# Instituto Politécnico Nacional


## Escuela Superior de Cómputo

Sistemas Distribuidos

**Clase 25: Tres videos para analizar**

7CM1

Alumno: Franco Olvera Demian Oder
Boleta: 2021630278

Profesor: Ukranio Coronilla Contreras

Fecha: 22 de abril de 2024

# Contenido



## Video 1: Hoy sí vas a entender qué es el Blockchain

Uno de los temas más tensos y recientes que ha existido en el mundo de la computación han sido las Criptomonedas o Cryptocurrency. Curiosamente, el principal atractivo del tema para la media de la población nunca ha tenido algo que ver con aspectos tecnológicos o incluso financieros, sino simplemente llenarse de dinero formando parte de la comunidad.

Sea cual fuere la intención de las personas para entrar en este mundo, nada de esto sería posible sin la existencia del concepto de la Blockchain o Cadena de Bloques.

Para entenderlo, hay que tener en cuenta lo que es un sistema descentralizado, el cual —en el ámbito de las redes— se enfoca en que sean todos los participantes quienes tomen las decisiones, donde todos tengan la misma importancia y se evite la imprescindibilidad.

Ello trae consigo también varios retos, principalmente con la sincronización de la información y actividades que se realizan.

La solución ante este problema pareció venir en la forma de un documento emitido en 2009 por un tal *Satoshi Nakamoto*, donde se proponía una descentralización del sistema financiero en un sistema nuevo que hoy conocemos como Bitcoin.

En este caso, la moneda se da en la forma de las transacciones que se realizan como tal y donde todos los usuarios del sistema tienen la capacidad de generar y archivar las transacciones. Esto trae problemas debido a la descentralización, pero es aquí cuando entra el Blockchain al rescate. Para poder realizar las verificaciones de dichas transacciones, se añade un costo computacional en la forma de un puzzle criptográfico basado en funciones Hash. Quien tenga el suficiente poder computacional para completarlo, tiene el derecho de escribir el siguiente o los siguientes bloques en el registro de toda la red. A esta acción se le conoce como minado de bloques y siempre está sujeto a una recompensa, criptomonedas para quien pueda añadir el bloque.

Al tener sistemas de seguridad como el principio de la cadena más larga, es difícil vulnerarlo dado que una cadena errónea afectaría a las siguientes y que tiene que realizarse en tiempo real para evitar que la cadena avance mientras se intente falsificarla.

Es interesante este último aspecto dado que, como es un sistema complicado de romper, ha tenido aplicaciones incluso fuera del mundo de las criptomonedas, como la Inteligencia Artificial y el arte digital.

## Video 2: El Ciber Ataque más grande de la historia ¿Empezó con Minecraft?

El internet, más allá de todo, no es más que redes que contienen redes, las cuales contienen todavía más redes. Es una red enorme, la cual está basada principalmente bajo el concepto

de Cliente-Servidor. Los importantes son principalmente los servidores, ya que son ellos quienes terminan ofreciendo la mayoría de los servicios que los clientes consumen. Esta es la forma en la que comúnmente suele funcionar. Sin embargo, existe una forma de atacar a los servidores basada en este principio tan simple.

Hipotéticamente, si la cantidad de peticiones o clientes de un servidor excede por mucho a la que éste puede tolerar, pueden pasar dos cosas principalmente: el servidor se vuelve lento o se cae para todos. Este principio puede utilizarse para atacar a los servidores y recibe el nombre de ataque DOS (Denegación de Servicio). Sin embargo, es imposible que una persona por sí sola pueda conseguir esto de forma por más máquinas virtuales u otras artimañas que pueda conjurar; sigue estando sujeto al ancho de banda que le otorga su proveedor de servicio. Es por ello que existe otra técnica mucho más efectiva e ilegal para accionar dichos ataques, los DDOS (Denegación de Servicio Distribuido); esto ocurre cuando el atacante dispone de dispositivos remotos en todo el mundo, los cuales se infectan gracias a Malware y están a merced de un controlador.

