



electric cash

Libro blanco v1.0

electriccash.global

2021

Índice de contenidos

1. Introducción	4
1.1. Planteamiento del problema y enfoque de la solución	4
2. Estructura de Electric Cash	5
2.1. Capa de transacciones rápidas	5
2.2. Transacciones gratuitas	6
2.3. Reducción de bloque y estrategia de recompensa	8
2.4. Tesorería para el Desarrollo	9
3. Ecosistema de Electric Cash	10
3.1. Staking	11
3.1.1. Proceso de Staking	11
3.1.2. Monedero del Staking y de Gastos	11
3.1.3. Fondo de Recompensas por Staking	11
3.2. Sistema de gobernanza	12
3.2.1. La importancia de la gobernanza	12
3.2.2. Poder de Gobernanza (GP)	13
3.3. Minería combinada	15
Hoja de ruta de Electric Cash	16
Resumen	16
Definiciones	17
Fuentes	17
Referencias	18

Aviso legal

Este documento no contiene las especificaciones técnicas finales.

El proyecto presentado se encuentra en su fase conceptual inicial y puede ser modificado, cambiado o incluso abandonado (debido a circunstancias tecnológicas, económicas o de reglamento, por ejemplo) y ninguna parte de este documento se puede considerar una descripción final del proyecto o de cualquiera de sus partes o componentes en aquello que se refiere a su ejecución.

Este documento no aporta asesoramiento financiero.

La información contenida en este documento (Libro blanco) no debe ser considerada como un consejo de inversión. El mercado de las criptomonedas es muy volátil. Debe considerar cuidadosamente si la criptomoneda es adecuada para usted teniendo en cuenta sus circunstancias y recursos financieros. Al seguir el resto del documento (Libro blanco), usted reconoce que no ha buscado asesoramiento en materia de inversiones por parte del autor, ni de ninguna de las partes formalmente relacionadas con el autor, ya que dicho autor y las partes no pueden proporcionar tal asesoramiento. No se espera de usted, ni se le ofrece, que invierta, compre o lleve a cabo cualquier actividad financiera, de cualquier forma o manera, sobre la base de cualquier información contenida en este Libro blanco y usted reconoce que cualquier acción de este tipo es únicamente de su responsabilidad personal.

Libro blanco Electric Cash

Eyal Avramovich
Libro blanco v1.0

Extracto. En 2009, la primera criptomoneda, Bitcoin (1) entró en el mercado. A día de hoy, tras 11 años y pese a romper precios récord, tanto Bitcoin como otras criptomonedas no han sido adoptadas por el público general. La mayor parte de las criptomonedas, pese a ser seguras, no están diseñadas para funcionar como efectivo. Las transacciones no son eficientes, tienden a ser costosas y la experiencia del usuario tiende a ser un asunto secundario en muchos proyectos. A pesar de esto, hay nuevos avances tecnológicos que nos permiten diseñar una mejor criptomoneda que sea tan segura como la mayoría de las blockchains y a la vez rápida y barata en términos de su uso (o incluso sin coste). En este documento, presentamos un nuevo protocolo de pago descentralizado: Electric Cash (ELCASH), una moneda basada en SHA-256 diseñada para el uso cotidiano. Sus transacciones rápidas y baratas (o incluso sin coste) la convierten en una moneda de cambio perfecta y una genial herramienta a usar en pagos diarios. Además, el sistema de control del protocolo Electric Cash proporciona a quienes posean la moneda el poder de decidir acerca del futuro desarrollo de su ecosistema. Creemos que este proyecto llena una brecha en el mercado, ya que promete ser para público general.

1. Introducción

1.1. Planteamiento del problema y enfoque de la solución

Tarifas de la blockchain

La primera criptomoneda, Bitcoin, introdujo un mecanismo de transacción simple pero confiable, diseñado para proteger a la red de transacciones descontroladas. Las tasas en transacciones pueden variar y dependen de varios factores, tales como el uso de la red, el tiempo de confirmación de una transacción y la cantidad de dinero a transferir. Cuando hay poco tráfico, las transacciones se procesan con rapidez con tasas mínimas. Estas tasas son lo suficientemente bajas como para permitir que haya muy poco coste para un individuo que solicite una transacción. Conforme aumenta la carga y se acerca a los límites predeterminados, la demanda para confirmar transacciones aumenta hasta el punto en que un minero puede aumentar las tasas que cobra (2). Muchos proyectos copiaron este sistema sin solucionar el problema del aumento de tasas con el crecimiento de la red.

A día de hoy, conforme las criptomonedas ganan popularidad, se ven obligadas a cargar con el lastre que son unas tasas de transacción elevadas. En algunos casos, el precio resultante es de varios dólares por transacción. Un coste como éste convierte a estas criptomonedas en algo poco rentable para su uso diario, lo que impulsa tanto a usuarios nuevos como existentes a no utilizarla. En el caso de las criptomonedas con Prueba de Trabajo, las tasas se utilizan para proteger a la red de tráfico excesivo malicioso y para priorizar transacciones añadidas a la blockchain. Lo mismo se aplica al protocolo ELCASH. Sin embargo, ELCASH recompensa a los usuarios que participen en la red de forma activa, permitiendo transacciones baratas e incluso gratuitas. Los usuarios que apuesten por ELCASH recibirán un reembolso de su tasa de transacción a sus monederos como una de las recompensas por participar en la red.

