



SAGRAT  
COR  
SARRIÀ

# **LAS CRIPTOMONEDAS**

A TRAVÉS DE LA CADENA DE BLOQUES



**Autor: Guido Biosca**

**Curso: 2020-2021**

**Tutor/a: Cristina García-Ventosa**

**Centro: Sagrat Cor Sarrià**

# Índice

1	Introducción.....	3
1.1	Justificación.....	3
1.2	Objetivos .....	3
2	Marco Teórico .....	5
2.1	Evolución de la forma de pago .....	5
2.1.1	¿Cuál fue el inicio del dinero? .....	5
2.1.2	Conceptos de la oferta y la demanda.....	6
2.2	El Blockchain.....	10
2.2.1	El inicio de la criptografía .....	10
2.2.2	Las transferencias .....	12
2.3	Criptomoneda.....	16
2.3.1	¿Qué es una criptomoneda? .....	16
2.3.2	La participación en las criptomonedas .....	18
2.3.3	Las Altcoins .....	24
2.3.4	El Exchange.....	25
3	Marco Práctico .....	28
3.1	Entrevista Carlos Flores .....	28
3.2	Inversión en criptomonedas .....	30
3.2.1	ShareRing.....	30
3.2.2	Unitrade .....	33
3.2.3	Cardano.....	36
3.3	La creación de una criptomoneda .....	40
3.3.1	Idea Principal.....	40
3.3.2	La red.....	41
3.3.3	La creación .....	41
4	Conclusión.....	45
5	Limitaciones y prospectiva.....	47

# **1 Introducció**

## **1.1 Justificació**

El tema en el que se va a basar mi Treball de Recerca es en las criptomonedas. Me interesa conocer por qué la criptomoneda ha generado tanto interés lo cual ha permitido que su valor crezca en tan poco tiempo. Para ello investigaré la historia de la moneda, sus usos, en que respaldan su valor y qué problemas tiene para permitir el crecimiento de otras monedas como las criptomonedas. Por último, me interesa conocer la arquitectura tecnológica: basada en la fortaleza de la criptografía, las GPU que minan las monedas y exploraré los riesgos a los que se enfrenta.

Desde pequeño me he interesado por la tecnología ya que es algo que de un día para otro puede cambiar completamente. Lo que veo más importante de la tecnología es que siempre se puede crear más, siempre puedes llegar a una nueva invención que cambie el mundo. Y cuando conocí las criptomonedas me encantaron ya que es una tecnología totalmente digital la cual no se puede tocar y que sigue viva gracias a otras máquinas que hacen que funcione.

## **1.2 Objetivos**

En este trabajo mi principal objetivo es llegar a entender su funcionamiento. También he querido adentrarme un poco más en la criptomoneda y analizar las formas que hay de sacarle provecho. También me planteo un objetivo mucho más ambicioso de crear mi propia criptomoneda. Mi hipótesis es la siguiente: ¿Llegaran las criptomonedas a sustituir la forma de pago convencional?

**Objetivo teórico:**

Antes de empezar a investigar sobre las criptomonedas como tal, me he puesto a conocer un poco el camino que se ha recorrido hasta llegar a ellas, hablando de la historia del dinero físico el cual lleva en la humanidad mucho tiempo y del digital que es el que más utilizamos hoy en día. Una vez conocida toda la historia de la moneda me he puesto a investigar sobre las criptomonedas y su contexto.

**Objetivo práctico:**

La parte práctica del trabajo se dividirá en tres partes:

Primero me gustaría hacer una entrevista a una persona el cual lleva mucho tiempo metido en el ámbito de las criptomonedas y vive de ello. Su principal integración es en la minería, concepto que explicare más adelante.

Segundo haré una inversión con una cierta cantidad de dinero en diferentes criptomonedas que vea óptimas para generar un beneficio a medio/largo plazo y así poder analizar su progreso mientras dure este trabajo.

Por último, creare una criptomoneda desde cero, la cual estará publica en el mercado para así poder hacer intercambios con ella. Mi principal idea es que esta tenga los fees (precio por envío) muy bajos, ya que el gran problema de las monedas más utilizadas es que estos fees son muy altos.

## **2 Marco Teórico**

La criptomoneda, está formada por las características de la moneda que conocemos hoy en día. Por eso, comenzaré hablando sobre cómo y cuándo se creó la moneda que actualmente conocemos y, seguidamente, lo enlazaré con las criptomonedas.

### **2.1 Evolución de la forma de pago**

#### **2.1.1 ¿Cuál fue el inicio del dinero?**

Hace miles de años la población ya intercambiaba sus bienes. Los productos en general no tenían un valor fijo ya que un año podía ser más valioso y otro año podía ser muy poco importante, entonces aparecieron las primeras formas de trueque. Con el paso de los años, se comenzó a intercambiar consumibles por huesos o piedras, que fueron las primeras formas que tuvo el dinero.

Las primeras monedas no se crearon hasta el siglo VII antes de Cristo. Se formaron a partir de una aleación de oro y plata. Fueron creadas por los griegos en la actual Turquía.

Al cabo de un tiempo, surgieron nuevas monedas en China e India, pero estas tenían formas muy peculiares, como delfines o lingotes. Por el otro lado, en Grecia tenían formas circulares, muy parecidas a las actuales monedas, hechas a partir de oro, plata y bronce, que en función del peso que tenía cada moneda tenía diferente valor.

Los metales valiosos que se utilizaban como moneda anteriormente fueron dando paso, siglos más tarde, a otros materiales bastante más baratos y fáciles de conseguir. Entonces llegó el sistema fiduciario. En el siglo XVII, en Suecia, surgieron los primeros billetes. Esta nueva manera de poder pagar se basó en la confianza de la población, ya que el billete era solamente un papel.

## 2.1.2 Conceptos de la oferta y la demanda

De manera global, el mercado se basa principalmente en la ley de la oferta y la demanda. Indica la relación que hay entre la demanda de un producto y la cantidad de bienes o servicios que hay dispuestos a venderse, la oferta.

Entonces, el precio es directamente proporcional a la oferta y la demanda porque si la oferta baja y la demanda sube, el precio del producto es más alto. Se le llama equilibrio de mercado o punto de equilibrio cuando los compradores están dispuestos a comprar la misma cantidad que de los que lo fabrican.

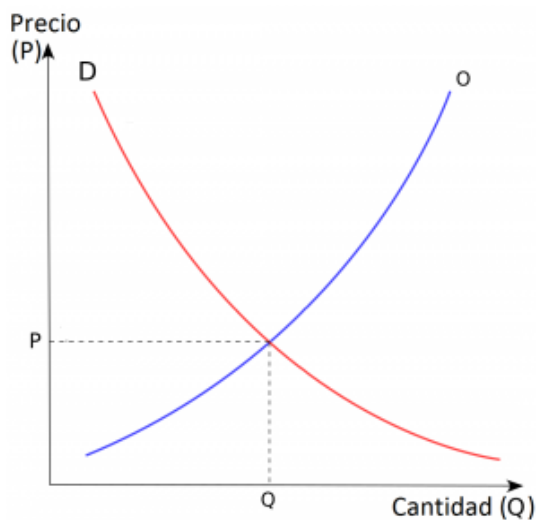


Figura 1. Fuente: economy-wiki

Se puede ver que la curva de oferta, la línea azul, es creciente y la curva de la demanda, la línea roja, es decreciente. Donde se cruzan las dos curvas se conoce como equilibrio de mercado

Pueden aparecer hasta tres situaciones diferentes:

- Exceso de oferta: Aparece cuando hay bastante más producto del que la gente quiere comprar, entonces los vendedores bajan los precios para así poder vender más producto.
- Exceso de demanda: Aparece cuando los vendedores tienen menos producto del que la gente está dispuesta a comprar, entonces los vendedores aumentarían el precio.
- Punto de equilibrio: Es cuando no hay ni exceso de demanda ni exceso de oferta, existe igual de oferta que de demanda.

El precio de un producto se determina por su oferta y su demanda. Y el dinero no es una excepción. Si la oferta incrementa, pero su demanda decrementa, el precio tendera a depreciarse (inflación); si la demanda tiende a crecer y su oferta a bajar, tendera a apreciarse (deflación). Un incremento de la oferta de dinero significa que hay más dinero en circulación, por lo tanto, la gente está dispuesta a gastar más dinero.

La inflación (situación que sucede cuando se crea, de forma exagerada, más moneda) se forma en el sistema fiduciario. Las grandes guerras han sido los momentos en los cuales ha llegado a suceder los peores casos de hiperinflación. Durante estos momentos varios países empezaron a fabricar inmensas cantidades de billetes entonces la moneda se iba devaluando cada vez más.

### **La crisis del Tulipán**

Durante el siglo XVII, en los Países Bajos, algunos tipos de flores empezaron a valer mucho dinero. El tulipán llevo a valer tanto que provocó la primera burbuja especulativa de la historia.

El tulipán llevo en el siglo XVI desde Turquía a Holanda para adornar los jardines del emperador Maximiliano. La demanda de la flor empezó a crecer, pero la oferta era muy pequeña, ya que la flor tardaba siete años en madurar.

Entonces, apareció el mercado de futuros. Los comerciantes se dieron cuenta que podían vender los bulbos que sacarían en la siguiente cosecha. El comprador obtenía un documento conforme podría obtener los bulbos cuando florecieran y el vendedor obtenía el pago anticipado.

Mucha gente, poco adinerada, dejo su trabajo, pidió créditos e hipoteco su casa para poder trabajar en el mercado de futuros con los bulbos de tulipán.

Cada vez el precio de los tulipanes iba subiendo, en 1635 un solo bulbo se cambió por una mansión.

En 1637 los contratos de bulbos empezaron a caer en picado por unas malas cosechas, la burbuja exploto. La economía holandesa entro en quiebra y muchas familias se arruinaron.

## Alemania en los años 20

La hiperinflación es la subida rápida e incontrolada de los precios.

El gobierno empezó a imprimir numerosas cantidades de billetes para poder hacer frente a los pagos del Tratado de Versalles. En 1923 cada billete aumento su valor casi un 30.000%, lo que costaba un marco anteriormente ahora costaba 300.

Según Arnulf Scriba, podías estar en un restaurante y durante ese tiempo tu cuenta se podía duplicar.



Figura 2. Fuente: [claseshistoria.com](http://claseshistoria.com)



## La burbuja puntocom

Entre los años 1997 y 2001 las bolsas occidentales experimentaron un rápido aumento de su valor gracias a las nuevas empresas tecnológicas (Amazon, eBay, Microsoft...). Mucha gente empezó a comprar acciones. La burbuja continuó inflándose hasta llevar al Nasdaq (segunda bolsa de valores electrónica automatizada más grande de Estados Unidos) a una subida del 416% y empezó a bajar radicalmente. Muchas empresas que habían salido a bolsa empezaron a desaparecer (desaparecieron 4.854 empresas puntocom). En España el caso más sonado fue el de Terra (compañía dedicada a contenidos de Internet del Grupo Telefónica), en noviembre de 1999 Terra salió a cotizar en el Ibex a un precio de 11,81€ y en apenas 3 meses, en febrero de 2000, llegó a su máximo, un precio de 157,6€. Entonces Terra comenzó a bajar sin parar hasta julio de 2005 que su precio era de tan solo 3.04€.



