EBOOK

# Riesgos digitales en **Blockchain** y **Web3**

Descubra la tecnología disruptiva que podría dar lugar a una nueva Internet, y prepárese para prevenir fraudes y ataques.

**Jônadas Techio**
Arquitecto de Soluciones Blockchain
y Evangelista de Web3 en Axur

///AXUR

# Riesgos digitales en Blockchain y Web3


**Introducción** ..... 03

**¿Qué es Blockchain?** ..... 06

**Factores de riesgo y tipos de ataque** ..... 11

Vulnerabilidades de la tecnología ..... 11

Vulnerabilidades de implementación ..... 12

Ataques orientados al usuario ..... 13

**Ransomware** ..... 13

**Crypto-Malware** ..... 14

**Blind Signing** ..... 17

**Dusting** ..... 17

**Airdrops of tokens** ..... 17

**Rug Pulls** ..... 18

**Phishing** ..... 18

Spear phishing ..... 19

DNS Hijacking ..... 21

Phishing bots ..... 21

Fake browser extensions ..... 22

Ice Phishing ..... 23

**Conclusión** ..... 24

**Referencias y lecturas complementarias** ..... 25

**Refuerce su operación de ciberseguridad con la gestión de riesgos digitales de la plataforma Axur** ..... 26

**Sobre Axur** ..... 27


© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados 

# Introducción

El Blockchain ofrece un enfoque innovador para almacenar e intercambiar información y valor de forma segura, descentralizada y trustless[1]. Este enfoque se basa en una combinación de tecnologías que incluyen criptografía, algoritmos hash, mecanismos de consenso, sistemas informáticos distribuidos y contratos inteligentes, que a su vez se conectan con el mundo físico a través de las redes inteligentes y los dispositivos del Internet de las Cosas (IoT).

Las aplicaciones más conocidas de blockchain son, sin duda, las criptomonedas como Bitcoin y Ether (la moneda de la red Ethereum), seguidas por los servicios financieros descentralizados (DeFi) y, más recientemente, por las sobredimensionadas NFTs. Pero el potencial disruptivo de esta tecnología va mucho más allá de estos usos iniciales, dando paso a la aparición de toda una nueva generación de aplicaciones descentralizadas (dApps) que, junto con la infraestructura distribuida de blockchain, prometen servir de base para una nueva iteración de la propia internet: la llamada "Web3" o "internet del valor".

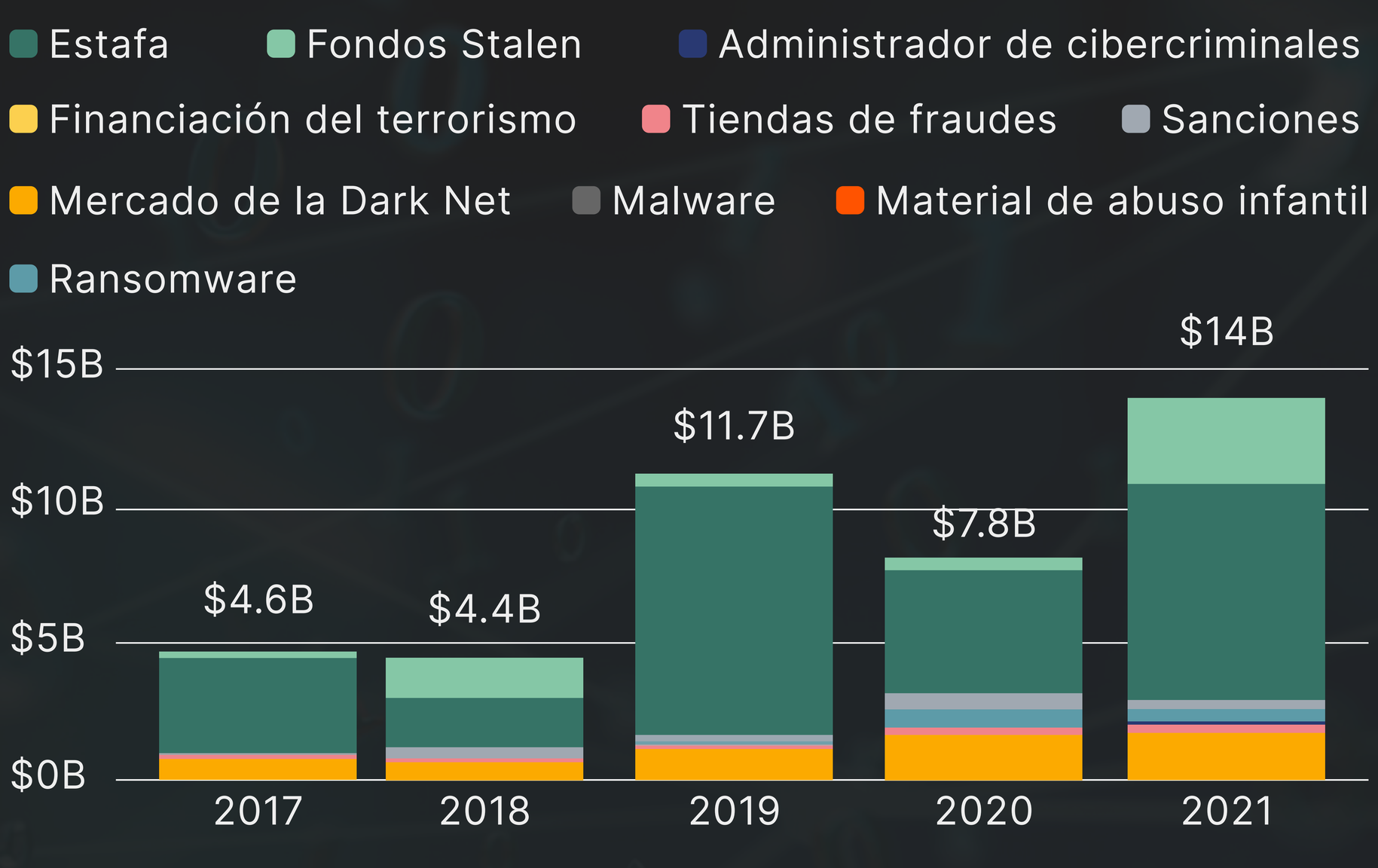
Aunque el blockchain ha sido objeto de interés creciente por parte del mundo académico de la industria e incluso de los medios de comunicación en general, aún queda mucho trabajo por hacer en cuanto a la educación del público sobre las mejores prácticas y la seguridad de las aplicaciones basadas en dicha tecnología; A medida que crece el uso y los montos de las transacciones que ocurren a través de dichas aplicaciones, el tema de la seguridad se vuelve cada vez más valioso.

Para hacernos una idea, según un reciente informe de la plataforma de datos Chainalysis, el volumen total de transacciones con las criptodivisas rastreadas por la empresa alcanzó los 15,8 billones de dólares en 2021 (un aumento del 567% respecto a los totales de 2020). Al mismo tiempo, el número de transacciones ilícitas con estas criptodivisas también alcanzó un máximo histórico en 2021, moviendo más de 14.000 millones de dólares a lo largo del año (frente a los 7.800 millones de 2020).

1 A lo largo de este ebook se ha hecho un esfuerzo por proporcionarle enlaces a recursos adicionales cada vez que se introduce una noción técnica o un tema específico, para dar un contexto más detallado a los datos y fuentes citados.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados.

**Valor total de criptodivisas recibido por direcciones ilícitas | 2017-2021**




Fuente: The Chainalysis 2022 Crypto Crime Report

Como se aprecia en el gráfico, las estafas son la mayor fuente de estas cantidades ilícitas. Chainalysis estima que los ingresos procedentes de las estafas aumentaron un 82% en 2021, alcanzando los 7.800 millones de dólares en criptodivisas robadas a las víctimas.

Con el intenso ritmo de desarrollo de esta industria, y con la creciente popularización de sus aplicaciones, es razonable esperar que se implementen continuamente nuevos y más sofisticados tipos de fraude y ataques. Por ejemplo, a principios de marzo de este año, el director general de Meta Platforms, Mark Zuckerberg, anunció que la empresa estaba "trabajando para llevar las NFT a Instagram a corto plazo". Con este anuncio, Instagram se une a las filas de otras grandes plataformas de contenidos (como YouTube y Spotify) que pretenden explorar esta aplicación de blockchain en sus servicios.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados. 

Al comentar este anuncio en una reciente entrevista con la revista FinTech, Steve Mitobe, director general y fundador de WestCoastNFT, dijo que es inevitable que esto atraiga a los malos actores, y con ellos más fraudes y estafas. En nuestra opinión, esto no hace más que reforzar la importancia y la necesidad de educar al público sobre la seguridad y las vulnerabilidades de blockchain, dado que, tarde o temprano, es probable que esta tecnología forme parte de la vida cotidiana de todos nosotros.

Esperamos que este e-book pueda contribuir a dicho objetivo, proporcionando información crucial para todo aquel que quiera entender, prevenir, mitigar e investigar los delitos y ataques basados en blockchain de forma más eficaz. Para ello, presentamos una visión global del tema de la seguridad de blockchain y Web3, estructurada de la siguiente manera:

Para facilitar la comprensión, comenzamos con una presentación introductoria de la tecnología blockchain, definiendo algunos de sus conceptos clave, sus aplicaciones más comunes, y explicando cuáles son las principales medidas que deben adoptarse para garantizar la seguridad del sistema.

