**CipherShop: Un Mercado Eléctronico Automatizado Entre Pares Descentralizado y Controlado por los Usuarios**

CipherShop Dev Team

[dev@ciphershop.org](mailto:dev@ciphershop.org)

[www.ciphershop.org](http://www.ciphershop.org)

**Resumen**: un mercado electrónico descentralizado controlado por sus usuarios, permitiría evitar intermediarios, con comisiones muy bajas o nulas. No como los mercados electrónicos actuales, que tienen términos de uso y controlan a su merced las tarifas y las condiciones. Por lo que se propone crear un protocolo, en un escalado de segunda capa de Ethereum 2.0, que permitiría el desarrollo del protocolo teniendo como prioridad la evitación del fraude, la falta de confianza por parte de los usuarios al comprar directamente y evitar en lo posible el uso de intermediarios. Siendo estos últimos necesarios, solo cuando un usuario lo reclame debido a un posible fraude, el cual, un intermediario de confianza, pudiendo ser elegido por la comunidad, se encargará en base de las pruebas de resolver la incidencia. Además, el protocolo contaría con un sistema automático para que, cuando los usuarios decidan hacer cambios al protocolo, estos se hagan automáticamente, para esto se crearía un estándar ERC-20 de Ethereum, denominado CSHOP, que además permitiría incentivar a los usuarios que usen el protocolo y mediante un algoritmo de reputación, dar más incentivos a los usuarios, cuyas acciones sean benignas.

Contenido

[**1.** **Introducción** 3](#_Toc94467900)

[**2.** **Motivación** 4](#_Toc94467901)

[**3.** **Mecanismo del protocolo** 5](#_Toc94467902)

[**3.1.** **Descripción del protocolo** 5](#_Toc94467903)

[**3.2.** **Estados de las transacciones** 6](#_Toc94467904)

[**3.3.** **Compensación por reputación** 7](#_Toc94467905)

[**3.4.** **Gobernanza y control del protocolo** 7](#_Toc94467906)

[**3.5.** **Distribución de tokens inicial** 8](#_Toc94467907)

[**4.** **Arquitectura** 8](#_Toc94467908)

[**5.** **Conclusión** 8](#_Toc94467909)

[**6.** **Referencias** 8](#_Toc94467910)

# **Introducción**

En 2008, se presentó al mundo el protocolo Bitcoin, por Satoshi Nakamoto, un modelo financiero digital alternativo, que a lo largo de estos años, ha demostrado ser una alternativa al dinero tradicional, que lentamente cada vez va adoptando el público en general [1]. Como se ha demostrado con El Salvador que, en septiembre del 2021, adoptó como moneda legal el Bitcoin [2].

Posteriormente al Bitcoin, en 2013, Vitalik Buterin, presentó al mundo el protocolo Ethereum, cuyo proyecto se lanzó en 2015 [3].

Este protocolo cuyo objetivo es construir aplicaciones descentralizadas, a través de una *blockchain* integrado con un lenguaje de programación. Permitiendo escribir programas.

Ethereum se creó utilizando el mecanismo de consenso denominado prueba de trabajo, comúnmente conocido como *PoW*. Este mecanismo, propuesto por Satoshi Nakamoto, pretende construir un mecanismo de consenso distribuido sin intermediarios y resolver el problema de doble gasto.

Pero en 2020, como parte de la estrategia de la comunidad para escalar Ethereum, se plantea cambiar al mecanismo de consenso denominado prueba de participación (*PoS*) [4]. *PoW* y *PoS*, son dos mecanismos diferentes con sus respectivas desventajas y ventajas, pero no es objetivo de este artículo entrar en los detalles técnicos de los respectivos mecanismos.

Si bien, el objetivo de escalado de Ethereum pretende rendir según las necesidades demandadas, debido al incremento en el número de transacciones, por lo que las tarifas de *gas*, que es la unidad que mide el trabajo computacional requerido para ejecutar una acción en la red de Ethereum, aumentan a un nivel que actualmente son caras para las futuras aplicaciones descentralizadas [5].

Por esto cabe mencionar las alternativas a Ethereum, que actualmente son:

* Solana, lanzado en 2020, cuenta inicialmente con un alto procesamiento de transacciones por segundo. Utiliza Rust como lenguaje de desarrollo [6].
* Polkadot, lanzado también en 2020, pero ellos mismos indican que es pronto para ejecutar programas, por lo que queda descartado [7].
* Cardano, lanzado en 2017, pero aún está en una fase muy temprana, al igual que Polkadot [8].