Figura 3. Fuente: [claseshistoria.com](http://claseshistoria.com)

## 2.2 El Blockchain

Entre otras cosas, es una de las palabras de moda en los últimos tiempos. El blockchain o la cadena de bloques es un concepto que plantea una enorme revolución no solo en nuestra economía, sino en todo tipo de ámbitos. Un aspecto importante es que en la mayoría de blockchain se utiliza la criptografía de llave pública, concepto que más adelante se desarrolla.

### 2.2.1 El inicio de la criptografía

La criptografía la usamos a diario, por ejemplo, cuando enviamos un mail que se cifra y hasta que no llega al destinatario no se descifra. Todo ello para que solamente el emisor y el destinatario puedan saber que contiene ese mensaje y que nadie más pueda conocerlo.



Figura 4. Fuente: dornica.net

El cifrado de mensajes lleva activo desde hace más de 4000 años.

Una comunicación está totalmente cifrada cuando solamente el emisor y el receptor son capaces de sacar la información del mensaje.

Los jeroglíficos del Antiguo Egipto son uno de los primeros ejemplos de mensajes ocultos, ya que para poder descifrar el mensaje se necesitó la Piedra de Rosetta.

Los espartanos también ocultaban sus mensajes. Utilizaban una técnica llamada cifrado por transposición, enrollaban un pergamino sobre una estaca que servía para poder ordenar las letras y ver el mensaje. Para poder descifrar el mensaje el receptor debía tener la misma estaca, con el mismo diámetro, que el emisor y así podría obtener la información.

A lo largo del tiempo la criptografía cada vez fue siendo más importante. Estuvo presente en la gran mayoría de los conflictos armados. Antoine Rossignol era uno de los criptógrafos más importantes de Francia, trabajó en el primer centro de criptología de Francia, Cabinet Noir.

En la Guerra de Crimea, Reino Unido consiguió una gran ventaja gracias a Charles Babbage (pionero en el ámbito de la computación gracias al desarrollo de la Máquina analítica). Los códigos de Vigenère se consideraban extremadamente robustos, pero, los consiguió descifrar.

Durante la Primera Guerra Mundial, la criptografía se usó mucho. Unchi fue un código encriptado creado por Alemania y Francia lo consiguió descifrar.

En la Segunda Guerra Mundial, una de las partes clave fue la criptografía. Alemania consiguió apoderarse del Atlántico Norte gracias a sus comunicaciones encriptadas por la máquina Enigma. Así que romper las comunicaciones enemigas se convirtió en un nuevo campo de batalla entre matemáticos, ingenieros y físicos.

Una de las labores criptográficas más conocidas fue el trabajo de Alan Turing y sus aliados, sin embargo, no fue el único. Por ejemplo, Estados Unidos, utilizó una técnica que utilizaron en la Primera Guerra Mundial, ya que apostaron por usar como código los idiomas de los nativos americanos. El Cuerpo de Marines de Estados Unidos contaba con medio millar de operadores de radio que cifraban, en americano nativo, los mensajes a enviar para que el Ejército Japonés no pudiese extraer la información del mensaje.

Después de la Segunda Guerra Mundial, hubo un gran avance en la criptografía gracias a Claude Shannon. En 1948, Shannon publicó "A Communications Theory of Secrecy Systems" en el cual se modernizaron las técnicas de codificación y se convirtieron en procesos matemáticos avanzados. Shannon demostró que el análisis de frecuencia se podía calcular matemáticamente e introdujo la distancia de unicidad (marcaba la longitud de un texto cifrado que se necesitaba para poder descifrarlo).

La computación se convirtió en algo esencial en el ámbito del cifrado y descifrado de mensajes. Por seguridad, la mayoría de los países vincularon la criptografía con tareas de inteligencia y espionaje. Desde los años 50 hasta los 70, la NSA bloqueó y censuró todas las publicaciones relacionadas con la criptografía en Estados Unidos.

El 17 de marzo de 1975, llegó el primer avance público (no dependiente de la NSA). IBM consiguió desarrollar el algoritmo de cifrado Data Encryption Standard (DES).

### 2.2.2 Las transferencias

Normalmente a la hora de hacer una transferencia de dinero hacia otra persona o hacia una empresa, la operación se realiza a través de un banco. Dicho banco interactúa entre el emisor y el receptor de la transferencia, así pues, centralizando el movimiento de capital de un lugar a otro.

Para explicar vamos a utilizar un ejemplo: Tenemos a Juan, que quiere retirar 500 euros hacia la cuenta de su hijo Luis. En apenas unas pocas horas, el banco habrá anotado en su base de datos que a Juan hay que restarle esos 500 euros de su cuenta y a Luis hay que sumarle 500 euros en su cuenta.

Pero aquí hay un problema, y es que ni Juan ni su hijo tienen control sobre la transacción efectuada. Dicha transacción depende únicamente de cómo lo gestionan los bancos. Esto quiere decir que están sometidos a sus condiciones, es decir, a sus comisiones.

Para resolver el problema de la centralización apareció el blockchain, cuya principal función es solucionar el problema de los bancos, ya que, básicamente elimina a todo tipo de intermediario y descentralizando toda la gestión. Así, el control de la transferencia depende únicamente del usuario, no de los bancos, puesto que los usuarios no están sujetos a nada para poder efectuar sus transferencias.

Y ahora vamos a volver con Juan, pero gestionando sus transferencias desde el blockchain: Juan tiene sus 500 euros en su wallet para poder hacer el pago a su hijo Luis. Entonces, Juan solo necesitara que su hijo le pase la dirección de llave pública de su billetera. De esta manera, podrá efectuar la transferencia y en cuestión de minutos le habrá llegado el dinero a Luis sin ningún tipo de intermediario por en medio.

En definitiva, el blockchain es un gigantesco libro de cuentas en los que los diferentes registros están totalmente enlazados y cifrados para poder proteger la privacidad y la seguridad de las diferentes transacciones.



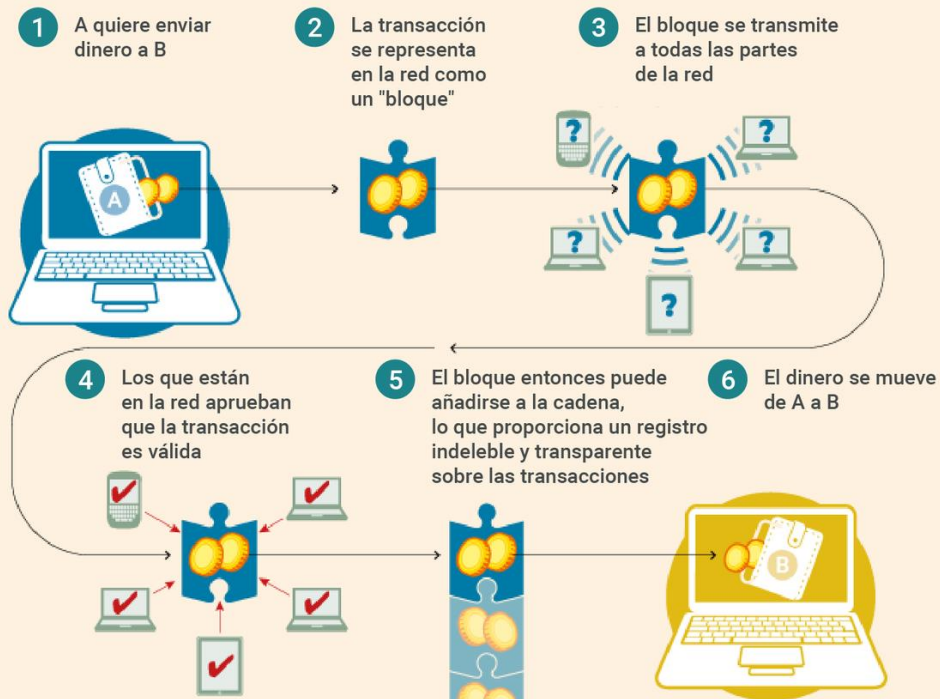
Figura 5. Fuente: elaboración propia

Esta gran cadena de bloques tiene una parte muy importante para su funcionamiento, debe haber varios usuarios (nodos) que se ocupen de llegar a verificar todas estas transacciones para que así el bloque de esa transacción pueda registrarse en ese gigantesco libro de cuentas.

El proceso es relativamente fácil y asequible para todas las personas, pero para que todo funcione correctamente es necesario que haya más usuarios en ese mismo instante encargándose de verificar todas estas transacciones.

Los usuarios o nodos que se encargan de la verificación son los llamados: mineros. Cuando ellos consiguen verificar con éxito una transacción, se llevan una pequeña cantidad de ella.

## Cómo funciona blockchain



Fuente: FT

INSIDER<sup>PRO</sup>

Figura 6. Fuente: insider

Este es un ejemplo extraído de INSIDER Si Juan quiere retirar una criptomoneda de su cartera digital, primero deberá avisar a todos los usuarios de que va a efectuar esa transacción, pero ninguno de esos usuarios sabe quién es ni Juan ni su hijo Luis. Entonces, los nodos verifican que Juan tiene dicha cantidad de criptomoneda y la transfieren vía la red hacia la cartera de Luis.

A medida que pasa el tiempo los bloques se van llenando ya que cada bloque tiene una limitación. Cuando un bloque ya no admite más transacciones, llega el momento de validarlo, que es donde los mineros suelen sacar más beneficios, ya que reciben una gran recompensa por sellarlo.

### 2.3.2.1 Satoshi Nakamoto

Satoshi Nakamoto es una de las identidades más anónimas del mundo de las criptomonedas. De esta persona o conjunto de personas, solamente conocemos su pseudónimo, Satoshi Nakamoto, y un conjunto de documentos que dejaron después de la creación de una tecnología tan importantes para humanidad: el bitcoin y la blockchain.

Desde la creación del bitcoin, se ha estado buscando al creador. Durante todo este tiempo se han identificado personas y organizaciones que tras diversas teorías que los señalan, con más o menos fuerza. Hasta ha habido personas que se han hecho pasar por Satoshi Nakamoto para conseguir fama.

