diferentes en la ronda semilla inicial en 2021-2022
Venta Pública	7%	126.000.000	Planificada para la venta pública / IEO / listado
Liquidez	10%	180.000.000	Separado en liquidez, envoltura (wrapping) y creación de mercado (market making) de DeFi
Desarrollo de comunidad	10%	180.000.000	Grupo de subvenciones, airdrops, competiciones y hackathons
Equipo	20%	360.000.000	Para el equipo, desarrolladores e inversores
Recompensas / Staking	50%	900.000.000	Para validadores y delegados que prestan servicios a la blockchain

Vesting y Distribución de Tokens

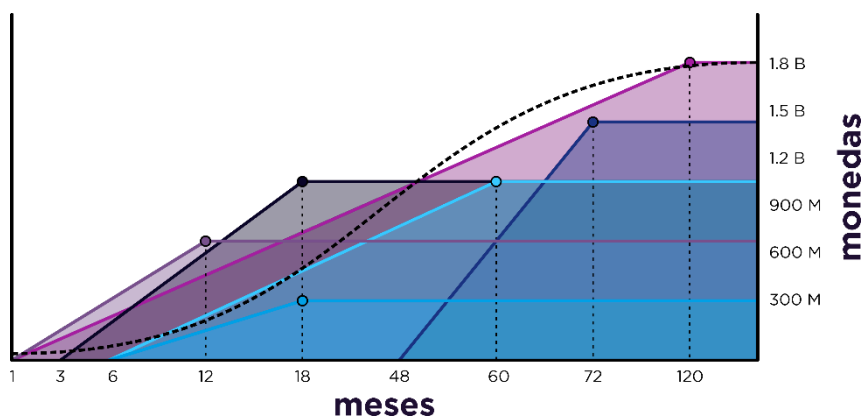
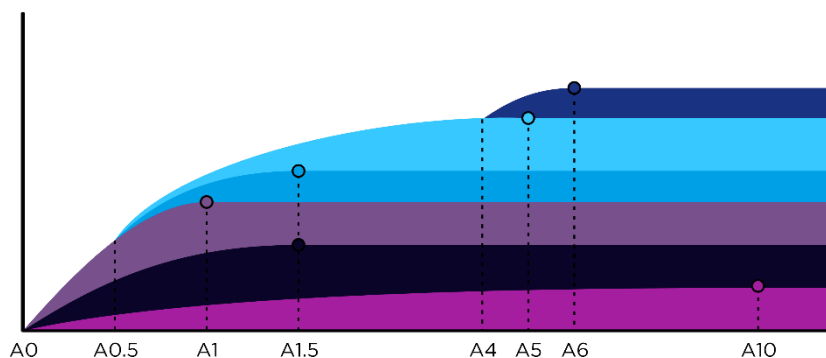
La distribución y adquisición (vesting) de tokens se desarrolló colectivamente entre los fundadores y desarrolladores y es el resultado de muchos años de experiencia colectiva como usuarios, inversores, participantes (stakers) y desarrolladores en otros

Hubo un énfasis particular en el largo acantilado y en la concesión de derechos a los miembros del equipo detrás del proyecto, para mostrar compromiso con la longevidad del ecosistema y su comunidad. Además, las diferencias notables son la baja cantidad vendida en preventa (3%), un factor diferenciador entre otros proyectos que venden más del 30% a los primeros inversores de riesgo que luego deshacen esas posiciones agresivamente en el mercado al momento del lanzamiento y los usuarios asumen la presión del lado de la venta. Además, todos los cronogramas de concesión/liberación se emiten diariamente. La ventaja de la emisión diaria es que los usuarios venderán o transferirán en días diferentes en lugar de concentrar todos los movimientos en un día o una semana. Al dotar a la empresa de inversión interna, la economía se diseñó teniendo como máxima prioridad los intereses de los usuarios de la comunidad.

		Calendario de Lanzamiento																															
Categoría	Número de monedas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	Año 3	Año 4	Año 5					
Preventa (3%)	56.000.000	N/A																															
Preventa 1 (2021)	6.000.000	Cliff				LD																											
Preventa 2 (iniciando 2022)	18.000.000	Cliff											LD																				
Preventa 3 (terminando 2022)	32.000.000	Cliff												Liberación Diaria																			
Venta Pública (7%)	126.000.000	Vesting diario o liberación inmediata para negociar, depende del launchpad																															
Liquidez (10%)	180.000.000	N/A																															
Defi	100.000.000	Cliff			Liberación para envolver "wrapping" a ETH, publicando liquidez para DEX																												
Exchanges	80.000.000	Liberación linear hasta el mes 18 según listados del exchange																															
Desarrollo Comunitario (10%)	180.000.000	N/A																															
Airdrops & Competiciones	20.000.000	Cliff						Vesting Diario																									
Concesiones	160.000.000	Cliff						Otorgado proyecto por proyecto. No se puede liberar más del 5% del fondo común en un mes determinado.																									
Equipo (20%)	360.000.000	N/A																															
Equipo Kiglobal	301.000.000																																
Desarrolladores	18.000.000											Cliff															Liberación Diaria						
Inversores en ronda SAFE	36.000.000							Cliff							Liberación Diaria								Liberación Diaria										
Asesores	5.000.000											Cliff																		Liberación Diaria			
Staking y recompensas (50%)	900.000.000	Distribución diaria de recomensas hasta el año 8																															

