Bitcoin, Lo Bueno, Lo Malo Y Lo Feo

En la actualidad asumimos que **Bitcoin está aquí para quedarse**. Sí, es un poco volátil y sí, otras **Crypto Monedas** son mucho más fácil de minar y mucho más barato al momento de comprarlas, pero la recibida de esta **Crypto Moneda** en el mundo superficial de la web, ha creado un sin número de transacciones para gastar estos **bitcoins. E**s un testimonio de la capacidad de recuperación de la **Crypto moneda más popular**, y de concentrar nuevamente la atención sobre las **Crypto Monedas que hay en el mundo.**

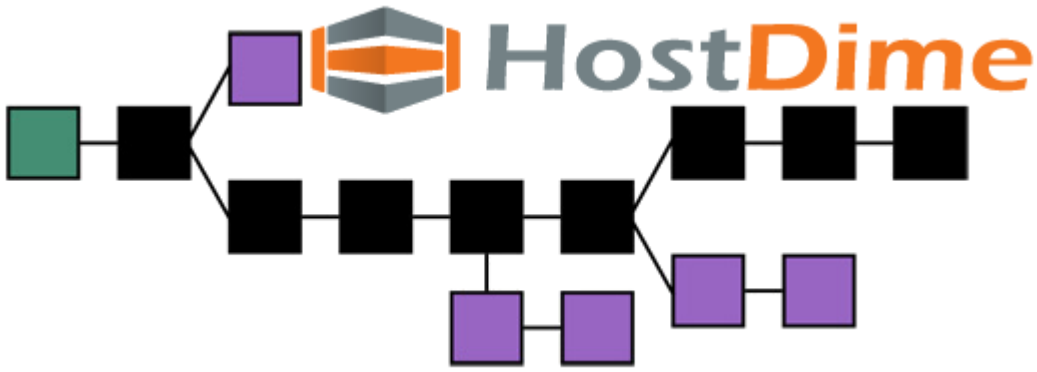
Anteriormente habíamos hablado sobre las [estadisticas del Malware en Android del 2013](), pues bien, el 2013 no solo ha dejado análisis en ese campo, sino tambien en el campo de las Crypto Monedas. Una serie de eventos **durante el año pasado** han demostrado que, si bien la encriptacion del **Bitcoin** en sí puede ser seguro, los Wallets y los servicios utilizados para almacenar e intercambiar el **Bitcoin** no.

Encriptación Y La Cadena De Bloques

Bitcoin es una de muchas **Crypto Monedas** disponibles en la actualidad. Las **Crypto Monedas son monedas digitales** que implementan la criptografía como una parte central del protocolo, a fin de establecer las divisas con seudónimos (o anónimos) y descentralizados en el rastreo. **Bitcoin utiliza cifrado SHA-256**, tanto por su **Proof-of-Work (POW)** y la comprobacion de transacciones. La s**eguridad del protocolo del Bitcoin** se encuentra en una de sus características fundamentales, la **Cadena De Bloques**.

Cadena De Bloques Ó BlockChain Del Bitcoin

El **Blockchain** es básicamente una cadena de varios «bloques» que contienen el historial de transacciones. El **blockchain** comienza con el bloque inicial, conocido como el bloque de inicial. Una vez se generan nuevas transacciones y hashes nuevos se añaden inmediatamente al bloque inicial, formando así lo que se conoce como BlockChain. Que mejor explicación que una imagen, podremos apreciar que el cuadro verde es el bloque inicial, luego se encuntra el blockchain los cuales son los cuadros negros:



Monederos De Bitcoin

El **Bitcoin** se almacenan en carpetas , pero a diferencia de una

cuenta de PayPal , estas » billeteras » no almacenan realmente los bitcoins en sí. A pesar de una serie de diferentes implementaciones y formatos, en general estos monederos contendrán una **clave pública** que se utiliza para recibir bitcoins (similar a un número de cuenta bancaria) . También contiene una **clave privada** que se utiliza para verificar que usted es el propietario de los bitcoins que está tratando de gastar.

Almacenamiento Bitcoins Offline

Pensando en la inseguridad y robos de datos de los servidores de la web, se penso en la forma de almacenar estos datos importantes de forma Offline, encontraremos:

- **Archivos (Bitcoin Wallet):** Estos podremos llevar en cualquier dispositivo de almacenamiento.
- **Papel corriente:** Imprimimos nuestra clave publica y privada con tal de que nadie tenga acceso, solo nosotros, recuerda que también podremos implementar algún código Qr para hacer mas accesible a los datos.
- **Hardware:** Tal es el caso de la Pi-Wallet, un dispositivo que almacena los datos en una seccion protegida del microcontrolador, evitando el robo de datos con virus, malware y todo código malicioso.

Delgada Linea De Seguridad

Como se mencionó al principio , el propio protocolo **bitcoin** puede ser lo suficientemente seguro, pero esto no se extiende a todos los sitios y servicios que se prestan para **bitcoin** . A continuación algunos sitios que fueron vulnerados y con esto se fueron a quiebra, ademas de la perdida de las preciadas **Crypto Monedas** de los usuarios:

- **Inputs.Io**: La vulneración de este sitio genero una perdida de $1,2 millones de dolares. El «hackeo» de esta

pagina se realizo a traves de ingenieria social, el metodo tal vez mas sencillo para obtener datos.

- **Monte Gox:** Los ataques DoS fueron los responsables de la caida de los servicios de esta plataforma, generando perdidas a la hora de las transaccion, lo que obligo a Monte Gox retirarse del mercado de la **Crypto Moneda mas popular**.
- **Silk Road 2.0:** Sufrio un ataque idéntico que al que se le realizo a Monte Gox, con la diferencia que el robo de datos en este servicio se produjo al relanzamiento de la plataforma, mientras los datos se «respaldaban» en «caliente» se robaban al mismo tiempo.
- **Botnet «Pony»:** Con esta Botnet se infecto millones de computadores, no solo para robar simples contraseñas como las de las transacciones bancarias online, sino de los monederos de Bitcoin que tenian las computadoras infectadas.

Como vemos, puede que el sistema para minar y obtener esta **Crypto Moneda** es bastante seguro, pero en contraparte encontramos que no es igual de seguro al momento de guardar las ganancias, ni los servicios en la web son lo bastante seguros como para confiar en que estas monedas virtuales estén seguras.