UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

LA MINERÍA EN CRIPTOMONEDAS

Trabajo de Fin de Grado

enviado por la Facultad

Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

por

Oriol Val Gangonells

En parcial cumplimiento de

los requisitos del grado de

Ingeniería en Sistemas y Servicios de Telecomunicación

Tutor: Francisco José Rico Novella

Barcelona, Enero 2020

Abstract

Some years ago, the world of the cryptocurrencies was not unreachable for anyone, but going through the years, this world has been popularized more and more. In this document, we have wanted to be focused in the privacy and mining process of the cryptocurrencies, explaining first a little background about how they treat and integrate the privacy into the transactions the user makes and how the mining is, in order to get mine any criptocurrency in different platforms, evaluating which it's better for earning benefits. Moreover, we have made a little review about how is the mining process nowadays and the effects that this process has with the environment, recognizing that we have a climatic emergency that we have to solve as a society.

Resum

Fa uns anys, les criptomonedes eren un tema molt desconegut pel món a peu, però a mesura que ha passat el temps, s'han anat popularitzant cada cop més. En aquest document hem volgut focalitzar-nos en la privacitat i el minat de les criptomonedas, explicant primer un petit *background* sobre com tracten i integren la privacitat a les seves transaccions i com és la seva mineria, per després aconseguir minar una criptomoneda en diferents plataformes i valorant la millor opció per aconseguir beneficis. A més a més, també s'ha fet una petita crítica a com es avui en dia el procés de minat i els efectes que aquest té sobre el medi ambient, reconeixent que avui dia hi ha una emergència climàtica que s'ha de resoldre.

Resumen

Hace unos años, las criptomonedas eran algo muy desconocido por el mundo a pie, pero a medida que pasa el tiempo se están popularizando cada vez más. En este documento hemos querido focalizarnos en la privacidad y el minado de las mismas, dando primero un pequeño *background* sobre cómo tratan e integran la privacidad en sus transacciones y cómo es su minería, para luego conseguir minar una criptomoneda en distintas plataformas y valorando la mejor opción para conseguir beneficios con dicho proceso. Además, también se ha hecho una pequeña crítica a cómo es hoy en día el proceso de minado y los efectos que este tiene sobre el medio ambiente, reconociendo que hoy en día hay una emergencia climática que debe resolverse.

Dedicatoria: Este trabajo lo dedico a mi familia, por ayudarme en todo lo que he necesitado en materia de educación.

Agradecimientos

Me gustaría dar las gracias y mi reconocimiento a Francisco José Rico Novella por asumir el reto de ser tutor de mi trabajo final de carrera y ayudarme en la consecución del mismo.

Historial de revisiones

Revision	Date	Purpose
0	26/12/2019	Creación del documento
1	25/01/2020	Primera revisión del documento

Tabla 1. Historial de revisiones

DOCUMENT DISTRIBUTION LIST

Name	e-mail
Oriol Val Gangonells	oriolvg@hotmail.com
Francisco José Rico Novella	f.rico@entel.upc.edu

Tabla 2. Document distribution list

Written by: Oriol Val Gangonells		Reviewed and approved by: Francisco José Rico Novella	
Date	25/01/2020	Date	dd/mm/yyyy
Name	Oriol Val Gangonells	Name	Francisco José Rico Novella
Position	Project Author	Position	Project Supervisor

Tabla 3. Participantes en el documento

Tabla de contenidos

Abstract 1
Resum 2
Resumen 3
Agradecimientos 5
Historial de revisiones 6
Tabla de contenidos 7
List of Figures 9
List of Tables: 10
1. Introducción 11
2. Estudio del arte sobre las criptomonedas 16
2.1. Bitcoin (BTC) 16
2.2. Ethereum (ETH) 17
2.3. Ripple (XRP) 19
2.4. Bitcoin Cash (BCH) 21
2.5. Litecoin (LC) 22
2.6. EOS (EOS) 24
2.7. Binance Coin (BNB) 25
2.8. Bitcoin SV (BSV) 27
2.9. Stellar (XLM) 29
2.10. Cardano (ADA) 31
2.11. Tron (TRX) 33
2.12. UNUS SED LEO (LEO) 34
2.13. Tezos (TEZ) 35
2.14. Monero (XMR) 36
3. Criptomoneda de mayor interés para su estudio 39
4. Minería de Monero 41
4.1. Ordenador con Linux 41
4.2. Ordenador con Windows 43
4.3. Raspberry Pi 48
5. Resultados 51
6. Costes 53
7. Impacto medioambiental 55

7.1. Método *Proof of Work* 55
7.2. Método *Proof of Stake* 56
7.3. Método *Algorand* 57
8. Conclusiones y desarrollo futuro 59
Bibliografía: 60
Glosario 63

Listado de Figuras:

1. **Figura 1.** Diagrama de Gantt inicial 14
2. **Figura 2.** Diagrama de Gantt final 15
3. **Figura 3.** Protocolo Ouroboros 31
4. **Figura 4.** Minado en Linux 41
5. **Figura 5.** Versiones software minado Windows 42
6. **Figura 6.** Redirección puertos en router 43
7. **Figura 7.** Minado en Windows 43
8. **Figura 8.** Configuración minado en Windows 44
9. **Figura 9.** Estado mining en Windows 45
10. **Figura 10.** Configuración proceso minado Raspberry Pi 47
11. **Figura 11.** AvalonMiner 1047 53
12. **Figura 12.** Red blockchain 60

Listado de Tablas:

1. **Tabla 1.** Historial de revisiones 6
2. **Tabla 2.** Document distribution list..... 6
3. **Tabla 3.** Participantes en el documento 6
4. **Tabla 4.** Workpackage 1 12
5. **Tabla 5.** Workpackage 2 12
6. **Tabla 6.** Workpackage 3 13
7. **Tabla 7.** Workpackage 4 13
8. **Tabla 8.** Milestones 13
9. **Tabla 9.** Costes totales..... 52

1. Introducción

Cada vez más el mundo de las criptomonedas está en auge y se está poniendo muy de moda. Mucha es la gente que opina sobre ello pero muy poca es la gente que realmente sabe de ello. Realmente, ¿qué quiere decir minar una criptomoneda? ¿Qué hay de privacidad en dichas transacciones?

Primero, en este documento se quieren despejar un poco las dudas de las preguntas anteriores, analizando las criptomonedas con más capitalización en el mercado poniendo el acento en la privacidad que cada una ofrece, para analizar si realmente estas criptomonedas son seguras; también se quiere analizar la minería de cada una de ellas y ver cómo este minado se regula y si realmente cumple con la filosofía inicial de las criptomonedas.

En segundo lugar, se quiere conseguir minar también la criptomoneda que más interés despierte, teniendo sobretodo en cuenta los aspectos de seguridad y minería expuestos en el apartado anterior. Para ello, se quieren hacer pruebas con distintos sistemas operativos y distintas máquinas. Primero, se probará en un ordenador portátil con el sistema operativo Windows, y luego se probará en una *Raspberry Pi 3* con un sistema operativo Debian. El objetivo de esta parte es ver si sale más a cuenta minar la criptomoneda con un ordenador más grande, o con más chips como la *Raspberry Pi* más pequeños.

Finalmente, también se quiere analizar el impacto medioambiental que este proceso de minado tiene en nuestro día a día. Cada vez más, el ser humano es más descuidado con el planeta, contaminando sin límites y no teniendo ningún tipo de interés en remediarlo. Para ello, el minado es un proceso que puede influir bastante en este ámbito, y en este documento se quiere hacer hincapié en ello.

Para desarrollar este proyecto, al inicio del mismo se hizo una planificación, que se ha intentado seguir con algunos imprevistos que también se van a comentar. Esta planificación constaba de unos *Work packages*, que se detallan a continuación:

<table>
<tr><td colspan="2">Project: Mining in Cryptocurrencies</td><td colspan="2">WP ref: 1</td></tr>
<tr><td colspan="2">Major constituent: Main documentation</td><td colspan="2">Sheet 1 of 1</td></tr>
<tr><td colspan="2" rowspan="2">Short description:
This work package is the most extensive and has the purpose of summarize the 15 cryptocurrencies with more capitalization in terms of privacy and mining, giving their pros and cons.</td><td colspan="2">Planned start date: 03/09/2019
Planned end date: 29/10/2019</td></tr>
<tr><td colspan="2">Start event: 03/09/2019
End event: 29/10/2019</td></tr>
<tr><td colspan="2">Internal task T1: Make a brief introduction of the cryptocurrency</td><td>Deliverables: 1</td><td>Dates:</td></tr>
</table>

Internal task T2: Make an explanation of the privacy and mining features Internal task T3: Valorate with pros and cons the interest that the cryptocurrency has in order to study it Internal task T4: Try to make an estimation about the environmental cost that the mining process has.		

Tabla 4. Workpackage 1

Project: Mining in Cryptocurrencies	WP ref: 2	
Major constituent: Select one cryptocurrency	Sheet 1 of 1	
Short description: Try to select one cryptocurrency among others and be able to argue why I have chosen this cryptocurrency	Planned start date: 01/11/2019 Planned end date: 10/11/2019	
	Start event: 01/11/2019 End event: 10/11/2019	
Internal task T1: Make an assessment to decide which cryptocurrency is better than others Internal task T2: Argue why I have chosen this information	Deliverables: 1	Dates:

Tabla 5. Workpackage 2

Project: Mining in Cryptocurrencies	WP ref: 3	
Major constituent: Software and Hardware	Sheet 1 of 1	
Short description: Be possible to compile a mining software of the cryptocurrency I desired and try to run into the OrangePi and in a Windows 10, in order to take conclusions about which is better.	Planned start date: 11/11/2019 Planned end date: 15/01/2020	
	Start event: 11/11/2019 End event: 15/01/2020	
Internal task T1: Download the source code about how	Deliverables:	Dates:

the mining works. Internal task T2:Compile it in the machine and in the Raspberry Pi and take conclusions about the performance.		

Tabla 6. Workpackage 3

Project: Mining in Cryptocurrencies	WP ref: 4	
Major constituent: Final documentation	Sheet 1 of 1	
Short description: In this workpackage we will finish the documentation, merging the information we collect in the two first workpackages and the information we collect with the third workpackage.	Planned start date: 01/01/2020 Planned end date: 26/01/2020	
	Start event: 01/01/2020 End event: 15/01/2020	
Internal task T1: Finish all the documentation Internal task T2:Make up all the work in order to deliver it	Deliverables:	Dates:

Tabla 7. Workpackage 4

Junto con los *Work packages* definidos arriba, se definieron también unas fechas límites de entrega para cada uno de ellos, organizando así el proyecto en distintas fechas límites para que no se juntara todo a último momento.

WP#	Task#	Short title	Milestone / deliverable	Date (week)
1	1	Brief introduction of cryptocurrency	NO	N/A
1	2	Explanation of privacy and mining features	NO	29/10/2019
1	3, 4	Pros, cons and environmental test of every cryptocurrency	YES	29/10/2019
2	1, 2	Assessment of which cryptocurrency is better and argue	NO	11/11/2019
3	1, 2	Download the source code and compile it to the Raspberry Pi	YES	15/01/2019

Tabla 8. Milestones

También, para una mejor comprensión y una ágil lectura, se elaboró también un conocido *Diagrama de Gantt*, donde se dibujan los anteriores *Work packages* en función de las fechas límites establecidas en la tabla anterior. Así, el *Diagrama de Gantt* que se estableció al inicio es el siguiente:

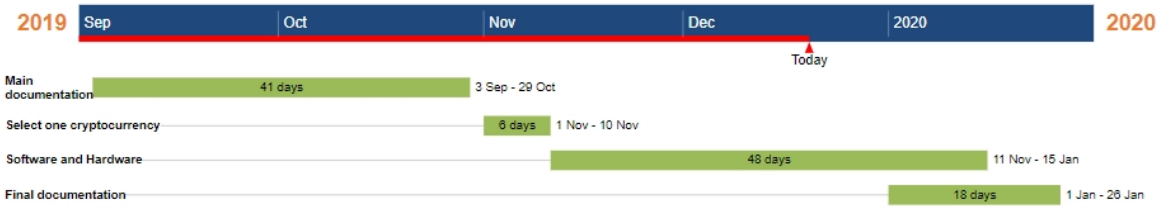

Figura 1. Diagrama de Gantt inicial

A pesar de esta organización que hubo des del principio, siempre salen contratiempos e imprevistos que hacen que no se lleguen a las fechas previstas o establecidas. En nuestro caso, podemos destacar las siguientes incidencias:

- Primero, afectó a este proyecto que a nivel personal y deportivo se añadieran nuevos objetivos a cumplir. Esto ha supuesto que mucho del tiempo libre que al principio se preveía no ha resultado ser tiempo libre, por lo que ha retrasado un poco las fechas límites comentadas arriba.
- En segundo lugar, un poco menos importante han sido diversos problemas que he tenido con el ordenador de trabajo. De repente, un día el ordenador dejó de funcionar durante un mes, que afortunadamente se resolvió.
- En tercer lugar, otro imprevisto con el que he tenido que lidiar es la falta de información sobre algunas criptomonedas o, lo peor de todo, la desinformación que circula por la red. Desde este trabajo me gustaría hacer una crítica a todas aquellas personas que quieren contribuir al conocimiento pero que, muchas veces sin saberlo, provocan que haya una desinformación subiendo conocimiento falso. Esto ha provocado que la información que podía encontrar en la propia red tuviera que ser verificada en numerosas ocasiones para no causar una incongruencia.
- Otro imprevisto con el que me he encontrado es la demora del pedido de la placa *Orange Pi PC Plus 2*. Tenía que ser un pedido normal por internet como cualquier otro pero, por algún motivo u otro, tardó más de dos meses en llegar.
- Finalmente, el último imprevisto con el que me he encontrado ha sido que esta *Orange Pi PC 2* no ha llegado con periféricos. Esto ha supuesto que, por mi parte y con un espacio de tiempo muy limitado buscara una fuente de alimentación para la placa. Esto finalmente no ha podido ser y se optó por comprar una placa *Raspberry Pi 3*, mucho más accesible y con muchos más recambios, consiguiendo así los objetivos planteados en este mismo documento.

Así, debido a estos imprevistos el diagrama de Gantt sufrió algún pequeño cambio. Para ilustrarlo, se actualizó el diagrama de Gantt, que es el mismo que se entregó junto con el documento *Critical_Review_cryp.docx*. Así, el diagrama final es el siguiente:

Figura 2. Diagrama de Gantt final

2. Estado del arte sobre las criptomonedas

En este apartado se va a documentar el *state of the art* que se ha realizado para conseguir los objetivos de este proyecto. Para ello, se han estudiado las criptomonedas más importantes, o las que más capitalización de mercado tienen, poniendo el acento sobretodo en la privacidad que cada una otorga y cómo es la minería de cada una de las critpomonedas.

2.1. BITCOIN (BTC)

2.1.1. Introducción

Bitcoin fue la primera criptomoneda que vio la luz, con el *whitepaper* llamado *Bitcoin: A Peer-to-Peer Electronic Cash System*, escrito por alguien apodado Satoshi Nakamoto, cuya identidad nunca ha sido revelada. Este *whitepaper* describía cómo era la red blockchain que sustentaba dicha criptomoneda, explicando todas sus características y peculiaridades.

Un 22 Mayo de 2010 se produjo la primera venta registrada, que fueron dos *pizzas* por una cantidad de 10.000 BTC y en Julio del mismo año, se llevó a cabo el primer intercambio de moneda. En 2014 fue hackeada la mayor plataforma de intercambio de monedas, que provocó que el valor del Bitcoin se devaluara un 50% de su precio y no se recuperara hasta el año 2016. A partir de entonces, la moneda no paró de revalorizarse hasta llegar a un máximo histórico de unos 20.000$ a finales de 2017. Actualmente, según coinmarketcap, a fecha que se escribe este documento, la moneda es la que mayor capitalización presenta en el mercado con un total de 175,12 billones de dólares y tiene un precio aproximado de unos 10.000$.

2.1.2. Privacidad

Al contrario de lo que muchos piensan, en Bitcoin no existe un perfecto anonimato ni un alto nivel de privacidad. Cualquier transacción en Bitcoin se lleva a cabo con una dirección de origen y otra de destino, junto a la cantidad transferida. Estas direcciones de origen y destino identifican unívocamente a la persona, pero la identidad de la misma queda escondida detrás de estas direcciones. Así, sabiendo la dirección desde la que se transfiere el dinero no se puede identificar a la persona. Esto cambia cuando, por cualquier motivo, se consigue relacionar a la persona con dicha dirección[3][4]. Debido a la propiedad de inmutabilidad (véase el Apéndice sobre *¿Cómo funciona Blockchain?*), no se puede eliminar ningún registro de la cadena, por lo que una vez se puede relacionar un usuario con su respectiva cuenta, siempre se va a poder saber los movimientos que ha hecho y sigue haciendo este usuario, sin poder eliminarla del libro central. Es por eso que los expertos consideran que no existe la anonimización en Bitcoin, sino que existe una seudonimización.

Aún así, esta seudonimización ocurre cuando se puede lograr relacionar un usuario con la dirección que usa, puesto que sino solamente vemos una cadena alfanumérica sin poderlo relacionar con una identidad.

2.1.3. Minería

Bitcoin usa el método de consenso *Proof of Work* (más información en el apartado *Glosario*), de manera que el proceso de minado se lleva a cabo con muchas computadoras que minan simultáneamente y, el primero en resolver el problema matemático y una vez está validado por los demás mineros, se lleva la recompensa. De esta manera, se premia el trabajo hecho por cada minero y busca impartir una mínima justicia.[5]

Bitcoin popularizó el concepto de *pools de minado*. Estos pools tienen como función agrupar distintos mineros, de manera que si uno de ellos mina, la recompensa es para todos. Así, suben las probabilidades de que un minero cualquiera pueda ingresar monedas a cambio de minar pero también disminuye la recompensa que se lleva cada uno de los mineros (en el apartado *Glosario* hay más información sobre ello).

El precio de la recompensa va en función de la dificultad que tenga en cada momento la red, es decir, en función de cómo de difícil sea resolver estos problemas matemáticos. Para ello, los creadores de Bitcoin establecieron la cifra límite de 10 minutos, de manera que cuando la dificultad de la red disminuye por debajo de dicha cifra, la misma dificultad se redimensiona para que se mantenga por encima de los 10 minutos. De igual manera sucede cuando la dificultad sube por encima de los minutos comentados, la red va a disminuir la dificultad para mantenerla constante.[5]

Todo esto lleva a que se conozca el hashrate de la red de Bitcoin, que indica la capacidad o velocidad de resolver los problemas matemáticos asociados a la minería de Bitcoin que, a fecha que se escribe este documento, alcanza los 75,5 millones de Hashes por segundo.