La circulación de tokens es una guía anticipada de cómo se liberarán y distribuirán los tokens. En cualquier caso, es muy poco probable que todos los tokens estén disponibles para negociarse en el mercado durante estos momentos exactos y deberían usarse más como referencia para la liberación de tokens que para la disponibilidad en el mercado.

● Equipo	4 - 6 años
● Desarrollo de comunidad	0.5 - 5 años
● Preventa	0.5 - 1.5 años
● Venta Pública	0 - 1 años
● Liquidez	1 - 1.5 años
● Recompensas /Staking	0 - 10 años



Utilidad de KII Coin

Si bien Kii Blockchain es su propia blockchain independiente conectada al Cosmo's Hub, la blockchain ejecutará su token nativo, KII. KII es el único token para staking de Kii Blockchain. KII es una licencia para que el titular vote, valide o delegue en otros validadores. Al igual que el Ether de Ethereum, KII también se puede utilizar para pagar tarifas de transacción para mitigar el spam. KII es un token de utilidad con los siguientes casos de uso:

- Estado y Actividad de la Red: KII actúa como una herramienta comunitaria y es el único activo utilizado entre Validadores, Delegados, Operadores y

Colaboradores. No se puede utilizar ningún otro activo digital para dar servicio a la red.

- Pagos: KII se puede utilizar para pagos, remesas y cualquier tipo de liquidación de valores. Su utilidad se deriva de poder transferir valor de billetera a billetera.
- Precios de tokenización: los usuarios que implementan contratos inteligentes en la blockchain pueden fijar el precio de sus productos o activos en KII y utilizar el token como medio de valoración.
- Recompensas de comisiones: KII actuará como token digital para recompensas a los usuarios que validen y deleguen en la blockchain. Además, dentro de varios modelos para sus protocolos DeFi, KII actuará como token de comisión para el comercio y la cobertura de contratos al contado y a plazo.
- Gobernanza: KII permite una gobernanza descentralizada, donde los poseedores de tokens pueden votar sobre propuestas y cambios en la red.
- Seguridad: mediante el uso descentralizado de validación y staking, los usuarios pueden proteger contra ataques maliciosos a la red.
- Autonomía como comunidad: el ecosistema Kii Global es independiente y completamente funcional. No depende de otros grandes partidos para su funcionamiento. Por lo tanto, KII empodera a los usuarios en el corazón de las finanzas descentralizadas.
- Diseño no inflacionario: KII es un activo digital no inflacionario utilizado en sus modelos, por lo que los usuarios no sufrirán problemas comunes relacionados con la inflación.

Fondo de Recompensas Evergreen

A diferencia de la mayoría de los ecosistemas blockchain, el 5% del flujo de efectivo de Kii Global se redirigirá a la compra de monedas a través del creador de mercado líder y a reponer el fondo de recompensas de Kii para validación y staking. Kii Global está comprometido con un entorno no inflacionario donde los usuarios puedan participar en una blockchain no inflacionaria respaldada por todo el ecosistema de Kii Global.

Tres meses después del lanzamiento público, Kii Global informará públicamente el flujo de efectivo de las operaciones de la empresa y realizará pagos a nuestro creador de mercado líder con instrucciones para comprar KII en el mercado abierto y enviar el KII a la dirección pública para obtener recompensas. El KII no se comprará todo en un día,

sino durante un período más largo para evitar fuertes fluctuaciones de precios. Esta operación se realizará trimestralmente.

Limitaciones y Requisitos del Validador

A diferencia de Bitcoin, Dash u otras blockchains proof-of-work, el mecanismo de consenso de Tendermint se vuelve más lento con más validadores debido al incremento de complejidad en la comunicación. Afortunadamente, la velocidad de la Kii Blockchain sigue siendo 300 veces más rápida que la de sus contrapartes proof-of-work. Kii Blockchain aún puede admitir fácilmente suficientes validadores para mantener la red completamente descentralizada.

