



UNIVERSIDAD LATINA CAMPUS HEREDIA  
CENTRO INTERNACIONAL DE POSGRADOS

MAESTRÍA PROFESIONAL EN GERENCIA DE PROYECTOS  
TRABAJO FINAL DE GRADUACIÓN

OPORTUNIDAD DE NEGOCIO: EL SERVICIO DE MINERÍA DE BITCÓIN COMO  
UNA ACTIVIDAD ECONÓMICA RENTABLE – LA CRIPTOMONEDA MÁS  
POPULAR Y UTILIZADA EN EL MUNDO

ELABORADO POR

IGNACIO BLANCO ZAMORA

HEREDIA, COSTA RICA

AÑO 2017



UNIVERSIDAD LATINA  
DE COSTA RICA  
LAUREATE INTERNATIONAL UNIVERSITIES\*

UNIVERSIDAD LATINA CAMPUS HEREDIA  
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL TUTOR  
DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 31 de agosto del 2016

Señores

Miembros del Comité de Trabajos Finales de Graduación

SD

Estimados señores:

He revisado y corregido el Trabajo Final de Graduación, denominado:

OPORTUNIDAD DE NEGOCIO: EL SERVICIO DE MINERÍA DE BITCOIN COMO  
UNA ACTIVIDAD ECONÓMICA RENTABLE – LA CRIPTOMONEDA MÁS  
POPULAR Y UTILIZADA EN EL MUNDO, elaborado por el estudiante: José Ignacio  
Blanco Zamora, como requisito para que el citado estudiante pueda optar por el  
grado académico MASTER PROFESIONAL EN GERENCIA DE PROYECTOS.

Considero que dicho trabajo cumple con los requisitos formales y de contenido  
exigidos por la Universidad, y por tanto lo recomiendo para su entrega ante el  
Comité de Trabajos Finales de Graduación.

Suscribe cordialmente,

MASTER EN GERENCIA DE PROYECTOS: ING. ROCÍO BRICEÑO LÓPEZ



UNIVERSIDAD LATINA  
DE COSTA RICA  
LAUREATE INTERNATIONAL UNIVERSITIES\*

UNIVERSIDAD LATINA CAMPUS HEREDIA  
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL LECTOR  
DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 31 de agosto del 2016

Señores

Miembros del Comité de Trabajos Finales de Graduación

SD

Estimados señores:

He revisado y corregido el Trabajo Final de Graduación, denominado:

OPORTUNIDAD DE NEGOCIO: EL SERVICIO DE MINERÍA DE BITCOIN COMO UNA ACTIVIDAD ECONÓMICA RENTABLE – LA CRIPTOMONEDA MÁS POPULAR Y UTILIZADA EN EL MUNDO, elaborado por el estudiante: JOSÉ IGNACIO BLANCO ZAMORA, como requisito para que el (los) citado (s) estudiante (s) pueda (n) optar por el grado académico MÁSTER PROFESIONAL EN GERENCIA DE PROYECTOS.

Considero que dicho trabajo cumple con los requisitos formales y de contenido exigidos por la Universidad, y por tanto lo recomiendo para su entrega ante el Comité de Trabajos Finales de Graduación.

Suscribe cordialmente,

Ing. Luis Cordero Calvo MPM, PMP



UNIVERSIDAD LATINA  
DE COSTA RICA  
LAUREATE INTERNATIONAL UNIVERSITIES\*

UNIVERSIDAD LATINA CAMPUS HEREDIA  
CENTRO INTERNACIONAL DE POSGRADOS

CARTA DE APROBACIÓN POR PARTE DEL FILÓLOGO  
DEL TRABAJO FINAL DE GRADUACIÓN

Heredia, 31 de agosto del 2016

Señores

Miembros del Comité de Trabajos Finales de Graduación

SD

Estimados señores:

Leí y corregí el Trabajo Final de Graduación, denominado : OPORTUNIDAD DE NEGOCIO: EL SERVICIO DE MINERÍA DE BITCOIN COMO UNA ACTIVIDAD ECONÓMICA RENTABLE – LA CRIPTOMONEDA MÁS POPULAR Y UTILIZADA EN EL MUNDO, elaborado por el estudiante: JOSÉ IGNACIO BLANCO ZAMORA para optar por el grado académico MÁSTER PROFESIONAL EN GERENCIA DE PROYECTOS.

Corregí el trabajo en aspectos, tales como: construcción de párrafos, vicios del lenguaje que se trasladan a lo escrito, ortografía, puntuación y otros relacionados con el campo filológico, y desde ese punto de vista considero que está listo para ser presentado como Trabajo Final de Graduación; por cuanto cumple con los requisitos establecidos por la Universidad.

Suscribe de Ustedes cordialmente,

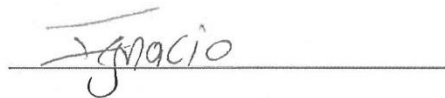
---

Filóloga española. Alejandra Brenes Rodríguez

## DECLARACIÓN JURADA

El suscrito(a), Ignacio Blanco Zamora con cédula de identidad número 113180225, declaro bajo fe de juramento, conociendo las consecuencias penales que conlleva el delito de perjurio: Que soy el autor(a) del presente trabajo final de graduación, modalidad memoria; para optar por el título de Master Profesional en Gerencia de Proyectos de la Universidad Latina, campus Heredia, y que el contenido de dicho trabajo es obra original del (la) suscrito(a).

Heredia, setiembre del dos mil diecisiete

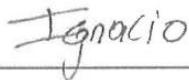
A handwritten signature in black ink, appearing to read "Ignacio", is written over a horizontal line.

Ignacio Blanco Zamora

## MANIFESTACIÓN EXONERACIÓN DE RESPONSABILIDAD

El suscrito, Ignacio Blanco Zamora con cédula de identidad número 113180225, exonero de toda responsabilidad a la Universidad Latina, campus Heredia; así como al Tutor y Lector que han revisado el presente trabajo final de graduación, para optar por el título de Master Profesional en Gerencia de Proyectos de la Universidad Latina, campus Heredia; por las manifestaciones y/o apreciaciones personales incluidas en el mismo. Asimismo, autorizo a la Universidad Latina, campus Heredia, a disponer de dicho trabajo para uso y fines de carácter académico, publicitando el mismo en el sitio web; así como en el CRAI.

Heredia, setiembre del dos mil diecisiete.



---

Ignacio Blanco Zamora

## Resumen Ejecutivo

El presente trabajo final de graduación desarrolla el tema titulado “OPORTUNIDAD DE NEGOCIO: EL SERVICIO DE MINERÍA DE BITCOIN COMO UNA ACTIVIDAD ECONÓMICA RENTABLE – LA CRIPTOMONEDA MÁS POPULAR Y UTILIZADA EN EL MUNDO”. Su objetivo principal consiste en establecer una empresa dedicada a la actividad económica de la minería del bitc in, as  como definir y explicar la teor a y conceptos que representan las bases necesarias para construir una gu a con el fin de brindar el servicio de la miner a del bitc in.

El bitc in es la criptomoneda de mayor precio, con mayor capitalizaci n y la m s utilizada en el mercado. La facilidad y las ventajas que presenta el bitc in la han convertido en la criptomoneda m s confiada y m s utilizada en todo el mundo. El bitc in como medio de intercambio para bienes y servicios representa una ruptura al actual modelo econ mico de monedas centralizadas. Considerado como una revoluci n y una innovaci n en el actual modelo econ mico mundial, el uso del bitc in y su miner a representan un nuevo nicho de mercado en el cual sus emprendedores pueden verlo como una gran oportunidad de negocio. En cuanto a la presente investigaci n, esta se desarrolla en seis cap tulos principales:

Cap tulo I. Problema y Prop sito: Se exponen los antecedentes del tema con referencias bibliogr ficas, as  como el planteamiento del problema u oportunidad propuesta, las definiciones te ricas, as  tambi n como el objetivo general y los objetivos espec ficos.

Cap tulo II. Fundamentaci n Te rica: Se explican conceptos te ricos de administraci n de proyectos para ser tomados como una base en cuanto a la realizaci n de la obra. Adem s, incluye una revisi n del actual modelo econ mico

mundial y del bitc33n como criptomoneda, as33 como la menci33n de sus ventajas y desventajas.

Cap33tulo III. Metodolog33a: En dicho cap33tulo se brinda una explicaci33n del enfoque metodol33gico cuantitativo seleccionado para la realizaci33n de las fases de la investigaci33n y recolecci33n de la informaci33n.

Cap33tulo IV. An33lisis de Resultados: Se expone c33mo crear una billetera de bitc33n. El cuerpo principal del cap33tulo consiste en la descripci33n textual y gr33fica de las ocho variables de las que depende la miner33a del bitc33n. Tambi33n se presenta una entrevista corta a un profesional en el 33rea de la econom33a.

Cap33tulo V. Conclusiones y Recomendaciones: Se enumeran las conclusiones en relaci33n con los objetivos y seg33n el estudio realizado, comprobado a partir de la teor33a desarrollada en los cap33tulos anteriores. Adem33s, se presentan recomendaciones acerca de la actividad como parte de una gu33a o metodolog33a.

Cap33tulo VI. Propuesta: Se presenta en un formato de gerencia de proyectos un conjunto de entregables para la implementaci33n del estudio realizado como una propuesta oficial de proyecto.

Las 33ltimas secciones corresponden a la bibliograf33a y los anexos utilizados para el estudio.



## Tabla de contenidos

CAPÍTULO I: PROBLEMA Y PROPÓSITO.....	1
1.1 Estado Actual de la Investigación.....	2
1.2 Planteamiento del Problema.....	7
1.2.1 ¿Qué es la minería del Bitc33n? .....	8
1.3 Justificaci33n .....	11
1.4 Objetivo General y Espec33ficos .....	12
CAPÍTULO II: FUNDAMENTACI33N TE33RICA.....	14
2.1 Gerencia y Administraci33n de Proyectos.....	15
2.2 Grupos de Procesos y 33reas de Conocimientos de la Direcci33n de Proyectos 17	
2.3 Actual Modelo Econ33mico Mundial.....	19
2.4 El Bitcoin como Criptomoneda .....	22
2.4.1 Ventajas .....	25
2.4.2 Desventajas .....	27
2.5 ¿Qu33 es una Billetera de Bitcoins? .....	29
CAPÍTULO III: METODOLOG33A.....	32
3.1 Enfoque Metodol33gico y M33todo Seleccionado.....	33
3.2 Descripci33n del Contexto o del Sitio en D33nde se Lleva a Cabo el Estudio	40
3.3 Caracter33sticas de los Participantes y las Fuentes de Informaci33n.....	41
3.4 T33cnicas e Instrumentos para la Recolecci33n de Datos.....	41
CAPÍTULO IV: AN33LISIS E INTERPRETACI33N DE RESULTADOS.....	43
4.1 An33lisis .....	44
4.1.1 Creaci33n de una Billetera de Bitc33n .....	44
4.1.2 Selecci33n del Minero de Bitcoins .....	49
4.1.3 Variables de la Miner33a de Bitc33n .....	52
4.1.3.1 Tasa de Hash (Hashes/s).....	52
4.1.3.2 Consumo El33ctrico (Watts).....	53
4.1.3.3 Costo del Consumo El33ctrico (\$).....	53
4.1.3.4 Tarifa de la Piscina de Miner33a (%) .....	54
4.1.3.5 Dificultad del Bitc33n .....	56

4.1.3.6	Recompensa del Bloque (BTC).....	58
4.1.3.7	Bitcoin al Dólar (\$).....	58
4.1.3.8	Costo del Equipo (\$).....	58
4.1.4	Resultados de una Calculadora de Minería .....	59
4.1.5	Entrevistas Realizadas.....	64
4.1.6	Interpretación de los Resultados.....	67
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES .....		69
5.1	Interpretación de los Resultados .....	70
5.2	Recomendaciones.....	73
CAPÍTULO VI: PROPUESTA.....		77
6.1	Introducción.....	78
6.2	Justificación.....	78
6.3	Entregables para la Propuesta del Proyecto .....	79
6.3.1	Alcance del Proyecto.....	79
6.3.2	Estructura de Desglose de Trabajo (EDT) .....	81
6.3.3	Lista de Interesados.....	82
6.3.4	Cronograma .....	84
6.3.5	Análisis de Factibilidad.....	86
6.3.6	Diagrama de Causa y Efecto .....	88
Bibliografía: Citada y Consultada .....		89
Glosario.....		91
ANEXOS .....		92

## Índice de Gráficas

Gráfica N° 1. Precio del Bitc�in en el mercado en los �ltimos dos a�os.....	4
Gráfica N° 2. Cantidad de Bitc�in en circulaci�n hasta la fecha.....	24
Gráfica N° 3. Tasa de Hash (trillones de hashes por segundo) durante el �ltimo a�o.....	53
Gráfica N° 4. Distribuci�n de la tasa de hash en las m�s grandes piscinas de mineros.....	56
Gráfica N° 5. Dificultad de minar el Bitc�in en los �ltimos dos a�os.....	57

## Índice de Figuras/Imágenes

Figura N° 1. El Bloque Génesis o el primer bloque de una transacción de Bitc�in en el mundo.....	3
Figura N° 2. Primera compra de un bien/servicio usando Bitc�in.....	5
Figura N° 3. Proceso general del m�todo cuantitativo.....	33
Figura N° 4. Ventana de ingreso a Electrum.....	46
Figura N° 5. Interfaz de Electrum.....	47
Figura N° 6. Inicio del programa de Bitcoin Core.....	48
Figura N° 7. Comparaci�n entre Actuales ASIC en el Mercado .....	51
Figura N° 8. Calculadora de Miner�a para un Antminer S9 al 10 de agosto de 2017.....	60
Figura N° 9. Calculadora de Miner�a para seis Antminer S9 al 13 de agosto de 2017.....	62
Figura N° 10. Estructura de Desglose de Trabajo del Proyecto.....	81
Figura N° 11. Cronograma del proyecto.....	85
Figura N° 12. Diagrama de causa y efecto.....	88



# CAPÍTULO I: PROBLEMA Y PROPÓSITO

## 1.1 Estado Actual de la Investigación

El bitc3in sali3 a la luz al mundo en el a3o 2008, cuando el documento llamado *Bitcoin: A Peer-to-Peer Electronic Cash System*, del autor con el seud3nimo de Satoshi Nakamoto fue publicado en internet. En dicho texto se describe una manera de utilizar un libro contable mayor p3blico fortalecido criptogr3ficamente para grabar y proteger transacciones. En aquel entonces el bitc3in era solo una idea, pero despu3s de unos meses de planeaci3n, una comunidad de personas obsesionadas por la computaci3n cre3 el primer bloque de 50 bitcoins, llamado tambi3n el Bloque G3nesis (Ver figura N31). Esta comunidad pronto cre3 esta idea en un sistema funcional. Una parte importante de este sistema era poder lanzar bitcoins a trav3s del tiempo para recompensar a aquellos usuarios que dedicaban su poder de procesamiento computacional a que la infraestructura del sistema funcionara.

Figura N° 1 . El Bloque Génesis o el primer bloque de un transacción de Bitcoin en el mundo.

Fuente: Blockchain.info, 2017.

## Block #0

Summary		Hashes	
Number Of Transactions	1	Hash	00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Output Total	50 BTC	Previous Block	00
Estimated Transaction Volume	0 BTC	Next Block(s)	0000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Transaction Fees	0 BTC	Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Height	0 (Main Chain)		
Timestamp	2009-01-03 18:15:05		
Received Time	2009-01-03 18:15:05		
Relayed By	Unknown		
Difficulty	1		
Bits	486604799		
Size	0.285 KB		
Version	1		
Nonce	2083236893		
Block Reward	50 BTC		

## Transactions

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b		2009-01-03 18:15:05
No Inputs (Newly Generated Coins)	 1A1zP1eP5QGeFi... (Genesis of Bitcoin <a href="#">ⓘ</a> )	50 BTC
		

Durante los primeros años, el bitcoin tuvo un valor de \$0, pues era simplemente un experimento o juguete de este grupo de aficionados informáticos en Estados Unidos. Ver Gráfica N°1.



Gráfica N° 1 . Precio del Bitc6in en el mercado en los 6ltimos dos a6os.

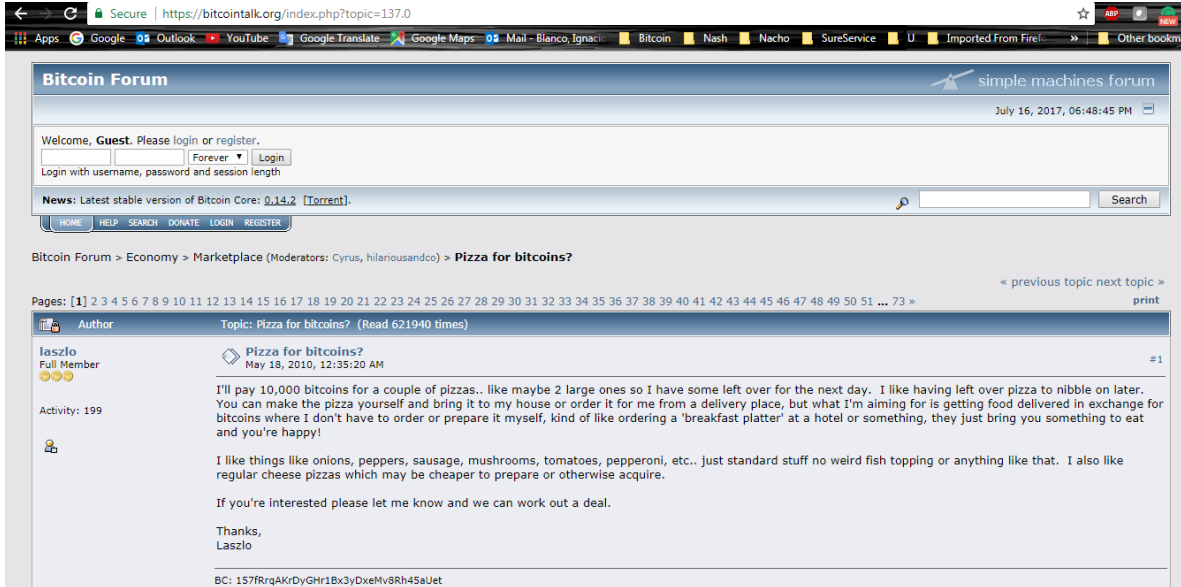
Fuente: Blockchain.info, 2017.



La historia cambia cuando alguien en internet ofreci6 pagar 10,000 bitcoins por un par de pizzas en el foro en l6nea bitcointalk.org, todav6a equivalente a \$0. Efectivamente la transacci6n se dio y el hombre comparti6 las fotos de las pizzas que le fueron entregadas en la misma p6gina de internet al haber pagado a un usuario 10,000 BTC a cambio de dos pizzas expr6s. Ver figura N°3. Actualmente esos 10,000 BTC costar6an m6s de \$2,000,000.

Figura N° 2 . Primer compra de un bien/servicio usando bitcoins.

Fuente: <https://bitcointalk.org/index.php?topic=137.0>, 2017.