2.1.4. Ventajas e inconvenientes

- ✔ No hay relación de las transacciones con el usuario
- ✔ Más facilidad de documentación
- ✔ Tiene muchas pools de minado, aspecto que permite adherirse a una y obtener recompensas más fácilmente
- ✕ No hay *full-privacy*, usando Snarks o alguna construcción similar
- ✕ Red demasiado masificada, que hace que sea muy complicado minar
- ✕ Demasiado gasto computacional, puesto que usa PoW

2.2. ETHEREUM (ETH)

2.2.1. Introducción

Ethereum fue concebida a finales de 2013 por un gran programador llamado Vitalik Buterin, antiguo programador en el ecosistema Bitcoin. En enero de 2014, Vitalik Buterin presentó Ethereum justificándolo con alusiones a los serios problemas de escalabilidad que se presentan al construir sobre Bitcoin, y añadiendo los contratos inteligentes (*smart contracts*) que actúan como un agente automatizado para realizar transacciones (más información sobre los *smart contracts* en el apartado Glosario de este mismo documento).

El 22 de julio de 2014 Ethereum lanzó la preventa de su criptomoneda que no sería minada hasta el invierno de 2014-2015. En julio de 2015 se empezaron a escribir contratos inteligentes y aplicaciones descentralizadas para la red y, en marzo de 2016, se lleva a cabo lo que se considera el primer lanzamiento estable en la historia de Ethereum.

Los contratiempos llegaron para Ethereum, y el 17 de junio de 2016 se robaron alrededor de 50 millones de dólares en ether de una de las aplicaciones que más éxito había tenido dentro de la red Ethereum. Para solventar dicho problema, desde los mismos desarrolladores se realizó un *hard fork* (más información en el apartado *Glosario)*. También, entre octubre y noviembre de 2016, se llevaron a cabo otras dos bifurcaciones de la red Ethereum para enfrentar ataques DDoS.

En el siguiente año, debido a una saturación de la red de Ethereum, se lanzaron un par de actualizaciones de la red, la última de las cuales incluía la introducción de transacciones a través del protocolo zkSNARK, que permite demostrar y validar la identidad de la transacción sin desvelar el propietario de la misma. En diciembre de 2017 aparecieron en el mercado los tokens no fungibles ERC721, que se popularizaron con el juego *CryptoKitties*, donde se podía coleccionar, intercambiar y negociar gatitos virtuales. Esto popularizó cada vez más la red Ethereum y se siguieron desarrollando contratos inteligentes, haciendo crecer así la moneda hasta que el 13 de enero de 2018 registró la valoración más alta de su historia llegando a costar 1 ether 1432,88$. En este punto, su capitalización rozó los 139 millones de dólares.

Si hablamos del valor actual, a fecha que se escribe este documento, el ether tiene un valor de 183,87 dólares, con una capitalización total de 19,7 mil millones de dólares.

2.2.2. Privacidad

Vitalik Buterin, en la red de Ethereum, defiende la idea de que la información está *completamente ofuscada*, desde el punto de vista criptográfico. Para él, la idea de la ofuscación de la información, equivale a la idea de convertir el programa en una caja negra, de la que sabes las entradas y las salidas, mantiene la misma lógica interna pero no puedes saber cómo funciona realmente el programa. Desafortunadamente, esta idea desde el punto de vista matemático es imposible, pero en blockchain se puede conseguir. Esto en Ethereum se consigue haciendo trabajar el smart contract con *inputs* y *outputs* cifrados, de esta manera no se puede saber qué operaciones realiza el smart contract internamente puesto que no podemos descifrar los datos de entrada a la red.[6][7]

Otro aspecto que destaca de la privacidad en la red Ethereum es el uso de los Zk-SNARKS[6], que son construcciones matemáticas que permiten anonimizar la transacción y que no se conozcan origen y destino de la misma pero, a la vez, no generar dudas sobre si origen y destino son quien dicen ser. Es decir, demuestra que origen y destino son quienes realizan la transacción pero sin desvelar su identidad (en el apartado *Glosario* de este mismo documento hay una ilustración del ejemplo, para más información).

2.2.3. Minería

La minería en Ethereum sigue el mismo funcionamiento que con Bitcoin. Cada minero gana una recompensa en función del trabajo hecho y, cómo más difícil sea realizar el trabajo, más recompensa se lleva. De esta manera, se promociona y se favorece que los mineros tengan que trabajar para conseguir dicha compensación y se imparte un mínimo de justicia, por lo que se premia el trabajo.[8]

Igual que en Bitcoin, los mineros se agrupan en pools de minado, en los que si uno de los mineros consigue la recompensa se reparte por igual a todos los que participan en dicho pool de minado. De esta manera, es más fácil conseguir una recompensa por el trabajo realizado.[8]

La dificultad de minado, se va redimensionando en función de cuánto tardan los mineros en minar cada bloque. Se fija un tiempo de minado alrededor de unos 12 segundos, por lo que si el tiempo empieza a bajar considerablemente, la dificultad de la red sube y, si sube de los 12 segundos, la dificultad de la red baja.[8]

El algoritmo específico de prueba de trabajo que utiliza Ethereum se llama *Ethash*. Este está diseñado para requerir más memoria en la computadora para dificultar la extracción de criptomonedas con ASICs más costosos.[8]

2.2.4. Ventajas e inconvenientes

- ✔ Se usan Zk-Snarks, por lo que se consigue la *full-privacy*
- ✔ Tiene un gran uso comercial, debido a la facilidad de construir SmartContracts sobre la misma red
- ✔ Facilidad para basar una nueva ICO sobre la red de Ethereum, gracias a los tokens ERC20 y ERC721
- ✕ Usa PoW, que supone demasiado gasto computacional y eléctrico
- ✕ Demasiado masificada, que conlleva a que sea muy complicado minar Ethers

2.3. <u>RIPPLE (XRP)</u>

2.3.1. Introducción

Ripple fue fundada en 2012 con el objetivo de llevar a cabo el *Internet of Value*, y que sea una plataforma blockchain que sea usada para transacciones de uso cotidiano con la ayuda de una plataforma bancaria.[9]

Poco tiempo más tarde, se formó una organización llamada *SBI Ripple Asia* para acelerar el uso comercial de blockchain en Japón y Corea. Luego, para asegurar una consistencia y una claridad legal, se formo el *RippleNet Committee*, que permitió que más de 100 instituciones financieras se unieran rápidamente.[9]

Actualmente, Ripple es la tercera moneda más capitalizada en el mercado, con un valor de 0,21$ por moneda de Ripple, moviendo un poco más de mil millones de dólares.[10]

2.3.2. Privacidad

Desde Ripple nos aseguran que los datos de los clientes permanecen privados y seguros, donde el historial de transacciones se almacena en bases de datos y estas no están relacionadas con información identificable ni pueden ser asociadas con ninguna cuenta ni institución financiera.

Una característica relativa a privacidad que se añade en Ripple son los HTLC (Hash Time Lock Contracts). Estos contratos están ideados para que un atacante, en caso que intercepte la transacción, si no sabe el secreto bajo el cual se ha encriptado dicha transacción no podrá desviar fondos o modificar dicha transacción. Este tipo de contratos funcionan de la siguiente manera:[11]

1. Origen y destino intercambian un secreto, bajo el que se encriptará la transacción.
2. El origen, encripta la transacción con el secreto intercambiado con el destino y le añade un contador que tendrá la función de timeout, para que si un atacante intenta por fuerza bruta descifrar el secreto, tenga un límite de intentos o un tiempo limitado.
3. Cuando la transacción llega al destino, este desbloquea la información que va dentro con el secreto que han intercambiado con el origen antes de realizar esta transacción.
4. Una vez desbloqueada la transacción, el destino obtiene los fondos que le ha enviado el origen y proceden a realizar la transacción.

De esta manera, se produciría una transferencia cifrada con un secreto y un atacante que se encontrara en medio tendría un tiempo limitado para descifrarla, puesto que hay un timeout que expiraría.

2.3.3. Minería

La minería en Ripple es muy diferente que en las demás criptomonedas. Así, como si queremos cualquier criptomoneda podemos poner nuestro ordenador a calcular y, si conseguimos resolver un problema matemático vamos a ser recompensados, en Ripple no se puede. No se pueden minar monedas.[14][15]

Cuando iniciamos en este mundo, damos por supuesto que el minado es un proceso que se cumple en cualquier criptomoneda y mediante el minado podemos obtener una mínima cantidad de cualquiera, pero esto no se cumple en todas, y Ripple es un ejemplo de estas. Desde que salió, solo hay un organismo que puede poner en circulación monedas de Ripple, que es *Ripple Labs*, organismo propio de Ripple. Un usuario cualquiera no puede obtener monedas XRP con su propio ordenador, mediante el proceso de minado. La única manera que un usuario puede obtener monedas XRP sería la de comprar cualquier otra criptomoneda y realizar un exchange para cambiar a Ripple.[14][15]

Este aspecto de Ripple, es muy discutido entre la comunidad debido al alto grado de centralización que ello supone. Una de las características más importantes de las criptomonedas es que, en general, consiguen un entorno descentralizado, en el que

nadie ni ningún organismo ni organización consigue controlar el flujo que tienen las mismas ni su entrada en el mercado. Esto, no se cumple en Ripple, puesto que el mayor organismo que sustenta Ripple es el encargado y la única organización que puede añadir cuando quiera monedas XRP al mercado. Es por ello que Ripple sufre bastantes críticas relacionadas con la descentralización, donde grandes expertos consideran que no es una moneda descentralizada, crítica que defienden desde *Ripple Labs* considerando que sí que es descentralizada porque ahora mismo, si desapareciera dicha organización, Ripple podría seguir funcionando sin que nadie la controlara.[15]

2.3.4. Ventajas e inconvenientes

- ✔ Consigue un plus de seguridad con los HTLC, aunque no llega a la *full-privacy* que ofrecen los Snarks
- ✔ Transacciones casi inmediatas
- ✔ Las transacciones son anónimas
- ✕ Red blockchain no-descentralizada, puesto que es Ripple Labs quién controla la red
- ✕ No usa Snarks, que aunque tenga un plus de seguridad con los HTLC, no llega a la *full-privacy*.

2.4. BITCOIN CASH (BCH)

2.4.1. Introducción

Bitcoin Cash fue un *Hard Fork* de Bitcoin realizado el 1 de Agosto de 2017. Este *Hard Fork* se hizo debido a unas diferencias de opinión entre los desarrolladores de Bitcoin, puesto que unos cuantos querían establecer el límite de creación de bloque en un tamaño de 1MB (tal y como está actualmente en Bitcoin) y otros en 8MB (tal y como está actualmente en Bitcoin Cash). De esta manera, se creó Bitcoin Cash con un tamaño de bloque máximo de 8MB.

La moneda fue creciendo e incorporando más privacidad en las transacciones (explicado con más detalle en el siguiente apartado) y en Setiembre de 2018 se hizo un *stress test* que dio un resultado de 25.000 transacciones por bloque.[16]

Actualmente, a fecha que se escribe este documento, la moneda tiene un valor de 207,82$ y es la quinta en capitalización, sumando un total de casi 4 mil millones de dólares, moviendo un volumen de poco más de mil millones de dólares.[17]

2.4.2. Privacidad

En BitcoinCash aparece un nuevo concepto relacionado con la privacidad, que busca dar más privacidad a las transacciones. Este concepto llamado *CashShuffle* es un protocolo de privacidad completamente descentralizado que enmascara los Bitcoin Cash de una transacción con los otros participantes de la red. Este proceso consigue ofuscar las

transacciones reales y hace extremadamente difícil realizar un análisis completo de la cadena por parte de empresas que quieran rastrear tus monedas.[16]

El procedimiento consiste en encriptar cada una de las transacciones con las de cada uno de los participantes de un grupo. A grandes rasgos, funcionaría de la siguiente manera:

1. Un grupo de participantes se ponen de acuerdo en usar una clave privada y una clave pública
2. El participante *i*, cifra su transacción con la clave de *i+1*. A la vez, el participante *i+1* cifra la suya con la de *i+2*, y así sucesivamente.
3. También, a parte de cifrar la transacción, añaden elementos como un tiempo acordado en el punto 1 (que funcionará como timeout) o almacenan el hash de cada transacción (que funcionará como control de errores).

De esta manera, se consigue un procedimiento de envío de transacciones en las que cada una está cifrada con otra del grupo de participantes aleatoria con unas claves privadas acordadas, que hace mucho más difícil de interceptar y descifrar cada una por separado.

2.4.3. Minería

La minería en Bitcoin Cash funciona muy parecido a la de Bitcoin, debido a que se formó a partir de la red de Bitcoin por un problema de tamaño del bloque. Así, en Bitcoin Cash se comparten muchos aspectos de Bitcoin, como el algoritmo de consenso, que también usan *Proof of Work*; las *pools* de minado y su funcionamiento, que son el mismo en ambas criptomonedas; o el tiempo de generación de bloques, que también está en 10 minutos.[17]

La principal novedad que incorpora Bitcoin Cash respecto a Bitcoin, es el tamaño de cada uno de los bloques que, mientras en Bitcoin es de 1MB, en Bitcoin Cash pasa a ser de 8MB. Esto conlleva a que se tarde mucho más a generar un bloque en Bitcoin Cash que en Bitcoin, por lo que para llegar al mismo número de bloques tiene que haber un número de transacciones en Bitcoin Cash mucho mayor que en Bitcoin.[17]

2.4.4. Ventajas e inconvenientes

- ✔ Incorpora un plus de seguridad respecto a Bitcoin, con el algoritmo *Cash shuffle*.
- ✔ Comparte la red de Bitcoin, aspecto que da confianza a la comunidad.
- ✔ Tiene muchas pools de minado, aspecto que permite adherirse a una y obtener recompensas más fácilmente.
- ✔ Las transacciones son anónimas.
- ✕ Demasiado gasto computacional al minar, debido al protocolo de PoW.
- ✕ No usa construcciones matemáticas como los Snarks que den una *full-privacy*.

2.5. LITECOIN (LC)

2.5.1. Introducción

Litecoin fue creada por el desarrollador y formador de Google Charlie Lee. En el momento de su creación, fue creada con la misión de ser una criptomoneda *peer-to-peer* que permita transacciones instantáneas y costes alrededor del cero (si no fueran cero, supondrían muy poco coste).

En sus inicios, Litecoin sufrió mucho en cuanto a popularidad, debido a la gran cantidad de bugs que había en su red. Esto cambió en 2013 cuando se lanzó la versión 0.8.5.1, que mejoró por un lado, el minado, haciéndolo más eficiente; en segundo lugar, se introdujeron muchas más criptomonedas en comparación con las otras que estaban en el mercado; y finalmente, se solucionaron los bugs y se introdujeron mejoras, por lo que a la comunidad blockchain les fascinó la capacidad de adaptación de los desarrolladores de Litecoin. Así, en 2013, llegó a cotizar mil millones de dólares, subiendo como la espuma en el ranking global de las criptomonedas.[20]

Actualmente, Litecoin se encuentra en la sexta posición en niveles de cotización, con un precio de 43,69$ cada moneda de Litecoin y con un volumen superior a los dos mil millones de dólares. [21]

2.5.2. Privacidad

Litecoin no es una moneda que se caracterice por una gran privacidad, puesto que goza de las mismas medidas que otras criptomonedas que consiguen una seudonimización, como puede ser el ejemplo de Bitcoin. Aún así, la comunidad de Litecoin se ha dado cuenta de este hecho, y se han puesto manos a la obra para remediarlo. Para ello, en un corto plazo tienen previsto implementar alguna solución y mejorar así su privacidad.

La solución que tienen previsto implementar es la del protocolo Mimblewimble. Este protocolo lo usan otras criptomonedas, y es una evolución de las llamadas transacciones confidenciales. Las transacciones confidenciales se caracterizan porque pueden encriptar el monto de la transacción, mediante *factores ciegos*, que ayudan a ofuscar la cantidad de la transacción. Mimblewimble funciona de la misma manera pero, en lugar de *factores ciegos*, se usa un rango de *factores ciegos*. De esta manera, el receptor escoge qué *factores ciegos* usar (dado por el emisor) y estos se usarán para demostrar que la transacción es válida.[22]

2.5.3. Minería

La minería en Litecoin, al ser una criptomoneda que deriva de Bitcoin, se diferencia muy poco de la misma. Aún así, hay alguna diferencia que se va a comentar a continuación.

La primera diferencia que encontramos es el tiempo de generación del bloque. Mientras en Bitcoin es de 10 minutos, en Litecoin es de 2.5 minutos. Esto a su vez, provoca que la dificultad de la red se disminuya a la mitad cada 600.000 bloques más que en Bitcoin. También conlleva a que, al cerrar un bloque cada menos tiempo, la red pueda gestionar mejor las transacciones que van llegando, minimizando así su pérdida. Una

consecuencia negativa que tiene la disminución entre bloques, es la capacidad de la red, puesto que se necesita mayor capacidad en la misma para almacenar nuevos bloques de transacciones.[23]

2.5.4. Ventajas e inconvenientes

- ✔ Las transacciones son anónimas
- ✔ En el futuro, gozará de un plus en seguridad con el protocolo Mimblewimble
- ✔ Mejor manejo de transacciones debido a la disminución del bloque
- ✕ Debido a la disminución del bloque, se necesita mayor capacidad en la red
- ✕ Para minar Litecoin, es necesario un alto gasto en CPU debido a que su mecanismo de consenso es PoW
- ✕ Aunque se quiere implementar el protocolo Mimblewimble, no se usa de construcciones que den *full-privacy* como los Snarks

2.6. EOS (EOS)

2.6.1. Introducción

EOS fue una criptomoneda fundada a mediados de 2017 por la compañía *Block.one*, una compañía de soluciones tecnológicas incluyendo soluciones en desarrollos de software en Blockchain, bajo el eslogan *Decentralize Everything*.