El día génesis, el número máximo de validadores en el conjunto abierto se establecerá en 100. Al principio, cada validador deberá publicar un mínimo de 10.000 KII para realizar la transición de un nodo a un validador y se clasificará según la cantidad total de KII a la que se le haya hecho stake. Cuanto mayor sea el rango, mayores serán las recompensas. El número total de validadores en el conjunto abierto se ajustará según la evaluación de Kii Global de la red y los participantes en el conjunto no activo. El número de validadores en el conjunto abierto se puede ampliar a 300 validadores sin perder métricas de rendimiento; sin embargo, con 100 validadores la red aún debería tener una proporción saludable de descentralización y rendimiento de la red. El número aumentará para proporcionar una mayor descentralización para cuando la blockchain hace la transición a una gobernanza abierta.

Convertirse en Validador después del día Génesis

Los titulares de KII que aún no se han convertido en validadores pueden hacerlo firmando y enviando una transacción BondTx. La cantidad de KII proporcionada como garantía debe ser de 10.000 KII como mínimo. Cualquiera puede convertirse en validador en cualquier momento, excepto cuando el tamaño del conjunto de validadores actual sea mayor que el número máximo de validadores permitidos. En ese caso, la transacción solo es válida si la cantidad de KII es mayor que la cantidad de KII efectivo en poder del validador más pequeño, donde los KII efectivos incluyen los KIIs delegados. Cuando un nuevo validador reemplaza a un validador existente de tal manera, el validador existente se vuelve inactivo y todos los KII y los KII delegados entran en el estado de desvinculación.

Validadores Corporativos de Kii

Kii Global ejecutará un validador particular llamado El Validador MasterNodo. Para realizar stake de KII en el Validador MasterNodo, los delegados deberán comprometer 150.000 KII, pero serán compensados con recompensas mínimas mediante staking, ajustadas mediante airdrops.

Sanciones para los Validadores

Para garantizar el cumplimiento del protocolo, los validadores enfrentan sanciones por cualquier desviación, ya sea deliberada o accidental. Las infracciones incluyen firmas duales al mismo bloque emitido (height) y ronda, o romper la regla de "prevote-the-lock" del protocolo de consenso de Tendermint. Tales violaciones conducen a la pérdida del status del validador y a la incautación de sus KII vinculados, junto con su parte de los tokens del fondo de reserva, conocidos colectivamente como su "stake".

Hay casos en los que los validadores pueden dejar de estar disponibles debido a problemas como interrupciones de la red o cortes de energía. Si un validador no realiza un voto en la blockchain más de un número máximo especificado de veces dentro de un cierto número de bloques anteriores, se le considerará inactivo y perderá una penalización predeterminada del 1% de su participación.

Es posible que algunas actividades dañinas no dejen rastros claros en la blockchain. En estos casos, los validadores pueden colaborar externamente para imponer tiempos de espera (timeouts) a estos validadores dañinos, siempre que exista un consenso abrumador.

En escenarios en los que más de un tercio del poder de voto de Kii Blockchain está fuera de línea, lo que provoca una interrupción, o si una coalición similar impide que se registren pruebas de actos maliciosos en la blockchain, se inicia una recuperación a través de una propuesta de reorganización hard-fork.

Tarifas de Transacción

Los validadores de Kii Blockchain obtienen tokens KII como recompensas por procesar transacciones. Tienen la libertad de establecer sus propios tipos de cambio y seleccionar las transacciones que procesan, siempre y cuando no excedan el BlockGasLimit. Las tarifas recaudadas se comparten con los poseedores de stake que han vinculado su Kii, y se distribuyen proporcionalmente en cada ValidatorPayoutPeriod (el predeterminado es 1 hora).

Los poseedores de tokens Kii que confían su poder de voto a otros validadores deben pagar una comisión a estos validadores. La tasa de esta comisión la determina cada validador individualmente.

Hackers Incentivados

La seguridad de Kii Blockchain depende de la solidez de sus validadores y de las opciones de delegación de los delegados. Para promover la detección temprana y la notificación de fallas de seguridad, Kii Blockchain motiva a hackers informáticos a

revelar violaciones exitosas a través de una transacción ReportHackTx. Esta transacción esencialmente comunica: "Este validador ha sido comprometido. Asigne una recompensa a esta dirección". Tras tal incumplimiento, el validador afectado y sus delegados quedan inactivos. Se deduce un valor predeterminado del 5% del KII de todos (HackPunishmentRatio) y se otorga un porcentaje igual (HackRewardRatio) al hacker en la dirección especificada. Luego, el validador debe restaurar el KII restante utilizando una clave de respaldo.