Después de esta fecha, algunos hechos interesantes hicieron subir la importancia del bitc on e incrementar su valor en poco tiempo:

1. Dada su disponibilidad, la gente empez  a utilizarlo a cambio de bienes y servicios reales. Principalmente algunos criminales cibern ticos en los primeros meses atra dos por la facilidad de transacci n del bitc on y su naturaleza semian nima en sus inicios. Posteriormente, organizaciones leg timas como wordpress.com e internetarchive.org aceptaron el bitc on como moneda para donaciones y pagos.
2. Los servicios brindaron a las personas diferentes maneras de comprar, vender, almacenar, proteger y aprender acerca de sus

bitcoines (importancia a la moneda) con el uso de páginas como bitpay.com y coinbase.com.

3. Personas en países financieramente inestables empezaron a sacarle provecho al bitc on como una manera de almacenar sus riquezas. Por ejemplo, cuando el gobierno de Chipre anunci  en el 2013 que detendr  los servicios de transacciones para ciertos bancos, el bitc on subi  a m s de \$250/BTC. Unos meses despu s, se estabiliz  alrededor de \$130.

Despu s de este auge del bitc on empezaron a circular diferentes tipos de acusaciones y etiquetaci n hacia este, debido a sus caracter sticas naturales, tales como transferencias r pidas en cualquier momento desde cualquier parte del mundo, identidad an nima y transacciones seguras y reversibles. En varias partes del mundo se le quer a regular o prohibir del todo su uso (sin  xito) como Vietnam, China, Corea del Norte e incluso Estados Unidos. Dichas caracter sticas naturales del bitc on deben verse como una ventaja para los individuos y para todos los usuarios, pues el sistema es muy seguro y m s barato que el uso de transacciones bancarias actualmente. Sin duda alguna dicha situaci n significa una amenaza para muchos gobiernos y bancos centrales.

En un intento de prohibir el bitc on en Estados Unidos, el entonces senador Joe Manchin (2014) envi  una carta al Departamento de Tesorer a de los Estados Unidos, en ella se resaltaban los usos negativos que posiblemente las personas podr an llegar a darle, sin importar los beneficios en la sociedad actual: "El bitcoin tambi n se ha convertido en un refugio para las personas para comprar art culos en el mercado negro. Los individuos son capaces de comprar ilegalmente art culos de manera an nima como drogas y armas" (p. 1).

Ahora bien, los gobiernos y autoridades realmente no pueden bloquear el bitc33n como tal, pero pueden herir partes de la cadena de valor del bitc33n, como su intercambio a d33lares.

Efectivamente, alrededor de medio bill33n de d33lares en bitcoins se han malversado o perdido, esto debido, en la mayor33a de los casos, a fraude comercial com33n, incompetencia administrativa y financiera o a mala implementaci33n t33cnica. A pesar de los muchos peque11os orificios por los que ha pasado el bitc33n, ninguno de los hechos sucedidos en la historia hasta ahora se11alan un defecto b11sico del bitc33n como tal. Despu33s de todo, a pesar de los ataques de hackers, negocios de bitcoins en ruina, amenazas de los gobiernos y cambios en el mercado; el bitc33n siempre ha logrado regresar. Su valor se ha estado estabilizando a trav33s del tiempo cuando cada vez m11s y m11s comerciantes optan por aceptar el bitc33n como medio de pago junto con su moneda local.

## 1.2 Planteamiento del Problema

Al conocer los antecedentes del bitc33n quedan claros tanto su nacimiento como su crecimiento. El bitc33n no es una moneda f33sica almacenada en b33vedas o en las residencias de las personas; es m11s bien una moneda digital a partir de la cual se pueden obtener beneficios, tales como la miner33a del bitc33n; comprender esas utilidades es el objetivo principal de la presente investigaci33n. La necesidad de este estudio consiste en entender la situaci33n de la econom33a mundial actual, el uso de las diferentes monedas y los conceptos b11sicos del bitc33n, as33 como su red y su miner33a. El problema derivado de dicha moneda no es un problema u obst11culo como tal, sino que m11s bien representa una oportunidad de negocio, la cual consiste en brindar el servicio de la miner33a del bitc33n como una actividad econ33mica viable y rentable, de manera que se participe en una piscina de mineros una vez completados todos los requerimientos de *hardware* y *software*.

Para tener claro el tipo de actividad económica por realizar se debe entender el concepto de la minería del bitc in, este es explicado a continuaci n.

### 1.2.1  Qu  es la miner a del Bitc in?

La miner a del bitc in se refiere al proceso de realizar una verificaci n de trabajo (*proof-of-work*, en ingl s) de un bloque de la cadena de transacciones de bitcoins. El bloque de cadena de bitcoins presente contiene las m s recientes transacciones de bitcoins realizadas durante los  ltimos minutos en el mundo. Puede contener una o cientos de transacciones, y estas transacciones pasan a ser parte oficial de libro contable en los nodos del protocolo de bitc in hasta que la funci n de hash criptogr fico resulta y es verificada seis veces. As , incluido en la cola de bloques, todo esto es realizado en el proceso llamado miner a de bitc in. Dichos bloques requieren de muy poco trabajo (poder computacional) para ser verificados.

En la actualidad, el equipo f sico de infraestructura de la tecnolog a utilizado para minar se llama ASIC (del ingl s, *Application-specific integrated circuit*). Como su nombre lo indica, consiste en un conjunto de circuitos integrados dise ados y contruidos especialmente para un solo prop sito: la miner a de bitc in.

El proceso de la miner a tiene dos prop sitos principales: primero, la creaci n o emisi n de nuevos bitcoins en cada bloque cuando un minero resuelve el hash criptogr fico del bloque de transacciones. La cantidad de bitcoins creados por bloque es un valor fijo, pero disminuye en el tiempo, espec ficamente cada 4 a os, lo que equivale a 210000 bloques de transacciones (esta variable se explica en la secci n 4.1.3.6 Recompensa del Bloque). Segundo, la miner a crea seguridad y

confianza a la red de bitc in. Con el paso del tiempo m s mineros se adhieren a la red de bitc in y m s bloques se verifican y adhieren al libro contable de bitcoins, hecho que aumenta la confianza en el protocolo. De manera similar, cuantos m s mineros haya, aumenta la dificultad del bitc in (Blanco, 2017, p. 56).

De manera general, el protocolo de bitc in env a una transacci n (mensaje) a la red, utilizando una funci n de hash criptogr fico (transformaci n matem tica) para obtener una salida. A esta salida se le llama un digerido o resumen; en ingl s tambi n presenta diferentes nombres como *digest*, *hash*, *tag*, entre otros. La funci n de hash criptogr fica es una funci n determinista y la salida siempre ser  la misma para una entrada dada. Un detalle importante por resaltar es que las funciones de *hash* tradicionales utilizadas en las ciencias de la computaci n han sido implementadas principalmente en otros tipos de funciones llamadas tablas de *hash*, empleadas para realizar b squedas en una cantidad muy extensa de datos ordenados en una tabla, para filtrar y buscar m s eficiente y r pidamente. Por ejemplo, en el uso de un diccionario en donde existen miles de palabras que pueden ser ordenadas y usadas para realizar b squedas de palabras. En el protocolo de bitc in, estas funciones de *hash* no son necesariamente las mismas que las funciones de hash criptogr ficos. El dise o y prop sito de estas funciones de hash criptogr ficas utilizadas en el protocolo de bitc in tienen un conjunto de propiedades especiales en cuanto a seguridad, autenticaci n y privacidad, lo cual las hace m s apropiadas para el protocolo de bitc in (criptograf a).

Se puede mencionar una analog a de este *hash* criptogr fico (problema computacional) como un crucigrama o un sudoku de cierta dificultad para un humano. Cada 10 minutos aproximadamente una persona debe resolver el crucigrama y otras personas verifican el crucigrama resuelto, se considera aprobado el bloque de transacciones y el resto de personas que tambi n estaban intentando resolver ese crucigrama queda excluido de la competencia, en otras palabras,

pierden el juego. Los otros jugadores pueden verificar rápidamente si el crucigrama resuelto está correcto, pues pueden revisar por encima si las respuestas efectivamente cumplen con las condiciones del crucigrama. Esta verificación es muy sencilla en comparación con resolver todo el crucigrama en sí. Una vez resuelto el crucigrama, se adhiere a la cadena de crucigramas de toda la red mundial y se ajusta la dificultad de los próximos crucigramas para que sean siempre resueltos en 10 minutos, aproximadamente. Lo anterior dependerá de las habilidades de la persona (o grupo de personas) que resolvieron el crucigrama anterior para que logren ser resueltos en aproximadamente 10 minutos.

Volviendo al *hash* criptográfico, una vez resuelto el bloque de transacciones, otros mineros de la red pueden actuar como verificadores de la respuesta del *hash* criptográfico y se agrega el bloque a la cadena troncal de bloques de transacciones, esta actúa como un único libro contable para toda la red y todas las transacciones de bitcoins. Finalmente, se considera un bloque como oficialmente resuelto y cerrado cuando ha sido verificado seis veces por otros mineros.

Los resultados son grabados en todos los miembros de la red que actúan como nodos, técnicamente llamados “clientes completos de bitcoin”; estos son computadoras normales de los usuarios con un programa instalado de una billetera de bitcoin completa (o en inglés, *full bitcoin client*). Las billeteras de bitcoin serán cubiertas en la sección 2.5. Estos nodos que copian toda la lista de transacciones de bloques de cadenas de la red de bitcoin agregan seguridad a la red y evitan tanto transacciones dobles como ataques a los bloques. Una vez resuelto el *hash* criptográfico, el minero es recompensado con el correspondiente valor actual que exista en el protocolo de bitcoin, como se explicó al inicio de la sección.

### 1.3 Justificación

El bitc in (BTC) es la criptomoneda m s popular y utilizada en el mundo. Desde su nacimiento, en el a o 2009, hasta la fecha de elaboraci n de esta justificaci n de proyecto (julio de 2017), creci  su valor de \$0 a \$1943,45 por BTC. La miner a, explicada en la secci n 1.2.1, representa una actividad econ mica innovadora,  nica en el mundo de los servicios digitales y de internet, rentable bajo las condiciones apropiadas, adem s no requiere de mano de obra especializada para su operaci n diaria. En general, es un servicio que se puede dejar corriendo solo, pues  nicamente requiere ser instalado y configurado apropiadamente, as  como cierto nivel de supervisi n y mantenimiento para su correcta operaci n a largo plazo.

Algunas ventajas de la miner a del bitc in son:

- No requiere una inversi n muy elevada para iniciar y poner en funcionamiento la actividad econ mica. Tampoco necesita una alta y t cnicamente complicada configuraci n del equipo para la miner a de bitc in
- Puede ser llevada a cabo en una casa, apartamento, bodega, local, etc. Se requiere que el espacio f sico sea ventilado, tenga electricidad y buena conexi n a internet (por lo menos 10 Mbps de bajada y 1 Mbps de subida).
- Si se localiza en un sitio de clima fr o, el *hardware* puede servir para calentar el espacio f sico.



- El *hardware* puede ser vendido en caso de querer sustituirlo por uno mejor o más moderno.
- No se requiere contratar personal adicional para la operación a largo plazo de la minería. Una persona puede ser capaz de administrar una cantidad específica de ASICs, incluyendo lo pronosticado en este trabajo de investigación, de 1 a 6 ASICs.

Otros detalles acerca del bitc in y el entorno de la econom a en el mundo ser n expuestos en los siguientes cap tulos.

#### 1.4 Objetivo General y Espec ficos

Objetivo general:

Plantear la creaci n de una empresa (ficticia) llamada Bitc in CR con el prop sito de desarrollar la miner a de bitc in como actividad rentable y empezar operaciones en un periodo no m s amplio de tres meses. Con el equipo necesario (*software* y *hardware*) y las condiciones apropiadas (variables de la miner a), poner en funcionamiento la miner a de bitc in para finalmente obtener remuneraci n o recompensa por el servicio brindado. La miner a conforma la infraestructura y legitimidad del bitc in como moneda, no un gobierno y un banco centralizado.

### Objetivos específicos:

- Resumir la información necesaria para sentar una base y fundamentación teórica acerca de la administración de empresas y gerencia de proyectos con el fin de desarrollar la actividad de la minería del bitc in.
- Explicar los conceptos b asicos y funcionamiento del bitc in como criptomoneda y de la miner a de este.
- Crear una billetera de bitc in para realizar transacciones de bitcoins (ingresos y egresos).
- Medir y analizar las variables involucradas por la miner a del bitc in y elegir el equipo de infraestructura tecnol gica (ASIC: *Application-specific integrated circuit*) necesario para operar de manera rentable.
- Calcular el tiempo que trascurrir a operando para obtener el retorno de la inversi n inicial.

## CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

## 2.1 Gerencia y Administración de Proyectos

Como parte de los objetivos específicos del presente trabajo, se pretende utilizar una base teórica acerca de la gerencia y administración de proyectos, esto con el fin de proceder apropiadamente en cuanto a la creación de la empresa Bitc in CR, as i como para recolectar y utilizar la informaci n del alcance del proyecto relacionada con el bitc in, apearse a las mejores y m as recomendadas pr cticas de gerencia de proyectos y trabajar m as eficientemente con las  reas de conocimiento y grupos de procesos relacionados con la direcci n de proyectos expuestos en el PMBOK, los cuales se puedan utilizar para el tema expuesto.

Seg n la Gu a de los Fundamentos para la Direcci n de Proyectos:

Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado  nico. La naturaleza temporal de los proyectos implica que un proyecto tiene un principio y un final definidos. El final se alcanza cuando se logran los objetivos del proyecto, cuando se termina el proyecto porque sus objetivos no se cumplir n o no pueden ser cumplidos, o cuando ya no existe la necesidad que dio origen al proyecto. (Gu a del PMBOK , 2013, p. 3)

Para el caso de Bitc in CR, el proyecto se basa en la creaci n de un servicio. Cabe aclarar que un servicio se entiende como la capacidad de brindar un trabajo o una acci n; esta misma actividad se relaciona con las labores de todos los empleados en cualquier empresa, en donde prestan sus servicios profesionales, los cuales son intangibles, todos ellos son acciones para ejecutar una obra o trabajo en espec fico. El servicio o funci n tratada en este trabajo es de naturaleza digital. Se necesita equipo f sico inform tico, herramientas y conocimiento del gerente del

proyecto para la realización y generación de dicho servicio. Cuando la empresa entre en operación, el servicio de la minería de bitc in b asicamente se dedicar a aportar su capacidad de procesamiento en *hashes* por segundo para descifrar *hashes* criptogr aficos de bloques de transferencias electr nicas de la red de protocolo de bitc in. Asimismo, deber  operar diariamente y preferiblemente las 24 horas del d a.

El gerente de un proyecto es la persona encargada de dirigir, administrar y controlar todas las tareas generales de un proyecto. Entre sus funciones m s importantes se encuentran integrar a todas las partes y equipos de un proyecto, as  como mantener una comunicaci n clara entre todos los involucrados del proyecto.

El caso de Bitc in CR posee una situaci n muy particular. El proyecto en s  es ambicioso, requiere de una apropiada investigaci n, planeaci n, ejecuci n, control y mantenimiento de la obra de servicio como cualquier proyecto de peque a o mediana escala. Sin embargo, en el presente documento se plantea el desarrollo del proyecto con solo un miembro: el gerente del proyecto. Debido a las dimensiones y tipos de tareas meta, se estima que una sola persona –en este caso el gerente del proyecto –es capaz de ejecutar por completo el proyecto de la miner a de bitc in. El proyecto solamente utiliza activos electr nicos (ASICs, fuentes de poder, equipo de red y ventiladores) y programas que requieren ser configurados (billetera de bitc in, *software* para la miner a de bitc in y asociarse a una piscina de mineros) para entrar en operaci n. Una vez configurados los ASICs y los programas, pueden mantenerse funcionando por s  solos durante las 24 horas del d a, con m nima supervisi n y con cierto nivel mantenimiento. Para el alcance de este proyecto, se desea minar utilizando de 1 a 6 ASICs, algo completamente manejable para una sola persona.

Según el diseño organizacional de este proyecto, el único interesado dentro del proyecto es el mismo gerente de esta, pues trabajando para él mismo como empresa. Los ingresos son las recompensas en bitcoins que la piscina de mineros le paga dependiendo de la capacidad de tasa de *hash* que aporte a esta. También, directamente, el gerente pone a funcionar los ASICs para la piscina de mineros a la que se asocia. Indirectamente, la red de bitcoin y los usuarios se pueden interpretar como beneficiarios del pequeño aporte que estaría brindando Bitcoin CR a ellos, siendo parte de la red y fortaleciéndola.

## 2.2 Grupos de Procesos y Áreas de Conocimientos de la Dirección de Proyectos

Dentro de la administración y gerencia de proyectos, tras años de prueba y error en proyectos de la vida real, miembros del PMI han logrado unificar y describir a los llamados grupos de procesos de la dirección de proyectos como la integración de conocimientos y mejores prácticas o recomendaciones para ser capaces de cumplir con los objetivos establecidos por el patrocinador, director de proyecto y otros interesados. La Guía del PMBOK® resume los grupos de procesos de la dirección de proyectos de la siguiente manera:

- Grupo de Procesos de Inicio. Aquellos procesos realizados para definir un nuevo proyecto o nueva fase de un proyecto existente al obtener la autorización para iniciar el proyecto o fase.
- Grupo de Procesos de Planificación. Aquellos procesos requeridos para establecer el alcance del proyecto, refinar los objetivos y definir el curso de acción requerido para alcanzar los objetivos propuestos del proyecto.

- Grupo de Procesos de Ejecución. Aquellos procesos realizados para completar el trabajo definido en el plan para la dirección del proyecto a fin de satisfacer las especificaciones del mismo.
- Grupo de Procesos de Monitoreo y Control. Aquellos procesos requeridos para rastrear, revisar y regular el progreso y el desempeño del proyecto, para identificar áreas en las que el plan requiera cambios y para iniciar los cambios correspondientes.
- Grupo de Procesos de Cierre. Aquellos procesos realizados para finalizar todas las actividades a través de todos los Grupos de Procesos, a fin de cerrar formalmente el proyecto o una fase del mismo. (Guía del PMBOK®, 2013, p. 49)

Dentro de la teoría del PMBOK®, la dirección de proyectos también se apoya en las llamadas áreas de conocimiento. Estas encapsulan conceptos, actividades, herramientas y técnicas más específicas en cuanto a un tipo de área de trabajo en particular para la administración. A continuación, se mencionan las áreas de conocimiento que mejor encajan dentro de la ejecución de las tareas del proyecto.

Gestión del Alcance del Proyecto: Identificar y categorizar las diferentes áreas de trabajo que se deben incluir como parte del proyecto, recopilar requisitos, crear una Estructura de Desglose de Trabajo (EDT), validar el alcance y controlar el alcance. Aquí se desarrolla una descripción detallada del proyecto y del producto o servicio.

Técnicas herramientas para la gestión del alcance del proyecto: Juicio de expertos, entrevistas, investigaciones, documentación en internet, observaciones, estudios comparativos, matriz de trazabilidad de requisitos, entre otros.

Gestión de los Costes del Proyecto: Funciona como guía para poder planificar, estimar, presupuestar, financiar, obtener financiamiento y gestionar los costos con el fin de satisfacer las necesidades del proyecto sin salirse del presupuesto obtenido para el proyecto.

Gestión de la Calidad del Proyecto: Procesos y actividades de la organización que tienen como función establecer políticas de calidad y regulaciones para que el proyecto satisfaga las necesidades para las que fue acometido.

