

Aprende con la

GÍA BÁSICA DE ATAQUES CRYPTO



¿Qué es un ataque crypto?

Amenaza que se utiliza para “extraer” diversas formas criptomonedas.



Existen diversos tipos de ataque a criptomonedas.

El cryptojacking (también denominado minería de criptomonedas maliciosa) es una amenaza emergente de Internet.



Se aprovechan de la tecnología blockchain.

puede apoderarse de navegadores web, comprometer todo tipo de dispositivos, e incluso servidores de red.

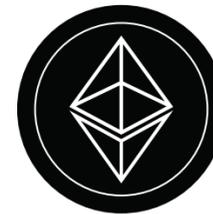
Principales ataques de la historia.

Algunos ataques han dejado huella debido a sus graves consecuencias.



Mt. Gox, 744.408
Bitcoins
2011

Bitfinex, 119.756
Bitcoins
2016



Swarm City,
Edgeless Casino y
æternity, 153.037
ETH

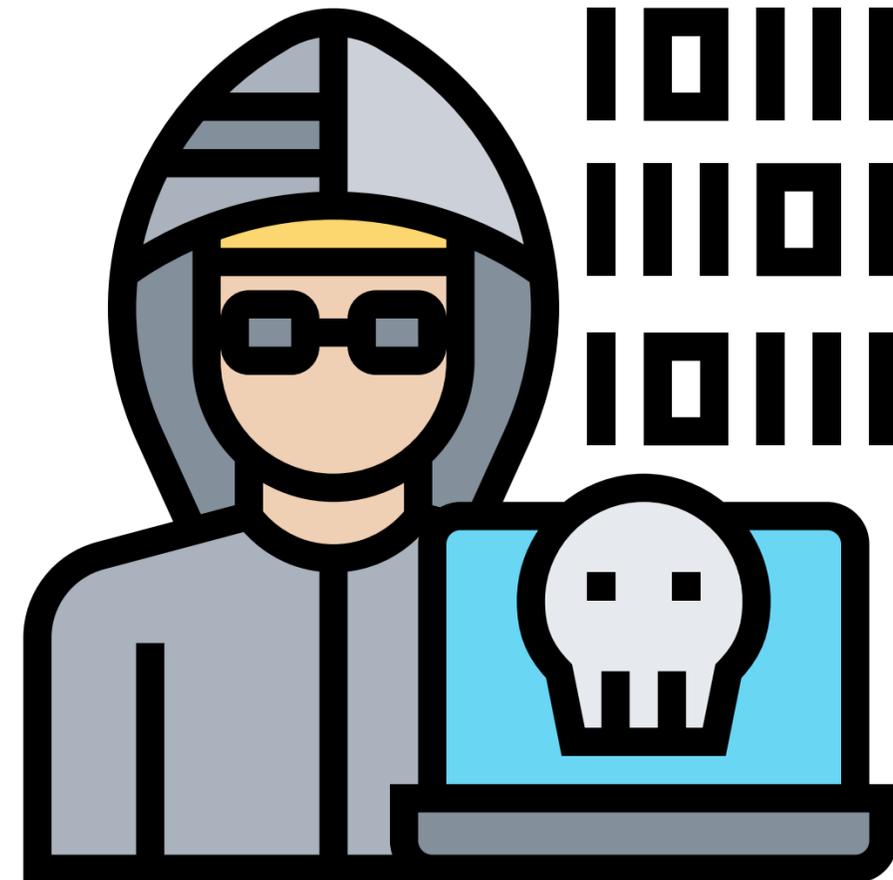
2017

Principales tipos de ataques

- Ataque de Vector 76
- Ataque del 51%
- Ataque de doble gasto

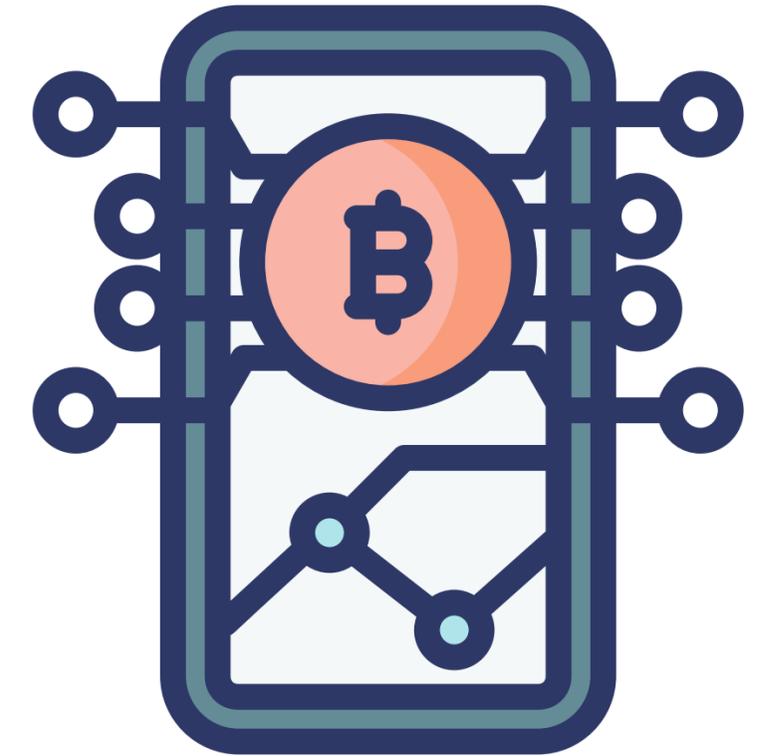
Otros ataques

- Ataque eclipse
- Ataque Sybil
- Ataque Finney



Principales ataques

Existen determinados ataques cuyos resultados son devastadores para la red. De estos pueden desatarse otros muchos ataques.



✓ Ataque del 51%