A mediados de 2017 se lanzó la ICO (*Initial Coin Offering*) y se distribuyeron un total de mil millones de tokens en la red Ethereum. Un año más tarde, a mediados de 2018, la criptomoneda se había convertido en una de las más capitalizadas del mercado. [24]

Actualmente, el valor de la moneda se sitúa en dos dólares y medio, consiguiendo un volumen total de un poco más de un millón de dólares. Con estos datos, EOS se sitúa en séptima posición en cuanto a capitalización de mercado, a fecha que se escribe este documento.[25]

2.6.2. Privacidad

La criptomoneda EOS por sí sola carece de privacidad, debido a que no se implantaron medidas de anonimización ni privacidad a la hora de realizar transacciones. Es por esto que se ha creado *pEOS*, que es un token que da esta anonimización y privacidad que le falta a la propia criptomoneda.

Este token está creado mediante una clave pública y privada intercambiados por el protocolo *Diffie-Hellman,* de manera que un atacante no puede interceptar dichas claves (una explicación sobre el protocolo Diffie-Hellmann se encuentra en el apartado *Glosario* de este mismo documento). A su vez, este token usa la curva elíptica *secp256r1*, muy parecida a la que usa Monero, criptomoneda conocida por su alta privacidad. [27]

Finalmente, otro aspecto clave en este token de EOS, es la no-trazabilidad de la transacción debido a las signaturas en anillo de las que dispone. Estas signaturas se

usan para esconder quién es el que firma cada transacción, por lo que permite que nadie sepa el origen de las transacciones pero, a su vez, se tenga la certeza de que estas firmas son válidas.[27]

2.6.3. Minería

La criptomoneda EOS usa el protocolo *Delegated-Proof-of-Stake*, en el que intenta mejorar el protocolo *Proof-of-Stake* que ya han adoptado algunas criptomonedas. En esta red, no hay *Hard Forks*, ya que todos los nodos trabajan de forma cooperativa.

La fuerza de producción de un bloque es de 3 segundos, por lo que constantemente se está firmando un bloque nuevo. Aún así, cada minero cuando lo requiera, puede crear un bloque nuevo. Luego, cada 21 bloques generados se genera un bloque EOS, que será el que se añadirá a la misma blockchain.[26]

Otro aspecto a destacar es la importancia que se le da a los productores más eficientes y constantes, debido a que si un minero se ausencia 24h de la red, se le retira del sistema hasta que justifique la ausencia. Esto provoca que los mineros más constantes van a ser los que se lleven las recompensas.[26]

2.6.4. Ventas e inconvenientes

- ✔ Usa el protocolo *Delegated Proof-of-Stake*, que no supone un gran gasto energético y mejora *Proof-of-Stake*
- ✔ Se premia a los mineros más eficientes, puesto que un minero que se ausenta 24h se expulsa de la red
- ✔ En el token pEOS se usa la curva elíptica *secp256r1*, que goza de una alta seguridad
- ✔ Existe el cifrado en anillo, que no permite trazar las transacciones al desconocerse quién ha cifrado la transacción
- ✕ Se requiere una red con una capacidad elevada, puesto que se genera un bloque cada 5 segundos
- ✕ La propia moneda EOS no goza de privacidad, por lo que si no se usa pEOS, no hay anonimización en las transacciones
- ✕ Ni EOS ni pEOS gozan de la propiedad de *full-privacy*, puesto que no usan construcciones matemáticas parecidas a los Snarks

2.7. <u>BINANCE COIN (BNB)</u>

2.7.1. Introducción

Binance coin, cuyo nombre procede de la fusión de *binary* y *finance*, nace básicamente para soportar las transacciones dentro de la propia plataforma de Binance. Trata de un token que permite realizar transacciones sencillamente gracias a su compatibilidad con diferentes sistemas operativos y divisas digitales.[31]

Esta criptomoneda fue lanzada a través de una ICO el 26 de junio de 2017, tan solo once días después de que el exchange de Binance hubiera abierto las puertas. En su momento, Binance Coin fue lanzada como un token ERC-20. Más tarde, la criptomoneda fue migrada a una red propia para así despegarse de la red Ethereum. Siguiendo la misma línea, en Abril de 2019, el propio exchange de Binance dejó de dar soporte al token ERC20 dejando así solamente abierto las criptomonedas Binance que circularan dentro de su propia red.[28][29]

Actualmente, Binance Coin se encuentra en octava posición dentro del total de capitalización, con un valor de catorce dólares y medio por cada token de Binance, y un volumen total de 156 mil millones de dólares.[30]

2.7.2. Privacidad

La criptomoneda de Binance no añade aspectos de seguridad respecto al token ERC20, su origen. De esta manera, referente a la seguridad que nos aporta Binance Coin, podemos decir que las transacciones son seudoanónimas, puesto que no se acaba de anonimizar al completo.

Respecto a las demás características, se comporta como una criptomoneda más en el mercado.

2.7.3. Minería

En la criptomoneda del Exchange de Binance, no existe ningún tipo de minería, puesto que la puesta en el mercado de cada unidad de criptomonedas es Binance quien las distribuye por el mercado. En Exchange de grandes dimensiones como Binance o iFinex, es una práctica habitual, puesto que estas criptomonedas solo se utilizan para gastar en el mismo Exchange.[31]

Así, igual que nos hemos encontrado con otras criptomonedas, no podemos hablar de un algoritmo de consenso puesto que no existe el minado. Esto hace que esta criptomoneda pierda interés en el estudio.

2.7.4. Ventas e inconvenientes

- ✔ Fácil de adquirir y obtiene beneficios a la hora de realizar Exchanges en el portal de Binance
- ✔ Consigue una seudonimización de las transacciones
- ✕ No añade características adicionales relativas a Seguridad
- ✕ No existe un minado de la criptomoneda, por lo que el Exchange de Binance centraliza absolutamente todas las criptomonedas

2.8. BITCOIN SV (BSV)

2.8.1. Introducción

BitcoinSV (Bitcoin Satothi's Version) intenta recuperar la visión que tenía Satoshi Nakamoto (fundador de Bitcoin) para implantarla en la versión de BitcoinSV. Esta criptomoneda surgió después del *hard fork* que hubo en Bitcoin convirtiéndose en Bitcoin Cash. Para ello, se aumentó el tamaño de bloque a 128MB y se hicieron más cambios a nivel más técnico.

De los fundadores de BitcoinSV, destacan que quieren una red blockchain que sea estable, para que las empresas tengan confianza en la misma y se desarrollen soluciones empresariales sobre esta red; también destacan la escalabilidad que quieren que tenga esta red, puesto que cuando una red adopta un uso comercial las transacciones incrementan de tal forma que este volumen de transacciones generan problemas de capacidad. Para ello, como quieren que esta red sea de uso comercial, quieren solventar estos problemas de capacidad que se pueden ocasionar; también destacan la seguridad que puede tener y, finalmente, destacan también la *payment experience*, poniendo el acento la velocidad de propagación de las transacciones y las políticas de recompensas de los mineros configurables.[32]

2.8.2. Privacidad

Bitcoin SV hereda todas las propiedades de las que dispone Bitcoin en cuanto a privacidad, debido que es un hard fork de la propia cadena. Así, podemos hablar de una anonimización de la identidad, debido a que los únicos datos que se muestran en el libro central de la red Bitcoin son direcciones de cuentas, nunca datos de personas. En cambio, en caso que se pudiera relacionar una identidad a cualquier dirección alfanumérica, hablaríamos de seudonimización.[32][33]

Por otro lado, no podemos hablar de construcciones matemáticas que sí existen en otras criptomonedas como pueden ser las pruebas de conocimiento cero, que otorgan una mayor privacidad al ecosistema Bitcoin.[32][33]

2.8.3. Minería

En Bitcoin SV se usa el mismo método de consenso que en la famosa criptomoneda Bitcoin, *Proof of Work*. Como ya se ha comentado a lo largo de este documento, el proceso de minado se lleva a cabo con muchos computadores que minan simultáneamente y, el primero en resolver el problema matemático y una vez está validado por los demás mineros que participan en este proceso, se lleva la recompensa estipulada por la red.[32][33]

También en Bitcoin SV, al igual que Bitcoin, podemos hablar de *pools de minado*. Estos pools tienen como función agrupar distintos mineros de manera que si uno de ellos mina, la recompensa es para todos (una mayor explicación se encuentra en el apartado *Glosario)*. En BitcoinSV, disponemos del pool *SVPool*, que ha sido el más exitoso desde la creación de la criptomoneda.[34]

Si nos fijamos en la red de Bitcoin SV, podemos hablar que, a fecha que se escribe este documento, dispone de 458 nodos con 611514 bloques y un tiempo de 128 días para que la red disminuya a la mitad la recompensa que le da a cada uno de los mineros.[35]

2.8.4. Ventajas e inconvenientes

- ✔ Es un hard-fork de Bitcoin, por lo que le ha sido más fácil que a otras criptomonedas crecer en cuanto a valor bursátil debido a la confianza que esta última otorga
- ✔ Las transacciones no son totalmente públicas, sino que están seudonimizadas igual que en Bitcoin
- ✔ Hay algún pool de minado famoso como *SVPool*, que hace más fácil que mineros anónimos se adhieran a este para empezar a minar
- ✕ Usa el algoritmo *Proof of Work*, que gasta recursos de la máquina que a su vez, se traduce en dinero a la hora de minar
- ✕ No introduce ninguna mejora de seguridad en cuanto a Bitcoin

2.9. STELLAR (XLM)

2.9.1. Introducción

Stellar fue fundada por los desarrolladores Jed McCalbe y Joyce Kim. Inicialmente estaba basada en el protocolo de Ripple, mientras los desarrolladores estuvieron trabajando paralelamente al desarrollo del que ahora se conoce como SCP (Stellar Consensous Protocol).[36]

Stellar fue creada para ser una red de pago descentralizada que permitiera transacciones internacionales entre cualquier criptomoneda.[36]

Hoy en día, Stellar es una de las criptomonedas con más personalidad en el mercado, debido al elevado grado de privacidad que esta contiene (que se explica en el apartado siguiente) y al protocolo de consenso que implementa, que también es único en las criptomonedas.[36]

2.9.2. Privacidad

En Stellar se introduce un concepto nuevo relativo a la privacidad de las transacciones como es la *Lightning Network*. Este tipo de red permite que la transacción se cifre con parámetros que se detallarán a continuación de cada uno de los nodos por los que pasa dicha transacción.

Los bloques fundamentales de la *Lightning Network* son los nodos y los canales de pago que conectan nodos con otros nodos. Para poner ejemplos, los nodos pueden ser los propios usuarios, ya sean vendedores o compradores. Para enrutar cada una de las transacciones que circulan a través de la red, *Lightning* funciona con *source routing* u *onion routing*:[37]

- *Source routing.* En esta modalidad de routing, el nodo origen es responsable de calcular la ruta de origen a destino. Para ello, tiene que descargarse las conexiones de todos los canales públicos de pago, para calcular la ruta más eficiente, considerando la capacidad de todos los canales en el camino, el coste en *fees* y el número de saltos requeridos. Este tipo de routing produce muchos datos que solo crecerán con la red, por lo que se anticipa un problema de escalabilidad.
- *Onion routing.* Este tipo de routing imita al modelo de red Tor. Imaginemos que quiero enviar un pago a Pepe pero no tengo conexión directa. Sí que la tengo con Manuel, este a su vez con Daniel, y el último con Pepe:
    1. Bloqueo el pago en una caja, y la bloqueo con otra caja cifrada con la dirección y la clave pública del siguiente nodo con el que tengo conexión directa.
    2. Luego, encajo la estructura anterior con el siguiente nodo por el que pasará la transacción. Esta operación se repite por cada uno de los nodos por los que va a pasar mi operación.
    3. De esta manera, cuando el paquete llegue a Manuel, este desbloqueará la caja y le enviará a Daniel, que a su vez desbloqueará la caja y la enviará al siguiente nodo… Hasta llegar al destino deseado, Pepe.

2.9.3. Minería

La moneda Stellar tiene un mecanismo propio de consenso, que supone la primera implementación del famoso protocolo *Federated Byzantine Agreement*. Este mecanismo de consenso consigue que los nodos se pongan de acuerdo en una decisión, teniendo en cuenta que pueden haber nodos maliciosos que quieran modificar la decisión de la mayoría. Este protocolo consigue:[38][39]

- Control descentralizado. Todos los nodos pueden ser validadores de una transacción, no hay restricciones
- Baja latencia. Al no tener que calcular como en *Proof of Work*, el proceso de validar una transacción se produce con una latencia muy baja.
- Confianza libre. Los participantes son libres de decidir qué deciden, sin ninguna restricción
- Seguridad asintótica. Se usan signaturas digitales y familias de hashes para combatir al alto consumo de potencia de los ordenadores.

Para ello, Stellar hereda este protocolo pero le añade una modificación, el concepto de *Federated Voting*. Este concepto consigue que el proceso de dar por buena una decisión se componga de:[39]

1. Votar → En este punto, los nodos votan si dan por buena una transacción o no.
2. Aceptar → Los nodos votan si los resultados de los demás nodos son válidos, repitiendo la votación en caso que sea fraudulenta

3. Confirmar → En este último punto, los nodos confirman que la transacción es válida puesto que todas las decisiones de los nodos son válidas.

Esta característica añadida no modifica en exceso las que ya tenía el protocolo *Federated Byzantine Agreement*. Si echamos un vistazo a las que ya había, vemos que solo queda afectada la característica de baja latencia. Ahora, al incorporar tres nuevas fases que anteriormente era una sola, la latencia incrementa. Aún así, se puede comprobar cómo la disminución de esta latencia no supone un contratiempo para la propia red de Stellar, puesto que la latencia sigue siendo mucho inferior que otros algoritmos de consenso.

2.9.4. Ventajas e inconvenientes

- ✔ En Stellar se introduce el concepto de *Lightning Network*, que proporciona una seguridad adicional de manera muy notable
- ✔ No usa protocolos como *Proof of Work*, en el que hay un gasto computacional muy elevado, ni *Proof of Stake*, que puede llegar a ser injusto por quienes tienen poco peso en la red.
- ✔ La latencia de minado del nuevo protocolo aumenta respecto al que ha heredado, el *Federated Byzantine Agreement*.

- ✕ En el protocolo del que hereda Stellar, sigue habiendo un alto consumo de potencia por parte de los mineros, que se combate con la característica de seguridad asintótica anteriormente explicada
- ✕ Este consumo de potencia se traduce en alta inversión a la hora de comprar un hardware para ser capaz de minar Stellar, por lo que inversores con poco peso en la red pierden importancia

2.10. CARDANO (ADA)

2.10.1. Introducción

Cardano fue una criptomoneda que se fundó con el objetivo de crear un ecosistema y una plataforma de *smart contracts* de nueva generación, aprendiendo de lo sucedido con las criptomonedas Bitcoin y Ethereum. Este proyecto presume de ser *la primera plataforma blockchain que evolucionó a partir de una filosofía científica y un enfoque impulsado por la investigación*. De esta manera, quieren proporcionar una plataforma basada en *smart contracts* que sea de uso comercial para que las empresas consigan soluciones blockchain basadas en Cardano.[40]

Igual que Ethereum, Cardano también tiene una organización sin ánimo de lucro que da soporte a los desarrolladores de la misma criptomoneda en materias de investigación y desarrollo del protocolo. También hay otras organizaciones como IOHK, que contribuyen al desarrollo de la misma criptomoneda.[40]

Una curiosidad respecto al token de Cardano, es que su nombre (ADA) proviene de *Ada Lovelace*, una matemática del siglo 19 reconocida como la primera mujer programadora e hija del poeta *Lord Byron*.[40]

2.10.2. Privacidad

La privacidad en Cardano no es una de las políticas de privacidad de referencia en el mundo blockchain y de las criptomonedas, pero tampoco significa que carezca de privacidad ni mucho menos que sea una comunidad que se vea estancada por este rasgo.[42]

En Cardano, al igual que en Bitcoin, hay una seudonimización en las transacciones dentro de la blockchain. Esto significa que se puede conseguir ver las direcciones de origen y destino así como también la IP de origen, pero nunca se va a poder relacionar la transacción con una identidad. Esto nos obliga a denominar que Cardano goza de una seudonimización, debido a que la anonimización sería el hecho de no revelar absolutamente nada. Aún así, aunque no sea una anonimización total, podemos dar por supuesto que Cardano no tiene fugas de seguridad (conocidas por el momento) y mantiene a la perfección la política de seudoanonimato de la blockchain.[42]

Como muchas otras criptomonedas, Cardano tiene previsto dar el salto a los ZK-SNARKS, que son construcciones matemáticas que permiten dar validez a una transacción sin la necesidad de ser validada por un minero, con lo que se aseguraría la veracidad de la blockchain sin gastar recursos ni tiempo de los mineros en ello. Según la comunidad de Cardano, este salto está previsto para 2020, en el que aseguran que ya están colaborando con este desarrollo.[43]

2.10.3. Minería

Cardano es una criptomoneda que tiene un algoritmo de consenso propio, basado en *Proof of Stake*. Como ya se ha comentado, *Proof of Stake* es un protocolo de consenso que evita el gasto en potencia y electricidad que sí que tiene *Proof of Work* y un bloque es validado por un minero que tiene un alto poder adquisitivo.[43]

Así, Cardano innova con el protocolo *Ouroboros* en el que divide el tiempo en distintas épocas y estas, en distintos slots:[44]

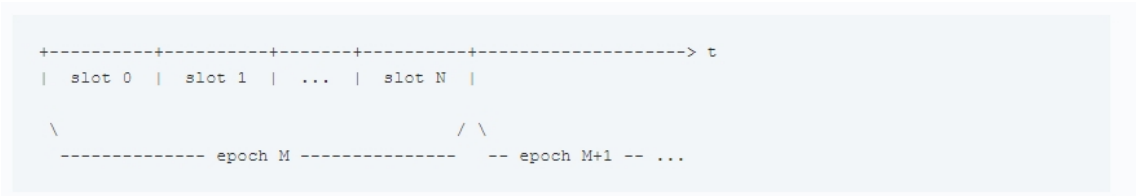

Figura 3. Protocolo Ouroboros

En cada slot va haber un solo líder, llamado *slot leader*, que va a ser el único que va a validar en este periodo de tiempo y va a construir un bloque por cada slot. Este *slot leader* es elegido en función de la cantidad de dinero que alberga en la cuenta cada participante. Esta cantidad de dinero es establecida en la configuración de la red. Para elegir cada uno de los *slot leaders*, se gasta el tiempo que dura una época, de manera que en la época N, se elige el *slot leader* de la época N+1.

