UNIVERSIDAD TORCUATO DI TELLA

Escuela de Negocios

MBA 2020

La Criptominería como modelo de negocio

¿La fiebre del oro digital puede cambiar nuestra economía social?

Autor: Raúl Guillermo Boccardo

Tutor: Javier Epstein

Lugar: Buenos Aires, Argentina

Año: Julio 2022

Agradecimientos

"No es la especie más fuerte la que sobrevive, ni la más inteligente, sino la que responde mejor al cambio", Charles Darwin.

Realizar este trabajo me hizo reflexionar sobre la evolución de nuestra especie, enfrentándose a grandes desafíos durante toda su historia. Hoy soy consciente que me tocó vivir en una época en donde se están gestando grandes cambios de paradigma, que sin duda seguirán moldeando nuestra concepción de la realidad.

Mis agradecimientos son para nuestra especie, que no deja de sorprender, crear y construir futuro en base a los conocimientos acumulados durante toda su existencia.

Resumen

Bitcoin es conocido como un activo digital, originado bajo un movimiento que defiende el uso generalizado de la criptografía y de las tecnologías que mejoran la privacidad como vía para el cambio social y político. A poco más de una década desde su creación, su uso y adopción se ha espiralizado en todos los estratos sociales, sin embargo, poco se sabe de la tecnología que hay detrás y de las nuevas posibilidades de negocio que se pueden crear con ella. La tecnología Blockchain nació para corregir las imperfecciones que posee la internet moderna. Entre sus principales atributos se destaca la seguridad, inmutabilidad, confiabilidad y descentralización. No existe un servidor central que ejerza gobernanza unánime sobre este ecosistema, por lo tanto, al ser un sistema descentralizado, la validación de sus operaciones se basa en protocolos de consenso distribuidos entre sus miembros. Los nodos validadores, aquellos que pasarían a reemplazar al servidor central de la internet moderna, se llaman mineros. Por cada bloque de información que se confirma en el sistema, estos validadores reciben una recompensa de la Blockchain llamados *tokens* o criptomonedas, en alusión a todo el trabajo criptográfico que las originan, llegándose a convertir en un modelo de negocio muy rentable en los días que vivimos. Sin embargo, estos mecanismos de validación tienen ciertas barreras de entradas y dependencia de variables altamente fluctuantes, haciéndonos preguntar ¿hasta cuándo seguirá siendo rentable este modelo de negocio?, y si el progreso de la tecnología, ¿permitirá su evolución o deceso?

La propuesta de este trabajo se basó en estudiar la minería de criptomonedas como modelo de negocio, orientado principalmente a proyectos que funcionen bajo protocolos de consenso *Proof of Work* o similares. En la misma se exponen los resultados obtenidos de un caso real de minería doméstica, repasando su alcance, rentabilidad y estrategias de diversificación de riesgo. Al finalizar el estudio se presentará una conclusión sobre las distintas alternativas que posee un inversor para abordar esta actividad y consideraciones importantes para determinar si es recomendable ingresar al negocio de la criptominería en estos momentos, principalmente en países emergentes dónde las criptomonedas están jugando un papel predominante como refugio de valor.

Palabras clave

Bitcoin - Blockchain - Token - Criptominería

Índice

Lista de tablas y figuras

Introducción

El presente trabajo tiene como objetivo general introducir al lector en la tecnología blockchain, permitiéndole, entender cómo se originó, identificar las nuevas oportunidades de negocio que aporta y analizar si es factible lograr un modelo de negocio rentable en países macroeconómicamente inestables como el nuestro.

Si bien la euforia por adquirir equipos de criptomonedas ha venido creciendo en estos últimos años, es importante entender, antes de desembarcar en cualquier inversión de criptominería, en que estadio se encuentra cada proyecto criptográfico, sea de bitcoin o alguna de las distintas *altcoins* existentes, para no caer en la trampa de querer incrementar nuestro capital de forma efímera en proyectos que se encuentren en su etapa final de desarrollo. Como objetivo específico, se profundizó en la criptominería como modelo de negocio buscando responder si es el momento adecuado para ingresar en esta actividad. Para ello, se analizaron los dos proyectos de minería más importantes bajo el protocolo *proof of work*, siendo estos Bitcoin y Ethereum. Se aportó un caso real de estudio de criptominería a una escala doméstica y se analizó cómo se comporta y ejecuta el negocio a través de un referente de nivel industrial. Para responder a esta pregunta también se estudiaron otros modelos de criptominería alternativas al PoW, como ser el PoS o la minería de criptomonedas como proveedores de servicios. Esto último permitiría al inversor diversificar el riesgo y generar ganancias adaptándose a las nuevas modalidades de negocio que presentasen las cadenas de bloques a futuro (3ra generación o superior), en caso de que el PoW quede sin uso por la propia evolución tecnológica.

La presente investigación responde a un estudio de tipo descriptivo con una metodología basada en una combinación de enfoque cuantitativo/cuantitativo. Aplicando razonamiento inductivo se llegó a una conclusión que permitió responder a la pregunta planteada como objetivo principal del proyecto. La técnica utilizada para la recolección de información se nutrió de fuentes de datos primarios, a través de observaciones directas, y de fuentes de datos secundarios, como análisis de contenido de entrevistas y datos públicos de mercado.

Los temas a desarrollar en este documento se dividen en nueve capítulos. Los primeros cinco contienen el desarrollo teórico de la investigación, explicando desde los fundamentos estructurales de la tecnología blockchain, pasando por los requerimientos necesarios para

iniciarse en la actividad de la criptominería como modelo de negocio, hasta un breve repaso histórico de su evolución a nivel mundial. Luego, se continua con los últimos cuatro capítulos donde se expone el trabajo de campo. Finalizando con una conclusión y una serie de recomendaciones sobre los resultados y desafíos identificados en la investigación.

Antes de comenzar con el marco teórico es importante hacer un poco de historia e identificar las raíces que originaron la creación de esta revolucionaria tecnología llamada blockchain.

El World Wide Web

Vivimos en un mundo globalizado, donde todo está conectado entre sí gracias a Internet. Esta tecnología fue adaptada para facilitar la comunicación y realizar transacciones de una forma rápida y barata, representando el mayor avance y desarrollo en el cambio de costumbres y modo de vida en los últimos tiempos. Sin embargo, aunque Internet ha permitido una mayor conectividad y revolucionar el sistema de comunicación del siglo XX, aún tiene algunos problemas. No se puede estar seguro de la entidad que se encuentra al otro lado de la red, poniendo en peligro lo más importante para un usuario, la confianza. Principalmente cuando proviene de transacciones monetarias. (Gralla, 2007)

A continuación, se detallarán los planteos fundamentales que se le hacen a la internet moderna que fueron causales de la búsqueda de un sistema más seguro y confiable, devenido hace algunos años en una tecnología llamada Blockchain:

Planteos estructurales y de seguridad

En sus inicios, el fundamento básico de Internet era que, independientemente de la función interna de un dispositivo, debería tener la capacidad de poder conectarse a la red. Sin embargo, como cualquier sistema imperfecto, también tiene sus propios problemas. Estos problemas pueden ser de orden psicológicos como *trolls* y memes, como también se puede ser víctima de estafas en línea - *online scams*. En esta última, los estafadores imitan a la autoridad para obtener acceso a las cuentas legítimas. Este tipo de ataque se llama *phishing* o suplantación de identidad. Si bien la medida preventiva de evitar ejecutar un archivo ".exe" desde internet es conocida por todos, aun así, la gente se deja engañar y, a menudo, compromete su sistema conduciéndolas a la situación de *ransomware* o secuestro de datos.

A parte de todos los asuntos mencionados anteriormente, el mayor problema con internet se basa en la confianza. La mayoría de los servicios de internet están basados en una

comunicación bidireccional cliente-server. Esto significa que proveedor del servicio se encuentra centralizado en un único servidor. Al igual que los clientes, al no estar seguros del servidor, los servidores tampoco están seguros de con quién están tratando. Por esta razón, un montón de nuevas técnicas se fueron creando para identificar correctamente a los clientes de aquellos perfiles falsos. Técnicas como:

- *Two-factor authentication*, una contraseña de un solo uso u *OTP (One-Time Password)*.
- Biométricos, para reconocer a una persona por alguna de sus características biométricas.
- *Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart)*, se trata de una simple prueba lógica para determinar cuándo el usuario es un humano o un programa automático (bot).

Los servidores también utilizan un *firewall o* cortafuegos para restringir el movimiento de la comunicación a los clientes maliciosos. Esto quiere decir que, si cualquier cliente malintencionado intenta comunicarse, el servidor simplemente lo ignora o, como su nombre indica, quema el mensaje. Las técnicas mencionadas hasta ahora se encargan únicamente de la identificación del cliente. La identificación del servidor se puede realizar mediante certificados de confianza colocados en él, pero no hay verificación para ello. Además, si un servidor es atacado por un pirata informático, toda la información del cliente está en juego.

Planteos sobre las bases de datos tradicionales

Todos los servicios a través de Internet tratan con datos. Actualmente, dentro del Big Data, se distinguen dos principales tipos de datos: datos estructurados y datos no estructurados (ver figura 1). Los datos estructurados se compilan en tablas compuestas por filas y columnas. Utilizan tablas de distintos archivos para eliminar la duplicación, permitiendo almacenarse de manera más conveniente y lógica. Debido a que cada fila y columna almacena una información distinta, resulta más fácil buscar cualquier información. Los datos estructurados están altamente organizados y formateados de tal manera que se pueden buscar fácilmente en bases de datos relacionales. El problema con los datos estructurados es que se necesita mucho esfuerzo para reunir los datos en ese formato, además de que los usuarios finales no les gusta buscar información en múltiples tablas.

Por otro lado, los datos no estructurados no tienen un patrón de orden establecido, lo que hace que sea mucho más difícil de recopilar, procesar y analizar. Pueden venir en texto, imágenes, sonido, vídeos u otros formatos, y su búsqueda y análisis es más difícil. Con este

tipo de datos, hay mucha incertidumbre. También es difícil almacenar este tipo de información en formato tabular. Al día de hoy se han desarrollado muchas técnicas modernas para realizar un seguimiento de toda esa información.

Figura 1: Tipos de datos

Fuente: Certia.net.

Planteos sobre el acceso a los datos y el rol del administrador

El método Cliente-Servidor, también conocido como acceso centralizado a los datos, es cuando todos los dispositivos acceden a un mismo servidor que reside en el centro de todas las bases de datos. Por lo cual, debe ser lo suficientemente potente como para poder atender todas las solicitudes de forma simultánea. Esto claramente hace que el servidor sea propenso a posibles ataques cibernéticos. Si el servidor deja de funcionar por cualquier motivo, todos los servicios se verán afectados. En tal escenario, el servidor se convierte en un cuello de botella para la continuidad de sus procesos. Una de las formas de limitar el daño a una base de datos es mediante la definición de roles de acceso. Este rol define las actividades permitidas para un usuario en particular. Esta decisión normalmente la toma un administrador del sistema según las reglas preestablecidas, determinando distintos grados de privilegios para cada usuario. Este tipo de método introduce una jerarquía y hace que el sistema sea menos transparente. Los que toman las decisiones están absolutamente aislados y todos los demás siguen sus reglas.

En contra partida a los principales planteos que derivan de la internet moderna, podemos enunciar las principales características de Blockchain que la perciben como una tecnología superadora. Blockchain es el tipo de base de datos donde no hay un servidor centralizado. Todos los participantes tienen acceso a los mismos datos, pero almacenados dentro de sus propios sistemas. Junto con esto, Blockchain trabaja sobre un consenso común entre todos sus participantes, evitando, así, la investidura del poder dentro de una sola entidad. A continuación, se explicará cómo Blockchain supera los problemas mencionados

anteriormente. Ya sean los problemas de confianza en internet o los problemas relacionados con las bases de datos. El siguiente tema comenzará con los conceptos básicos de Blockchain y se retomará desde allí.

El nuevo orden que ofrece Blockchain

En 2008, un seudónimo misterioso llamado Satoshi Nakamoto presentó la idea de una red *Peer-to-Peer* (red de pares o red entre iguales). Idea que ilumino a Satoshi después de ver desbarrancarse el sistema financiero mundial con la crisis subprime del 2008[1]. En el abstracto de dicho trabajo se presentaba lo siguiente (Nakamoto, 2008).

> ***"Abstracto**. Una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera. Firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si existe un tercero confiable para prevenir el doble-gasto. Proponemos una solución al problema del doble gasto utilizando una red usuario-a-usuario. La red coloca estampas de tiempo a las transacciones al crear un hash de las mismas en una cadena continua de pruebas de trabajo basadas en hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo. La cadena más larga no solo sirve como la prueba de la secuencia de los eventos testificados, sino como prueba de que vino del gremio de poder de procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de los nodos que no cooperan para atacar la red, estos generarán la cadena más larga y le llevarán la ventaja a los atacantes.*
>
> *La red en sí misma requiere una estructura mínima. Los mensajes son enviados bajo la base de mejor esfuerzo, y los nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia."*

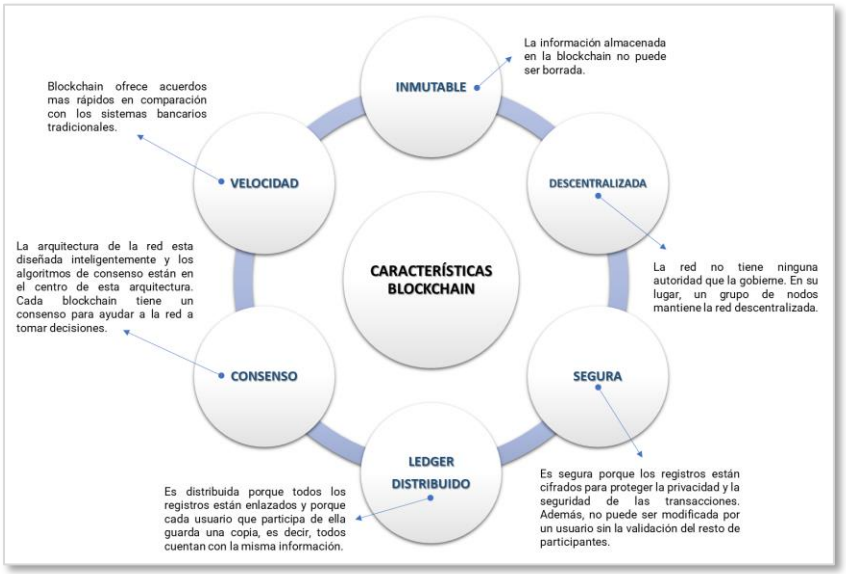
No era como si el mundo nunca hubiera oído hablar de un fenómeno de este tipo antes, pero el periódico informaba de que el dinero podía fluir por la red sin una sola jurisdicción. Antes de que la gente pudiera entender el concepto en detalle, Bitcoin hizo su primera aparición en enero de 2009. Desde entonces, se ha visto un aumento en la cantidad de transacciones que

[1] (Alizart, 2020)

se han realizado con este criptoactivo[2]. Bitcoin se ocupa específicamente de transacciones monetarias, pero la tecnología en la que se encuentra toda la red *peer-to-peer* es un dominio aún más fascinante y confuso. Blockchain es algo muy nuevo y, por lo tanto, todos tienen sus propias opiniones al respecto. En sus comienzos los escépticos la consideraban simplemente una moda pasajera, sin embargo, hoy podemos decir, dada a la rápida adopción que tuvo en estos últimos años, que está ampliamente considerada como el futuro de internet. Cualquiera que sea el resultado, es importante conocer la tecnología que sacudió los fundamentos del sistema bancario (Ammous, 2018).

La tecnología Blockchain llego para corregir las imperfecciones que posee la internet moderna. Entre sus principales atributos se destaca la seguridad, inmutabilidad, confiabilidad y descentralización. No existe un servidor central que ejerza gobernanza unánime sobre este ecosistema, por lo tanto, al ser un sistema descentralizado, la validación de sus operaciones se basa en un protocolo de consenso distribuido entre sus miembros. Para mantener este sistema, existen diversos mecanismos de validación, todos tienen por finalidad procesar algoritmos que permitan validar operaciones y escribir bloques de información dentro de la Blockchain. En la figura 2 se resaltan las principales características mencionadas.

Figura 2: Características claves de la tecnología blockchain



Fuente: elaboración propia.

[2] Un criptoactivo es un tipo de activo virtual, el cual tiene su origen en la criptografía. Los diferentes criptoactivos poseen un determinado valor de mercado, el cual permite al poseedor, generar ingresos al venderlos o al intercambiarlos por bienes y servicios.

Si bien el presente trabajo da por asumido el funcionamiento general de blockchain, cabe destacar que sus principales características de descentralización, inmutabilidad y transparencia decantan en el valor intangible tan anhelado por los usuarios, y que la internet moderna siempre puso en duda, la confianza, ofreciendo una nueva propuesta de valor para el desarrollo de nuevos modelos de negocios. Para entender el funcionamiento técnico y sus fundamentos criptográficos se adjunta el *Whitepaper* original publicado por Satoshi Nakamoto en 2008 (ver Anexo I: Bitcoin P2P e-cash paper).

Diferentes usos de blockchain

Hasta ahora solo se ha explicado sobre Blockchain con respecto a las transacciones financieras. Dado que estas transacciones son bastante riesgosas, tiene sentido tener una red segura como Bitcoin para protegerlas. Pero también es válido imaginar otros escenarios en los que se pueda utilizar una Blockchain. La creación de contenido digital es bastante fácil hoy en día, desde las melodías de un músico hasta las palabras de un escritor, todo se almacena digitalmente. Pero con esta facilidad de acceso surge el problema de la propiedad. Cualquiera que tenga una copia digital de una obra real puede afirmar que es de su propia autoría. La mayor parte del trabajo digital creado se publica en internet, cualquiera puede descargarlo y reclamarlo como su propio trabajo. Aquí es donde surge el problema de los derechos de autor. Tal problema se puede resolver con blockchain, ya que una vez que los datos se registran en ella, es casi imposible editarlos. Así es como se puede mantener un registro histórico de cada elemento en internet.

Otro escenario en el que se puede implementar una blockchain es en el ámbito gubernamental. El alto nivel de burocracia por parte de las instituciones tiende a retrasar el trabajo. Además, existe una falta de confianza cuando se trata de situaciones de este tipo, razón por la cual que se requiere una autoridad central. Incluso en tales situaciones, la cronología y los registros históricos juegan un papel importante. Un caso representativo de esto ocurre en la compra de un terreno. Para registrarlo a nombre de alguien se debe crear una gran cantidad de libros de contabilidad y registros. Con Blockchain, la idea principal no es digitalizar y crear solo una base de datos, sino que la solución debe garantizar que dos partes puedan llegar a un acuerdo sin que un solo organismo valide el trato (aquí se expone otra característica fundamental de blockchain: quita de la intermediación).

Futuro de la innovación de blockchain

La realidad en la cual vivimos se basa en un mundo gobernado por un tercero. Desde nuestras redes sociales, servicios de comunicación, hasta las películas que vemos, todo se rige por algún intermediario. Blockchain como tecnología está tratando de eliminar este negocio de los intermediarios. Un elemento fundamental que lo ayuda a hacerlo son los Contratos Inteligentes o *Smart Contracts*. Idealmente, los contratos inteligentes no deberían verse como algo que viene solo con blockchain, pero su reconocimiento se debe a su implementación temprana a través de esta tecnología. Los contratos inteligentes no son más que un contrato autoejecutable, es como un contrato físico, donde habrá múltiples participantes, cláusulas y consecuencias, convertido en un código informático que se pueda ejecutar cuando se cumplan determinadas condiciones. Los contratos inteligentes, al estar codificados, se almacenan en una red blockchain, por tanto, son inmutables y distribuidos. Esto significa que la satisfacción de una condición depende del consenso de la mayoría de los participantes.

Ethereum es una plataforma open source al igual que bitcoin. Pero la distinción que trae esta plataforma es la posibilidad de crear contratos inteligentes de forma totalmente descentralizada, a diferencia de otras cadenas de bloques. Es programable, lo que significa que los desarrolladores pueden usarlo para crear nuevos tipos de aplicaciones descentralizadas. Dado que este contrato inteligente se ejecuta en la red de ethereum, se deberá pagar un pequeño cargo para ejecutar todo el contrato. Esto es insignificante en comparación con el valor real del trato. (Russo, 2020)

Los desafíos para la adopción de blockchain

En línea con el concepto de la internet moderna podemos decir que blockchain también es una tecnología fascinante, pero cada buen producto también tiene su propio conjunto de desafíos. A continuación, se detallarán los planteos que debe resolver la tecnología blockchain (Binance Academy, 2018):

Planteos intrínsecos

Estos planteos derivan de un concepto llamado “El trilema de la cadena de bloques” (ver figura 3), concepto acuñado por Vitalik Buterin (CEO Ethereum) que propone un conjunto de tres problemas principales (descentralización, seguridad y escalabilidad) que los desarrolladores encuentran al crear cadenas de bloques, obligándolos a sacrificar un "aspecto" como compensación para adaptarse a la otros dos. Es una creencia generalizada que las redes descentralizadas solo pueden proporcionar dos de tres beneficios en un

momento dado en relación con la descentralización, la seguridad y la escalabilidad. A continuación, se detallará cada problema por separado:

- Problemas de descentralización: esto está relacionado con la arquitectura de esta tecnología en sí. Blockchain es una red *peer-to-peer*, esto significa que cada nodo tiene la copia del registro completo de transacciones hasta la fecha. Entonces, una sola adición o modificación en la base de datos genera un efecto dominó en toda la red. Debido a esto, el tiempo necesario para completar una transacción aumenta considerablemente. Por supuesto, la red funciona con rapidez, pero lo que requiere tiempo es la validación de una transacción. A menos que los mineros[3] puedan agregar un bloque a la cadena existente, un participante no está seguro del resultado. Además de este problema, el escenario donde se crean múltiples cadenas o *forks*[4], encontrar la cadena correcta para continuar implica algo más de tiempo en la finalización de una transacción.
- Problemas de seguridad: a pesar de que blockchain crea un entorno a prueba de piratería, al igual que cualquier otra tecnología, una clave privada siempre está en peligro de ser robada. Si esta clave se ve comprometida, es poco lo que blockchain pueda hacer para protegerse. Debido a esto, se puede procesar un gran número de transacciones sin el consentimiento real del usuario. Las características fundadoras de blockchain son el anonimato y la realización de transacciones irreversibles. Ambas características son opuestas al sistema tradicional con el que todos han crecido.
- Problemas de escalabilidad: dentro de blockchain pueden existir una infinidad de aplicaciones que se centran en un solo objetivo o más. Pero para escalar la adopción de blockchain, se requiere que las diferentes cadenas, que están completamente separadas en términos de registros poseídos, puedan comunicarse.