Gestión de los Riesgos del Proyecto: Procesos que tienen como función identificar y gestionar los riesgos asociados con la actividad o fin del proyecto respecto a todas sus actividades. Se realiza un análisis cualitativo y cuantitativo de los riesgos. También se recomienda tener un plan para la respuesta de los riesgos y un plan para el control de los riesgos.

### 2.3 Actual Modelo Económico Mundial

La mayoría de lugares del mundo llevan menos de 100 años utilizando monedas impresas. Sin embargo, la emisión de dinero que está respaldada por nada excepto por la fe de las personas (que creen que está respaldada o guardada) y cuánto de ese dinero está en circulación es algo reciente, porque no fue sino hasta en 1972 que la mayoría de este dinero estaba respaldado por oro. Por su parte, la deuda se considera aún más antigua que el dinero mismo, desde el primer "le debo



y después le pago” la deuda siempre es algo que de alguna u otra manera ha existido en la naturaleza de las personas.

A partir del siglo XIII en adelante muchos países comenzaron, a como pudieron, a crear instituciones bancarias como en China y en Holanda, utilizando diferentes tipos de monedas (oro, plata, bronce, etc.). En Italia, durante las décadas de 1300 y 1400 surgió la cultura de la mafia, sus participantes se dedicaban a prestar algún tipo de dinero y cobrar las deudas e intereses a través del miedo y la violencia.

Cuando comenzaron los bancos centralizados como El Banco de Inglaterra, funcionaban bajo el patrón oro internacional, lo que significaba que papel moneda podría ser cambiado por oro o plata y viceversa.

En 1783 las colonias americanas ganaron su independencia de Inglaterra; sin embargo, el gobierno continuaría luchando con el concepto de un banco central. Esencialmente, un banco central es una institución que produce la moneda de una nación o región entera. Este banco central controla las tasas de interés y controla el suministro de dinero (inflación).

Naturalmente, el dinero no tiene valor en sí, lo que hace valioso al dinero es la escasez, el deseo y la fe que la gente tiene en él. Si demasiado dinero entra en circulación, entonces los precios suben y el valor de ese dinero se reduce, al igual que lo que sucedió en España y en toda Europa después de que encontraron la montaña de plata junto con El Dorado; pues engañados por sus propios recursos, el valor del oro decayó.

Lo que los bancos centrales buscan llevar a cabo es controlar el suministro de dinero de una nación al prestar cierta cantidad al gobierno en intereses y controlar la cantidad de dinero que puede circular en cualquier momento dado. Cuando un banco central le presta dinero al gobierno, le presta con intereses. También, con el uso del aumento y disminución del suministro de dinero, el banco es capaz de regular el valor de la moneda en circulación. En efecto, por cada colón o dólar suministrado al gobierno, no es en realidad un colón o un dólar, es una unidad más un porcentaje de deuda con base en esa unidad. Cada banco central tiene un monopolio en la producción de la moneda de todo el país entero. Se le suma, además, que el dinero para pagar esa deuda adjunta con cada unidad de moneda debe ser pagado con dinero de ese mismo banco central. Lo que significaría que el banco central debe perpetuamente incrementar el suministro de dinero para temporalmente cubrir la deuda creada. Como cada nuevo tiraje de dinero es prestado con un interés, crea una deuda montada sobre la anterior, la cual nunca puede ser realmente pagada.

En los últimos 80 años la mayoría de los países del mundo han sido estandarizados por un sistema de banco central, en dicha situación han ocurrido extravagantes fluctuaciones y altos picos de inflación. La mayoría de los países del mundo actualmente no ve la luz al final del túnel, pues ellos están inevitablemente atados a media mano a una eterna deuda de la cual realmente nunca van a poder salir, y la única respuesta a estos síntomas siempre es imprimir más dinero o pedir prestado del exterior, lo cual causa que los precios de los bienes y servicios continúen subiendo y que la moneda pierda valor.

Lo descrito anteriormente ha causado inconformidad en muchas personas, pues provoca cuestionar a todos los bancos centrales, así como desear una solución más tangible y predecible. De hecho, muchos grandes grupos han pensado en regresar al estándar del oro.

Todos estos hechos y la entrada del bitc33n al mundo han hecho que millones de personas vuelvan sus ojos hacia los beneficios de este como medio de intercambio o pago descentralizado. ¿Será que el bitc33n y otras criptomoneda pueden llegar a ser la soluci33n a uno de los problemas m33s grandes de la actualidad?

## 2.4 El Bitcoin como Criptomoneda

En el cap33tulo anterior, se explic33 de manera general el nacimiento y la introducci33n del bitc33n en el mundo. A continuaci33n, se detallar33 el concepto fundamental del bitc33n con el fin de explicar su existencia.

En el libro “Mastering Bitcoin” se sintetiza el concepto del bitc33n y su ambiente como a continuaci33n se muestra:

Conjunto de conceptos y tecnolog33as que forman la base de un ecosistema de dinero digital. Las unidades de moneda llamadas Bitcoins se utilizan para almacenar y transmitir valor entre los participantes en la red de Bitcoin. Los usuarios de bitcoin se comunican entre s33 utilizando el protocolo Bitcoin principalmente a trav33s de Internet, aunque tambi33n pueden usarse otras redes de transporte. La pila de protocolos bitcoin, disponible como software de c33digo abierto, se puede ejecutar en una amplia gama de dispositivos inform33ticos, incluidos ordenadores port33tiles y tel33fonos inteligentes, lo que hace que la tecnolog33a sea f33cilmente accesible. (Antonopoulos, 2015, p. 1)

As33, el bitc33n lleg33 para revolucionar la econom33a en el mundo y la vida de las personas que saben aprovecharlo. El bitc33n es una moneda enteramente virtual,

no existen monedas físicas y tampoco monedas virtuales como tal. Son transacciones que transfieren valor del emisor hasta el receptor. Los usuarios poseen una llave secreta que les ayuda a aprobar las transacciones como legítimas en los bloques de transacciones. A través de la red, el usuario puede hacer lo mismo que con monedas tradicionales, como vender, comprar y extender crédito.

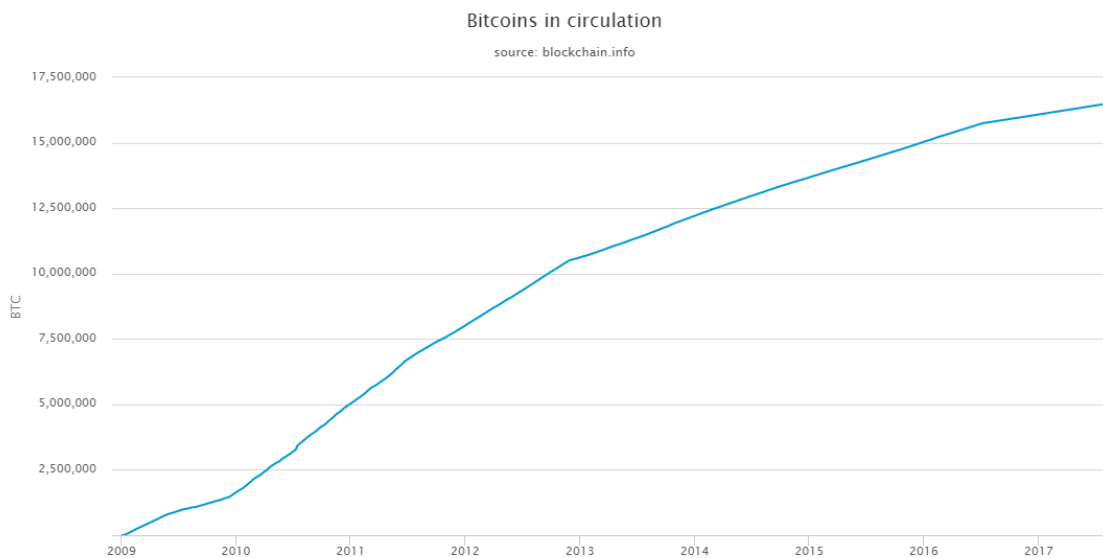
El bitc in no posee una autoridad centralizada o reguladora, pues su protocolo est  dise ado para funcionar a trav s de una red punto a punto con las computadoras y servidores de todos los usuarios (interesados). Los bitcoins son creados o agregados a la red con el proceso de la miner a explicado en el cap tulo anterior: Cada 10 minutos, en promedio, alguien es capaz de validar un bloque de transacciones y es recompensado (actualmente) con 12.5 bitcoins. As , el bitc in se descentraliza de una autoridad reguladora como un banco central que se encargar a de la emisi n de la moneda tanto f sica como digital y funciones de compensaci n, de esta manera suplanta dicha necesidad con una red global en constante y activa competici n.

Como se estudi  en el cap tulo I, el protocolo del bitc in incluye algoritmos incorporados que regulan la funci n de miner a. La dificultad para que el minero resuelva el algoritmo (para efectivamente grabar el bloque de transacci n en la red de bitc in) es ajustada din micamente para que en promedio alguien triunfe cada diez minutos sin importar cu ntos mineros y ASICs est n trabajando en cualquier momento. El protocolo fue construido de manera que cada cuatro a os se disminuyera a la mitad la cantidad de bitcoins de recompensa por cada bloque (actualmente 12.5 BTC). Tal situaci n genera un aproximado de la cantidad total de bitcoins que llegar  a circular en el mundo (l mite). La figura N 3 muestra la cantidad de bitcoins en circulaci n hasta la fecha: alrededor de 16 millones de bitcoins. Los bitcoins en circulaci n con el resultado de la compra de bitcoins con monedas de otros pa ses y de la generaci n de bitcoins con la miner a. Dada

la disminución existente en cuanto a la recompensa de bitcoins, eso limitará la cantidad de bitcoins en circulación para aproximadamente el año 2140 a 21 millones de bitcoins, aproximadamente (Ver gráfica N°2). Dada esta disminución de la tasa de emisión de bitcoins al largo plazo, el bitc6in es deflacionista. Adicionalmente, el bitc6in no puede ser inflado “creando” o “imprimiendo” nuevo dinero m1s all1 de la tasa de emisi6n esperada.

Gr1fica N° 2 . Cantidad de Bitcoin en circulaci6n hasta la fecha.

Fuente: <https://blockchain.info/charts/total-bitcoins?timespan=all>, 2017.



### 2.4.1 Ventajas

En esta sección se mencionarán ventajas del bitc3in como moneda.

- Los usuarios de bitc3in no est3an en riesgo por ruptura de seguridad. En contraste, cuando un comerciante (mayorista o menorista) sufre una ruptura de seguridad al usar m3todos financieros tradicionales, la informaci3n financiera de los usuarios puede ser robada y utilizada. Por su parte, al utilizar bitcoins, el comerciante al ser atacado compromete 3nicamente sus fondos si es que el atacante pudo obtener su llave privada. Ni el comerciante ni el atacante pueden descubrir a trav3s del comerciante la llave privada de los usuarios. Cr3ticas al bitcoin recaen en que pueden existir fallas de seguridad en las billeteras y en las transacciones de bitcoins, pero estos problemas realmente no se han reportado como debilidades oficialmente reportadas en m3ltiples ocasiones.
- Las tarifas de las transacciones de bitcoins son mucho menores que las transacciones de tarjetas de cr3dito, transacciones de bancos diferentes y transacciones internacionales. Algunas cr3ticas resaltan que una vez que otros costos son agregados, como la protecci3n antirobo y costos de cumplimiento y regulaci3n, el bitc3in no mantiene una diferencia muy marcada.
- Los comerciantes que usan bitc3in est3an protegidos contra el fraude de devoluci3n, es decir, un cliente que busca una retracci3n de un pago una vez que el bien ha sido enviado o entregado.

- Las transferencias bitc in son casi instant neas (10 minutos para revolver y verificar varias veces el bloque de transacciones), en comparaci n con las transferencias bancarias que pueden tomar varios d as para liquidar. Los cr ditos pueden quedar flotantes durante d as y las disputas con los bancos, de manera similar, duran abiertas d as.
- No se cobra ninguna tarifa base con bitc in, a diferencia de las tarjetas de cr dito (aunque actualmente existe costo m nimo de transacci n en el protocolo bitc in establecido en 0.00001 BTC a partir de la versi n 0.9.1 de Bitcoin Core). Esto podr a permitir micropagos, especialmente si las nuevas tecnolog as para manejar los micropagos son adoptadas por los usuarios. Los micropagos podr an permitir a los proveedores de contenido, como peri dicos o video bajo demanda (*pay-per-view*), cobrar por trozos de contenido m s peque os. Y a n m s importante es la inmensa cantidad de negocios y usuarios que se ver an beneficiados por compra y venta de servicios y productos de muy bajo costo con estos micropagos. El bitc in se puede ver como una gran facilidad para pagar literalmente por cualquier cosa.
- Bitc in y otras tecnolog as relacionadas permiten la transferencia de cualquier activo digital aparte de la moneda. Adem s, los nuevos protocolos abren la puerta a la ejecuci n de contratos m s complicados y a otras aplicaciones relacionadas.
- Bitc in es un sistema de pago “*push*” (utilizando su llave privada), similar al efectivo, con esto el usuario debe generar de manera proactiva la transacci n. Por el contrario, otros sistemas de pago, como las tarjetas de cr dito, son sistemas de atracci n, en ellos los usuarios autorizan a un

minorista (a menudo revelan información confidencial) y el minorista retira el pago de la cuenta del usuario. Los sistemas de pago proactivos pueden tener ventajas en la reducción del fraude o compras no deseadas, ya que los usuarios están en control del proceso de compra. En otras palabras, ellos fuerzan y autorizan el pago.

- Los pagos de bitc in pueden ser m s an nimos por medio del uso de seud nimos.

Bitc in es un nuevo sistema de pagos, independiente del sector financiero tradicional, que podr a aportar resistencia a la econom a en caso de crisis, ya que crea un sistema de pagos paralelo.

#### 2.4.2 Desventajas

Desventajas de la nueva tecnolog a del bitc in como nuevo modelo econ mico hasta el momento:

- La mayor a de los usuarios de bitc in acabar an usando intermediarios (para pagos, cobros, intercambios de monedas, etc.), ya sea por conveniencia o porque encuentran la tecnolog a demasiado desalentadora. En este caso, la nueva tecnolog a ser a utilizada principalmente por las empresas y no habr a una disminuci n significativa en los costos.
- El bitc in es il quido en comparaci n con las monedas leg timas, como lo atestigua el volumen de los mercados de divisas para cruces como el euro /



dólar, que son hasta tres órdenes de magnitud más grandes que la facturación cambiaria del bitc in. Adem as, el bitc in y otras monedas alternativas tienen una desventaja muy marcada a la hora de competir contra las monedas de divisas ya establecidas.

- Actualmente, las transacciones de bitc in no ofrecen la opci n de cr dito, opuesto a las tarjetas de cr dito, pues con ellas el cr dito es una opci n incorporada por defecto o puede ser solicitado f cilmente. Los partidarios del bitc in resaltan que este servicio podr a ser agregado f cilmente a las transacciones de bitcoins por proveedores de las billeteras de bitc in, o mejor a n por instituciones financieras que ya han tenido experiencia gestionando cr ditos a clientes.
- Algunas regulaciones en Estados Unidos, como la normativa de la IRS (Internal Revenue Service) que clasifica al bitc in como un bien capital, podr a incrementar los costos de informes y de conformidad, hecho que frenar a el uso del bitc in como un medio de intercambio.
- Una misma moneda para todo el mundo puede que no sea una soluci n general eficiente. Por ejemplo, respecto a la inserci n del euro se puede destacar la siguiente consecuencia:

Est n sacrificando su poder nacional m s soberano, el derecho a emitir su propia moneda. A cambio, un Banco Central Europeo manejar a la Uni n Monetaria Europea. Sus miembros renunciar n a dos de sus m s poderosas salvaguardias econ micas, el derecho a devaluar sus monedas para corregir problemas internos, o incurrir en d ficit presupuestales para aliviar el desempleo masivo (De Zubir a, 1998, p. 1).

Si aumenta el uso del bitcoin, o si se llegara a usar en todo el mundo, podría darse un problema de escalabilidad, el cual consiste en que los bloques de transacciones (usualmente 300 o más transacciones por bloque) no puedan aguantar la demanda de transacciones en la red del protocolo, comparado con las redes más maduras de métodos de pagos actuales.

- La tecnología (código del *software* abierto y de libre uso) podría ser adoptado (sacarle provecho) por sólidas compañías o gobiernos para emitir su propia criptomoneda totalmente aprobada por el gobierno para ser intercambiado por moneda real, esto dejaría al bitcóiin atrás con mayores desventajas que la nueva moneda virtual local.

## 2.5 ¿Qué es una Billetera de Bitcoines?

Como la palabra lo indica es una billetera, un lugar personal de cada usuario donde se almacenan, envían y reciben bitcoines. Al igual que una billetera física en donde se almacena y administra monedas reales, los bitcoines se quedarán almacenados en la billetera. En la billetera de bitcoines es fundamentalmente un programa que puede correr en diferentes tipos de sistemas operativos (Windows, Mac OS, Android, Linux, etc), pues esto permitirá utilizarla en diferentes dispositivos, como computadoras y teléfonos móviles. Existen cuatro tipos principales de billeteras, estas serán explicadas a continuación:

- Billeteras de *Software (Software Wallets)*: Las más populares y utilizadas en el mundo. Estos programas son instalados en la computadora y dan control total sobre la moneda; la seguridad es

completamente administrada por el usuario. Si la computadora falla, se pierde la información de la billetera, incluyendo el dinero contenido en ella. Existen diferentes métodos de seguridad para proteger a los usuarios de este tipo de situaciones, como encriptar con claves la billetera y realizar respaldos de esta que deben ser almacenados en lugares diferentes a la computadora. Con estos respaldos se puede volver a cargar la información personal de la billetera en otra instancia del programa. Entre los programas más utilizados se pueden destacar: Bitcoin Core, Armory, Electrum, entre otros.

- Billeteras de papel (*Paper Wallets*): También conocidas como “Almacenaje en frío” (*Cold Storage*), son la forma más segura de almacenar bitcoins porque permite guardarlos independientemente de una computadora u otro dispositivo fuera de línea, brinda, además, mucha más seguridad. Consisten en una billetera de papel, una llave pública y una llave privada (como en una billetera de *software*) impresos en un papel generados por un programa o una página de internet. La diferencia es que la llave secreta o privada nunca ha estado almacenada en una computadora y nunca podrá ser accedida maliciosamente a través de internet, no hay rastro de ella, solo puede ser revisada físicamente desde ese papel. Las casas de cambio le permiten retirar el dinero con la clave privada. Si el código de la llave privada se extravía, no se puede recuperar el dinero almacenado en esa billetera, se pierde para siempre. Es ideal para almacenar grandes cantidades de dinero durante largos lapsos. Asimismo, esta llave privada impresa se puede almacenar en bancos o cajas fuertes, ya que representa un bien de alto valor.