Uno de los casos más sonados tuvo que ver con algo denominado Botnet Mirai (una Botnet siendo una red interconectada de estos dispositivos infectados durmientes, preparados para realizar cualquier ataque coordinado), la cual atacó dominios importantes desde mediados de la década de 2010’s. La mayoría de ellos se dieron porque uno de los primeros perpetradores mencionó en un post dentro de un foro cómo es posible construir una red Mirai, lo que produjo más ataques mediante modificaciones del código.

Más allá del asunto de Minecraft y la forma divertida y rebuscada en que se encontró al autor intelectual del ataque, me resulta impactante e inteligente el *modus operandi* que se tuvo en cuenta. La idea de utilizar dispositivos de los que nadie sospecharía nada para un ataque coordinado me parece ingeniosa y un poco aterradora por las consecuencias que puedan representar. Si fue sumamente sencillo implementar un Malware para realizar ataques DDOS, literalmente podían tener esos equipos a merced de los atacantes, lo que abre las puertas a muchas posibilidades. Se supone que se está trabajando en soluciones desde entonces, pero la idea de que un refrigerador puede ser usado para cualquier otra cosa resulta muy macabra.

## Video 3: Nos atacó un Hacker y te lo explico todo

El autor del video explica que tiene una página enfocada a cursos que tienen que ver con el mundo de la tecnología, llamada Mastermind. La plataforma se mantuvo caída por más de una semana y que tuvo una duración de dos semanas. Los proveedores enviaron un email a los administradores de la página preguntando por si se estaban realizando pruebas de carga. Ellos no estaban haciendo nada y notaron que estaban siendo víctimas de un ataque DDOS gracias a un correo electrónico enviado por su atacante, dentro del cual se exigía un rescate de la página.

La batalla comenzó cuando se decidió que no iba a pagarse por el rescate de la página, la cual se terminó saturando enormemente. De entre todos los escenarios posibles, optaron por defenderse del ataque, pidiendo disculpas de por medio a los alumnos inscritos en los cursos de la página. El ataque como tal fue estudiado y sumamente premeditado gracias a la poca información que fue posible recopilar, por lo que todo ya estaba fríamente calculado. Dada la

efectividad, se estima que se usó una Botnet (de la cual ya se habló previamente); esto significa que la gravedad del ataque era sumamente palpable y notable.
Pese a que no lo aparentase, Mastermind sí contaba con una plataforma que lo ayudaba a bloquear y defenderse de ataques de DDOS, llamada Cloudflare, la cual no funcionó dada la gravedad del ataque.
Fue en ese momento en que se pusieron manos a la obra porque Cloudflare era incapaz de detectar al ataque de forma eficiente; se comenzó con un bloqueo de los países donde no se hablaba español. Una vez que los atacantes notaron el patrón, la escala del ataque subió en buena medida, dado que el ataque era —tomando en consideración todo el poder que tenía el atacante— de pequeña escala.
Ante dicha respuesta, el autor del video contrató una cuenta con mayores funciones en Cloudflare con la finalidad de activar el Antibot, una función diseñada para prevenir y defenderse de ataques así mediante el uso de IA. Como no funcionó al inicio, duplicó el Servidor para evitar las pérdidas en su negocio hasta que el Antibot comenzó a funcionar adecuadamente y el ataque fue repelido a pesar de la completa potencia que tuvieron como respuesta.
En mi opinión, este video enseña un par de cosas importantes:
La primera es que, por más pequeño que pueda ser el negocio que corre tras una plataforma o servidor web, nadie está exento de estos ataques por parte de cualquier persona con la suficiente infraestructura a la mano. Además de ello, darles lo que quieren es —con toda posibilidad— la peor opción que se puede elegir ya que el pago no es un cheque para considerar excepciones. Es por este hecho que defenderse siempre va a ser la mejor opción, cueste lo que cueste.
Y considerando que la defensa del servidor es lo mejor por lo que se puede optar, este video enseña que siempre existe una solución. Puede que Cloudflare haya salvado el día después de todo, pero estrategias como el manejo de servidores espejo también es sumamente útil para mantener vivo el servicio siempre y cuando el atacante no sepa de su existencia.
Es complicado afrontar una situación así, pero la perseverancia terminó recompensando al final-