[3] Los ***mineros*** son agentes que se encargan de validar y agrupar las transacciones hechas por los usuarios dentro de la red determinada, en bloques que posteriormente serán unidos a la cadena de bloques conocida como Blockchain.

[4] Un ***fork*** (bifurcación, escisión) es un cambio en el protocolo o una divergencia de la versión anterior de Blockchain. Cuando un minero genera un bloque alternativo con fines fraudulentos, el sistema consensua la invalidez del bloque, de manera que el resto de mineros abandona éste "bloque huérfano" rápidamente.

Figura 3: Trilema de blockchain

Fuente: Criptotario.com.

Planteos extrínsecos

- Problemas de diseño: blockchain requiere una codificación compleja. Además, es importante conocer primero la parte conceptual para comenzar incluso con la codificación.
- Problemas de confianza: blockchain cambia la forma tradicional de hacer negocios. A veces, en lugar de esperar que esto sea un nuevo cambio, la gente lo toma más como un shock. La ausencia de terceros o intermediarios genera dudas entre los participantes. Además, la posibilidad de que un sistema se gobierne solo, aumenta el nivel de ansiedad de los participantes. Un problema mayor que este, reside en el nivel de conciencia de las masas. Muy pocas personas entienden cómo funciona blockchain, pero incluso menos que eso comprenden el verdadero potencial de la tecnología.
- Problemas regulatorios: se refiere a como la adopción institucional se verá directamente afectada por esta tecnología. Va a ser más difícil para entidades bancarias y gobiernos aceptar tal tecnología. Además de esto, con una arquitectura autónoma donde ningún nodo es superior a otro, surge la falta de propiedad. Esto requiere la creación de leyes y regulaciones más disruptivas.

Por supuesto, todos los problemas anteriores tienen algunas soluciones alternativas. Blockchain es una tecnología bastante nueva, seguirá evolucionando y, por lo tanto, surgirán nuevas inquietudes con el paso del tiempo.

Marco teórico

Capítulo 1. Conceptos técnicos de Blockchain

Se han mostrado los fundamentos de blockchain, su origen y necesidad. También se ha especificado los distintos usos que se le puede dar a esta tecnología y los desafíos que presenta a futuro. Si bien la blockchain ha abierto un sinfín de posibilidades para crear compañías y modelos de negocios que resuelvan problemas con esta tecnología, en el presente trabajo se analizará el rol del validador o minero como actor principal en el sostenimiento de estas nuevas redes de información. Minar criptomonedas no es una tarea compleja, pero requiere de un conocimiento básico del funcionamiento de blockchain para entender en donde se está embarcando. En el presente capítulo se comenzará explicando los conceptos claves para entender su funcionamiento técnico e introducirse posteriormente en la criptominería como modelo de negocio (Binance Academy, 2019).

Conceptos principales:

- ***Estructura del bloque***

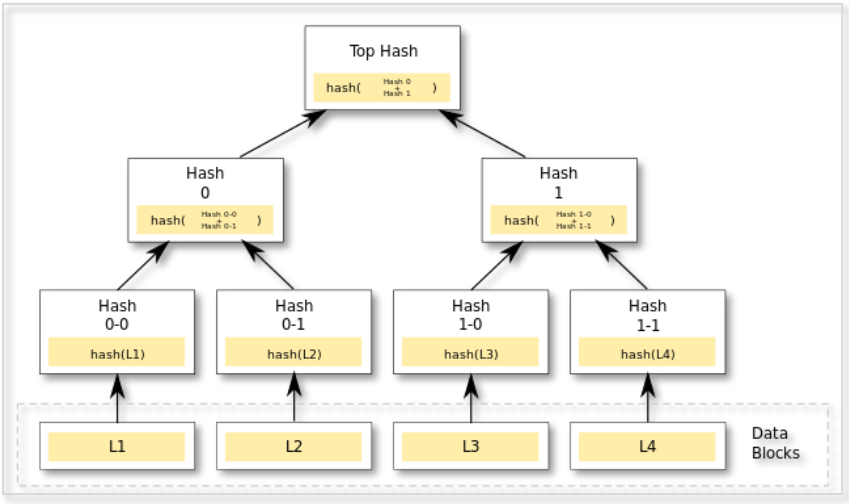
Una blockchain es un tipo de base de datos especial o también llamada tecnología de registros distribuidos *(distributed ledger technology o DLT)* que presenta ciertas propiedades únicas. Existen reglas que determinan cómo deben ser añadidos los datos, y una vez éstos han sido almacenados, resulta virtualmente imposible modificarlos o eliminarlos. Los datos se añaden a lo largo del tiempo en estructuras denominadas bloques. Cada bloque se construye encima del anterior e incluye una porción de información que lo vincula a éste. Fijándonos en el bloque más reciente, podemos comprobar que ha sido creado después del anterior. Así que, si seguimos descendiendo por la "cadena", llegaremos hasta nuestro primer bloque, conocido como bloque génesis.

Como su nombre lo indica, una blockchain, se encuentra representada por una cadena de bloques, los cuales, a su vez, vendrían a representar cada uno, uno conjunto de información encriptado entrelazados entre sí (ver figura 4). Un bloque se encuentra identificado por su función *hash*[5] y compuesto por la información de sus transacciones, estructurada a través de

[5] Una función criptográfica hash - usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

un árbol Merkel[6]. Si una función *hash* cambia su input altera radicalmente su resultado, esto es útil porque si alguien intenta alterar la información de un bloque, su *hash* cambiará por completo. Pero no solo eso, el diseño de este registro incluye algo muy especial. El contenido del bloque que un validador construye no solo incluye los datos de la transacción y el número de verificación, sino que incluye además cual fuel el *hash* del último bloque aceptado, es decir, se están encadenando cada bloque con el anterior, creando así una cadena de bloques. Por lo tanto, la blockchain representa una cadena de bloques encadenados unos con otros por su *hash* y, por el propio diseño de la red, se representa como inmutable, dado que, si alguien quiere manipular la información de una cadena, deberá cargar con el *hash* del bloque y todos sus posteriores. Para lograrlo se requerirá una potencia de cálculo acumulada mayor al del 51% de los participantes de la red. De esta forma la seguridad e inmutabilidad de la cadena se garantiza a través de algoritmos de criptografía, matemática e informática.

Figura 4: Estructura de una cadena de bloques



Fuente: Criptonoticias.com.

- ***Algoritmos de consenso***

Un algoritmo de consenso es un mecanismo que permite a los usuarios o máquinas coordinarse en un entorno distribuido. Debe garantizar que todos los agentes del sistema puedan ponerse de acuerdo respecto a una fuente única de verdad, incluso en el caso de que

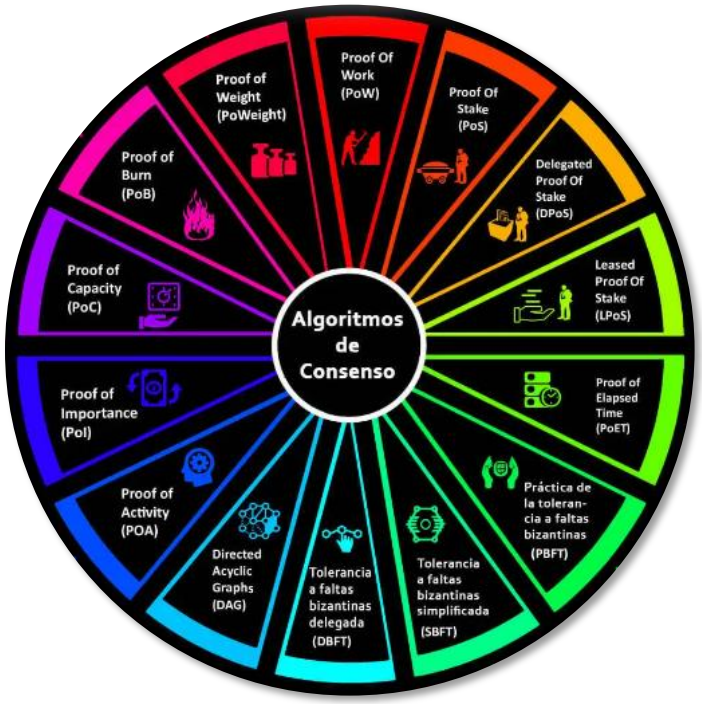
[6] Un árbol hash de Merkle o árbol de Merkle o árbol hash es una estructura de datos en árbol, binario o no, en el que cada nodo que no es una hoja está etiquetado con el hash de la concatenación de las etiquetas o valores de sus nodos hijo. Son una generalización de las listas hash y las cadenas hash.

algunos de ellos fallen. En otras palabras, el sistema debe ser tolerante a faltas (ver "problema de los generales bizantinos")[7].

En un esquema centralizado, una entidad única tiene poder sobre todo el sistema. En la mayoría de casos, podrá realizar los cambios que quiera. Pero en un esquema descentralizado, ponerse de acuerdo respecto a qué entradas añadir resulta más complejo. Superar dicho desafío en un entorno en el que extraños no confían entre sí fue, quizás, el desarrollo más importante que allanó el camino a las blockchains.

El algoritmo de consenso está relacionado con el acuerdo entre todos los usuarios o miembros de una red de criptomonedas en cuanto a su funcionamiento, qué transacciones cumplen con los criterios de validez, el orden de los bloques en la cadena, etc. Cabe destacar que existen una amplia variedad de algoritmos de consenso como se expone en la siguiente figura.

Figura 5: Tipos de algoritmos de consenso



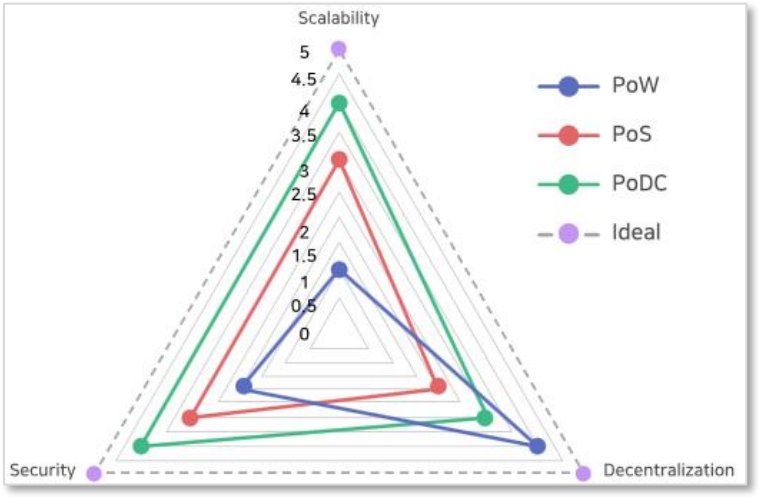
Fuente: 101blockchains.com.

Si bien los distintos tipos de algoritmos de consenso tienen la misma finalidad, la eficacia en resolver el trilema de blockchain difiere en sus resultados. Por lo tanto, la elección final de cuál de ellos aplicar en una cadena blockchain, dependerá del problema se priorice resolver

[7] El informático estadounidense Robert Shostak planteó el "problema de los generales bizantinos" a finales de la década de 1970.

sobre el resto. Para que se entienda mejor, en la siguiente figura se expone un ejemplo simplificado de los efectos que se pueden alcanzar sobre las distintas aristas del trilema utilizando diferentes algoritmos de consenso. Como se puede observar, al utilizar los algoritmos PoS o DPoS se permite mejorar los problemas de escalabilidad y de seguridad, considerando las debilidades de PoW, pero en contrapartida se debe resignar descentralización.

Figura 6: Comparación de soluciones al Trilema de blockchain



Fuente: ReapChain.

En el presente trabajo solo se hará foco en los dos tipos de algoritmos de consenso más populares entre las redes de criptomonedas: la prueba de trabajo (PoW) y la prueba de participación (PoS). Los mismos se explicarán en el siguiente capítulo con más detalle.

Resumen

Como se ha visto, la tecnología blockchain no es más que un mecanismo matemático, criptográfico e informático de consenso para registrar bases de datos de forma distribuida. Habiendo entendido los principales conceptos técnicos que representan y componen a la tecnología blockchain, se estaría en condiciones de poder iniciarse como un nodo validador y empezar a minar las recompensas.

Capítulo 2. Los protocolos de consenso más utilizados

Para iniciarse como nodo validador primero será importante elegir sobre cual cadena y mediante que mecanismo de consenso efectuar trabajo. Es por eso que en el presente capítulo se explicara en forma detallada el *Proof of Work (PoW)* y el *Proof of Stake (PoS)* siendo los mecanismos de consenso más comunes adoptados por las principales criptomonedas para proteger su red. (Binance Academy, 2018)

Proof of Work (PoW)

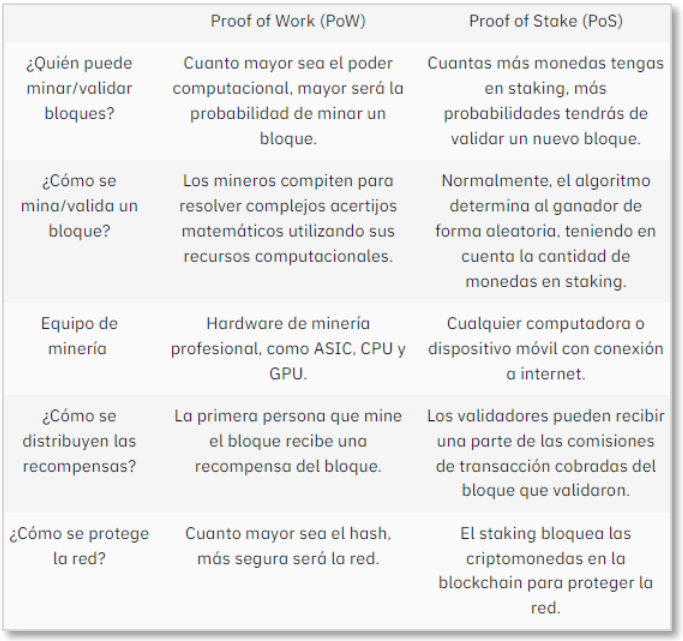
Fue el primer mecanismo de consenso en emplearse. Se utiliza en la red de Bitcoin para validar transacciones y proteger la red. Aparte de otras cosas, PoW evita el doble gasto. La blockchain está asegurada por participantes llamados mineros, que utilizan el poder computacional para competir por el derecho a confirmar nuevos bloques y actualizar la blockchain. Esto se realiza a través de resolver un acertijo mediante cálculos matemáticos. Al conseguir la respuesta de dicho acertijo de la forma más rápida posible, le permitirá anexar un nuevo bloque de registros de transacciones a la cadena de bloques. A febrero de 2022, un minero podía obtener una recompensa del bloque de 6.25 BTC más comisiones de transacción al minar con éxito un bloque de Bitcoin.

Proof of Stake (PoS)

La principal diferencia entre PoW y PoS es la forma en que determinan quién puede validar un bloque de transacciones. *Proof of Stake* es la alternativa más popular a *Proof of Work*. Es un mecanismo de consenso que tiene como objetivo mejorar algunas de las limitaciones de PoW, como problemas de escalabilidad y consumo de energía. En PoS, los participantes se denominan validadores. No necesitan utilizar hardware potente para competir por la oportunidad de validar un bloque. En cambio, necesitan poner en *stake* (bloquear) la criptomoneda nativa de la blockchain. Luego, la red selecciona un ganador en función de la cantidad de *tokens* bloqueados, quien será recompensado con una proporción de las comisiones de transacción del bloque que valide. Cuantas más monedas tenga en *staking*, mayor será la probabilidad de ser elegido como validador.

En la siguiente figura se pueden observar las principales diferencias de estos dos protocolos de consenso previamente descriptos.

Figura 7: PoW vs PoS



	Proof of Work (PoW)	Proof of Stake (PoS)
¿Quién puede minar/validar bloques?	Cuanto mayor sea el poder computacional, mayor será la probabilidad de minar un bloque.	Cuantas más monedas tengas en staking, más probabilidades tendrás de validar un nuevo bloque.
¿Cómo se mina/valida un bloque?	Los mineros compiten para resolver complejos acertijos matemáticos utilizando sus recursos computacionales.	Normalmente, el algoritmo determina al ganador de forma aleatoria, teniendo en cuenta la cantidad de monedas en staking.
Equipo de minería	Hardware de minería profesional, como ASIC, CPU y GPU.	Cualquier computadora o dispositivo móvil con conexión a internet.
¿Cómo se distribuyen las recompensas?	La primera persona que mine el bloque recibe una recompensa del bloque.	Los validadores pueden recibir una parte de las comisiones de transacción cobradas del bloque que validaron.
¿Cómo se protege la red?	Cuanto mayor sea el hash, más segura será la red.	El staking bloquea las criptomonedas en la blockchain para proteger la red.

Fuente: Binance Academy.

Por lo tanto, para garantizar que las transacciones registradas en una blockchain sean válidas, estas redes adoptan diferentes mecanismos de consenso. *Proof of Work (PoW)* es el más antiguo, fue creado por Satoshi Nakamoto y es considerado por muchos como una de las alternativas más seguras. Además de Bitcoin, PoW también se utiliza en otras criptomonedas importantes como Ethereum (ETH) y Litecoin (LTC). *Proof of Stake (PoS)* se creó más tarde, pero ahora se ve utilizado en una diversidad de proyectos importantes. Entre ellos se pueden nombrar a Binance Coin (BNB), Solana (SOL), Cardano (ADA) y Polkadot (DOT). Vale la pena señalar que Ethereum planea cambiar de PoW a PoS durante el 2022.

Resumen

Proof of Work nace con Bitcoin, blockchain de primera generación. Luego, con el fin buscar mejoras a algunas de las limitaciones intrínsecas del PoW, se desarrollaron nuevos mecanismos de consenso como el *proof of stake* implementado en blockchains de segunda y tercera generación. Aun así, si bien cada uno de ellos resuelven con mayor o menor eficacia los problemas del trilema blockchain, al día de hoy, ninguno se identifica como una solución superadora. La elección final en la utilización de un determinado protocolo de consenso dependerá de la prioridad que se defina al problema que se desee resolver.

Capítulo 3. La minería de criptomonedas

3.1. Minería con prueba de trabajo (PoW)

Lo interesante de minar criptomonedas es que por una parte se contribuye a la validación de bloques, permitiendo que se realicen transacciones entre usuarios favoreciendo la construcción de una red de información descentralizada, y a cambio, se obtiene una recompensa económica aportada por la misma red. Esta nueva actividad instaló la posibilidad de descentralizar la economía, rompiendo los paradigmas existentes, principalmente en países emergentes como el nuestro dónde las criptomonedas están jugando un papel predominante como refugio de valor.