Una vez se ha determinado el *slot leader* de una época, este será el encargado de firmar el único bloque que aparecerá en esta época. De esta manera, se consigue optimizar el tiempo en el que se elige el *slot leader*, puesto que el proceso se lleva a cabo paralelamente a la firma de bloques y el proceso de cifrado de bloque tampoco gasta recursos puesto que la firma es instantánea.[44]

2.10.4. Ventajas e inconvenientes

- ✔ Consigue seudonimizar las transacciones
- ✔ Hay previsión de futuro con la implementación de los Zk-Snarks
- ✔ Usa el protocolo *Proof of Stake*, por lo que no hay un gasto de potencia por parte de los mineros tan elevado como en *Proof of Work*
- ✔ Hay una rotación en los validadores de los bloques, por lo que no siempre minan los mismos

- ✕ Aún y haber la rotación para validar un bloque que ya se ha comentado, para poder ser uno de los validadores se tiene que tener unos ingresos mínimos dentro de la red
- ✕ Aunque sea un proyecto de futuro, todavía no hay implementados construcciones matemáticas que den *full-privacy* como los Zk-Snarks
- ✕ El tiempo de minado aumenta debido a que para cada bloque se define una época y se mina un solo bloque en cada época

2.11. TRON (TRX)

2.11.1. Introducción

Tron, como muchas otras criptomonedas, dispone de una fundación (*Tron foundation*) sin ánimo de lucro que se compromete en operar y mantener la red de Tron en los principios de franqueza y sinceridad, transaparencia y justicia.[45]

Los inicios de Tron fueron dentro de la red de Ethereum, mediante tokens ERC20. Más tarde, se desarrolló la red blockchain propia de Tor y se hizo la migración, tanto de la propia red que corría en Ethereum, como del mismo token que pasó a adquirir un token propio (TRX) en lugar de usar el token ERC20 de Ethereum.[45]

Los beneficios que este cambio otorgó a Tron, entre muchos otros, incluían la velocidad de las transacciones, que incrementaban hasta las 2.000 transacciones por segundo, muy lejos del ratio de Ethereum; y también la facilidad de programar los smart contracts,

puesto que se haría en un lenguaje mucho más común como es Java, en lugar de Solidity, con el que se programaba en Ethereum.[45]

2.11.2. Privacidad

Referente a la privacidad que otorga Tron, actualmente no podemos asegurar que realmente consigue anonimizar al completo las transacciones ni los elementos que la rodean. Aún así, sí que podemos decir que está en el plan de ruta mejorar la privacidad en la nueva red de Tron (después que se separara del token ERC20 de Ethereum).

Parece ser que de cara al 2020, Tron va a lanzar distintas mejoras en su red blockchain, que van a hacer Tron más seguro, con la incorporación de los ya comentados ZK-SNARKS. Estos, según las propias fuentes de Tron, van a conseguir:[47]

- Alta anonimidad. Tanto el origen, como el destino y el monto de la transacción serán completamente confidenciales
- Alto ratio de transacciones por segundo (TPS). Conseguirá un ratio de alrededor de unas 100 transacciones por segundo

Estos beneficios vendrán dados por la incorporación de los ZK-SNARKS a la propia red de Tron, de cara al 2020.

2.11.3. Minería

Igual que otras criptomonedas, Tron no puede ser minada. La emisión de criptomonedas es totalmente controlada por la comunidad Tron, que hasta el momento ha liberado unos 66 millones de criptomonedas.[46]

Esto es un inconveniente fuerte para esta criptomoneda, puesto que no goza de la propiedad de descentralización tan importante en el mundo de las criptomonedas. Si la propia comunidad puede introducir libremente criptomonedas, puede regular la inflación y la deflación que supone tanto problema en la economía actual.

2.11.4. Ventajas e inconvenientes

- ✔ Hay una previsión en un futuro cercano de poder implementar tecnología que otorgue una *full-privacy* como pueden ser los Zk-Snarks.
- ✔ Consigue seudonimizar las transacciones, por lo que no son totalmente públicas
- ✕ Aunque haya la previsión de adoptar Snarks, hoy en día Tron no consigue anonimizar por completo las transacciones
- ✕ No existe la minería en Tron, por lo que lo convierte en una criptomoneda totalmente centralizada por su comunidad

2.12. UNUS SED LEO (LEO)

2.12.1. Introducción

UNUS SED LEO fue un token lanzado por el famoso exchange iFinex, que sirvió para añadir capacidades a todos los usuarios y servicios de la plataforma al propio exchange. Entre estas nuevas capacidades, destacan la reducción de comisiones en Bitfinex; descuentos mensuales en el propio exchange, promocionando así que los usuarios sigan usando iFinex; descuentos en los impuestos a la hora de retirar criptomonedas en el propio exchange iFinex.[48]

De esta manera, UNUS SED LEO sirvió para incentivar los exchanges iFinex y Bitfinex y que los usuarios siguieran usando el mismo para intercambiar criptomonedas y seguir invirtiendo en las mismas.[48]

2.12.2. Privacidad

Igual que la criptomoneda del Exchange de Binance, la criptomoneda de iFinex tampoco aporta características relevantes para el estudio en cuanto a privacidad.

Esta ausencia de privacidad provoca que pierda interés para el estudio, puesto que es uno de los grandes focos de atención a la hora de analizar una criptomoneda.[49]

2.12.3. Minería

No existe la minería en la criptomoneda de iFinex UNUS SED LEO. Esto implica que no existe un algoritmo de consenso como PoW, PoS entre otros, puesto que las criptomonedas no se pueden conseguir minando la red.[49]

Estas criptomonedas, solamente se pueden conseguir intercambiando moneda actual por la criptomoneda. Los sitios web o establecimientos físicos que permiten esto son llamados *exchanges*. Un ejemplo de ellos puede ser iFinex, Bitfinex, Binance… que algunos de ellos también tienen su propia criptomoneda.[49]

2.12.4. Ventajas e inconvenientes

- ✕ No existe el proceso de minado de la criptomoneda, por lo que la propia casa de Exchange iFinex controla al completo su inclusión en el mercado
- ✕ No tiene beneficios en cuanto a seguridad o privacidad de la criptomoneda

2.13. TEZOS (TEZ)

2.13.1. Introducción

En Agosto de 2014, se lanzó el primer *whitepaper* de Tezos, que fue desarrollado el mismo año por un grupo de desarrolladores. Un año más tarde, se fundó la *Dynamic Ledger Solutions*, que dio soporte al proyecto y, en Setiembre de 2016 el código fuente se publicó en Github. En Febrero de 2017 se lanzó la primera *alphanet*, testeando la

nueva criptomoneda Tezos y habilitando a los usuarios a que la pudieran explorar para su estudio.[50]

Diversas instituciones como el gobierno Suizo o el Banco de Francia se han interesado por esta joven criptomoneda. Esto ha provocado que despierta el interés general y que la propia fundación reciba muchas ayudas para el seguimiento del proyecto, y poder algún día ser una de las blockchains de referencia para soluciones comerciales.[50]

2.13.2. Privacidad

Tezos es una moneda que, como ya se ha comentado, ha llamado a muchas instituciones importantes. Aún y el interés que algunas de estas instituciones han despertado sobre esta moneda, han puesto algunas restricciones para usarla, como la privacidad.

En concreto, han establecido el requisito de lo que se llama *fine-tunned privacy*, que es la privacidad más acurada, optimizada para que no existan brechas de seguridad ni fugas de datos de los usuarios o instituciones que usen esta moneda. Para ello, Tezos se puso a trabajar y recientemente anunciaron que sacaran una mejora sustancial en la moneda, la incorporación de los ZK-SNARKS. Como ya se ha comentado en este mismo documento, los ZK-SNARKS son construcciones matemáticas que permiten que el probador de la transacción convenza al verificador que su transacción es válida sin tener que enseñar ni mostrar ningún dato de la misma transacción.[51][52]

De esta manera, se conseguiría nutrir de privacidad la red blockchain de Tezos, aspecto que conseguiría que instituciones importantes como el ya comentado Banco de Francia empezaran a confiar más en esta moneda y la adoptaran como solución empresarial, aspecto que sería muy beneficioso para la misma.

2.13.3. Minería

La minería en Tezos se basa en el ya conocido algoritmo de *Proof of Stake*, en el que hay unos *stakeholders* seleccionados, en función el poder adquisitivo dentro de la red blockchain de cada uno, que van a ser los únicos que van a poder minar cada uno de los bloques. Para ello, tienen que tener una cantidad estipulada suficientemente grande como para que sean considerados *stakeholders* y, por lo tanto, puedan minar criptomonedas.

Además, Tezos incluye una novedad en el protocolo de *Proof of Stake* que permite regular la emisión de bloques. Esta novedad es interponer un tiempo de *delay* entre cada bloque que se mine en la red. Esto se quiere conseguir estableciendo un orden de los *stakeholders* que van a poder minar bloques, de manera que el primero de ellos se tendrá que esperar un minuto; el segundo, se tendrá que esperar dos minutos; el tercero tres minutos… y así sucesivamente. De esta manera, se consigue un minado de bloques controlado pero, a la vez, descentralizado.[51]

Respecto a las recompensas que Tezos ofrece cada vez que se mina un bloque, podemos decir que minar un bloque supone un aumento de 512 tz y signar un bloque supone $32\Delta T^{-1}$ tez, donde ΔT es el intervalo de tiempos entre el bloque signado y su predecesor.[51]

2.13.4. Ventajas e inconvenientes

- ✔ Hay previsión de futuro con la adopción de los Zk-Snarks, para nutrir de seguridad la criptomoneda
- ✔ Consigue controlar la emisión de bloques añadiendo un tiempo de delay entre la generación cada uno de ellos
- ✔ Adopta el mecanismo de consenso *Proof of Stake*, por lo que desaparecen los grandes consumos que hay en protocolos como *Proof of Work*
- ✔ Es una criptomoneda por la que muchas instituciones han mostrado interés, aspecto que demuestra que hay interés por adoptarla
- ✕ Hoy en día, aunque haya previsión de adoptar Snarks, es una moneda que apenas goza de privacidad
- ✕ Adopta el protocolo de *Proof of Stake*, por lo que inversores con menos peso en la red no entran en la validación de bloques

2.14. MONERO (XMR)

2.14.1. Introducción

Monero fue lanzada en 2014 con el nombre inicial de *BitMonero*, pero rápidamente fue reducido a *Monero*, que es la traducción de *coin* al lenguaje *Esperanto*.[53]

Fue una moneda diseñada para proveer características como la fungibilidad y la privacidad de las transacciones, que era necesario para cualquier criptomoneda para que fuera factible para un uso general. De esta privacidad se hablará en el próximo apartado.[53]

Además, desde la fundación de Monero se percibió que el minado de cualquier criptomoneda podría aumentar a medida que los usuarios iban adquiriendo hardware cada vez más potentes. De esta manera, quien se pudiera pagar un hardware más costoso y con más potencia, acabarían consiguiendo ellos las recompensas de minar los bloques y se rompería con la descentralización de la criptomoneda, propiedad fundamental de la misma. Este problema se explica cómo se afrontó en el apartado *3.14.3. Minería* a continuación.[53]

2.14.2. Privacidad

Monero es la criptomoneda que más privacidad ofrece y es el referente en este ámbito para todas las otras criptomonedas. Monero dispone de más de un mecanismo para ofrecer privacidad y anonimato tanto en sus transacciones como en los usuarios que las realizan.

El primer mecanismo son las *Ring Confidential Transactions*. Esto consigue anonimizar la cantidad que se transfiere de origen a destino de manera que un usuario externo a esta transacción no consiga ver cuánto dinero se ha transferido. ¿Qué pasaría si, sabiendo que la cantidad de la transacción va a ser anónima, un usuario maliciosamente intenta hacer una transacción con un importe igual a cero o negativo? En este caso,

entraría en juego las *range proofs*, que son pruebas de conocimiento cero que consiguen demostrar, sin revelar la cantidad, que esta misma nunca es negativa y siempre es mayor que cero. Cuando esta característica se añadió a Monero, solamente dos meses más tarde el 98% de las transacciones ya usaban las *Ring Confidential Transactions*. Tanto fue el éxito que hoy en día es obligatorio usar este tipo de transacciones.[53]

La segunda característica que Monero usa para anonimizar sus transacciones, son las *stealth address*. Para ello, son direcciones de uso único generadas aleatoriamente que no identifican al recipiente y permiten enviar o recibir una transacción de manera que si alguien la intercepta, no pueda relacionar origen o destino con una identidad.[53]

Otra característica que añade Monero son las *Ring Signatures* o firmas en anillo. Este tipo de firmas se caracterizan por la no capacidad de identificar el firmante entre los que forman el anillo, de manera que nunca sabes quién es el que firma dicha transacción. Tal y como los propios fundadores de este tipo de firmas dijeron, *puedes tener la certeza que uno de los usuarios del anillo lo ha firmado, pero no puedes saber quién de ellos es el responsable de ello*. Para hacerlo todavía más difícil de averiguar, como mayor sea el anillo, más difícil resulta adivinar quién ha sido el encargado de firmar, por lo que llega un punto en el que acaba siendo casi imposible.[53]

Finalmente, el último mecanismo que aporta Monero para su privacidad, es el llamado *Kovri*. Este añade más seguridad y anonimato al usuario que inicia la transacción, anonimizando la IP del mismo, así como también su ubicación. De esta manera, no se puede hacer un *tracking* hasta el origen, puesto que ya no aparece ningún dato asociado al mismo.[53]

2.14.3. Minería

Como en muchas criptomonedas explicadas anteriormente, en Monero se usa el mecanismo de consenso *Proof of Work*. Este consiste en hacer calcular problemas matemáticos cada una de las máquinas que está minando en la red para conseguir cifrar antes el bloque y llevarse la recompensa. Este algoritmo, que parece el más justo puesto que se premia al mejor trabajador, con el avance del tiempo y de la tecnología ha sufrido algún retroceso importante. Como lo importante es tener el mayor *Hashrate* en tu ordenador (esto es la capacidad que tiene de calcular), el minado se convirtió en una tarea muy cara de realizar, puesto que el hardware que se necesitaba cada vez era más caro. Fue tan caro, que se acabaron cambiando las CPU por ASIC (*Application-specific integration circuits)* que pasaron a valer mucho dinero y muy poco asequible por algunos mineros. Esto provocó que, hoy en día, existan colonias de ordenadores albergados por unos pocos que se llevan toda la recompensa. Este problema rompe con una de las ideas iniciales de las criptomonedas, donde defendían la descentralización, es decir, el hecho de que nadie pudiera controlar su emisión ni su cantidad.[53]

Para solventar el problema anterior, Monero hizo una actualización del protocolo de *Proof of Work* que, por ejemplo, se usa en Bitcoin. Este nuevo algoritmo fue llamado *CryptoNight algorithm*. Este nuevo mecanismo de consenso, Monero consigue evitar el uso de estas nuevas CPU llamadas ASICs, con un algoritmo que es muy difícil de acelerar y que, por lo tanto, invertir en ASICs muy caras no acarrea tantos beneficios

como sí que puede traer a la red de Bitcoin. De esta manera, en Monero se quiere mantener esta idea de descentralización de la moneda y, así, seguir siendo fieles a la filosofía que se prometió con ello.[53]

En el momento de su emisión, la tasa de emisión de la moneda era de más de 30 XMR cada 2 minutos. Esta tasa ha ido decreciendo en el tiempo a medida que la dificultad de la red ha ido subiendo y, por lo tanto su Hashrate, haciéndola así más difícil de minar y consiguiendo recompensas más pequeñas. Actualmente, sigue decreciendo y se estima que seguirá con el mismo comportamiento hasta 2022, año en el que la recompensa se estabilizará a 0.6 XMR cada 2 minutos y permanecerá constante.[53]

2.14.4. Ventajas e inconvenientes

- ✔ Consigue anonimizar la cantidad que va dentro de la transacción con *Ring Confidential Transactions*
- ✔ Gracias a las *Stealth Address* y las *Ring Signatures*, se consigue anonimizar también tanto origen como destino de la transacción
- ✔ Debido al mecanismo *Kovri*, se consigue anonimizar también datos del origen como la IP y la ubicación propia
- ✔ Con el mecanismo *CryptoNight*, se consigue mantener una descentralización de la criptomoneda, evitando el uso de las ASICs ya comentadas anteriormente
- ✕ El minado de la criptomoneda se realiza mediante el mecanismo de consenso *Proof of Work*, por lo que supone un aumento de la capacidad de la máquina que está minando

3. Criptomoneda de mayor interés para su estudio

Con la finalidad de estudiar el minado de las criptomonedas, se decidirá una de las que se ha expuesto en el apartado anterior y se realizará el minado de la misma. Para ello, en esta sección del documento se van a comentar las criptomonedas que más interés han despertado a lo largo del estudio del arte, así como también se recordarán las ventajas e inconvenientes que cada una tenía con el fin de decidir de la mejor manera posible.

Empezando por el orden en el que se han descrito las criptomonedas en el apartado anterior, la primera en la que nos hemos fijado es **Bitcoin**. Fue así porque, aunque no presente prestaciones tecnológicas únicas o importantes, es la criptomoneda más cotizada y la que ha conseguido más nombre. Aún así, enseguida cuando la analizamos, vimos que no aportaba mucho desde el punto de vista de la privacidad de la criptomoneda ni de minería. En cuanto a privacidad, no implementa las construcciones matemáticas Snarks, claves para conseguir una completa anonimización en las transacciones que ya están implementando muchas criptomonedas; tampoco ofrece ninguna mejora de privacidad adicional al cifrado de los datos de las transacciones, como pueden ser signaturas en anillo que otras criptomonedas sí que implementan. En cuanto a la minería, usa el algoritmo *Proof of Work* que, como ya se ha ido comentando a lo largo del documento, supone un gasto en computación muy elevado. Tampoco vemos ninguna mejora adicional en cuanto a la minería, por lo que no nos despierta ningún interés.

Siguiendo el orden descrito, la siguiente criptomoneda que nos preguntamos si sería una buena candidata, fue **Ethereum**. Esto fue así debido a la posibilidad que nos presenta de ser usada para el mundo comercial con la implementación de los Smart Contracts. En cuanto a privacidad, destacaríamos la privacidad de Ethereum puesto que ha evolucionado hacia la adopción de los Snarks, que proporcionarían una medida adicional de seguridad y una anonimización completa de las transacciones. Aunque todavía no sea una realidad, podemos decir que en un futuro próximo hará un salto de calidad en este campo. En cuanto a minería, ahora mismo usa el protocolo *Proof of Work* pero hay previsto que se haga el salto a *Proof of Stake*. Este cambio mejoraría en el sentido del gasto computacional pero el protocolo sería menos justo, puesto que no se premiaría el esfuerzo empleado en la red sino que sería la reputación en la red la que ganaría.