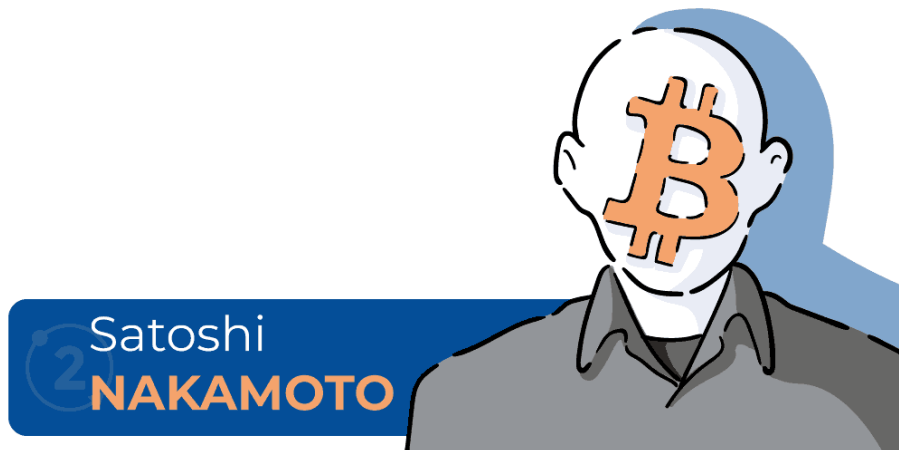


Figura 7. Fuente: xataka

La verdad es que hoy en día no se ha encontrado la verdadera identidad. Otra teoría probable es que Satoshi Nakamoto hubiese fallecido tras la gran creación, ya que, en la blockchain de Bitcoin se puede ver cómo hay varios bitcoins suyos que no se han movido todavía.

## 2.3 Criptomoneda

A continuación, se va a explicar que es la criptomoneda y varios conceptos relacionados con ella como la minería de criptomonedas, el staking, las altcoins y el exchange. Se acompañan estos conceptos con ejemplos prácticos y personales que ayudan a entenderlos y contextualizarlos.

### 2.3.1 ¿Qué es una criptomoneda?

Las criptomonedas son monedas virtuales que, mediante un intercambio electrónico, permiten comprar productos y servicios como cualquier otra moneda tradicional o física.

Una criptomoneda es una moneda digital, no física y que está basada en el empleo de la criptografía como medio para realizar transacciones muy seguras en internet. La técnica criptográfica, que es el cifrado, también permite controlar la transferencia de fondos e introducir nuevas unidades de criptomonedas al mercado. Se pueden



Figura 8. Fuente: investing

considerar como divisas alternativas, funcionan a nivel mundial y no están sujetas a la centralización por los bancos que es lo que ocurre en todos los países del mundo.

Para llevar el control de cada criptomoneda que se emite se utiliza el blockchain, donde se guarda un registro de todas las transacciones efectuadas. Son intercambiables por cualquier divisa local. No admiten la cancelación de transacción, por ejemplo, si tu envías una criptomoneda a una empresa, no hay forma de cancelar esa transacción como con tarjeta de crédito. Sería como poner billetes de 100 euros en un sobre y enviarlos a un lugar, no hay forma de recuperarlos a menos que esa persona te los envíe de vuelta.

Una de las cosas positivas de hacer una transacción con la criptomoneda es que tú puedes enviarla hacia cualquier país sin necesidad de comisiones ni largos tiempos



de espera. Existen dos tipos de criptomonedas: las “stable-coin”, que son las que no cambian de valor nunca. Por ejemplo, la llamada Tether, siempre tiene un valor fijo de 1 USD y se suele utilizar para la mayoría de los intercambios entre criptomonedas. Y las “no-stable-coin” que son las criptomonedas más comunes como el bitcoin, que su precio fluctúa constantemente.

Seguramente para todos nosotros la moneda más conocida es el bitcoin ya que es una de las mayores creaciones tecnológicas de la humanidad. Es la primera criptomoneda que se creó, y es la única aplicación basada en la tecnología de blockchain que lleva activa desde el año 2009. Es la criptomoneda más famosa, se usa exclusivamente para transacciones en internet y empieza a tener valor en el mundo real. Sirve para intercambiar bienes y servicios gracias a su eficacia, seguridad y facilidad de intercambio. Bitcoin es un software, un protocolo y una moneda. Estas tres características permiten que Bitcoin pueda ser una red de pagos global basada en código abierto y única.

Se creó con la finalidad de ser una moneda totalmente descentralizada, sin tener la necesidad de tener todo gestionado por un banco o un gobierno. El valor de la moneda depende únicamente de los usuarios. Si varias instituciones con gran capital se pusieran de acuerdo para comprar bitcoin, el precio de este subiría hasta un nuevo máximo histórico.

Otra gran característica del bitcoin es que es la primera forma de dinero que se crea, distribuye y se custodia mediante una gran red de ordenadores. Actualmente esta red de ordenadores es la red con más poder de cálculo del mundo.

Cada vez más tiendas físicas y digitales aceptan el método de pago Bitcoin. Se dice que sustituirá a la forma de pago convencional. El primer pago que se hizo mediante Bitcoin fue el 17 de mayo de 2010 en una pizzería, cuando un programador pagó dos pizzas con 10.000 Bitcoin que en su momento eran 80\$, actualmente el valor actual de los 10.000 Bitcoin es de 80 millones de dólares.

### 2.3.2 La participación en las criptomonedas

Existen dos formas de validar y hacer funcionar esta red descentralizada o blockchain. Por un lado, está la prueba de trabajo, la minería, que consiste en que varias personas llamadas mineros, destinan cierto poder computacional para validar los bloques de la red, estos mineros por lo tanto están compitiendo entre ellos. Y, por otro lado, está la prueba de participación, el staking, donde los participantes de una red descentralizada pueden bloquear cierta cantidad de criptografía para que así el protocolo les pueda considerar como validadores de la red. En este sentido la recompensa no viene por el poder computacional como los mineros, sino que tiene un carácter más aleatorio y requiere que las personas apalanquen (con un capital inicial, poder pedir un préstamo y así tener la posibilidad de invertir con más dinero del que tienes) ese valor.

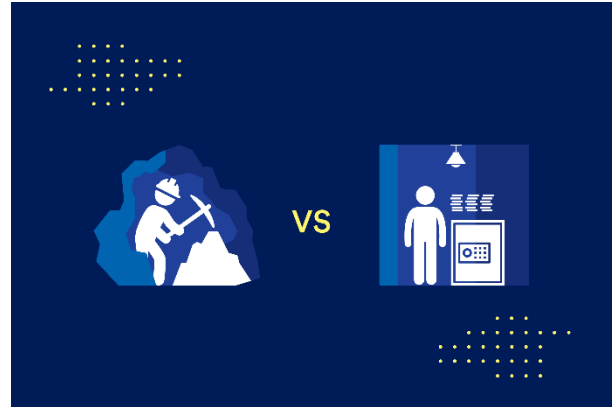


Figura 9. Fuente: bit24

A continuación, se desarrollan estas dos acciones detalladamente.

#### 2.3.2.1 La Minería

La minería de criptomonedas es el proceso donde se validan todas las transacciones que realizan los usuarios con la moneda digital. Los mineros tienen varias labores durante el proceso de minado:

- Comprueban que diferentes usuarios no utilicen el mismo bitcoin más de una vez. Esto elimina el robo de criptomonedas.
- Facilitan la transmisión de las diferentes cadenas de datos, lo que asegura el funcionamiento de este sistema.

Pero la gran pregunta es, ¿por qué los mineros dejan sus ordenadores encendidos todo el día consumiendo electricidad? La razón es porque los mineros reciben diferentes tipos de recompensas:

- Reciben las comisiones que cobran a los usuarios por la transacción que efectúen.
- Reciben nuevos Bitcoins que ellos mismos generan al cerrar un bloque.

Al final gracias a todas estas recompensas que reciben, consiguen una fuente de ingresos totalmente pasiva y rentable.

La minería de criptomonedas la podríamos comparar con la minería de oro. Para poder conseguir oro debes tener unas buenas excavadoras y herramientas. Aunque también podrías conseguirlo con un solo pico, pero se tardaría mucho más que con las máquinas. Pues con las criptomonedas es igual, pero lo que necesitamos es el poder de procesamiento para tener una buena rentabilidad. Para ello, se necesita un buen rig de minería; es un conjunto de máquinas con gran poder de procesamiento. Nosotros también podríamos minar con nuestro propio ordenador y hasta con nuestro teléfono móvil, pero en esta opción la rentabilidad que existe es una cantidad mínima.



*Figura 10. ambitott*

Para poner un ejemplo, con el móvil podríamos estar hablando de céntimos al día, mientras que con un buen rig, de unos 5000 euros invertidos, rondaría los 30 euros al día de beneficio, que eso es al mes una ganancia de unos 800 euros, pero a todo este total habría que restarle el consumo eléctrico, que en este caso sería de unos 200 euros al mes.

Ahora vamos a ver como serían los pasos para conseguir minar. Nos centraremos en la criptomoneda Ethereum (ETH) porque es la más recomendada para la minería actualmente. Lo principal es crear nuestra wallet para poder guardar todas las “recompensas” de nuestra minería. Existen dos tipos de wallet, la fría, que es un dispositivo físico en el cual puedes almacenar tus criptomonedas y es el más seguro. Y, por otra parte, tienes la wallet caliente, que es la que se crea en línea y siempre está conectada con la blockchain, esta no es tan segura como la anterior, pero tiene una gran comodidad utilizarla. Para comenzar, se recomienda la caliente porque no tiene ningún costo, así que es la que utilizaremos, yo en específico, utilizaré la TrustWallet, que es una aplicación para el teléfono móvil.

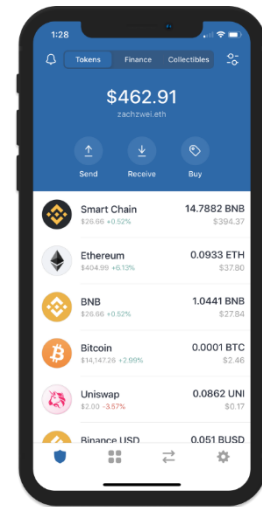


Figura 11.

Al crearla, nos dará una frase con 12 palabras, es muy importante guardarla porque si perdemos el teléfono móvil, esa será la única forma de conseguir de vuelta nuestra wallet.

Fuente: TrustWallet

En este momento, lo único que nos falta es configurar nuestro ordenador para minar, para ello utilizaré el software NiceHash, que se instala en la bios de nuestro ordenador para así poder utilizar todo el potencial. Cuando ya lo tengamos instalado lo único que faltará es copiar nuestra dirección de llave pública de nuestra wallet anteriormente creada y pegarla en el controlador de NiceHash, y ya estará todo listo para empezar a minar.

Pero, la cosa más importante para minar es, ¿qué criptomoneda debo minar? Actualmente, hay miles incluso millones para poder elegir, pero no todas son igual de rentables, incluso algunas son estafa. Las más conocidas y las que más se suelen minar, son Bitcoin y Ethereum.