Rendimiento de la blockchain

Pese a su popularidad creciente en el mundo de las finanzas, las blockchains sufren de una falta de escalabilidad (3) que afecta negativamente a su utilidad como una tecnología confiable. Las mayores blockchains con Prueba de Trabajo tienen una capacidad limitada de procesamiento de transacciones. Conforme crecen la popularidad y el uso de la red y se realizan más transacciones a través de la blockchain, la red pierde capacidad para procesar estas transacciones de manera rápida. Es por esto que muchas de las monedas basadas en Prueba de Trabajo que se consideran más seguras no se suelen utilizar a diario y actúan más como un sustituto del oro. Otras criptomonedas como Ethereum (4), se dieron cuenta de este problema y cambiaron de Prueba de Trabajo a Prueba de Participación.

Se han propuesto muchas soluciones. En este proyecto, implementamos la más prometedora: los llamados sistemas “fast layer” para mejorar la capacidad de la blockchain. Combinamos lo mejor de ambas partes: los bloques se minan con Prueba de Trabajo, que mantiene la seguridad en la red, pero las transacciones se pueden procesar en la segunda capa (L2) de la blockchain, lo que las hace casi instantáneas (5).

Influencia de la comunidad

Para apoyar el crecimiento del proyecto, se deberán añadir nuevas funcionalidades y modificar las funcionalidades existentes. Normalmente, los proyectos que tratan con las criptomonedas suelen estar regidas por un equipo dedicado a la blockchain o por los programadores, con lo cual se ven controlados de forma centralizada. Las decisiones acerca de cualquier otro desarrollo o cambio en la red son realizados y controlados por un número de individuos relativamente pequeño. La mayor parte de los usuarios no pueden opinar ni tienen suficiente influencia en las decisiones debido a una falta de conocimientos técnicos o capacidad financiera.

Electric Cash cambiará esto estableciendo un Fondo de Tesorería para el Desarrollo. Los recursos se tomarán de las recompensas por la minería con Prueba de Trabajo, almacenándose en dicha “Tesorería”. Además, los miembros de la comunidad Electric Cash recibirán poder de gobernanza. Esto permite un funcionamiento plenamente descentralizado de la red, donde las decisiones sobre el futuro y el uso de los fondos de la Tesorería de Fondo de Desarrollo son tomadas por la comunidad del proyecto. La democracia en la red se logra gracias al sistema de votos integrado en la blockchain (6).

2. Estructura de Electric Cash

Electric Cash es un protocolo de pagos diseñado para ser accesible y ligero, con el objetivo de reducir las tasas de transacción y permitir su uso diario sin complicaciones. Lo que convierte a ELCASH en algo ideal para los pagos del día a día son sus transacciones rápidas y baratas (e incluso gratuitas) en una red segura y descentralizada.

2.1. Capa de transacciones rápidas

Para implementar transacciones rápidas, la blockchain requiere una capacidad suficiente para incluir todas las transacciones en espera de ser confirmadas y para informar a la red sobre las transacciones tan pronto como sea posible. En las blockchains con Prueba de Trabajo tradicionales, las transacciones instantáneas son difíciles de lograr debido a ciertos aspectos sobre seguridad.

En este proyecto, se crea una capa de transacciones rápidas (Capa 2) en la red para mejorar la velocidad de las transacciones.

Capa 2

Permite transacciones rápidas.

Capa 1

Capa de consenso garantiza la integridad de la blockchain ejecutando el algoritmo de consenso entre los participantes.

Capa 0

La capa de cadena de bloques tiene una importancia crucial en cuanto a la escalabilidad, seguridad y privacidad de la red

Capa de hardware

Permite la ejecución eficiente del protocolo en otras capas.



Figura 1. Estructura del ecosistema de la blockchain de Electric Cash (7).

Esta solución de capa rápida permite agilizar las transacciones y mantiene un alto nivel de seguridad en la red. Las transacciones se propagan a la blockchain principal usando la Capa 2 en la que las transacciones se confirman fuera de la cadena antes de ser aprobadas por los mineros mediante Prueba de Trabajo.

2.2. Transacciones gratuitas

Las transacciones sin coste se logran gracias a la estructura de la blockchain. Durante el proceso de participación, los participantes generan el “límite de transacciones gratuitas” para gastar. La tasa se aplica a todas las transacciones, lo que hará que los ataques maliciosos a la red sean más difíciles de ejecutar. El coste de transacción, no obstante, será devuelto a los usuarios dependiendo de su límite. Para nosotros, esto es un factor importante que contribuirá a la adopción de las criptomonedas por parte del público general. En este aspecto, competimos no sólo con otros proyectos de blockchain, sino que también con las instituciones financieras tradicionales. Las criptomonedas, sin importar su seguridad, tienen un coste de utilización, especialmente cuando el proyecto gana popularidad y el uso de la red aumenta. Esto crea una situación en que cuánto más popular sea un proyecto, más caro resulta utilizarlo. Cada vez, menos nuevos usuarios quieren participar, lo que ralentiza el crecimiento del proyecto. Para conseguir una aceptación global, los proyectos necesitan alcanzar una masa crítica, es decir, que haya un cierto número de usuarios que hagan que la blockchain sea un proyecto atractivo para nuevos usuarios. Los proyectos como criptomonedas o plataformas de redes sociales se vuelven más útiles con cada nuevo usuario porque asimismo dan la posibilidad de conectar con más personas. De hecho, cuando un proyecto se limita a sí mismo aumentando las tasas de transacción mientras más usuarios haya en la red, su adopción global se hace más difícil o incluso imposible de lograr (8).