Por tanto, las opciones actualmente viables son: Ethereum 2.0 y Solana. Ethereum 2.0, es el conjunto de actualizaciones que llevarán a Ethereum, a ser una *blockchain* con más rendimiento, si bien, las tarifas de gas, es probable que no se reduzcan con las futuras actualizaciones.

Pero, Ethereum 2.0 cuenta con una comunidad muy grande y, además, según su fundador Vitalik Buterin, si bien Ethereum 2.0 no será lo suficiente escalable y descentralizado, existen los denominados *rollups* de segunda capa, como Arbitrum, Optimism, Polygon, Loopring, etcétera. Lo que permitirían unos costes de gas muy bajos, al estar la ejecución de la transacción, fuera de la principal cadena de Ethereum. Por este motivo, nos decantamos por desarrollar el protocolo, en Ethereum 2.0, a través de los *rollups* de segunda capa [9].

Si bien, es posible que a medida que otras alternativas, vayan creciendo e implementando y depurando la funcionalidad de ejecutar contratos inteligentes, el protocolo se adaptará para que acepte varias *blockchains*, pero esto queda para el futuro y la decisión de la comunidad.

# **Motivación**

Existen numerosos mercados muy grandes a nivel internacional entre pares, como EBay, Wallapop, etcétera. Pero estos mercados, o bien, están regulados por intermediarios y normas de uso, que ponen las propias empresas o creadores. Además, están centralizados, siendo de esta manera más vulnerables a ataques informáticos. También usan dinero estándar para las compras de bienes físicos y/o digitales. Y lo más importante, llevan un importante riesgo de fraude, y posible falta de confianza por parte de los compradores.

Por lo que proponemos crear un protocolo que:

* Utilice como pago criptomonedas, siendo estas una alternativa al dinero usado actualmente, con el beneficio de que no conllevan el uso de intermediarios, como los bancos.
* Permita la compra de cualquier material físico y/o digital, siendo opcional el uso del estándar ERC-721 (NFTs). Favoreciendo así el uso de criptomonedas. Pues son en realidad las aplicaciones, las que añaden valor real al ecosistema de las criptomonedas.
* Incentive a los usuarios que usen la plataforma, de esta forma que sean los propios usuarios quienes manejen el futuro del protocolo, mediante un sistema de gobernanza. Además se utilizará un sistema de reputación como comprador y vendedor, que permita obtener más recompensas o menos, en función de las acciones que decidan hacer los usuarios del protocolo.
* Minimice el fraude y la falta de confianza de los compradores y vendedores, a través de unas reglas establecidas.
* Evite a toda costa el uso de terceros o intermediarios, pero al tratarse de un sistema entre pares, a pesar de que el protocolo minimice el fraude lo máximo posible, siempre pueden encontrarse incidencias, para esto, de forma opcional, el protocolo contará con un sistema con el cual un administrador fiable, inicialmente del equipo de CiperShop, y posteriormente pudiendo ser otros administradores elegidos por la comunidad, resolverán la incidencia en base a las pruebas proporcionadas.
* Sea en todo momento transparente, de código abierto, bien documentado y disponible desde el inicio para los usuarios.
* Tenga una interfaz simple y de fácil acceso para cualquier tipo de público.

Vemos necesario, buscar posibles alternativas de mercados como el propuesto, los cuales son:

* 4k.com, un mercado que permite a los usuarios crear NFT’s representando, objetos físicos. Pero examinando la web, el proceso de listar productos, pasa por intermediarios, la tienda misma. CipherShop busca algo más intuitivo, entre pares, sin intermediarios.
* Monacomarket.co, otro mercado, que igualmente utiliza NFT’s. Pero no parece que sea controlable por los usuarios. Ni tenemos acceso al mercado. Un problema es que limita la compra/venta a un único token. En CipherShop, buscamos que el usuario decida que token ERC-20 usar. Y tampoco es de código abierto.
* OpenBazaar: mercado descentralizado, que permite crear tu propia tienda y vender con criptomonedas. Es la alternativa más parecida y viable, pero CipherShop busca automatización en la compra y venta de productos y, sobre todo, que sea controlado por sus usuarios.