A continuación, describimos los principales tipos de vulnerabilidades y ataques a los que están expuestos los usuarios de aplicaciones basadas en blockchain.

Luego, veremos de los riesgos que son intrínsecos a la tecnología, así como de los riesgos que provienen de los problemas de la implementación.

Por último, describiremos algunos de los principales ciberataques[2] orientados al usuario, como los basados en la ingeniería social, que son con diferencia los más extendidos y, por tanto, los más preocupantes en este espacio.

**Jônadas Techio**
Arquitecto de Soluciones Blockchain y Evangelista de Web3 en Axur

@Web3Axur

2 Dado que sería imposible abordar todos los tipos de ataques existentes (este documento, por ejemplo, enumera más de 200 variedades en el momento de su redacción, y se actualiza continuamente), hemos tenido que ser selectivos. Por ello, hemos optado por abordar sólo algunos de los casos más representativos.

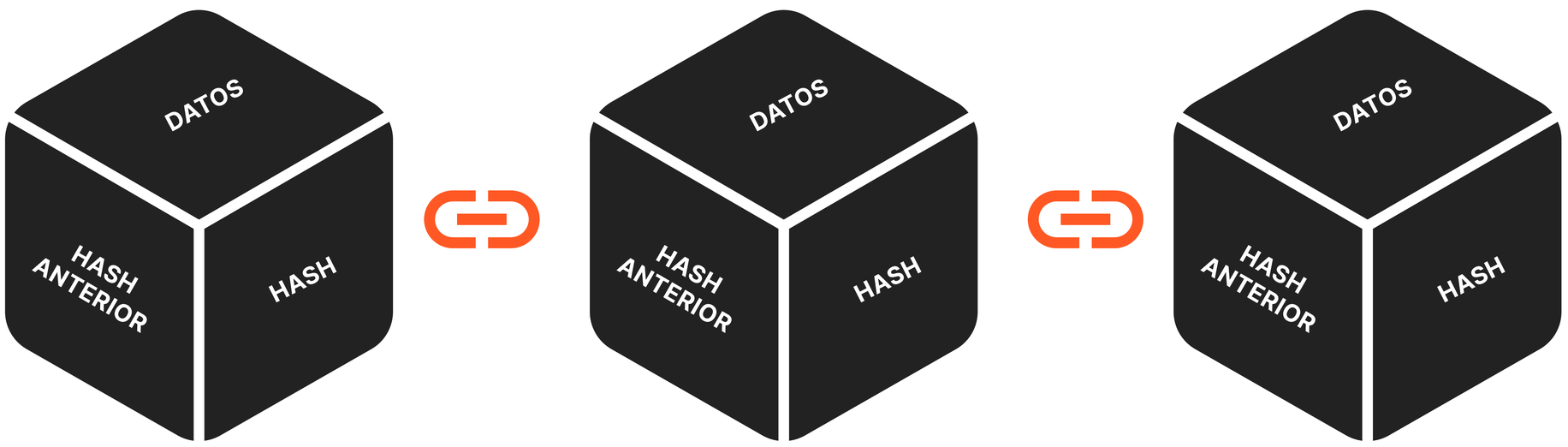
© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados. 

# ¿Qué es Blockchain?

En su sentido más general, "blockchain" se refiere a un conjunto de registros que se recolectan en bloques de información, que a su vez se concatenan en una serie o cadena (de ahí el nombre "blockchain").

En el caso de las blockchains públicas, que son el foco de interés exclusivo de este e-book, la cadena se copia y distribuye entre todos los pares de una red P2P descentralizada, y sirve como libro de contabilidad al que puede acceder cualquier persona en Internet.

Para que un registro se añada a un bloque, primero debe ser validado mediante un procedimiento criptográfico que hace uso de un par de claves (clave pública + clave privada) para firmar digitalmente los datos de la transacción, lo que permite al protocolo verificar que dicha transacción no ha sido manipulada y que fue efectivamente enviada por la persona o entidad que posee la clave privada a la clave pública proporcionada. Además de los registros de las transacciones y otra información relevante, cada bloque de la cadena contiene también un hash del contenido del bloque que le precede, que actúa como una especie de "huella digital" de ese contenido.



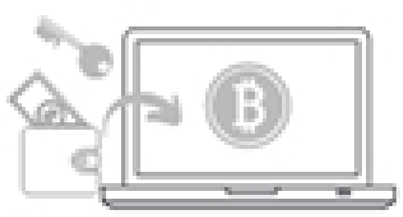

Fuente: Salesforce Ben

Para que cada nuevo bloque se cree y se añada a la cadena, el protocolo requiere un tipo de prueba adicional, que puede variar en función de la implementación del blockchain. Esta condición se denomina mecanismo de consenso, ya que en ella se basa el "acuerdo" (es decir, el consenso) entre los nodos de la red respecto al siguiente bloque que se añadirá a la cadena.

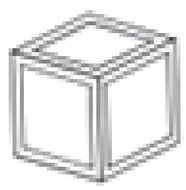
© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

El mecanismo de consenso más conocido es la prueba de trabajo, en la que determinados nodos, llamados mineros, compiten para resolver un rompecabezas matemático que requiere grandes cantidades de potencia de cálculo. Una vez que un minero ha resuelto el rompecabezas, recibe tokens como recompensa, mientras que esta información es transmitida y verificada por todos los demás nodos de la red. Sólo después de este proceso se añade el nuevo bloque a la cadena, cambiando así el estado de la blockchain.

## ¿Cómo llega una transacción al blockchain?



Una transacción se solicita y se autentifica

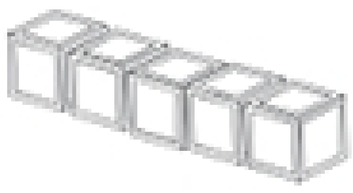


Se crea un bloque que representa esa transacción

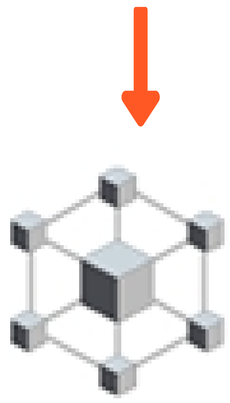
El bloque se envía a todos los nodos (es decir, participantes) de la red

El bloque se añade a la cadena de bloques existente

Los nodos reciben una recompensa por la prueba de trabajo, normalmente en criptomoneda



Los nodos validan la transacción



La actualización se distribuye por la red

La transacción se completa

Fuente: Euromoney Learning

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

Dado este intrincado mecanismo de creación y adición de bloques a la cadena de bloques (que combina la validación criptográfica, las funciones hash y un mecanismo de consenso), un ciberdelincuente no sólo tendría que manipular los datos de un bloque concreto para cambiar la información contenida en el libro de contabilidad, sino que también tendría que modificar todos los bloques posteriores; además, toda la nueva cadena de bloques creada tendría que ser distribuida y validada por más de la mitad de los nodos de la red. Y para llevar a cabo este proceso, se necesitaría una cantidad absurda de recursos informáticos.

**Por este motivo, la manipulación de los datos ya incluidos en la cadena resulta prácticamente imposible** (aunque, como veremos más adelante, es teóricamente posible). Por ello, el blockchain se convierte en una base de datos muy segura, sobre todo si se compara con otros tipos de bases de datos disponibles en la actualidad.

Esta base tecnológica permite diferentes tipos de implementaciones. La más conocida de estas implementaciones, como decíamos, son las criptomonedas, que son representaciones digitales de valor que pueden ser utilizadas en transacciones por los participantes de la red. Dado que este es probablemente el uso más relevante de la blockchain para la mayoría de la gente, a continuación describiremos con más detalle los diferentes elementos que intervienen en una transacción de criptodivisas, así como sus respectivas funciones y algunas de las principales vulnerabilidades asociadas a ellas.

**Dirección:** una cadena de caracteres única que, de forma análoga a un código postal o una dirección de correo electrónico, sirve para representar la ubicación de tu wallet en la cadena de bloques, lo que te permite recibir y enviar criptomonedas y otros tipos de activos digitales.

**Clave Pública y Clave Privada:** su dirección es una forma abreviada de tu clave pública; ésta, a su vez, está siempre emparejada con una clave privada. Cualquiera puede enviar transacciones a su clave pública, pero usted necesita su clave privada para desbloquear los activos recibidos; la clave privada también sirve para "firmar" sus transacciones y demostrar que los activos vinculados a su dirección pública le pertenecen realmente.