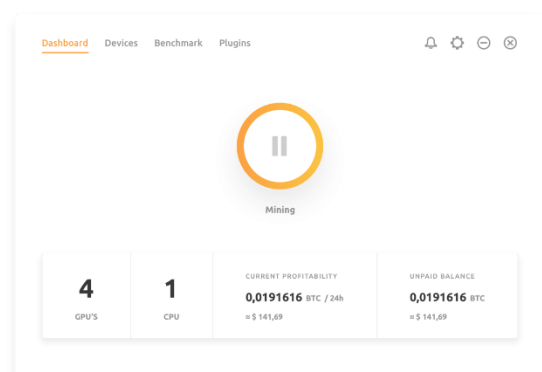


Figura 12. Fuente: nicehash

Primero empezaremos con Bitcoin, actualmente, si minas esta criptomoneda, todavía sigues saliendo positivo, pero con un rendimiento muy pequeño. Esto se debe a que la dificultad de minar cada bloque ha ido aumentando cada vez que se minaban. En 2017, minar un bloque, te daba exactamente 50 bitcoins. Mientras que actualmente, te otorga 12,5 bitcoins que, comparando con la anterior cantidad, es ridícula. Si convertimos todas estas cantidades de bitcoins a euros, estamos hablando de una diferencia de aproximadamente 2 millones de euros. Lo que significa que, si en 2017 minabas un bloque en el mismo tiempo, recibías 2 millones de euros más que si lo minas actualmente.

Este proceso se asemeja mucho al sistema bancario actual. Igual que los países pueden imprimir dinero, el sistema de Bitcoin también puede hacerlo, pero con una serie de limitaciones:

- La máxima cantidad de bitcoins que pueden ser creados es de 21 millones
- Actualmente, por cada bloque minado de bitcoin, se añaden 12,5 bitcoins nuevos. Pero este incentivo se reduce a la mitad cada 210.000 nuevos bloques.



Figura 13. Fuente: coinwarz

Mientras que si hablamos de Ethereum hoy en día, tiene una alta rentabilidad. Por cada bloque que minas, recibes 2 ETH, unos 4000 euros, comparado con los bloques de bitcoin, esta es una pequeña cantidad, pero la cosa es que minar un bloque de Ethereum es muchísimo más rápido que uno de bitcoin. A parte, no solo se reciben recompensas de estos bloques, sino que también reciben por cada transacción que un usuario hace con sus Ethereum. Bitcoin también ofrece esta característica, pero no es tan llamativa. Esa parte es incluso más rentable que la de minar bloques ya que las comisiones a los usuarios por hacer envíos, es altísima. Un usuario llegó a pagar 36.000 dólares, por una transacción en el Exchange Uniswap, es un exchange totalmente descentralizado.

El tema más importante para esta minería es el hardware que se usa. Se pueden utilizar varios tipos, los más conocidos suelen ser, las GPU, que son las tarjetas gráficas de los ordenadores. Lo que hacen los mineros es comprar grandes cantidades de estas y las agrupan en un mismo ordenador, eso se



*Figura 14. Fuente: nmint*

llama rig de minería. Estas tarjetas gráficas tienen miles de núcleos pequeños y cada uno trabaja por su parte, entonces eso a la hora de minar va muy bien ya que pueden hacer esos cálculos matemáticos en cuestión de segundos. Las tarjetas que más se suelen utilizar son las de “Gaming” ya que están hechas para dar una gran potencia y que el videojuego vaya muy fluido. Entonces, en vez de utilizarlas para jugar, las ponen a minar. También existe otra opción de los “ordenadores para mining” creados específicamente para esta actividad. Estos son altísimamente caros, uno te puede llegar a costar hasta 50.000 euros, pero son la mejor opción si quieres conseguir buenos beneficios.

La parte negativa de estos es que se crean solamente para poder minar una única criptomoneda, y luego no la puedes cambiar a otra.

También existen las “pools” de minería, que consiste en diferentes personas u organizaciones que juntan su poder de computación para trabajar juntos y así poder conseguir mejores recompensas. Esta opción es muy rentable para los pequeños mineros con poco capital para poder minar.

### 2.3.2.2 El Staking

El staking de criptomonedas se puede imaginar como la alternativa perfecta de la minería pero sin necesitar de tantos recursos para ser rentable. En resumen, consiste en guardar en una wallet tus criptomonedas y así poder respaldar todas las operaciones en la blockchain y mantener la seguridad. Es una forma de conseguir recompensas en forma de criptomoneda tras bloquear cierta cantidad de esa misma moneda en una red o protocolo. Es una mejora sustancial a la minería ya que hemos visto que es limitada. En el protocolo de consenso, los diferentes nodos son conocidos como validadores, y

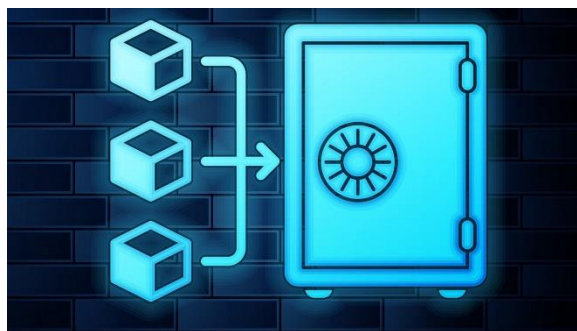


Figura 14. Fuente: xataka

son los que se encargan de validar los bloques generados. La elección de todos estos nodos es completamente aleatoria, aunque tienen mayor posibilidad de que les toque aquellos que tienen más cantidad de criptomoneda.

La parte positiva del staking es que no es necesario adquirir ningún tipo de hardware para poder conseguir esas recompensas y, así, no hacer una inversión que al largo plazo ya sea inutilizable, ya que las máquinas con el tiempo van perdiendo potencia.

Hacer staking es algo muy llamativo, pero aun que lo puedes hacer incluso con un euro, no es algo que te vaya a traer ganancias muy significativas. A menos que encuentres una moneda muy potenciada para el staking.

Una de las criptomonedas más conocidas para hacer staking es Stellar (XLM), con una rentabilidad del 2% al 4% anual. Para la gente con grandes cantidades de esa misma crypto, por ejemplo, a uno que tiene 5 millones de euros en esa misma moneda, equivale a unos 8 mil euros de ganancia al mes. Está claro que esta puede parecer una opción solamente para gente con gran capital almacenado. Pero hay grandes criptomonedas poco conocidas que pueden llegar a hacer un 100% al mes.

En el presente, el staking todavía le queda mucho camino por recorrer y en un futuro, seguro que será una opción muy viable.



### 2.3.3 Las Altcoins

En el mundo de las criptomonedas, no solamente existen las más famosas como Bitcoin. Los altcoins son aquellas alternativas al bitcoin. El desarrollo de estas es relativamente sencillo debido a que bitcoin es de código abierto y muchas de las criptomonedas del mercado también lo son. Así que es sencillo obtener su código y realizar los cambios pertinentes para que se adapte a una nueva idea o una concepción ligeramente diferente del proyecto. Algunas criptomonedas como Ethereum ofrecen la sencillez de poder

desarrollar tokens sin necesidad de crear una red blockchain nueva. Mediante un Smart Contract podemos crear las bases de un nuevo token, reduciendo así los costes de desarrollo y haciendo más simple la financiación de los proyectos.

La característica más importante en las altcoins es su innovación y su gran potencial de crecimiento a través de los tokens. Cada una puede estar soportada por diferentes proyectos de una empresa o persona. Muchas tienen un gran trabajo y esfuerzo detrás, con unas proyecciones y un roadmap (plan de acción durante varios años) buenos. Hay personas que no solo invierten para luego poder sacar un gran beneficio, sino que también hay quienes invierten por la idea o plan de ese token, pueden ser desde altcoins sobre los bolígrafos hasta altcoins sobre una aplicación que te ayuda con tu día a día. Pero no es todo bueno, hay que saber bien en qué invertir y en qué no, porque hay muchos casos en los que se crea una altcoin solamente para quedarse con todo el dinero que la gente haya invertido en esa moneda, por eso es muy importante investigar bien cada criptomoneda antes de invertir, el CEO de ese proyecto, mirar si tiene buenos fundamentos y planes de expansión.

Lo sorprendente de estas altcoins son su capacidad de impulsión, ya que, a diferencia de Bitcoin, Ethereum, Litecoin, etc. Estas tienen todavía un gran camino por recorrer. Y pueden hacer tanto perder mucho dinero como hacerte una multiplicación de mil a tu inversión. Si se invierte en una altcoin, la cual hayas investigado a fondo, y que creas que tiene un buen potencial, puede subir su precio hasta un por mil, si tu



Figura 15.

Fuente: *alternativekoin*



inversión principalmente era de cien euros. En este momento se podrían retirar unas ganancias de cien mil euros, pero, también es posible que pase al revés y esa inversión se quede en cero euros.

Me gustaría añadir un ejemplo de altcoin, que me ha fascinado. Su nombre es Sharetoken (SHR) y es de la empresa ShareRing que está a punto de lanzar una aplicación la cual sirve para poder almacenar todos tus documentos en la nube con una cifrado de datos y en esa misma poder tener tu wallet de tokens. Tras varios días de investigación y charlas con los administradores de esta moneda, me decidí a comprarla en 0,03\$.

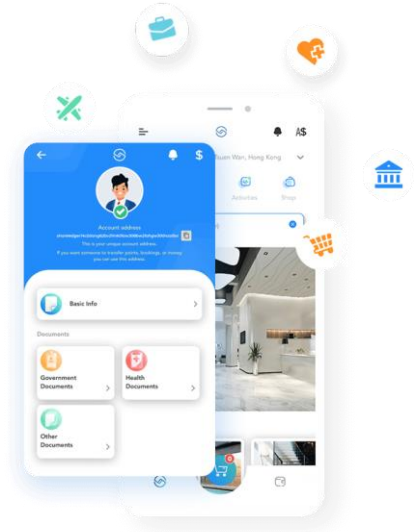


Figura 16. Fuente: trustwallet

### 2.3.4 El Exchange

Para poder obtener una criptomoneda es muy importante saber cómo comprarla y qué hacer con ella. Para adquirir la moneda, necesitas un Exchange (plataforma de intercambio) en el cual haya gente que la venda entonces tú se la compras. Este proceso es automático, no es



Figura 17. Fuente: xataka

necesario contactar con una persona para poder comprarla sino, que hay un gran libro de órdenes para cada criptomoneda el cual guarda toda la información. Cuando una o varias personas ponen a la venta criptomoneda, el libro de ordenes lo anota y cuando otra persona la compre, se transferirá la criptomoneda del vendedor a tu wallet y la divisa que se haya utilizado para la compra, se la quedará el vendedor.

En un mismo Exchange no se puede comprar todas las criptomonedas que existen, ya que no todas están listadas en todas. Normalmente, las más conocidas sí que suelen estar en los exchanges más famosos, pero para obtener altcoins poco conocidos, se debe buscar diferentes formas para comprarlos.