La tercera criptomoneda que nos llamó la curiosidad fue **Stellar**. En cuanto a privacidad, Stellar no implementa los Snarks para la completa anonimización pero sí que añade características adicionales como el protocolo de enrutamiento *Onion routing*. Este protocolo añade tantas capas de protección como nodos intermedios hay en la transmisión de la transferencia, de tal manera que solo la pueden descifrar los nodos que tengan la clave privada. En cuanto a minería, tal y como se ha descrito en el apartado anterior, añade la característica del *Federated Voting* al protocolo *Federated Byzantine Agreement*. Esto supone que los nodos decidirán la validez del bloque en función del número de mineros que están de acuerdo en su validez evitando así que nodos maliciosos puedan decidir. Un problema que supone este protocolo es la demora en tiempo de validación de bloque que supone la característica *Federated Voting*, puesto que para cada bloque hay que vota, aceptar y confirmar que el bloque es válido.

Otra criptomoneda que nos ha llamado la atención es **Cardano**. En cuanto a privacidad, goza de seudonimización puesto que todavía no implementa ningún cifrado adicional, como podrían ser los ya comentados Snarks. Aún así, está en la hoja de ruta de la misma criptomoneda que, en un futuro próximo, se consigan implementar los Snarks, por lo que no estaríamos muy lejos de una criptomoneda a tener en cuenta desde el punto de vista de la privacidad. En cuanto a minería es donde esta criptomoneda nos ha parecido interesante. El algoritmo de consenso es propio de la criptomoneda, llamado *Ouroboros* que, como ya se ha comentado, está basado en *Proof of Stake* y se determina una época como el tiempo que hay para minar un bloque escogiendo así un minero para cada época. Este algoritmo, por un lado tiene alguna ventaja respecto a *Proof of Stake* puesto que aumenta el número de candidatos a minar el bloque, pero, por otro lado, tiene problemas con el tiempo de minado de bloque puesto que no acaba de ser eficiente, porque a veces el tiempo de minado es muy inferior a lo estipulado como época.

Finalmente, la última criptomoneda que nos llamó la atención es **Monero**. Desde el punto de vista de privacidad, Monero es la criptomoneda que más beneficios nos aporta. Por un lado, consigue encriptar el monto de las transacciones con las *Ring Confidential Transactions*; consigue también anonimizar las direcciones de origen y destino de una transacción con las *Stealth Adresses*; cifra cada una de las transacciones con las *Ring Signatures*, que no permite identificar quién ha firmado dicha transacción entre unos candidatos distribuidos en un anillo; y finalmente, consigue anonimizar la IP del origen de la transacción mediante el protocolo *Kovri*. Si nos fijamos en la minería, Monero está basado en *Proof of Work* pero controla el gasto computacional evitando el uso de ASICs. Cuando detecta que un minero está minando demasiado la criptomoneda, consigue cambiar el algoritmo de cifrado para que dicho minero tenga que cambiar el hardware usado para minar. Esto provoca que no esté tan masificada la red de minado y consigue también que los mineros no puedan invertir en hardware para centralizar la liberación de tokens de Monero.

Después de investigar las criptomonedas más famosas o con más cotización en el mercado y luego seleccionar las que mayor interés nos han despertado teniendo en cuenta sobretodo la privacidad y la minería, sin lugar a dudas nos quedamos con **Monero**. Esta criptomoneda tiene claros beneficios tanto relativos a privacidad como en minería. A continuación, explicamos los argumentos que nos han llevado a tomar dicha decisión:

- Es la única moneda que, mediante el protocolo *Ring Confidential Transactions*, consigue anonimizar el monto de la transacción
- Consigue anonimizar las direcciones de origen y destino mediante las *Stealth Adresses*
- Es la única criptomoneda que consigue anonimizar la IP del usuario que realiza la transacción.
- En cuanto a minería, aunque usa el protocolo *Proof of Work*, consigue controlar la minería de un minero, cambiando el algoritmo de cifrado
- Con este cambio de cifrado, también se consigue que la moneda no se centralice en los mismos mineros, por lo que evita que se establezcan mineros con ASICs muy potentes que consigan toda la criptomoneda.

4. Minado de Monero

En esta sección se va a explicar cómo se ha conseguido minar la criptomoneda Monero en distintos sistemas operativos y en distintas máquinas, estableciendo así una comparativa entre cada uno de ellos. En total se han probado dos ordenadores y una placa Raspberry Pi 3, con sistemas operativos diferentes. La razón de usar una Raspberry Pi 3 en lugar de una *Orange Pi PC 2* está explicado en la sección *Introducción* de este documento. Básicamente, fue un problema de demoras en pedidos y tiempos a manejar.

Minar con cada una de las máquinas no ha sido tarea fácil, puesto que la documentación es un poco confusa y muchas veces no describe el escenario exacto que hay en tu máquina. Es muy fácil encontrar documentación obsoleta o, simplemente, casos particulares que se documentan cómo si fueran el procedimiento habitual, por lo que en la máquina en la que tú quieras minar no se podrá seguir la documentación.

A continuación se detalla cómo es este proceso en cada uno de ellos.

4.1. Ordenador con Linux

Primero, se consiguió minar en un ordenador con un sistema operativo Linux. Para ello, se alquiló un *droplet* en Digital Ocean[54], puesto que no era posible minar con un ordenador personal y físico. Este *droplet*, tiene las siguientes características:

- Sistema operativo Linux
- 16 GB de memoria RAM
- 320 GB de disco duro
- 6 vCPUs

Para empezar, nos descargamos el software del repositorio oficial de Monero adecuado a nuestra infraestructura mediante el comando[55]:

```
wget https://github.com/monero-project/monero/releases/download/v0.15.0.1/monero-linux-x64-v0.15.0.1.tar.bz2
```

A continuación, siguiendo la documentación oficial de monero[56], verificamos que nos hemos descargado el software original que ha firmado el *core developer* de Monero, Ricardo Spagni. Para ello, primero importamos dicha firma:

```
curl https://raw.githubusercontent.com/monero-project/monero/master/utils/gpg_keys/fluffypony.asc | gpg --import
```

Y luego indicamos que confiamos en dicha firma:

```
gpg --edit-key 'BDA6BD7042B721C467A9759D7455C5E3C0CDCEB9'
trust
```

Para comprobar que los *hashes* que aparecen en la página oficial de monero son confiables, ejecutamos lo siguiente:

```
curl https://www.getmonero.org/downloads/hashes.txt | gpg --verify
```

Y comprobamos que en su *output* aparezca lo siguiente:

```
gpg: Good signature from "Riccardo Spagni <ric@spagni.net>" [full]
```

Ahora que ya hemos confiado con el hash del *core developer* de Monero y hemos comprobado que los hashes de la página oficial de monero no han sido manipulados, procederemos a comprobar que el hash del fichero descargado es el que corresponde con el de la web oficial de Monero[56]. Para ello, ejecutamos:

```
file_name=monero-linux-x64-v0.14.0.0.tar.bz2
file_hash=`sha256sum $file_name | cut -c 1-64`
curl https://www.getmonero.org/downloads/hashes.txt &gt; /tmp/reference-hashes.txt
gpg --verify /tmp/reference-hashes.txt
grep $file_hash /tmp/reference-hashes.txt
```

Si ambos hashes coinciden, la salida de los comandos anteriores tiene que ser el nombre del fichero y su correspondiente hash, que fue el resultado.

Una vez comprobada la integridad y la autenticidad del software de Monero descargado, descomprimimos la carpeta y creamos una wallet en la blockchain de Monero mediante el comando:

```
./monero-wallet-cli
```

Y una vez con la wallet creada, nos enseñó por pantalla la dirección de la misma junto con el *mnemonic* y nos guardamos ambos strings para su uso.

A continuación, antes de empezar a minar, necesitamos sincronizar nuestro nodo con la blockchain de Monero. Para ello, necesitamos habilitar las conexiones entrantes al puerto 18080, puesto que Monero escucha por este puerto y es necesario tenerlo abierto para su minado. Así, ejecutamos el siguiente comando que nos va a permitir establecer nuevas conexiones entrantes o ya establecidas:

```
iptables –A INPUT –ctstate ESTABLISHED,RELATED –j ACCEPT
```

Una vez abierto el puerto, queremos sincronizar nuestro nodo con la blockchain de Monero. Para ello, ejecutamos el comando:

```
./monerod –detach
```

Y lo dejamos un día sincronizando. Pasado un día, teníamos ya el nodo sincronizado con la blockchain y solo faltaba minar[56]. Para ello, ejecutamos:

```
./monerod –detach start_mining <@_wallet> --log-level 2
```

Y el nodo empezó a minar. Una prueba de ello fue la captura de pantalla que se adjunta a continuación, viendo que el nodo ya está minando en la blockchain de Monero:

```
2020-01-25 14:51:47.470 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:120   PERF            ----------
2020-01-25 14:51:47.470 [P2P9]  DEBUG   blockchain      src/cryptonote_core/blockchain.cpp:2993 Mixin: 10-10
2020-01-25 14:51:47.470 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:156   PERF        6      expand_transaction_2
2020-01-25 14:51:47.470     7fd5e9398700        INFO    perf.ringct     src/common/perf_timer.cpp:120   PERF            ----------
2020-01-25 14:51:47.477     7fd5e9398700        INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     6214    verRctMGSimple
2020-01-25 14:51:47.477 [P2P9]  INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     6613        verRctMGSimple
2020-01-25 14:51:47.477 [P2P9]  INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     6813      verRctNonSemanticsSimple
2020-01-25 14:51:47.477 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:156   PERF     7161    check_tx_inputs
2020-01-25 14:51:47.477 [P2P9]  DEBUG   txpool  src/cryptonote_core/tx_pool.cpp:1352      added, new block weight 15620/599400, coinbase 1.968168291551
2020-01-25 14:51:47.477 [P2P9]  DEBUG   txpool  src/cryptonote_core/tx_pool.cpp:1263    Considering <050d2eld3d4a0318d28d9fbef7d9d4996785b74b4cd55c73b7e8dca55cca2c2b>,
weight 2604, current block weight 15620/599400, current coinbase 1.968168291551
2020-01-25 14:51:47.478 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:120   PERF            ----------
2020-01-25 14:51:47.478 [P2P9]  DEBUG   blockchain      src/cryptonote_core/blockchain.cpp:2993 Mixin: 10-10
2020-01-25 14:51:47.478 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:156   PERF        4      expand_transaction_2
2020-01-25 14:51:47.478     7fd5e8996700        INFO    perf.ringct     src/common/perf_timer.cpp:120   PERF            ----------
2020-01-25 14:51:47.485 [P2P9]  INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     6612        verRctMGSimple
2020-01-25 14:51:47.487     7fd5e8996700        INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     9284    verRctMGSimple
2020-01-25 14:51:47.487 [P2P9]  INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     9543      verRctNonSemanticsSimple
2020-01-25 14:51:47.488 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:156   PERF    10042    check_tx_inputs
2020-01-25 14:51:47.488 [P2P9]  DEBUG   txpool  src/cryptonote_core/tx_pool.cpp:1352      added, new block weight 18224/599400, coinbase 1.968339041551
2020-01-25 14:51:47.488 [P2P9]  DEBUG   txpool  src/cryptonote_core/tx_pool.cpp:1263    Considering <0b31f42e6b6c0c895b8974ed150eb2b951de29d842d9adfe2f92358fa6d97140>,
weight 2604, current block weight 18224/599400, current coinbase 1.968339041551
2020-01-25 14:51:47.488 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:120   PERF            ----------
2020-01-25 14:51:47.488 [P2P9]  DEBUG   blockchain      src/cryptonote_core/blockchain.cpp:2993 Mixin: 10-10
2020-01-25 14:51:47.488 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:156   PERF        7      expand_transaction_2
2020-01-25 14:51:47.489     7fd5e9398700        INFO    perf.ringct     src/common/perf_timer.cpp:120   PERF            ----------
2020-01-25 14:51:47.496     7fd5e9398700        INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     6995    verRctMGSimple
2020-01-25 14:51:47.496 [P2P9]  INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     7388        verRctMGSimple
2020-01-25 14:51:47.496 [P2P9]  INFO    perf.ringct     src/common/perf_timer.cpp:156   PERF     7596      verRctNonSemanticsSimple
2020-01-25 14:51:47.496 [P2P9]  INFO    perf.blockchain src/common/perf_timer.cpp:156   PERF     7597    check_tx_inputs
2020-01-25 14:51:47.496 [P2P9]  DEBUG   txpool  src/cryptonote_core/tx_pool.cpp:1352      added, new block weight 20828/599400, coinbase 1.968509791551
```

Figura 4. Minado en Linux

Siguiendo este procedimiento, es como conseguimos minar en el sistema operativo Linux mediante un *droplet* alquilado en *Digital Ocean*.

Ahora, con el fin de comparar los sistemas operativos Linux, Windows y la placa Raspberry Pi 3 con el ordenador y el droplet, buscamos comparar el ratio de hashes por cada vatio de potencia. De esta manera, vamos a buscar las medidas que nos faltan para encontrar este ratio y poder comparar los 3 casos comentados:

- Hashrate: Para este hashrate, hemos ejecutado otro cliente de Monero que nos daba métricas sobre la velocidad a la que minábamos[57]. Así, hemos conseguido ver el hashrate de nuestra máquina, que es aproximadamente de 1780 H/s.
- Potencia: Mediante la herramienta *powerstat*, conseguimos ver que nuestro droplet consume una potencia de 420 W.[58]

Conseguidas las medidas necesarias para calcular el ratio entre el hashrate y la potencia consumida, pasamos a calcularlo para poder comprobar con los demás escenarios. Así, calculamos el ratio (S) entre el hashrate que el mismo *droplet* consigue ofrecer y la potencia en vatios que consume:

$$S = \frac{H(\frac{H}{s})}{P(W)} = \frac{1780\ H/s}{420\ W} = 4.23\ H/W$$

4.2. Ordenador con Windows

Después de conseguir minar en Linux, se pasó a minar con Windows. El ordenador con el que se minó, esta vez sí que era un ordenador personal, y se hizo estando dentro de una red local. Así, las características del ordenador con el que se hizo la prueba son las siguientes:

- Sistema operativo Windows
- 4GB de memoria RAM
- 500GB de disco duro SSD
- 1 CPU

Con las características anteriores, se intentó minar Monero en Windows. Para ello, se puede hacer de dos maneras:

- Mediante una consola *git* que emula un sistema operativo Linux dentro del Windows.[55]
- Descargándose el ejecutable desde la página oficial de Monero y realizarlo mediante interfaz gráfica.[59]

Para este caso, se escogió la segunda opción de las expuestas anteriormente, puesto que la primera era repetir con exactitud los pasos seguidos en el apartado *4.1. Ordenador con Linux*.

Para descargarse el ejecutable, nos dirigimos a la página oficial de Monero[59] y, en la sección de *Downloads*, nos descargamos el instalador para Windows:

Figura 5. Versiones software minado Windows

En nuestro caso, seleccionamos el primero, *Windows 64-bit (Installer)*. Esto nos descargó un ejecutable donde nos creamos una *wallet* (distinta a la del caso anterior). Antes de proseguir con el ejecutable, igual que con Linux, necesitamos abrir el puerto 18080 y 18081 para realizar el minado. Ahora, como nos encontramos en una red local doméstica, tuvimos que entrar al router mediante el usuario y contraseña que el fabricante nos proporcionó y tuvimos que abrir los puertos correspondientes:

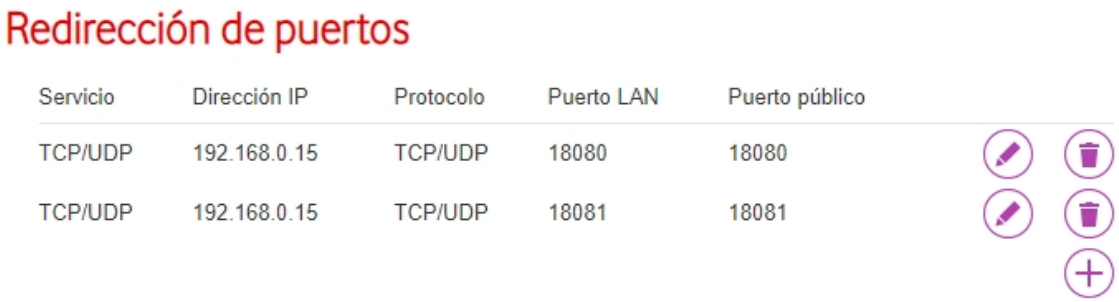

Figura 6. Redirección puertos en router

Finalmente, con la interfaz ya abierta:

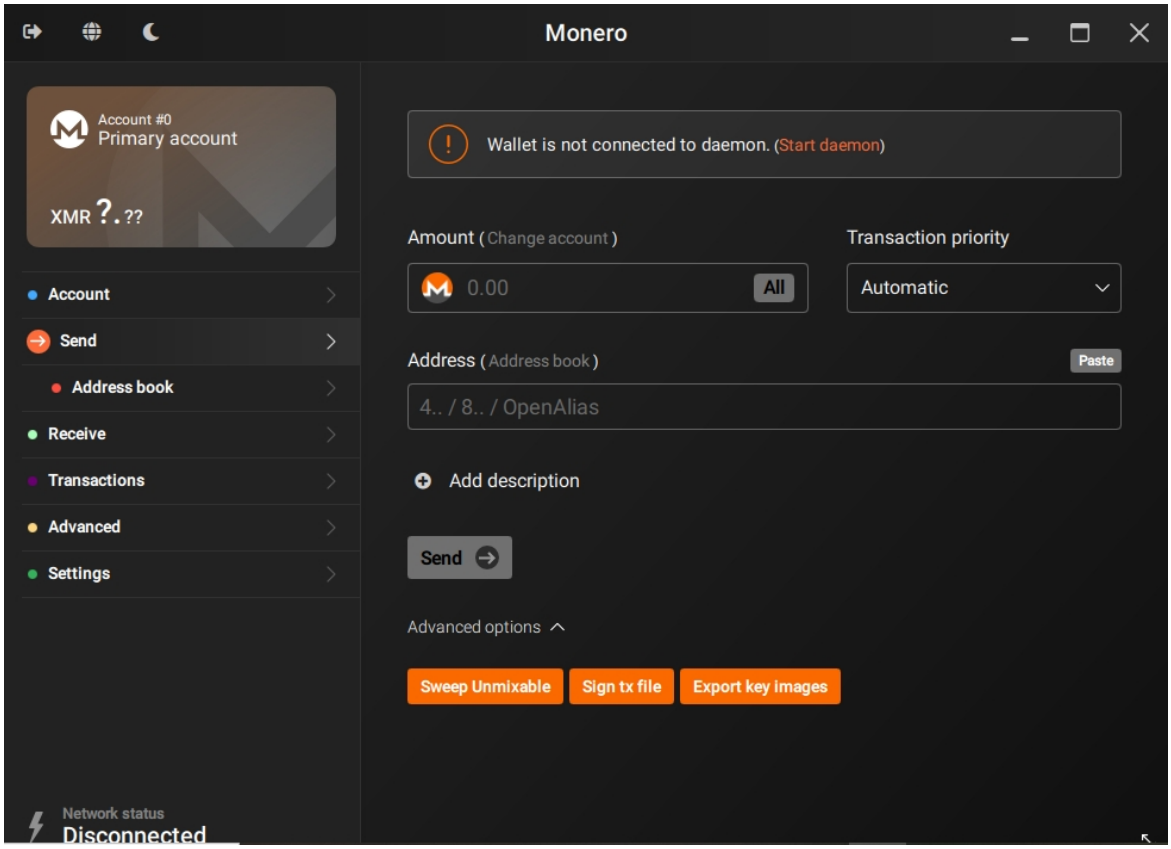

Figura 7. Minado Windows

Haciendo un clic en la opción *Start daemon*, se crea un proceso que empieza a sincronizar el nodo con la red blockchain de Monero. Una vez dicho proceso ha finalizado, nos dirigimos a la pestaña *Advanced* > *Mining* donde podremos cambiar la configuración para el minado:

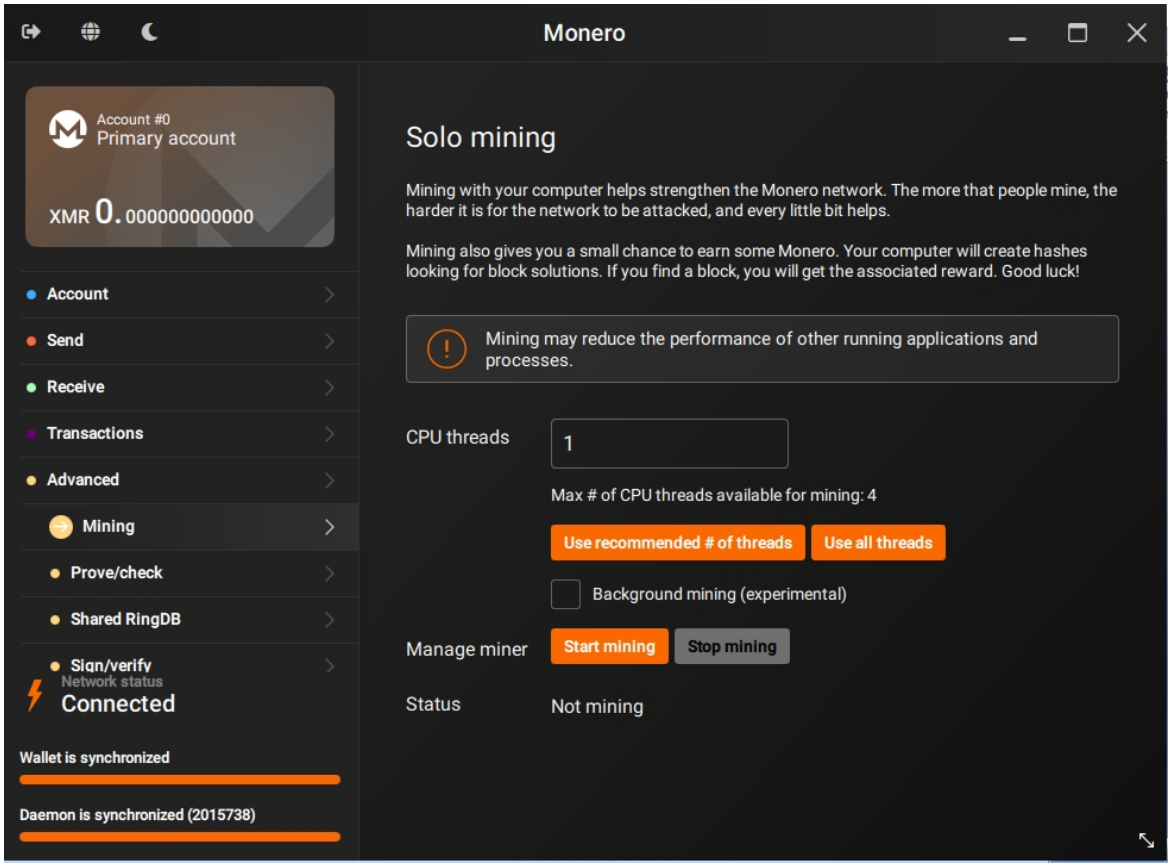

Figura 8. Configuración minado en Windows

Como podemos ver, podemos seleccionar el número de threads que queremos que ejecuten este minado y también podemos pedirle que el minado lo ejecute en *background*. Finalmente, si queremos empezar a minar, solamente tenemos que hacer clic en el botón de *Start mining*, y veremos como el nodo empieza a minar:

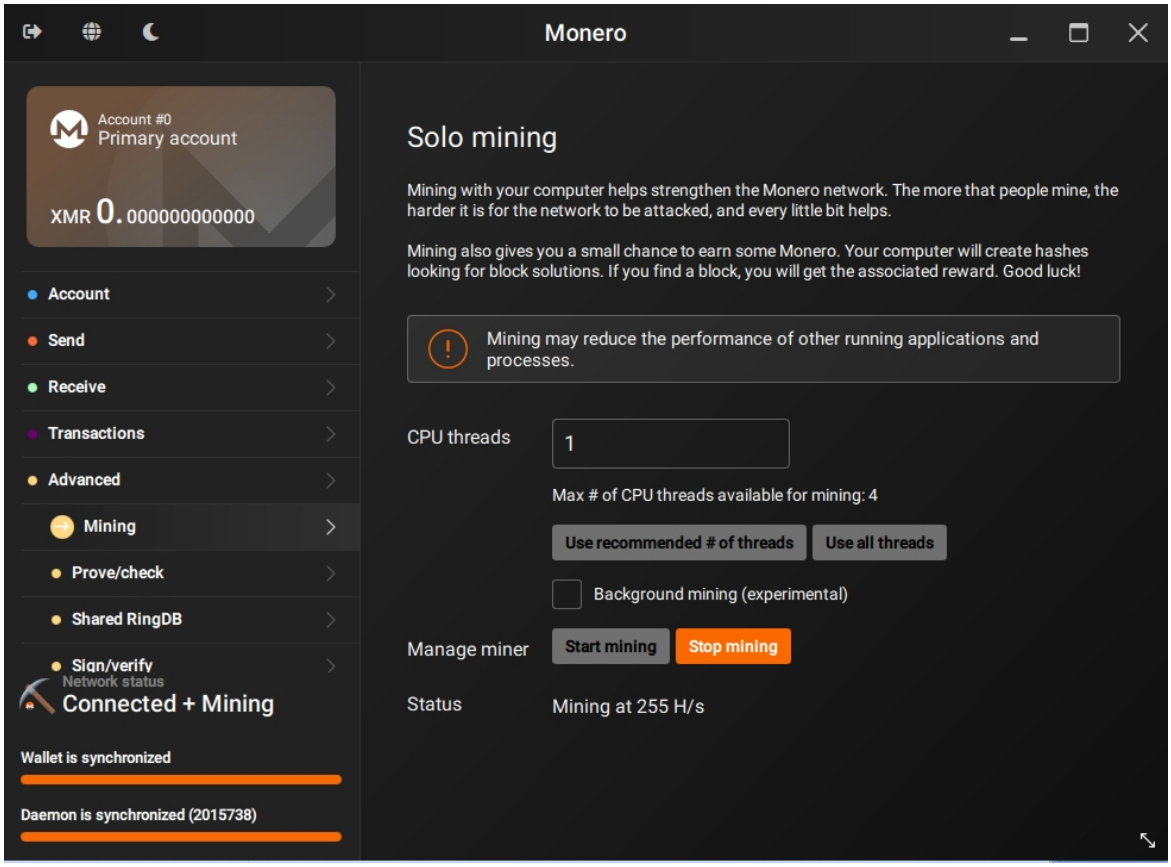

Figura 9. Estado mining en Windows

Como podemos ver, el *status* es *Mining* y estamos minando a 255 hashes por segundo. También, abajo a la izquierda, vemos como el nodo está en el estado *Connected + Mining*.

De esta manera, mediante la interfaz gráfica que nos proporciona Monero, conseguimos minar con el sistema operativo Windows.

Con el objetivo de poder comparar la capacidad de minado de este ordenador con el anterior explicado o la placa Raspberry Pi 3, vemos que este ordenador es capaz de minar a un ratio de 280 H/s, aproximadamente. Para ver la relación entre la potencia que consume y el hashrate que este saca de salida, calculamos estos dos valores:

- Hashrate: Lo obtenemos de la propia interfaz del programa que se ha usado. A modo de corroborar que el valor es correcto, también se ha minado con el programa de *Minergate*, que más o menos ha sacado el mismo output. De esta manera, podemos comprobar que el hashrate del ordenador es de 280 H/s.
- Potencia: La potencia del ordenador la podemos obtener mediante la siguiente ecuación:
  $P = \frac{V^2}{I}$, donde V es la tensión de alimentación que necesita el ordenador e I la intensidad que el mismo soporta. De esta manera, para una tensión de 19V y una intensidad de 3.42A, obtenemos una potencia de 105,55W.

Con las métricas calculadas arriba, podemos obtener la capacidad de cálculo o hashrate por cada vatio de potencia (S). Así, conseguimos la medida que buscamos y nos servirá para comprobar cada casuística, de la siguiente manera:

$$S = \frac{H}{P} = \frac{280\ H/s}{105.55\ W} = 2.65\ H/W$$

Con este resultado, podemos asegurar que nuestro ordenador es capaz de sacar 2.65 hashes por cada vatio de potencia.

4.3. Raspberry Pi

Tal y como ya se ha comentado al principio de este documento, por problemas de tiempo no hemos podido minar con la placa Orange Pi PC 2 y lo hemos acabado haciendo con una Raspberry Pi. La Raspberry Pi es mucho más conocida y hay menos problemas para encontrar recambios, por lo que ha sido más rápido conseguir una para poder minar. Si miramos diferencias entre esta placa y la Orange Pi, podemos destacar que la Orange Pi es un poco más rápida que la Raspberry Pi, puesto que consigue más hashes por segundo. Aún así, el valor que hemos conseguido se acerca mucho al que conseguiríamos con una Orange Pi.

Así, vamos a explicar cómo se ha conseguido minar con la Raspberry Pi, aunque antes vamos a detallar los requisitos de dicha placa:

- Sistema operativo Linux
- 2GB de memoria RAM
- Tarjeta SD de 32GB
- 1 CPU

Como vemos, en cuanto a prestaciones muy inferior a los dos ordenadores que hemos presentado en las secciones anteriores. Esto implica que, por un lado, el hashrate que vamos a obtener con esta placa es muy inferior a los dos anteriores; aún así, esto se compensa por el precio, que también es muy inferior al de un ordenador. Esto nos abre la puerta a evaluar y pensar qué nos va a salir más a cuenta, si minar a menor hashrate con más de una placa más barata o a mayor hashrate con un ordenador bastante más caro.

Si nos fijamos en el proceso que nos ha llevado a conseguir minar con la Raspberry Pi, vamos a ver que ha sido muy parecido al primero, debido al sistema operativo. Para empezar, tuvimos que cargar un sistema operativo a la placa. El que nos hubiera gustado probar era el sistema operativo Raspbian, aunque por cuestiones de tiempo, le cargamos un Ubuntu 16 para agilizar el trabajo. Así, grabamos un Ubuntu 16 en la tarjeta SD y, una vez conectada con un cable Ethernet al router, un USB para tener control sobre la misma con el ordenador y el cable de la alimentación, conseguimos arrancar la Raspberry Pi con un sistema operativo Ubuntu 16. Para poder hacer login con una consola remota, obtuvimos la IP de la placa entrando en la interfaz del router. Una vez conocida, conseguimos hacer un *ssh* para hacer login en la placa y cambiar la contraseña por defecto. Llegados a este punto, ya teníamos la placa lista para descargarnos el software y minar.

A continuación, para no repetir el mismo procedimiento que en los casos de arriba, decidimos coger un cliente diferente a los anteriores, el *xmrig*. Este cliente nos da mucha facilidad a la hora de minar una criptomoneda, dándonos muchos más datos que los anteriores y una facilidad muy grande para levantar un minero en la misma red. Así,

empezamos ejecutando el siguiente comando para descargarnos las librerías y dependencias que vamos a usar para minar[57]:

```
sudo apt-get install git build-essential cmake libuv1-dev libssl-dev libhwloc-dev
```

A continuación, procedemos a descargarnos el software que usaremos para minar directamente de github:

```
git clone https://github.com/xmrig/xmrig.git
```

Luego, entramos dentro de la carpeta clonada y creamos una nueva carpeta donde vamos a dejar el software compilado:

```
cd xmrig && mkdir build && cd build
```

Compilamos el software que nos hemos descargado:

```
cmake ..
make
```

Ahora ya tenemos el software compilado y listo para usarlo. Para poderlo usar, nos dirigimos a la página oficial del cliente de minado[60] y configuramos nuestro minero XMRig:

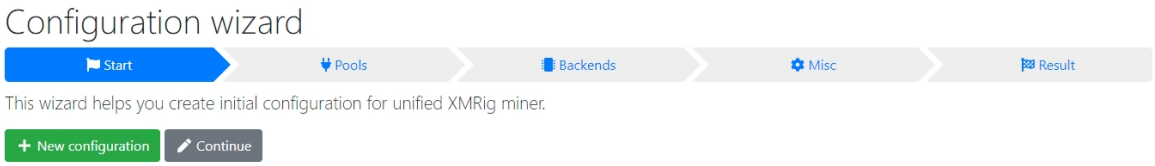

Figura 10. Configuración proceso minado Raspberry Pi

Para ello, en la página configuramos las siguientes opciones:

- Añadimos un proceso *solo mining*, esto es sin participar en ninguna *pool*, escuchando en nuestra máquina por el puerto 18081. Configuramos también una de las wallets de las que ya disponíamos.
- En la pestaña *Backend*, seleccionamos CPU
- En la siguiente dejamos la donación por defecto (5%)

Finalmente, la última pestaña nos da el comando que debemos utilizar en función de la configuración que hemos escogido. Así, vamos a la Raspberry Pi y ejecutamos el comando que nos han dado:

```
./xmrig -o 127.0.0.1:18081 -u
56ix6ibaYSBQCmQEt1GQ8uAGhw3by7ecRBuALFjKuvu5NcmLsXMHkbsVytbe7fdhstYFUct8PGf4ggt
hcUThE4uy5aiqBgg --coin monero –daemon
```

Y empezamos a minar con la Raspberry Pi. De esta manera tan fácil, utilizando Ubuntu y el cliente de minado XMRig, conseguimos minar en la Raspberry Pi. Así, para poder comparar entre la propia Raspberry Pi y los ordenadores anteriores, sacamos las siguientes medidas:

- *Hashrate:* A través de la propia interfaz, podemos sacar el hashrate que, aproximadamente, es de unos 13 hashes por segundo.

- <u>Potencia:</u> Igual que hemos calculado en apartados anteriores, calculamos la potencia mediante la siguiente fórmula:
  $P = \frac{V^2}{I}$, donde V es la tensión de alimentación a la que se conecta la Raspberry Pi y la Intensidad es la que permite que dicha placa tenga corriente para funcionar. De esta manera, la fórmula seguiría de la siguiente manera:
  $P = \frac{V^2}{I} = \frac{5{,}1^2}{2.5} = 10.4\ W.$

Conseguidas las medidas necesarias para calcular el ratio entre el hashrate y la potencia consumida, vamos a calcular los hashes por cada vatio de potencia que consigue la Raspberry Pi 3. Para ello, resolvemos la siguiente ecuación:

$$S = \frac{H}{P} = \frac{13\ h/s}{10.4\ W} = 1.25\ ha\ \ he.\ /W$$

De esta manera, podemos ver como una Raspberry Pi 3 como la que nos hemos comprado, puede conseguir un ratio de 1.25 hashes por cada vatio de potencia consumida.

5. Resultados

En esta sección, se van a presentar los resultados del estudio realizado a lo largo de este documento. Estos resultados están basados sobre todo en la sección anterior, dónde se explica cómo se ha realizado el minado en cada una de las máquinas dependiendo del sistema operativo y se calcula la potencia y el hashrate de cada uno de los casos junto con el ratio de hashes por vatio de potencia. Para ello, el objetivo es saber si nos va a salir más a cuenta minar con un ordenador o con placas más pequeñas como una Raspberry Pi.

Empezando por el primer caso, un ordenador con un sistema operativo Linux con las características que arriba se explican, obtenemos las siguientes medidas:

- Hashrate: 1780 hashes por segundo
- Potencia: 420 vatios
- Ratio hashes/vatios: 4.23 hashes por cada vatio

Tal y como se explica arriba, este ordenador es el más potente, puesto que tiene muchos más cores que los otros y más memoria RAM. Aún así, habrá que comparar la potencia y el ratio de hashes por vatio con los demás para comprobar si es cierto que nos sale más a cuenta este. Un aspecto a tener en cuenta también es la inversión inicial que se hace por el ordenador en cuestión. En este caso, un ordenador de estas dimensiones está valorado en aproximadamente unos 700€

El segundo caso, un ordenador con un sistema operativo Windows valorado en unos 350€ y unas prestaciones inferiores (arriba explicadas) conseguimos las siguientes medidas:

- Hashrate: 280 hashes por segundo
- Potencia: 105.55 vatios
- Ratio hashes/vatios: 2.65 hashes por segundo

Como vemos, este ordenador consigue un hashrate y un ratio de hashes/vatio muy inferior al anterior, debido a que sus características son inferiores. Aún así, también vemos que su potencia es bastante inferior al anterior, así como su precio de mercado.