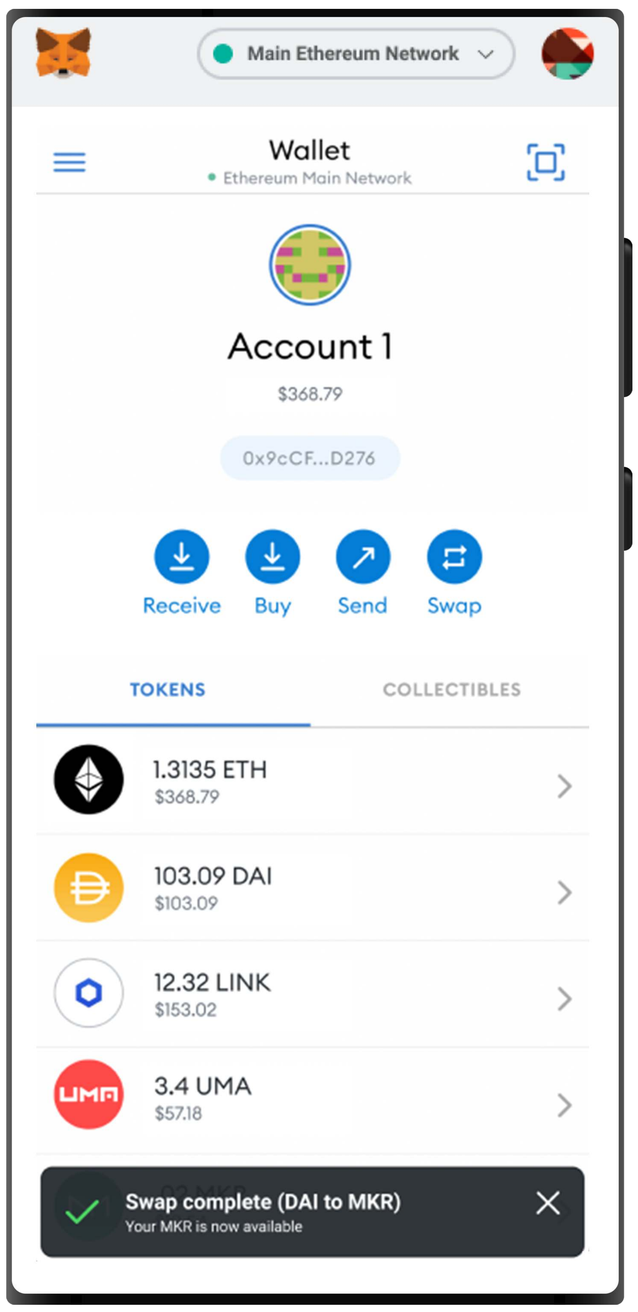
**Frase Semilla:** una serie de palabras vinculadas a su clave privada que tiene una función mnemotécnica, y que puede utilizarse para volver a acceder a una wallet. Su frase semilla debe guardarse "bajo llave", porque si alguien consigue acceder a ella puede robar todos los activos vinculados a su wallet.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

**Hot Wallet:** también llamada "software wallet", es una aplicación de almacenamiento de claves privadas a la que puedes acceder en tu ordenador o en tu teléfono, y que está conectada a Internet. Uno de los software wallet más comunes es MetaMask. Debido a la conexión a Internet, estas wallets son menos seguras contra los ataques que las "Cold Wallet".

**Cold Wallet:** también llamada "hardware wallet", es un dispositivo físico, similar a una unidad USB, que almacena claves privadas fuera de línea. Entre las hardware wallet más populares están los de los fabricantes Ledger y Trezor.

“cold” wallet Nano Ledger S




“hot” wallet MetaMask

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

El principal objetivo de un ciberdelincuente es robar su frase semilla o la clave privada asociada a su criptobilletera. Con esta información a mano, puede entrar con sus credenciales y transferir todos sus criptoactivos a otra(s) cartera(s) que tenga. Una vez que esto sucede, no hay absolutamente ninguna manera de recuperar sus activos. Por eso es vital que usted mantenga su frase semilla y su clave privada seguras, y que no las compartas con nadie.

Además de los registros de transacciones de criptomonedas y otros criptoactivos, es posible añadir otro tipo de información a los bloques del blockchain. Por otra parte, desde la implantación de Bitcoin, el blockchain también es programable, lo que permite crear funciones que pueden ejecutar automáticamente las transacciones según reglas y condiciones previamente establecidas; esta es la función de los llamados "contratos inteligentes."

Con la aparición de blockchains de segunda generación, como Ethereum, la capacidad de ejecutar código ha evolucionado, permitiendo la aparición de contratos inteligentes más complejos y sofisticados. Esto abre la posibilidad de muchos usos adicionales para el blockchain. Por citar algunos ejemplos, ya existen aplicaciones de blockchain para:

Registro de la propiedad intelectual

Intercambio seguro de datos médicos

Seguimiento de la logística y la cadena de suministro

Identidad personal

Mecanismos de votación

Creación de dominios descentralizados

Financiación inmobiliaria

Muchas más posibilidades

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

# Factores de riesgo y tipos de ataque

## Vulnerabilidades de la tecnología

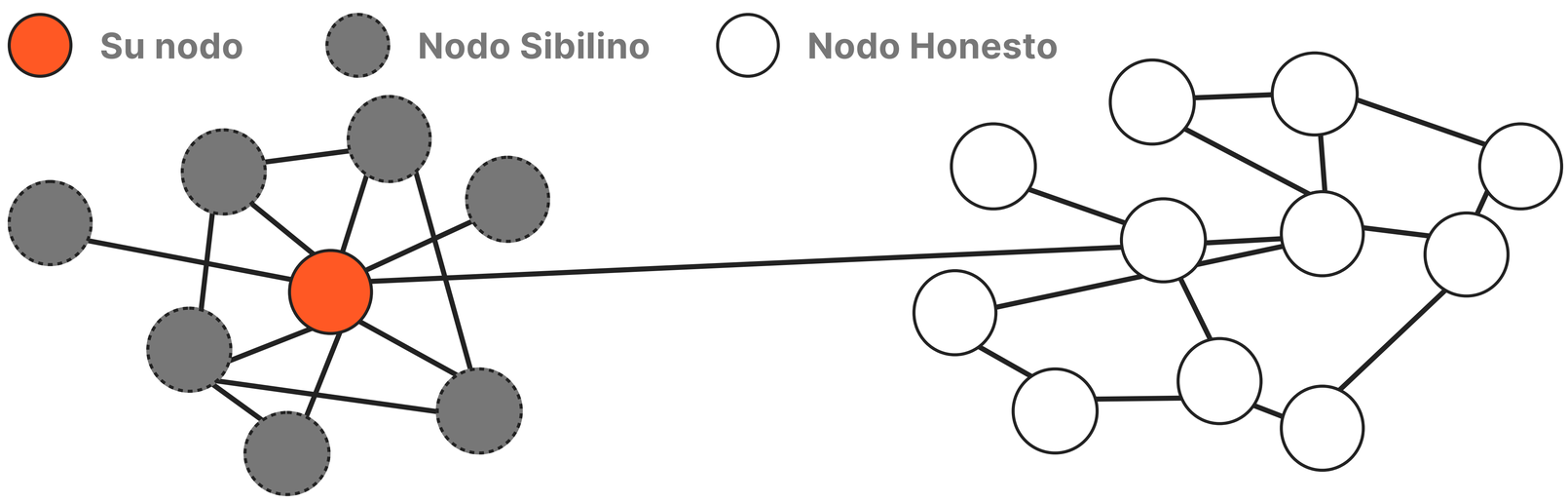
Como hemos visto, la seguridad de un blockchain depende de ciertas suposiciones relacionadas con sus elementos tecnológicos, y si estas suposiciones no se cumplen, pueden surgir vulnerabilidades y riesgos.

Uno de estos riesgos se produce cuando el procesamiento de la red en su conjunto no está suficientemente distribuido, en concreto, cuando una entidad o grupo es capaz de procesar más del 50% de la producción del blockchain. Esto abriría la posibilidad de un ataque mayoritario (también llamado "ataque del 51%"), en el que dicha entidad o grupo podría producir bloques de forma arbitraria y, en última instancia, crear su propia cadena, lo que a su vez facilitaría la ejecución de otro tipo de ataques (por ejemplo, un ataque de doble gasto, en el que un token se gasta más de una vez).

La probabilidad de que se produzca un ataque mayoritario en blockchains que tienen un gran número de nodos (como las redes Bitcoin y Ethereum, por ejemplo) es muy baja, pero los perpetradores han sido capaces de implementarlos en redes más pequeñas (como los blockchains Shift y Krypton).

Otro supuesto importante para el funcionamiento de un blockchain es que la mayoría de sus nodos de minería sean "honestos"; es decir, que trabajen para reforzar la seguridad de la red, no para socavarla. Pero si esta suposición no se cumple, surge la posibilidad de un ataque Sybil. En ese caso, una entidad o grupo sería capaz de crear múltiples nodos "deshonestos" que, a su vez, enviarían información falsa a otros participantes.

**Nodos Sibilinos que intentan influir en el flujo de información de una red**




fuente: Coincentral

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

Los ataques de denegación de servicio distribuidos (DDoS) también son posibles, aunque son difíciles de ejecutar en un blockchain. (Los pocos casos reales que conocemos tenían como objetivo específico las plataformas de intercambio de divisas). En este tipo de ataque, los ciberdelincuentes buscan hacer caer un servidor consumiendo todos sus recursos de procesamiento con numerosas peticiones. Los atacantes DDoS pueden intentar de este modo desconectar los pools de minería, las wallets, los intercambios y otros servicios financieros de una red. Una blockchain también puede ser hackeada con DDoS en su capa de aplicación utilizando botnets DDoS.