El exchange más conocido y utilizado por la gente es Binance, ya que es el más completo y el que ofrece más características, pero como se ha comentado anteriormente, no se encuentran todas las criptomonedas listadas.

Para poder utilizarlo, es necesario saber qué es y para qué sirve cada apartado.

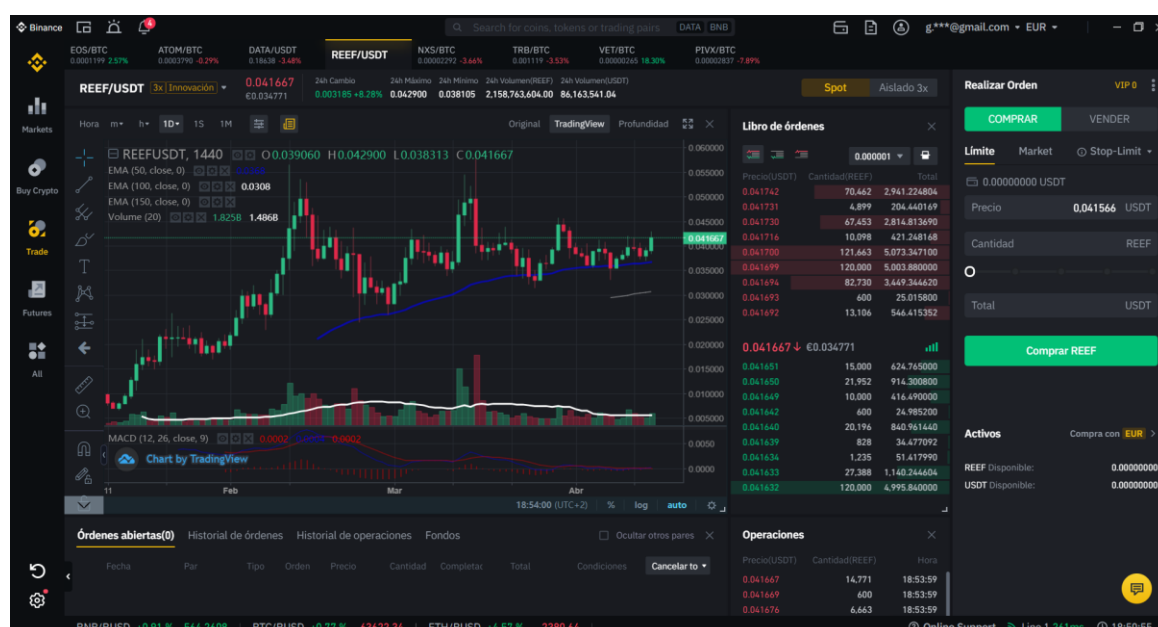


Figura 18. Fuente: elaboración propia

En la imagen se representa el panel principal en el momento de adquirir alguna criptomoneda. En este caso utilizaremos la criptomoneda REEF, con el par REEF/USDT, esto significa que para poder comprar REEF se necesita de la criptomoneda USDT. En la parte principal se puede ver la gráfica de la criptomoneda en cuestión la cual muestra la fluctuación del precio con las velas japonesas. La derecha se puede ver el libro de ordenes el cual muestra, por cada precio, cuántos USDT, lo mismo que dólares, han puesto o están dispuestos a pagar cuando llegue a ese precio.

A la derecha del todo ya se puede ver la parte de compra y venta de criptomonedas.

Para conseguir beneficios con tus criptomonedas, existen varias formas:

Consiste en que, en pequeños periodos de tiempo, se compra, una moneda a un bajo precio y cuando sube un pequeño porcentaje, se hace la venta de esta. Esto consiste en repetir este proceso varias veces.

## Holding

Considero que es la mejor opción el holding, ya que no es algo que debas hacer diariamente para así poder sacar un buen beneficio. Sino que es algo que al principio debes investigar mucho pero más tarde lo único que debes hacer es dejar que fluctúe el mercado y ver lo que sucede. Pero está claro, que no hay una opción que te dé más chance de ganar la operación.

### **3 Marco Práctico**

La parte práctica se divide en 3 partes. La primera parte es la realización de una entrevista para profundizar conceptos, la segunda parte se basa en las diferentes inversiones y su análisis y la tercera parte creo el prototipo de mi criptomoneda.

#### **3.1 Entrevista Carlos Flores**

Esta entrevista se va a basar en las criptomonedas tanto en el ámbito de la inversión como en el de la minería. El entrevistado, llamado Carlos Flores, lleva en el ámbito de las criptomonedas desde 2015. Su participación se basa mayoritariamente en la minería. La principal fuente de la cual empezó a escuchar de estas criptomonedas fue en la televisión, en concreto en el Big Bang Theory.

##### **¿Qué valor tienen las criptomonedas?**

Si tú por ejemplo tienes mil euros en el banco quien confirma que tú tienes ese dinero, un ordenador. Y si tú tienes una criptomoneda, quien da fe de que tienes esa cantidad son los mineros, cuando tú transfieres una criptomoneda muchos ordenadores confirman esa transacción. Normalmente estas transacciones constan de 14 confirmaciones que se deben efectuar antes de que esta llegue al destinatario. Por ejemplo, si una compañía de vuelos tiene habilitada la forma de pago de criptomonedas, lo que harían sería pedir un mínimo de 14 confirmaciones antes de que la compra se haya llevado a cabo.

##### **¿Qué opinas de que las criptomonedas no estén regularizadas por ningún gobierno?**

Como las criptomonedas no son controladas por ninguna institución ni gobierno, se pueden utilizar como forma de evadir de los impuestos o para el traspaso del dinero “sucio”. Pude comprar una casa con Bitcoins.

### **¿Cuál ha sido tu inversión?**

Mi principal inversión es la minería, la inversión directamente en las criptomonedas es mera especulación ya que no puedes predecir que va a pasar con ellas, en cambio con la minería sí que sabes la inversión que te va a devolver en un tiempo.

### **¿Qué te parece utilizarla como forma de pago?**

A diferencia de las divisas, estas no se pueden devaluar por el gobierno, sino que quien las controla es el mercado. En Argentina, un día puedes pensar que un cierto dinero te llega para unas alubias, pero al día siguiente puede ser que necesites diez veces eso.

### **¿Cómo empezaste en la minería?**

Para poder empezar a minar me puse a buscar, y primero encontré un hardware llamado asick que sirve únicamente para minar la criptomoneda bitcoin. Pero en ese momento ya estaba bastante saturado. Entonces me fui para las tarjetas gráficas ya que era una inversión más estable y si no funciona bien se pueden vender casi al mismo precio perfectamente. Al principio tenía problemas para configurarlas ya que debía medir el calor de cada una, y a la hora de hacer overclock debía encontrar que frecuencias eran las correctas.

Empecé minando ZCash, pero a los tres meses me cambió al Ethereum ya que era mucho más eficiente. Mi actual instancia de esta minería es en una especie de hangar el cual tiene paneles solares y así no gasta nada en electricidad.

Una cosa muy importante es el momento en el cual lo cambias a dinero, ya que al comenzar puedes ganar una cierta cantidad, pero en unos días puede devaluarse ese valor o viceversa.

### **Conclusión**

Esta entrevista se ha basado principalmente en la minería de criptomonedas. Por eso en ese ámbito he aprendido bastantes cosas nuevas y me ha hecho cambiar la manera de ver esta forma de inversión.

## 3.2 Inversión en criptomonedas

Como segunda parte práctica, he optado por invertir una cierta cantidad de dinero en diferentes criptomonedas las cuales he investigado cuidadosamente. Estas inversiones las comencé a principios de febrero de 2021 y tengo previsto no convertirlas en dinero hasta febrero de 2022. También tengo inversiones que ya han acabado porque son de muy corto plazo, como horas. En esta parte del TR podemos el análisis y ver el progreso que han tenido estas inversiones. Es importante destacar que mis inversiones principalmente son en tokens los cuales tienen una empresa o una idea detrás.

### 3.2.1 ShareRing

#### ¿Qué es? (Información extraída de la página oficial de ShareRing)

“ShareRing ha sido pionera en una plataforma basada en blockchain que puede almacenar su identidad digital y documentos clave. Con su bóveda de información personal excepcionalmente segura, puede guardar documentos como su pasaporte, identificación nacional, licencia de conducir, resultados de pruebas COVID y certificados de vacunación, con la seguridad de que solo usted decide cómo y cuándo se accede a ellos o se usan. Con su ID de ShareRing, tendrá acceso al ecosistema de cadena de bloques más completo para acceder y comprar de forma segura bienes y servicios en todo el mundo, al servicio de industrias desde viajes hasta seguros, atención médica, logística, educación, criptomonedas, caridad y más. “

Principalmente, me llamó la atención la nueva aplicación que están desarrollando a partir de la propia criptomoneda SHR. Esta pretende funcionar como billetera digital en la cual puedas guardar tus SHR. Y no solo funciona como cartera de criptomonedas, sino que también puedes guardar todos tus documentos fiscales.

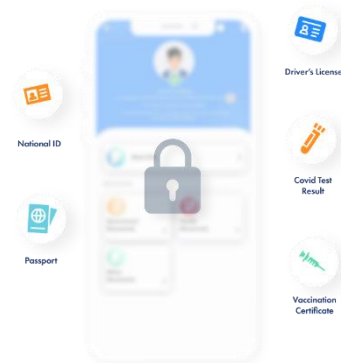


Figura 19. Fuente: TrustWallet

## ¿Cómo invertir?

Para poder invertir en SHR hay que utilizar un Exchange llamado Binance DEX, es uno poco conocido ya que es donde van las criptomonedas que no tienen mucho peso en el mercado. Para poder empezar a cambiar tu dinero en criptomoneda, necesitas descargarte la cartera Trust Wallet, que es donde se podrán guardar las otras criptomonedas para así poder hacer un intercambio. Entonces lo único que se tiene que hacer es conectar la wallet con Binance DEX. Cuando ya tenemos todo conectado, lo único que hay que hacer es intercambiar SHR por alguna criptomoneda que tengas, yo por ejemplo utilizo la criptomoneda USDT.