Antes de empezar a minar es probable que uno se pregunte ¿Cuánto es lo que se puede ganar por minar Bitcoin u otra *altcoin*, o qué es lo que se debe saber para aprender a calcular si es rentable minar criptomonedas? La minería de criptomonedas es un negocio, y como todo negocio, para llevarlo a cabo, se requiere de una inversión financiera, administrar las ganancias y gestionar los gastos generados. Es decir, se debe calcular la rentabilidad del negocio en cada momento con un horizonte temporal determinado para identificar si es viable o no ejecutar dicho negocio. En base a la experiencia adquirida es recomendable analizar y entender los siguientes aspectos primordiales para saber qué es lo que se requiere y cuánto se debe invertir antes de iniciarse en la criptominería, principalmente en proyectos que utilicen algoritmos de consenso PoW. (Rojas, 2018)

1. ***Estudiar el proyecto bitcoin o altcoin. ¿Cómo se consigue la recompensa y cuanta cantidad?***

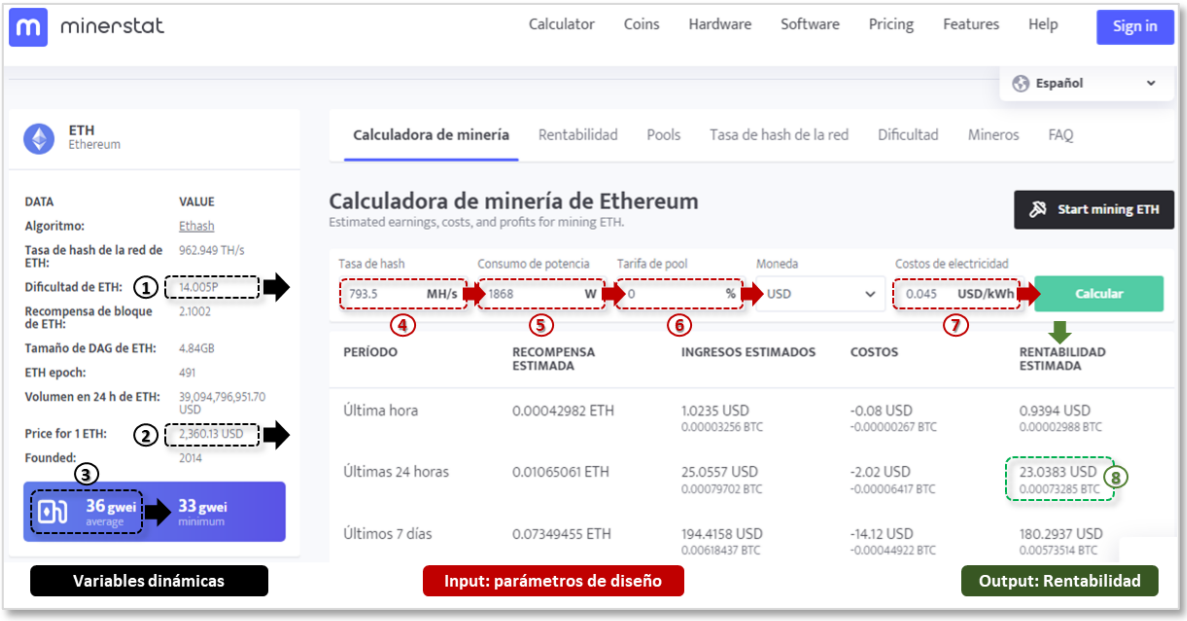
El minero que valide el bloque aprobado por consenso, se llevará la recompensa. Cada red de criptomonedas tiene diferentes recompensas, en el caso de bitcoin se obtiene 6.25 BTC por bloque minado (dato a feb/2022), y cada 4 años aproximadamente se reduce a la mitad por el evento llamado *halving*. En caso de minar Ethereum, se obtiene 2 ETH más las tarifas de transacción por cada bloque minado (dato a feb/2022). Se puede consultar las recompensas por bloque en sitios como etherscan.io, que proporciona estadísticas actualizadas diariamente sobre las recompensas de bloque de Ethereum.

Conocer la cantidad de dinero que se puede ganar por día se trata de una de las inquietudes que despierta mayor interés a la hora de prestar tiempo y capital para procesar las transacciones de una red de criptomonedas. Sin embargo, no resulta tan sencillo conocer con

exactitud cuál será la rentabilidad final, puesto que hay varios factores que influyen sobre la misma.

Para exponer un ejemplo práctico, en la siguiente figura se puede observar cómo accediendo a minerstat.com, uno de los portales más utilizados por la comunidad minera, uno puede calcular la rentabilidad diaria de minería seleccionando la criptomoneda deseada e ingresando ciertos parámetros de entrada como la tasa de *hash* aportada a la red, el consumo de potencia del equipo y el costo eléctrico local.

Figura 8: Calculadora de minería Ethereum al 10/05/2022



Fuente: minerstat.com.

Según este portal, con un equipo de minería de 793,5MH/s, 1.898W de consumo de potencia y un costo eléctrico de 0,45 USD/kWh (tarifa Edesur, Caba, Argentina), se pueden generar hasta 23 dólares diarios por minar en la red de Ethereum. Claro está, esto también dependerá del precio de ETH para ese momento, la dificultad de la red y el precio del Gas (gwei) identificados como las variables dinámicas en la figura 8, pudiendo llegar el caso que la combinación de los valores de estas variables pueda arrojar saldos negativos viéndose superada por los costos de operación.

En resumen, podemos asumir que en algunos casos minar en una red de criptomonedas sea rentable y en otros casos no lo sea. En este negocio no hay una única manera de medir la rentabilidad ni tampoco arroja un número exacto. En la minería se puede ganar como perder

dinero, por lo que siempre es importante procurar mantenerse rentable o al menos sin pérdidas. A la hora de calcular la rentabilidad de la minería, no se puede depender únicamente de las ganancias que generan las comisiones por transacción o las recompensas del bloque. Los ingresos de un minero también se ven afectados por factores externos como las tarifas eléctricas, las variaciones en el precio de la criptomoneda y los costos de mantenimiento de los equipos. Por lo tanto, para saber si para es rentable minar una criptomoneda en particular, se debe evaluar al menos cuatro variables esenciales:

- El precio del criptoactivo en el mercado (promedio histórico).
- La dificultad de la minería.
- El precio del hardware y de su mantenimiento.
- El costo de los servicios, tales como el de internet y el precio local de la electricidad.

En caso de querer escalar el negocio desde un simple equipo a una granja de minería doméstica, se deberá considerar otras variables adicionales relacionadas con los costos de adecuación del espacio donde funcionará la granja. Esto implica evaluar la inversión en la instalación de transformadores, tableros eléctricos, extractores, aires acondicionados u otros sistemas de refrigeración para los equipos, además del mantenimiento de dichos equipos.

En conclusión, no existe un cálculo preciso de rentabilidad que se pueda obtener por la minería de una red como Bitcoin, Ethereum, etc. El resultado dependerá de cuánto se esté dispuesto a invertir para empezar a minar, en qué lugar del mundo se encuentren instalados los equipos y cómo se comporte el mercado/red al momento de llevar a cabo dichas actividades. Asimismo, las ganancias que genera la minería pueden variar en cortos plazos, por lo que en un periodo especifico puede llegar a ser un trabajo sumamente rentable y en otro momento puede generar pérdida de dinero.

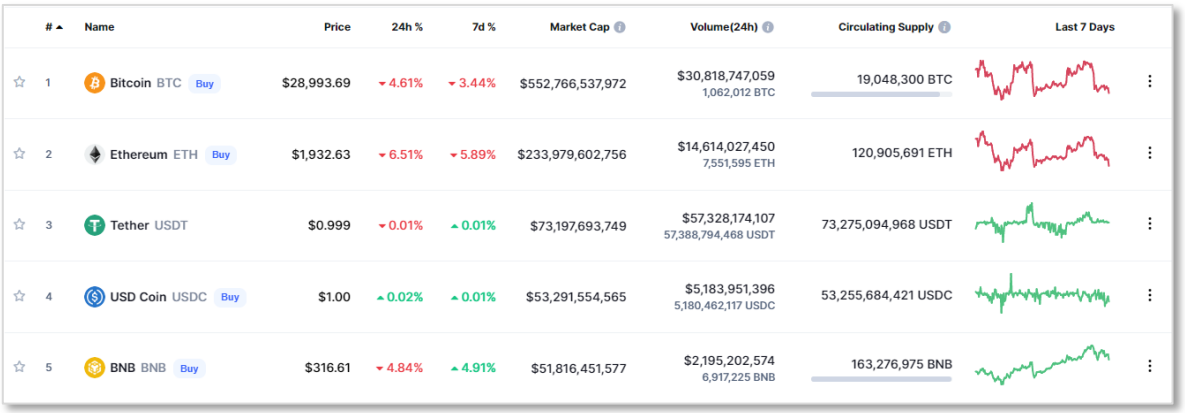
2. *Estrategias.*

Asumida la decisión de comenzar a minar, la experiencia ha demostrado que se pueden adoptar distintas estrategias defensivas para para afrontar la variabilidad intrínseca de la renta obtenida por dicho negocio.

- ***Estrategia de monetización:*** Decidir entre cobrar y vender la moneda versus *holdear*[8] a largo plazo, esperando que el precio se valorice y obtener mayores ganancias a futuro. Ambas opciones son óptimas y pueden incrementar o hacer decrecer la ecuación de rentabilidad. Dependerá de la correcta lectura del contexto y del estudio previo que se haya hecho sobre el proyecto criptográfico.

  El precio de la criptomoneda: En general el mercado de criptomonedas es muy volátil. En un mercado alcista los mineros podrían registrar una buena rentabilidad por el aumento del precio del activo, permitiéndoles no solo contar con mayores ganancias, sino que también podrían cubrir con mayor facilidad los gastos que generan sus actividades de minería y permitirles acortar el tiempo de recuperación de la inversión que hicieron al comprar los equipos especializados. Sin embargo, aun así, hay que saber gestionar los gastos, porque si sucediera el caso contrario, se podrían sufrir fuertes caídas de ganancia por el desplome del mercado. Por esta razón, es recomendable siempre estar atento a los movimientos de precio. Para monitorear la evolución de precios se puede ingresar a la página de CoinMarketCap, siendo uno de los sitios web de seguimiento de precios más utilizado del mundo para criptoactivos (ver figura 9).

Figura 9: Criptoactivos y su capitalización de mercado



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC Buy	$28,993.69	4.61%	3.44%	$552,766,537,972	$30,818,747,059 1,062,012 BTC	19,048,300 BTC	
2	Ethereum ETH Buy	$1,932.63	6.51%	5.89%	$233,979,602,756	$14,614,027,450 7,551,595 ETH	120,905,691 ETH	
3	Tether USDT	$0.999	0.01%	0.01%	$73,197,693,749	$57,328,174,107 57,388,794,468 USDT	73,275,094,968 USDT	
4	USD Coin USDC Buy	$1.00	0.02%	0.01%	$53,291,554,565	$5,183,951,396 5,180,462,117 USDC	53,255,684,421 USDC	
5	BNB BNB Buy	$316.61	4.84%	4.91%	$51,816,451,577	$2,195,202,574 6,917,225 BNB	163,276,975 BNB	

Fuente: CoinmarketCap.

- ***Estrategia de diversificación:*** Decidir minar una sola criptomoneda resulta similar a conformar una cartera de inversión con un único activo. Al realizar correctamente el

[8] El Holder se puede considerar como un inversor. Es una figura que considera más rentable almacenar y acumular una criptomoneda a largo plazo que negociar con ella.

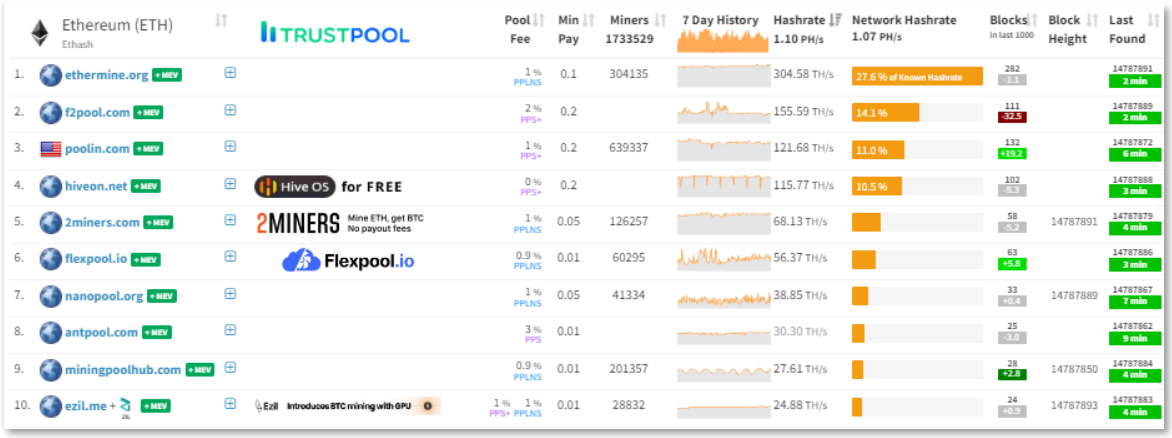
estudio preliminar de cada proyecto, se podrá observar que sus correspondientes *roadmaps* evidenciarán hitos de proyectos que podrían impactar fuertemente en el desempeño del precio de la moneda que respaldan, alterando la ecuación de rentabilidad y definiendo los momentos claves para entrar o salir. Por otro lado, van surgiendo nuevos proyectos que, si bien requieren de una nueva inversión de capital, también permitirán diversificar el riesgo y reforzar la ecuación de rentabilidad.

3. *¿Minar en solitario o en pool?*

Decidir minar en solitario implica llevarse la recompensa entera en caso de conseguir validar un bloque. Pero también implica poseer cientos o miles de dispositivos potentes para poder competir con el *hashrate* de otros mineros o *pool*. Hay un solo resultado correcto para cada acertijo propuesto en una red de criptomonedas y una sola forma de obtener esta respuesta. La probabilidad de que un nodo minero resuelva dicho acertijo depende de su poder de cálculo en comparación con el de los demás nodos mineros de la red. Por tal razón, para la gran mayoría de los mineros resulta más conveniente minar en un *pool* y repartir las recompensas.

Los *pools* de minería son nodos mineros a los que se conectan un grupo de personas para llevar a cabo la actividad de generar criptomonedas en conjunto. La suma del poder minado (*hashrate*) de todos los participantes se suman en una sola entidad, por lo que tienen mayores probabilidades de dar con la respuesta de un bloque que en el caso de que minar en solitario. Así mismo, al compartir poder computacional para minar los bloques de una red, la recompensa recibida se divide entre todos los colaboradores. De igual manera, los operadores de *pool* suelen cobrar comisiones por agrupar a todos los mineros en un mismo nodo, generándose un gasto que debe ser tomado en cuenta para calcular la rentabilidad del negocio. Ingresando al portal de *Mining Pool Stats* se puede acceder a un listado completo de todas las *pool* y redes disponibles. En la figura 10 se puede observar el top 10 de los principales *pools* de minería de Ethereum ordenadas por el tamaño del *hashrate* mundial.

Figura 10: Top 10 pools de minería de ETH



Fuente: Mining Pool Stats.

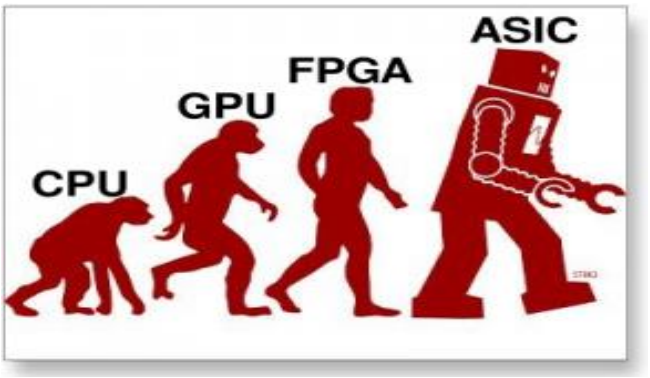
Antes de aventurarse a seleccionar un *pool* se debe estudiar sus características y estado actual, como la comisión que cobran, el pago mínimo, el tamaño de *hash* que aportan a la red, la cantidad de bloques minados en las últimas 24hs, etc. No hay un *pool* ideal, cada una se adaptará a las necesidades y estrategia de cada minero. Existen diferentes métodos que usan los *pools* para pagar a los mineros por su trabajo. Algunos operadores pueden distribuir las monedas emitidas entre los mineros, pero quedarse con toda la comisión de transacciones que tenía el bloque. Por otro lado, existen *pool* que entregan un valor fijo por cada share que entrega el usuario (PPS: Pay per share) o calculan un porcentaje en relación a los shares con los que contribuyeron para minar en un período específico (PPNS: Pay per last N shares). Seleccionar un *pool* es una decisión que debe meditarse. Algunos *pools* no comparten entre sus mineros las comisiones por transacción registradas en el bloque, por lo que es una disminución en el total de ganancias que puede hacer un minero por su trabajo.

4. Equipamiento: ¿Qué se requiere para poder minar?

- ***Hardware:***

Corresponden a los equipos físicos para minar la criptomoneda deseada. Pueden ir desde equipos genéricos (CPU/GPU) hasta procesadores dedicados y optimizados específicamente para la minería (FGPA/ASIC). En la siguiente figura se observa un ejemplo figurativo de cómo fue evolucionando la tecnología de minería en el hardware.

Figura 11: Evolución del hardware para minería



Fuente: bitcoin.org.

Decidir el hardware depende de varios factores: el presupuesto que se tenga para poder invertir, el poder de minado que se desee obtener y el tipo de algoritmo de minería con el que esté diseñada la red de la criptomoneda a minar.

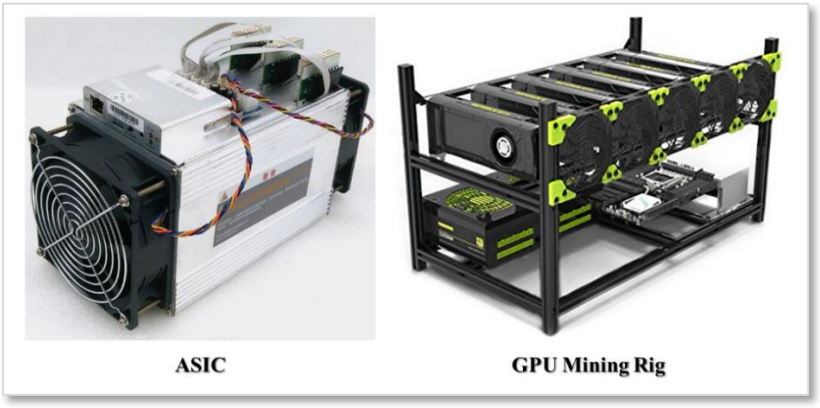
> **Algoritmos de minería:** Estos son algoritmos que permiten hacer posible la minería de la criptomoneda, son funciones hash criptográficas muy complejas y pueden ajustar la dificultad[9] de la minería. El algoritmo se encarga de establecer las normas de encriptado y desencriptado de la información. Convierte un mensaje fácil de entender en algo indescifrable. Además, se asegura de que sea imposible repetir el mismo resultado con otro mensaje. De esta forma se consigue seguridad en la red y se garantiza que ninguna criptomoneda pueda ser falsificada. Los algoritmos de minería más utilizados son los de Bitcoin conocido como SHA256 y el de Ethereum llamado Ethash.

Los equipos ASIC suelen ser los más costosos y son usados para la minería de criptomonedas como Bitcoin, Litecoin o Dash. Por otro lado, las tarjetas gráficas pueden minar de forma rentable en redes como Ethereum, Ethereum Classic, Ravencoin o Monero. Además, son más versátiles y menos costosas que los ASIC (ver figura 12). En el momento de tener que seleccionar un hardware, se debe tener claro que, más caro no significa que sea mejor y más potente no significa que genere más ganancias. Hay hardware minero que, a pesar de ser muy potente, consume mucha energía. También hay equipos muy buenos en calidad y potencia,

[9] La dificultad de minería funciona como un parámetro dinámico que se ajusta constantemente según las condiciones de la red. El objetivo del minado es descubrir y generar un nuevo bloque según la programación de la red. Entonces, la dificultad es ajustada por el mismo sistema.

pero que son tan costosos que recuperar la inversión puede llevar años. Como recomendación se debe buscar equipos que ofrezcan una buena rentabilidad para cada caso en particular. Hardware minero que mine efectivamente la criptomoneda de preferencia, que tenga un buen balance entre potencia y consumo eléctrico, que se pueda pagar y recuperar la inversión en un tiempo prudencial y que esté disponible en el mercado donde uno se encuentre.

Figura 12: Hardware de minería



Fuente: catálogos de mercado.

Un factor no menos importante que puede afectar directamente la ecuación de rentabilidad en este negocio deriva del correcto mantenimiento de los equipos. Si se desea dedicar a la minería, es fundamental mantener limpio el espacio físico y realizar mantenimientos preventivos a los equipos con la finalidad de extender su vida útil. Siempre es necesario que el lugar tenga buena ventilación, refrigeración y las condiciones de aire seco para que las máquinas o las GPUs no se dañen fácilmente. En esta misma línea, hay que tener en cuenta que las máquinas de minería necesitan mantenimiento periódico, tales como limpieza profunda, revisión del ventilador y fuentes de energía, y chequeo de temperaturas de procesadores y memorias. Es decir, se podría perder dinero por ser negligentes en el mantenimiento de los equipos.

Un minero o responsable del negocio tiene que estar monitoreando y administrando sus equipos constantemente, estar pendiente de la inversión que ha realizado y de las posibilidades que tiene de aumentar la rentabilidad de sus máquinas. Es prioritario revisar diariamente que equipos no estén trabajando a su máximo rendimiento o si existe alguna falla que los pueda estar ralentizando. La minería es un trabajo de tiempo completo, un

mantenimiento optimo y sostenido a los equipos es la clave para prolongar su vida útil y por consiguiente maximizar la rentabilidad del negocio.

- ***Software:***

El software es el programa que se necesita para poder empezar a minar. Existen diferentes tipos de software o programas que permiten que el hardware seleccionado interactúe con la red de la criptomoneda y pueda minarla. En función del tipo de hardware a utilizar dependerá el software a instalar. Entre los más populares se encuentran CGMiner para minar Bitcoin y Hive Os para para minar Ethereum. Para monitorear el desempeño del proceso de minado estos programas ya incluyen un *dashboard* con los principales datos estadísticos como potencia de minando en Mh/s, ganancias netas diarias y mensuales, potencia de consumo en Kwh, etc. En la web del *pool* de minería seleccionado también se puede visualizar el desempeño del hardware.

En la siguiente figura se puede observar un ejemplo de *dashboard* de una granja de minería domestica propia compuesta por tres *workers* o trabajadores/mineros de Ethereum utilizando el software Hive Os.

Figura 13: Dashboard de una granja de minería en Hiveos

Fuente: elaboración propia.

