MKTCASH

Tecnología descentralizada y segura en cualquier lugar.

White Paper

versión 1.2

www.mktcash.org

Tabla de Contenidos:

Introducción 1

Que es Mktcash 1

Especificaciones Técnicas 2

Tecnología 3

Economía 4

Halving 4

Modelo Económico 5

Precio 6

Usabilidad 6

Prueba de Participación 6

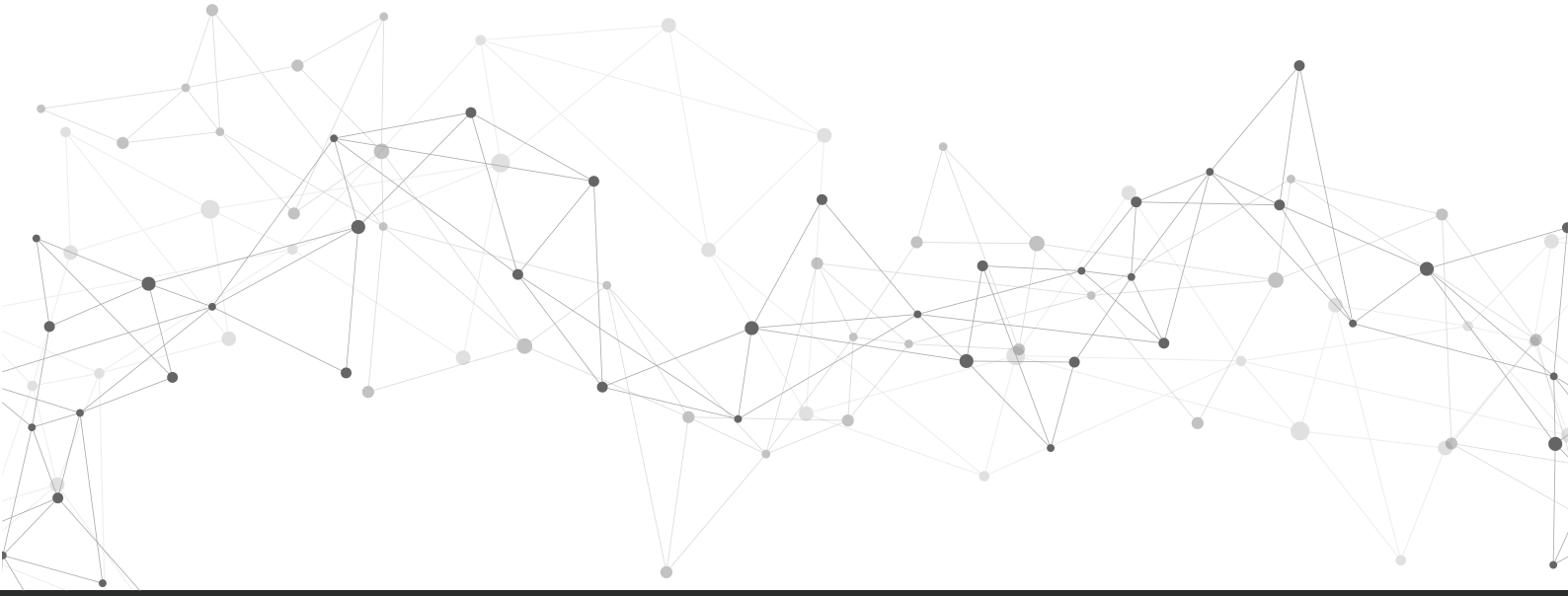
Recompensa Masternode 8

Privacidad 9

Gobernanza X Coin = 1 Voto 10

Nota Legal 12

Referencias 12



Introducción

En el año 2009 comienza la era de las criptomonedas, se publica el código fuente de la primera con un sistema único descentralizado, Bitcoin. Creada por la entidad Satoshi Nakamoto, bitcoin es una moneda que ha tenido un fuerte e importante crecimiento, pero aún tiene obstáculos para ser una moneda de adopción masiva o alterna al dinero fiduciario.

Mktcash es un sistema de dinero digital con el objetivo de empoderar a los usuarios con una estructura descentralizada y segura para el comercio y uso cotidiano, con transacciones casi instantáneas a un coste bajo de comisión y con algoritmo de consenso POS y Masternode. Es una moneda con una arquitectura peer to peer, para ser utilizada en las múltiples plataformas de comercio sin necesidad de un intermediario, ni validación de cuenta, ni autoridad central.