- Billeteras móviles (*Mobile Wallets*): Generalmente son aplicaciones para móviles contenidas a una billetera de la red (*web wallet*), en otras palabras. Consisten en características adicionales de una billetera de red, por ejemplo el tener un puente de operación o control de la billetera en el teléfono celular.
- Billeteras de la red (*Web Wallets*): Billeteras más convenientes de todas y más sencillas. Residen en una computadora o servidor que no es propiedad de del usuario. Ellos dan el acceso en la red a la billetera, por lo tanto, son ideales para manipular cantidades pequeñas de dinero, así como para pagar y recibir dinero rápidamente. El anfitrión guarda el dinero de todas las personas, de esta manera recaen sobre él la seguridad y confianza de que todas las transacciones sean verídicas, reales y que no lleguen a ser hackeados y que pierdas sus bitcoins. Cabe destacar que hoy toda la red de bitcoins y las billeteras se están fortaleciendo y mejorando su seguridad.

## CAPÍTULO III: METODOLOGÍA

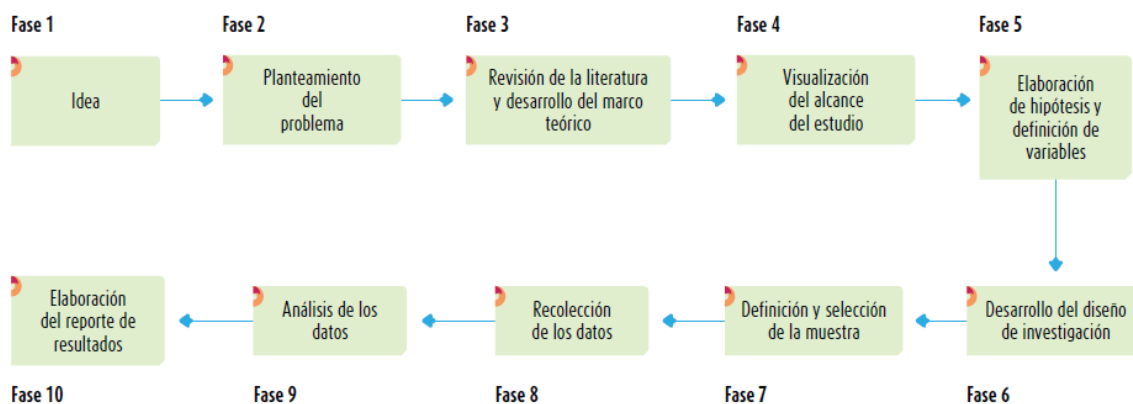
### 3.1 Enfoque Metodológico y Método Seleccionado

El presente estudio se centrará mayoritariamente en el extremo cuantitativo del continuo espacio de los métodos de la investigación. Según Hernández, Fernández y Baptista (2014), el enfoque cuantitativo “es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos “brincar” o eludir pasos, aunque desde luego, es factible redefinir alguna fase” (p. 18).

Se argumenta utilizar un enfoque cuantitativo debido a que el tema que se está analizando y desarrollando (la minería del bitc oin) es un tema de investigaci on con varias ramas combinadas entre s ı: La administraci on de negocios, gerencia de proyectos, econom ıa e infraestructura de la tecnolog ıa. Estas  reas de estudio requieren ser analizadas objetivamente, as ı como comprender la realidad de sus hechos de una manera externa y aut onoma a las opiniones internas o personales del autor. La siguiente imagen muestra de manera general el proceso de an lisis de un enfoque cuantitativo. La figura N 3 ayuda a comprender el orden l gico del enfoque del m todo cuantitativo.

Figura N  3 . Proceso general del m todo cuantitativo.

Fuente: Hern ndez, Fern ndez y Baptista, 2014.



En el libro “Metodología de la Investigación”, de los autores Hernández, Fernández y Baptista, 2014, pp. 5-6, se citan las características de un enfoque cuantitativo:

1. Refleja la necesidad de medir y estimar magnitudes de los fenómenos o problemas de investigación: ¿cada cuánto ocurren y con qué magnitud?
2. El investigador o investigadora plantea un problema de estudio delimitado y concreto sobre el fenómeno, aunque en evolución. Sus preguntas de investigación versan sobre cuestiones específicas.
3. Una vez planteado el problema de estudio, el investigador o investigadora considera lo que se ha investigado anteriormente (la revisión de la literatura) y construye un marco teórico (la teoría que habrá de guiar su estudio), del cual deriva una o varias hipótesis y las somete a prueba mediante el empleo de los diseños de investigación apropiados. Si los resultados corroboran las hipótesis o son congruentes con éstas, se aporta evidencia a su favor. Si se refutan, se descartan en busca de mejores explicaciones y nuevas hipótesis. Al apoyar las hipótesis se genera confianza en la teoría que las sustenta. Si no es así, se rechazan las hipótesis y, eventualmente, la teoría.
4. Así, las hipótesis se generan antes de recolectar y analizar los datos.
5. La recolección de los datos se fundamenta en la medición (se miden las variables o conceptos contenidos en las hipótesis).

6. Debido a que los datos son producto de mediciones, se representan mediante números (cantidades) y se deben analizar con métodos estadísticos.
7. En el proceso se trata de tener el mayor control para lograr que otras posibles explicaciones a la propuesta del estudio (hipótesis), se desechen y se excluya la incertidumbre y minimice el error. Es por esto que se confía en la experimentación o en las pruebas de causalidad.
8. Los análisis cuantitativos se interpretan a la luz de las predicciones iniciales (hipótesis) y de estudios previos (teoría). La interpretación constituye una explicación de cómo los resultados encajan en el conocimiento existente (Creswell, 2013, citado en Hernández et al., 2014, p 5).
9. La investigación cuantitativa debe ser lo más “objetiva” posible. Los fenómenos que se observan o miden no deben ser afectados por el investigador, quien debe evitar en lo posible que sus temores, creencias, deseos y tendencias influyan en los resultados del estudio o interfieran en los procesos y que tampoco sean alterados por las tendencias de otros (Unrau, Grinnell y Williams, 2005, citado en Hernández et al., 2014, p 5).
10. Los estudios cuantitativos siguen un patrón predecible y estructurado (el proceso) y se debe tener presente que las decisiones críticas sobre el método se toman antes de recolectar los datos.



11. En una investigación cuantitativa se intenta generalizar los resultados encontrados en un grupo o segmento (muestra) a una colectividad mayor (universo o población). También se busca que los estudios efectuados puedan replicarse.
12. Al final, con los estudios cuantitativos se pretende confirmar y predecir los fenómenos investigados, buscando regularidades y relaciones causales entre elementos. Esto significa que la meta principal es la formulación y demostración de teorías.
13. Para este enfoque, si se sigue rigurosamente el proceso y, de acuerdo con ciertas reglas lógicas, los datos generados poseen los estándares de validez y confiabilidad, las conclusiones derivadas contribuirán a la generación de conocimiento.
14. Esta aproximación se vale de la lógica o razonamiento deductivo, que comienza con la teoría, y de ésta se derivan expresiones lógicas denominadas “hipótesis” que el investigador somete a prueba.
15. La investigación cuantitativa pretende identificar leyes “universales” y causales (Bergman, 2008, citado en Hernández et al., 2014, p 6).
16. La búsqueda cuantitativa ocurre en la “realidad externa” al individuo. Conviene ahora explicar cómo se concibe la realidad con esta aproximación a la investigación.

Tomando como referencia esta metodología cuantitativa, se puede identificar cada fase para la realización de la investigación de la minería del bitc in.

- Idea: Es el planteamiento central del problema. Realizar la miner a del bitc in como una actividad viablemente rentable, por medio de la compra del equipo necesario y de ponerlo en operaci n.
  
- Planteamiento del problema: Establecido tambi n en los objetivos espec ficos en el cap tulo I. Se desea realizar la miner a del bitc in, para eso se necesita invertir en por lo menos 1 ASIC y operar durante un plazo de 12 meses con una inversi n determinada y con las variables medidas en Costa Rica. Parte del problema son las preguntas,  cu al ASIC escoger?  C mo ponerlos a funcionar?  En cu al piscina de miner a participar?, entre otras.
  
- Revisi n de la literatura y desarrollo del marco te rico: Bibliograf a citada y consultada y el cap tulo II (Fundamentaci n Te rica).
  
- Visualizaci n del alcance del estudio: Estimar tentativamente cu al ser  el alcance final de la investigaci n. Esta investigaci n tiene un alcance tipo descriptivo. Seg n Hern ndez et al (2010), el alcance descriptivo "busca especificar propiedades y caracter sticas importantes de cualquier fen meno que se analice. Describe tendencias de un grupo o poblaci n" (p.92). En este paso se define el objetivo general y los objetivos espec ficos.

- Elaboración de hipótesis y definición de variables: Medir las variables de la hipótesis (Precio del *hardware*, cantidad de ASICs, tasa de *hash*, consumo de electricidad, costo de la electricidad, precio del bitc in, la dificultad del bitc in y la tarifa de la piscina de mineros). La hipótesis consiste en que la minería del bitc in es una actividad rentable y se puede recuperar la inversión inicial en un plazo de 12 meses. Las variables de la minería afectan este plazo tanto para bien como para mal, pues actúan como un juego para el margen de ganancia del negocio.
- Desarrollo del diseño de investigación: A pesar de que la investigación tiene ciertas variables dependientes que pueden ser seleccionadas por el investigador, el diseño de la investigación es mayoritariamente no experimental, transeccional-descriptivo. La mayoría de variables es independiente del gerente del proyecto y se debe seleccionar el equipo de *hardware* adecuado para alcanzar los objetivos del estudio. Según Hernández, Fernández y Baptista (2014) “Los diseños de investigación transeccional o transversal recolectan datos en un solo momento, en un tiempo único (Liu, 2008 y Tucker, 2004). Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado. Es como “tomar una fotografía” de algo que sucede” (p. 154). Esto se puede apreciar durante el análisis e interpretación, pues en este se exponen dos resultados tomados en momentos diferentes, hecho que cambia el valor de algunas variables de la minería de bitc in.
- Definición y selección de la muestra: No probabilística. Se revisarán los 3 ASICs de los más populares creados en la industria, diseñados para la minería con el fin de determinar cuál es el que mejor puede satisfacer o cumplir con los requerimientos y necesidades del proyecto. Así como

también se analizarán el resto de las variables que influyen en la minería de bitc in.

- Recolecci n de los datos: Informaci n directa recolectada del fabricante de los ASICs, m s toda la informaci n disponible en internet acerca del uso de la infraestructura de informaci n y utilizaci n del bitc in como criptomoneda.
  
- An lisis de los datos: Los datos recolectados ser n analizados e interpretados por el gerente del proyecto.
  
- Elaboraci n del reporte de resultados: La interpretaci n de los resultados ayudar n a tomar las decisiones finales.

En la secci n 2.2 se explic  la teor a en cuanto a los grupos de procesos y  reas de conocimiento de la direcci n de proyectos necesarios para ejecutar la obra con unas bases te ricas mejor establecidas. Adem s, como parte de la metodolog a que se elabora para guiar el desarrollo del proyecto, se utilizar n las siguientes  reas de conocimientos para la creaci n de entregables presentados en el Cap tulo VI –Propuesta del Proyecto –. Estas  reas del conocimiento son las que mejor cubren las necesidades del proyecto en cuanto a tareas por organizar y completar.

- Gesti n del Alcance del Proyecto: Definir el alcance del proyecto (desarrollo de los objetivos del proyecto) y EDT (Estructura de Desglose de Trabajo).
  
- Gesti n del Tiempo del Proyecto: Un cronograma definir  la fecha y duraci n necesaria para cada etapa del proyecto.

- Gestión de los Costes del Proyecto: Con un análisis de factibilidad se pueden estimar los costes del proyecto.
- Gestión de la Calidad del Proyecto: Un diagrama de causa y efecto puede significar un ahorro de tiempo y de trabajo para averiguar cuál es la causa de algo que no esté funcionando apropiadamente dentro de todo el sistema que compone la minería de bitc in. Este entregable en particular se considera muy  til, ya que se puede utilizar como una gu a de resoluci n de problemas. Muchas causas pueden provocar que el sistema no mine o que no funcione el sistema como tal, o que no se puedan transferir los ingresos a la billetera de *software*. Existen muchas posibilidades, y para perder la menor cantidad de tiempo –porque en la miner a de bitc in, el tiempo es literalmente dinero –un diagrama de causa y efecto puede ayudar mucho a descartar problemas y guiar hacia la soluci n de estos.
- gesti n de los Interesados del Proyecto: Se implementar  una lista de los involucrados e interesados en todo el proyecto, los cuales son personas o entidades que pueden ejercer total a parcial influencia sobre el proyecto.

### 3.2 Descripci n del Contexto o del Sitio en D nde se Lleva a Cabo el Estudio

El estudio realizado por el gerente del proyecto y emprendedor del negocio ser  llevado a cabo en su gran mayor a de manera virtual. Lo que significa que toda la investigaci n y estudios realizados se hacen en una computadora con acceso a internet. El bitc in, al ser una moneda virtual, esto significar  tambi n que la mayor a de su literatura, informaci n, herramientas y plataformas de la infraestructura de la informaci n se encuentran funcionando en l nea. Es decir, el internet es

intrínsecamente el hábitat del bitc in. Todas las investigaciones y consultas se realizan en una computadora; el gerente del proyecto se puede encontrar en cualquier pa s y podr  continuar trabajando de manera ininterrumpida en el proyecto durante el lapso establecido para realizar el estudio.

### 3.3 Caracter sticas de los Participantes y las Fuentes de Informaci n

Las fuentes de informaci n consultadas para la realizaci n del estudio son la bibliograf a citada y consultada, las p ginas de internet de los servicios de bitc in, que contienen informaci n vital para el entendimiento del funcionamiento de la criptomoneda en el mundo real, y otras p ginas de internet de comunidades de usuarios del bitc in que pueden aportar valiosa informaci n gracias a sus experiencias reales y personales en cuanto al uso de la criptomoneda. Ser  preciso, adem s, consultar a un experto en econom a acerca del uso del bitcoin en la econom a mundial.

### 3.4 T cnicas e Instrumentos para la Recolecci n de Datos

Como se mencion  en las fases del proceso de investigaci n del m todo cuantitativo, la recolecci n de datos se llevar  a cabo mayoritariamente por internet, se consultar  la informaci n disponible en las p ginas de internet de inter s, se examinar  informaci n en las p ginas de internet de las piscinas de miner a del bitc in, adem s se consultar  con el cliente seleccionado para abrir la billetera de bitcoins. Esta t cnica tiene un alto grado autodid ctico, en el que el ejecutor del proyecto es el que se informa con todas las fuentes de informaci n posible.

De manera similar, usuarios y expertos se encuentran disponibles en páginas de internet, especialmente en foros, en donde su conocimiento y experiencia se encuentra disponible gracias a su buena voluntad. También, todos los temas tratados en estos foros se encuentran disponibles en las bases de datos de las páginas de internet para uso de todos los usuarios que visiten la página o que busquen algún tema o problema en específico.

## CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS



## 4.1 Análisis

En esta sección se analizarán los resultados obtenidos a partir de la selección y utilización de la billetera de bitcoin y de todas las variables por considerar para la selección apropiada del equipo de infraestructura tecnológica de los ASIC con el fin de implementar la minería de bitcoin.

### 4.1.1 Creación de una Billetera de Bitcoin

Se escogió utilizar la billetera de *software* llamada Electrum, la cual presenta las siguientes características:

- Control sobre su dinero: Brinda control total del dinero. Ningún tercero puede congelar o perder sus fondos. Sin embargo, el usuario es responsable de la seguridad y de respaldar la billetera.
- Validación simplificada: Esta billetera utiliza verificación de pago simplificado (SPV por sus siglas en inglés) y servidores aleatorios de una lista; lo cual significa que se requiere poca confianza en terceros al verificar pagos. Sin embargo, no es tan seguro como un nodo completo, como la billetera Bitcoin Core.
- Transparencia básica: Los desarrolladores de esta cartera publican el código fuente para el cliente, esto significa que cualquier persona puede auditar el código. Sin embargo, todavía se necesita confiar en los desarrolladores de esta cartera al instalar o actualizar el *software*

final porque no fue construido de forma determinista como Bitcoin Core.

- Autenticación de dos factores: Esta cartera se puede utilizar en entornos inseguros. Sin embargo, este servicio requiere autenticación de dos factores, esto significa que el acceso a múltiples dispositivos o cuentas es necesario para robar los bitcoins.
- Privacidad básica: Previene el espionaje de sus pagos, pues esta cartera hace que sea más difícil espiar su saldo y pagos mediante direcciones rotatorias.

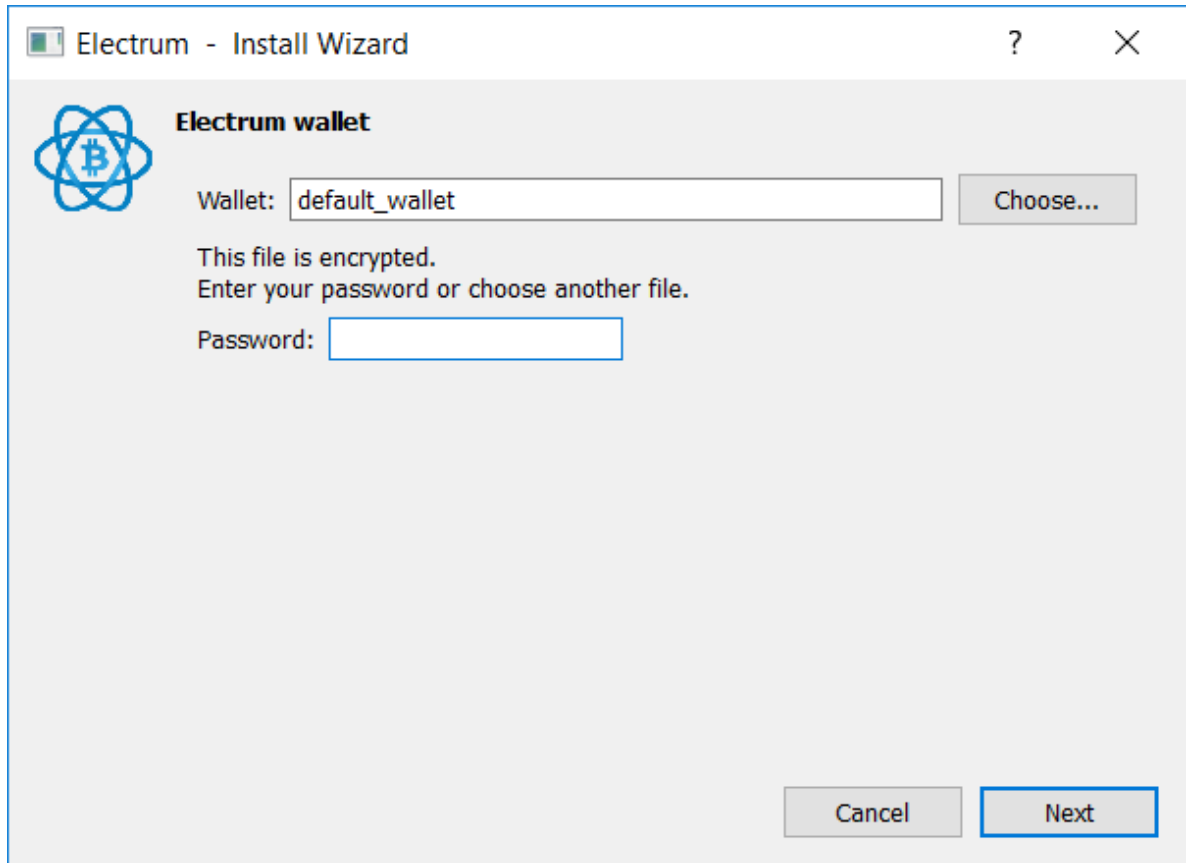
Divulga información a un tercero. Esta cartera utiliza servidores centrales que pueden asociar sus pagos y registrar su dirección IP.