Límite de transacciones gratuitas de ELCASH

En el proyecto ELCASH, las tasas de blockchain se pagan por adelantado y se devuelven a los usuarios si les corresponden transacciones gratuitas. Cualquier usuario que participe en ELCASH es elegible. El límite de transacciones gratuitas se calcula a diario y depende de los parámetros de participación del usuario. Después de realizar una transacción, la tasa se devuelve al monedero del usuario.

Este diseño ayuda a mantener la red a salvo del uso excesivo malicioso, convirtiendo los ataques en algo caro, mientras que los usuarios pueden realizar transacciones gratuitas.

Los mineros no se ven cargados de trabajo adicional sin una recompensa. Si se realiza una transacción gratuita, la dificultad de la minería se reduce automáticamente de forma proporcional al valor de las transacciones gratuitas incluidas en el bloque. Como resultado, las recompensas totales y finales por bloque para los mineros no se verán afectadas en ningún sentido por las transacciones gratuitas y el trabajo adicional de los mineros será recompensado como corresponde.

2.3. Reducción de bloque y estrategia de recompensa

La minería de Electric Cash se pone en marcha a partir de un nuevo bloque de génesis. La estrategia presentada en el cuadro 1 tiene por objeto satisfacer la demanda prevista del mercado para la moneda, evitando al mismo tiempo un exceso de oferta durante los primeros años.

Está previsto que la preminería continúe hasta minar un 10% de la oferta, asignándose a las actividades que incluyan el desarrollo de proyectos, la comercialización y los esfuerzos de promoción.

Nos esforzamos por evitar cualquier actividad no deseada que pueda surgir al principio de la existencia de la moneda, cuando la moneda y su ecosistema aún no están maduros. El plan para asegurar el anteriormente mencionado 10 por ciento de la oferta total de ELCASH también incluye el beneficio añadido de desalentar la manipulación del mercado por parte de potenciales poseedores de volúmenes sustanciales de ELCASH.

Tabla 1. Estrategia de reducción de bloques y recompensas.

Período	Fecha	Bloques	Recompensa de bloque	Coins
1	Diciembre de 2020	4,200	500	2,100,000
2	Enero de 2021	52,500	75	3,937,500
3	Enero de 2022	52,500	70	3,675,000
4	Enero de 2023	52,500	65	3,412,500
5	Enero de 2024	52,500	55	2,887,500
6	Enero de 2025	52,500	40	2,100,000
7	Enero de 2026	52,500	25	1,312,500
8	Enero de 2027	52,500	15	787,500
9	Enero de 2028	52,500	7.5	393,750
10	Enero de 2029	52,500	3.75	196,875
...

Las monedas preminadas se utilizarán en diversas actividades que tienen un objetivo principal: atraer la atención y los usuarios al ecosistema ELCASH. Es una solución común y ampliamente aceptada que los proyectos destinen un número determinado de monedas a actividades de marketing y desarrollo. Creemos que esta solución proporcionará una forma saludable de financiar el desarrollo del proyecto y crear un futuro más brillante para el ecosistema de blockchain.

Ejemplos de casos de uso para este 10% de monedas Electric Cash pre-minadas:

- Esfuerzos promocionales
- Desarrollo del negocio
- Recompensas adicionales para los stakers
- Esfuerzos de marketing
- Anuncios en redes sociales
- Presupuesto para el software

Durante el primer año, la recompensa por bloque equivaldrá a 75 monedas. En cada período tras este, será reducida gradualmente. Después de siete años, la red cambiará a una estrategia de recompensas llamada “halving” en la que la recompensa por bloque se reducirá en un 50% cada año a partir de ese momento.

La oferta total de Electric Cash está actualmente limitada a 21.000.000 monedas, siendo idéntica a la oferta total de Bitcoin. Una oferta fija ayuda a minimizar la posible inflación y dilución. Sin embargo, si el proyecto gana popularidad en el futuro y la demanda de la moneda crece, los usuarios más activos de la red podrán aumentar la oferta a través de la votación democrática gracias a las herramientas del sistema de gobernanza, teniendo en cuenta que esto puede dar lugar a una pequeña inflación.

Es importante tener en cuenta que Electric Cash adopta un sistema de gobernanza a través de su comunidad y que será posible realizar cambios a todos sus aspectos según sea necesario. Esto hará posible que la comunidad tome decisiones sobre la economía de la criptomoneda. Además, el sistema de gobernanza servirá no sólo para mejorar la salud y la transparencia del proyecto, sino que también ayudará a que la moneda se adapte más rápidamente a las condiciones del mercado y a las necesidades de los usuarios, permaneciendo uno de los mejores proyectos en el mundo de las criptomonedas.