Figura 20. Fuente: Binance



Figura 21. Fuente: TrustWallet

## Información de la moneda en el momento de la inversión

*Capitalización de mercado (Dinero total invertido):* 91,978,079.09\$

*Volumen de comercio (Dinero que se ha intercambiado):* 1,772,644.98\$

*Fecha de inversión:* 22/02/21

*Precio de la compra:* 0,031\$

*Cantidad de SHR:* 3220

*Cantidad invertida:* 100€

## La inversión y su progreso



Figura 22. Fuente: [tradingview.com](https://tradingview.com)

Esta es la gráfica del precio de SHR donde se puede ver cómo el precio va subiendo y bajando a medida que pasa el tiempo. El momento en el cual invertí se puede ver marcado por un rectángulo. En cuanto hice la inversión, hubo unos días bastante tranquilos, pero llegó un día en el cual se empezó a disparar, llegó hasta un máximo histórico (un precio el cual nunca había llegado) de 0,096\$. En ese momento llevaba un beneficio del 300%, es decir, aproximadamente mis 100€ se habían convertido en 300€. A partir de esa subida el precio empezó a estabilizarse, entonces decidí vender de esos 540SHR al precio de 0,091\$ y con ello asegurarme 50€. El precio bajo un poco y entonces decidí volver a invertir esos 50€ en la misma moneda al precio de 0,083\$ y con ello sacarme 230SHR, entonces así me quedé con 3450SHR, con esta pequeña operación (duro aproximadamente un día) saqué un beneficio de unos 35€ (a toda esta operación se le denomina “trading”). A partir de ahí, ya no hice más operaciones y la deje en la billetera. Por el mes de abril la moneda empezó a caer hacia antiguos precios (caída la cual tiene una causa y la explicaré en el último apartado de esta parte práctica).



Sobre el mes de junio es cuando la moneda bajó hasta un precio el cual hacía tiempo que no tocaba. En ese momento, yo llevaba una pérdida de aproximadamente el 50%, es decir, unos 50€, pero en ese momento no me preocupaba porque sabía que la moneda era fuerte y con futuro, ya que toda esta bajada era una bajada general de todo el mercado.

Después de unos meses que estuviese en mínimos, se puede ver como vuelve a coger fuerza y ya vuelve a tocar ese precio el cual había hecho la compra de la criptomoneda.

### 3.2.2 Unitrade

#### ¿Qué es? (Información extraída de la página oficial de Unitrade)

“La característica principal de la plataforma, y el inicio de la plataforma UniTrade, es la capacidad de automatizar operaciones estableciendo órdenes de límite y stop loss para casi todos los tokens ERC-20 (Tokens creados a partir de Ethereum) y BEP-20 (Tokens creados a partir de Binance) . Esto está auditado y completamente protegido, y los usuarios no necesitan una cuenta o KYC (Control para verificar que tienes 18 años

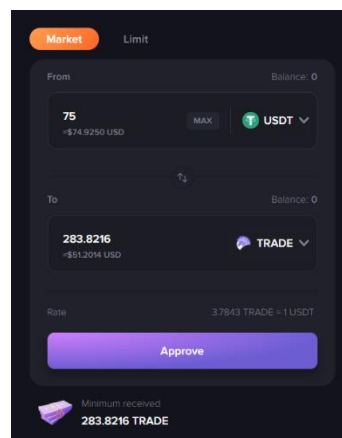


Figura 23. Fuente: Unitrade

o más) para acceder a él. Otras características de la plataforma UniTrade incluyen: granjas de rendimiento con APY actual y retornos esperados, y ofertas agrícolas iniciales (IFO) para los titulares de TRADE; plataforma de apuestas para ganar ETH y BNB para los titulares de tokens TRADE; La plataforma de lanzamiento UniTrade IDO que presenta proyectos examinados y de alta calidad; lotería con ganancias diarias y semanales en ETH y BNB; acuñación y comercialización de nuevos NFT en el portal de creación de UniTrade; UniTrade Exchange, su DEX que se basa en proporcionar la mejor experiencia de usuario. (Esto en resumen es el staking que anteriormente había hablado)”

Lo que me llamó principalmente la atención fue su página web V.2 que estaba en desarrollo la cual va a implementar muchas funciones nuevas para así poder hacer más fácil la compra de la moneda Unitrade. También prometían añadir nuevas funciones de staking para así poder hacer beneficios pasivamente.

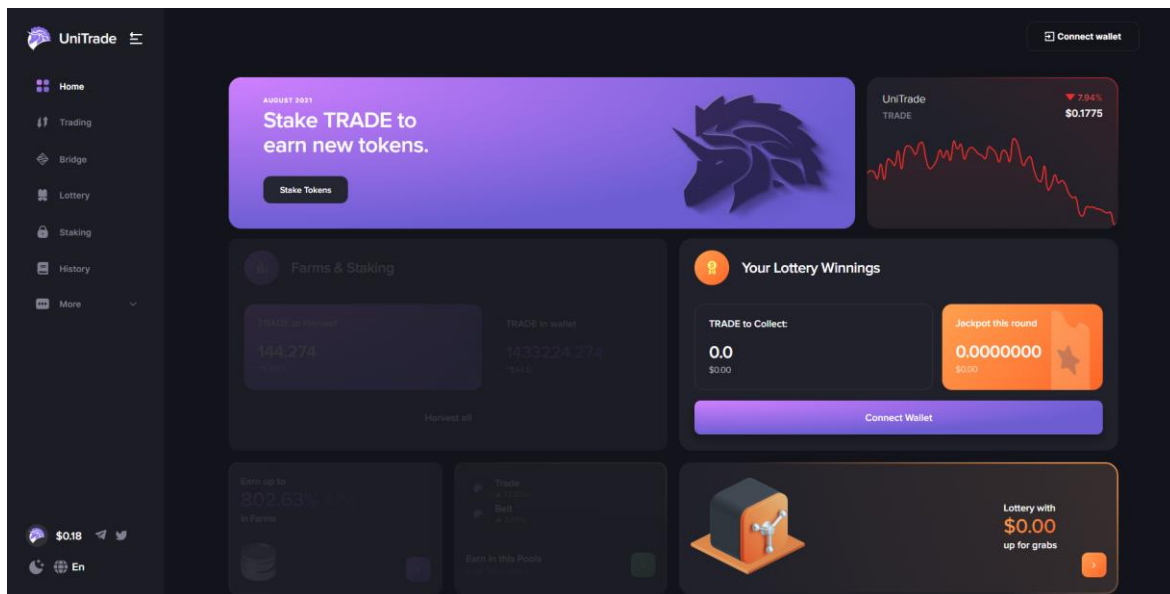


Figura 24. Fuente: Unitrade

## ¿Cómo invertir?

En estos momentos hay dos maneras de invertir en Unitrade, cuando yo hice mi inversión solo había una ya que la página web todavía estaba en desarrollo. Para las dos maneras necesitas tener una wallet con tu moneda preferida de intercambio, yo por ejemplo siempre tengo USDT. A partir de ahí, hay dos caminos:

- Puedes conectar tu wallet a la página oficial de Unitrade y así hacer el intercambio y, a parte de intercambiar podrás utilizar todas las funciones de la página web: staking, stoploss y order limit.
- Puedes conectar tu wallet a la página de Uniswap que es una página de intercambios de miles de monedas las cuales no están listadas en exchanges conocidos.

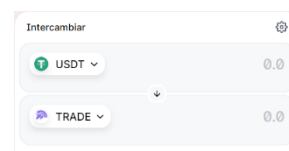


Figura 23. Fuente: Unitrade

### Información de la moneda en el momento de la inversión

*Capitalización de mercado (Dinero total invertido): 18,562,043.12\$*

*Volumen de comercio (Dinero que se ha intercambiado): 1,383,237.17\$*

*Fecha de inversión: 03/03/21*

*Precio de la compra: 0,31\$*

*Cantidad de TRADE: 136,49*

*Cantidad invertida: 55,34€*

## La inversión y su progreso



Figura 25. Fuente: [tradingview.com](https://tradingview.com)

Esta es la gráfica del precio de Unitrade donde se puede ver como el precio va subiendo y bajando a medida que pasa el tiempo. El momento en el cual invertí se puede ver marcado. Ya llevaba tiempo escuchando sobre esta moneda ya que se estaba haciendo bastante famosa. Y hasta que no anunciaron que iban a lanzar la nueva web de trading no me dispuse a invertir. En cuanto invertí, por el precio de 0,31\$, esta empezó a bajar ya que hubo una falsa alarma de que esta moneda era una estafa ya que uno de los CEO tuvo unos problemas fiscales hace tiempo.

Llegó a bajar un 20% el precio respecto al que yo compré, pero a partir de ahí se disparó hasta el precio de 0,9\$, con esa subida llevaba aproximadamente una subida del 200%, es decir, había duplicado mi inversión inicial. Pero hay una cosa que los traders siempre dicen y es que nunca has ganado hasta que vendes. Y efectivamente fue así, yo no vendí nada. Entonces, al cabo de un mes y medio, el precio empezó a bajar por un conjunto de cosas: la salida de la página web se retrasó y hubo una bajada general en todo el mercado, cosa que ya explicaré más adelante. El precio llegó hasta 0,15\$ y se estabilizó por ese precio, en el cual yo llevaba una pérdida aproximada del 50%. Ya más tarde, por el mes de junio se lanzó oficialmente la nueva página web con casi todas las funciones listas para usarlas, pero a pesar de esa gran noticia, el precio no subió y se ha mantenido estable desde entonces.

### **3.2.3 Cardano**

#### **¿Qué es? (Información extraída de la página oficial de Cardano)**

“Cardano está construido por una comunidad descentralizada de científicos, ingenieros y líderes de opinión, unidos en un propósito común: crear una plataforma tecnológica que encenderá el cambio positivo que el mundo necesita. Creemos que el futuro no debe definirse por el pasado y que es posible hacer más y que, a través de la tecnología, puede ser posible para todos. Medimos el valor de una tarea no por su desafío, sino por sus resultados. Cada poseedor de ADA (Cardano) también tiene una participación en la red Cardano. Ada almacenada en una billetera se puede delegar a un grupo de participación para ganar recompensas, para participar en el funcionamiento exitoso de la red, o comprometerse a un grupo de participación para aumentar la probabilidad de que el grupo reciba recompensas. Con el tiempo, ADA (Cardano) también se podrá utilizar para una variedad de aplicaciones y servicios en la plataforma Cardano. “

Lo que principalmente me llamó la atención esta moneda fueron dos cosas. La primera es todos los proyectos para futuro que tienen, ya que son un gran grupo de trabajadores con grandes ideas.

Y segundo, me llamó la atención la gran cantidad de gente que invertía en esta moneda, esto me creó mucha seguridad y confianza en esta moneda.

### ¿Cómo invertir?

Esta criptomoneda es muy conocida y gracias a eso esta listada en la mayoría de exchanges más conocidos. Por esa razón la dificultad de invertir en esta moneda es casi nula. Lo único que debes hacer es entrar a la página oficial de Binance y registrarte con tu email. A partir de ahí



Figura 26. Fuente: Binance

ya puedes acceder a la zona de compra de criptomonedas y utilizar tu forma de pago preferida.