- Control total sobre tarifas: Esta cartera admite un control total sobre las tarifas. Además, permite cambiar los honorarios después de que los fondos se envíen usando RBF o CPFP. Esta cartera también ofrece sugerencias de tarifas basadas en las condiciones actuales de la red para que las transacciones se confirmen de manera oportuna sin tener que pagar más de lo necesario.

Después de instalar Electrum, cada vez que se abre la billetera se debe ingresar la clave. Esto significa que la billetera está encriptada, tal y como se puede apreciar en la figura N° 4.

Figura N° 4 . Ventana de ingreso a Electrum.

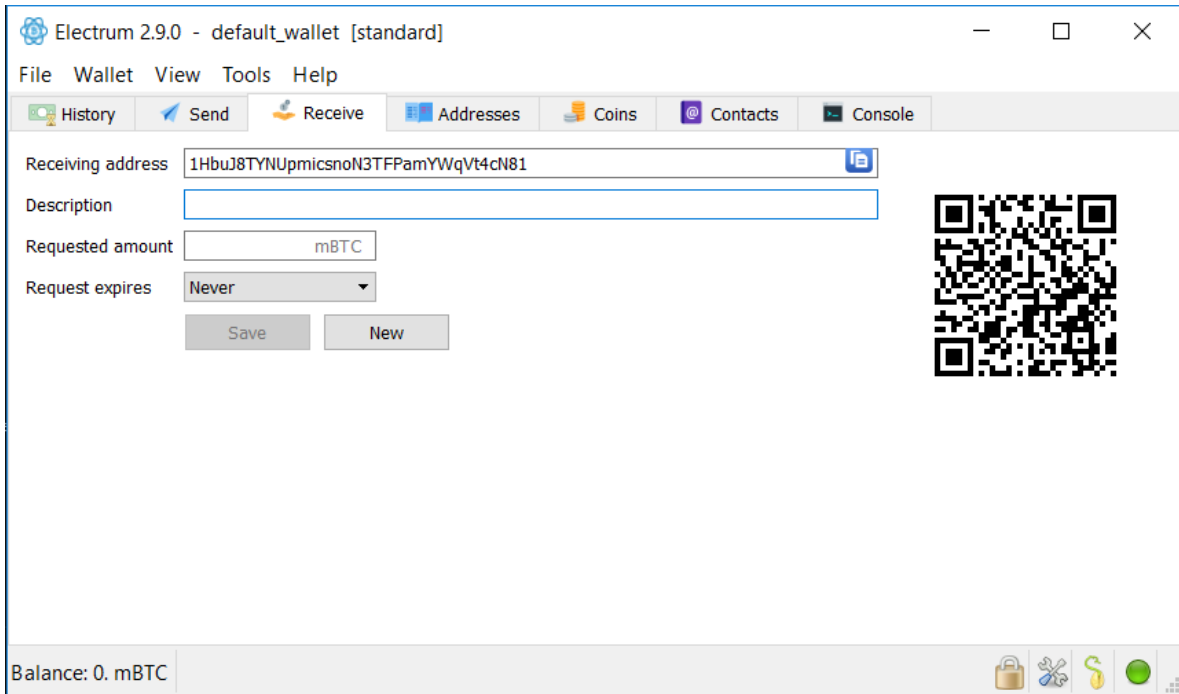
Fuente: Elaboración propia, 2017.



La siguiente imagen muestra la interfaz de Electrum. Entre sus funciones principales se puede mencionar la capacidad de revisar el historial de las transacciones, enviar y recibir bitcoins y revisar todas las diferentes direcciones diferentes para recibir bitcoins.

Figura N° 5 . Interfaz de Electrum.

Fuente: Elaboración propia. 2017.

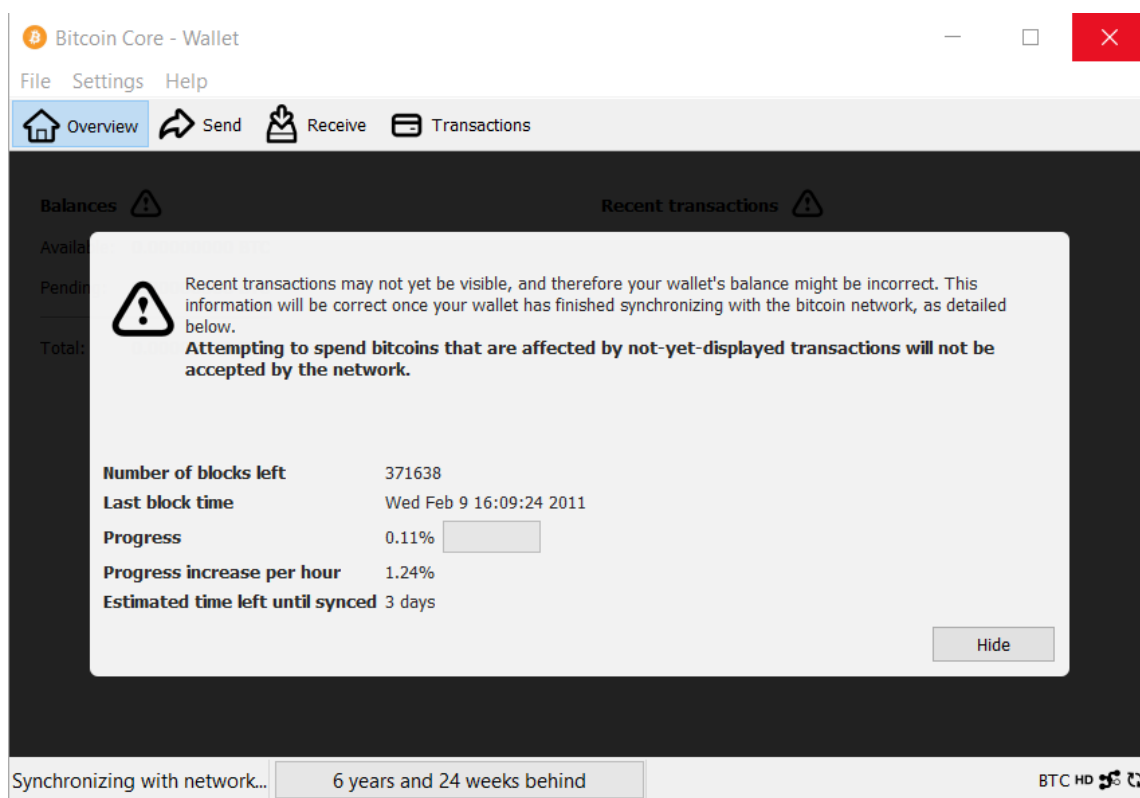


A manera de ejemplo, también se descargó el *software* Bitcoin Core, el cual es una billetera *software* con la particularidad de contener toda la cadena de bloques de transacciones de bitc oin, o sea, toda la red troncal de bitcoins, actuando oficialmente como un nodo de la red de bitcoins. La billetera de *software* estar a actuando como un verificador de la red de bitcoins, sin depender de ning un tercero para comprobar al 100% cualquier transacci on realizada. El detalle con este tipo de clientes completos es que se tiene que descargar la cadena de bloques completos (red troncal) de bitcoins, la cual actualmente es de 125 GB aproximadamente, este espacio (y m as para el futuro de la red) tiene que estar disponible de espacio de almacenamiento. Al descargar e instalar el programa, comienza la descarga de 125 GB de todos los datos de bloques de transacciones de la historia desde el 2008 hasta la fecha. Como se puede observar en la figura N o 6, se requieren m as de 3 d as de descarga para completar los m as de 100 GB de datos en la computadora. Eventualmente, la conexi on se

estabiliza y muestra que se requieren seis horas aproximadamente para completar la descarga. Cabe destacar que se utilizó una conexión de internet con una velocidad de 250 Mbps, pero la velocidad de la conexión con el servidor de Bitcoin Core recibida variaba de entre 2 a 20 Mbps.

Figura N° 6 . Inicio del programa de Bitcoin Core.

Fuente: Elaboración propia. 2017.



#### 4.1.2 Selección del Minero de Bitcoins

Para seleccionar el minero adecuado o que se adapte mejor a las necesidades del proyecto, se requiere estudiar la oferta del mercado y analizar las variables que afectarán la operatividad del proyecto.

La infraestructura antigua u obsoleta de minería del bitc in no ser  abordada en este an lisis porque ya no es capaz de competir con la velocidad de la miner a en la actualidad, ya no los venden y no existe beneficio alguno utilizarlos. Estos se componen de CPU Mining, GPU Mining y FPGA Mining. Actualmente se utilizan infraestructura ASIC (Application-Specific Integrated Circuit, por sus siglas en ingl s), se puede traducir como un circuito integrado espec fico para una aplicaci n. Como su nombre lo indica, es un microchip dise ado y fabricado para un prop sito muy espec fico. Los ASIC dise ados para la miner a de bitc in fueron lanzados por primera vez en 2013. Adem s, debido a la cantidad de energ a que consumen, son mucho m s r pidos que todas las tecnolog as anteriores. A diferencia de los dispositivos antiguos, los ASIC no pueden ser utilizados para ning n otro prop sito. Un ASIC dise ado para minar bitcoins solo puede minar bitcoins. La inflexibilidad de un ASIC se compensa por el hecho de que ofrece un aumento de cientos de veces en la potencia de *hashing*, de manera que reduce el consumo de energ a en comparaci n con todas las tecnolog as anteriores.

A diferencia de todas las anteriores, ASIC puede ser el  ltimo de los cambios o el final de la l nea cuando se trata de la tecnolog a de miner a disruptiva. Las CPU fueron reemplazadas por GPUs que fueron sustituidas por FPGAs, estos, a su vez, fueron reemplazados por ASICs. No hay nada que reemplace ASIC ahora o incluso en el futuro inmediato ya que, a diferencia de sus predecesores, los ASIC fueron dise ados  nica y exclusivamente para minar bitcoins, cabe se alar que ninguno

de estos ASIC se refieren a computadoras o aparatos electrónicos modificados o programados para minar, sino de elementos creados para ello.

Habr  un refinamiento gradual de los productos ASIC y un aumento de la eficiencia, pero nada ofrecer  otro brinco de 50 a 100 veces en la potencia de *hashing* o la reducci n de 7 veces en el uso de energ a que viene de las tecnolog as anteriormente ofrecidas. Dicha situaci n provoca que el consumo de energ a en un dispositivo ASIC sea el factor m s importante de cualquier producto ASIC, ya que la vida  til esperada de un dispositivo de miner a ASIC es m s larga que toda la historia de la miner a del bitc in.

Es concebible que un dispositivo ASIC comprado hoy todav a est  minando en dos a os, si el dispositivo es suficientemente eficiente en cuanto a energ a y al costo de la electricidad (que no exceda su capacidad de producci n). La rentabilidad de la miner a tambi n est  dictada por el tipo de cambio del bitc in con respecto a la moneda local, pero en todas las circunstancias, cuanto m s eficiente en cuanto energ a sea el dispositivo, m s rentable ser .







Existen varios fabricantes de mineros ASIC para bitc in, uno de los m s reconocidos y confiables son lo Antminer fabricados por la marca Bitmain, esta es una de las marcas m s utilizadas, sencillas de usar, comprar, revender y configurar. Dada la preferencia y confiabilidad a esta marca se ha optado por utilizar su modelo m s reciente y poderoso, el Antminer S9, lanzado el 12 de junio de 2017 con un precio inicial de \$2100 en Amazon. El Antminer S9 puede ser de los ASIC m s caros en el mercado, pero sin duda alguna es el mejor minero en el mercado. En las siguientes p ginas se describir n las variables que afectan la eficiencia y la rentabilidad de la miner a del Bitcoin, pero es respecto al poder de procesamiento de 14 TH/s (Tera *Hashes* por segundo) que el Antminer es el que se encuentra en

el tope de la carrera de resolución de *hashes* criptográficos de bloques de transacciones de bitcoins. En otras palabras, es la unidad de procesamiento ASIC más eficiente actualmente.

A manera de ejemplo, en la figura N° 7 se puede observar el precio y la velocidad de procesamiento de los ASIC más utilizados en el mercado.

Figura N° 7 . Comparación Entre Actuales ASICs en el Mercado.

Fuente: [www.buybitcoinworldwide.com](http://www.buybitcoinworldwide.com), 2017.

Imagen	Minero	Poder de Hash	Precio
	Antminer S5	1.16 TH/s	\$139.99
	Antminer S7	4.73 TH/s	\$489.99
	Antminer S9	14.0 TH/s	\$3,000
	Avalon 6	3.50 TH/s	\$559.95
	SP20 Jackson	1.3-1.7 TH/s	\$90.00
	Antminer R4	8.6 TH/s	\$1,000



### 4.1.3 Variables de la Minería de Bitc in

Para entender el funcionamiento  ptimo de la miner a y c mo llegar a alcanzar una  ptima eficiencia, es necesario comprender las variables que afectan el rendimiento y rentabilidad de esta actividad para tomar mejores decisiones y saber elegir y gestionar el equipo apropiado. Existen ocho variables en la miner a del bitc in.

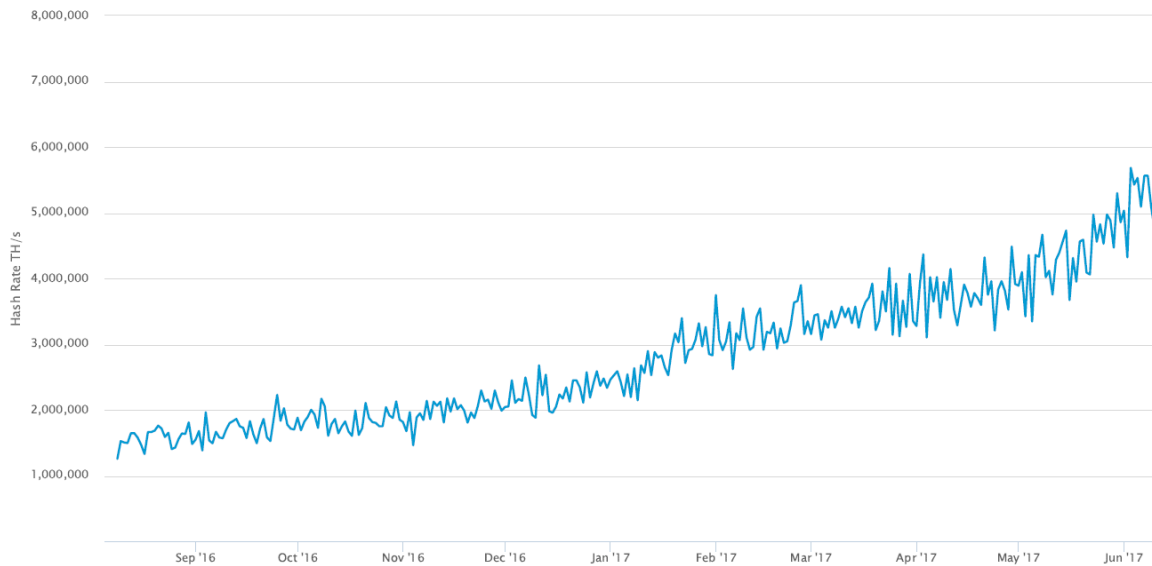
#### 4.1.3.1 Tasa de *Hash* (*Hashes/s*)

Un *hash* es la salida de una funci n *hash* y, en lo que se refiere a bitc in, la Tasa de *Hash* es la velocidad a la que un c lculo completa una operaci n en el c digo bitc in. Una tasa de *hash* m s alta es mejor en cuanto a la miner a, ya que aumenta la probabilidad de encontrar la soluci n del algoritmo *hash* del bloque de transacci n actual y as  recibir la recompensa del bloque (BTC), el cual es el objetivo principal de la miner a.

La suma total de la tasa de *hash* de todos los mineros trabajando en la red de bitc in se le denomina como la tasa de *hash* de la red. En el cap tulo 1 se explic  qu  es la miner a del bitc in y se coment  acerca de la competencia global entre todos los mineros y piscinas de mineros por resolver los bloques de transacciones, lo cual permite que la red sea cada vez m s grande y segura. Esta adici n de mineros en el mundo y aumento en la tasa de *hash* total se puede observar en la Gr fica N  4, en ella se muestra el n mero estimado de *hashes* por segundo (billones de *hashes* por segundo) de la red bitc in en operaci n. As , cada ASIC tiene una variable de operaci n en *hashes* por segundo, lo cual significa la rapidez en la que puede resolver los problemas criptogr ficos.

Gráfica N° 3. Tasa de Hash (trillones de hashes por segundo) durante el último año.

FUENTE: <https://blockchain.info>, 2017.



#### 4.1.3.2 Consumo Eléctrico (Watts)

En cuanto al consumo de potencia eléctrica (voltaje por corriente) del ASIC, este dato lo proporciona el fabricante del ASIC. Dicha variable es importante porque al estar en funcionamiento en la red eléctrica, se cobrará por la electricidad consumida en Kilowatt/hora.

#### 4.1.3.3 Costo del Consumo Eléctrico (\$)

El costo del consumo eléctrico se refiere al costo de la electricidad utilizada en kilowatt/hora cobrada en colones en Costa Rica. Para propósitos de este trabajo el precio se convertirá a dólares. Según el Instituto Costarricense de Electricidad, la tarifa mensual para el área residencial se puede ver en la siguiente tabla:

Tabla N° 1. Tarifa eléctrica residencial mensual

Primeros 200 kWh a	¢77.67 /kWh
Por cada kilovatio adicional	¢140.00 /kWh

FUENTE: Tarifa ICE Alcance 152 III Trimestre 2017

Los primeros 200KWh son relativamente baratos, y rápidamente cualquier hogar puede exceder los primeros 200KW de consumo en un día. Para propósitos de este trabajo, tomar en cuenta 77.67 colones por kWh es prácticamente despreciable, por tanto, se tomará como tarifa fija 140.00 colones por kWh como variable constante para la tarifa de consumo eléctrico. También, se utilizará la tarifa residencial, ya que la actividad de la minería no está registrada en Costa Rica como una actividad económica oficialmente lucrativa y se puede realizar de manera privada en una casa o una bodega de alquiler, como se estipuló en el alcance del trabajo.

Por tanto, 140 colones equivalen a 24 centavos de dólar según el tipo de cambio del Banco de Costa Rica de 583 colones por cada dólar al 9 de septiembre de 2017.

#### 4.1.3.4 Tarifa de la Piscina de Minería (%)

En este ambiente altamente competitivo, los mineros individuales que trabajan solos (también conocidos como mineros solistas) no tienen prácticamente ninguna posibilidad. La probabilidad de que encuentren un bloque para compensar

sus costos de electricidad y *hardware* es tan baja que representa una apuesta, como jugar a la lotería. Incluso el sistema de minería de ASIC de consumo más rápido no puede mantenerse al día con los sistemas comerciales que apilan decenas de miles de estos chips en almacenes gigantes. Los mineros ahora se agrupan para formar piscinas de minería, de esta manera unen su poder de distribución y comparten la recompensa entre miles de participantes. Al participar en una piscina, los mineros obtienen una porción menor de la recompensa general, pero normalmente reciben recompensas cada día, situación que reduce la incertidumbre.