# Vulnerabilidades de implementación

Incluso si se cumplen todas las condiciones tecnológicas para la seguridad del blockchain, una implementación inadecuada abre otras oportunidades de ataque.

Los ciberdelincuentes suelen aprovechar los problemas relacionados con el software tradicional y las aplicaciones web que se utilizan para proporcionar acceso al blockchain. Un objetivo principal de estos ataques son las wallets, que, como hemos visto, no son más que aplicaciones que almacenan las direcciones, la información de pago y las claves de los usuarios, y que pueden utilizarse para firmar transacciones y autorizar pagos en otros sitios web y aplicaciones.

Como recordará, las wallets utilizan pares de claves criptográficas, y sus direcciones se generan a partir de las claves públicas del usuario. Algunas implementaciones, sin embargo, truncan la clave pública para derivar la dirección de la wallet, y esto puede crear un problema. Si una dirección no está vinculada a un par de claves específico, es posible aplicar la fuerza bruta para encontrar otro par de claves que pueda controlar dicha wallet, y esto puede hacerse en un tiempo razonable, dependiendo del tamaño de la dirección.

En relación con esto, también es posible aplicar ataques de diccionario, en los que un ciberdelincuente intenta descifrar el hash y la sal criptográfica de la víctima utilizando valores hash de contraseñas comunes (como "contraseña" o "123456"). Al traducir las contraseñas de texto plano en hashes criptográficos, los atacantes pueden encontrar credenciales para acceder a una wallet.

Las wallets también pueden ser "robadas": en concreto, los ciberdelincuentes ya han conseguido cambiar la dirección de las wallets alojadas por los mineros conectados a Internet, haciendo que las recompensas recibidas por ellos se envíen a una dirección diferente controlada por el delincuente.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

Otro supuesto para el funcionamiento de un blockchain se refiere a la seguridad de sus algoritmos de cifrado. Por lo tanto, cabe señalar en este contexto que el riesgo teórico lo suponen los futuros desarrollos de la computación cuántica. Según algunas estimaciones, en el 2035 debería existir un ordenador cuántico capaz de romper al menos algunos de los protocolos criptográficos que funcionan hoy en día, lo que podría hacer que muchas de las subrutinas esenciales de los blockchain, incluido el sistema de seguridad de las wallets, no funcionaran.

Además de las wallets, algunos fallos en la implementación de los contratos inteligentes también pueden exponer a los usuarios a ataques. Recuerde que un contrato inteligente es un tipo de código que permite verificar y ejecutar transacciones de forma automática. Estos contratos se ejecutan en el blockchain de forma transparente, y sin requerir la intervención humana previa para verificar y hacer cumplir las condiciones establecidas en el código. Una vez implementados, los contratos inteligentes son básicamente inmutables. Estos atributos, fundamentales para su funcionamiento, también los convierten en un riesgo para la seguridad y en un objetivo de gran interés para los ciberdelincuentes.

# Ataques orientados al usuario

El principal foco de vulnerabilidad de las aplicaciones de blockchain no es la tecnología que la sustenta ni su implementación, sino su usuario. Los usuarios suelen descuidar las mejores prácticas de seguridad, y lo mismo ocurre con algunas empresas que ofrecen servicios basados en blockchain.

Los ciberdelincuentes aprovechan esta oportunidad para dirigirse a los consumidores y a las empresas aplicando métodos bien conocidos dirigidos a los usuarios finales, en particular métodos de ingeniería social, que se aprovechan principalmente de la credulidad y la falta de atención del ser humano. A continuación, describiremos algunos casos representativos de esta categoría de ataques.

## Ransomware

Como una de las herramientas más utilizadas por los ciberdelincuentes para adquirir criptomonedas de forma ilícita de personas u organizaciones, el ataque de ransomware cifra los datos de la víctima hasta que se realiza un pago al atacante. Si no se realiza el pago, los atacantes pueden vender la información del usuario en la Deep Web como una forma alternativa de ingresos. El ransomware es también una de las tácticas más lucrativas para los ciberdelincuentes, con un coste global estimado de más de 692 millones de dólares en 2020.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

El ransomware GandCrab (añadido al popular kit de exploits RIG) fue ampliamente utilizado en ataques lanzados contra los difuntos Microsoft Internet Explorer y Adobe Flash Player. A través de sitios web y anuncios maliciosos (o "malvertising"), el ramsomware encriptó archivos utilizando un algoritmo RSA y exigió el pago en "altcoins" menos volátiles y menos conocidos que Bitcoin, como Dash. A partir de 2018, nuevos ramsomware como HC7 Planetary adoptaron Ethereum como método de pago (además de aceptar Bitcoin y Monero).

Un caso más reciente y notorio ocurrió el 7 de mayo de 2021, cuando Colonial Pipeline -una empresa de oleoductos que suministra energía al sureste de Estados Unidos- fue víctima de un ataque de ransomware que la obligó a detener temporalmente sus operaciones hasta que pagara el rescate requerido de 75 Bitcoins (con un valor aproximado de 4,4 millones de dólares en ese momento) a DarkSide, el grupo cibercriminal ruso responsable del ataque. Seis días después, Colonial pudo reanudar sus operaciones, pero el cierre, junto con el aumento de la demanda debido al pánico de los consumidores, provocó escasez de combustible en varias zonas durante ese tiempo.

# Crypto-Malware

Los ataques de malware contra criptomonedas -también llamados cryptojacking- son cada vez más populares. Según Tech Monitor, este tipo de ataque ha crecido un 300% en el último año, lo que ha enriquecido a los delincuentes y ha puesto en alerta a las redes indefensas. A diferencia del malware tradicional, el cripto-malware no pretende robar datos, sino que se aprovecha del dispositivo de la víctima para minar criptomonedas de forma continua y discreta durante el mayor tiempo posible.

A menudo el malware se disfraza de software legítimo que, una vez descargado, incorpora código malicioso en varias aplicaciones y programas. Este código se ejecutará en segundo plano para minar criptomonedas cada vez que la víctima utilice su dispositivo. De este modo, los atacantes pueden recibir un rendimiento constante mientras el código no sea detectado.

Un método avanzado de infección es a través de un anuncio o un sitio web comprometido. Cuando el usuario visita el sitio infectado, se ejecuta automáticamente un script en el dispositivo de la víctima. Esta forma de ataque es difícil de detectar porque el código malicioso no se almacena en el propio ordenador, sino en el navegador.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

A finales de 2017 se descubrió que el complemento Archive Poster para el navegador Chrome estaba minando monedas Monero sin el consentimiento de los usuarios. Algunas víctimas se dieron cuenta del problema cuando notaron un alto uso de la CPU, pero para entonces más de 100.000 personas habían descargado el minero. Al menos cuatro versiones de la aplicación incluían el código JavaScript de Coinhive, que permite incorporar fácilmente el minado a sitios o herramientas web, originalmente a través de una API de código abierto y fácil de usar.

En 2018, un fallo en YouTube permitió a los anunciantes maliciosos inyectar código de malware en los anuncios de la plataforma para minar Bitcoin o Ethereum. (YouTube retiró rápidamente a los anunciantes de la red y bloqueó los anuncios de minería). Se sabe que hay más de 30.000 sitios que alojan código de Coinhive para minar -con o sin consentimiento-. Este cálculo incluye sólo los sitios no ofuscados, pero el número real es probablemente mucho mayor.

Además de Coinhive, otros ejemplos importantes de cripto-malware son:

**WannaMine v4.0:** Este malware utiliza el exploit EternalBlue para comprometer hosts almacenando binarios en un directorio C:\Windows llamado "NetworkDistribution".

**BadShell:** Un malware que no implica la descarga de archivos, sino que utiliza procesos nativos de Windows como PowerShell, el Programador de Tareas y el Registro, lo que lo hace especialmente difícil de detectar;

**PowerGhost:** Al igual que BadShell, este script sin archivos utiliza herramientas nativas de Windows para infectar ordenadores  y servidores de redes corporativas.