De la figura se desprenden los siguientes datos observados:

Dashboard General

- Equipos: 3 *workers* / 28 GPUS
- Estado: ONLINE
- Consumo: 2.980kW
- Potencia de cálculo: 1.313GH/s
- Algoritmo de minería: ETASH
- Altcoin: ETH

Monitor de funcionamiento

- Temperaturas de microprocesador: 55°C…
- Temperaturas de memorias: 75°C…
- Velocidad del ventilador en %: 80% …

Rentabilidad

- Ganancias estimadas por
  - día: 0,0087 ETH / 17,85 USD
  - semana: 0,06091 ETH / 124,92 USD
- Balance de pagos histórico: 15,0664 ETH / 30.901,21 USD

Potencia de minado

- *Hashrate* real: 808,89MH/s
- *Hashrate* reportado: 793,55MH/s
- *Hashrate* promedio 24hs: 761,22MH/s

- ***Billetera:***

Para poder recibir el pago de la criptomoneda se necesitará una dirección de billetera. Se podrán asignar billeteras físicas como Ledger, una digital como Metamask, o simplemente usar la dirección de un *exchange* como Okex o Binance. Si lo que se busca es seguridad lo ideal será tener las criptomonedas guardadas en una *cold wallet*, en donde el propietario será el único que posea las palabras semilla, imposibles de hackear de forma directa. En la siguiente figura se expone las principales características de cada una de ellas.

Figura 14: Tipos de wallets de criptomonedas

Fuente: elaboración propia.

No existe la billetera perfecta. Combinar varios tipos de *wallets* según las necesidades que se tenga en cada momento puede ser lo más inteligente.

5. La instalación del equipo y su ubicación

Una vez realizado el análisis preliminar de rentabilidad y habiendo decidido que hardware comprar para iniciar con el negocio de la minería, queda un aspecto fundamentalmente importante que se debe contemplar: el espacio físico donde se instalarán los equipos para que trabajen. La opción más práctica sería contratar un servicio de *housing*[10]. Hoy en día existen muchos proveedores que ofrecen este servicio a cambio de una comisión. De escoger esta opción se deberá descontar los gastos de la ecuación de ganancias.

Por el contrario, si se desea tener los equipos de minería (ASIC o GPU) en casa o montar una granja de minería en una locación propia se deberá contemplar todo lo referente a las condiciones de temperatura, limpieza del aire y al consumo eléctrico a la hora de calcular los gastos y comenzar con su instalación. Como consecuencia del alto nivel de procesamiento de datos que requiere la minería de criptomonedas, el hardware que se emplea para estas actividades tiende a elevar su temperatura y puede llegar a recalentarse. Por lo tanto, es primordial que el espacio en donde se instalen los equipos esté refrigerado. Es decir, que en caso de no realizar un buen mantenimiento y garantizar un ambiente fresco y limpio se correría el riesgo de perder el equipo o acelerar su deterioro. Todo esto tiene incidencia en el costo final de las actividades de minería que se deberá calcular mes a mes para saber cuán rentable está siendo el negocio.

- ***Conexión eléctrica:***

Las desventajas del PoW es que requiere de hardware que consume mucha potencia. Antes de instalar cualquier equipo de minería se deberá analizar si la red eléctrica disponible tiene la capacidad de soportar su consumo. Es importante medir el diámetro de los cables y ver en qué estado se encuentran. También es recomendable que cada equipo posea una línea de consumo independiente, seccionada con sus propios instrumentos de seguridad. Por último, se debería garantizar la protección mecánica de los equipos con una correcta puesta a tierra.

La factura eléctrica tomará en cuenta los gastos que generen los equipos, la refrigeración e iluminación del lugar. Asimismo, se deberá contemplar un servicio de internet estable que

[10] El servicio de *Housing* ofrece la posibilidad de alojar los equipos en un warehouse o datacenter. La propuesta incluye todos los gastos de locación, electricidad, mantenimiento y supervisión de los equipos a cambio del pago de una comisión porcentual sobre las ganancias obtenidas de la minería.

permita conectar los equipos a la red. El costo de la electricidad y de internet, así como la calidad de tales servicios, es crucial para evaluar la rentabilidad de la minería de criptomonedas. Mientras más poder de minado se desee tener, mayor será el consumo de electricidad. Las tarifas eléctricas variarán conforme al lugar en el que se desee instalar los equipos**,** por lo que no hay un costo fijo definido. Los mineros profesionales prefieren radicarse en países o zonas donde la electricidad sea más barata y la temperatura ambiente sea relativamente más baja, con el objetivo de disminuir los gastos y sacarle mayor provecho al negocio. El precio de la electricidad es un elemento clave en la rentabilidad, por lo que buscar la mejor configuración de rendimiento será un objetivo fundamental.

- ***Refrigeración:***

Como se ha mencionado anteriormente, el proceso de minería supone de hacer cálculos matemáticos complejos que requieren de altos consumos de potencia provocando que se recalienten los procesadores. De esta forma se deberá controlar la refrigeración del hardware para evitar el sobrecalentamiento. Las formas más efectivas son incorporando refrigeración directamente en el hardware, generar un ambiente fresco y ventilado, o usar sistemas de refrigeración líquida en caso de no alcanzar la temperatura deseada con los métodos anteriores. Siempre se deberá monitorear la temperatura y el rendimiento de los equipos para lograr los mejores resultados en el minado de criptomonedas.

3.2. Minería con prueba de participación (PoS)

Hacer *staking* supone depositar criptomonedas bloqueadas en la red para la validación de bloques y obtener recompensas. Es una alternativa al PoW que no requiere de hardware, reduciendo así los costes energéticos. Para poder hacer *staking* solo se requiere poseer la criptomoneda en cuestión y bloquearla en su red blockchain. A través de este proceso uno certifica que no usará esos fondos para otros fines que no sean para la validación de transacciones. Dando garantía de su compromiso, ya que si actúa de forma irresponsable queriendo dañar el ecosistema podría perder todas las criptomonedas que tenga bloqueadas.
La selección del nodo validador que agregará el siguiente bloque a la cadena es semi aleatoria, pero, mientras más criptomonedas se tenga asignadas a este fin, mayores serán las posibilidades de ser elegido. En consecuencia, se ganará más dinero. También puede ser visto

como el proceso de restringir el uso comercial de las monedas criptográficas con el fin de obtener recompensas. (Perez, 2021)

Ventajas de hacer staking

- Obtener ingresos pasivos: los usuarios obtienen recompensas por sus esfuerzos de *staking*. Simplemente manteniendo activos en un monedero y permaneciendo conectado a la red, se puede obtener un ingreso pasivo.
- Participar en una comunidad más amplia: los validadores y nominadores trabajan arduamente para garantizar que la red sea un lugar seguro para realizar transacciones. Al convertirse en un *staker*, se puede unir a esa comunidad y contribuir al esfuerzo general, con recompensas por hacerlo.
- No es difícil empezar: si bien hay varias formas de comenzar a hacer *staking*, algunas más complejas que otras, al final resulta ser más simple que comenzar montando una granja de minería.

Desventajas de hacer staking

- Los fondos están bloqueados: al realizar *staking*, los fondos se bloquean en la red. Si bien técnicamente se pueden sacar cuando se desee, hacerlo significa perder las tasas de interés y comenzar de nuevo desde cero.
- Alta presión: si hace *staking*, también se le está indicando a la red que se desea participar. Al no permanecer conectado y realizando *staking* en la red, se puede enfrentar a *slashing* y perder las ganancias. Participar no es una solicitud masiva de ninguna manera, pero requiere algo de dedicación y esfuerzo. Además, si un validador por el que votó actúa mal, también puede estar sujeto a un *slashing*. Vale la pena tomarse el tiempo para estudiar validadores potenciales antes de nominar para evitar perder dinero.

Formas de hacer staking

Hay varias formas de comenzar a hacer *staking* algunas más complejas que otras:

- On-chain - convertirse en un *masternode*: Los *masternodes* son solo para partidarios incondicionales de la red. Configurar uno es bastante difícil, ya que requiere tener una máquina dedicada conectada a la red las 24 horas del día, los 7 días de la semana. Esa máquina conectada también debe ser potente, lo que significa que se tendrá que invertir en un buen hardware para comenzar. Convertirse en un *masternode* requiere descargar un software específico y aprender a operar a través de comandos binarios.

- Utilizar un *exchange*: es probablemente la forma más fácil de hacer *staking*. Usualmente el proceso es similar en la mayoría de las plataformas que permitan hacer *staking* en la red deseada. Se deberá abrir una cuenta, comprar el *token* de gobernanza de la red, dirigirse a la sección de inversiones (*earn*), ingresar a la sección de *staking* y, por último, seleccionar el *token* deseado dentro de una lista de activos disponibles. Utilizar un *exchange* para hacer *staking* puede ser más fácil que configurar un nodo, pero también tiene un costo. La *exchange* seleccionada tomará un porcentaje de todas las recompensas de *staking* que se gane, lo que significa que se estará ganando un poco menos de lo que se ganaría de otra manera. Cada *exchange* tiene diferentes tarifas, así que se deberá incluir el costo de la tarifa en el cálculo de rentabilidad.
- Utilizar un monedero: si bien usar un monedero es un poco más complejo que usar un *exchange*, puede ser mucho más gratificante. Dado que se está exento de pagar tarifas a un tercero, pudiendo capitalizar la totalidad de la tasa de rendimiento del *staking*.

Resumen

La rentabilidad de la minería de criptomonedas depende de diversos factores externos e internos. Se trata de una actividad que puede ser altamente lucrativa si se cuenta con las variables a favor, como estar ubicado en un lugar con tarifas eléctricas baratas, regulaciones flexibles y un clima que beneficie el funcionamiento de los equipos. Asimismo, otras características dependerán de las propias decisiones como consumidor, tales como la calidad del hardware adquirido para minar, cuánto dinero se planea invertir en la instalación de los equipos e, incluso, el *pool* que se prefiera para trabajar. Lo más recomendable para todos aquellos que deseen empezar el negocio de la minería, que primero se investiguen y analicen todos estos factores, para poder realizar un análisis de factibilidad. Solo así será posible tener un panorama realista de cuán beneficiosa pueda ser esta actividad para vuestra economía, o si más bien convenga buscar otras maneras para generar ganancias con criptomonedas. Las estrategias de inversión a largo plazo, el *trading/scalping* o bien la minería a través de otros protocolos de consenso como el PoS son otras de las opciones más populares para aumentar las ganancias con criptomonedas.

Capítulo 4. La evolución de la minería de criptomonedas

Emprender en el negocio de la criptominería es una actividad enriquecedora, totalmente impensada hace diez años atrás. Con solo iniciarse en esta actividad, uno no solo se capitaliza rendimientos económicos, sino que también se convierte en un agente importante en el sostenimiento de la red descentralizada más grande y extensa conocida, además de adquirir aprendizaje y conocimiento sobre una tecnología que viene a patear el tablero en muchas industrias. El conocimiento es un valor intangible que no siempre se tiene en cuenta en la ecuación de rentabilidad, pero es sumamente valioso como el bitcoin, más en esta época de maduración tecnológica temprana en que vivimos, donde las oportunidades para emprender en proyectos blockchain son altamente redituables. En el presente capítulo se hará un breve repaso de la historia de la minería de criptomonedas, desde sus inicios hasta la actualidad, destacando los hitos más importantes que generaron su adopción y evolución tecnológica.

Si bien la euforia por adquirir equipos de minería ha venido creciendo en estos últimos años, es importante entender, antes de desembarcar en cualquier inversión de criptominería, en que estadio se encuentra cada proyecto criptográfico, sea de bitcoin o alguna de las distintas *altcoins*[11] existentes, para no caer en la trampa de querer incrementar nuestro capital de forma efímera en proyectos que se encuentren en su etapa final de desarrollo.

En la actualidad existe una batalla cultural por la hegemonía de los dos protocolos de consenso más utilizados. Por un lado, están los defensores del PoW que abogan por un mundo libre y descentralizado, y por el otro, se encuentran los que están a favor del PoS que persiguen un mundo eficiente, limpio y verde. Sea cual fuere el resultado en el futuro, claro está que Bitcoin, como red pionera del PoW, marca la tendencia de todas las *altcoins* que se construyan en protocolos de consenso de prueba de trabajo. Entender en que etapa se encuentra Bitcoin facilitará la comprensión y el análisis preliminar de cualquier proyecto PoW que se quiera abordar.

El diseño de la red bitcoin

Antes de analizar en que etapa de adopción se encuentra bitcoin es importante repasar algunos conceptos de diseño de su red. En primer lugar, hay que entender que la propia red

[11] Este término se utiliza para referirse a las monedas digitales alternativas a Bitcoin, es decir, criptomonedas que no son el Bitcoin.

controla la emisión de bitcoins, derivada por consenso de todos sus participantes y siguiendo las siguientes reglas:

- Emisión total 21,000,000 Bitcoins.
- Objetivo de intervalos de bloque de 10 minutos.
- Evento de reducción de emisión a la mitad (evento *halving*) que ocurre cada 210.000 bloques (aproximadamente cada 4 años).
- Recompensa de bloque que comienza en 50 BTC y se reduce a la mitad continuamente en cada evento de *halving* hasta que llega a 0 (aproximadamente en el año 2140).
- Cualquier cambio en estos parámetros requiere que todos los participantes de Bitcoin estén de acuerdo por consenso para aprobar el cambio.

Cada 4 años la emisión monetaria de BTC se reduce a la mitad por el evento de *halving*, y como el *supply* se encuentra limitado en 21M de unidades, se produce un efecto deflacionario en cada evento. Por lo tanto, al ser una red totalmente descentralizada y autónoma, sumado a su diseño monetario deflacionario, convierte a Bitcoin en la red más deseada por los mineros.

Breve repaso de la adopción de bitcoin

La génesis de la minería de criptomonedas inicia con bitcoin en el 2009. Por aquel entonces, uno de los primeros sitios de intercambio P2P llamado *New Liberty Standar* había establecido el primer precio de bitcoin en 0,08usd, basándose en los costos de la electricidad y gastos necesarios para mantener las computadoras que los minaban. Esta actividad fue iniciada por los visionarios o también llamados *early adopters*, representados mayoritariamente por criptógrafos, informáticos y *cyberpunks*[12] que ya estaban preparados para entender técnicamente la importancia del invento de Satoshi Nakamoto. Ellos fueron pioneros, verificando que el protocolo de bitcoin no tuviera fallas técnicas. En épocas tempranas existían pocos jugadores concentrando la totalidad de los activos generados.

Una segunda ola de adopción se produjo luego del primer *halving*, atrayendo tanto a inversores tempranos o visionarios de nuevas tecnologías como a una corriente de inversores motivados ideológicamente y entusiasmados por el potencial de una moneda libre del control estatal. Los libertarios se sentían atraídos por actividades antisistema que eran posibles con

[12] Un cypherpunk es cualquier individuo que defiende el uso generalizado de la criptografía fuerte y de las tecnologías que mejoran la privacidad como vía para el cambio social y político.

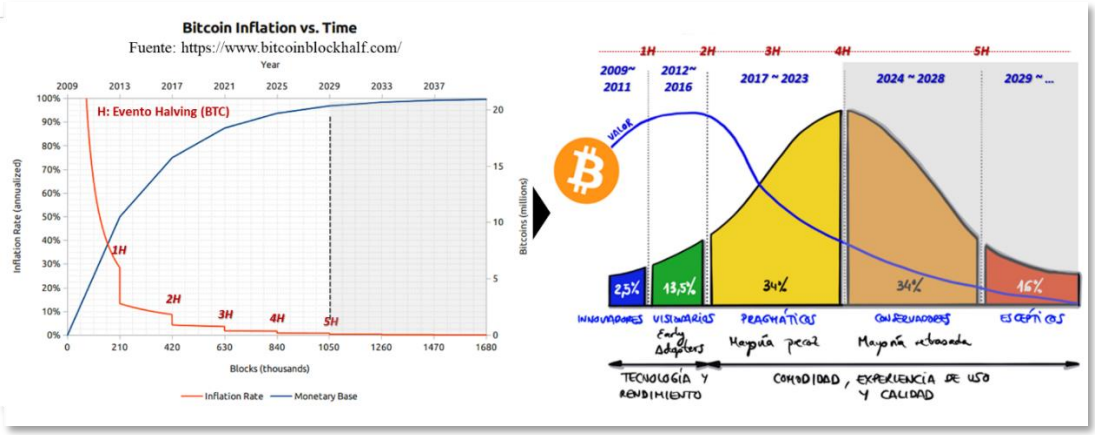
la adopción amplia de esta tecnología naciente. A partir del 2013 empezaron a aparecer los primeros inversores minoristas e institucionales, los que se atrevieron a navegar los complicados canales de liquidez donde se podía adquirir bitcoin.

Entre el 2014 y 2017 los participantes generaron un nuevo impulso de adopción comenzando a aparecer en los medios tradicionales haciendo crecer su popularidad. En 2021 atravesó un nuevo pico de euforia con una masiva adopción institucional. En enero 2022 el precio experimentó una importante corrección. Con fuentes de liquidez profundas y maduras, grandes inversores institucionales tienen ahora la oportunidad de participar a través de bancos o *exchanges* regulados.

En la actualidad el precio de bitcoin atraviesa un periodo bajista, muchos analistas afirman que tocara un piso antes de comenzar con un nuevo ciclo alcista, sin embargo, como se puede apreciar en la siguiente figura, se puede interpretar que la criptominería se encuentra en la recta final de adopción por el segmento denominado *early majority* o pragmáticos.

Tal vez, el período 2024~2028 sea considerado el momento de adopción para los conservadores y la última ventana rentable de ingreso al negocio de la minería bajo el protocolo de consenso PoW. Dado el historial de crecimiento que viene demostrando la red, quizás para ese momento ya no resulte tan atractivo arrancar de cero para montar una granja de minería. Para el 2028 se espera que la ganancia por minar un bloque de Bitcoin descienda a 1,56BTC, por lo tanto, el precio debería aumentar lo suficiente para compensar la rentabilidad de los mineros como incentivo para seguir garantizando la seguridad de la red. (Cointelegraph, 2022)

Figura 15: Curva de adopción tecnológica cripto en la minería de la red de Bitcoin



Fuente: elaboración propia.

Ante el aumento de la demanda de criptomonedas, no solo por personas físicas sino por una acelerada adopción institucional, la rentabilidad por tenencia de Bitcoin ha venido demostrando mayores rendimientos que los mercados de valores. En la figura 16 se puede observar los rendimientos porcentuales durante el 2020, considerando que el último *halving* se produjo el 11 de mayo de dicho año.

Figura 16: Rendimiento de Bitcoin vs Oro vs SP500 en 2020

Fuente: Nasdaq.com.

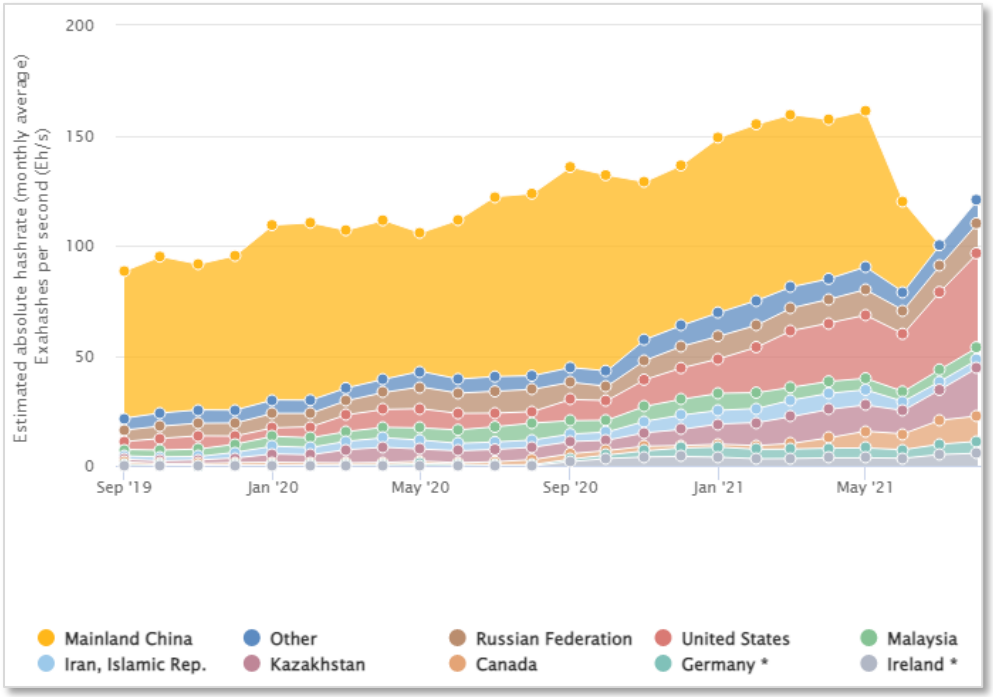
Estos resultados fueron detonantes para que muchos emprendedores/inversores se vean incentivados a pasar de la inversión directa, en la compra y venta de criptoactivos, a la indirecta, como la minería, con visión de largo plazo. Ya sea para la red de bitcoin como para cualquier otra red que permita generar ingresos a través de la minería. Tal es así que esta actividad ha tomado mayor popularidad principalmente en países emergentes donde la moneda doméstica pierde cada vez más valor, producto de las malas prácticas en materia económica y monetaria impulsada por los gobiernos y sus bancos centrales.

La minería a escala global

Actualmente existen aproximadamente diez mil *altcoins*, muchas de ellas con propuestas de valor totalmente diferentes, y su número seguirá crecimiento en tanto nuevos emprendedores decidan montar proyectos sobre esta nueva tecnología. En este sentido, la industria de las energías renovables, como mayor complemento y sustento a la criptominería, fue uno de los sectores que estuvo creciendo considerablemente. En parte, fue gracias a una de las críticas eternas contra bitcoin por su baja eficiencia energética en el minado. Sin embargo, lo que

pocos sabían era que, gran parte de ese consumo provenía de la energía hidroeléctrica, aprovechando la capacidad ociosa en países como China, que generaba más de 60% del *hashrate* mundial, hasta que en julio del 2021 decidió prohibir la minería y el uso de las criptomonedas en todo su territorio, favoreciendo el éxodo a otros países. Hoy el mayor porcentaje de las granjas de minería de bitcoin se concentran a nivel industrial, localizándose principalmente en Estados unidos, seguido por países como Rusia, Kazajistán, Malasia, Irán, Venezuela, entre otros (ver figura 17).