Para garantizar que esta característica no se aproveche para transferir ilegítimamente KII no *vested*, la proporción de KII *vested* y no *vested* para validadores y delegados antes y después de la transacción ReportHackTx permanecerá sin cambios. La recompensa del hacker también incluirá una parte de KII no *vested*, si está disponible.

Esta función se utilizará especialmente durante las competiciones de Testnet y relacionadas con Testnet.

Especificaciones de Gobernanza

En los primeros 12 a 14 meses, Kii Blockchain tendrá una gobernanza cerrada para proteger la integridad de la red en su infancia. El equipo de desarrollo interno revisará los cambios propuestos en la red y la adición de contratos inteligentes para auditar el código y proteger la red de ataques maliciosos.

Cuando la red haya llenado sus 100 validadores en el conjunto abierto, y el validador promedio tenga al menos 12 meses de experiencia protegiendo el servidor y ofreciendo los servicios de staking a sus delegados, el equipo de Kii Global comenzará la transición a la gobernanza abierta.

La gobernanza abierta en Kii Blockchain será administrada por una organización descentralizada que se basa en un proceso de gobernanza formal para coordinar las actualizaciones de la blockchain. Esto incluye ajustar los parámetros del sistema, implementar actualizaciones de software y realizar cambios en la constitución.

Todos los validadores deben votar sobre cada propuesta. Si un validador no vota dentro del tiempo establecido, se desactiva automáticamente por el período de penalización por ausentismo o *AbsenteeismPenaltyPeriod* (el predeterminado es una semana).

Los votos de los delegados se alinean automáticamente con el voto del validador elegido, pero pueden cambiar este voto manualmente. Kii, que no está vinculado, no tiene derecho a voto.

Las propuestas requieren un Depósito Mínimo por Propuesta o *MinimumProposalDeposit* en tokens, que pueden ser KII u otros tipos de tokens. Los votantes pueden decidir

apoderarse de este depósito. Si más de la mitad de los votantes optan por aceptar el depósito (por ejemplo, en el caso de una propuesta de spam), se agrega al grupo de reserva, excepto los KII, que se destruyen.

Las opciones de votación para cada propuesta incluyen:

- Yea
- YeaWithForce
- Nay
- NayWithForce
- Abstain

Una propuesta se aprueba (o fracasa) si obtiene más de la mitad de los votos Yea or YeaWithForce (or Nay or NayWithForce). Sin embargo, una decisión puede ser vetada por más de un tercio de los votantes que opten por una opción "with force". Si se veta una decisión mayoritaria, todos pierden VetoPenaltyFeeBlocks (equivalente a un día de bloques) en tarifas (sin incluir impuestos), y el grupo que vetó la decisión también pierde VetoPenaltyKii (por defecto, 0,1%) de su KII.

Propuesta de cambio de parámetro

Cualquiera de los parámetros definidos aquí se puede cambiar pasando una ParameterChangeProposal.

Propuesta de Recompensa

KII se puede inflar y gastar los fondos del fondo de reserva con la aprobación de una BountyProposal.

Propuesta de Prueba

Todas las demás propuestas, como una propuesta para actualizar el protocolo, se coordinarán a través de la TextProposal genérica.

Resumen

En recapitulación, la arquitectura técnica de Tendermint ofrece un conjunto completo de ventajas que lo convierten en el algoritmo de consenso elegido para aplicaciones de alto riesgo, incluidas las implementadas por Kii Blockchain. Es el epítome de la velocidad, seguridad y sostenibilidad, y establece efectivamente un nuevo estándar de la industria para los mecanismos de consenso de blockchain. Combinado con el ecosistema de productos de Kii Global y la infraestructura empresarial del mundo real, todo el equipo de Kii está dedicado a construir un futuro mejor para nuestros

homólogos cercanos en América Latina y todos los demás en los mercados emergentes.

Citas

Un agradecimiento especial a nuestros amigos en Cosmos:

<https://v1.cosmos.network/resources/whitepaper>

Tendermint: <https://github.com/tendermint/tendermint/wiki>

ABCI: <https://github.com/tendermint/abci>

—

Bitcoin: <https://bitcoin.org/bitcoin.pdf>

ZeroCash: <http://zerocash-project.org/paper>

Ethereum: <https://github.com/ethereum/wiki/wiki/White-Paper>

TheDAO: <https://download.slock.it/public/DAO/WhitePaper.pdf>

Lightning Network: <https://lightning.network/lightning-network-paper-DRAFT-0.5.pdf>

BitShares: <https://bitshares.org/technology/delegated-proof-of-stake-consensus/>

Ethereum Sharding: <https://github.com/ethereum/EIPs/issues/53>

Ethereum 2.0 Mauve Paper: http://vitalik.ca/files/mauve_paper.html