**Graboid:** un gusano que se propaga utilizando contenedores Docker Engine (Community Edition)

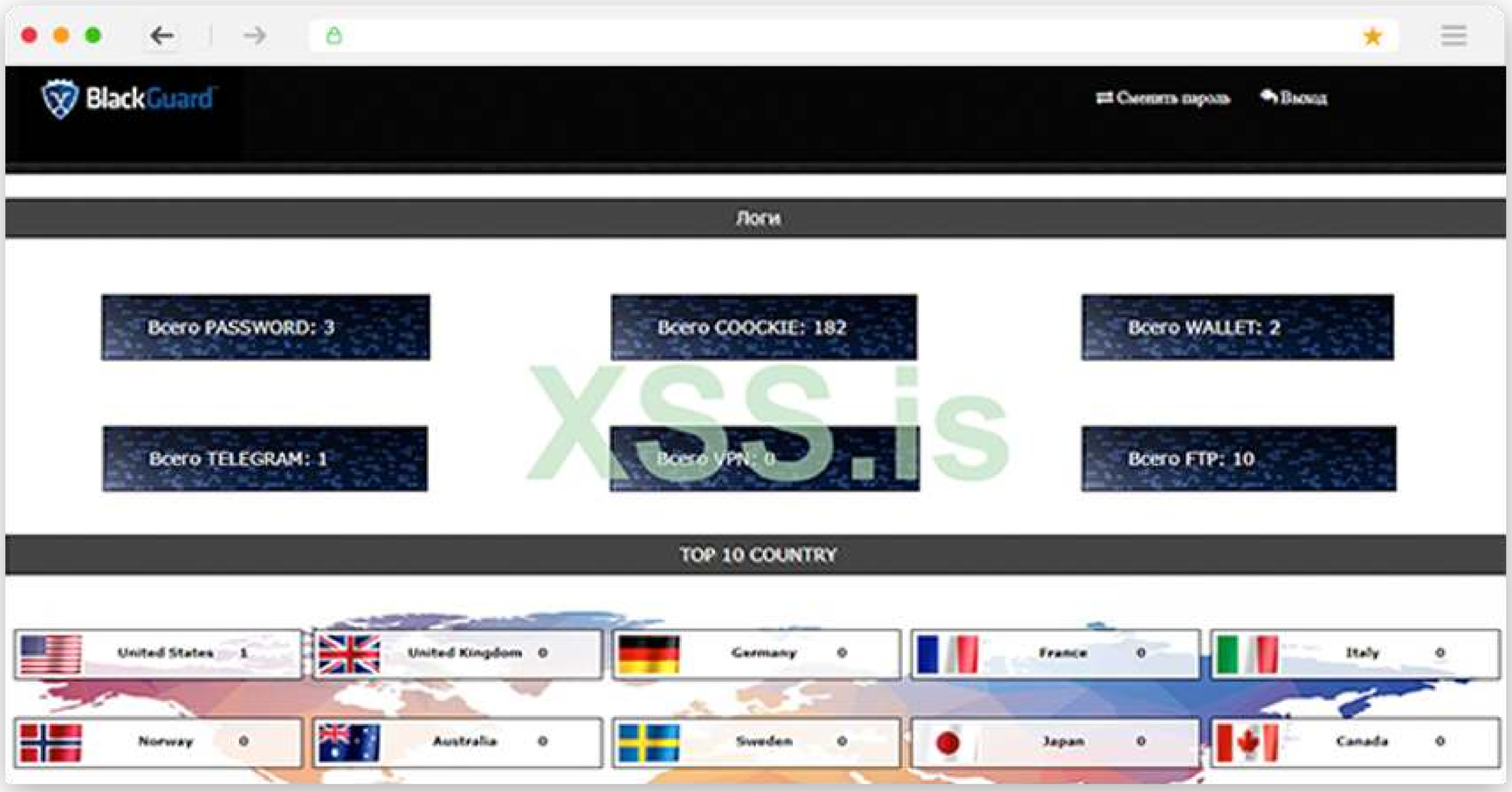
**Facexworm:** Mediante ingeniería social, este malware atrae a los usuarios de Facebook Messenger para que hagan clic en un enlace falso de YouTube, que pide al usuario que descargue una extensión de Chrome para ver el contenido, pero acaba secuestrando las cuentas de las víctimas para difundir el enlace a las redes de sus amigos.

**Black-T:** Ataca a clientes de AWS que utilizan las daemon APIs de Docker que están expuestas.

Un caso más reciente de cripto-malware que está llamando la atención de la comunidad de ciberdelincuentes es BlackGuard. El malware se está vendiendo en varios mercados y foros de la Dark Web por un precio vitalicio de $700 dólares o una suscripción mensual de $200 dólares.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

Una vez instalado, el software puede capturar información sensible de una amplia variedad de aplicaciones, empaquetarla toda en un archivo ZIP y enviarla al C2 de la operación de malware como servicio (MaaS). Los ciberdelincuentes que han adquirido la suscripción pueden entonces acceder al panel web de BlackGuard para recuperar los registros de datos robados, explotándolos o vendiéndolos a otros.




Captura de pantalla del panel de control de BlackGuard - Fuente: Zscaler

Según una investigación del proveedor de ciberseguridad Darktrace, además de los ataques individuales, el cripto-malware se distribuye cada vez más a través de botnets, lo que permite a los delincuentes aprovechar la capacidad de procesamiento de cientos o incluso miles de máquinas. Estas redes de bots suelen dirigirse a las vulnerabilidades de los sistemas orientados a Internet, como los servidores web, las pasarelas VPN o las plataformas de entrega de aplicaciones en la nube. La red de bots de minería Lemon Duck, por ejemplo, compromete objetivos a través de un grupo de vulnerabilidades en Microsoft Exchange Server llamado ProxyLogon. Darktrace predice un aumento de este tipo de ataques, especialmente después de la represión de las granjas de minería de bitcoins en China.

**Con la creación continua de nuevas variantes de cripto-malware, es probable que veamos un aumento aún mayor de estos ataques en un futuro próximo.**

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

# Blind Signing (Firma ciega)

Con la explosión del uso de las criptomonedas y la creciente popularidad de las dApps, las finanzas descentralizadas (DeFi) y las NFT, los usuarios interactúan con los contratos inteligentes de forma cada vez más compleja. Y los estafadores siempre están al acecho de nuevas vulnerabilidades. La firma ciega es un tipo de ataque reciente y aún poco conocido que los ciberdelincuentes utilizan para robar criptoactivos. Este ataque se aprovecha del hecho de que los usuarios que emplean sus wallets para interactuar con dApps y NFTs a menudo no revisan el código completo de los contratos inteligentes subyacentes a estas aplicaciones, y por lo tanto terminan firmando y autorizando transacciones sin saber exactamente lo que están firmando y autorizando.

# Dusting

Esta es otra forma relativamente nueva de actividad maliciosa en la que los hackers y estafadores envían cantidades muy pequeñas de criptodivisas (comúnmente denominadas "polvo") a las wallets con la intención de romper su privacidad. Los monederos son entonces rastreados por los delincuentes que, mediante un cuidadoso análisis de su historial de transacciones y de las direcciones utilizadas, son capaces de desanonimizar a la persona o empresa que está detrás de ellos. Estas personas o entidades, una vez conocidas, pueden convertirse en objetivo de otras estafas, como ataques de phishing, extorsión o incluso secuestro de familiares a cambio de un rescate en criptodivisas.

# Airdrops of tokens (Lanzamiento de fichas)

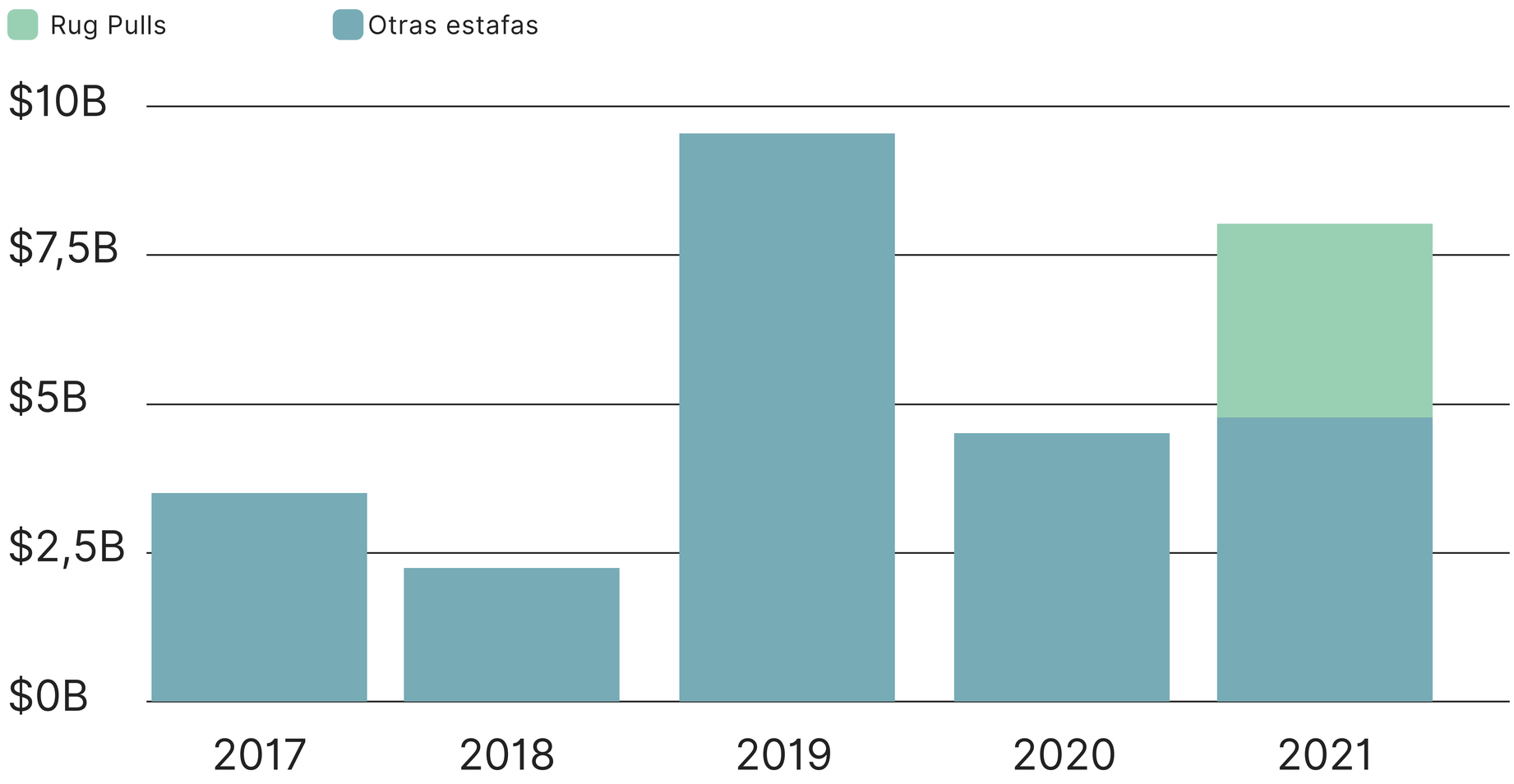
Otra técnica reciente que todavía es poco comprendida por mucha gente es la oferta de tokens maliciosos. Como las direcciones de las wallets son públicas, literalmente cualquiera puede enviar tokens o NFTs a estas direcciones. Normalmente esto no es un gran problema, porque simplemente puedes elegir ignorarlos; pero algunos ciberdelincuentes han desarrollado formas de enviar tokens que pueden ejecutar transacciones en tu cuenta tan pronto como interactúes con ellos. En este sentido, se podrían comparar estos tokens con un troyano que permite a los hackers acceder a tu ordenador en cuanto interactúas con un archivo malicioso. Pero al igual que no puedes evitar que un troyano llegue a tu correo electrónico, tampoco puedes evitar recibir estos tokens maliciosos, simplemente no necesitas interactuar con ellos. Puede encontrar un análisis más detallado de este tipo de estafa, en este vídeo explicativo.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