### Información de la moneda en el momento de la inversión

*Capitalización de mercado (Dinero total invertido):* 54,520,954,211.23\$

*Volumen de comercio (Dinero que se ha intercambiado):* 6,630,813,227.73\$

*Fecha de inversión:* 21/02/21

*Precio de la compra:* 1,05\$

*Cantidad de ADA:* 110,74 + 51,32

*Cantidad invertida:* 100€ + 43€

## La inversión y su progreso



Figura 27. Fuente: tradingview.com

Esta es la gráfica del precio de ADA donde se puede ver como el precio va subiendo y bajando a medida que pasa el tiempo. El momento en el cual invertí se puede ver marcado. Llevaba un tiempo pensando en invertir o no, ya que esta moneda había subido ya bastante. Pero empecé a escuchar más sobre ella y, además los trabajadores de cardano anunciaron nuevos proyectos que venían. Entonces decidí invertir la cantidad de 100€ al precio de 1,05\$. Después de esa inversión, el precio estuvo subiendo y bajando levemente, hasta que llego un día el cual explotó ya que la moneda empezó a salir por varios sitios de comunicación provocando que más gente invirtiese, y lo que llevó a que el precio subiese aún más. Sobre el mes de mayo llegó a un máximo histórico de 2\$ lo que indicaba que aproximadamente había doblado mi inversión. Seguidamente, el precio se desplomó, algo totalmente normal e incluso sano para el precio. Esta moneda había subido mucho en muy poco tiempo lo cual indicaba que en algún momento esta subida debía acabar y así la moneda hacer una corrección.

Ya después de la caída, cuando el precio se estabilizó un poco, decidí invertir algo más de dinero, 43€, al precio de 1,23\$ ya que creía mucho en este proyecto.

Después de unos dos meses de grandes bajadas y correcciones, la moneda recupero, y empezó a escalar. Llego al máximo histórico de 2,85\$ lo cual indica que, si en ese momento hubiese vendido las dos inversiones, hubiese sacado un beneficio de aproximadamente 400€.

## Conclusión

Desde que me interese sobre las criptomonedas queria empezar a invertir y este trabajo me dio esa fuerza a seguir adelante. Con todas las inversiones a corto y a largo plazo he aprendido mucho sobre el mercado y sobre como analizarlo. Y la parte que sinceramente veo mas importante, es que he sacado beneficios con el dinero que inverti haciendo algo que me gusta. A continuacion dejare una tabla en forma de resumen del progreso de las inversiones.

	FECHA DE INVERSION - 14/02/2021		GUIDO BIOSCA
	PRECIO DE COMPRA	PRECIO DE 31/08/2021	PORCENTAJE
SHARETOKEN  SHR  98,56€	0.31\$	0.89\$	+187%
JULSWAP  JULD  143€	0.31\$	0.19\$	-32%
UNITRADE  TRADE  45,32€	0.35\$	0.72\$	+104%
CARDANO  ADA  101,4€	1.04\$	2.75\$	+172%

### 3.3 La creación de una criptomoneda

En esta tercera parte práctica explicaré todos los pasos que hay que seguir para poder crear una criptomoneda y, junto a ellos iré creando la mía. Cabe destacar que la criptomoneda que crearé para esta parte práctica se basará en una red “ficticia”. Todos los pasos que deberé seguir serán idénticos. La única diferencia es que todo el dinero que se debe ingresar para la creación será totalmente falso. Ya que para la creación de una criptomoneda se necesita de bastante capital. De esta forma, después de aprender a crear una criptomoneda a partir de un dinero falso, se podría crear una moneda totalmente verdadera que esté lista para salir al mercado.

#### 3.3.1 Idea Principal

Como ya he explicado anteriormente, la moneda que creare a medida que vaya aprendiendo como crear una criptomoneda, estará basado en una red paralela la cual es “falsa”, una testnet. Pero los planes que quiero hacer en un futuro con mi criptomoneda serán totalmente los mismos.

La parte principal de mi criptomoneda es que traiga algo positivo para nuestro planeta. Después de pensar, me decanté por las energías renovables ya que son algo muy importante ahora mismo.

Por esa razón, quiero que una gran parte del dinero que recaude la criptomoneda (función que explicaré más adelante), restando el capital necesario para que la criptomoneda siga funcionando correctamente, vaya dirigido a la creación de nuevas fuentes renovables.



Figura 28. Fuente: ecology



### 3.3.2 La red

Antes de empezar con la creación de tu propia criptomoneda debes elegir en qué red o blockchain va a estar basada tu moneda. Existen miles de redes las cuales funcionan a la perfección, pero hay unas que son más utilizadas que otras. Yo principalmente tengo dos preferidas: la red de Ethereum y la de BinanceSmartChain. Ethereum tiene un inconveniente y es que el coste por cada transferencia es elevadísimo, hay casos en los que si envías 20\$ a un amigo, el coste de transferencia es de 21\$, por lo que cuesta más la transferencia que el dinero que envías. Por esa razón, finalmente me decanto por la red BEP-20 (la red de Binance). La red de Binance me fascina principalmente por el coste de sus transferencias, que es casi nulo. Esta red funciona de una manera diferente a las demás, ya que para poder hacer una transferencia necesitas de su moneda oficial, BNB (BinanceCoin). Para entenderlo mejor podemos ver a BNB como la gasolina de un coche. El coche para poder ir hacia una ubicación necesita de gasolina, pues con las transferencias es igual, tu envías una criptomoneda basada en la red de Binance y el requisito que te pide es un poco de BNB.

### 3.3.3 La creación

Para comenzar, lo primero que se debe hacer es crear una billetera para poder conectar la criptomoneda. Para ello, utilizaré metamask ya que con esta billetera puedo crear la testnet (la red falsa). Cuando ya se crea la testnet, lo único que se ha de hacer es ir a la página oficial de Binance y añadir dinero “falso” a la billetera. Yo, por ejemplo, he añadido 1BNB que son aproximadamente 300€. Con este capital ya podremos crear la criptomoneda a nuestro gusto.

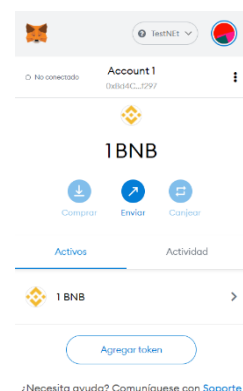


Figura 29. Fuente: TrustWallet



Cuando ya tenemos todos los puntos esenciales configurados, lo único que hay que hacer es compilar los datos, para ello utilizaré el compilador remix de Ethereum.

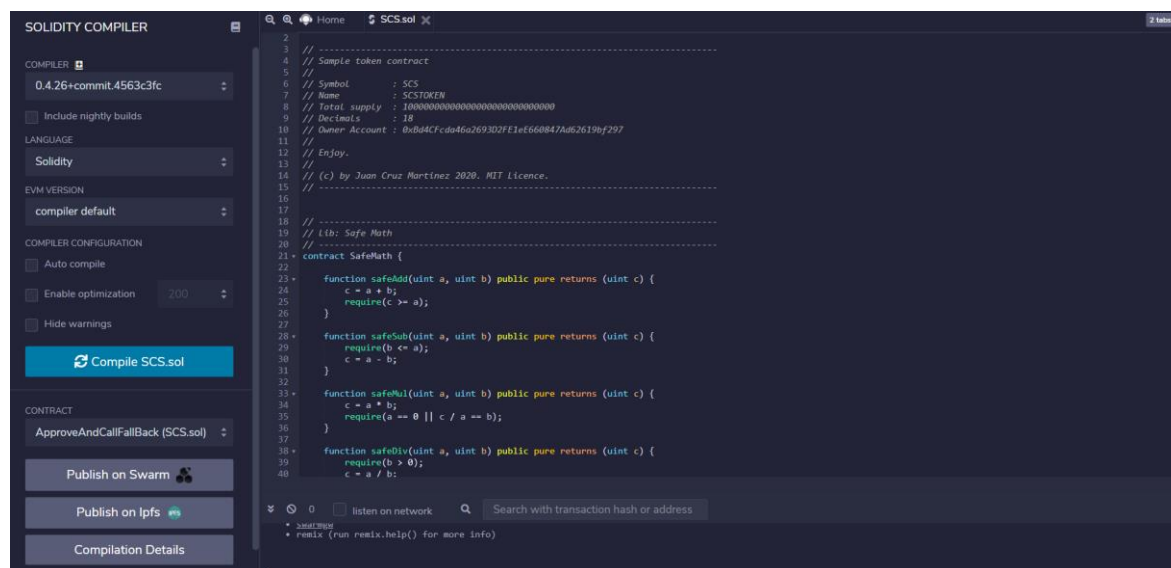


Figura 30. Fuente: elaboración propia

Cuando ya compilamos todos los datos, hay que hacer que estos datos salgan al mercado y a la red BEP20. Para eso, tenemos que pagar una comisión para que se efectúe.

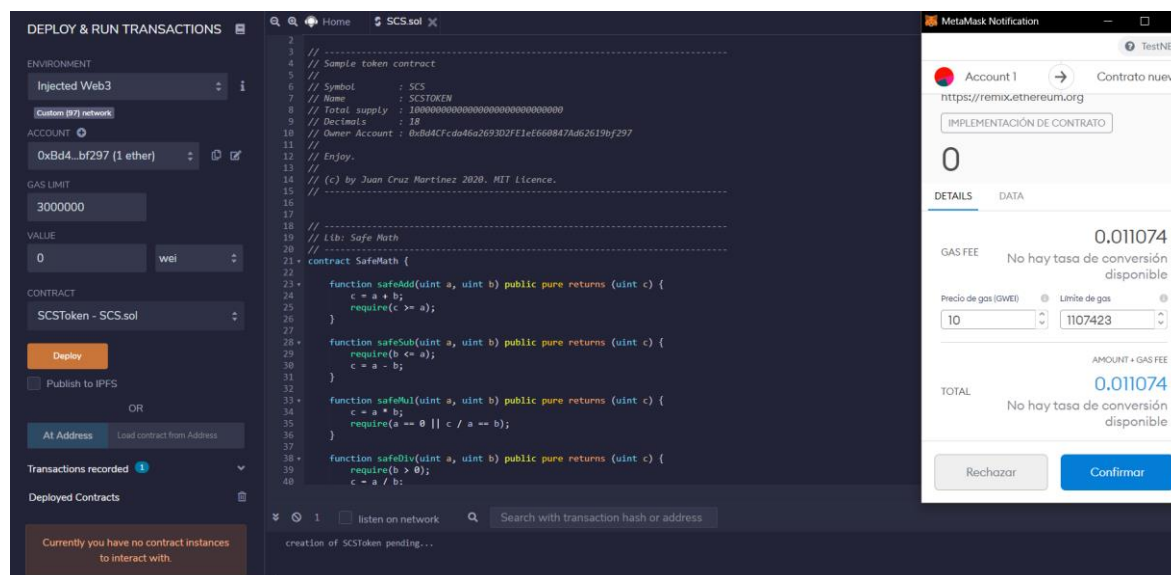



Figura 31. Fuente: elaboración propia

Una vez pagada la comisión que nos piden, ya estará lista en el mercado. Nos soltará una dirección de mercado la cual es la dirección principal para poder intercambiar con ella.