Que es Mktcash

Mktcash es dinero digital global, una moneda orientada en la descentralización y rapidez de transacciones.

El objetivo principal de la moneda es ofrecer a los usuarios un activo criptográfico electrónico capaz de ser usado como medio de pago online, como inversión o negocio, sin pasar por una entidad financiera o autoridad central, el control de las transacciones se verifica a través de la cadena de bloques, que ofrece información anónima de las entradas y salidas de cada transferencia entre monederos, funciona como un libro contable público descentralizado y verificable. El proyecto es de código abierto, con un suministro total de 500.000.000 MCH de las cuales se preminaron 23 Millones de MCH, en el bloque génesis.

El porcentaje de monedas pre-minadas para el proyecto representa el 4,6% en relación al suministro máximo de monedas, un porcentaje de monedas adicionales fueron entregadas a la comunidad MCH, como un intercambio sin costo, pero con una serie de requisitos específicos. Tenemos el premine de monedas mch para dar sostenimiento inicial a la infraestructura, sin posibilidad de manipular el ecosistema MCH, y que será utilizado para financiar temporalmente parte de las actualizaciones del software base mktcash ya que, en la distribución por bloque, no se contempla porcentaje de recompensa destinado para el desarrollo.

Especificaciones Técnicas

Moneda: Mktcash
Ticker: MCH
Protocolo: Pos + Masternodos
Algoritmo: Quark
Recompensas por bloque: 372 MCH
Recompensas por POS: 40% POS
Recompensas por Masternodo: 60% MN
Tiempo de bloque: 4 minutos
Pre-minado: 4,6% - 23 millones MCH
Suministro máximo: 500.000.000 MCH
Colateral MN: 150.000 MCH
Mínimo para Estaca: 100.000 MCH
Tamaño de bloque: 8 Mb
Moneda Usable: Después de 6 confirmaciones

Halving: 5 halvings
Decimales: 8
Subdivisión: MCHTOSHIS
Comisión por transacción: 0.0001 MCH
Minable: Si
Envíos instantáneos: Si
Puerto: 17223

Tecnología

Mktcash es un fork del código fuente de Pivx, esta tiene características mejoradas del código fuente de la moneda Dash, pero ambas manteniendo similar estructura base del código fuente de Bitcoin. Mktcash funciona de la misma manera, con la clave pública y privada, mediante el uso de firmas digitales, se intercambian monedas entre usuarios, al firmar digitalmente un hash de la transacción previa, donde se obtuvo monedas y la clave pública del próximo dueño y agregando estos datos al final de la transacción.
El beneficiario puede verificar las firmas digitales en la cadena de bloques una vez hecha la transacción. Se genera una nueva dirección publica para cada transacción para agregar más anonimato para el dueño de las monedas debido a que la dirección publica deja un rastro de transacciones pasadas.
La firma digital evita que la transacción sea modificada una vez que ya fue emitida y es utilizada para verificar la autenticidad e integridad de los datos digitales.

Economía

El suministro total de monedas es limitado y la oferta diaria decreciente en el largo plazo por los halvings, una característica importante de la moneda es el tiempo de bloque de 4 minutos para no inyectar demasiadas monedas nuevas a la economía MCH y tener el problema de sobreoferta descontrolada, otro parámetro es el colateral necesario para participar en Masternodos y Pos, de 0,03% en relación al suministro total, para masternodo y 0,02% para stake. Al ser una cantidad porcentualmente baja en relación al suministro total, es una forma de promover una participación de usuarios más global.

Mientras más masternodos participen en la red, se logrará que más monedas estén holdeadas, y produzca una mayor escasez de monedas, por lo que contribuye de manera positiva al ecosistema mktcash. En el largo plazo cuando el total del suministro entre en circulación las recompensas por bloque serán de las comisiones por transacción y la red seguirá dando incentivos a los participantes activos.

Halving

Es un proceso automático, escalado, preestablecido en el código fuente, en el cual se reducen las recompensas a la mitad cada 25.000 bloques aproximadamente, con un tiempo de 4 minutos por cada bloque, solo se producirán 5 halvings, luego del ultimo halving la recompensa sera de 10 MCH por bloque hasta el fin de nuevas emisiones de monedas con el objetivo de obtener un modelo deflacionario, ya que la cantidad de monedas es finita y no hay una autoridad que regule la base monetaria.