# Rug Pulls (Tiradores de alfombra)

Más de $2.800 millones de dólares han sido desviados con ataques rug-pull, una estafa relativamente nueva en la que los desarrolladores construyen lo que parecen ser proyectos legítimos de criptodivisas antes de tomar el dinero de los inversores y desaparecer. Según este informe de Chainalysis, los rug pulls ya se han convertido en el principal tipo de estafa aplicada en el ecosistema DeFi, representando el 37% de todos los ingresos por estafa relacionados con las criptodivisas en 2021 (frente a solo el 1% en 2020). Como dijimos al principio en total, los rug pulls han recaudado más de $2.800 millones de dólares en criptodivisas de las víctimas en 2021.

**Valor total anual de criptodivisas recibidas por los estafadores | 2017-2021**




Fuente: Chainalysis

# Phishing

Las estafas de Phishing son los ataques de blockchain más conocidos debido a su prevalencia y tasa de éxito. En este tipo de ataque, un ciberdelincuente intenta obtener fraudulentamente información sensible haciéndose pasar por una entidad de confianza en una comunicación electrónica (por ejemplo, correo electrónico, redes sociales y aplicaciones de mensajería instantánea).

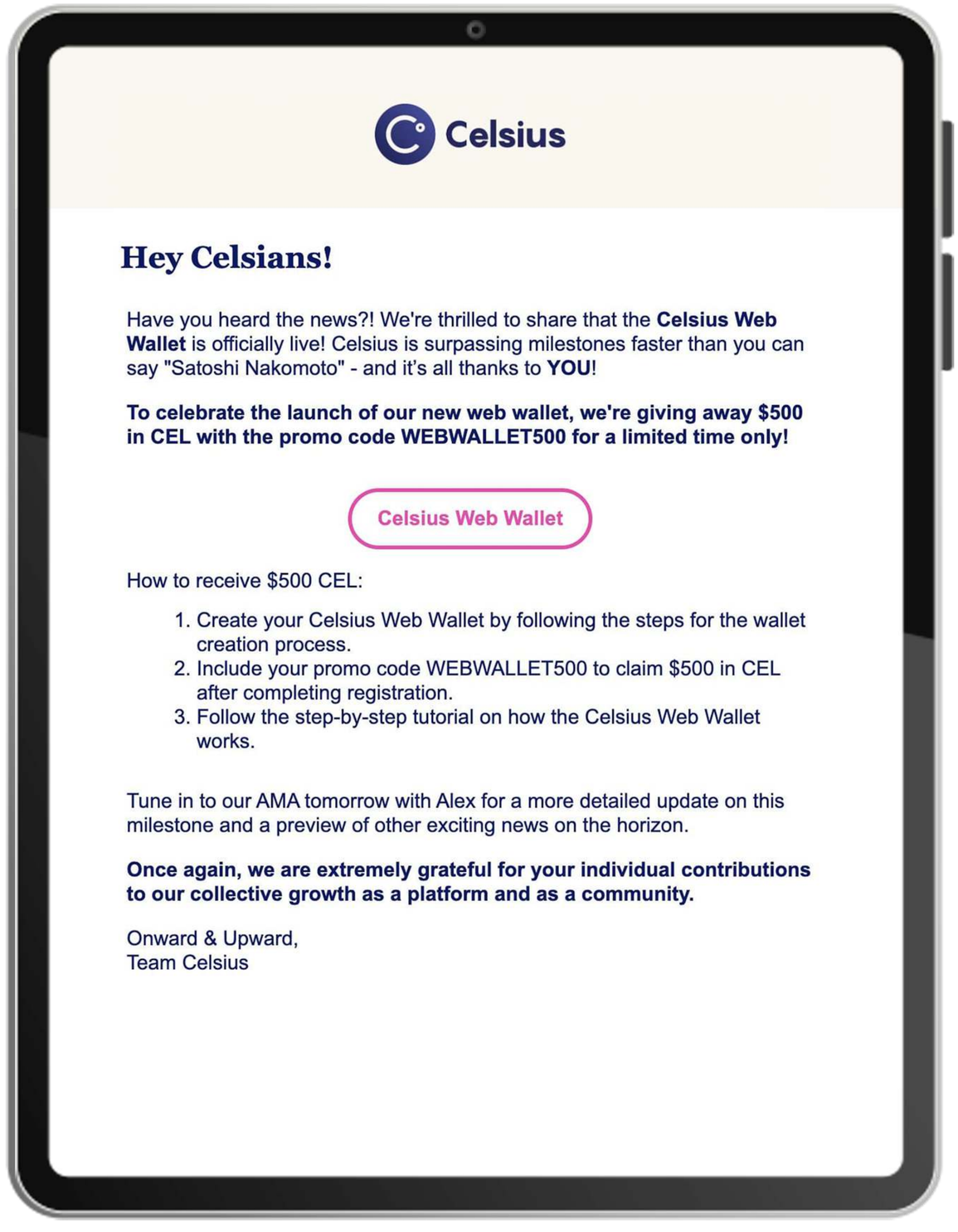
Muchos proyectos de blockchain que cuentan con sólidas políticas de seguridad en lo que respecta a su tecnología e implementación han demostrado ser vulnerables a los ataques de phishing, provocando pérdidas millonarias a los miembros de sus comunidades y a los inversores. El tipo y el propósito de estos ataques pueden variar mucho, pero los siguientes se encuentran entre los más comunes.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

## Spear phishing

Este tipo de ataque se produce cuando un atacante se dirige a personas concretas con mensajes personalizados -por ejemplo, un correo electrónico falso que parece proceder de un remitente de confianza- con el objetivo de obtener información sensible o inducir a esas personas a visitar sitios web que contienen malware.