2.4. Tesorería para el Desarrollo

El proyecto ELCASH implementa un Fondo de Tesorería para el Desarrollo que consiste en el uno por ciento de las recompensas mineras recaudadas en un monedero especial gestionado por el sistema de gobernanza de Electric Cash. Los fondos se guardan de forma segura hasta que la comunidad vota para gastarlos. Puede cubrir los costes de las mejoras y cambios del protocolo, como el desarrollo de nuevas funcionalidades en el ecosistema de Electric Cash. Para que todo el proceso sea transparente, el saldo de los fondos recaudados se presenta en el Explorador de Gobernanza.

3. Ecosistema de Electric Cash

Electric Cash está diseñada para ser una criptomoneda similar al dinero en efectivo para el uso diario con una funcionalidad adicional de staking. El protocolo de Electric Cash está gobernado por los titulares de las monedas, los cuales tienen derecho a gestionar el desarrollo futuro del ecosistema. Todos estos aspectos están integrados en un único ecosistema, lo que permite a Electric Cash cubrir una mayor variedad de necesidades del mercado y de los usuarios.



STAKING



GOBERNANZA



MINERÍA COMBINADA

Para incorporar incentivos dedicados no sólo a los mineros, sino también a otros usuarios de la red, las recompensas por bloque de Electric Cash se dividen en tres partes. La primera y la más importante es para los mineros con Prueba de Trabajo. Los mineros son cruciales para garantizar el buen funcionamiento de la red y su seguridad. Pero los mineros no son los únicos interesados. Las personas que utilizan la red a diario y amplían el ecosistema de ELCASH son esenciales para que el proyecto crezca.

La moneda ELCASH como parte integrante del ecosistema

En este proyecto, el aspecto clave de la moneda ELCASH es su oferta a largo plazo para cada usuario activo. Por lo tanto, se ha diseñado un ecosistema integral en el que el poner las monedas en staking desbloquea recompensas y posibilidades adicionales. Gracias al sistema de gobernanza, los recursos internos pueden destinarse a la mejora de la red.

Para lograr esto, se ha implementado en la red un modelo de distribución única, en el que cada usuario es recompensado por su contribución, es decir:

- Una vez terminada la pre-minería inicial para acumular las monedas asignadas según el plan de distribución de monedas, la mayor parte de la oferta total de monedas se asigna a los mineros.
- Una parte de la oferta total se utiliza para las recompensas de staking.
- Una parte de la oferta total se destina al Fondo de Tesorería para el Desarrollo. Sólo puede utilizarse para futuros desarrollos (mejoras del protocolo) y sólo los miembros de la comunidad de la red (usuarios que participan y ganan GP) tienen derecho a gestionarlo (por ejemplo, mediante votación).

Creemos que este enfoque atraerá a los mineros en el lanzamiento. Como resultado, al final de la fase de arranque debería haber suficientes monedas en circulación y una cantidad significativa de poder de hash asegurando la red para que otras funcionalidades de la red puedan ser utilizadas y facilitar la adopción masiva en el uso diario.

3.1. Staking

3.1.1. Proceso de Staking

Staking es una forma de almacenar fondos. Al hacer staking, cada usuario puede contribuir activamente al crecimiento de la red a largo plazo y ayudar a prevenir el problema de exceso de oferta que podría afectar al tema de la inflación general a lo largo de los años. Esto, a su vez, aumenta la estabilidad de la red.

Los participantes de la red Electric Cash pueden poner ELCASH en staking para gobernar la red y obtener recompensas de la cantidad depositada. Las apuestas también recompensarán a los usuarios con beneficios adicionales como transacciones gratuitas y poder de gobierno (GP). Cada titular de Electric Cash puede poner en staking cualquier número de sus monedas.

3.1.2. Monedero del Staking y de Gastos

Uno de los elementos clave del ecosistema de Electric Cash es un monedero fácil de usar e intuitivo. La aplicación ELCASH Wallet incluye un Monedero de Gastos y un Monedero del Staking. El Monedero del Staking permitirá a los usuarios poner en staking sus monedas para recibir el poder de gobierno, transacciones gratuitas y recompensas por staking. Los usuarios tienen el control constante de los fondos y de la clave privada relacionados tanto con el Monedero del Staking como con el de Gastos, por lo que la seguridad es tan fuerte como los estándares personales del usuario.

3.1.3. Fondo de Recompensas por Staking

Una parte de la oferta total se reserva para la iniciativa de staking y se bloquea en el Fondo de Recompensas por Staking. Las recompensas se distribuyen periódicamente entre los participantes en función del importe y la duración de su staking. Las recompensas sólo pueden transferirse a los stakers una vez finalizado el periodo de bloqueo (staking). La retirada anticipada de fondos conlleva penalizaciones como la pérdida de las recompensas obtenidas hasta la fecha. No se acumula ninguna recompensa antes de la finalización de un periodo de staking predefinido. Las recompensas que no se acumulan permanecen en el fondo común y se distribuyen posteriormente entre otros stakers que mantienen su posición.