Sinceramente, no se ha encontrado mucho más en la web, y lo que se ha encontrado no es lo que busca CipherShop, por este motivo, nos consideramos pioneros en este campo.

# **Mecanismo del protocolo**

# **Descripción del protocolo**

El protocolo consiste en una serie de contratos inteligentes de Ethereum que permiten crear todo lo mencionado anteriormente.

El funcionamiento del protocolo no es ninguna complejidad, consiste en el uso de una tercera parte como intermediario. En este caso, la tercera parte consiste en un contrato inteligente de Ethereum en el que se guardarán los depósitos, cuando el comprador haya recibido el producto, el vendedor recibirá el dinero.

En detalle, un usuario con una cartera con acceso a la Web 3.0, como MetaMask, Fortmatic, WalletConnect, etcétera. Tendrá acceso a la interfaz diseñada para interactuar con el protocolo.

Un usuario, en este caso un vendedor, mediante una dirección de Ethereum podrá registrar un producto físico o digital, junto a unas características: título, descripción, fotos del producto, categoría, precio, tipo de criptomoneda, país desde el que se envía, país o países a los que se envía, método de envío, tiempo de envío, si admite devoluciones, si es visible para el público o si es solo visible para ciertas direcciones de Ethereum.

Otro usuario, en este caso un comprador, podrá realizar ofertas por un precio menor, o comprar el producto directamente. En caso de ser una oferta, está irá al contrato inteligente creando un depósito, con los detalles de la oferta y una fecha de validez. Pasado el tiempo de validez si el vendedor, no acepta la oferta, este depósito será reembolsado al comprador. Si la acepta, pasará a ser como si fuera una compra directa, con lo que el resto de las ofertas serán canceladas y los depósitos devueltos a sus correspondientes usuarios. Y se iniciará una transacción.

En la transacción, se detalla las características de la compra, como el producto, la cantidad y su estado, es decir, si se ha marcado como enviado por el vendedor, recibido por el vendedor, recibido por el comprador, si se ha solicitado una devolución, en caso de que el vendedor haya indicado que acepta devoluciones, y en caso de la devolución, lo mismo pero de manera reversa, si el comprador lo ha marcado como, enviado, recibido, etcétera.

La transacción finalizará en varios estados, pudiendo finalizar exitosamente, cobrando una comisión del 0,3%, de la cual un 70% irá para el tesoro de la comunidad, y un 30% para el propio contrato inteligente, para pagar futuras transacciones automatizadas. Dependiendo de cómo finalice el estado de la transacción, esta influirá en la reputación como vendedor o la reputación como comprador, según el caso.

En caso de incidencias, participará en la transacción un administrador fiable, inicialmente del equipo de CiperShop y, posteriormente pudiendo ser elegido por la comunidad. El cual se encargará de resolver la transferencia en favor del comprador o del vendedor en base a las pruebas proporcionadas. Cabe destacar que el vendedor se encarga de todo el proceso hasta la recepción del producto por el comprador, en caso contrario, el intermediario actuará en favor del comprador.

# **Estados de las transacciones**

Los posibles estados son los siguientes:

1. Si el vendedor cancela el envío antes de marcarlo como enviado, se devolverá el depósito íntegro al comprador. Pero esto bajará la reputación como vendedor, del vendedor.
2. Si el vendedor marca el producto como enviado y posteriormente como recibido, y el comprador no realiza ninguna acción en 14 días posteriormente a que el vendedor haya marcado la transacción como recibida, se considerará una compra exitosa, enviando el depósito al vendedor previamente aplicando comisiones, y no pudiendo ser revertida. Esto bajará la reputación de comprador del comprador, y subirá la reputación de vendedor del vendedor.
3. Si el vendedor, marca el producto como enviado y el comprador marca el producto como recibido, se considerará una compra exitosa, enviando el depósito al vendedor previamente aplicando comisiones, y no pudiendo ser revertida. Esto subirá la reputación como vendedor del vendedor y también subirá la reputación de comprador del comprador.
4. Si el vendedor, no marca el producto como enviado pasados 14 días, el comprador podrá marcar el producto como recibido, si lo hace, esto se considerará una compra exitosa, enviando el depósito al vendedor previamente aplicando comisiones, y no pudiendo ser revertida por el comprador. Esto bajará la reputación como vendedor del vendedor y subirá la reputación de comprador del comprador.
5. Si el vendedor, no marca el producto como enviado en un periodo de 30 días, y el comprador no realiza ninguna acción en este periodo de tiempo, el depósito se devolverá íntegro al comprador. Bajando la reputación del vendedor como vendedor y también bajando la reputación de comprador del comprador.
6. Si el vendedor, marca el producto como enviado y pasados 14 días, el vendedor si no ha recibido el producto podrá poner una reclamación, dejando a un administrador resolver la incidencia, decidiendo este a favor de quien resuelve la incidencia. La reputación si se resuelve la incidencia en favor del vendedor, aumentará la reputación de vendedor del vendedor y bajará la reputación de comprador del comprador. En caso contrario, si se resuelve en favor del comprador, la reputación de comprador del comprador subirá, y la reputación de vendedor del vendedor bajará.
7. Si el vendedor, acepta devoluciones en el pedido y marca como enviado el pedido, y el comprador lo recibe y este opta por una devolución, se aplicarán los estados 2, 3, 4, 5 y 6, pero al contrario, pasando a ser el rol de vendedor el del comprador.