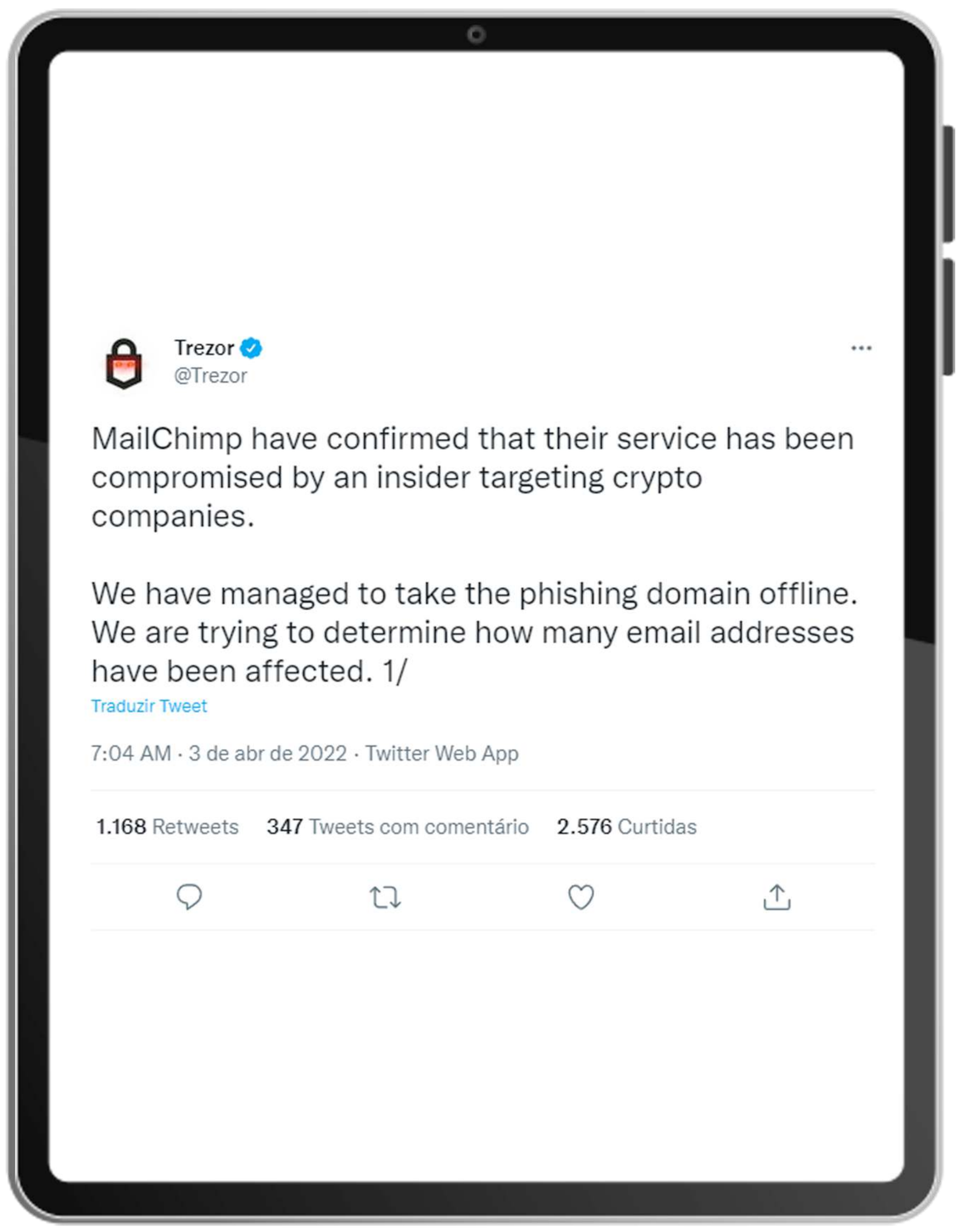
En lo que respecta al blockchain, los casos más comunes se desencadenan a través de correos electrónicos y mensajes directos en redes sociales enviados por cuentas fraudulentas que se hacen pasar por proveedores de wallets digitales o por bolsas de criptomonedas, con el objetivo de inducir a los destinatarios a "actualizar" su frase de semilla o cambiar su contraseña, lo que permite al ciberdelincuente robar sus credenciales de acceso y vaciar sus carteras. Otra táctica es atraer a los usuarios con "promociones", como fue el caso del ataque a los usuarios de Celsius Network a principios de 2021.




Fuente: Twitter

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

Hace apenas unos días, se produjo un ataque de spear phishing más complejo, que implicaba dos pasos: En primer lugar, los ciberdelincuentes hackearon MailChimp, la conocida empresa de marketing por correo electrónico, infiltrándose en sus sistemas y robando información de más de 100 usuarios; después, los delincuentes reutilizaron los datos robados para hacer spear phishing a los usuarios del popular hardware wallet Trezor, enviando correos electrónicos dirigidos en los que les decían que Trezor había sufrido un "incidente de seguridad" y que si estaban recibiendo el correo electrónico debían descargarse una versión actualizada de la app, que resultó ser un clon malicioso que pedía a los usuarios sus frases semilla.




Fuente: Twitter

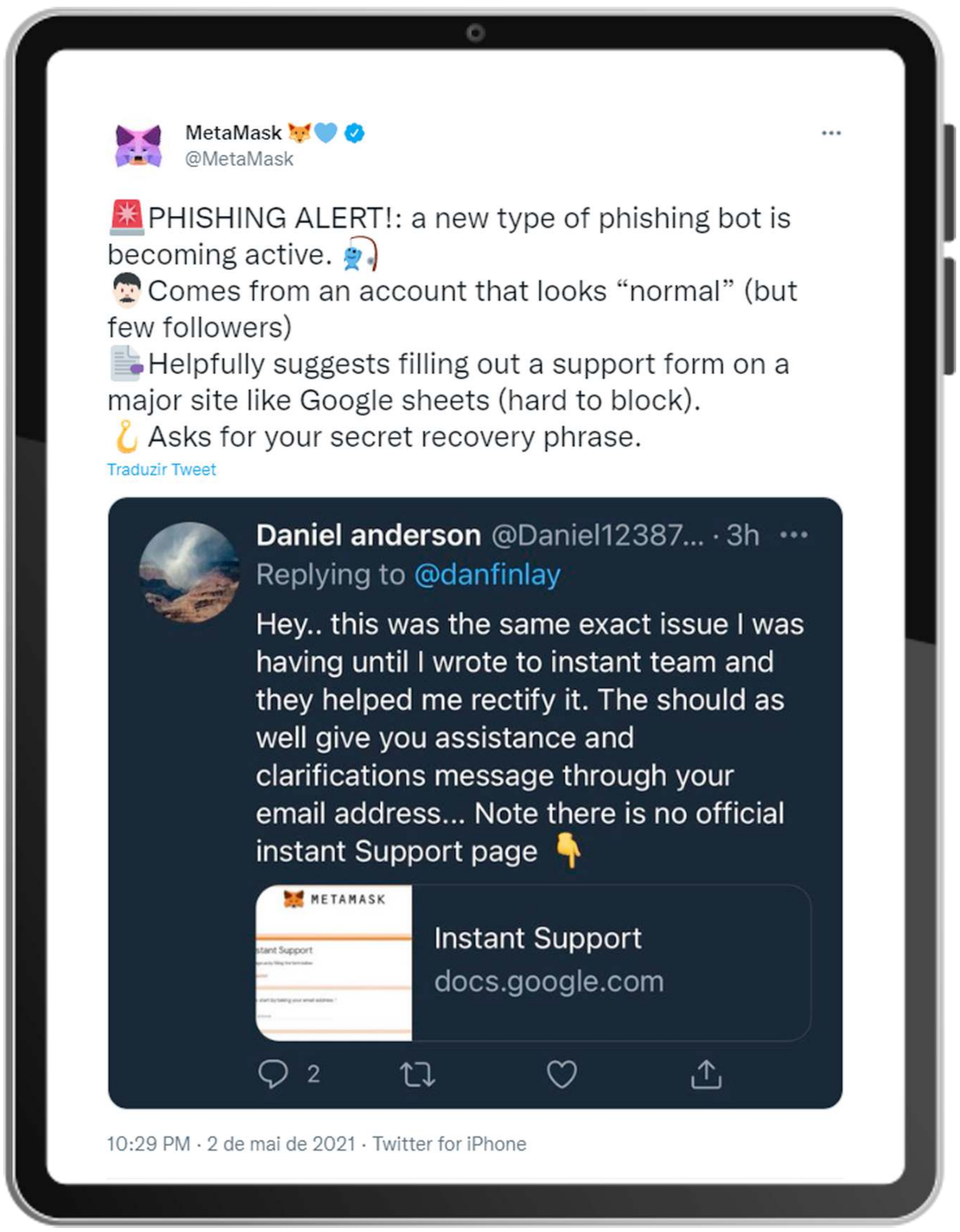
© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

## DNS Hijacking

Algunos esquemas de phishing son más sofisticados. Tal es el caso de los ataques de suplantación de DNS, en los que los ciberdelincuentes secuestran sitios web legítimos y los sustituyen por una interfaz maliciosa, engañando a los usuarios para que introduzcan sus claves privadas en el dominio fraudulento. En 2018, por ejemplo, los atacantes secuestraron las DNS de una aplicación de monedero de Stellar Lumen llamada BlackWallet. A principios de 2021, dos grandes proyectos DeFi construidos en la cadena inteligente Binance -PancakeSwap y Cream Finance- fueron víctimas de un ataque de este tipo.

## Phishing bots

En este tipo de ataque, se utiliza un ejército de bots para robar frases semilla que, a su vez, permiten al ciberdelincuente recuperar una wallet de criptomonedas. Como en los casos anteriores, la solicitud suele llegar al usuario a través de una cuenta falsa en una red social, sugiriendo que se rellene un formulario (por ejemplo, utilizando Google Sheets). En mayo de 2021, la cartera digital MetaMask llamó la atención de sus usuarios sobre un ataque de este tipo originado en Twitter.