Figura 17: Evolución network hashrate



Fuente: Cambridge BTC Consumption Index.

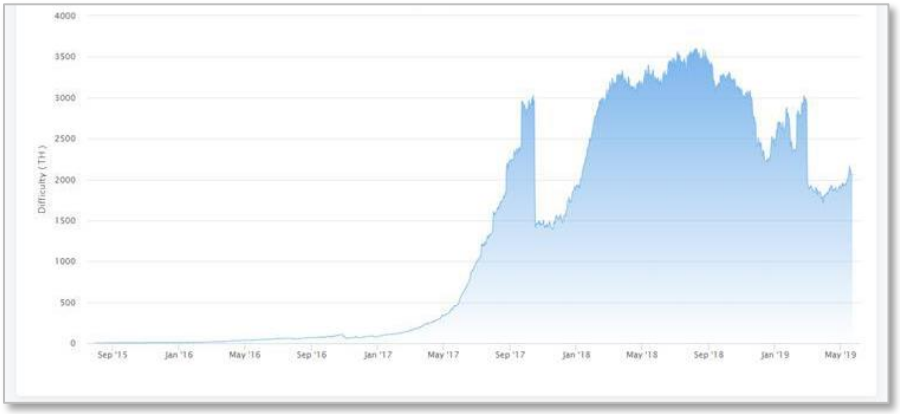
Alternativas de minería a la red de Bitcoin

Retomando con la historia y evolución de la criptominería, al comienzo, la dificultad del algoritmo de minería se encontraba en valores relativamente bajos y no se requería de hardware complejo para poder minar. Con el paso del tiempo, la adopción fue tan abrupta que se empezaron a requerir procesadores más potentes, como los ASICs, para poder compensar el salto de dificultad del algoritmo de minado. Si bien estos equipos se encuentran disponibles en el mercado, dado su elevado costo y requerimiento energético, los hacen poco atractivos para armar una granja de minería doméstica. Esto generó que muchos emprendedores independientes busquen otras alternativas de minería más económicas.

Breve repaso de la red de Ethereum y su adopción

A partir de 2015 con el nacimiento de ETH muchas personas han visto la minería de ETH como la mejor alternativa a Bitcoin. De la misma manera, el algoritmo de minería de Ethereum fue incrementando su dificultad, teniendo que pasarse de minar desde una simple CPU a procesadores más potentes como las GPUs. Cuando se trata de la dificultad de minería, la tendencia de aumentar su complejidad en el tiempo es similar para todas las redes por igual. Sin embargo, aun compartiendo la misma tendencia, como se puede apreciar en la figura 18, las propias variaciones que pueda atravesar la dificultad de minería dependerán intrínsecamente del desarrollo y evolución de cada proyecto.

Figura 18: Curva de dificultad Ethereum.



Fuente: Etherscan.io.

En este gráfico se puede extraer información enriquecedora observando como la dificultad de una criptomoneda, en este caso Ethereum, tiene fluctuaciones intrínsecas de la situación de su proyecto madre, pero también, como se mencionó al comienzo del capítulo, tiene una estricta correlación con el comportamiento de Bitcoin. El margen temporal seleccionado no es arbitrario, se tomó el periodo correspondido entre el segundo y tercer *halving* de Bitcoin. En octubre del 2017 pasó de 3k Tera *hashes* a 1,5k. Posteriormente, la dificultad fue aumentando durante el 2018 hasta llegar al pico de 3,6k Tera *hashes* en agosto del mismo año. En el 2019 la red también sufrió cambios drásticos al pasar de 3k Tera *hashes* en febrero a 1,7k a finales del mes de marzo. Estas fuertes variaciones se deben a que la red de Ethereum fue experimentando grandes cambios. Ahora, si hacemos un *zoom out*, se puede observar que la volatilidad desaparece mostrando dos escenarios totalmente distintos. En el primero, comprendiendo los dos primeros dos años posteriores al segundo *halving* de bitcoin, la

dificultad de minería de ethereum se mantuvo estable, y al acercarnos a la fecha del siguiente *halving*, la dificultad empieza a acelerarse alcanzando máximos históricos, pasando luego a un nuevo periodo de estabilización. Si uno se pone a analizar el *track record* de la dificultad de minería para todos los proyectos PoW mostrarán un patrón similar a descripto.

Actualmente el proyecto Ethereum se encuentra en un punto de transición, en algún momento de este año o el próximo, el equipo de desarrollo está planeando deshacerse de su algoritmo de prueba de trabajo y adoptar el protocolo *Proof-of-Stake* o "Prueba de Participación". Para lograr dicho cambio, ya se han desplegado las actualizaciones correspondientes en el sistema que permitirán allanar el camino. Una vez que esto ocurra, la red ya no necesitará que los mineros aseguren y confirmen la transacción, ya que esto lo harán los propietarios de los *tokens.* Los creadores de nuevos *tokens* serán elegidos de forma determinista, en función de su riqueza, que también se define como una apuesta. Lo más importante es que los mineros ya no recibirán recompensas en bloque, sólo cobrarán las cuotas de transacción. Por lo tanto, aquellos que deseen continuar minando en busca de recompensas podrían hacerlo en la versión antigua de Ethereum (ETH Classic) u otras *altcoins* disponibles. Sin una fecha fija para la actualización, es realmente difícil predecir cuán rentable puede ser entrar en la minería en ese momento.

Resumen

Siempre que uno mira los gráficos, Bitcoin es alcista a largo plazo y es la cadena que arrastra al resto de protocolos PoW, ya sea en la suba como en la baja. Nunca se debe olvidar que invertir en criptominería conlleva a asumir un riesgo que viene atado al propio desarrollo de cada cadena blockchain en cuestión. Lo importante, a fin de cuentas, es que cada minero evalúe lo que le resulte más conveniente y empezar a prepararse para el momento en el que Ethereum se convierta en una red sin minería o bitcoin alcance su próximo *halving*.

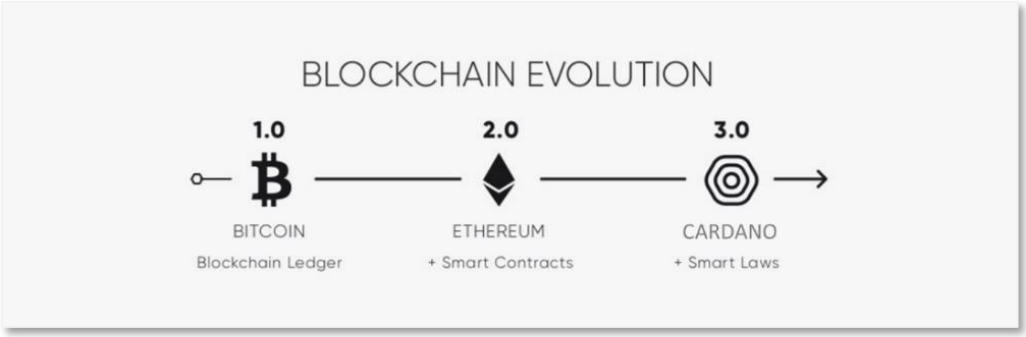
Lo importante es que, a nivel mundial, cada vez se registran más transacciones y transferencias en cripto activos, por lo que el valor de mercado a largo plazo continuará creciendo. Lo beneficioso para empezar a minar es que, en la actualidad, han bajado mucho los precios de los equipos de minería, lo que abre una buena oportunidad para entrar, siendo el valor completamente proporcional a la cotización de la moneda.

Capítulo 5. Blockchain de 3ra Generación

En los capítulos anteriores se hizo un repaso general de la historia y evolución de la minería basadas en las dos principales cadenas de bloques con mayor capitalización de mercado (Bitcoin 43% y Ethereum 15% a Julio 2022). Ambas cadenas representan las primeras generaciones de blockchain diseñadas con un algoritmo de consenso de prueba de trabajo. En el presente capitulo se explicará el estado de maduración actual de la tecnología blockchain, la cual se encuentra caracterizada por una constante adopción a protocolos de consenso alternativos como *proof of stake* en el diseño original de los nuevos proyectos que salen al mercado, haciéndonos preguntar que protocolos terminarán siendo predominantes en la validación de bloques y por consiguiente en modelo de negocio de la minería a adoptar.

Aunque la tecnología Blockchain tiene tan solo poco más de una década de existencia, para los expertos resulta práctico dividir por etapas su desarrollo histórico (ver figura 19), segmentándola en tres generaciones bien definidas (Platzi, 2020):

Figura 19: Generaciones blockchain



Fuente: Academia Platzi.

1er Generación: ledger distribuido

La primera etapa histórica de Blockchain corresponde a Bitcoin. En ese momento, Blockchain se estableció como un libro de contabilidad público compartido con el principal objetivo de soportar una red de monedas digitales. Bitcoin se creó para mejorar radicalmente el sistema financiero actual, permitiendo a las personas hacer transacciones directas entre ellos sin depender de una entidad centralizada. De esta idea inicial surgieron otras plataformas Blockchain con su propia criptomoneda nativa, como son el caso de Litecoin, Monero, Bitcoin Cash y otras.

2da Generación: smart contracts

Con el paso del tiempo, los desarrolladores empezaron a darse cuenta de que en la blockchain se podía hacer más que documentar y validar transacciones entre personas. Por eso empezaron a desarrollar nuevas funcionalidades hasta que surgió Ethereum, la segunda generación blockchain. La principal innovación que trae Ethereum a la mesa son los *smart contracts* o contratos inteligentes. Las blockchains de segunda generación introdujeron además el concepto de DApps o aplicaciones descentralizadas e hicieron posible la tokenización digital de activos físicos. Esto ha permitido la creación de nuevos productos como los protocolos de finanzas descentralizadas (DeFi), videojuegos NFTs y navegadores web. Pero eventualmente, el avance y la masificación de estas plataformas blockchains generaron discusiones en torno a las dificultades presentes como la escalabilidad, la sostenibilidad y la velocidad de las transacciones. Desde este horizonte, y con el objetivo de superar estos problemas, surgen las blockchains de tercera generación.

3ra Generación: escalabilidad e interoperabilidad

En resumen, la tercera generación de Blockchain busca resolver problemas específicos como la escalabilidad, la interoperabilidad, la sostenibilidad, la velocidad de transacción, los costos de envío, la eficiencia de la red, entre otras. Hoy estamos mirando a grandes posibilidades que pueden cambiar radicalmente la manera en la que usamos distintos productos: un modo más privado, más seguro y más descentralizado.

Características de las blockchain de tercera generación:

- **Escalabilidad:** la escalabilidad es el tema que ha estado ocupando a todos los desarrolladores desde el inicio de Bitcoin. El propio Satoshi Nakamoto dejó el tamaño de bloque de Bitcoin fijado en 1 MB temporalmente mientras se investigaban soluciones (en pro de la descentralización). Sin embargo, otras blockchains suprimen descentralización en busca de escalabilidad (trilema blockchain). Otra forma en que las blockchains de tercera generación consiguen más escalabilidad es mediante el sharding[13]. Una forma con más potencial que está siendo investigada, sobre la red de Ethereum, son las *rollups*[14]. A

[13] El ***sharding*** trata de un proceso de fragmentación de las bases de datos en partes o fragmentos más pequeños. El sharding se creó con la finalidad de permitir una mayor escalabilidad en sistemas distribuidos y descentralizados. Pero en la actualidad, su aplicación en la tecnología blockchain podría mejorar considerablemente los problemas de escalabilidad a los que se enfrentan redes como Bitcoin y Ethereum.

[14] Los ***rollups*** son una solución de escalado. Consisten en enrollar (de ahí el nombre) colecciones de transacciones. La transacción final, enrollada, se presenta a la cadena de bloques de Ethereum como una única transacción. Los rollups reducen los costes: el coste de una transacción de Ethereum, más el pequeño coste de

diferencia del *sharding*, las *rollups* pueden considerarse soluciones de segunda capa. Otras soluciones de segunda capa son Plasma (usada en Polygon), *Lightning Network* (sobre todo usada en Bitcoin) y las *sidechains*.

- **Sostenibilidad:** en general se usa el *Proof of Stake (PoS)* para tener un consumo mínimo de la red. En PoS, los mineros son grandes *holders* de la moneda y no les interesa atacar la red ya que podría tener un efecto negativo sobre su precio. El *tradeoff* de esto es que se tiende a la centralización. Los mayores *holders* de una moneda son los que más recompensas ganan haciendo *staking*. Por esta simple teoría de juegos se produce una presión hacia la centralización del suministro. Otro protocolo de consenso destinados a reducir el consumo energético son el *Proof of Space and Time* de Chia (explicado en el siguiente capitulo).
- **Velocidad:** Los sistemas PoS generan mayor velocidad de transacción (confirmaciones rápidas). Aunque nuevamente, con su lado negativo de menores garantías de seguridad. Otra forma de mejorar la velocidad de las transacciones es el modelo de microbloques usado en *stacks*, e incluso las soluciones de segunda capa.
- **Interoperabilidad:** En una red de blockchains, como todo apunta que en el futuro será el internet del valor, la interoperabilidad y estandarización entre diferentes cadenas serán necesarias. Según *Binance Academy, Multichain*, en su visión por convertirse en el "enrutador definitivo en Web3", ofrece una de las mayores selecciones de *tokens* trasladables. Al aumentar la interoperabilidad, *Multichain* facilita el traslado entre DApps y todo el ecosistema de tecnología blockchain. Con la interoperabilidad como un pilar de Web3, parece que *Multichain* será una parte importante para que esto suceda.

El futuro del Internet del Valor

Actualmente todos los datos apuntan a que el futuro del Internet del Valor será conformado por diferentes blockchains y activos (multichain). Muchos no pasarán la prueba del tiempo y otros seguramente perdurarán al encontrar un nicho de mercado.

Resumen

enrollar lotes de transacciones, se divide entre los usuarios. También aceleran las cosas: el rollup es muy rápido de realizar y la blockchain de Ethereum sólo necesita procesar una única transacción en lugar de muchas.

Tanto Bitcoin como Ethereum se han establecido en sus respectivos nichos, pero este último ha ganado muchos competidores que prueban diseños diferentes para imponerse con la *mainnet* del mercado. Lo más posible es que Ethereum 2.0 siga consolidándose al mismo tiempo que sus competidores ganen terreno. Cuando todas estas tecnologías hayan madurado, tendremos una consolidación de las cadenas supervivientes. Como analogía podemos decir que estamos en los años 90 de Internet, viviendo un momento histórico de experimentación tecnológica que las próximas generaciones podrán estudiar sus resultados.

Metodología de la investigación

La siguiente investigación responde un estudio de tipo descriptivo, que busca especificar las propiedades y atributos de "La Criptominería como modelo de negocio", caracterizarla y medirla de alguna forma apropiada para su evaluación, permitiendo realizar predicciones basados en modelos no probabilísticos.

La metodología utilizada se basa en un enfoque cuantitativo para analizar la rentabilidad del modelo, y de un enfoque cualitativo para evaluar posibles alternativas de inversión. Aplicando razonamiento inductivo se llegará a una conclusión que permita responder a la pregunta planteada como objetivo principal del proyecto.

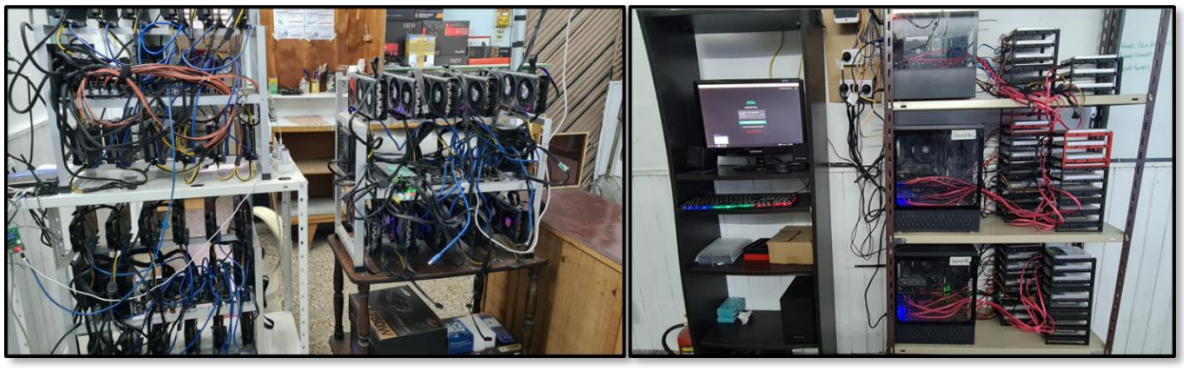
La información analizada se nutre de fuentes de datos primarios a través de observaciones directas y de fuentes de datos secundarios como análisis de contenido de entrevistas y datos públicos de mercado.

Trabajo de campo

Capítulo 6. Minería doméstica

La minería de cripto activos puede analizarse desde distintas dimensiones en base a su alcance y tamaño. En el presente trabajo se abordará desde el punto de vista del negocio, comenzando por la minería doméstica y luego se pasará al formato industrial. En este capítulo se expondrá el trabajo de campo presentando la información generada de la propia experiencia adquirida durante el período oct/2020~mar/2022 utilizando algoritmos de minería de distintas cadenas, principalmente Ethereum y Chia Network bajo el formato de criptominería doméstica (ver figura 20).

Figura 20: Mineros de Ethereum / Farmers de Chia Network



Fuente: elaboración propia.

A continuación, se describirá el cronograma y requerimientos necesarios para llevar a cabo la construcción de una granja de minería doméstica, a modo de ejemplo de cómo se puede desarrollar un proyecto de criptominería a escala personal. También se mencionarán los hitos que afectaron al proyecto y propusieron cambios de estrategia. Por último, se presentarán los cuadros de resultado y conclusiones finales.

Ethereum:

El proyecto fue iniciado en septiembre de 2020 localizado en Caba, Argentina. Los lineamientos a seguir fueron en base a las premisas explicadas en el capítulo anterior. Se comenzó con la selección del *altcoin* a minar. En base a los requerimientos de equipos, infraestructura, acondicionamiento y consumo eléctrico se decidió optar por adquirir equipos para la minería de ETH. Si bien era sabido que ETH iba a cambiar de protocolo de consenso

de PoW a PoS, se consideraba que, llegado el momento del "*Merge*"[15], esos mismos equipos podrían continuar con su vida útil minando otras *alcoins* alternativas, principalmente ETC[16] por considerarse la *altcoin* alternativa con mayor rendimiento económico al momento del estudio.

Análisis preliminar Ethereum:

Los cálculos preliminares (ver figura 21) para construcción de una granja de dos Rig de minería de Ethereum indicaban un periodo de recupero de la inversión de 12 meses con un ROI mensual del 8% (seteando el precio de ETH en 500usd y el costo eléctrico en 0,045usd/Kwh).

Figura 21: Análisis preliminar sep/2020

	ETH/USD	500
Costo Inversion aprox. (ARS)	*800.000*	*1.200.000*
Costo Inversion aprox. (USD) ex.164ARS/USD	**4.878**	**7.317**
CANTIDAD GPUs	12	12
MODELO GPU	AMD XR 580	AMD RX 5700XT
MH/s	**30**	**53**
MH/s x 12 placas	360	636
ETH daily 100MHS/s	**0,00772949**	
ETH diarios	0,028	0,049
ETH monthly	**0,835**	**1,475**
Usd monthly	**417,392**	**737,393**
Consumo xGPU - W	**96**	**125**
Consumo TTL GPU - W	1.146	1.500
Consumo RIG general - W	300	300
Consumo TTL - W	**1.446**	**1.800**
Consumo electrico mensual - kWh	1.041	1.296
Costo electrico - usd/kWh	0,045	0,045
Costo eléctrico mensual - Usd	**46,85**	**58,32**
Consumo - A	*6,57*	*8,18*
Consumo TTL - A		*14,75*
Utilidad neta diaria (USD)	**12,35**	**22,64**
Utilidad neta mensual (USD)	**370,54**	**679,07**
ROI mensual USD	**7,60%**	**9,28%**
Payback (MESES)	**13,16**	**10,78**
Utilidad neta mensual Compuesta (USD)		**1.049,62**
Payback compuesto (MESES)		**11,62**

Fuente: elaboración propia.