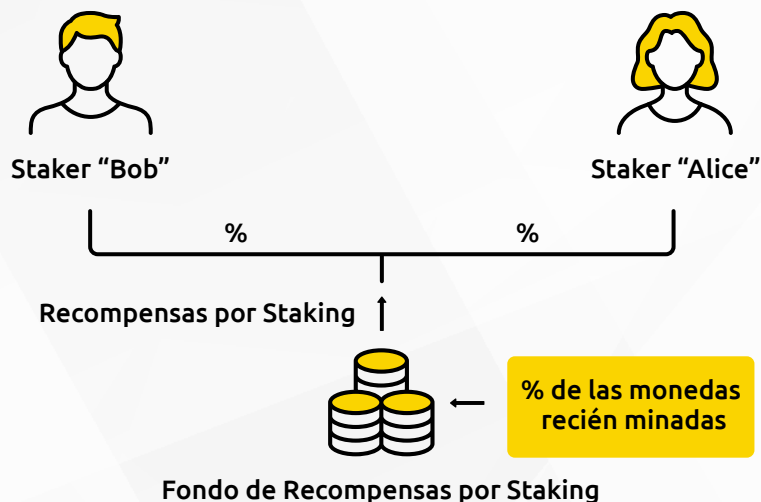


Figura 2. Flujo de distribución de las Recompensas por Staking

Una vez finalizado el periodo de staking acordado, los usuarios deciden qué hacer con los fondos adicionales recibidos. Pueden volver a poner ELCASH en staking o simplemente retirar las recompensas al Monedero de Gastos y utilizarlas como quieran. Sin embargo, al cerrar el staking se pierden los beneficios que vienen con la duración del staking acumulado.

3.2. Sistema de gobernanza

Con tal de lograr una democracia directa, Electric Cash implementa un sistema de gobernanza. En el proceso de gobernanza, se pueden proponer, diseñar, acordar e implementar nuevos cambios. Estos cambios no se limitan al código de fuente de la blockchain sino que también pueden cubrir otros aspectos importantes de la comunidad y de la red. Gracias al sistema de votos integrado en la blockchain, los usuarios podrán votar sobre las propuestas hechas por los miembros de la comunidad y/o el equipo de administración central de Electric Cash.

3.2.1. La importancia de la gobernanza

La gobernanza de la blockchain no es solamente un gesto simbólico hacia la comunidad. También es un elemento importante en el ecosistema de la blockchain. Hace que el proyecto sea más transparente y fácil de administrar. El hecho de introducir un sistema de gobernanza para Electric Cash hace que el proyecto sea más competitivo, ya que las decisiones se pueden tomar de forma más rápida, ajustándose mejor a las necesidades del mercado y de los usuarios.

Las monedas existentes se suelen crear en un código de fuente abierto y son fáciles de copiar. La diferencia entre ellas estriba en las personas que apoyan el proyecto. Las comunidades son la parte más importante y única de todo ecosistema de blockchain. No hay éxito en el mercado de las criptomonedas sin participación por parte de stakers.

3.2.2. Poder de Gobernanza (GP)

Durante el proceso de staking, los participantes de la red (stakers) obtienen Poder de Gobernanza (GP). El Poder de Gobernanza está directamente condicionado por los parámetros del staking: cuanto más alto sea el valor del staking y más largo sea el periodo del staking, más derechos de voto (gobernanza) tendrán los stakers sobre el ecosistema. El Poder de Gobernanza es intransferible (de monedero a monedero) y crea un ecosistema de usuarios confiables con “piel en el juego” que ponen más en staking y para más tiempo. Queremos hacer todo lo posible para garantizar que un mayor GP esté disponible sólo para los miembros más activos y dedicados de la comunidad ELCASH. Por lo tanto, el Poder de Gobernanza obtenido por un usuario cambiará con el tiempo si éste deja de ser activo en la red.

El sistema de gobernanza de Electric Cash tiene por objetivo crear un proyecto que sea:

- **Descentralizado:** Cada usuario de la red puede participar en la gobernanza. Cada usuario puede hacer propuestas y votar.
- **Transparente:** Todos los resultados de los votos, junto con su estado de implementación, están visibles en la página del Explorador de Gobernanza.
- **Inmutable:** Las decisiones tomadas en las votaciones son vinculantes y sólo pueden modificarse mediante una nueva votación.
- **Seguro y privado:** Todos los usuarios pueden votar de forma anónima. Sin embargo, si un usuario quiere que su nombre sea visible, el voto que emite puede ser verificado.