Dirección Token: **0xbDe8746F9E51ac0F37041D8b202969C6d6CE3ec7**


BSC Testnet Network

All Filters
Search by Address / Txn Hash / Block / Token

Home
Blockchain
Validators
Tokens
Resources
Misc
Testnet

Contract 0xbDe8746F9E51ac0F37041D8b202969C6d6CE3ec7

**Contract Overview**

Balance: 0 BNB

**More Info**

My Name Tag: Not Available

Contract Creator: 0xbd4cfda46a2693d2fe... at bn 0xb4884e2123cc5b4311...

Token Tracker: SCSTOKEN (SCS)

Transactions
Contract
Events

Latest 1 from a total of 1 transactions

Txn Hash	Method	Block	Age	From	To	Value	[Txn Fee]
0xb4884e2123cc5b4311...	0x60806040	11900098	5 mins ago	0xbd4cfda46a2693d2fe...	IN Contract Creation	0 BNB	0.01107423

Download CSV Export

Figura 32. Fuente: elaboración propia

De esta forma, la criptomoneda ya estaría creada y lista para su funcionamiento.

## 4 Conclusión

Para acabar, he de concluir si mi hipótesis planteada al principio del trabajo es cierta o no y porque y también sobre mis partes prácticas.

En la hipótesis (¿Llegaran las criptomonedas a sustituir la forma de pago convencional?), después de ya haber investigado a fondo y haber hablado con expertos de este ámbito, pienso que la criptomoneda si va a sustituir a la moneda convencional. Una de las primeras razones es la seguridad y la fiabilidad, ya que el dinero que tienes en el banco de tu país, de un día para otro se puede devaluar, como lo que paso en Venezuela que se quitaron hasta 6 ceros al precio de la moneda. Está claro que esto en las criptomonedas no pasa ya que el precio no está controlado por una persona o un grupo de personas, sino que está controlado por todo el mercado en general. Y, por otra parte, las criptomonedas cada vez se están utilizando más como forma de inversión eso lo que quiere decir es que cada vez más gente se está adentrando en este mundo y con ello pone gran cantidad de su dinero. Con esto quiero decir que llegara un día en que prácticamente la mayoría de la población tendrá su dinero almacenado en sus billeteras y distribuido por las diferentes criptomonedas y eso llevara a que en cada vez más sitios se acepte la forma de pago de criptomoneda. Sobre el objetivo que me puse de poder conocer más a fondo la criptomoneda y todo lo que le lleva a ser posible, puedo decir que he aprendido mucho e incluso más de lo que esperaba. Me he dado cuenta del inmenso mundo que hay detrás de las criptomonedas, ya que se divide en miles de partes diferentes que constituyen la criptomoneda. Si que es verdad que me quedan cosas por aprender ya que es un largo camino.

Respecto a las partes prácticas, con la entrevista he podido conocer a una persona que lleva ya tiempo metido en el ámbito de las criptomonedas y con ello poder aprender muchas cosas nuevas. La verdad es que me hacía bastante ilusión tener frente a frente con una persona tan experimentada. Sobre todo, me impresiono el tema de que podía llegar a vivir de la minería, de ingresos pasivos.

Con la práctica de las inversiones puedo decir que es en la que más me he divertido y más he podido aprender. A parte de poder conocer el mundo de las criptomonedas, me he podido adentrar y formar parte de ella. Con las inversiones he podido llegar a aprender desde como encontrar una buena empresa o token hasta como poder analizar una gráfica. Y a parte de todo lo que he aprendido he podido llegar a sacar unos beneficios bastante buenos. A día de hoy, haciendo un resumen de todas las inversiones, he sacado aproximadamente un 400% de beneficio, estamos hablando de que mi inversión total inicial, se ha multiplicado por cuatro.

Y, por último, la creación de una criptomoneda. Desde un principio creí que no podría llegar a crearla ya que se necesita de muchas bases y de bastante capital. Pero, después de aprender bastante sobre las partes más importantes para crearla y con ayuda externa. La he podido crear, pero cabe destacar que la creación fue en una red virtual, es decir, que no tuve que gastar de mi dinero real. Pero gracias a aprender a crearla, ya estoy listo para el día que tenga todo organizado y tenga más tiempo, poder crearla en una red verdadera.

## 5 Limitaciones y prospectiva

La tecnología de seguridad ha permitido el desarrollo de un sustituto de la moneda tradicional. Desde un punto de vista de seguridad permite transacciones garantizando el origen y destino de todas ellas. Con ello puedes realizar un registro de todos los movimientos. Por lo tanto, puede cumplir con las necesidades básicas de una moneda eliminando también la necesidad de intermediarios y así como de los gastos de intermediación y control externo.

El hecho de que no exista una autoridad central significa que estas monedas no pueden ser controladas por los gobiernos y esto ha provocado que estas monedas se presten a la especulación o que se refugien algunos capitales de orígenes inciertos. Estas inversiones masivas provocan que exista mucha volatilidad y por lo tanto también mucho interés por especular con el valor de la moneda. Como vimos la moneda no tiene ningún valor intrínseco ni está respaldada por ningún activo (como por ejemplo el oro)

Un ejemplo es Tesla que a través de Elon Musk decide invertir en Doge, lo publica en internet y en los días posteriores la moneda sube como la espuma. En poco tiempo el Bitcoin ha pasado de 9.000€ a 48.000€. Esto es claramente una burbuja especulativa como ocurrió con los tulipanes en Holanda. Por otro lado, Tesla ya incorpora la posibilidad de comprar coches con este tipo de moneda, o Messi permite que parte de su ficha se pague con criptomoneda, con lo que se está extendiendo su uso en el mundo empresarial.

El caso de Tesla se contradice con la idea fundacional de la empresa que pretende un mundo más limpio (al utilizar baterías frente combustibles fósil) pero permite el uso de una moneda que requiere una ingente cantidad de energía para mantener las operaciones (ya vimos que las operaciones están consumiendo energía como toda Holanda).

Así, desde un punto de vista de inversión, tenemos una moneda que está extendiendo su uso por lo que ha crecido su valor, pero está basado en pura especulación y tiene mucha volatilidad. Creo que la moneda poco a poco extenderá su usabilidad en muchos negocios y países y será cuando se establezca una regulación que permita a los gobiernos controlar su uso.

## **Referencias bibliográficas**

- Academy, B. (2020). *¿Qué es la criptografía de clave pública?* Binance Academy. <https://academy.binance.com/es/articles/what-is-public-key-cryptography>
- Aldekoa, J. (2020). *Oferta monetaria, inflación y señoreaje*. Instituto Juan de Mariana. <https://juandemariana.org/ijm-actualidad/analisis-diario/oferta-monetaria-inflacion-y-senoreaje/>
- Arias, A. S. (2020). *Ley de oferta y demanda*. Economipedia. <https://economipedia.com/definiciones/ley-de-oferta-y-demanda.html>
- *Cardano is a decentralized public blockchain and cryptocurrency project and is fully open source*. (2018). Cardano. <https://cardano.org/>
- *CoinGecko: Cryptocurrency Prices and Market Capitalization*. (2013). CoinGecko. <https://www.coingecko.com/en>
- CoinMarketCap. (2015). *Cryptocurrency Prices, Charts And Market Capitalizations*. <https://coinmarketcap.com/>
- *Cryptocurrency Converter and Calculator Tool*. (2015). CoinMarketCap. <https://coinmarketcap.com/converter/>
- *Cryptocurrency List*. (2018). CoinLoop. <https://coinloop.io/cryptocurrency-list>
- *cryptovest.com | 520: Web server is returning an unknown error*. (2019). Cryptovest. <https://cryptovest.com/>
- Figuera, A. J. L. (2020). *CRIPTO TENDENCIA - Todas las criptomonedas en un solo lugar*. CRIPTO TENDENCIA. <https://criptotendencia.com/>
- *¡Habla claro!* (2016). SEGURIDAD INFORMÁTICA. <https://seguridadinformatica1com.wordpress.com/practica-3-2/>
- *Lightning Network*. (2020). Lightning Network. <https://lightning.network/>



- Lynn, M. (2020). *Las lecciones de la «burbuja puntocom» veinte años después.* elEconomista.es. <https://www.eleconomista.es/opinion-blogs/noticias/10313700/01/20/Las-lecciones-de-la-burbuja-puntocom-veinte-anos-despues.html>
- *LA MONEDA - Infogram.* (2017). Infogram. <https://infogram.com/la-moneda-1hzj4oq0lz072pw>
- Napolitano, A. C. (2016). *Los mejores exchange de criptomonedas.* Herramientas Bitcoin. <https://herramientasbitcoin.com/herramientas/exchange-de-criptomonedas/>
- Napolitano, A. C. (2017). *Las mejores pools de minería de Bitcoin y criptomonedas.* Herramientas Bitcoin. <https://herramientasbitcoin.com/herramientas/pools-de-mineria/>
- Napolitano, A. C. (2018). *Las mejores webs para seguimiento del precio de Bitcoin y criptomonedas.* Herramientas Bitcoin. <https://herramientasbitcoin.com/herramientas/seguimiento-del-precio/>
- *Noticias de Cointelegraph sobre blockchain, Bitcoin y Ethereum.* (2021). Cointelegraph. <https://es.cointelegraph.com/>
- Ortiz, S. (2017). *El tulipán que nunca floreció: la primera burbuja especulativa de la historia.* elEconomista.es. <https://www.eleconomista.es/economia/noticias/8244134/03/17/El-tulipan-que-nunca-floreccio-La-primera-burbuja-especulativa-de-la-historia.html>
- Pastor, J. (2018). *Qué es blockchain: la explicación definitiva para la tecnología más de moda.* Xataka. <https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>

- *El período de Entreguerras. Hiperinflación alemana.* (2018). Claseshistoria. <http://www.claseshistoria.com/entreguerras/periodocrisisalemania.htm>
- *ShareRing.Network | Open the world with ShareRing ID.* (2020). ShareRing.Network. <https://sharering.network/>
- T. (2015). *Historia del dinero: monedas y billetes.* Tinsa Tasaciones Inmobiliarias. <https://www.tinsa.es/blog/historia/historia-del-dinero-monedas-y-billetes/>
- *Unitrade Exchange.* (2020). Unitrade. <https://www.unitrade.app>
- Velasco, J. J. (2011). *La máquina Enigma, el sistema de cifrado que puso en jaque a Europa.* Hipertextual. <https://hipertextual.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa>
- Velasco, J. J. (2014). *Breve historia de la criptografía.* ElDiario.es. [https://www.eldiario.es/turing/criptografia/breve-historia-criptografia\\_1\\_4878763.html](https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html)
- *vitalik.eth (@VitalikButerin) | Twitter.* (2019). Vitalik Buterin. <https://twitter.com/VitalikButerin>