Hardware:

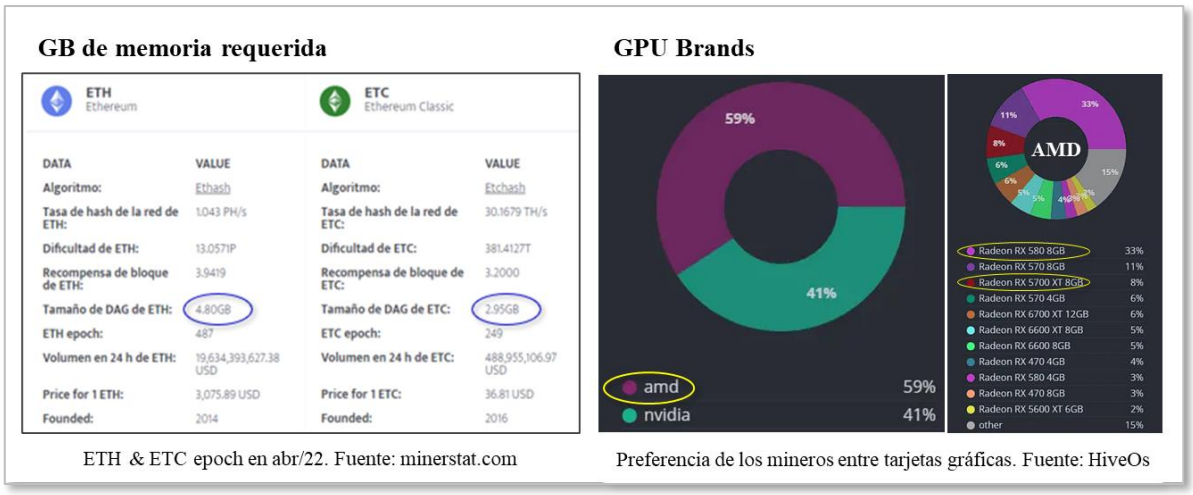
A diferencia de Bitcoin, cuyos equipos de minería más eficientes han alcanzado el nivel de ASICs, en Ethereum se utilizan GPUs (unidades de procesamiento gráfico). Para su selección entre todo el universo de marcas y modelos existentes, se priorizaron tres criterios: precio y disponibilidad, eficiencia energética (mayor *hash* entregado por kWh de consumo) y cantidad

[15] https://ethereum.org/en/upgrades/merge/

[16] Ethereum Classic (ETC) es una es una bifurcación dura de Ethereum (ETH) que se lanzó en julio de 2016. Su objetivo principal es funcionar como una red de contratos inteligentes, con la capacidad de alojar y admitir aplicaciones descentralizadas (DApps). Su token nativo es el ETC. https://ethereumclassic.org/

de memoria, priorizando GPUs con más de 4GB de memoria[17]. Utilizando los criterios mencionados se decidió avanzar con dos tipos de tarjetas gráficas (1) AMD Radeon RX 580 8GB y (2) AMD Radeon RX 5700XT 8GB persiguiendo el objetivo de todo minero, encontrar la mejor relación entre bajo costo y alta cantidad de trabajo (ver figura 22).

Figura 22: Criterios de selección de GPUs para minería de ETH



ETH & ETC epoch en abr/22. Fuente: minerstat.com

Preferencia de los mineros entre tarjetas gráficas. Fuente: HiveOs

Fuente: Minerstat.com (izq) / HiveOS (der).

Infraestructura:

En caso de no disponer de una locación para instalar los equipos, se deberá considerar el costo de alquiler o *housing* en el cálculo de rentabilidad. Para el presente caso de estudio se cuenta con un local propio de 3x3x5m (ver figura 23), en el cual se realizaron las siguientes actividades de acondicionamiento antes de instalar los equipos:

- Acondicionamiento el inmueble tapando todas las posibles entradas de polvo. Para extender la vida útil de los equipos se debe garantizar un ambiente seco y libre de polvo[18].
- Aislamiento térmico. Las paredes vidriadas se cubren con film polarizado y se recubren con membranas aluminizadas con aislante térmico. El control de temperatura ambiente es una condición necesaria para mantener los equipos funcionando. En caso de superar el umbral de temperatura ambiente de 35°, o de funcionamiento de 70° para los

[17] Según la velocidad promedio de producción de bloques en Ethereum y Ethereum Classic (12 segundos por bloque), el DAG epoch cambia cada cinco días, aproximadamente

[18] Las GPUs generan un campo electroestático que atrae las partículas de polvo con cargas negativas. La acumulación de estas partículas en la placa genera un aumento de temperatura pudiendo afectar el correcto funcionamiento de las mismas.

procesadores y 85° para las memorias, se corre el riesgo de fallas que pueden detener el equipo, o en los peores casos, poner en riesgo todo el sistema.

- Otro trabajo prioritario que se debió realizar previo a la instalación de los mineros fue el de robustecer todo el sistema eléctrico, colocando cables con un diámetro superior a la potencia requerida considerando un factor de seguridad del 15%. Asimismo, se colocó una llave térmica independiente por cada equipo de minería con el fin de seccionar las fallas eléctricas y un disyuntor central. También se instala una jabalina para proteger los equipos de posibles descargas mecánicas.

Figura 23: Infraestructura

Fuente: elaboración propia.

- Por último, se instala un monitor de consumo eléctrico (ver figura 24) para poder visualizar en tiempo real el consumo de los equipos. Esto permite anticiparse ante una posible sobrecarga del sistema y, por otro lado, llevar el control del principal componente de los costos operativos del negocio. De esta manera se podrá trabajar proactivamente buscando mejorar el rendimiento de los equipos.

Figura 24: Sistema de monitoreo de consumo eléctrico

Fuente: elaboración propia.

Refrigeración:

- Ventilación forzada.

Se diseña y ejecuta un circuito de ventilación forzada para mantener la temperatura ambiente dentro de los parámetros necesarios y mantener bajo el consumo energético. Se realizan aberturas inferiores (cubiertas por filtros de aire) en un extremo del local para que ingrese aire fresco del exterior, luego se colocan ventiladores fijos apuntando a cada minero forzando el flujo de aire a través de ellos y por último se colocan extractores en la parte superior de local para forzar la expulsión del aire caliente. Este esquema de ventilación forzada es aplicable de abril hasta mediados de noviembre. En épocas de altas temperaturas se debe recurrir a un sistema de refrigeración más potente.

- Sistema de refrigeración.

Se instala un aire acondicionado de 4.500 frigorías para que actúe en época de verano. Su requerimiento energético medio se midió en 1.700W generando un consumo de 8A. Su régimen de funcionamiento está seteado 24x7 desde mediados de noviembre hasta fines de marzo. Se deberá contemplar el costo de mantenimiento preventivo una vez finalizado su periodo de puesta en marcha.

Estrategia:

Para aquellos que deseen comenzar a minar criptomonedas debe estar consciente que las rentabilidades que ofrece este negocio pueden resultar más volátiles que los modelos de negocios tradicionales. Como se mencionó en el capítulo anterior, la acelerada adopción institucional que sufrió la blockchain de Ethereum a finales del 2020, sumando al crecimiento acelerado en la utilización de plataformas de finanzas descentralizadas (ej. Uniswap, Curve, etc.) en el primer semestre del 2021 y el boom de los Play to earns (ej. Axe Infinity) y el

mercado NFT (ej. Open Sea) hicieron aumentar exponencialmente el tráfico y uso de la red, provocando un aumento en los costos de transacción y valorización de su *token* de gobernanza (ETH), mejorando radicalmente los ingresos de los mineros. Este escenario permitió mejorar todos los números calculados en el preanálisis de rentabilidad, llevando de 12 a 8 meses el payback y de 8% a 12% el ROI mensual. Tal es así que a partir del cuarto mes operativo (fines de febrero 2021) se decide invertir en un Rig de minería adicional de 520MH/s (ver figura 25). La decisión se tomó asumiendo que el período de repago era menor al tiempo que restaba para alcanzar el Merge de ETH, estimado para mediados del año 2022.

Figura 25: Análisis preliminar feb/2021

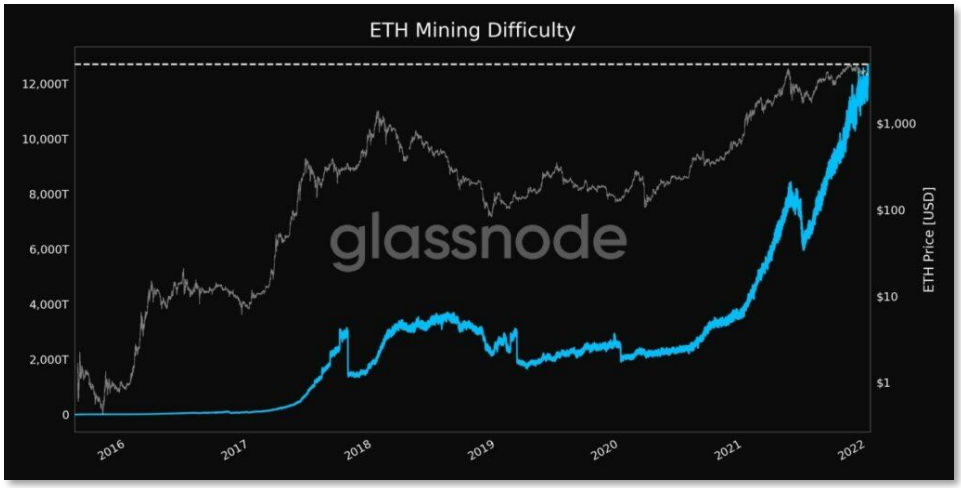
	ETH/USD	1.418,00
	Costo Inversion aprox. (ARS)	*2.650.000*
Costo Inversion aprox. (USD) ex.149ARS/USD		**11.073**
	CANTIDAD GPUs 10	
	MODELO GPU	AMD RX 5700XT-XFX
MH/s		**53**
MH/s x 12 placas		530
ETH daily 100MHS/s		**0,006**
ETH daily		0,032
ETH monthly		**0,954**
USD monthly		**1.352,77**
Consumo xGPU - W		**115**
Consumo TTL GPU - W		1.150
Consumo RIG general - W		300
Consumo TTL W		**1.450**
Consumo electrico mensual KWh		1.044
Colsto electrico - USD/kWh		0,045
Costo eléctrico mensual		**46,98**
	Consumo TTL - A	*6,59*
Utilidad neta diaria (USD)		**43,53**
Utilidad neta mensual (USD)		**1.305,79**
ROI mensual USD		**11,79%**
Payback (MESES)		**8,48**

Fuente: elaboración propia.

Esta decisión no fue al azar, existía un desfasaje entre la conformación de precios del hardware y la rentabilidad que ellos mismos generaban. El efecto del *bullmarket* fue tan rápido que la corrección de precio tardo unos meses en llegar. Con el diario de hoy se podría decir que fue la última ventana de entrada para acceder a la criptomineria de ETH con precios de hardware que ofrecían un *payback* menor a un año. Después de marzo del 2021 ya todo había cambiado, tanto a nivel local, donde la oferta de proveedores de rig de minería se masifico por todo el país, como a nivel internacional donde el *hashrate* de ETH no paro de crecer. Desde entonces el ingreso de nuevos mineros a la red no ha dejado de crecer y la

dificultad de minado no paro de subir, alcanzando un *ATH (All Time High)* o punto más alto histórico en enero del 2022 (ver figura 26).

Figura 26: Evolución de la dificultad de minería y precio de ETH



Fuente: Glassnode.

En este negocio también es importante conocer los ciclos del mercado para entender el movimiento del precio del *token* a minar. Pero si se desea tener una mayor proyección a largo plazo, es fundamental monitorear el *roadmap* (ver anexo II: ETH 2.0 Roadmap) del proyecto y las comunicaciones oficiales que hagan sus CEOs y desarrolladores (ver figura 27). Como se mencionó en el capítulo anterior, cada hito de proyecto podría estar marcando la antesala de un evento de corrección en los precios de su *token* de gobernanza.

Figura 27: Tweet de Vitalik Buterin (CEO Ethereum) sobre el RoadMap de ETH2.0

Fuente: Twitter.

Por definición, la dificultad de la minería mide cuán complejo es el problema matemático que los mineros deben resolver para encontrar la identificación de un bloque y minarlo, actividad con la cual obtienen recompensas, en este caso, en ethers. La dificultad de la minería de ETH responde a la propia protección de la red que, ante la llegada de más mineros, hace más difícil la actividad, como una política de emisión que mantiene segura a la blockchain. Esto, al mismo tiempo, se traduce en más competencia para los mineros. Cabe mencionar que antes de llegar a Ethereum 2.0, se debe producir *The Merge* (fusión) que supone una transición del algoritmo de PoW al de Prueba de Participación (PoS). En ese momento, explotará la bomba de dificultad, que literalmente limitará la minería de ETH y hará que la red entre en una suerte de "era de hielo", que finalizará una vez se haya completado el cambio.

Al ingresar a la criptominería es importante establecer una estrategia de entrada y de salida, permitiendo capitalizar la mayor cantidad de ganancia durante el proceso. Tal es así que, luego de abril 2021 donde el precio de las GPUs se había encarecido en promedio un 160% (ej. AMD Radeon RX 5700XT paso de valer 800usd en oct/2020 a 2.075usd en jun/2021), seguir invirtiendo en Rigs de minería por GPU no sería un buen negocio. Es aquí donde muchas veces la miopía del negocio puede llevar a malas decisiones. Lo mejor que uno podría hacer, si uno decide continuar inmerso en este negocio, es readaptar la estrategia continuamente haciendo referencia al famoso ciclo PDCA.

Tal fue así que se volvió a analizar en que estadio se encontraba cada proyecto vigente para ver si se podía encontrar una nueva ventana de entrada "rentablemente atractiva". Para entonces se estaba presentando un nuevo proyecto criptográfico llamado Chia Network[19]. Lo novedoso de Chía era que cambiaba el concepto de "*Minning*" por "*Farming*", es decir, que pasaba de la minería a través de un consenso PoW caracterizado por poder de cálculo y consumo eléctrico, a la de "cosechado" utilizando un algoritmo de conceso basado en «Prueba de espacio y tiempo» (Pietrzak, 2009). Otro atractivo que aportaba Chia Network para el momento, donde las criticas medioambientales al consenso PoW estaban tomando impulso, era que este protocolo no requería de alto poder computacional para validar nodos en el sistema, sino que utilizaba un mecanismo de votación utilizando hardware con capacidad de almacenamiento como los discos rígidos. Estaba naciendo un nuevo proyecto

[19] https://www.chia.net/

de criptominería con el slogan de ofrecer una red descentralizada y segura como bitcoin, pero más económica y limpia, reduciendo significativamente en un 95% la energía requerida para sostenerse. Por lo tanto, el algoritmo de consenso de Chia tiene como objetivo crear una alternativa descentralizada, segura y respetuosa con el medio ambiente a la prueba de trabajo y la prueba de participación.

Chía Network

Los algoritmos de consenso descentralizados requieren de un mecanismo de protección frente a un ataque Sybil[20], con un recurso que es criptográficamente verificable y escaso (no infinito). En los sistemas blockchain anteriores, los recursos escasos eran la potencia de cálculo y la participación. La prueba de espacio es una alternativa que se acerca mucho más al ideal original de Bitcoin de "una CPU por voto" al utilizar la capacidad de almacenamiento como recurso escaso. Por ejemplo, si alguien almacena 500GiB tiene 5 "votos", alguien que almacena 100GiB tiene 1 "voto"", donde un voto se refiere a la posibilidad de ganar y validar un bloque, no un voto real en una cadena. Sin embargo, utilizar solo la capacidad de almacenamiento no es seguro. Para sumar mayor seguridad al sistema se suma otra pieza al rompecabeza criptográfico, una función de retardo verificable, que es una prueba criptográfica del tiempo real que ha transcurrido. Creando un sistema justo combinando pruebas de espacio y tiempo.

En tal sistema, los usuarios almacenan aleatoriamente, buscando datos en sus discos duros durante períodos de tiempo y su oportunidad de ganar Chías es proporcional a su espacio asignado. Además, dicho sistema se escala a miles de millones de participantes de manera similar a la lotería de prueba de trabajo. No se requieren fondos, hardware especial, registro o permiso para unirse, solo un disco duro. Y el sistema es completamente transparente y determinista: cualquiera puede verificar de manera eficiente y objetiva qué cadena es genuina.

Análisis preliminar Chia Network:

[20] Un Ataque Sybil hace referencia a cuando un sistema es vulnerado por una entidad que controla dos o más identidades distintas en una red. Es decir, cuando una persona controla dos o más puntos que se suponen pertenecen a personas o identidades distintas. El nombre de Ataque Sybil proviene del libro "Sybil", una obra de la conocida escritora Flora Rheta Schreiber. En dicho libro, se habla de Sybil Dorsett, una joven que sufre del trastorno de identidad disociativa (TID), un trastorno psicológico que lleva a una persona a crear varias identidades distintas de sí misma. Fuente: bit2me ACADEMY.

Los cálculos preliminares (ver figura 28) para construcción de una granja de tres "farmers" de Chia indicaban un periodo de recupero de la inversión de 14,5 meses con un ROI mensual del 6,8% (seteando el precio de XCH en 211usd y el costo eléctrico en 0,045usd/Kwh).

Figura 28: Análisis preliminar XCH Jun/2021

Costo Inversion aprox. (ARS)	*2.700.000*
Costo Inversion aprox. (USD) ex.164ARS/USD	**16.463**
Plot Size (TiB)	**0,10887742**
TiB	**0,90949470**
XCH/10TB	**0,0026**
XCH Price	**211**
TB	700
Plots	5.847
XCH/día	0,182
XCH/mes	5,460
Usd/mes	1.152,060
Consumo electrico mensual - kWh	504
Costo electrico - usd/kWh	0,045
Costo eléctrico mensual - Usd	**22,68**
Utilidad neta mensual (USD)	**1.129,38**
ROI mensual USD	**6,86%**
Payback (MESES)	**14,58**

Fuente: elaboración propia.

Equipamiento:

Chía fue un proyecto que genero mucho FOMO (*Fear of missing out*) en los emprendedores. Apenas se dio a conocer el anuncio de su lanzamiento, el mercado de discos rígidos empezó a escasear. Fue complejo conseguir proveedores que ofrezcan discos de gran capacidad y precios accesibles. Para minar ChiaCoin se requiere de unidades de almacenamiento, preferentemente discos rígidos de gran capacidad, una PC para gestionarlos y algunos componentes adicionales.

ChiaCoin se genera «cultivando» o haciendo «*farming*» mediante archivos de parcelas, llamados «*plots*», que se almacenan en disco duro. Una vez creados los *plots* el propietario va ganando monedas ChiaCoin con un mínimo consumo de energía y recursos del ordenador (procesador, memoria, ancho de banda). Las ganancias calculadas en la figura 28 supone que los discos se encuentran llenos de plots (1 plot = 0,10887742TiB), sin embargo, hay un delay entre la generación de *plots* y el inicio del proceso de *farming*. Cada *plot* tarda 1 hora en generarse, por lo tanto, para llenar un disco de 18TB se requieren de 11 días aproximadamente. Por tal motivo se decidió repartir los 700TB en tres equipos independientes para reducir el tiempo de ploteado y anticipar el inicio del farming.

Los discos seleccionados fueron WD Purple y Seagate Skywalk de entre 8 y 18TB de capacidad dado que están diseñados para un uso continuo con mayor vida útil que los discos tradicionales (ver figura 29).

Figura 29: Unidades de farmeado Chia Network

Fuente: Proveedores de mercado.

Infraestructura:

La infraestructura requerida para utilizar estos equipos no es compleja, dado su bajo consumo eléctrico y emisión térmica. Para su instalación se utilizó la misma locación que los Rigs de minería de ETH. En la siguiente figura se puede observar la instalación de los tres farmers de Chia Network.

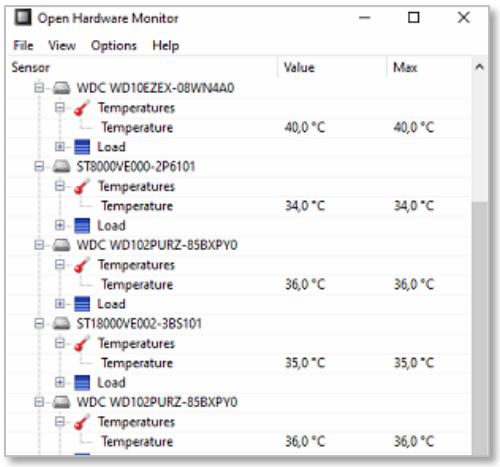
Figura 30: Farmers de Chia Network

Fuente: elaboración propia.

Refrigeración:

La refrigeración para estos equipos no resulta ser un requerimiento clave para su correcto funcionamiento, pero si se desea extender la vida útil de las unidades de almacenamiento será necesario mantener la temperatura de los discos por debajo de los 55°C. Para ello se puede utilizar diversos tipos de software gratuitos que permitan monitorear en tiempo real la temperatura de los discos (ver figura 31). En caso de requerir refrigeración puede utilizarse un ventilador para forzar flujo de aire fresco a través de ellos, o colocar *cooler fans* directamente en el hardware.

Figura 31: Software de monitoreo de dispositivos



Fuente: Open Hardware Monitor.

Estrategia:

El 19 de marzo de 2021 se lanzó la *mainnet*, una versión ya operativa de la blockchain de Chia Network, donde se podía empezar a minar. Las transacciones de Chia se habilitaron el 3 de mayo de 2021, listándose también en algunas *exchange* con el nombre Chia Network y el símbolo XCH. Como se mostró en el análisis preliminar, la rentabilidad esperada para Chia Network era de 7% mensual a un precio de XCH = 211USD. Sin embargo, el precio de Chia no ha parado de caer desde su creación (ver figura 32). Esto es entendible debido a que cualquier nuevo proyecto genera una expectativa de precio de mercado superior a su valor real. La volatilidad en estos estadios de proyecto siempre termina siendo tormentoso para los inversores. Habrá que ser paciente hasta que el proyecto madure y encuentre un período de lateralización hasta consolidarse dentro de un rango de precio determinado. Recién en ese momento podemos decir que el mercado encuentra la calma.