Grafico distribución de recompensas por bloque

FASE	ALTURA DEL BLOQUE	RECOM-PENSA	INCREMEN-TO	TOTAL
1	0-250000	372 MCH	18,6%	500M
2	250000-275000	180 MCH	0,90%	500 M
3	275000-300000	80 MCH	0,40%	500 M
4	300000-325000	40 MCH	0,20%	500 M
5	325000-350000	20 MCH	0,10%	500 M
6	350000-400000	10 MCH	0,20%	500 M
-	400000-500000	10 MCH	0,20%	500 M
-	500000-600000	10 MCH	0,20%	500 M
-	600000-700000	10 MCH	0,20%	500 M
-	700000-800000	10 MCH	0,20%	500 M
-	800000-900000	10 MCH	0,20%	500 M
-	900000-EN ADELANTE	10 MCH	N/A	500 M

Precio

El valor de mktcash está determinado por la ley de oferta y demanda, cuantos más usuarios soliciten la moneda en el mercado, la oferta disminuye por lo que el valor aumenta, caso contrario el valor baja. Mientras siga en aumento la demanda y al existir una cantidad máxima establecida de monedas, sumado a que los traders y comerciantes mantendrán un volumen de comercio constante y usuarios utilicen la moneda para efectuar compras, pagar servicios y otros bienes, el precio ira con volatilidad al alza y encontrara una estabilidad de precio. En el caso del dinero fíat, la constante emisión de papel moneda y políticas económicas de los países ocasionan crisis, y pérdida de valor de las divisas en el mercado. El precio de la moneda también puede calcularse en el acuerdo libre entre usuarios.

Usabilidad

Nuestra prioridad es desarrollar soluciones y aplicaciones tecnológicas que faciliten una adopción fácil y sencilla para el usuario, mktcash es funcional como medio de pago y el desarrollo inicial de un monedero Web, Android e IOS , facilita la portabilidad y flexibilidad en el uso de los Monederos, ya que actúan como clientes ligeros sin necesidad de descargar la cadena de bloques completa, reduce la dificultad de configuración y consumo de espacio en disco, además ofrecen un alto nivel de seguridad. El almacenamiento de las claves esta en el mismo dispositivo que las ejecuta, para las carteras móviles las claves privadas o frase de recuperación se pueden importar o exportar, otorgando el control al usuario sobre sus fondos y para el monedero web, que funcionan sobre una plataforma web, se puede agregar capas de seguridad extra para operar desde cualquier lugar.

Prueba de Participación

El protocolo de consenso adoptado por mktcash es Proof of Stake y Masternodos, Proof of Stake es más eficiente que la prueba de trabajo, ya que no demanda un alto coste económico a la red, y en el largo plazo es más escalable porque la participación no se determina en los usuarios que inviertan más dinero en poder de CPU para validar los bloques.
El nodo pos se dedica a validar bloques o transacciones y los masternodos agregan servicios integrales a la red de dos niveles que posee mktcash. La probabilidad de validar un bloque o conjunto de transacciones es aleatoria y en base a una serie de criterios. Es importante incentivar a los usuarios porque a más usuarios participando en la red, más segura será esta. A los nodos que hacen Pos se denominan validadores, y los usuarios deben mantener bloqueadas sus monedas en un monedero para votar el siguiente bloque, una vez validados los bloques se agregan a la cadena y son permanentes. La red incentivara con nuevas monedas como recompensa al usuario que valide un bloque o transacciones, la probabilidad de validar bloques o transacciones y recibir la recompensa correspondiente es directamente proporcional a la cantidad de monedas que el participante tenga acumuladas.

Un elemento necesario para la seguridad de la red es penalizar a los participantes que no deseen respetar el protocolo, el proceso consiste en eliminar una parte de las monedas bloqueadas por el validador en caso que intente romper el consenso, o no ejecute correctamente el software durante el proceso de validación.

La recompensa para el stake es de 40% por bloque, 148,8 MCH actualmente.

Elegibilidad de estaca PoS edad mínima de entrada: 60 minutos.