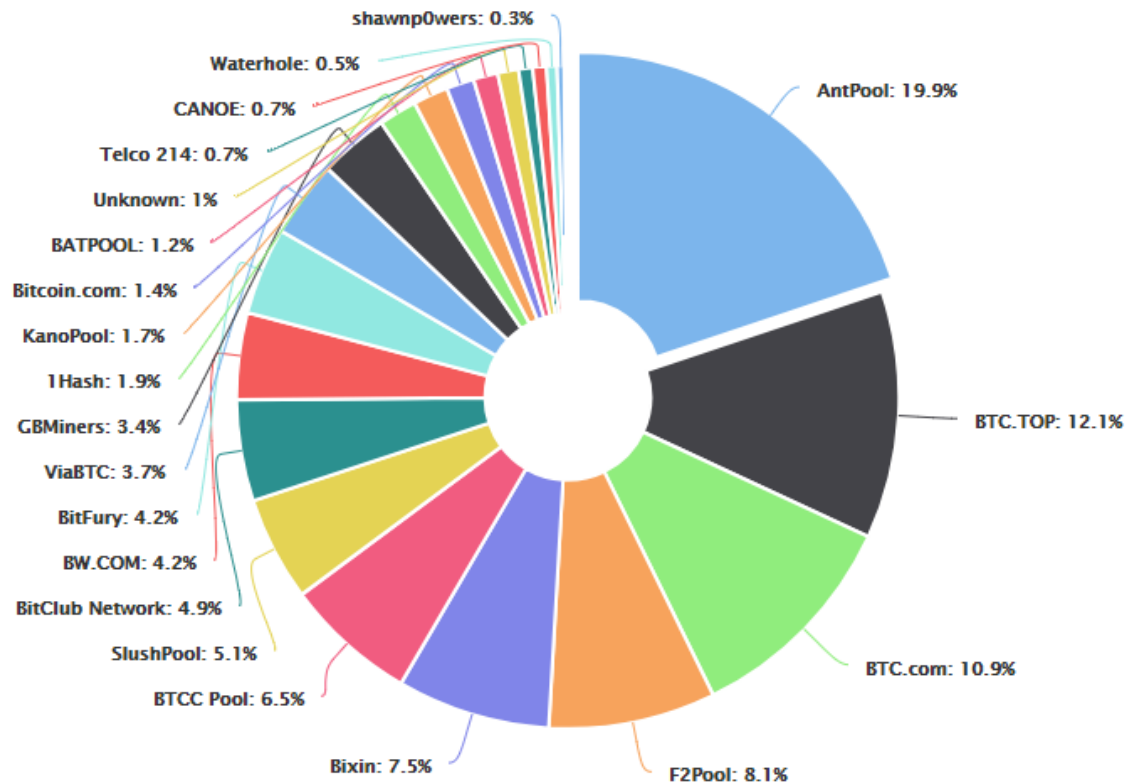
Las piscinas son grupos de mineros cooperando entre sí para compartir recompensas de bloques, cada recompensa individual es directamente proporcional al poder de *hash* de cada minero (en *Hashes* por segundo). Mientras que las piscinas de mineros son deseables para el minero promedio por las razones anteriormente descritas. Desafortunadamente, concentran el poder en el propietario de la piscina. Los mineros pueden; sin embargo, optar por redirigir su poder de *hashing* a una piscina de minería diferente en cualquier momento.

La mayoría de ASICs de piscinas se encuentra ubicada en China (cerca del 80% de ellas) y existen varias decenas de servidores a los cuales unirse. Muchos son privados, otros públicos; todos con diferentes tipos de tarifas y condiciones para asociarse. En la gráfica N° 5 se puede observar el tamaño de las principales piscinas en el mundo de acuerdo con el poder distribuido de *hash*.

Dada la facilidad en manejar una cuenta de usuario en Antpool y la confiabilidad del sitio, se ha decidido utilizar la piscina de antpool.com, la cual cobra una tarifa de 1,5% sobre las recompensas recibidas por su contribución al poder o tasa de *hash*.

Gráfica N° 4. Distribución de la tasa de *hash* en las más grandes piscinas de mineros.

FUENTE: <https://blockchain.info/pools>, 2017.



#### 4.1.3.5 Dificultad del Bitc in

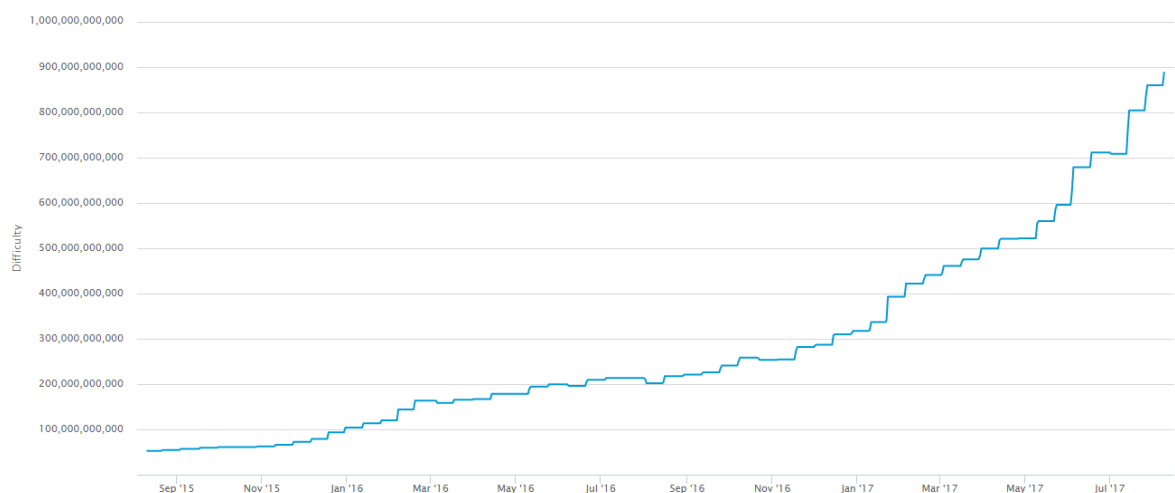
Es una medida relativa de lo dif cil que es encontrar un nuevo bloque. La dificultad se ajusta peri dicamente en funci n de la cantidad de energ a de *hashing* que ha sido desplegada por la red de mineros. Un bloque se genera cada 10 minutos, en promedio. Este latido del bitc in determina la frecuencia de emisi n de bitcoins y la velocidad del establecimiento de las transacciones. Adem s, debe mantenerse constante no solo en un periodo corto, sino tambi n durante varias d cadas. A lo largo de ese tiempo se espera que el poder computacional de las

computadoras (y de los ASICs) continúe incrementando. De igual manera, el número de usuarios y de mineros también cambiará. Para mantener el bloque de transacción en 10 minutos, la dificultad del algoritmo criptográfico (minería) debe ser ajustada para satisfacer esta constante. En consecuencia, la dificultad es una variable dinámica que será periódicamente ajustada para satisfacer este objetivo de 10 minutos por bloque. En simples palabras, la dificultad es establecida para que con la tasa de *hash* existente de la red de bitc in se resuelva un bloque en 10 minutos. La dificultad es una magnitud adimensional, lo que significa que se maneja sin unidades. Seg n el protocolo de bitc in en los nodos completos, se realiza este ajuste cada 2016 bloques (2 semanas). La diferencia existente entre el bloque anterior y el tiempo en que fue resuelto es la que se aplicar  al siguiente valor de dificultad. Actualmente, el valor de la dificultad es de: 923.233.068.448.

En la gr fica N  6 se puede observar el incremento de la dificultad en los  ltimos 2 a os, esto dado al aumento en la tasa de *hash* en el mundo (el cual se observ  en la Gr fica N  4).

Gr fica N  5. Dificultad del minar el Bitc in en los  ltimos dos a os.

FUENTE: <https://blockchain.info/charts/difficulty?timespan=2years>, 2017.



#### 4.1.3.6 Recompensa del Bloque (BTC)

Como se mencionó en el capítulo II, la recompensa por haber descifrado un bloque de transacción es actualmente de 12,5 BTC. El protocolo de bitc in fue establecido de manera que, en su lanzamiento en el 2008, la recompensa fuera de 50 BTC por bloque acertado, cada 210000 bloques (4 a os en tiempo) se disminuir a a la mitad. Actualmente, rige la tercera divisi n (12.5 BTC por bloque).

#### 4.1.3.7 Bitcoin al D lar (\$)

En la Gr fica N 1 se observa que a la fecha actual (8 de agosto de 2017) el precio del bitc in es de aproximadamente \$3357. Esta variable es din mica y cambia todos los d as. El precio del bitc in var a por muchas razones, principalmente debido a la importancia que le dan las personas, los bitcoins en circulaci n y al uso del bitc in como medio de pago o de intercambio.

#### 4.1.3.8 Costo del Equipo (\$)

Costo del equipo necesario para minar. B sicamente el costo del ASIC y la respectiva fuente de poder.

1 Antminer S9 tiene un precio de \$2299.

1 Fuente de poder APW3 tiene un precio de \$269.

#### 4.1.4 Resultados de una Calculadora de Minería

Las calculadoras de la minería de bitc in disponibles en l nea son herramientas que aproximan los resultados lo m s precisamente posible considerando las ocho variables descritas anteriormente. Con ellas, los usuarios se pueden informar acerca de los resultados esperados en cuanto a los valores de las variables que pueden utilizar dependiendo de d nde vivan. Por ejemplo, en algunas partes de China la electricidad es gratuita, mientras que en otras ciudades de Estados Unidos y de Europa la electricidad es tan cara que puede tornar la actividad totalmente improductiva.

La siguiente Figura N 8 recopila todas las variables analizadas con los valores utilizados en la realidad para realizar un c lculo aproximado de gastos e ingresos. Los valores hacen referencia a una captura tomada al 10 de agosto de 2017.



Figura N° 8. Calculadora de Minería para 1 Antminer S9 al 10 de agosto de 2017.

Fuente: <https://www.coinwarz.com/calculators/bitcoin-mining-calculator>, 2017.

<b>Hash Rate (GH/s):</b>	<b>Power (Watts):</b>
<input type="text" value="13500.00"/>	<input type="text" value="1350.00"/>
<b>Power Cost (\$/kWh):</b>	<b>Pool Fees %:</b>
<input type="text" value="0.24"/>	<input type="text" value="1.50"/>
<b>Bitcoin Difficulty:</b>	<b>Block Reward:</b>
<input type="text" value="923233068448.905000"/>	<input type="text" value="12.50000000"/>
<b>Bitcoin to Dollar (USD):</b>	<b>Hardware Costs (USD):</b>
<input type="text" value="3439.49430000"/>	<input type="text" value="2299.00"/>
<input type="button" value="Calculate"/>	

Traducción: Tasa de Hash/Energía/Costo de energía/Cuota de piscina/Dificultad del Bitcoin/Recompensa del bloque/Bitcoin al Dólar/Costo del equipo.

Tabla N°2. Resultados de la Calculadora de Minería para 1 Antminer S9 al 10 de agosto de 2017.

Time Frame	BTC Coins	USD	Power Cost (in USD)	Pool Fees (in USD)	Profit (in USD)
Hourly	0.00015321	\$0.53	\$0.32	\$0.01	\$0.20
Daily	0.00367694	\$12.65	\$7.78	\$0.19	\$4.68
Weekly	0.02573857	\$88.53	\$54.43	\$1.33	\$32.77
Monthly	0.11030814	\$379.40	\$233.28	\$5.69	\$140.43
Annually	1.34208238	\$4,616.08	\$2,838.24	\$69.24	\$1,708.60

Fuente: <https://www.coinwarz.com/calculators/bitcoin-mining-calculator>, 2017.

Traducción: Rango de tiempo/Monedas BTC/Dólares/Costo de electricidad/Cuota de Piscina/Ganancias.

Con el fin de obtener un criterio y un entendimiento más amplio de los resultados que se pueden obtener con la minería del bitc oin, se realiz  el mismo an lisis y c lculo utilizando seis unidades de AntMiner S9. Despu s de todo, el prop sito de la miner a es trabajo (o minar) con la mayor cantidad de recursos disponibles para poder aportar la mayor cantidad posible de poder de tasa de *hashes* por segundo a la piscina de miner a en la que se est  trabajando. Cuanto m s poder de procesamiento, mayor es el tama o de la recompensa en una piscina. Por lo tanto, uno de los prop sitos m s importante de la miner a es entrar a esta con la mayor cantidad posible de ASICs (tasa de *hash*). La siguiente Figura N  9 y la Tabla N  3 extrapolan el mismo an lisis utilizando seis unidades de AntMiner S9 al d a 13 de agosto de 2017.

Figura N° 9. Calculadora de Minería para seis Antminer S9 al 13 de agosto de 2017.

Fuente: <https://www.coinwarz.com/calculators/bitcoin-mining-calculator>, 2017.

<b>Hash Rate (GH/s):</b>	<b>Power (Watts):</b>
<input type="text" value="81000.00"/>	<input type="text" value="8100.00"/>
<b>Power Cost (\$/kWh):</b>	<b>Pool Fees %:</b>
<input type="text" value="0.24"/>	<input type="text" value="1.50"/>
<b>Bitcoin Difficulty:</b>	<b>Block Reward:</b>
<input type="text" value="923233068448.905000"/>	<input type="text" value="12.50000000"/>
<b>Bitcoin to Dollar (USD):</b>	<b>Hardware Costs (USD):</b>
<input type="text" value="4030.10190000"/>	<input type="text" value="13794.00"/>
<input type="button" value="Calculate"/>	

Traducción: Tasa de Hash/Energía/Costo de energía/Cuota de piscina/Dificultad del Bitcoin/Recompensa del bloque/Bitcoin al Dólar/Costo del equipo.

Tabla N°3. Resultados de la Calculadora de Minería para seis Antminer S9 al 13 de agosto de 2017.

Fuente: <https://www.coinwarz.com/calculators/bitcoin-mining-calculator>, 2017.

Time Frame	BTC Coins	USD	Power Cost (in USD)	Pool Fees (in USD)	Profit (in USD)
Hourly	0.00091923	\$3.70	\$1.94	\$0.06	\$1.71
Daily	0.02206163	\$88.91	\$46.66	\$1.33	\$40.92
Weekly	0.15443140	\$622.37	\$326.59	\$9.34	\$286.45
Monthly	0.66184885	\$2,667.32	\$1,399.68	\$40.01	\$1,227.63
Annually	8.05249430	\$32,452.37	\$17,029.44	\$486.79	\$14,936.15

Traducción: Rango de tiempo/Monedas BTC/Dólares/Costo de electricidad/Cuota de Piscina/Ganancias.

#### 4.1.5 Entrevistas Realizadas

Se realizó una entrevista a Luis E. Loria, economista graduado de la escuela de negocios de Harvard, con más de 25 años de experiencia como consultor público y privado, y presidente de Strategic Advantage Consulting Group:

- 1) ¿Considera usted el bitc in (como moneda descentralizada y universal) una soluci n potencial a la mayor a de problemas que representa el uso de diferentes tipos de monedas centralizadas y a las decisiones que toman los gobiernos y los bancos centrales respecto a la econom a?

Una moneda descentralizada y universal podr a, eventualmente, contribuir a solucionar varios de los problemas relacionados con el uso de monedas centralizadas y las decisiones que toman los gobiernos y bancos centrales con respecto a la econom a. Estos problemas guardan relaci n, por ejemplo, con el abuso de emisi n monetaria sin respaldo con consecuencias inflacionarias y decisiones arbitrarias en el manejo de la pol tica cambiaria, que tienen como consecuencia una redistribuci n injusta de la riqueza, al generar artificialmente grupos ganadores y grupos perdedores.

El uso de una moneda descentralizada y universal eliminar a, tambi n, los costos de transacci n asociados con el cambio entre monedas y los costos relacionados con el uso y reposici n de efectivo, ya que todas las transacciones ser an electr nicas.

Sin embargo, todav a no parece que el mundo est  listo para eliminar las monedas nacionales para adoptar una moneda descentralizada

independiente. Para empezar, mientras los gobiernos cuenten con el poder para obligar a los ciudadanos a llevar las cuentas en moneda nacional, recibir los pagos de salarios, pensiones y contratos, y pagar impuestos en esa moneda, aunque los ciudadanos prefieran otra moneda internacional (dólares, por ejemplo) o una moneda como el bitc in, no podr n migrar a ella totalmente y, adicionalmente, tendr n que incurrir en costos de transacci n para cambiar la moneda internacional o el bitc in por moneda local o viceversa.

Tambi n, el bitc in todav a no es una moneda universalmente aceptada y existe discusi n alrededor de si cumple todas las funciones de dinero: medio de cambio, unidad de cuenta y dep sito de valor. Para que sirva como medio de cambio, las personas deben confiar en esa moneda para utilizarla para las transacciones. Muchas personas y negocios, hasta ahora, no conf an en monedas independientes y, por lo tanto, no la aceptar an para ser utilizada en sus transacciones. Para que sirva como unidad de cuenta, se debe poder fijar los precios para todos los bienes y servicios en esa moneda. Hasta la fecha, la mayor a de los precios se fijan en monedas nacionales y no en bitcoins o en otras monedas descentralizadas. Para que sirva como dep sito de valor, el dinero deber a mantener su valor relativamente bien (al compararse con otras monedas) a lo largo del tiempo. Este es uno de los puntos que m s preocupan, ya que el valor del bitc in y monedas similares ha fluctuado significativamente en el tiempo. Mientras no se pueda reducir esa incertidumbre con respecto al valor que tendr  una moneda descentralizada en el futuro, es poco probable que las personas est n dispuestas a adoptar masivamente –y, eventualmente universalmente– una moneda descentralizada.

- 2) ¿Considera que el bitc33in, o alguna otra criptomoneda universal, descentralizada y administrada por la misma red de usuarios, sea una opci33n m33s beneficiosa para el mundo entero (moneda universal), considerando que la mayor33a de dinero emitido actualmente existe solamente en formato digital y no impreso?

Los beneficios de la adopci33n y uso de una criptomoneda universal pueden ser importantes, pero todav33a existen desaf33os importantes para que esta se adopte de manera masiva o incluso universal (ver respuesta anterior). Adicionalmente, a pesar de que el uso de medios electr33nicos de pago y de cuentas electr33nicas se ha generalizado, todav33a un porcentaje importante de la poblaci33n, particularmente en pa33ses de menor desarrollo relativo, no se encuentra bancarizado (no utiliza los bancos), no utiliza medios de pago electr33nicos y prefiere utilizar el efectivo en sus transacciones. Entonces, mientras esa realidad no se supere, una adopci33n universal de una criptomoneda no ser33a viable.