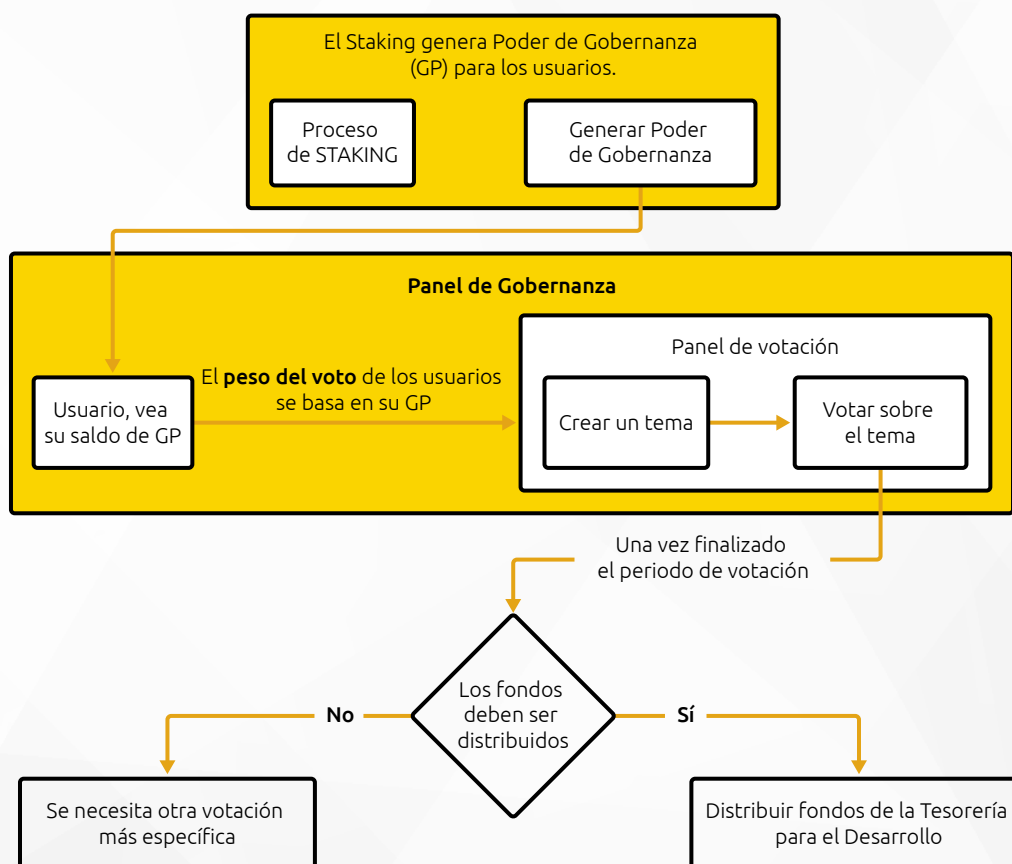


Figura 3. Sistema de gobernanza de Electric Cash.

Calcular el Poder de Gobernanza

El Poder de Gobernanza se calcula para recompensar a los usuarios más valiosos y más activos de la red. Cada usuario que haga staking con Electric Cash recibirá Poder de Gobernanza (GP). El factor del Poder de Gobernanza depende de los siguientes parámetros:

- **Cantidad en staking:** cuanto más ELCASH se ponga en staking, más poder de gobernanza obtendrá el usuario durante el período de staking.
- **Duración del staking:** dado que staking a largo plazo beneficia más a la red, los usuarios que hagan staking por más tiempo reciben más beneficios. Es decir, los usuarios que hagan staking para un período más largo o continuo recibirán más GP que los usuarios que pongan sus fondos en staking repetidamente, incluso si el tiempo acumulado de staking es el mismo.
- **Actividad en la red:** cuantos más usuarios activos haya y más contribuyan a la red, más GP pueden obtener. Puesto que el ecosistema ELCASH incluye staking, gobernanza, minería, etc., la participación en todas estas actividades será recompensada con GP respectivo.
- **Participación activa** en el proceso de voto y de gobernanza.

GP no es una moneda independiente. Es un derecho no monetario conectado a la dirección ELCASH del usuario y es no comerciable e intransferible (de monedero a monedero).

Crear propuestas

Cada usuario puede crear una nueva propuesta para que la red la vote. Para crear una nueva propuesta, el usuario debe pagar con su GP. Esto es para evitar inundar la comunidad con demasiadas propuestas.

La comunidad ELCASH decide sobre la economía y el ecosistema de la moneda. Los miembros pueden votar no sólo sobre funcionalidades adicionales, sino también sobre los parámetros de minería de Electric Cash, como la oferta total de la moneda. Esto ayudará a ELCASH a que sea competitiva y a que se mantenga actualizada en el futuro.

Votos

Todos los usuarios pueden votar sobre las propuestas presentadas en el panel de gobernanza. El voto de un usuario es proporcional a la cantidad de Poder de Gobierno obtenido. Para que la votación sea válida, debe alcanzarse un quórum basado en el total de GP de la red. Una vez finalizada la votación, cada usuario puede comprobar los resultados en el Explorador de Gobernanza.

3.3. Minería combinada

Durante las primeras etapas de desarrollo, ELCASH funcionará utilizando un proceso de minería combinado. Esto permitirá a ELCASH aprovechar la potencia de hash de cadenas más grandes basadas en SHA-256 (tipo Bitcoin), garantizando la seguridad general de la nueva red.