En resumen, los estados normales son el 1, 2, 3, 4 y 5. Los estados con incidencias son el 6. Y el estado de devoluciones el 7, 2, 3, 4, 5 y 6, pero cambiando los roles de vendedor y comprador, como se especifica en el estado 7.

# **Compensación por reputación**

Cada usuario, tiene asociado una reputación como vendedor y otra como comprador. El objetivo de esto, es fomentar el uso del protocolo dando recompensas en ventas exitosas a los usuarios. Para que sean los propios usuarios quienes puedan tener control sobre el futuro del protocolo. Para esto se creará un token ERC-20 de Ethereum, denominado CSHOP.

A los vendedores de base, en ventas exitosas, se les dará 300 CSHOP, mientras que a los compradores 50 CSHOP.

En base a la reputación, como vendedor o comprador, que tendrá un nivel de -20 a 150. Con las siguientes fases:

* De -20 a 0: 300 CSHOP al vendedor y 50 CSHOP al comprador en ventas exitosas.
* De: 1 a 10: 350 CSHOP al vendedor y 70 CSHOP al comprador en ventas exitosas.
* De 11 a 49: 460 CSHOP al vendedor y 100 CSHOP al comprador en ventas exitosas.
* De 50 a 99: 600 CSHOP al vendedor y 140 CSHOP al comprador en ventas exitosas.
* De 100 a 149: 760 CSHOP al vendedor y 200 CSHOP al comprador en ventas exitosas.
* Con 150: 1000 CSHOP al vendedor y 300 CSHOP al comprador en ventas exitosas.

Adicionalmente a las reputaciones marcadas por el protocolo, los compradores podrán valorar al vendedor, estando esta segunda opción visible.

# **Gobernanza y control del protocolo**

Mediante la incentivación a los usuarios que utilicen el protocolo, esto permitiría que sean los propios usuarios quienes puedan controlar actualizaciones del protocolo o cambios base de las condiciones.

Por lo que el protocolo contaría con un sistema de gobernanza en la que los usuarios con CSHOP, podrían votar en cambios o dar ayudas a organizaciones o financiar proyectos relacionados con CipherShop y así crear un gran ecosistema.

Para lanzar una proposición en la gobernanza, se necesitan al menos 100 CSHOP propios o delegados. Habrá un periodo de votación de 7 días, en el que cualquiera con CSHOP puede votar y dependiendo del tipo de propuesta, si alcanza al menos, 500.000 CSHOP de votos, propios o delegados y un 51% de votos positivos, se ejecutará automáticamente a los 2 días el código para ejecutar el cambio, si es un cambio de gobernanza. Puesto que habrá diferentes tipos de propuestas.

# **Distribución de tokens inicial**

En un inicio se generarán 1.000.000.000 (mil millones) de CSHOP, siendo estos distribuidos a lo largo de 4 años en las siguientes proporciones:

* 56% para la comunidad y el tesoro de la comunidad. A los 4 años: 560.000.000 CSHOP.
* 24.333% para el equipo de desarrollo. A los 4 años: 243.330.000 CSHOP.
* 18.069% para inversores. A los 4 años: 180.690.000 CSHOP.
* 0.968% para pequeños inversores iniciales. A los 4 años: 9.680.000 CSHOP.
* 0.63% para anunciantes. A los 4 años: 6.300.000 CSHOP.