Estos ataques permiten que una sola entidad sea capaz de adueñarse de más del 50% del hashing power.

✓ Ataque de doble gasto

Se basa en utilizar las mismas monedas para realizar varios pagos.

✓ Ataque de Vector 76

Un ataque de vector 76 se basa en aprovechar el mínimo error en el sistema de consenso de Bitcoin para llevarse a cabo.

Otros ataques de criptomonedas

01 Ataque Sybil

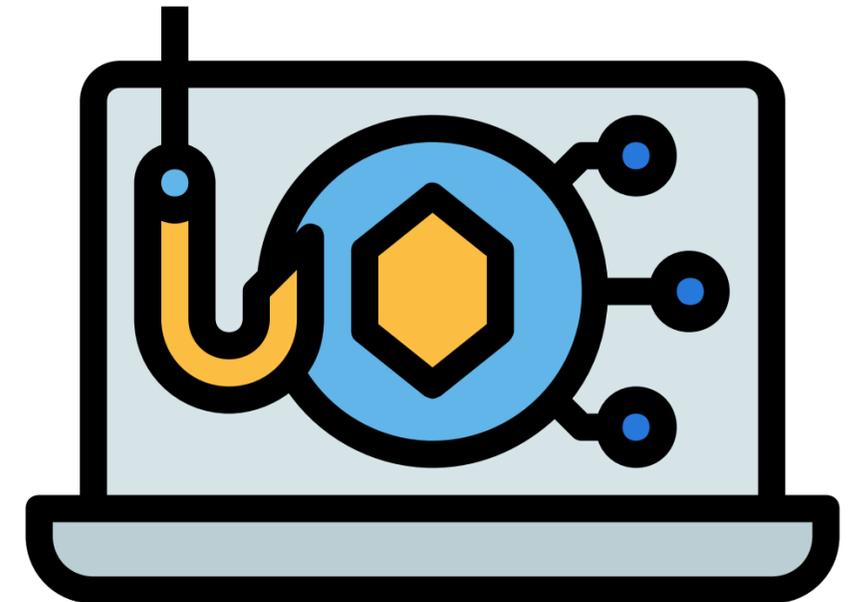
Consiste en que un usuario decida crear múltiples cuentas desde su ordenador en redes sociales.

02 Ataque Finney

Es un tipo de ataque de doble gasto que ocurre cuando un usuario acepta una transacción no confirmada.

03 Ataque Eclipse

Van dirigidos a un usuario en específico con el objetivo de interceptar los datos que recibe la víctima de la red, manipularlos y usarlos para otros fines maliciosos.



¿Cómo evitar los ataques crypto?



✓ Confirmaciones

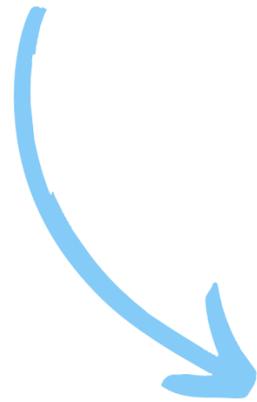
Fijarnos en el número de confirmaciones de una transacción.

✓ Autenticidad

Verificar el origen de cada transacción para comprobar su autenticidad.

¿Quieres aprender más?

Puedes acceder a más lecciones y cursos desde nuestra página web crypto4dummy.com.



@crypto4dummy



@crypt4dummy



@crypto_4dummy