La minería combinada se implementa con Bitcoin, ya que ambas criptomonedas utilizan la misma función hash SHA-256. En este caso, BTC es la cadena madre y ELCASH es la cadena auxiliar. Como resultado, las soluciones de Prueba de Trabajo de Bitcoin (madre) pueden utilizarse para validar ELCASH (cadena auxiliar) como mecanismo de consenso de Prueba de Trabajo auxiliar (AuxPoW) (9).

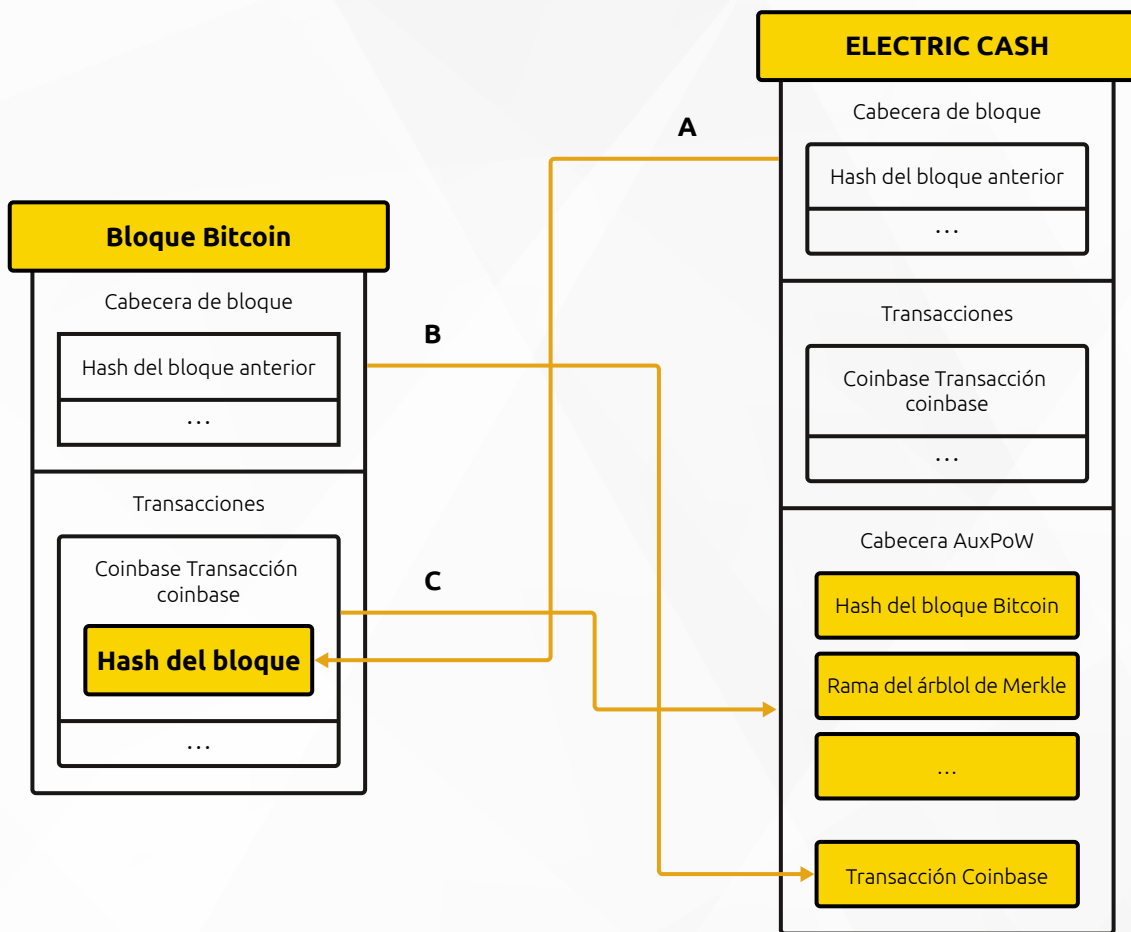
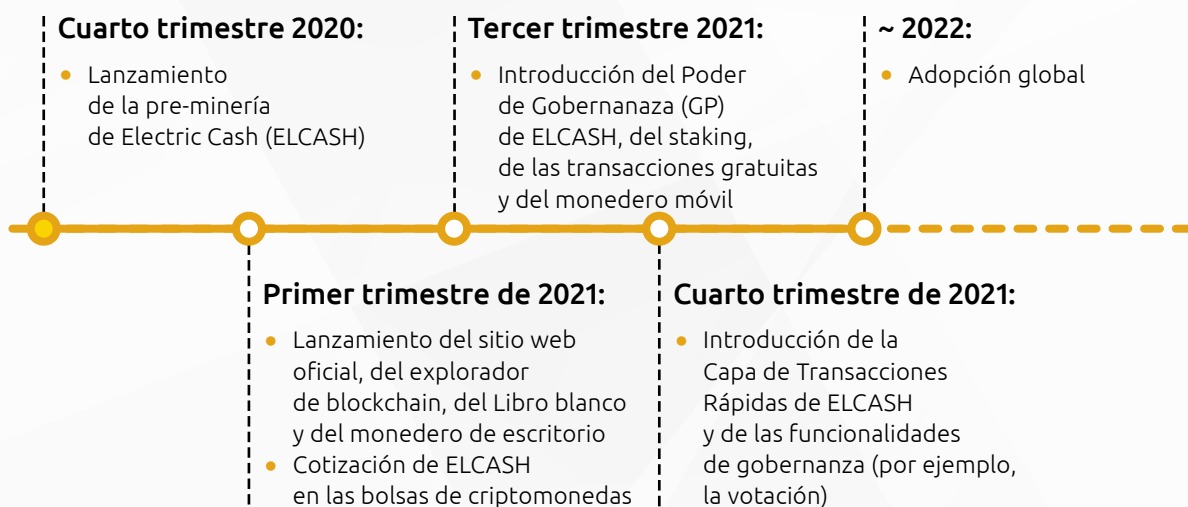


Figure 4. Structure of merged mined blocks in Electric Cash.