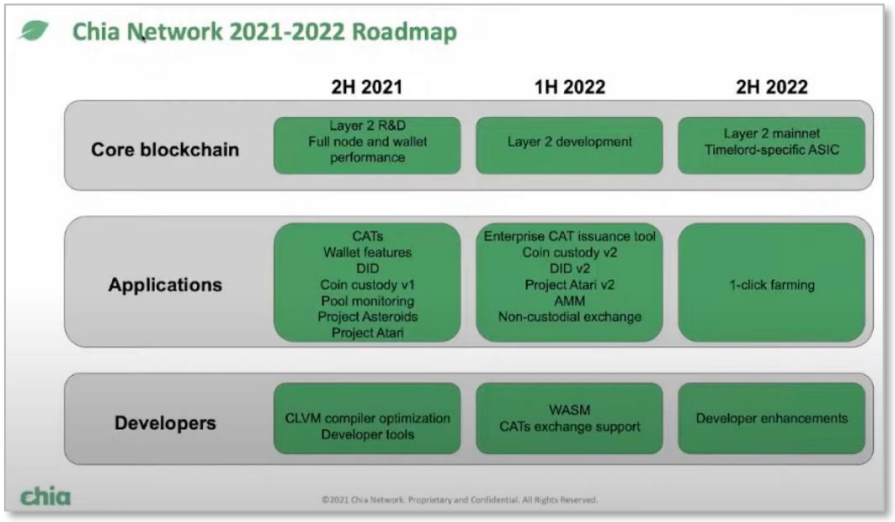
Figura 32: Historio de precio XCH a USD

Fuente: CoinmarketCap.

Finalmente, la rentabilidad proyectada cayó de un 6,8% mensual a 2%. En estos casos es conveniente, dada la falta de madurez del proyecto, en establecer una estrategia de *holdear*, manteniendo resguardadas las criptomonedas ganadas y esperar a que su precio vuelva a recuperar valor para poder venderlas en el mercado. Potencialmente esto podría ocurrir cuando XCH se liste en Binance y Coinbase, las dos *exchange* con mayor volumen de intercambio del mercado.

Como es harto conocido, el precio de un activo se rige por la puja de mercado entre la oferta y la demanda, pero si se desea saber si la inversión en un proyecto fue acertada, debemos regirnos por la propuesta de valor intrínseco que posee el proyecto y no tanto en el mercado. Para el caso de Chia, el proceso de evaluación del proyecto es similar al mencionado anteriormente. Se deberá seguir los anuncios oficiales de sus desarrolladores, verificar que las fechas y objetivos establecidos en el *roadmap* se cumplan (ver figura 33), analizar la evolución y el tamaño de la comunidad en Twitter, Reddit y otras redes sociales, etc.

Figura 33: Chia Network roadmap, publicado el 23/09/21



Fuente: Chia Network.

Chía es un proyecto dinámico, que muestra fortalecerse con el paso del tiempo, ha venido desarrollando partnerships estratégicos con proveedores, bancos y Estados, profundizando el desarrollo de la red e incorporando mayor seguridad y features de uso. Su desarrollador Brah Cohen ha anunciado su interés de emitir un IPO en el futuro próximo (ver Anexo III: Chia Network Future Roadmap).

El propósito de esta continua evaluación de los estadios de proyecto permitirá anticipar movimientos bruscos de precio al alza o a la baja que puedan ir en contra o validar la estrategia establecida. Al final de todo, como mineros, se querrá maximizar la inversión.

Resultados:

A continuación, se presentarán los resultados obtenidos durante el periodo bajo estudio para una granja de minería domestica compuesta por el siguiente equipamiento, potencia de minado, consumo energético y red blockchain (*altcoin*) seleccionada:

- ***Mineros de Ethereum***

  Miner #1 - 6 GPU AMD 580 - Pot. 1.148W - 338,4MH/s

  Miner #2 - 12 GPU AMD XR 5700XT - Pot. 1.295W - 624,4MH/s

  Miner #3 - 10 GPU AMD XR 5700XT - Pot. 1.104W - 519,9MH/s

- ***Farmers de Chia Network***

  Farmer #1 - 19 HDD - 2.618 Plots - Pot. 396W - 286TB

  Farmer #2 - 19 HDD - 2.544 Plots - Pot. 396W - 278TB

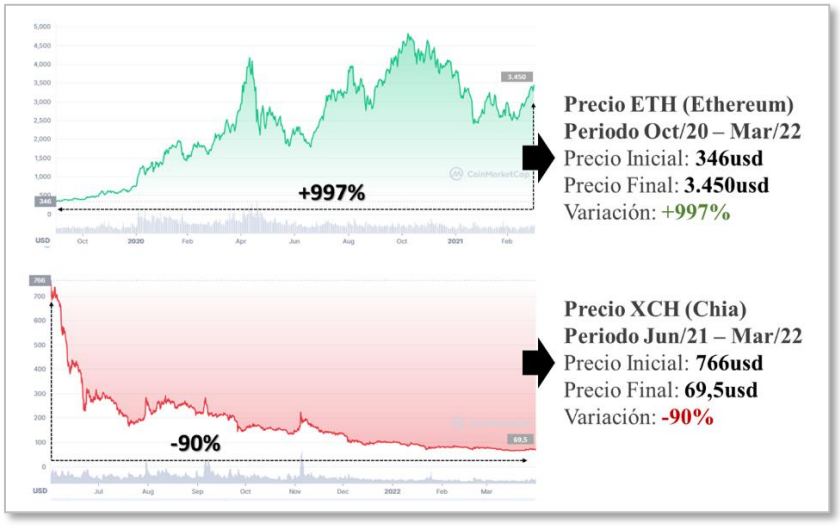
Farmer #3 - 9 HDD - 1.227 Plots - Pot. 188W - 134TB

Memoria técnica

En la figura 35 se presenta el cuadro de resultados económicos obtenido por la granja de minería doméstica en el periodo bajo estudio (Oct/20 a Mar/22). Se puede observar que durante los 17 meses analizados se logró recuperar la inversión inicial de 39.731USD en capital de trabajo, representado por #6 equipos de minería (#3 para la red de Ethereum y #3 para la red de Chia Network). La rentabilidad Bruta fue de 45.671USD (43.107,26USD de ETH / 2.564USD de XCH) y los gastos operativos (costo eléctrico) de 2.976,04USD representando el 7% de los ingresos generados. Estos resultados terminaron arrojando un saldo de rentabilidad Neta de 40.131USD, cuyo ROI para los primeros 17 meses fue de 101%, alcanzando un retorno mensual medio de 8,8%.

Para este análisis se tomó en cuenta las condiciones de trabajo de los equipos, es decir, el tiempo real que las maquinas se mantuvieron encendidas y operativas, habiendo logrado una eficacia aproximada del 89%. Esta merma se originó debido a diferentes factores como cortes en el suministro eléctrico y de internet, fallas o roturas en el hardware, como así también problemas originados por desconfiguración o desactualización en el software. Por último, también se llevó a cabo el monitoreo mensual de las variaciones de precios de las criptomonedas (ver figura 34) que permitió definir los momentos clave de venta para maximizar la rentabilidad de los equipos.

Figura 34: Variaciones de precio de ETH y XCH



Fuente: CoinmarketCap.

Figura 35: Cuadro de resultados consolidado

Período analizado: octubre 2020 a marzo 2022.

Blockchain (Altcoin)	Equipo	Inversion	Inversion Acc	Month	Year	ETH Mined	Price Close	vPM	Gross Profit usd	Miners #1 #2 #3	XCH Farmed	Price Close	vPM	Profit usd	Farmers #1 #2 #3	Expenses usd	Net Profit	ROI
Ethereum	Miner #1	4.878	4.878	10	2020	-	500,00	0,0%	-	✕ ✕ ✕	-	-	-	-	✕ ✕ ✕	-	-	-
Ethereum	Miner #2	7.317	12.195	11	2020	0,367	615,92	23,2%	226,17	● ✕ ✕	-	-	-	-	✕ ✕ ✕	87,45	138,71	1,14%
-	-	-	12.195	12	2020	1,394	735,94	19,5%	1.026,16	● ◐ ✕	-	-	-	-	✕ ✕ ✕	91,70	934,47	7,66%
-	-	-	12.195	1	2021	1,564	1.312,73	78,4%	2.053,14	● ● ✕	-	-	-	-	✕ ✕ ✕	145,38	1.907,76	15,64%
Ethereum	Miner #3	11.073	23.268	2	2021	2,126	1.418,76	8,1%	3.016,68	● ● ✕	-	-	-	-	✕ ✕ ✕	159,04	2.857,63	12,28%
-	-	-	23.268	3	2021	1,792	1.917,99	35,2%	3.436,48	● ● ◐	-	-	-	-	✕ ✕ ✕	202,94	3.233,55	13,90%
-	-	-	23.268	4	2021	1,897	2.772,78	44,6%	5.261,34	● ● ●	-	-	-	-	✕ ✕ ✕	212,97	5.048,37	21,70%
-	-	-	23.268	5	2021	1,667	2.708,47	-2,3%	4.515,76	◐ ● ●	-	-	-	-	✕ ✕ ✕	217,87	4.297,89	18,47%
Chia Net.	Farmer #1	5.488	28.756	6	2021	1,100	2.273,84	-16,0%	2.500,26	● ● ●	0,10	291,81	0,0%	29,22	● ✕ ✕	206,85	2.293,40	7,98%
Chia Net.	Farmer #2	5.488	34.243	7	2021	1,219	2.532,19	11,4%	3.086,63	● ● ●	0,63	265,38	-9,1%	166,06	● ● ✕	200,50	2.886,13	8,43%
-	-	-	34.243	8	2021	1,102	3.430,74	35,5%	3.781,47	● ● ●	1,31	222,00	-16,3%	291,19	● ● ✕	202,55	3.578,92	10,45%
Chia Net.	Farmer #3	5.488	39.731	9	2021	0,752	3.000,59	-12,5%	2.256,92	◐ ◐ ●	1,55	149,80	-32,5%	232,31	● ● ●	188,62	2.068,30	5,21%
-	-	-	39.731	10	2021	0,815	4.287,56	42,9%	3.496,09	● ● ●	2,18	145,42	-2,9%	317,63	● ● ●	188,21	3.307,88	8,33%
-	-	-	39.731	11	2021	0,461	4.628,90	8,0%	2.131,74	● ● ●	2,43	136,64	-6,0%	331,37	● ◐ ●	163,53	1.968,21	4,95%
-	-	-	39.731	12	2021	0,541	3.677,85	-20,5%	1.988,10	● ● ●	3,73	99,04	-27,5%	369,87	● ● ●	169,74	1.818,36	4,58%
-	-	-	39.731	1	2022	0,464	2.686,82	-26,9%	1.247,50	◐ ◐ ◐	3,34	80,82	-18,4%	269,69	◐ ◐ ◐	164,81	1.082,69	2,73%
-	-	-	39.731	2	2022	0,469	2.922,50	8,8%	1.371,44	● ● ●	4,20	78,26	-3,2%	328,44	● ◐ ●	166,70	1.204,74	3,03%
-	-	-	39.731	3	2022	0,521	3.282,35	12,3%	1.711,39	● ● ●	3,31	69,19	-11,6%	228,68	● ● ●	207,18	1.504,21	3,79%
TTL			39.731,00			18,25			43.107,26		22,77			2.564,47		2.976,04	40.131,22	101%

Referencias	
	✕ Equipo apagado/no instalado.
	● Equipo funcionando (no optimizado) *Solo en el caso de chia durante el proceso de ploteado.
	● Equipo funcionando.
	◐ Equipo inestable.

Fuente: elaboración propia.

Resumen

- Los mineros reciben una recompensa en criptomonedas por sus actividades.
- La electricidad, la adquisición del hardware y los mantenimientos son factores que afectan las ganancias de la minería.
- Todo minero debe hacer una inversión en equipos especializados antes de comenzar en la industria.
- Las tarifas eléctricas, instalaciones, mantenimiento e impuestos pueden disminuir la ganancia neta.
- El rendimiento de los mineros puede verse afectado por las variaciones en el precio de1 *altcoin* a minar.
- Los cumplimientos o retrasos del *roadmap* establecido en cada proyecto de minería pueden dar indicios de futuros cambios en el comportamiento de la dificultad de minería, precios de *token* de gobernanza, precios del hardware, etc., por lo cual, saber anticiparse a cada escenario posible y establecer una nueva estrategia será necesario si el inversor desea mantener, maximizar o evitar pérdidas en este modelo de negocio.
- El minero no debe ser un agente pasivo en este negocio, sino que debe estar monitoreando constantemente los equipos para garantizar que se mantengan encendidos y operativos el mayor tiempo posible. Así también, deberá planificar y ejecutar mantenimientos preventivos para prolongar su vida útil.

Capítulo 7. Minería industrial

En el capítulo anterior se describió el proceso de análisis, montaje y gestión de un proyecto de granja de minería doméstica. Quedó claro que la rentabilidad puede fluctuar en el tiempo en base a distintas variables dinámicas como el precio de la criptomoneda, la dificultad de minado o el costo energético en la región donde se encuentren instalados los equipos. La capacidad que pueda llegar a tener un individuo para montar una granja dependerá de sus conocimientos, disponibilidad de capital a invertir y accesibilidad a los equipos e infraestructura adecuada. Si bien se pudo visualizar en la Figura 35 que la minería de criptomonedas es un negocio que puede ser muy rentable en ciertos periodos, en otros, lo mejor será desconcertar los equipos o seguir acumulando activos adoptando una estrategia de *holdear*, esperando que las *altcoins* se valoricen antes de decidir tomar ganancias.

En este capítulo se abordará el modelo de la criptominería desde una óptica de mayor nivel, analizando como piensan y que estudios de factibilidad realizan los referentes del sector que llevaron a este negocio a una escala industrial. También se explicará las verticales de negocio que se fueron creando para complementar esta industria y cuáles son las expectativas del negocio para los próximos años. A continuación, se expondrá un caso representativo de grandes players internacionales de la industria de centros de datos blockchain a escala industrial.

Caso Cryptonix World

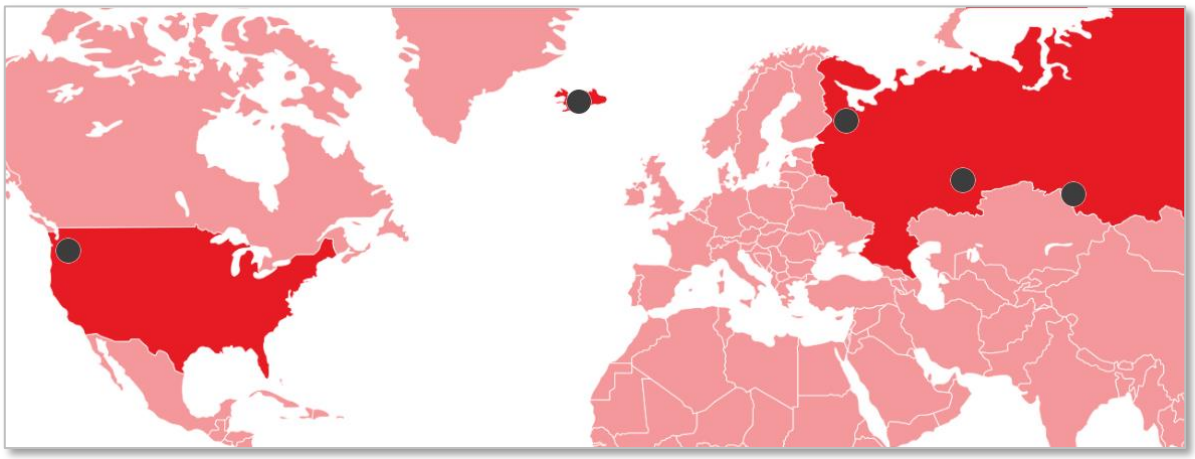
Extraído del Webinar de Luis Cáceres CEO NWC10Lab con Sergio Vela CEO CryptonixWorld para aprender sobre minería (Cáceres, 2022).

Cryptonix World nace en diciembre de 2019 como una empresa de servicios de centros de datos de minería en blockchain con el objetivo de desarrollar diferentes líneas de negocio en el sector de las criptodivisas. Algunos datos relevantes de la compañía son: poseen 5 centros de datos o producción de minería / 6 MW total de capacidad instalada / +1.200 unidades mineros operativos, entre propia y tercerizada / +2MM de EUR en ventas de equipos / >35 PH de capacidad / producen aproximadamente 6 BTC por mes. Entre sus principales socios estratégicos y proveedores de productos y servicios de minería poseen a Bitmain, Innosilicon, Fourbull Miner, whatmister, Luxor Mining y ViaBTC.

Análisis de escenarios

Actualmente se encuentran operando centros de datos dedicados a la minería de criptodivisas en Rusia y EEUU, y avanzando con nuevas aperturas en Canadá e Islandia, previstos para el segundo y tercer trimestre de 2022. Aquí es donde se puede identificar el primer análisis que se debería hacer como inversor de criptominería a escala industrial: la diversificación del negocio a través de la internacionalización en distintas regiones con el fin de minimizar su exposición al riesgo (ver figura 36).

Figura 36: Instalaciones Cryptonix World



Fuente: cryptonixworld.com/instalaciones.

El inversor de una granja industrial debe realizar el análisis del negocio con un horizonte a largo plazo 5-10 años, a diferencia de la minería domestica que podría plantearse con un horizonte de 3 años. En esta escala el periodo temporal deberá ser mayor para poder justificar los retornos de la inversión en equipos e infraestructura. Las variables para calcular la rentabilidad siguen siendo las mismas que se vieron en el capítulo anterior, solo que deben mirarse con un horizonte temporal mayor. En la figura 37 se puede observar las dos curvas con mayor relevancia para el cálculo de rentabilidad, el nivel de dificultad de minado, medido por la cantidad total de poder de cálculo de la red y el algoritmo de dificultad.

Las certezas que posee el inversor para calcular la rentabilidad futura se basan en las llamadas variables conocidas, como pueden ser el costo de los equipos, el costo de la energía con proyección a 12 meses y la previsión de cómo va a evolucionar la curva de dificultad. La única incógnita en cuestión seguirá siendo el precio del *altcoin* a minar, en este caso el Bitcoin. El análisis que realiza un minero industrial parte de visualizar el nivel de dificultad que se alcanzará en un *pool* concreto donde decida trabajar. Partiendo del valor actual y

conociendo que, para el caso del BTC, la dificultad se actualiza cada 15 días o 21 bloques, podrá estimar el nivel de dificultad futuro basándose en la cantidad de equipos que se vayan conectando. La capacidad de las maquinas se miden en TH, que son la cantidad de cálculos por segundo que puede arrojar al algoritmo y la ganancia en BTC a cobrar está ligado íntimamente a esas dos curvas. En resumen, sabiendo la capacidad de cómputo de los equipos se podrá calcular el pago diario. Por lo tanto, para un período de 30 días se podría tener cierta certeza de cuanto será la rentabilidad bruta del negocio.

Figura 37: Análisis de curva de dificultad Bitcoin

Fuente: Cryptonixworld.

Impacto de la geopolítica en las granjas industriales

La curva de dificultad se ve intrínsecamente influenciada por las decisiones geopolíticas, y los mineros no están exentos a las consecuencias que estas generan, teniendo que definir estrategias de negocios dinámicas y muy flexibles en caso de declararse decisiones no favorables para la industria. De la figura 37 también se desprende un análisis extraído de las declaraciones de Sergio Vela que ejemplifica como un inversor de grado industrial debe analizar el contexto y recalibrar su estrategia antes cambios políticos globales. En dicho análisis Sergio explica el comportamiento de la curva de dificultad relacionándola con hechos mundiales y decisiones geopolíticas relevantes:

(0) El tamaño de la red venia creciendo orgánicamente impulsada por la fabricación de nuevos equipos de minería. China había alcanzado un máximo de 68% del *hashrate* mundial para mediados del 2021.

(1) El primer episodio ocurrió en mayo del 2021 cuando el *hashrate* de la red se reduce en un 14% ante el fin de la temporada de lluvia en China, donde se desinstalaron los equipos conectados a la energía hidroeléctrica y se pasaron a energía en base a carbón. Estos tipos de hechos generan alteraciones en los cálculos de rentabilidad por variaciones en la dificultad de minería y en los precios del mercado por reducir la seguridad de la red.

(2) El segundo episodio se generó en julio del 2021 donde el 60% del *hashrate* mundial pasó a 0% con el China Ban. Esta decisión fue tomada con buenos ojos por la comunidad minera porque, por un lado, eliminaba el monopolio hegemónico que venía acarreando China en la red de Bitcoin, convirtiéndose en una economía de mercado, y por el otro, permitió la migración de los mineros industriales a demarcaciones muchísimo más estables como EEUU y Canadá.

(3) El tercer episodio ocurrió en noviembre del 2021 donde Kazajistán implementó un impuesto específico del 80% sobre la actividad de la minería, por lo cual, el negocio dejó de ser rentable en ese país.

Cryptonix comenzó en 2020 operando en China, Kazajistán y Rusia. De las primeras tres instalaciones, dados los acontecimientos mencionados previamente, dos centros se tuvieron que desmontar y mudar a otros países. El objetivo de Cryptonix es tener una distribución de centros de datos a nivel mundial que les permita por un lado establecerse cerca de centros de producción de energía renovable y limpia, y por el otro, buscar ubicaciones específicas que les permita compensar esos potenciales efectos de riesgo país.

Para enero 2022 el *hashrate* mundial ya había recuperado los niveles previos al China Ban, y su crecimiento siguió en ascenso. La previsión de la curva de dificultad es que se duplique en los próximos 3 o 4 años. Esta previsión la tienen relativamente bastante tasada por dos motivos. En primer lugar, la capacidad de producción de equipos nuevos y el cuello de botella de producción aproximada de semiconductores de los fabricantes mundiales ya es conocida, por lo que se puede estimar la fabricación en los próximos tres años. Y, por otro lado, la propia eficiencia de los chips está llegando al cenit de la curva. Hasta ahora cada equipo que salía al mercado era un 30/40% más eficiente que el anterior, sin embargo, dicha curva se está achatando. Por lo tanto, permite anticipar el comportamiento de la curva de dificultad para los próximos 3 años.