Un total de 120.000.000 CSHOP estarán inicialmente disponibles para la comunidad y el tesoro de la comunidad. De estos, 20.000.000 (un 16.6667%) estarán disponibles en el contrato inteligente del protocolo, para incentivos los incentivos de los usuarios que usen el protocolo.

Como se puede ver, hay dos fases de captación de inversores, la primera fase disponible para cualquier usuario tendrá como objetivo conseguir un mínimo de capital, para auditar el protocolo y ver vulnerabilidades, lanzar el protocolo y contratar miembros para el equipo, que actualmente es de una persona.

En la primera distribución para pequeños inversores, estarán disponibles para compra directa mediante un contrato inteligente, garantizando así la seguridad; 2.000.000 CSHOP. Con un precio inicial de 0,16$, con un incremento de 0.01$ por cada 400.000 CSHOP vendidos.

La segunda fase de captación de inversores corresponderá con el lanzamiento oficial de la moneda, junto al protocolo, una vez auditado y testeado correctamente. Con el objetivo de atraer a grandes inversores que quieran formar parte del proyecto, financiándolo y ayudar a crear un gran ecosistema.

La distribución de tokens CSHOP a lo largo de los 4 años será la siguiente:

* Año 1: 40%
* Año 2: 30%
* Año 3: 20%
* Año 4: 10%

Para la comunidad y el tesoro de la comunidad y los pequeños inversores iniciales, el porcentaje se calculará restando el monto total a los 4 años establecidos, menos la cantidad inicialmente disponible.

A partir de los 4 años, habrá una inflación anual del 1,6%.

# **Arquitectura**

El protocolo consiste en contratos inteligentes, alojados en la red *blockchain* de Ethereum. Lo que hace que el *back-end* de la aplicación, esté descentralizado. El *front-end*, se alojará usando IPFS, creando de esta manera una aplicación completamente descentralizada. Estando el código disponible tanto de los contratos inteligentes como del *front-end* abierto al público y disponible en GitHub.

Para servir la aplicación, si bien los archivos estáticos están alojados de manera descentralizada. Se usará un servidor *cloud* centralizado para dar servicio a esos archivos estáticos. Por lo que si bien no es 100% descentralizada, se utilizan todos los recursos disponibles en el momento, para que sea lo más descentralizada posible.

# **Conclusión**

Hemos definido un protocolo, para una tienda automatizada basada en Ethereum, con uso de intermediarios dado la necesidad. Desarrollada de manera descentralizada, aumentando de esta manera la seguridad.

Y lo más importante, teniendo el poder del futuro del protocolo en mano de los usuarios, mediante un sistema de gobernanza, como indicado anteriormente.

# **Referencias**

|  |  |
| --- | --- |
| [1] | S. Nakamoto, «Bitcoin white paper,» 2008. [En línea]. Available: https://bitcoin.org/bitcoin.pdf. [Último acceso: Enero 2022]. |
| [2] | O. Avan-Nomayo, «cointelegraph.com,» 7 Septiembre 2021. [En línea]. Available: https://cointelegraph.com/news/september-7-is-bitcoin-day-in-el-salvador-as-btc-becomes-legal-tender. [Último acceso: 6 Enero 2022]. |
| [3] | V. Buterin, «ethereum.org,» 2013. [En línea]. Available: https://ethereum.org/en/whitepaper/. [Último acceso: Enero 2022]. |
| [4] | ethereum.org, «ethereum.org,» 2022. [En línea]. Available: https://ethereum.org/en/upgrades/. [Último acceso: Enero 2022]. |
| [5] | ethereum.org, «etherscan.io,» 2022. [En línea]. Available: https://etherscan.io/gastracker. [Último acceso: Enero 2022]. |
| [6] | solana.com, «solana.com,» 2021. [En línea]. Available: https://solana.com/. [Último acceso: Enero 2022]. |
| [7] | polkadot.network, «polkadot.network,» 2020. [En línea]. Available: https://polkadot.network/. [Último acceso: Febrero 2022]. |
| [8] | cardano.org, «cardano.org,» 2017. [En línea]. Available: https://cardano.org/. [Último acceso: Febrero 2022]. |
| [9] | V. Buterin, «vitalik.ca,» 6 Diciembre 2021. [En línea]. Available: https://vitalik.ca/general/2021/12/06/endgame.html. [Último acceso: Febrero 2022]. |