La minería combinada es un buen método para las nuevas blockchains como ELCASH, para aumentar la seguridad y reducir la vulnerabilidad a los ataques del 51%. La implementación de esa arquitectura de minería integrada al ecosistema nos da la confianza de que ELCASH cumple con los estándares de seguridad actuales de la industria.

Hoja de ruta de Electric Cash



Resumen

En este documento, presentamos Electric Cash (ELCASH). El objetivo del proyecto es proporcionar un ecosistema completo y resolver varios problemas importantes en la industria de las criptomonedas.

ELCASH facilita los pagos cotidianos. Al implementar una capa 2 adicional a la blockchain, puede realizar transacciones rápidas sin dejar de garantizar la seguridad de la red.

El protocolo ELCASH, diseñado para ser accesible y ligero, también se centra en reducir las comisiones por transacción. El staking también se recompensa con transacciones gratuitas, que se conceden en función del tamaño y la longevidad del total del staking. El ecosistema no sólo introduce tarifas reducidas, sino también beneficios adicionales como el Poder de Gobernanza. Al participar activamente en la red, cada poseedor de la moneda gana Poder de Gobernanza (GP) y puede tener un impacto directo en los cambios del protocolo. El GP se distribuye en función de los parámetros de participación del usuario y de la actividad de la red. Da derecho a participar en el proceso de gobernanza y a votar sobre las propuestas disponibles.

Creemos que este ecosistema descentralizado y centrado en la comunidad garantizará un crecimiento saludable y una perspectiva de proyecto global a largo plazo.

Definiciones

Fondo de Tesorería para el Desarrollo: un monedero especial de fondos recaudados de las recompensas de minería. Ese fondo está gobernado por los participantes de la red y está destinado a cubrir los costes de las mejoras y cambios del protocolo, por ejemplo, del desarrollo de nuevas funciones en el protocolo Electric Cash.

Gobernanza: el proceso por el que se proponen, diseñan, acuerdan y aplican los cambios en la red. Los cambios no se limitan a los detalles técnicos del código fuente de la blockchain, sino que también abarcan otras cuestiones importantes como el marketing y la educación.

Poder de Gobernanza (GP): el derecho por el que las partes interesadas (las que se ven afectadas por la red y pueden afectarla) ejercen el poder sobre la red.

Halving: un evento en que la recompensa por minar una nueva moneda se divide por la mitad, lo que significa que los mineros recibirán un 50% menos de recompensa por cada transacción que verifiquen.

Staking: el acto de bloquear criptomonedas para recibir Poder de Gobernanza y otros beneficios de la red.

Fondo de Recompensas por Staking: una parte de la oferta total reservada para las recompensas del proceso de staking. Las recompensas del fondo se distribuyen periódicamente entre los participantes en función del importe y la duración de su staking.

Fuentes

Para saber más sobre el proyecto, visite:

Página web: electriccash.global

Twitter: twitter.com/elcash_official

Telegram: t.me/elcash_official

Facebook: facebook.com/electriccash.official

Instagram: instagram.com/elcash_official

GitHub: github.com/electric-cash

Referencias

1. Nakamoto, S. Bitcoin: A Peer-to-peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>: s.n., Oct 2008.
2. S DiRose, M Mansouri. Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations. s.l.: IEEE, 2018.
3. N. Papadis, S. Borst, A. Walid, M. Grissa, and L. Tassiulas. Stochastic models and wide-area network measurements for blockchain design and analysis. IEEE Conference on Computer Communications: IEEE INFOCOM, 2018.
4. A Next-Generation Smart Contract and Decentralized Application Platform. [Online] December 2020. <https://ethereum.org/en/whitepaper/>.
5. N Papadis, L Tassiulas. Blockchain-based Payment Channel Networks: Challenges and Recent Advances. New Haven, CT 06511 USA: Department of Electrical Engineering, and Yale Institute for Network Science, Yale University,, 2020.
6. N Kshetri, J Voas. Blockchain-Enabled E-Voting. University of North Carolina at Greensbor: IEEE SOFTWARE, 2018.
7. L Gudgeon, P Moreno-Sanchez, S Roos, P McCorry. SoK: Layer-Two Blockchain Protocols. London: Imperial College London, 2019.
8. Shapiro, C. Information rules: a strategic guide to the network economy. 1999.
9. Zamyatin, A. Merged Mining: Analysis of Effects and Implications-DIPLOMA THESIS. s.l.: TU Wien, 2017.