#### 4.1.6 Interpretación de los Resultados

Al haber analizado cada variable que afecta la minería y realizar un cálculo aproximado con los valores utilizados para la minería, se puede deducir que para ambas situaciones –trabajar tanto con 1 como con 6 AntMiner S9 durante las 24 horas del día los 365 días del año –la inversión inicial se recupera en un plazo superior a 12 meses. En la primera situación, al 10 de agosto de 2017, con una inversión de \$2999 y el precio del bitc in a \$3439, se necesitar a m as de 13 meses para recuperar la inversi n inicial del equipo; aproximadamente se requerir a un a o y medio para sobrepasar la inversi n inicial. En el segundo caso, con 6 AntMiner S9, se observa que se requiere menos tiempo para que se recupere la inversi n inicial. Cabe destacar que en tres d as el bitc in subi  de \$3439 a \$4030, situaci n que favoreci  considerablemente los resultados de la miner a, eso es parte de las fluctuaciones que enfrentan toda la red de usuarios del bitc in, la moneda se encuentra en constante cambio.

Un desglose de resultados m as exactos y apegados a la realidad se ubica en el an lisis de factibilidad en la secci n 6.3.5. En esta secci n se tomaron en cuenta otros costes adicionales que se le restan a las ganancias obtenidas al primer a o de operaci n de la miner a de bitc in. Tales costes que no son considerados en la calculadora de miner a son: un switch de red, seis fuentes de poder y el costo anual del servicio de conexi n a internet. Con estos elementos en juego, se requiere m as de 12 meses de operaci n para recuperar la inversi n inicial.

Las ganancias estimadas de bitc in se basan en un c lculo estad stico usando los valores ingresados y no consideran las fluctuaciones de las tasas de cambio y de dificultad, las tasas obsoletas/rechazadas/hu rfanas ni la eficiencia de un grupo en la piscina de mineros. Las ganancias estimadas esperadas de bitc in pueden variar mucho dependiendo de la eficiencia de la piscina, la tasa de



retraso/rechazo/huérfano y las tarifas. Por lo tanto, la tabla N° 3 y la figura N° 9 son resultados estáticos en un momento específico en el tiempo, es decir, no son resultados que toman en cuenta variables dinámicas en el tiempo, ni resultados 100% exactos.

Durante los últimos 12 meses el bitc in ha batido un r cord en cuanto al aumento de su precio en m s de \$3000. Los  ltimos dos a os han sido los m s fruct feros hist ricamente hablando para los mineros del bitc in; pues con el mejoramiento de procesamiento de los ASIC (ver Gr fica N  4) y el elevado precio del bitc in (ver Gr fica N  1), el negocio de la miner a ha tenido una amplia expansi n y aceptaci n en todo el mundo –a la vez, esto ha fortalecido la red del protocolo de bitc in –y es posible que la situaci n contin e mejorando, por lo menos hasta el a o 2020, cuando se volver  a reducir a la mitad el valor de la recompensa del (12.5 BTC actualmente). Sin embargo, se cree que cuando la recompensa sea dividida nuevamente, el precio del bitc in seguir  creciendo para compensar esta disminuci n en la miner a y seguir  aumentado la tasa de *hash* total de todo el mundo (adem s aumentar  el n mero de mineros), lo que ayudar a a que la miner a del bitc in contin e siendo un negocio rentable durante otros cuatro a os m s despu s de 2020.

## CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

## 5.1 Interpretación de los Resultados

Las conclusiones presentadas se desarrollaron con respecto a los objetivos del estudio realizado.

- Se recopilaron y utilizaron los conceptos necesarios en cuanto a gerencia de proyectos, tanto para realizar la investigación del tema como para la ejecución del proyecto. La Guía del PMBOK funcionó como base para identificar los grupos de procesos y las áreas de conocimientos de la dirección de proyectos, todos ellos facilitaron fundamentar una base teórica como una guía para la recolección y procesamiento de la información. También, esta guía teórica de la dirección de proyectos brindó técnicas y herramientas útiles para la ejecución y control del proyecto, como lo fueron las entrevistas, juicios de expertos (en internet), estimación de costos y estudios comparativos.
- Después de la recopilación y análisis de la información y literatura del tema estudiado; se detalló ampliamente el concepto del bitc in como criptomoneda, su origen, funcionamiento e impacto en el mundo. Se revel  la importancia y el impacto que ha producido el bitc in en el mundo, sus ventajas y desventajas, as  como la puerta que apenas se ha abierto al haber sido la primer criptomoneda en funcionamiento. Dicha circunstancia pone en alerta a gobiernos, empresas y bancos centrales que rigen el uso y desuso de las monedas tradicionales y centralizadas que circulan en el mundo.

Asimismo, se ilustr  el funcionamiento del bitc in como protocolo centrado en una red de nodos de usuarios y se explic  el concepto de

la minería del bitc33n (*bitcoin mining*) como parte de la red troncal de los bloques de transacciones de los bitcoins, pues estos funcionan como los engranajes que permiten el constante movimientos de las transacciones de bitcoins en el mundo, al mismo tiempo brindan seguridad y robustez a la red. Complementariamente, se demostr33 que la minería del bitc33n es una actividad lucrativa a partir de la cual se pueden generar ganancias o ingresos al formar parte de la red de tasa de procesamiento de *hash* de una piscina de mineros (*mining pool*), esto al utilizar el equipo apropiado (ASIC), hecho que brinda el servicio de la minería estando conectado a la red de bitc33n a trav33s de la misma infraestructura de red com33n y corriente de internet a la que gran cantidad de la poblaci33n mundial tiene acceso.

- Se cre33 satisfactoriamente una billetera (*bitcoin wallet*) por medio del uso del *software* llamado Electrum. De este programa, se obtuvo una direcci33n receptora (*public key*) la que es utilizada para recibir pagos en bitc33n. Una de estas direcciones es necesaria para que sea posible el dep33sito de las ganancias obtenidas a partir de la minería de bitc33n. Tambi33n, se explicaron las característic33s de Electrum como una billetera ligera (*light client wallet*).
- Se identificaron las ocho variables que influyen en el funcionamiento y rentabilidad de la actividad de la minería de bitc33n, las cuales son: Tasa de *hash*, consumo el33ctrico, costo de la electricidad, tarifa de la minería de bitc33n, dificultad del bitc33n, recompensa del bloque de transacci33n, precio del bitc33n y costo del equipo (ASIC). Todas las variables son dinámicas en el tiempo. Las que presentan un comportamiento menos variable son el costo del equipo y el consumo el33ctrico, ya que no cambia el precio de ellos a menos de que el

proveedor lo haga en algún momento del año. El costo del ASIC es utilizado una única vez y el consumo eléctrico podría variar en algún momento del año. Adicionalmente, se explicaron las razones por las cuales las otras variables pueden llegar a variar, ya sea cada día o cada 4 años; dentro de un rango de variación relativamente bajo de un cambio a otro, entre 0 a 15%, como se ilustró en las gráficas utilizadas en la sección 4.1.3: Variables de la minería de bitcoin. Sin embargo, durante el trabajo de investigación se comprendió que el bitc on como moneda puede llegar a tomar un giro inesperado en cualquier momento, dada su ilegitimidad como moneda no oficial, descentralizada e independiente (administrada por los usuarios mismos).

- Se calcul  un tiempo aproximado mayor a 12 meses de ingresos, minando las 24 horas del d a, para llegar a recuperar la inversi n inicial como se discuti  en la secci n 4.1.4: Resultados de la miner a de una calculadora de bitc on. El resultado de los ingresos es relativo al cambio de las variables de la miner a de bitc on en el momento en funcionamiento. N tese que de la primera a la segunda simulaci n de la calculadora, los resultados fueron m s eficientes debido al alza en el precio del bitc on, ya que se dio un cambio de \$3439.40 a \$4030.00 en el precio del bitc on en el mundo. Es decir, hubo \$590.51 de aumento en tres d as, esto benefici  los resultados de la segunda simulaci n. De hecho, al momento de redactar la presente conclusi n (16 de agosto de 2017), el bitc on subi  nuevamente a un valor de \$4421.26, cifra que dar a un resultado a n m s eficiente para la miner a del bitc on.

## 5.2 Recomendaciones

El gerente del proyecto y dueño de la empresa ficticia (Bitcoin CR) es el único responsable de la ejecución del proyecto y del mantenimiento de las operaciones después de la puesta en marcha, dicha empresa fue creada con el fin de realizar la actividad de la minería de bitc in. En otras palabras, no se identifica ning n otro responsable en el proyecto, ya que este se considera, hasta este alcance establecido en los objetivos, como un proyecto que se puede realizar en solitario.

Algunos interesados y participantes de la miner a de bitc in y del bitc in como criptomoneda son los siguientes: Usuarios del bitc in, personas que todav a no conocen o no han utilizados los beneficios del bitc in (no usuarios), Bitmain, productores de los ASIC utilizados (Antminer) y de la piscina de miner a seleccionada (Antpool), as  como el gobierno y el Banco Central de Costa Rica.

Al gerente del proyecto: La situaci n de la miner a se mantendr  estable hasta la pr xima divisi n de la recompensa por bloque de transacci n, el cual ser  en el 2020, por lo que los siguientes dos a os y cuatro meses presentan un panorama rentable para la miner a. No obstante, se recomendar  proceder con la actividad de la miner a del bitc in con la mayor cantidad posible de Antminer S9, ya que, como se demostr  anteriormente, se necesitan alrededor de 12 meses para recuperar la inversi n inicial y esta situaci n est  mejorando con el incremento del precio del bitc in. Al momento de redactar esta recomendaci n (13 de agosto de 2017), el precio del bitc in se ha mantenido por encima de \$4000. Al 20 de agosto de 2017 est  en \$4139.92. As , el Antminer S9 ser   til por 2 a os y medio m s hasta la pr xima divisi n de la recompensa, que se tornar  en 6.25 BTC por bloque resuelto; esto disminuir  el valor de la recompensa, pero muy probablemente el precio del bitc in ser  inflado para entonces. Tambi n se espera que existan ASICs m s potentes despu s de 2020, por lo que se podr a considerar reemplazar los

Antminer S9 por el modelo más reciente existente a la venta y realizar un nuevo análisis de rentabilidad con uso de un nuevo ASIC.

A los usuarios de bitc in: A las personas que ya hacen uso de las ventajas del bitc in, se les recomienda que contin en siendo beneficiarios de este servicio para sus diferentes necesidades y que esparzan la informaci n a otras personas (no usuarios) para que vean la realidad del mundo actual, pues es importante dar a conocer que la econom a y los precios de los bienes y servicios (inflaci n y tipo de cambio del d lar) se ven afectados por las decisiones de los gobiernos y los bancos centrales. Si todas las personas empiezan a darle importancia y a utilizar el bitc in, se podr  reforzar este movimiento y llegar a un estado econ mico mundial, no solo nacional, m s beneficioso para todos los usuarios y no basado en las entidades centrales y los gobiernos.

Bitmain: La empresa Bitmain de origen china es la que actualmente desarrolla lo que se considera en esta investigaci n como uno de los mejores ASIS de la industria y un servicio bastante eficiente y justo para participar en el servicio de la miner a de bitc in. Realmente no se puede influir en ella, pero se ha considerado al Antminer S9 como un aparato muy costoso. De hecho, despu s del an lisis de esta investigaci n se puede deducir que el precio que le asignan a esta unidad es tal que para las condiciones actuales de la miner a de bitc in, equivale a 12 meses de operaci n aproximadamente. Este beneficia principalmente a Bitmain como empresa y no a los usuarios. Por ende, se podr  pensar en este como un negocio dudoso. Si Bitmain vende los mismos Antminer S9, existir a la posibilidad de que ellos mismos implementen o puedan implementar enormes granjas de miner a de bitc in para minar y minar sin fin con sus propios ASIC y que la venta de los ASIC podr a representar una peque a fracci n de sus ganancias como empresa. Debido a lo anterior, se le recomendar a a Bitmain disminuir el precio del Antminer S9 para facilitar el proceso a los usuarios que deseen participar en la miner a del bitc in.

Al gobierno y el Banco Central de Costa Rica: Como se comentó en la entrevista realizada al economista Luis Loria, el uso de una moneda descentralizada y universal podría, eventualmente, contribuir a solucionar varios de los problemas relacionados con el uso del colón (o cualquier otra moneda centralizada) y las decisiones que toman los gobiernos y bancos centrales con respecto a la economía. Con el bitc in se podr an solventar problemas como la inflaci n, costos en las tasas de cambios a otras monedas (como el d lar) y mejorar para el usuario de la tasa activa de los bancos e intereses de los pr stamos.

Cualquier pago o cobro al exterior en una moneda extranjera se podr a realizar mucho m s sencillo utilizando bitc in y billeteras de bitcoins, tanto para usuarios individuales como para grandes empresas y el gobierno mismo; esto dejar a atr s las tasas de cambio y cobros por servicios de las transferencias bancarias internacionales.

Otra situaci n muy relevante para el pa s que puede mejorar considerablemente al incorporar el bitc in como moneda oficial, o como una de las dos monedas oficiales (el col n y el bitc in), ser a la mejora en el precio del combustible. Si bien es cierto, gran parte del alto precio de los combustibles existe debido a impuestos establecido a la gasolina por parte del gobierno. Otro factor del alza del combustible es el precio del d lar, dicha situaci n, con el bitc in, se podr a contrarrestar.

Por lo menos, la situaci n m s cercana que se puede ver como posible es que el gobierno cree leyes para autorizar el bitc in como una moneda reconocida y autorizada (como en el caso del d lar) para que muchas instituciones, empresas y bancos privados y p blicos acepten al bitc in como medio de pago. As , se ayudar a



mucho a los usuarios para que comenzaran a utilizar los beneficios del bitc33in como moneda.

## CAPÍTULO VI: PROPUESTA

## 6.1 Introducción

El presente capítulo constituye una propuesta de solución al problema tratado. Tras la investigación pertinente –descrita en todos los capítulos anteriores –se ha desarrollado una serie de entregables útiles para exponer a cualquier interesado un conjunto de planes o entregables que resumen una solución al conflicto expuesto, dicha información se resume en cómo realizar la minería de bitcoins y tener el servicio estable y funcionando adecuadamente.

## 6.2 Justificación

El bitc in (BTC) es la criptomoneda m s popular y utilizada en el mundo. Desde su nacimiento, en el a o 2009, hasta la fecha de elaboraci n de esta justificaci n de proyecto (julio de 2017), creci  su valor de \$0 a \$1943,45 por BTC. La miner a, explicada en la secci n 1.2.1, representa una actividad econ mica innovadora,  nica en el mundo de los servicios digitales y de internet, rentable bajo las condiciones apropiadas y que no requiere de mano de obra especializada para su operaci n diaria. En general, es un servicio que se puede dejar corriendo solo y  nicamente requiere ser instalado y configurado apropiadamente, as  como cierto nivel de supervisi n y mantenimiento para su correcta operaci n a largo plazo.

Algunas ventajas de la miner a del bitc in son:

- No requiere una inversi n muy elevada para iniciar y poner en funcionamiento la actividad econ mica. Tampoco requiere una alta y t cnicamente complicada configuraci n del equipo para la miner a de bitc in.

- Puede ser llevada a cabo en una casa, apartamento, bodega, local, etc. Se requiere que el espacio físico sea ventilado, tenga electricidad y buena conexión a internet (por lo menos 10 Mbps de bajada y 1 Mbps de subida).
- Si se localiza en una locación de clima frío, el *hardware* puede servir para calentar el espacio físico.
- El *hardware* puede ser vendido en caso de querer sustituirlo por un mejor o más moderno.
- No se requiere contratar personal adicional para la operación a largo plazo de la minería. Una persona puede ser capaz de administrar una cantidad específica de ASICs, incluyendo lo pronosticado en este trabajo de investigación, de 1 a 6 ASICs.

### 6.3 Entregables para la Propuesta del Proyecto

#### 6.3.1 Alcance del Proyecto

La gestión del alcance del proyecto se entiende como el diseño y desarrollo de los objetivos general y específicos del proyecto por parte del gerente del proyecto.

Objetivo general:

Plantear la creación de una empresa (ficticia) llamada Bitcoin CR con el propósito de desarrollar la minería de bitc oin como actividad rentable y empezar operaciones en un periodo no m as amplio de tres meses. Con el equipo necesario

(*software y hardware*) y las condiciones apropiadas (variables de la minería), poner en funcionamiento la minería de bitc in para finalmente obtener remuneraci n o recompensa por el servicio brindado. Cabe destacar que la minería conforma la infraestructura y legitimidad del bitc in como moneda, no un gobierno y un banco centralizado.

Objetivos espec ficos:

- Resumir la informaci n necesaria para sentar una base y fundamentaci n te rica acerca de la administraci n de empresas y gerencia de proyectos para la realizaci n de la actividad de la minería del bitc in.
- Explicar los conceptos b sicos y funcionamiento del bitc in como criptomoneda y de la minería del bitc in.
- Crear una billetera de bitc in para realizar transacciones de bitcoins (ingresos y egresos).
- Medir y analizar las variables que involucran la minería del bitc in y elegir el equipo de infraestructura tecnol gica (ASIC: *Application-specific integrated circuit*) necesario para operar de manera rentable.
- Calcular el tiempo que trascurriría operando para obtener el retorno de la inversi n inicial.

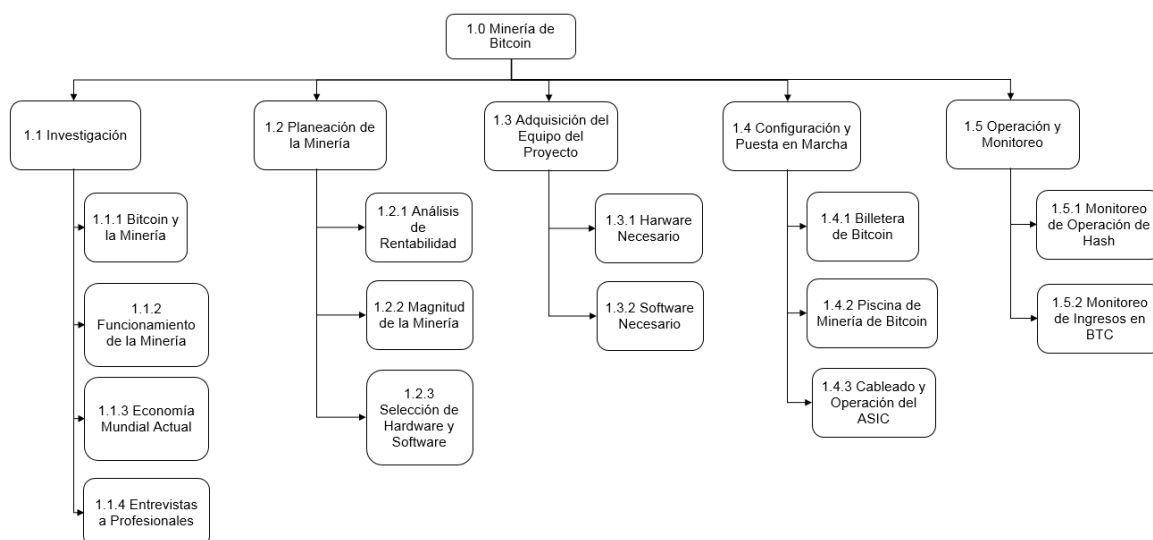
### 6.3.2 Estructura de Desglose de Trabajo (EDT)

Como parte del establecimiento del alcance y los objetivos del proyecto, se desarrolló una estructura de desglose de trabajo. El EDT es el proceso de determinar, documentar y gestionar las necesidades y los requisitos de los interesados para cumplir con los objetivos del proyecto. (Guía del PMBOK®, 2013, p. 105).