En tercer lugar, tenemos una Raspberry Pi 3 valorada en 50€ que nos da las siguientes medidas:

- Hashrate: 13 hashes por segundo
- Potencia: 10.4 vatios
- Ratio hashes/vatios: 1.25 hashes por segundo

Como comprobamos, el chip con menores prestaciones de los tres, también obtiene unas medidas muy inferiores. Aún así, vemos como su precio de mercado también es muy inferior.

Estudiados los tres ejemplos anteriores, queremos decidir qué nos puede salir más barato para minar, teniendo en cuenta las tres medidas observadas y su precio de mercado. La medida que nos marcará la potencia de cada ordenador es el ratio de hashes por vatio, puesto que nos indica cómo de potente es teniendo en cuenta el consumo de potencia. Como mayor sea este indicador, más potencia tendrá gastando la

misma o menor potencia. Así, si nos fijamos en este indicador, el ordenador escogido es el primero, puesto que resuelve más hashes por cada vatio que consume.

Aún así, hay un elemento diferencial en los tres que nos puede ayudar también a decidir. Este elemento es su precio de mercado. Mientras que el primer ordenador es el más potente, también es el más caro. Así, un elemento a tener en cuenta es comprar más de un ordenador menos potente, hasta llegar a la inversión inicial de un ordenador como el primer ejemplo. De esta manera, conseguiríamos multiplicar este ratio de hash por cada vatio y podríamos tener una inversión inicial más pequeña. Si nos fijamos en esto, vamos a ver cuántos ordenadores más pequeños necesitamos para tener la inversión inicial del primero y conseguir un ratio más elevado.

Para un ordenador como el segundo tipo, con dos ordenadores conseguiríamos la inversión inicial del ordenador más potente. Así, si multiplicamos por dos el ratio de hashes por cada vatio, conseguiremos un ratio de 5.3 hashes por cada vatio frente a los 4.23 hashes por cada vatio del primer ejemplo. Justo para este ordenador, ya tenemos más ratio de hashes por cada vatio por la misma inversión inicial, por lo que deduciríamos que preferimos minar con dos ordenadores del segundo tipo antes que con uno del primer tipo, sujetos a la misma inversión inicial.

Si ahora nos fijamos en una Raspberry Pi como las del tercer tipo, vamos a ver que, con cinco chips iguales, vamos a conseguir un ratio por cada vatio de potencia de 6.25 hashes por cada vatio. Como comprobamos fácilmente, conseguimos un ratio bastante mejor que con un ordenador del primer tipo y que con dos ordenadores del segundo tipo. Si nos fijamos ahora en la inversión que supone comprar cinco chips como la Raspberry Pi 3, vemos que tan solo nos cuesta 200€, incluso superior que un solo ordenador del tipo 2.

Para acabar, analizando los casos expuestos justo más arriba, vemos fácilmente cuál es el chip que nos sale más a cuenta para minar. Con cinco Raspberry Pi 3 con las características que se explican más arriba, que tienen un precio de mercado total de 200€, conseguimos nada más ni nada menos que 6.25 hashes por cada vatio de potencia, mientras que con dos ordenadores del segundo tipo, conseguimos tan solo 5.3 hashes por cada vatio por una inversión inicial de 700€. Así, deducimos y concluimos que la manera con la que nos sale más a cuenta minar la criptomoneda Monero es, sin duda, con **más de un chip como la Raspberry Pi 3** en lugar de un ordenador más potente pero que, a su vez, sea más caro.

6. Costes

En este proyecto no estaban previstos gastos muy elevados ni ningún tipo de inversión pero, por incidencias que han ocurrido que ya se han comentado en el mismo documento, han acabado habiendo unos mínimos costes. Aún así, no han sido elevados y han servido para conseguir los objetivos, así como también explorar distintas alternativas que han aportado valor al proyecto.

Entrando en materia, los costes que nos hemos encontrado durante el proyecto han sido los siguientes:

- Alquiler Droplet. Alquilamos un *droplet* en Digital Ocean para conseguir minar con un sistema operativo Ubuntu y el cliente *xmr-stack*. Este droplet costava 80$ al mes, si estaba las 24h encendido y funcionando. Como apenas ha estado un par de semanas funcionando, ha resultado un coste de 35.17$ en total, que equivalen a 31.90€.
- Compra Orange Pi PC 2. El segundo coste que nos encontramos fue la compra de la placa con la que queríamos minar al principio del proyecto. Como ya se ha comentado a lo largo del documento, por problemas con la fuente de alimentación, al final no se utilizó dicha placa y se compró una Raspberry Pi 3. El coste de la Orange Pi PC 2 consta de distintos elementos, que se detallan a continuación:
    - Placa Orange Pi PC 2. La placa en sí costó 23,51€, sin ningún cable para su utilización.
    - Tarjeta SD para Orange Pi PC 2. Para formatear la placa Orange Pi PC 2, se usó una tarjeta SD de 32 GB, cuyo coste fue un total de 4.95€
    - Periféricos para el uso de la placa: Tuvimos que comprar todos los periféricos para poder usar la placa. Estos periféricos, se componen de los siguientes elementos:
        - Cable Ethernet
        - Cable USB-USB
        - Cable microUSB de tipo OTG

      Todos los periféricos sumaron un total de 3,75€
- Cable alimentación placa Orange Pi PC 2. Aunque no funcionó, también compramos un alimentador para nuestra placa Orange Pi PC 2. Al no ser el original, nos dio problemas y al final optamos por sustituir la placa por una Raspberry Pi. Este alimentador nos costó un total de 25€.
- Placa Raspberry Pi 3. Debido al problema que tuvimos con la placa Orange Pi PC 2, acabamos comprando una Raspberry Pi 3, debido a que es mucho más accesible y así podíamos conseguir minar con una placa en lugar de un ordenador. Esta compra incluye tanto la propia placa como el alimentador, puesto que los periféricos reutilizamos los que ya habíamos comprado con la Orange Pi PC 2, que eran compatibles. Así, este costó fue un total de 51.85€.
- Coste humano. Finalmente, el último coste asociado a dicho proyecto es el coste humano o el valor de las horas invertidas en este proyecto. Para ello, se han invertido unas 550 horas, que equivalen a las 495 horas del precio medio de un crédito multiplicado por el número total de créditos ECTS de los que consta la asignatura, más un total de 55 horas de trabajo extra personal. Fijando que el

precio a la hora de trabajo se establece en 12€ cada hora, sale el coste humano que ha supuesto este trabajo:
$C = n * \mathrm{p}$, donde n es el número de horas invertidas y p el precio de la hora. De esta manera, sale un coste total de:
$C = \mathrm{n} * \mathrm{p} = 550 * 12 = 6600€$.

Para resumir el total de costes, se ha elaborado una tabla donde queda mejor explicado. A continuación, se resume el total de costes implicados en el mismo proyecto:

COSTES TOTALES	
Alquiler Droplet	31,90 €
Placa Orange Pi PC 2	23,51 €
Tarjeta SD 32GB	4,95 €
Periféricos Orange Pi PC 2	3,75 €
Alimentador Orange Pi PC 2	25,00 €
Raspberry Pi 3	51,85 €
Coste humano	6.600,00 €
TOTAL COSTE TRABAJO	6.740,96 €

Tabla 9. Costes totales

7. Impacto medioambiental

En esta sección del documento, se va a comentar el impacto medioambiental que tiene el tema que se ha tratado y los costes que ello provoca.

En efecto, la minería en las criptomonedas es un tema importante que afecta al medioambiente debido a la gran cantidad de potencia que ello supone, puesto que hay muchos mineros conectados a la vez haciendo trabajar cada uno de sus ordenadores, que a su vez es un gasto de potencia muy elevado.

Como ya se ha comentado a lo largo del documento, hay dos protocolos de consenso para el minado principales: *Proof of Work* y *Proof of Stake*. El primero, se basa en que el primer en calcular y cifrar el bloque siguiente consigue dicha recompensa, y el segundo, en cambio, se basa en la elección de un minero que tenga reputación en la red y este lo cifra automáticamente. Aún así, ambos protocolos contribuyen con fuerza en el medioambiente y desde este apartado se quería hacer una crítica a ello.

7.1. Método *Proof of Work*

Este protocolo de consenso es el más contaminante de todos los que existen. Esto es así porque muchos mineros a la vez ponen sus ordenadores a calcular a máximo rendimiento el *hash* del próximo bloque.

En este apartado, se ha analizado el consumo de potencia de distintos tipos de hardware que se utilizan en algunas criptomonedas que usan el mecanismo de consenso de *Proof of Work*. Para ello, se va a usar la misma medida que se ha usado para decidir qué máquina nos salía más a cuenta a la hora de minar, el ratio entre hashrate y potencia en vatios consumida, realizando a posteriori una estimación optimista de la potencia total consumida de la red.

Siguiendo el procedimiento descrito anteriormente, viendo el hardware que está disponible para minar criptomonedas que se basan en el algoritmo *Proof of Work*, buscamos el dispositivo que nos permita tener más alto el ratio entre hashrate y potencia consumida en vatios, que si luego extrapolamos a que toda la red tiene el mismo hardware, tendremos una estimación optimista[61]. Este dispositivo es la ASIC **AvalonMiner 1047**, que podemos ver en la siguiente imagen:

Figura 11. AvalonMiner 1047

De este modo, para calcular el gasto de energía que supone que todos los mineros de la red de Bitcoin estén usando el hardware más eficiente, disponemos de los siguientes datos:

- Hashrate de AvalonMiner 1047: 37.000 GH/s

- <u>Consumo de potencia de AvalonMiner 1047:</u> 1047 W

También sabemos que el hashrate total de la red de Bitcoin es de 11.649.657 TH/s[62]. Así, para calcular el consumo total de potencia que habría en la red de Bitcoin si todos los mineros usaran el hardware más eficiente, se calcularía de la siguiente manera:

$$A = \frac{H \quad hr \quad t}{H \quad hr \quad A} * P(W\ a \qquad) = \frac{11649657000\frac{G}{s}}{37000\frac{G}{s}} * 1047W = 329{,}65\ M$$

Un total de casi 330 MW es lo que gastarían todos los mineros de la red de Bitcoin si usaran este hardware. Como ya hemos comentado, esto es una estimación optimista, puesto que no todos utilizarán el más eficiente, puesto que también es el más caro.

Si de este consumo de potencia suponemos que está encendido todo el día minando sobre la misma red, a lo largo del mes obtenemos que toda la red de Bitcoin genera una energía de:

$$E = A * 24\text{h} * 31\text{días} = 329{,}65\ \text{MW} * 24\text{h} * 31\text{días} = 245{,}26\ \text{GWh/mes}$$

Si ahora vemos que el gasto de energía promedio de un ciudadano de Barcelona es de 349.53 kwh al mes[63][64], podemos deducir la cantidad de habitantes que generaran la potencia anteriormente calculada:

$$nhab \qquad = \frac{E}{E} = \frac{2 \qquad k \quad h}{3 \quad .5 \quad k \quad h} = 701685\ ha$$

Esta cifra nos indica que, en España, una media de 701685 habitantes generaran la misma energía que está generando toda la red de Bitcoin. Esto, si echamos un ojo al número de habitantes que tienen las principales ciudades del país, vemos que la cifra es mayor que el número de habitantes de Sevilla (cuarta ciudad más poblada en España) y menos que Valencia (tercera ciudad más poblada en España).[65]

Así, vemos que el algoritmo *Proof of Work* en la red de Bitcoin supone un gasto de energía que equivaldría a tener una ciudad más en España que ocupara el cuarto sitio en cuanto a población.

7.2. <u>Método *Proof of Stake*</u>

Una vez visto que el método de *Proof of Work* supone un gasto en potencia muy elevado, que se convierte en mucho gasto medioambiental, podemos pensar que el método de *Proof of Stake* es el idóneo para utilizar en blockchains.

En defensa del método de *Proof of Stake*, cabe decir que, como no existe el minado porque alguien que tiene una cierta reputación en la red cifra el bloque directamente, este protocolo no consume apenas potencia, por lo que sería el más viable y preferible desde el punto de vista medioambiental.

Aún así, *Proof of Stake* rompe un poco con la filosofía de blockchain, puesto que no puede minar un minero que acaba de llegar a la red puesto que no tiene ganada esta cierta reputación que se necesita. Esto es incompatible con la filosofía de que cada minero debería tener las mismas posibilidades de cifrar y minar un bloque, y desaparecería la famosa justicia que se encontraba en *Proof of Work* en la que como más se trabajaba, más probabilidad de conseguirla hay.

De esta manera, podemos concluir que desde el punto de vista medioambiental, es mucho más preferible el método de consenso *Proof of Stake*, puesto que el gasto en potencia es cero y no supone una contaminación para el medio ambiente. Aún así, como inconveniente grave tenemos que desaparece la justicia que tan famosa se ha hecho con la tecnología blockchain en la que como más se trabajaba, más probabilidad había de conseguir una recompensa.

7.3. Método *Alogrand*

Este protocolo de consenso está basado en el anterior *Proof of Stake*, aunque aporta beneficios en cuanto a la manera en la que los mineros llegan a un consenso.

Para empezar, la minería es exactamente igual que en el algoritmo de *Proof of Stake*, en el que un minero no tiene que calcular ningún hash, firma el bloque y lo añade automáticamente a la blockchain. Para ello, desaparece la minería y el gasto computacional, aspecto que valoramos muy positivamente desde el punto de vista medioambiental, debido a que no genera tanto residuo para la sociedad.

Por otro lado, el algoritmo de *Proof of Stake* decíamos que pierde un poco la justicia que sí que nos aportaba el algoritmo clásico de *Proof of Work*, puesto que quién más trabajaba se llevaba la recompensa y, en el algoritmo de *Proof of Stake*, necesitabas tener un mínimo de reputación o riqueza en la red para poder cifrar un bloque, por lo que dicho proceso no estaba abierto a todo el mundo. En cambio, el algoritmo *Algorand*[66] se desmarca en este punto de *Proof of Stake*, y abre el proceso de cifrado de bloque a todo el mundo. Para ello, solamente impone la condición que tiene que ser usuario de esta red y tiene que tener una wallet creada en la misma, desapareciendo así el requisito de tener un mínimo de reputación o riqueza en la red. De esta manera, no se llega a la justicia perfecta que otorga *Proof of Work* pero podemos decir que desaparece la injusticia que nos daba el protocolo de *Proof of Stake*.

Desde este trabajo, nos gustaría hacer una crítica al mundo blockchain y de criptomonedas en cuanto a los algoritmos usados para el minado de las mismas. Para empezar, nos gustaría dejar claro lo siguiente:

- Primero, no puede seguir incrementando el gasto computacional así como también de potencia y energía, puesto que hemos entrado en dimensiones muy grandes, equiparando el gasto computacional de la red de bitcoin con el gasto computacional de ciudades. Viendo los niveles de contaminación que hay hoy en día, consideramos que habría que solucionar este tema y migrar a protocolos en los que dicho gasto disminuya y nos proporcione una mínima justicia
- En segundo lugar, tampoco consideramos que sea de justicia que solamente algunos mineros puedan o tengan la capacidad de minar o cifrar un bloque nuevo en la blockchain. Esto acaba suponiendo una centralización de la blockchain, que va en contra de uno de los primeros principios que tiene esta tecnología.

Es por esto que nos gustaría que el mundo de las criptomonedas evolucionara hacia protocolos de consenso parecidos o derivados de Algorand, puesto que solventa los dos puntos anteriormente expuestos. Primero, no hay minado o, si más no, el minado es muy mínimo, consiguiendo despreciar dicho proceso para el medio ambiente. Además, no supone una centralización de la blockchain debido a que la comunidad no cierra a unos

cuantos (quién tenga riqueza o reputación en la misma red) la capacidad de minar o cifrar un bloque. Es por ello que animamos a todas las fundaciones y comunidades blockchain a promocionar y facilitar el uso de protocolos como Algorand. Hasta la fecha que se escribe este documento nos consta que ya hay criptomonedas que han alcanzado una cierta reputación o solo que son emergentes que se basan en dicho protocolo o protocolos similares, como puede ser Cardano, que se basa en el protocolo Ouroboros, ya comentada en este mismo documento; o Dusk, una criptomoneda emergente que consigue descentralizar la blockchain y eliminar este gasto computacional con el protocolo *Segregated Byzantine Agreement*, derivado de Algorand.

8. Conclusiones y desarrollo futuro

Este proyecto nos ha ayudado a entrar mucho más en el mundo de las criptomonedas, en el de la privacidad de cada una y, sobretodo, en el mundo del minado. La experiencia que teníamos era un poco vaga, había trabajado con redes blockchain pero nunca había entrado en el mundo de las criptomonedas.

A modo de resumen, los conocimientos adquiridos con este trabajo se pueden resumir en los siguientes puntos:

- Hemos estudiado las criptomonedas más famosas desde el punto de vista de la privacidad y la minería, descubriendo muchas de ellas que ni conocíamos.
- Hemos aprendido muchos algoritmos relativos a la privacidad de las transacciones en criptomonedas y muchos algoritmos de consenso para cifrar un bloque en una red blockchain
- Hemos conseguido, desde cero, descargarnos un software de minado, compilarlo y ejecutarlo, consiguiendo así minar una de las criptomonedas más seguras y más descentralizadas
- También hemos aprendido a utilizar una placa como la Raspberry Pi. Investigando sobre la misma, también hemos aprendido a manejarla y aprender cómo funcionan.
- Finalmente, hemos cogido conciencia sobre cómo afecta el minado de las criptomonedas en el mundo en el que vivimos, cada vez más contaminado y con una emergencia climática que, si no tomamos medidas, será irremediable.

