Incognito es un nuevo proyecto de privacidad e interoperabilidad que busca anonimizar los tokens de cualquier cadena de bloques. Como parte de su objetivo, la organización está lanzando versiones privadas de las plataformas financieras descentralizadas líderes de Ethereum (ETH).

Anunciada el 24 de abril, la iniciativa pKyber es la primera parte de la iniciativa Incognito para hacer que DeFi sea privado. Teorizado por primera vez en octubre, pKyber comenzó las pruebas a gran escala el 24 de abril. El equipo planea lanzar esto a la red principal de Incognito el 7 de mayo.

Funcionamiento

Incognito es una cadena de bloques independiente que se enfoca en transacciones privadas. Su tecnología de privacidad se basa en las mismas tecnologías utilizadas por Monero, incluidas las firmas de anillo, las direcciones ocultas y las transacciones confidenciales.

A diferencia de Monero, Incognito se centra en la interoperabilidad con otras blockchains y admite tokens privados. Andrey Bugaevski, líder del ecosistema en Incognito, dijo a Cointelegraph que el objetivo del proyecto es crear una cadena lateral universal para que las cadenas de bloques públicas se beneficien de las características de privacidad.

Bugaevski enfatizó que si bien Incognito no admite contratos inteligentes completos, todavía permite la creación de tokens y un conjunto limitado de instrucciones de scripting. Estos son suficientes para crear puentes sin confianza con otras plataformas de contratos inteligentes.

La plataforma pKyber utiliza el contrato inteligente de blindaje de Incognito para interactuar con el intercambio descentralizado Kyber en mainnet. Los usuarios realizan transacciones con pEthereum, un token privado, para iniciar una transacción con pKyber. El contrato de *«Broker»* de Incognito en Ethereum lee dichos datos e inicia una transacción de Ethereum en Kyber utilizando su grupo compartido de ETH público.

Especialmente, Incognito actúa como un proxy sin confianza para las instrucciones

comerciales privadas, lo que permite a una persona intercambiar ETH por la stablecoin DAI sin interactuar directamente con la cadena de bloques Ethereum.

La hoja de ruta de Incognito también incluye integraciones con 0x, Uniswap y la plataforma de préstamos Compound.

Aunque la integración de DeFi es la última actualización de Incognito, el proyecto logró muchos hitos desde el lanzamiento de su mainnet el pasado 31 de octubre de 2019. *El proyecto ahora ofrece una forma funcional para proteger Ethereum, Bitcoin, USDT, DAI, BAT, ZIL y otros tokens más.*

Cabe señalar que este sistema, como cualquier blockchain con privacidad opcional, debe usarse con cuidado al «mezclar» fondos.

Se puede acceder a la mayoría de las funciones por medio de una billetera de Incognito centrada en dispositivos móviles, disponible tanto para iOS como para Android. La billetera incluye características dedicadas como el intercambio descentralizado de Incognito, los servicios de replanteo y protección de tokens.

Existe un token patentado llamado PRV, cuyo propósito principal es ser utilizado para las tarifas de transacción. Pero las tarifas también se pueden pagar con el token utilizado para la transacción. Esto se hizo para mantener la usabilidad, con Bugaevski afirmando:

> *«No estamos tratando de construir una nueva moneda de privacidad. Nadie necesita un nuevo Monero o un nuevo Zcash».*

El PRV se utiliza como recompensa en bloque para los validadores, ya que Incognito usa el modelo de Prueba de Estaca (PoS). A diferencia de muchas otras cadenas de bloques PoS, no ejecuta una oferta inicial de tokens o lanzamiento aéreo como mecanismo de distribución de tokens. Aunque existe una «mina previa» inicial de 5 millones de PRV reservados para el desarrollo y el equipo, se espera que se creen 95 millones más como recompensas en el

bloque.

Esto genera un problema para la distribución, ya que un modelo de PoS puro simplemente haría que el equipo cuente con casi el 100% del suministro.

Para solucionar esto, Incognito empleó una solución innovadora en la que los apostadores pueden pedir prestados 1750 PRV (alrededor de 700 dólares), como su participación y obtener parte de las recompensas de ese préstamo. Actualmente, el replanteo solo se puede realizar en dispositivos de nodo dedicados, que simulan la adquisición de una plataforma minera.

Por lo tanto, el sistema está *«manipulado»* para funcionar como un sistema de Prueba de trabajo para la distribución inicial.

> *«El tema aquí es que cada nodo en la red tiene el mismo poder. Así que no hay forma de que pongas más fichas, y tienes más lotes de apuestas»,* explicó Bugaevski.

El proyecto también propone una solución innovadora para el problema del puente sin confianza en Bitcoin: custodios descentralizados. A diferencia de los sistemas de puente de custodia que se utilizan en la actualidad para Bitcoin tokenizado, el puente de Incognito usaría un sistema basado en incentivos económicos y reducción de garantías, similar a MakerDAO, para descentralizar completamente la custodia.