La figura N° 10 muestra la EDT descomponiendo jerárquicamente el alcance del proyecto por realizar con el equipo del proyecto. En este caso todo el trabajo queda a cargo del gerente del proyecto Bitcoin CR. Cada burbuja representa una tarea o un conjunto de tareas que generarán un entregable necesario para el avance del proyecto. Este EDT comprende 14 paquetes de trabajo

Figura N° 10 . Estructura de Desglose de Trabajo del Proyecto.

Fuente: Elaboración propia, 2017.



### 6.3.3 Lista de Interesados

Los interesados del proyecto son las personas o grupos de personas que podrían afectar o ser afectados por una decisión del proyecto. Su identificación es de suma importancia para conocer otros tipos de variables que pueden afectar el desempeño del proyecto, así como para tomar las mejores decisiones con la mayor cantidad de tiempo disponible antes de que surja un evento inesperado.

*Tabla N°4. Interesados del Proyecto.*

Rol	Descripción	Nombre/Título
Patrocinador del Proyecto	Coordinación de patrocinadores.	Ingeniero Ignacio Blanco Zamora
Gerente del Proyecto	Facilita los diseños necesarios para el Proyecto.	Ingeniero Ignacio Blanco Zamora
Proveedores de los ASICs/piscina de minería	Proveedores de equipo ASIC y del servicio de la piscina de minería.	Bitmain
Proveedor de la billetera de bitcoins	Desarrolladores del servicio de la billetera de <i>software</i> en donde se encuentran nuestras cuentas/billeteras.	Electrum
Proveedores de Electricidad e Internet	Facilita las relaciones con terceros hacia el proyecto.	CNFL/Telecable

Fuente: Elaboración propia, 2017.

Como se observa en la Tabla N° 4, el patrocinador del proyecto es la persona que brindará los recursos económicos para realizar el proyecto y también es el gerente o ejecutor del proyecto. Como se explicó durante el desarrollo del trabajo final, el trabajo necesario para realizar el servicio de minería con 6 ASICs no necesita más de una persona, esta situación reduce y simplifica la planeación y desarrollo del proyecto, así como también los riesgos del proyecto. El patrocinador y el gerente tienen como interés el alcanzar satisfactoriamente los objetivos del proyecto.

Otros interesados, como la compañía Bitmain y los proveedores de electricidad e internet, son considerados interesados porque sus servicios forman parte de la cadena de trabajo para operar la minería de bitc in. Adem as, son participantes externos en la compa a y sus aportes tambi en son fundamentales para el  xito del proyecto. El inter s de Bitmain es que le compren equipos ASIC y que mineros se unan a su servicio de piscina de miner a. Por su parte, los proveedores de electricidad e internet tienen como objetivo que personas obtengan y paguen por sus servicios de electricidad e internet.



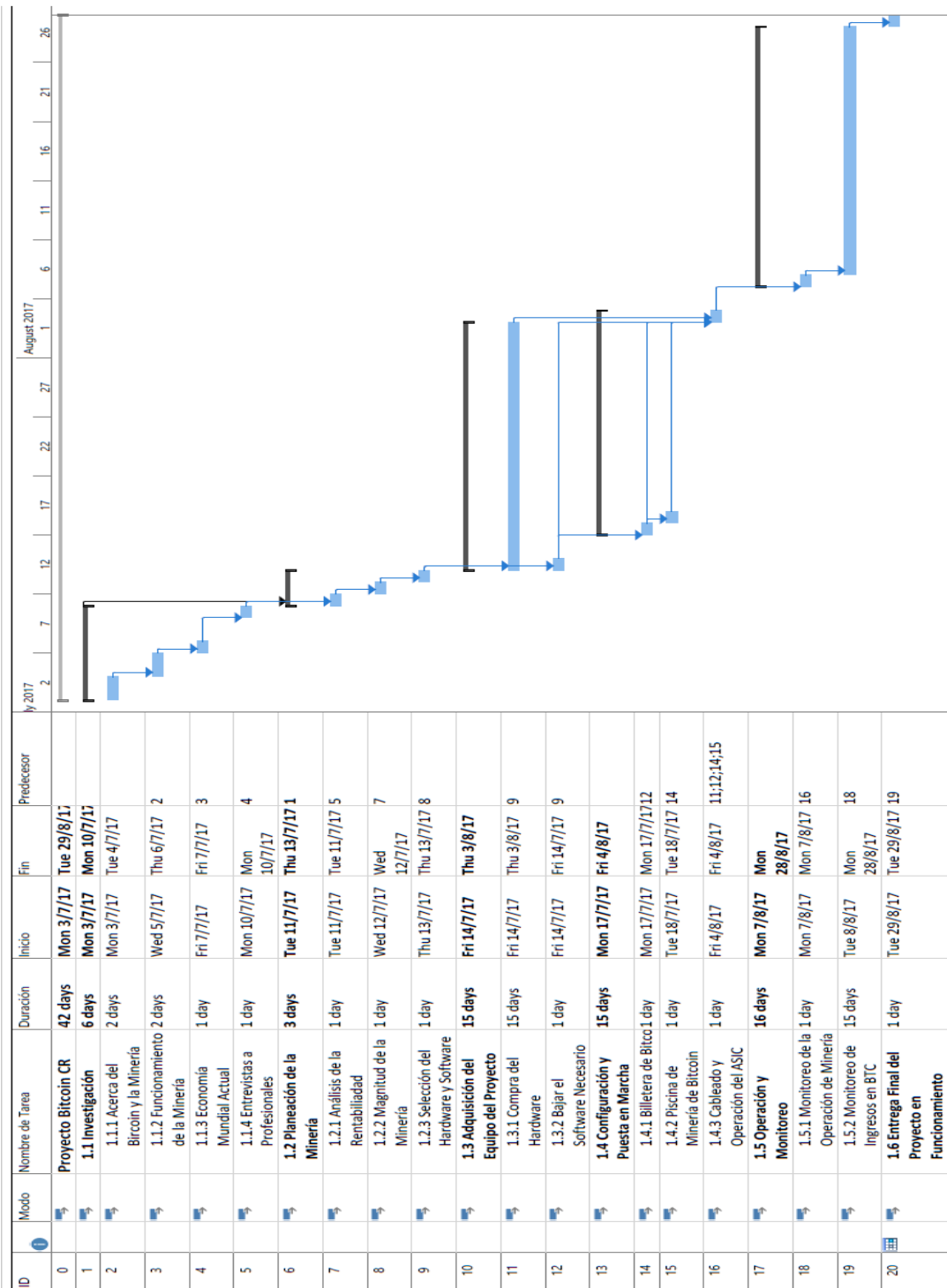
#### 6.3.4 Cronograma

Una de las herramientas más útiles de la gestión del tiempo del proyecto es el cronograma del proyecto. Se utilizaron entradas del alcance del proyecto como los objetivos del proyecto y los entregables identificados en la estructura de desglose del trabajo (EDT) para definir las actividades, estimar duración y gestionar el cronograma. Dicho cronograma del proyecto se puede observar en la figura N° 11.

El documento descrito contiene la lista de actividades por realizar en el lado izquierdo, las cuales se deben cumplir en su totalidad para poder alcanzar los objetivos específicos del proyecto. A su derecha, se despliega un diagrama de barras para cada una de las actividades de la lista, lo cual representa de manera gráfica las dependencias o predecesores y la duración de cada una de ellas.

Figura N° 11. Cronograma del proyecto.

Fuente: Elaboración propia, 2017.



### 6.3.5 Análisis de Factibilidad

El análisis de factibilidad es una herramienta que funciona para demostrar matemáticamente lo que debe resultar de los ingresos menos los costes del proyecto. Las siguientes tablas muestran la operación del proyecto entregado durante el primer y segundo año de trabajo.

*Tabla N°6. Análisis de rentabilidad para el primer año.*

Acción	Tipo de Acción	Descripción	Costos del primer año (- significa ingresos)
6 AntMiner S9	Costo	Costo de 6 AntMiner S9 para realizar la minería de bitc�oin para operar 1 a�o.	\$13.794,00
Costo de la Electricidad	Costo	Costo del consumo el�ctrico de 6 AntMiner S9 por 12 meses.	\$17.029,44
Fuente de poder AntMiner (APW3++ 1200W @110v 1600W @220v w/ 10 Connectors)	Costo	Costo de 6 fuentes de poder para los 6 AntMiner S9.	\$2.039,28
Switch de red Gigabit Linksys de 8 puertos (LGS108)	Costo	Switch de red no administrado para la red de los mineros.	\$36,14
Conexi�n a Internet	Costo	Costo anual por el servicio de internet de 10 Mbps de bajada de Telecable.	\$600,00
Ganancias de la miner�a	Ahorro	Ganancias anuales de la miner�a con 6 AntMiners S9 seg�n la tabla N� 3.	-\$32.452,37
Tarifa de AntPool	Costo	Con el avance de la tecnolog�a para la publicidad en plataformas de internet como las redes sociales, se reduce significativamente el costo de esta.	\$486,79
<b>Total del primero a�o</b>			<b>\$1.533,28</b>

Fuente: Elaboraci n propia, 2017.

**Tabla N°7. Análisis de rentabilidad para el segundo año.**

Acción	Tipo de Acción	Descripción	Costos del segundo año (- significa ingresos)
Deuda	Costo	Deuda de la operación del primer año.	\$1.533,28
6 AntMiner S9	Costo	Costo de 6 AntMiner S9 para realizar la minería de bitc�oin con el fin de operar 1 a�o.	\$0,00
Costo de la Electricidad	Costo	Costo del consumo el�ctrico de 6 AntMiner S9 por 12 meses.	\$17.029,44
Fuente de poder AntMiner (APW3++ 1200W @110v 1600W @220v w/ 10 Connectors)	Costo	Costo de 6 fuentes de poder para los 6 AntMiner S9.	\$0,00
Switch de red Gigabit Linksys de 8 puertos (LGS108)	Costo	Switch de red no administrado para la red de los mineros.	\$0,00
Conexi�n a Internet	Costo	Costo anual por el servicio de internet de 10 Mbps de bajada de Telecom.	\$600,00
Ganancias de la miner�a	Ahorro	Ganancias anuales de la miner�a con 6 AntMiners S9 seg�n la tabla N� 3.	-\$32.452,37
Tarifa de AntPool	Costo	Con el avance de la tecnolog�a para la publicidad en plataformas de internet como las redes sociales, se reduce significativamente el costo de esta.	\$486,79
<b>Total del primero a�o</b>			<b>\$13.289,65</b>

Fuente: Elaboraci n propia, 2017.

Se puede notar que, en el primer a o de operaci n, los ingresos no cubren todos los costes realizados para poner el proyecto en marcha, pero en la Tabla N 7 se arrastra la deuda del a o anterior y no es necesario incurrir en gastos de equipo, como fue necesario en el primer periodo. Por eso es que se incurre en gasto de \$0 para las l neas de AntMiner, Switch y fuentes de poder en el segundo a o. Al finalizar el segundo a o, se pronostica una ganancia de \$13.289,65. Cabe resaltar que estos c lculos fueron realizados con unos valores constantes de la Figura No 9., la Calculadora de Miner a para seis Antminer S9 al 13 de agosto de 2017 y la Tabla N 3: Resultados de la Calculadora de Miner a para seis Antminer S9 al 13 de

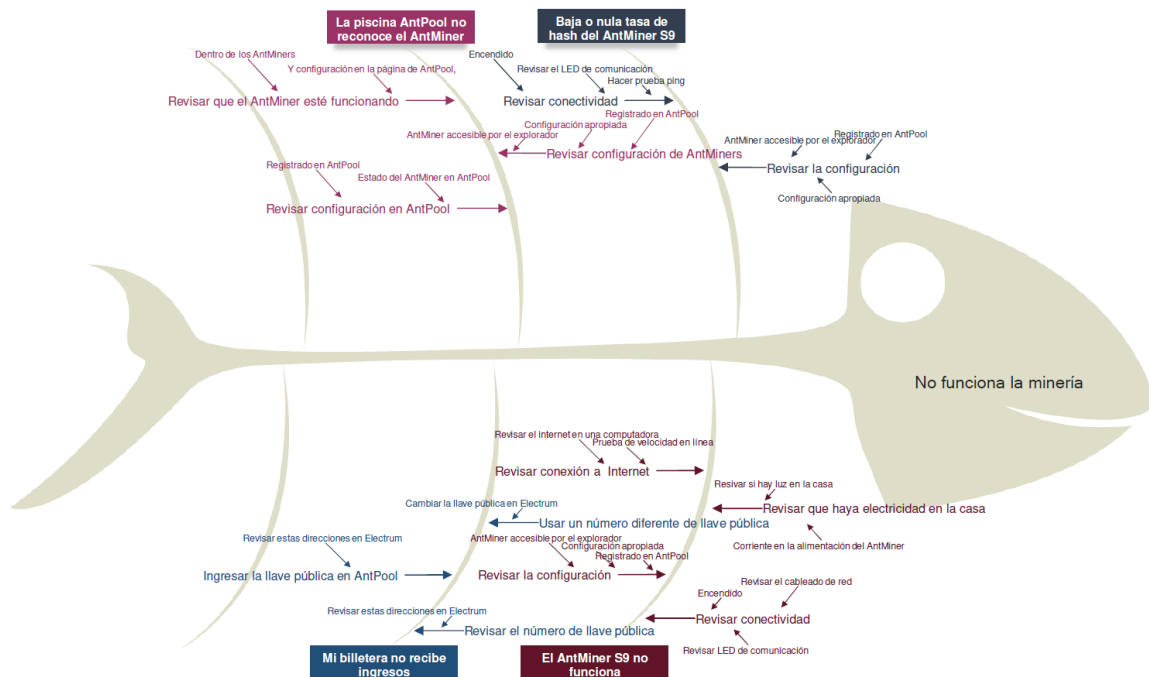
agosto de 2017. Como se explicó durante el desarrollo del trabajo, el precio del bitcóin cambia todos los días para bien o para mal de los diferentes interesados. Sin embargo, los resultados presentados se consideran válidos.

### 6.3.6 Diagrama de Causa y Efecto

El diagrama de causa y efecto ayuda a determinar la posible causa y solución a algún problema durante la ejecución y operación del proyecto, esto tiene importancia para no perder ingresos en el transcurso del tiempo durante la operación de la minería de bitcóin.

Figura N° 12. Diagrama de causa y efecto.

Fuente: Elaboración propia, 2017.



Bibliografía: Citada y Consultada

Bibliografía Citada

Project Management Institute (2013). *Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®)*. Quinta edición. Ciudad: Global Standard.

Nicolas de Zubiría Gómez (1998). *Consecuencias del Euro*. Recuperado de:  
<http://www.eltiempo.com/archivo/documento/MAM-738729>

Hernández, Fernández y Baptista (2014). *Metodología de la Investigación*. Sexta Edición. Ciudad: McGraw Hill.

## Bibliografía Consultada

Project Management Institute (2013). *Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®)*. Quinta edición. Ciudad: Global Standard.

Block Explorer (2017). *Título en cursiva*. Recuperado de: <https://blockexplorer.com/block/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>

Blockchain.org, (2017). *Average USD Market Price Across Major Bitcoin Exchanges*. Recuperado de: <https://blockchain.info/charts/market-price?timespan=all>

Lazlo (2010). *Pizza for Bitcoins? Forum*. Recuperado de: <https://bitcointalk.org/index.php?topic=137.0>

DPA (2014). *Vietnam bans Bitcoin. The Hindu*. Recuperado de: <http://www.thehindu.com/business/vietnam-bans-bitcoin/article5736019.ece>

Quora (2013). *Is it possible to make fake Bitcoins?* Recuperado de: <https://www.quora.com/Is-it-possible-to-make-fake-bitcoins>

Grupo ICE (2017). *Tarifas actuales del servicio eléctrico en Costa Rica*. Recuperado de: <http://www.grupoice.com/wps/portal/ICE/electricidad/servicios-residenciales/Tarifas+Actuales>

Banco Nacional de Costa Rica. *Tipo de cambio del dólar*. Recuperado de: <https://www.bncr.fi.cr/BNCR/TipoCambio.aspx>

Universidad Carlos III de Madrid (2011). *Tablas Hash*. Recuperado de: [http://www.it.uc3m.es/abel/as/MMC/M2/HashTable\\_es.html](http://www.it.uc3m.es/abel/as/MMC/M2/HashTable_es.html)

## Glosario

**Bitc3in:** Medio de intercambio de bienes y servicios. Funciona como una moneda digital, llamada criptomoneda de nivel mundial. El bitc3in utiliza la tecnolog3a peer-to-peer para funcionar sin autoridad central ni bancos.

**Peer-to-peer:** Denotando o relacionado con redes inform3ticas en las que cada computadora puede actuar como servidor para los dem3s, esto permite el acceso compartido a ficheros y perif3ricos sin necesidad de un servidor central.

**Criptomoneda:** Una criptomoneda o criptodivisa es un medio digital de intercambio. La primera criptomoneda que empez3 a operar fue bitc3in en 2009, y desde entonces han aparecido muchas otras, con diferentes caracter3sticas y protocolos, como Litecoin, Ethereum, Ripple, Dogecoin.

**Criptograf3a:** La criptograf3a (del griego κρυπτος (criptos), "oculto", y γραφη (graf3), "grafo" o "escritura", literalmente "escritura oculta") se define como el 3mbito de la criptolog3a que se dedica a las t3cnicas de cifrado o codificaci3n destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

**ASIC:** Circuito integrado espec3fico para una aplicaci3n (ASIC) es un circuito integrado (IC) personalizado para un uso particular, en lugar de ser destinado para uso general o m³ltiples aplicaciones.

**Funci3n Hash:** Cualquier funci3n que se puede utilizar para asignar datos de tamaño arbitrario a datos de tamaño fijo. Los valores devueltos por una funci3n *hash* se denominan valores *hash*, c3digos *hash*, digest, o simplemente *hashes*.

**Funci3n de Hash Criptogr3fica:** Una funci3n de *hash* criptogr3fica es una clase especial de funci3n *hash* que tiene ciertas propiedades que lo hacen adecuado para su uso en criptograf3a. Es un algoritmo matem3tico que mapea datos de tamaño arbitrario a una cadena de bits de un tamaño fijo (una funci3n *hash*) que est3 diseñada para ser tambi3n una funci3n unidireccional, es decir, una funci3n que es inviable invertir.

**AntMiner:** Familia de modelos de mineros ASIC de la empresa Bitmain.

**AntPool:** Servicio de piscina de mineros de la empresa Bitmain.



# ANEXOS

## ANEXO #1 El Bloque Génesis o el primer bloque de una transacción de bitc in en el mundo.

### Block #0

BlockHash 00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

### Summary

Number Of Transactions	1
Height	0 (Mainchain)
Block Reward	50 BTC
Timestamp	Jan 3, 2009 12:15:05 PM
Mined by	()
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Difficulty	1
Bits	1d00ffff
Size (bytes)	285
Version	1
Nonce	2083236893
Next Block	1 (block/00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb5048)

### Transactions

Loading Transactions...

ANEXO #2 Bitcoin: A Peer-to-Peer Electronic  
Cash System (Bitc3in: Un Sistema Electr3nico de  
Dinero Punto-a-Punto).



Adobe Acrobat  
Document

**ANEXO #3 TARIFAS DEL ICE. ALCANCE 152 III  
TRIMESTRE 2017.**



Adobe Acrobat  
Document