Para acabar con este proyecto, me gustaría también hablar de los próximos pasos o desarrollo futuro que nos puede ocupar en los próximos meses. Así, aspectos que creo que podrían ser buenos para seguir aprendiendo sobre este tema, podrían ser los siguientes:

- ✔ En primer lugar, conseguir minar con la Orange Pi PC 2, puesto que por problemas de tiempo y de hardware no ha sido posible
- ✔ Un punto que podría ser muy interesante a trabajar sería montar una pequeña granja de chips como la Raspberry Pi 3 o Orange Pi PC 2 y experimentar, de primera mano, los beneficios que ello aporta, corroborando así el trabajo hecho en este proyecto
- ✔ Otro punto que sería interesante trabajar, sería en el de optimizar el código del cliente de monero con el fin de conseguir una minería más óptima que nos permita, de manera local, minar a más hashes por segundo.
- ✔ Finalmente, encuentro muy interesante un estudio sobre cómo puede afectar el hecho de minar con pool o sin pool. En nuestro proyecto, se ha hecho todo sin pool, consiguiendo una recompensa nula, puesto que nunca nos llevábamos nosotros el cifrado del bloque. Aún así, sería interesante ver si, en una pool y con una granja de chips como los comentados, podría salir a cuenta minar o no

Así, cerramos este proyecto con unos objetivos planteados a principio de documento cumplidos, y con puntos que hemos ido descubriendo a lo largo del trabajo que serían interesantes trabajar en ellos.

Bibliography:

[1] "A brief history on Bitcoin & Cryptocurrencies". [Online] Available: https://www.ledger.com/how-it-all-began-a-brief-history-of-bitcoin-cryptocurrencies/

[2] Federico Ast. Breve historia del Bitcoin. [Online] Available: https://medium.com/astec/breve-historia-del-bitcoin-3cd9942debef

[3] "Bitcoin no es anónimo". [Online] Available: https://academy.bit2me.com/bitcoin-no-es-anonimo/

[4] "Bitcoin Transactions aren't as anonymous as everyone hoped". [Online] Available: https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/

[5] "Minar bitcoins, ¿en qué consiste y cómo funciona?". [Online] Available: https://academy.bit2me.com/que-es-minar-bitcoins/

[6] Vitalik Buterin. "Privacy on the blockchain". [Online] Available: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

[7] EthHub. "Privacy". [Online] Available: https://docs.ethhub.io/ethereum-roadmap/privacy/

[8] "How Ethereum Mining Works". [Online] Available: https://www.coindesk.com/information/ethereum-mining-works

[9] Ripple Foundation. "Ripple". [Online] Available: https://ripple.com/

[10] CoinMarketCap. "XRP Ripple". [Online] Available: https://coinmarketcap.com/currencies/xrp/markets/

[11] Ripple Labs. "Going beyond Blockchain, Pt. 2: Ensuring Transaction Privacy". [Online] Available: https://www.ripple.com/insights/going-beyond-blockchain-pt-2-ensuring-transaction-privacy/

[12] Satoshi. "Hash Time Locked Contracts (HTLCs) Explained". [Online] Available: https://medium.com/liquality/hash-time-locked-contracts-htlcs-explained-e88aa99cc824

[13] "Acerca de Ripple". [Online] Available: https://btcdirect.eu/es-es/acerca-de-ripple

[14] Coin Smart Canada. "Ripple Mining: An Urban Legend". [Online] Available: https://medium.com/datadriveninvestor/ripple-mining-an-urban-legend-81865f0e90ae

[15] The Cryptocurrency Consultant. "Is the Ripple Centralized or Decentralized". [Online] Available: https://medium.com/swlh/is-the-ripple-centralized-or-decentralized-e774706871de

[16] "The History of Bitcoin Cash". [Online] Available: https://www.bitcoin.com/get-started/the-history-of-bitcoin-cash/

[17] "Bitcoin Cash". [Online] Available: https://coinmarketcap.com/currencies/bitcoin-cash/

[18] "Cash Shuffle". [Online] Available: https://cashshuffle.com/

[19] SFOX. "Bitcoin Cash vs Bitcoin: How Bitcoin Cash is Measuring Up". [Online] Available: https://blog.sfox.com/bitcoin-cash-vs-bitcoin-how-bitcoin-cash-is-measuring-up-d5fcb6fea9c6

[20] Contentworks Agency. "A Brief History of Litecoin". [Online] Available: https://medium.com/@contentworks/a-brief-history-of-litecoin-260c96faa454

[21] "Litecoin (LTC)". [Online] Available: https://coinmarketcap.com/currencies/litecoin/

[22] Bisola Asolo. "Mimlewimble, The Ultimate Beginner's Guide". [Online] Available: https://www.mycryptopedia.com/mimblewimble-explained/

[23] BitDegree. "How to Mine Litecoin: Understand How Litecoin Mining Works". [Online] Available: https://www.bitdegree.org/tutorials/litecoin-mining/

[24] Chris Wheal. "A history of EOS". [Online] Available: https://dex.openledger.io/a-history-of-eos/

[25] "EOS". [Online] Available: https://coinmarketcap.com/currencies/eos/

[26] "¿Qué es EOS?". [Online] Available: https://www.bitcobie.com/eos/

[27] pEOS Foundation. "Private, untraceable transactions on EOS". *pEOS Whitepaper.* https://peos.one/docs/pEOS_whitepaper_rev1_1.pdf

[28] "Binance Coin (BNB)". [Online] Available: https://changenow.io/currencies/binance-coin

[29] Lenín Navas García. "Binance Coin en Review". [Online] Available: https://criptotendencia.com/2019/10/08/binance-coin-en-review/

[30] "Binance Coin (BNB)". [Online] Available: https://coinmarketcap.com/currencies/binance-coin/

[31] "Binance Coin (BNB): tutorial completo para dummies". [Online] Available: https://www.brokeronline.es/binance-coin/

[32] "Vision". [Online] Available: https://bitcoinsv.io/vision/

[33] Spilotro. "What is Bitcoin SV? Everything you need to know about BSV". [Online] Available: https://ci.covesting.io/news/altcoin-news/what-bitcoin-sv-everything-you-need-know-about-bsv

[34] Dr. Craig S. Wright. "SV Pool". [Online] Available: https://svpool.com/

[35] "Bitcoin SV". [Online] Available: https://blockchair.com/bitcoin-sv

[36] Chris Wheal. "A history of Stellar and the lumen". [Online] Available: https://dex.openledger.io/a-history-of-stellar-and-the-lumen/

[37] Roy Shienfield. "Lightning Network Routing: Privacy and Efficiency in a Positive –Sum Game". [Online] Available: https://medium.com/breez-technology/lightning-network-routing-privacy-and-efficiency-in-a-positive-sum-game-b8e443f50247

[38] Bob Glickstein. "Understanding the Stellar Consensous Protocol". [Online] Available: https://medium.com/interstellar/understanding-the-stellar-consensus-protocol-423409aad32e

[39] Yakko Majuri. "Simply Explained: Stellar Consensous Protocol". [Online] Available: https://medium.com/london-blockchain-labs/blockchain-definition-of-the-week-stellar-consensus-protocol-5006f42203b0

[40] Ed Posnak. "On the Origin of Cardano". [Online] Available: https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c

[41] Dail Hodl Staff. "Cardano Exploring Privacy Features that Power Zcash". [Online] Available: https://dailyhodl.com/2019/10/23/cardano-exploring-privacy-features-that-power-zcash-says-charles-hoskinson/

[42] Michael Parsons. "Cardano: A Blockchain with Privacy and Regulation". [Online] Available: https://medium.com/@BitcoinByte/a-blockchain-with-privacy-and-regulation-cardano-3606e1288bc2

[43] "Ouroboros". [Online] Available: https://www.cardano.org/en/ouroboros/

[44] Cardano Foundation. "Ouroboros Proof of Stake Algorithm". [Online] Available: https://cardanodocs.com/cardano/proof-of-stake/

[45] Chris Wheal. "A history of Tron (TRX)". [Online] Available: https://dex.openledger.io/a-history-of-tron-trx/

[46] "Tron: Tutorial completo para dummies". [Online] Available: https://www.brokeronline.es/tron/

[47] Tron Foundation. "Open Letter to the Community on TRON Protocol Progress in Q4, 2019". [Online] Available: https://medium.com/@TronFoundation/a96943d29e99

[48] Crypto Info. "What is UNUS SED LEO? The beginner's guide". [Online] Available: https://medium.com/@crypto_info/what-is-unus-sed-leo-the-beginners-guide-98419959d92a

[49] Mariia Rousey. "What is UNUS SED LEO (LEO) cryptocurrency?". [Online] Available: https://changelly.com/blog/what-is-unus-sed-leo-cryptocurrency/

[50] Tezos Foundation. "Our History". [Online] Available: https://tezos.foundation/history

[51] L.M. Goodman. "Tezos – a self-amending crypto-ledger". *Tezos Whitepaper*, September 2014. https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf

[52] William McKenzie. "The Sapling Protocol is coming to Tezos". [Online] Available: https://medium.com/tezoscommons/zk-snarks-and-fine-tuned-privacy-is-coming-to-tezos-77a4422ad991

[53] SerHack. *Mastering Monero: The future of private transactions*, 1st ed:LernoLibro LLC, December 2018.

[54] "Digital Ocean". [Online] Available: https://www.digitalocean.com/

[55] Monero Foundation. "Monero". [Online] Available: https://github.com/monero-project/monero

[56] MkDocs. "Monero Documentation". [Online] Available: https://monerodocs.org/

[57] Jtgrassie. "XMRig". [Online] Available: https://github.com/xmrig/xmrig

[58] Ubuntu. "Powerstat". [Online] Available: http://manpages.ubuntu.com/manpages/xenial/man8/powerstat.8.html

[59] Monero Foundation. "Monero". [Online] Available: https://www.getmonero.org/downloads/

[60] Monero Foundation. "Configuration Wizard". [Online] Available: https://xmrig.com/wizard

[61] Cryptocompare. "Equipment". [Online] Available: https://www.cryptocompare.com/mining/#/equipment

[62] Blockchain Luxembourg. "HashRate". [Online] Available: https://www.blockchain.com/charts/hash-rate

[63] Ajuntament Barcelona. "Estadística i Difusió de Dades". [Online] Available: https://www.bcn.cat/estadistica/castella/dades/anuari/cap14/C1404010.htm

[64] Idescat. "Municipi Barcelona en xifres". [Online] Available: https://www.idescat.cat/emex/?id=080193

[65] "Población España 2020". [Online] Available: https://www.enterat.com/actualidad/poblacion-espana-provincias-municipios.php

[66] Algorand Foundation. "Algorand". [Online] Available: https://www.algorand.com/

Glosario

En esta sección se van a definir conceptos clave para entender el texto expuesto en el presente documento.

- *Proof-of-Work.* Es un algoritmo de consenso que se basa en la capacidad de cálculo de las máquinas de cada uno de los mineros. Para minar, todos los mineros que participen en el proceso, pondrán su máquina a calcular. El primero que consiga calcular el *hash* válido para añadir el bloque a la última posición de la cadena, será el primer bloque candidato. Una vez todos los mineros verifiquen que el bloque es válido, dicho minero será el que se lleve la recompensa. Así, se premia el trabajo bien hecho de los mineros que lucharán por ser los más rápidos y habrá una cierta justicia a la hora de repartir las recompensas.

- *Proof-of-Stake.* Es un algoritmo de consenso que se basa en la confianza de los mineros más ricos o con más reputación dentro de la misma red. Para este proceso, se hace una selección antes de minar cada bloque para ver quién tiene permiso para minarlo y, en función de este grupo, se escoge quien va a ser. Una vez minado el bloque, los demás mineros no lo verifican puesto que ya se ha supuesto una cierta confianza al inicio de este proceso. Este algoritmo, frente al anterior de *Proof-of-Work*, ofrece ventajas como el gasto computacional, puesto que el mismo no existe al ser instantáneo el mismo minado; por otro lado, no existe tanta justicia debido a que existe una presupuesta confianza en lugar de dejar que cualquiera pueda conseguir minar el bloque.

- *Delegated-Proof-of-Stake.* Algoritmo de consenso que deriva del *Proof-of-Stake* pero que incluye mejoras en cuanto a la justicia de la decisión de quién mina el siguiente bloque. Para este algoritmo, el proceso es el siguiente:

  1. Todos los participantes de la red eligen unos delegados, que serán los principales mineros que puedan firmar bloques
  2. Una vez decididos estos delegados, se prosigue a minar el bloque siguiendo el mismo esquema que en el algoritmo *Proof-of-Stake*
  3. En este algoritmo no se valida el bloque firmado puesto que ya se han filtrado los delegados y se ha presupuesto una confianza en ellos.

  Así, siguiendo este esquema se desarrolla el algoritmo de consenso *Delegated-Proof-of-Stake*. Como mejora del protocolo de *Proof-of-Stake* incorpora un poco más de justicia, al ser los propios mineros quién votan a los encargados de minar el bloque, en lugar de decidirse en función de la participación que tengan en la red.

- *Federated Byzantine Agreement.* Este término hace referencia al momento en que, un número mínimo de nodos conocido como quórum, se ponen de acuerdo en que la solución presentada es válida y así proceder a incluirla en la blockchain. Para ello, el nodo no es necesario ser conocido ni ser verificado con anticipación y el control sobre el mismo es descentralizado, por lo que cada nodo decide a quién quiere creer.

- *Snarks.* Son construcciones matemáticas que permiten anonimizar la transacción y que no se conozcan origen y destino de la misma pero, a la vez, no generar dudas sobre si origen y destino son quien dicen ser. Es decir, se demuestra que origen y destino son quienes realizan la transacción pero sin desvelar su identidad. Para ilustrarlo, vamos a poner un ejemplo:
    1. Alice y Bob se encuentran en una habitación con dos pelotas, una verde y otra roja. Alice es una persona daltónica y ve de la misma manera las dos pelotas (pongamos que las ve verde), en cambio Bob las ve distinto, una de color verde y la otra de color rojo.
    2. Alice coge una de las pelotas, y le pregunta a Bob de qué color la ve. Este le contesta que la ve de color verde.
    3. Alice, queriendo saber si Bob se entera que ella ha cambiado de pelota, sin que la vea cambia la pelota. Alice la sigue viendo verde, pero cuando le pregunta a Bob si ha cambiado la pelota, Bob al verla roja le responde que sí que la ha cambiado.
    4. En este punto, Alice conoce con certeza que Bob sabe que ella ha cambiado la pelota, pero no conoce cómo lo puede saber, puesto que no le ha visto cambiar la pelota y ella las ve las dos iguales.

  Este tipo de construcciones matemáticas ayudan a las criptomonedas a anonimizar las identidades de las transacciones para que ninguna muestre datos sobre la misma transacción pero se pueda determinar su validez para añadirla a la blockchain.

- *Pools de minado.* Los *pools* de minado aparecen cuando la dificultad de minado incrementó hasta el punto que para los mineros más pequeños les costaría siglos generar un bloque. Consisten en una agrupación de recursos en las que varios mineros comparten potencia de cómputo en la red y, cuando se consigue minar un bloque, la recompensa se reparte equitativamente a los esfuerzos que cada minero ha empleado para generarlo. De esta manera, los mineros pequeños se nutren de potencia de computación de otros mineros y les permite generar bloques más fácilmente, cosa que si lo hicieran cada uno individualmente no conseguirían nunca cifrar un bloque.

- Hashrate. Unidad mediante la cual se mide la potencia computacional de los equipos, medida en el cálculo de resolución de hashes, estableciendo así una clasificación en función de cómo de potente es un ordenador cuando se quiere minar. Cuando hablamos del *hashrate* en una red, nos referimos a la potencia total que proporcionan los equipos que están minando en la misma red.

- *Full-privacy.* Entendemos como *full-privacy* los aspectos que nos dan una completa privacidad, haciendo anónimos todos los parámetros de una transacción sin necesidad que sean revelados.

- *Smart contracts.* Contratos que adquieren las propiedades de inmutabilidad, descentralizados y transparentes al estar corriendo sobre la misma tecnología

blockchain, que los hace más robustos que los contratos físicos que se usan hoy en día. La criptomoneda que permite programar dichos contratos inteligentes adquiere una ventaja importante entre las demás, puesto que se puede convertir en una criptomoneda de uso general y cotidiano.

- *Hard fork.* Bifurcación en la red de una criptomoneda cuando se modifica parte del código de la misma, haciendo incompatible los sucesos futuros con la versión anterior del código pero compartiendo el pasado de la misma. Hay muchas criptomonedas que han surgido a partir de un *hard fork* de otra, esto es, que en algún momento dado se modificó el código de la criptomoneda inicial (ya sea por creencias de que la criptomoneda debería seguir por otro camino, por errores de diseño…) y se creó otra criptomoneda que comparte el pasado pero cada una hará un camino distinto a partir del *hard fork*.

- *ASIC.* También conocidos como *Application-Specific Integrated Circuit*, son chips diseñados específicamente para minar criptomonedas. Estos chips son conocidos como evolución de las CPU. Nos dan mejores prestaciones que sus predecesoras pero eliminan la versatilidad que nos dan la CPU o GPU, puesto que, por ejemplo, no se puede correr un sistema operativo sobre una ASIC pero si queremos minar criptomonedas nos dará un hashrate más elevado.

- *Tokens ERC.* Smart Contracts que cuentan con una estructura ya preestablecida, pensada en facilitar la implementación de distintas funcionalidades sobre la red blockchain Ethereum, facilitando el trabajo a los desarrolladores. Dentro de estos tokens, podemos destacar los tokens ERC20, orientados a crear nuevas monedas sobre la red Ethereum; también podemos destacar los tokens ERC721, que fueron diseñados con el objetivo de crear tokens intercambiables pero con la particularidad de ser únicos y no-fungibles, por lo que cada token es único y no puede destruirse.

- *Internet of Value.* Es el espacio online en los que cada individuo puede realizar cualquiera transferencia de manera instantánea sin la necesidad de colaboración de terceras personas ni los costes en los que estas derivan.

- *Seudonimización.* El término seudonimización se creó un poco a raíz de la falta de la completa anonimización que hay en algunas criptomonedas. Cuando a lo largo del documento nos referimos a que una criptomoneda goza de seudonimización, nos estamos refiriendo a que no anonimiza por completo la transacción y que, por lo tanto, podemos ver alguno de sus parámetros como origen y destino, monto de la transacción…

- *ICO*. Las siglas de *Initial Coin Offering* simulan el concepto *Initial Public Offering (IPO)* al mundo de las criptomonedas. Es el proceso en el cual se empieza a

comercializar la moneda, se establece un valor y los inversores pueden empezar a invertir en ella.

- *Diffie-Hellmann*. Proceso criptográfico que se utiliza para enviar las claves de cifrado entre dos personas sin que una tercera la pueda interceptar. De esta manera, dos personas con la misma clave podrán intercambiarse mensajes cifrados sin que la tercera persona los pueda descifrar, puesto que no tiene la clave que se han intercambiado de forma segura.