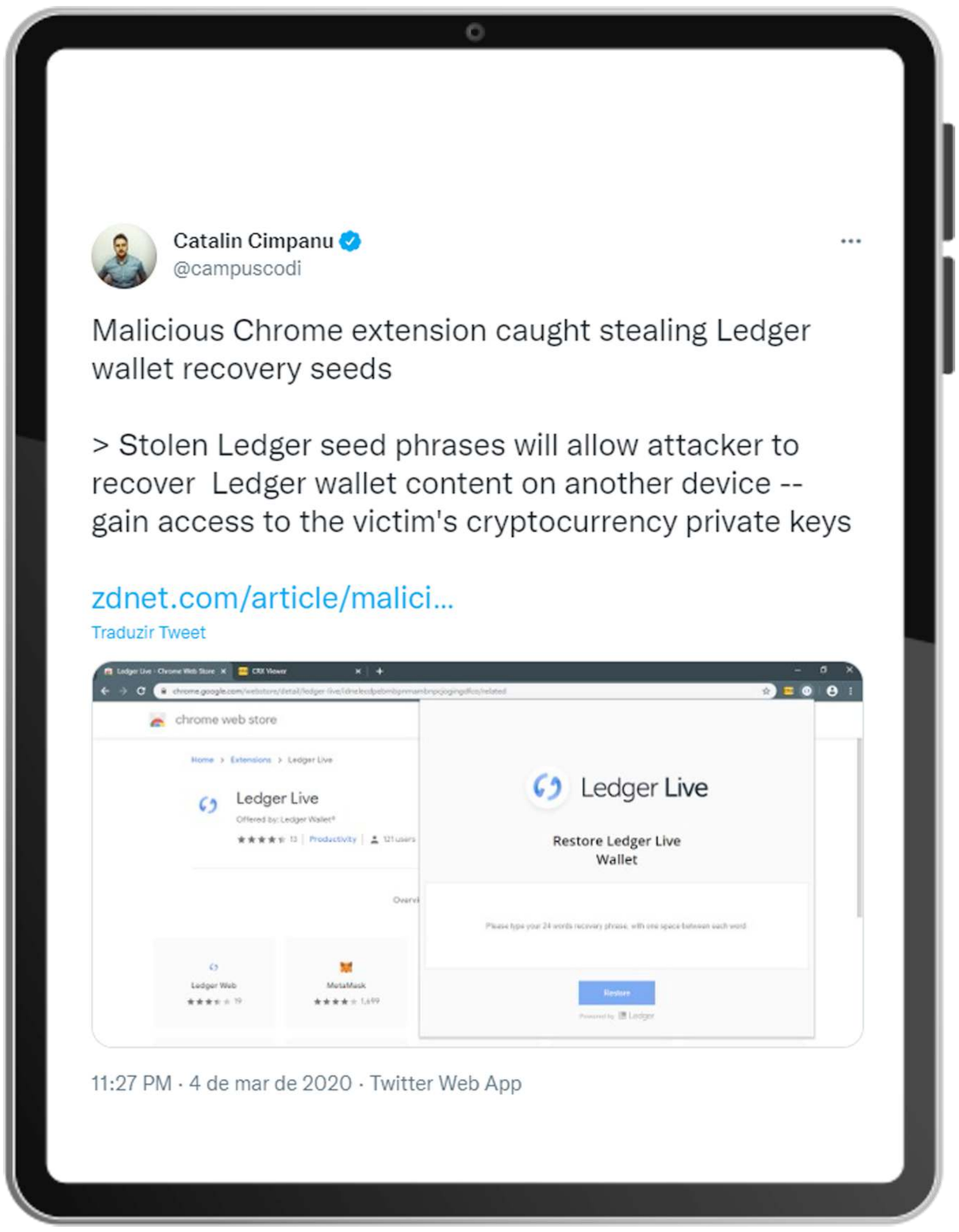



Fuente: Twitter

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

## Fake browser extensions

En el mundo de las criptomonedas y la Web3, el uso de algunas extensiones de navegador (como la mencionada MetaMask) es muy común, lo que da cabida a que los ciberdelincuentes se aprovechen de la situación creando extensiones falsas que les permitan robar fondos y criptoactivos a los usuarios. En 2020, una extensión maliciosa de Chrome llamada Ledger Live fue descargada más de 120 veces antes de ser retirada de la Chrome Web Store. En ese caso, los atacantes incluso utilizaron el propio servicio de publicidad de Google (Google Ads) para promocionar el producto y ganar un aire de legitimidad.




Fuente: Twitter

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

## Ice Phishing

La técnica del "ice phishing" es más nueva y compleja, y se analiza en detalle en este post del equipo de investigación de Microsoft 365 Defender. A diferencia de los anteriores, este tipo de ataque no implica el robo de frases semilla o claves privadas. En su lugar, la táctica consiste en engañar a un usuario para que firme una transacción que delegue la aprobación de sus tokens al atacante. (Este es un tipo de transacción común que permite interactuar con los contratos inteligentes DeFi que, a su vez, son capaces de interactuar con los tokens del usuario, por ejemplo, para intercambiar entre diferentes tipos de tokens). Estos ataques pueden ser bastante eficaces porque la interfaz de usuario no muestra toda la información pertinente que puede indicar que una transacción ha sido manipulada. Una vez firmada, enviada y minada la transacción que delega la aprobación del token, el ciberdelincuente puede acceder a los fondos del usuario. En algunos casos, el atacante puede acumular aprobaciones durante un período de tiempo y luego vaciar rápidamente las wallets de todas las víctimas. Esto es exactamente lo que ocurrió con el ataque de Badger DAO, que permitió al atacante drenar millones de dólares entre noviembre y diciembre de 2021.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

# Conclusion

No cabe duda de que blockchain es una de las tecnologías emergentes más disruptivas, especialmente en los ámbitos de las tecnologías de la información y las finanzas. Existen numerosas aplicaciones posibles para blockchain por parte de empresas y organizaciones que quieren explorar y desarrollar servicios basados en una plataforma descentralizada, fiable, segura y prácticamente inmutable.

A pesar de este potencial, en su forma actual, las aplicaciones basadas en blockchain todavía están sujetas a una serie de vulnerabilidades, sobre todo en relación con los hábitos de sus usuarios, que a menudo no toman las precauciones de seguridad necesarias.

Con la creciente popularización de esta tecnología, y con el aumento significativo de la cantidad de valor transaccionado en el ecosistema que ha creado, el número de ataques y su complejidad también tienden a crecer.

En este sentido, se hace cada vez más necesario entender y evaluar de antemano los riesgos que implican las diferentes implementaciones de blockchain y, sobre todo, educar a los usuarios en las mejores prácticas para garantizar la seguridad de las transacciones e intercambios.

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

# Referencias y lecturas complementarias

- **Bitcoin's Security Model: A Deep Dive - CoinDesk**
- **Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology | Apriorit**
- **Blockchain / DLT Attacks and Weaknesses Enumeration** (Planilha Google Doc)
- **Blockchain Threat Report** (McAfee)
- **Common Crypto Phishing Attacks & How to Avoid Them | by NGRAVE**
- **Crypto and Web3 scams**
- **Security and Privacy on Blockchain**
- **The Chainalysis 2022 Crypto Crime Report**
- **What is Crypto-Malware? Definition & Identifiers | CrowdStrike**

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

# Refuerce su operación de ciberseguridad con la gestión de riesgos digitales de la plataforma Axur

Nuestra plataforma es un hub de tecnologías y servicios gestionados que proporciona visibilidad de los riesgos digitales para los equipos y operaciones que desean ampliar la prevención y la respuesta a los incidentes.

**400**
empresas

**600**
marcas

**+ 3.700**
grupos cerrados en las redes sociales

**+ de 1.7 billones**
de señales analizadas

**Casi 3 milllones**
De mensajes con menciones de clientes interceptados en nuestra plataforma

Datos del 2021

Ofrecemos seguimiento, detección, revisión y respuesta para los principales grupos de riesgo que se encuentran en Internet:

- **Fraudes digitales**
- **Fugas de datos**
- **Piratería en línea**
- **Deep & Dark Web**

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

La Plataforma Axur ofrece asistencia experta para hacer frente a los ataques de alto impacto, dirigiendo las acciones tácticas y operativas de ciberdefensa.

Con los equipos CTI/ART de Axur, usted extiende la superficie de monitoreo, detección e investigación de amenazas de su equpo de Seguridad de la Información y Threat Intel, revelando patrones de fraude imperceptibles para estrategias reactivas

**DESCUBRA LAS VULNERABILIDADES DE SU MARCA**

**AGENDE UNA DEMO**

# Sobre Axur

Líder en la supervisión, respuesta y eliminación de riesgos y amenazas digitales en Internet, con el objetivo de crear experiencias digitales más seguras para las empresas y sus consumidores.

Mediante el uso de automatizaciones y aprendizaje automático mediante inteligencia artificial, supervisamos la web superficial, la Deep y la Dark para ofrecer protección contra riesgos como el uso indebido de marcas, robo de identidad, phishing, aplicaciones fraudulentas, ventas no autorizadas y fugas de datos.

Para más información, visite axur.com, si le interesan estos temas puede conocer más en nuestro blog: blog.axur.com

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados

Contacto para prensa: press@axur.com

# Direcciones

EUA
601 Brickell Key Drive, Suite 901 Miami, FL 33131

Singapur
109 North Bridge Road Cityhall District, 179097

Brasil
Rua Mostardeiro, 322  15o andar Porto Alegre, RS 90430000

© Axur 2022. Experiencias digitales más seguras. Todos los derechos reservados