



Binance, el mayor exchanger de criptomonedas, lanzó una versión inicial de su esperado servicio de comercio descentralizado (dex), que está disponible en [testnet.binance.org](https://testnet.binance.org).

El lanzamiento, que inicialmente es una red de prueba como se puede observar en la URL, lleva mucho tiempo en desarrollo y tiene el objetivo de complementar el intercambio principal de Binance, que genera alrededor de 1,000 millones de dólares en volúmenes de transacciones diarias, según datos de CoinMarketCap.

El servicio principal está centralizado, como la mayoría de los demás, lo que significa que el exchanger gestiona el saldo fiat o de criptomoneda de sus clientes. Los intercambios centralizados también fijan el precio, seleccionan los activos en oferta y ganan dinero con las tarifas de transacción. Algunos afirman que es necesario, pero otros se oponen al proyecto.

Vitalik Buterin, creador de Ethereum, dijo que los exchangers centralizados deberían «arder en el infierno» por su posición de control.

Según comerciantes criptográficos, los clientes están expuestos a pérdidas debido a cortes, además de otros problemas inesperados. El consejo común es que los usuarios tomen el control de su propia criptomonedas y la administren por medio de una billetera. Ahí entra en juego un dex, ya que les permite comerciar directamente desde su billetera, en oposición al difícil método de transferir tokens a un exchanger para luego intercambiarlas y retirar. Entonces, el dex de Binance es un complemento directo de su exchanger centralizado y brinda a los clientes más opciones.

«La cadena Binance tiene una finalidad de transacción casi instantánea, con tiempos de bloqueo de un segundo. Esto es más rápido que otras blockchains de hoy. Con la tecnología de la cadena de Binance central, Binance DEX puede manejar el mismo volumen de operaciones que Binance.com está manejando ahora. Esto resuelve los problemas que muchos otros exchangers descentralizados enfrentan con velocidad y potencia», dijo Changpeng CZ Zhao, CEO de Binance.



Zhao también promocionó el dex como un nuevo controlador de ingresos para la compañía porque se encuentra en la propia cadena de bloques de Binance, y la compañía opera varios nodos. Zhao afirmó que cuando sus nodos se utilicen en transacciones, la compañía ganará parte de la tarifa de la red.

No se trata de que Binance necesite ayuda para ganar dinero, pues un informe reciente de The Block especifica que la compañía obtuvo una ganancia de 446 millones de dólares en 2018, un año que definitivamente fue una decepción para la industria criptográfica en general.

Sin embargo, existe una preocupación acerca de la dex de Binance, ya que incluye una opción para desbloquear una billetera con una clave privada.

Esto es algo muy importante, pues pegar una clave privada en un navegador es un problema en círculos criptográficos, ya que deja a los usuarios vulnerables a los ataques de phishing.

Se recomienda a los usuarios que eviten esta opción para desbloquear un monedero porque existe una gran cantidad de alternativas como Metamask, una popular extensión de navegador con más de un millón de usuarios, dispositivos de hardware como Ledger, Trezor o Yubikey y más recientemente, aplicaciones de autenticación, como MyEtherWallet o Parity Signer.

De esas opciones seguras, Binance dex admite en la actualidad a Ledger, pero las otras opciones son la carga de archivos de KeyStore o la clave privada menos segura o la frase mnemónica.

Aunque la compañía puede argumentar que la responsabilidad recae en el usuario debido al manejo de claves privadas, los proveedores de servicios tienen una cierta responsabilidad.

Muchas personas, incluido Zhao, aseguran que la adopción de criptografía está en sus inicios, mientras que términos como «educación» y «democratización» se repiten a menudo por muchos en el espacio. Eliminar la clave privada y, por lo tanto, limitar los posibles ataques de



suplantación de identidad, parece ser parte de la educación de nuevos usuarios, ayudando a la criptografía a ser más segura para otros usuarios.

Los ataques de phishing son reales y más comunes de lo que se cree. La cartera MyCrypto.com aseguró que fue atacada regularmente, incluyendo un secuestro de sus servidores DNS de Amazon, mientras que MyEtherWallet fue atacada al menos dos veces el año pasado cuando los atacantes persiguieron su DNS y engañaron a otros usuarios al comprometer un servicio VPN gratuito.

Por otro lado, una investigación de Cisco sugiere que los ataques de phishing causaron una pérdida de 50 millones de dólares en tres años, mientras que los estafadores robaron 2.3 millones de dólares solo en el segundo trimestre de 2018, según datos de Kaspersky.

Estas amenazas llevaron a MyCrypto a eliminar la opción de clave privada de su servicio principal basado en la web.

«Estamos eliminando el soporte para claves privadas en la versión web de MyCrypto porque no es seguro, y alentamos a otros a que sigan su ejemplo», publicó la compañía en Medium.

MyEtherWallet, que compite directamente con MyCrypto, tiene una fuerte advertencia sobre su opción de entrada de clave privada, mientras que Binance, a su favor, advierte a los usuarios de dex que utilizar una clave privada o una frase mnemotécnica para desbloquear su cartera digital, significa que existe *«una posibilidad mucho mayor de perderlos debido a sitios web de phishing o aplicaciones»*.

Pero existe algo positivo, pues Binance dijo que planea agregar la opción de desbloquear una billetera en el dex con Trust Wallet, la aplicación móvil que adquirió el año pasado.

«Estamos trabajando hacia la accesibilidad descentralizada a la criptomoneda.



*Queremos que los usuarios tengan control total sobre sus claves privadas y un fácil acceso a las aplicaciones descentralizadas, para maximizar el potencial y la adopción generalizada de la criptomoneda. Binance DEX está un paso más allá para hacer realidad nuestra visión de una mayor libertad de dinero», dijo Viktor Radchenko, fundador de Trust Wallet.*

Eso sería un gran paso adelante para reforzar la seguridad. Sin embargo, resulta decepcionante que Binance no haya tomado una posición al respecto.