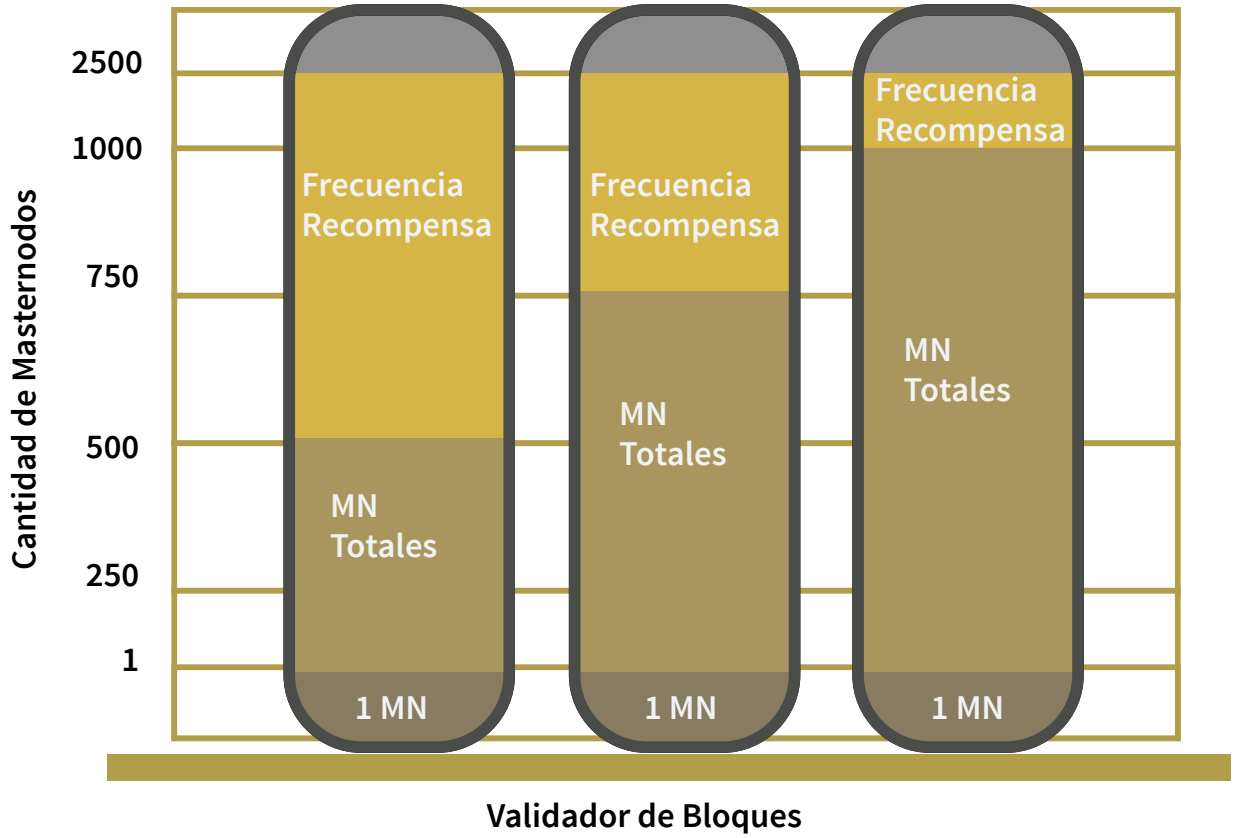
Confirmaciones de madurez: 60 confirmaciones.

Recompensa Masternode

El porcentaje más alto de nuevas monedas a la economía mktcash están destinadas para los masternodos, con el 60% de nuevas MCH por bloque son otorgadas por las múltiples funciones que ofrecen, los masternodos son servidores que almacenan una copia completa de la cadena de bloques deben estar conectados 24,7 a la red y operan con una cantidad fija de monedas. La función de un masternodo es mejorar la privacidad de las transacciones, reducir la volatilidad de la moneda, permite hacer transacciones de manera instantánea entre usuarios, además de mantener protegida y estable la red. El número diario de monedas otorgadas a cada masternode se calculará de acuerdo con la siguiente fórmula:

(Recompensas totales de masternode por bloque) x (número de bloques extraídos en 24 horas) / (número de masternodos ejecutados)

Gráfico Frecuencia de Recompensas:



La garantía requerida para crear un masternodo es 150.000 MCH, en la que se envía a una dirección del monedero, donde se activa y el masternodo se propagará en la red. En el proceso se crea una clave privada secundaria para firmar todos los mensajes posteriores. La última clave permite que la billetera esté bloqueada cuando se ejecuta en modo independiente. En cualquier momento el participante puede desactivar el nodo y liberar las monedas, sin penalización, pero dejara de recibir recompensas hasta que vuelva a crear nuevamente el masternodo. La recompensa de masternode es 223,2 MCH actualmente.

Privacidad

Mktcash permite hacer transacciones con una mínima comisión, entre pares con claves publicas únicas, registradas en un libro contable público descentralizado inalterable a lo largo del tiempo, sin intermediarios en el proceso, la información de una transacción es visible para el público, pero sin revelar datos que puedan ser asociados a un usuario. Las direcciones se crean de a pares, cada clave publica está asociada a una clave privada, estas se generan mediante criptografía de curva elíptica, y es la que permite enviar monedas a otro monedero. En el modelo bancario centralizado, se limita esa privacidad a la restricción de la información de las partes y de un tercero, básicamente el dinero que se comercializa posee una regulación que ralentiza y añade costos a las operaciones. Mktcash posee el algoritmo quark para proteger autenticar y mantener la confidencialidad de los datos, el algoritmo utiliza 18 funciones hashing hacia una sola dirección que, en conjunto, la posibilidad de que varias funciones se rompan al mismo tiempo es casi 0%, lo que la hace uno de los algoritmos más seguros.

Gobernanza X Coin igual 1 voto

Uno de los objetivos próximos es implementar una gobernanza descentralizada, debido a que es necesario integrar participantes en la toma de decisiones, también en el avance y mejoras con un mismo interés común para el protocolo mktcash. Para tener un crecimiento transparente y participativo, que la información sea visible para todos por igual. Las características de la gobernanza MCH son:

Participativa

Cualquier usuario puede obtener su derecho a voto, añadir fondos a la tesorería, y proponer propuestas. El modelo implementado es autónomo, necesita de la participación de varios usuarios para acumular la cantidad necesaria de votos para aprobar y ejecutar las acciones. Las propuestas deben aprobarse por mayoría o hasta alcanzar el presupuesto requerido de la misma.
Pueden enviar mayor cantidad monedas en el voto de acuerdo a la importancia que el usuario lo crea conveniente y esta se añadirá a la propuesta. La cantidad mínima para tener 1 voto es 3.000 MCH.

Organizada

La gobernanza mktcash no está basada en una estructura administrativa tradicional, la organización se basa en el consenso de los usuarios, con el cumplimiento de los criterios requeridos del sistema, y la verificación de las transacciones mediante el uso de la cadena de bloques. El equipo de mktcash esta integrado por colaboradores de

diferentes partes del mundo con un mismo objetivo común, también puede ampliarse con grupos de voluntarios distribuidos por internet, ya que el equipo se ajustará a medida que crezca la comunidad.

Descentralizada

Cada participante tiene los mismos derechos y están distribuidos en forma horizontal, sin jerarquías. El sistema esta diseñado para que tenga un autocontrol prestablecido, y no esté controlado por un grupo de personas o autoridad central, ya que se basa en la misma cadena de bloques mch para controlar las transacciones. Los usuarios pueden hacer propuestas de actualizaciones, de carácter comercial o social, inclusive de mejorar el protocolo mch, para impulsar la innovación. Los usuarios deben cumplir con el requisito de poseer 180.000 MCH como colateral, como norma principal para que pueden participar en las propuestas.

Código open source

El sistema implementado, será ejecutado de manera autónoma en la red con un código seguro diseñado para automatizar tareas, con la implementación del conjunto de normas para el correcto funcionamiento de la plataforma, utiliza la cadena de bloques mch para tener una base sólida, donde los usuarios podrán tener el control de sus transacciones.

Nota Legal

Este documento ha sido creado exclusivamente con fines informativos, no constituye o tiene la intención de ser una oferta para vender, transferir, emitir o adjudicar capital, bienes o servicios. Este documento no se entenderá como una invitación, publicidad, solicitud, recomendación o incentivo para invertir en cualquier instrumento financiero.
El proposito es presentar el proyecto Mktcash a las personas interesadas en tener monedas mch.
La información proporcionada en este documento no debe interpretarse como la base de una decisión o estrategia de inversión, su intención es solo proporcionar información general y preliminar a los interesados en hacer su aportación al proyecto.

Referencias:

[1] https://bitcoin.org/bitcoin.pdf

[2] https://cardaniers.com/proof-of-stake/

[3] Dominando-Bitcoin, Autor: Andreas Antonopoulos

[4] https://academy.bit2me.com/transacciones-bitcoin/

[5] https://medium.com/@riddo/introducci%C3%B3n-a-los-masternodes-80ea249275e8

MKTCASH

White Paper v. 1.2