Algo que el CEO de Cryptonix no menciona, y es oportuno aclarar, es sobre la situación de rentabilidad actual de los mineros. Para ello se toma el siguiente extracto de un estudio realizado por Glassnode Insight publicado en su newsletter Sem23, 2022 (Glassnode, 2022):

> "Hay una intrigante divergencia que merece la pena discutir, se trata del incesante aumento de la dificultad de minado de la red que ha crecido en nada menos que un 132% desde su ATH o máximo histórico, y todo a pesar de la desmotivación económica que supone el descenso del 56,7% de los ingresos mineros totales (ver figura 38). Este salto tan sustancial de la dificultad sugiere que los mineros existentes han expandido considerablemente su operativa, y que muchos nuevos mineros se han incorporado a la red a pesar de la imponente reducción salarial. Y como tal, es muy probable que esa nueva inversión de capital en hardware de minado y en las instalaciones pertinentes puedan seguir asfixiando el estado de cuentas de los mineros."

Figura 38: Dificultad de minado vs Ingresos

Fuente: Glassnode Insights.

Estrategia

Sergio aporta una definición muy simplificada de la minería, pero muy cierta desde el punto de vista de inversor inteligente: "La minería de criptodivisas es una forma de obtener BTC u otras *altcoins* a largo plazo a un precio muy inferior al de mercado". Esto explica que, asumiendo un ciclo de precios alcista, a largo plazo, la misma inversión que demanda los equipos de minería representaría una mayor cantidad de unidades de *altcoins* que si decidiéramos comprarlos directamente en el mercado.

Otra declaración asertiva importante de destacar es sobre su visión de futuro de la minería de Bitcoin, indicando que la misma será rentable hasta 2026 y luego del *halving* del 2028 la situación empezaría a cambiar, donde el formato industrial pueda llegar a perder sentido. Esto lo relaciona con el nivel de dificultad que pueda alcanzar la red para ese entonces, si no se llegan a soluciones energéticas eficientes y renovables donde el costo del kWh sea prácticamente cero, quizás la minería no siga siendo atractiva, salvo que exista un salto exponencial en el precio del Bitcoin que justifique seguir manteniendo el negocio.

Si bien Cryptonix nace con instalaciones de criptominería, considera que el proyecto industrial que corre por debajo es uno de sus grandes objetivos estratégicos, haciendo alusión a una frase popular bien conocida: “En la fiebre del oro, los únicos que ganaban dinero eran los vendedores de picos y palas”. Actualmente dichos objetivos se basan en ampliar las verticales de negocio apostando a I+D, principalmente en energías renovables orientadas a abastecer los centros de datos blockchain, como así también, a terceros domésticos.

Resumen

Los mineros parecen encontrar cada vez más dificultades económicas, con muestras de sufrir serios contratiempos en su balance financiero a la par que han expandido sus operaciones como da a entender la dificultad de minado. Esto quiere decir que cada nueva moneda resulta más cara de minar, mientras la recompensa denominada en términos de dólares americanos se mantiene en declive y eso puede suponer que quede por delante una capitulación minera. El futuro es incierto, es por eso que los grandes players están diversificando su cartera e invirtiendo en la investigación y desarrollo de nuevos verticales de negocio. Si algo es seguro, la tecnología blockchain requerirá de grandes centros de datos para seguir escalando. Sea como minero, validador o proveedor de tecnologías complementarias, el negocio de ofrecer servicios tecnológicos en blockchain seguirá creciendo. Simplemente habrá que ser dinámico y adaptarse a los cambios venideros para seguir capitalizando rendimiento en los modelos de negocios que se vayan presentando.

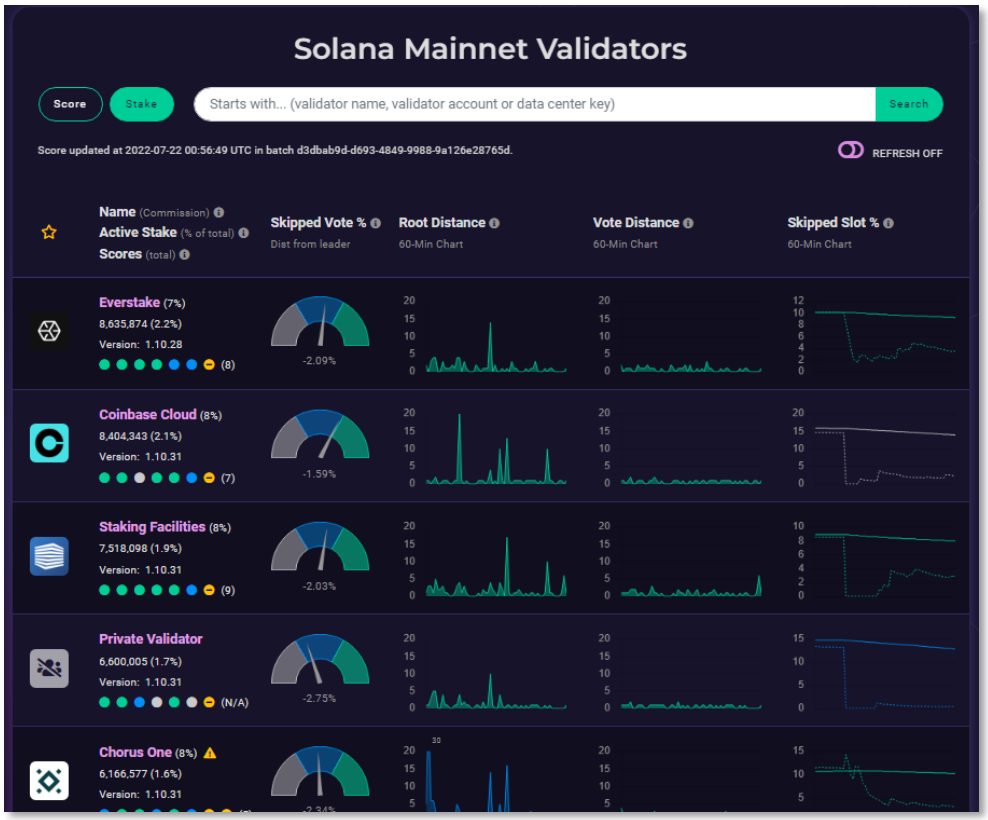
Capítulo 8. Hacer Staking como alternativa a la minería

La minería de criptomonedas se inició como forma dominante de ganar recompensas en una red blockchain bajo el protocolo de consenso PoW, sin embargo, con el paso del tiempo el *staking* ciertamente ha estado presentado una opción más democrática para aquellos que quieran minar criptomonedas, incentivada principalmente con la creación de las nuevas redes blockchain de tercera generación. Entre ellas, algunos de los proyectos más sólidos que están ganando terreno bajo el protocolo de consenso PoS se pueden mencionar a Cardano (ADA), Solana (SOL) y Polkadot (DOT) entre otros. Sin olvidar a Ethereum, que prevé pasarse a este protocolo en el corto plazo. En el presente capítulo se abordará la minería de criptomonedas a través del protocolo de consenso PoS o prueba de participación. De la misma forma que en el modelo de la minería PoW en este caso también se puede segmentar entre grandes jugadores que montan nodos validadores y cuyas barreras de entradas son mayores, y en pequeños inversores que solo deben delegar sus *tokens* a aquellos validadores que les brinden más confianza.

Validadores

Si bien los *rewards,* requerimientos iniciales y diseño de cada cadena son únicas, el modelo de negocio es prácticamente similar en cada una de ellas. Consta de montar una infraestructura de hardware con conexión 24hs a la red, tener mínimos conocimientos de blockchain y configuración de softhware, y depositar un mínimo de *tokens* (hacer *staking*) que brindará al validador la posibilidad de ser seleccionado para la validación de un bloque y ganarse la recompensa en su *token* nativo. La ventaja de ser validador es que puede atraer a nuevos inversores que quieran delegar *tokens* en su nodo. Esto permite por un lado incrementar el TVL o *total value locked* en su nodo incrementando la probabilidad de ser elegido y además cobrar un fee a sus depositantes incrementando la rentabilidad del negocio. En la siguiente figura se muestra un ejemplo de los principales validadores de la red de solana ordenados por el total de *stake* activo. También se observa la comisión que cobran para hacer *staking* con ellos y como otros indicadores propios del protocolo.

Figura 39: Lista de validadores Solana



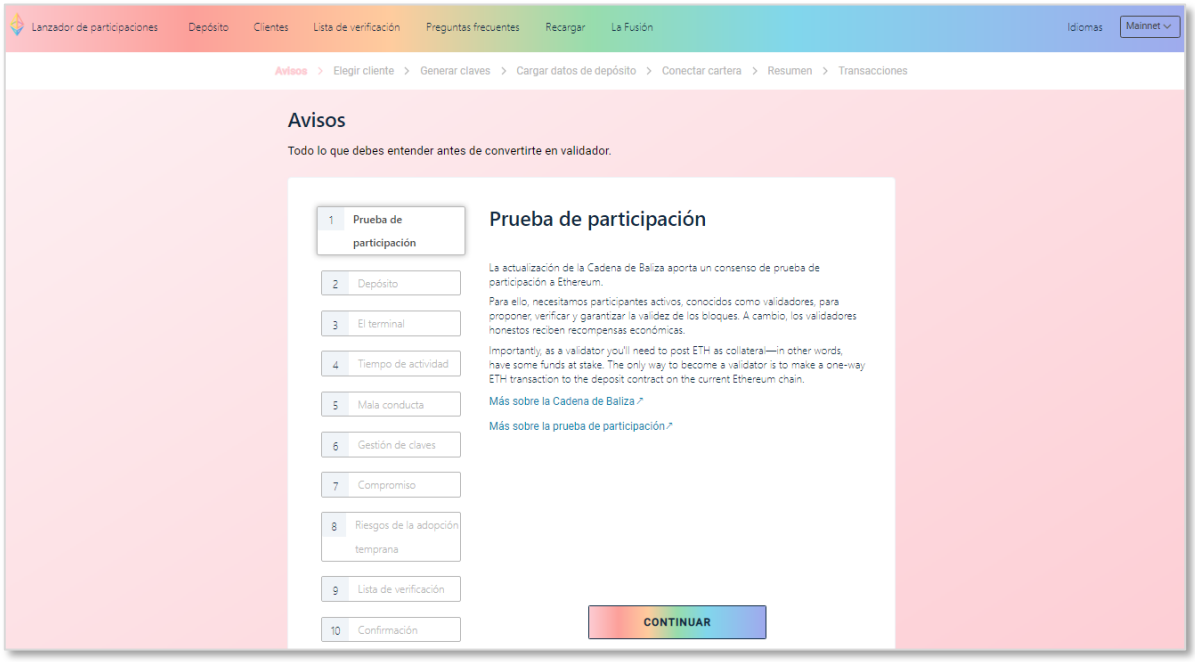
Fuente: www.validators.app.

En caso de querer ser validador, solo se debería ingresar en los siguientes links y seguir la guía de pasos para darse de alta como nodo en la red blockchain deseada:

- ***Ethereum:*** https://launchpad.ethereum.org
- ***Solana:*** https://docs.solana.com/running-validator/validator-start
- ***Avalanche:*** https://www.avax.network/validators
- ***Polkadot:*** https://wiki.polkadot.network/docs/maintain-guides-how-to-validate-polkadot

En cualquiera de los casos un inversor con intenciones de ser validador deberá afrontar las siguientes barreras de entrada: invertir en hardware específico y bloquear un importe mínimo de *tokens*. En la siguiente figura se puede observar el *launchpad* de ETH, sitio oficial para informarse de todos los requerimientos e iniciarse como validador de su cadena.

Figura 40: Launchpad ETH PoS



Fuente: ethereum.org.

Requerimientos para minar en Pos delegando los tokens

Para aquellos que no deseen invertir en hardware o no tengan los conocimientos técnicos requeridos podrán delegar sus *tokens* a alguno de los validadores listados en la red. En este caso, validar transacciones con *Proof of Stake* no requiere un consumo eléctrico elevado que implique minar, ni se necesita un hardware especializado. Basta con acceso a internet, un *pool* y tener un mínimo de monedas.

Decidir sobre cual red hacer *staking* dependerá de los siguientes factores:

- ***Reward:*** *APY (Annual Percentage Yield).* En la siguiente tabla (ver figura 41) se puede observar el top 10 de los principales criptoactivos para hacer *staking* bajo el protocolo PoS. Se puede observar que están ordenadas por *TSV - Total stake value* (valor total bloqueado en U$D) y el *redward* que ofrecen por bloquear *tokens* en su red.

Figura 41: Top 10 Crypto Assets by Staking Marketcap

#	Asset	Price	24h	Reward	Staking Marketcap	Market Cap	Staking Ratio	7d Price Change	Add
1	Ethereum 2.0 ETH	$1,079.77	3.08%	4.11%	$13,975,213,664	$128,785,186,125	10.67%		
2	Solana SOL	$34.06	-0.09%	8.2%	$13,228,697,697	$11,743,334,622	75.12%		
3	Cardano ADA	$0.42	-1.59%	4.96%	$10,431,065,042	$14,454,248,725	71.36%		
4	Avalanche AVAX	$17.92	0.95%	8.67%	$4,219,607,192	$5,096,641,460	58.65%		
5	BNB Chain BNB	$225.18	1.11%	5.14%	$4,214,003,391	$36,674,966,487	82.46%		
6	Polkadot DOT	$6.31	-2%	14.15%	$3,947,861,144	$7,198,210,902	51.79%		
7	Tron TRX	$0.07	0.42%	3.51%	$2,732,266,476	$6,076,514,852	45.52%		
8	Algorand ALGO	$0.3	2.55%	9.77%	$1,612,129,781	$2,103,034,461	72.67%		
9	Internet Compu ICP	$6.34	-2.31%	8.01%	$2,321,829,347	$1,572,746,336	76.34%		
10	Cosmos Hub ATOM	$7.6	-0.25%	17.87%	$1,502,072,819	$2,301,793,544	63.04%		

Fuente: stakingrewards.com.

- ***Diseño del sistema monetario:*** Inflacionario/Deflacionario. Si bien maximizar el *reward* es lo que buscaría cualquier inversor, antes de apostar por alguna red en particular se deberá analizar cómo está diseñado su sistema monetario, ya que no serviría de nada tener un *reward* elevado si la tasa de inflación de la moneda supera el porcentaje de ingresos. Además, es importante entender cómo se comportará el precio del *token* en base a la propuesta de valor de cada proyecto. En la siguiente figura se presentan ejemplos de los diseños del sistema monetario de Polkadot y Cardano.

Figura 42: Ejemplos de política monetaria DOT & ADA

Fuente: CoinmarketCap y Web oficiales.

- ***Plataformas de staking:*** protocolos centralizados vs descentralizados.

La finalidad de este capítulo no es ahondar en este tipo de minería, sino dejar planteado que existen otras alternativas de minería como modelo de negocio a la hora de analizar modelos de negocios de criptominería.

Resumen

Las criptomonedas representan un fenómeno muy reciente que apenas llevan un poco más de 10 años de vida, y si pensamos en las blockchain de tercera generación que nacieron con protocolos de consenso PoS, llámese Cardano, Solana, Polkadot o ETH 2.0, solo llevan 5 años y un camino muy largo por recorrer. La pregunta correcta no es si debemos invertir en criptomonedas sino en cual. Siguiendo el mismo mecanismo de análisis de proyectos que se recomendó para evaluar que red blockchain deberíamos minar bajo el protocolo de consenso PoW, en PoS se deberá realizar un estudio similar. Se debe investigar y entender cómo funciona cada moneda, su ecosistema, qué problema soluciona y el equipo humano de personas que hay detrás de cada proyecto. De esta manera se podrá entender si la criptomoneda tendrá utilidad y si apreciará su valor de forma considerable a largo plazo.

Capítulo 9. Minería de cripto activos como oferta de servicios

Con la llegada de blockchain de 3ra generación también nacieron proyectos de servicios que permiten asociar su modelo de negocio a la minería de su criptoactivo para fortalecer la seguridad de su red. En estos casos las redes suelen ser privadas y permisionadas a los fundadores del proyecto. Aun así, su modelo de negocio es descentralizado permitiendo a los usuarios ser proveedores y clientes al mismo tiempo. En el presente capítulo se expondrán ejemplos de proyectos que se encuentran activos, que permiten minar criptomonedas y al mismo tiempo fortalecer su estructura de servicios. Si bien aún se encuentran en etapa de maduración, se están fortaleciendo día a día, incrementando su base de usuarios y preparándose para la conformación de la Internet del Valor, un mundo de redes de servicios independientes asociadas a la web3.

Un producto operativo es algo que un potencial inversor puede ver y comprobar por sí mismo que funciona, que es usable y usado, con una comunidad de usuarios significativa y activa. A continuación, se presentarán tres ejemplos de productos operativos, usados y accesibles a cualquiera. En casi todos los casos, la criptomoneda se usa para generar un sistema de recompensas de enorme complejidad y completamente autónoma de cualquier moneda fiat, cocreando un ecosistema financiero propio para los usuarios del *token*.

1. **Helium (**https://www.helium.com)

Helium (HNT) es una red descentralizada impulsada por blockchain para dispositivos de Internet de las Cosas (IoT). Lanzada en julio de 2019, la red principal o *mainnet* Helium permite que los dispositivos inalámbricos de baja potencia que se comuniquen entre sí y envíen datos a través de su red de nodos. Los nodos vienen en forma de los llamados puntos de acceso o Hotspots (ver figura 43), una combinación de router inalámbrico y un minero blockchain. Por lo tanto, los usuarios que operan nodos, minan y ganan recompensas en el *token* de criptomoneda nativo de Helium, HNT. La red se ejecuta sobre *proof-of-coverage*, un nuevo algoritmo de consenso basado en el protocolo HoneyBadger BFT (POA Network, 2018) que permite a los nodos de una red alcanzar el consenso cuando la calidad de la conexión es altamente variable.

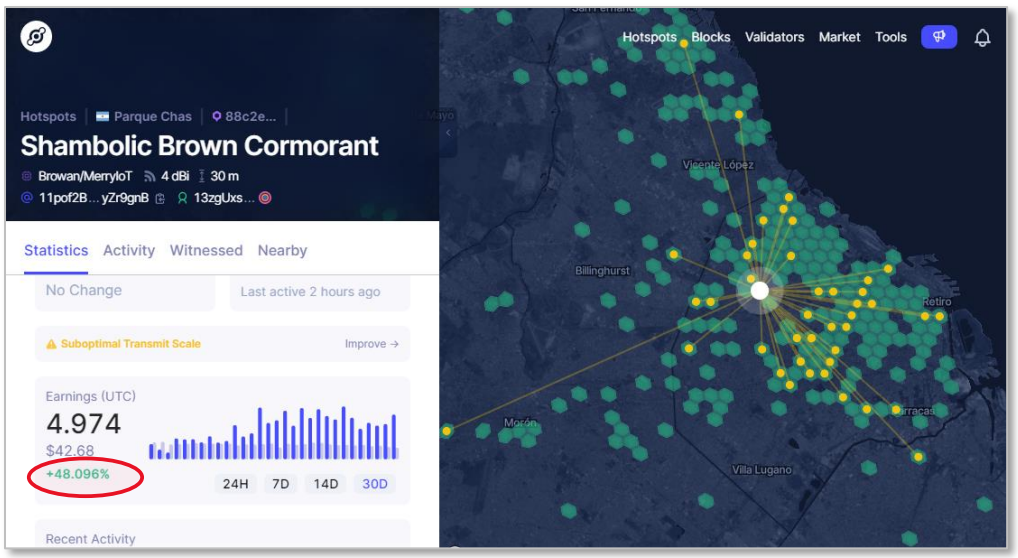
Figura 43: Línea Hotspot de Helium

Fuente: https://www.helium.com/mine.

En síntesis, el objetivo de Helium es preparar la comunicación de IoT para el futuro, identificando las ineficiencias de la infraestructura actual. Los desarrolladores buscaron agregar descentralización a su oferta permitiendo a los participantes de la red adquirir los hotspots para proporcionar cobertura de red y obtener recompensas a cambio.

En la siguiente figura se puede observar que la rentabilidad mensual que logró un usuario con su hotspot de 4dBi, a 30 metros de altura en la Ciudad de Buenos Aires, Argentina fue de 42,68usd.

Figura 44: Mapa de localización de hotspots en CABA, Argentina



Fuente: explorer.helium.com.

En síntesis, la rentabilidad que se pueda lograr en este proyecto dependerá del tipo y modelo de hotspot a utilizar, su ubicación, la altura de instalación, el rango de cobertura y la cercanía que tenga a otros dispositivos para verificar la trazabilidad de la información.

2. **Siacoin (**https://sia.tech)

Sia es un proyecto que permite a los usuarios arrendar el acceso a su espacio de almacenamiento no utilizado, como discos duros, y, a cambio, conseguir recompensas por ello. Este modelo de negocio monetiza una plataforma que permite almacenar archivos en la nube a muy bajo costo y con una seguridad y privacidad total. La información se rompe en segmentos y se encripta, guardándose por triplicado. Los acuerdos y las transacciones se aplican con contratos inteligentes, y Siacoin es el medio de intercambio para pagar el almacenamiento en la red. El objetivo principal del proyecto es convertirse en la "capa de almacenamiento central de Internet".

Sia se lanzó oficialmente en junio de 2015. Según su documento técnico, el objetivo a largo plazo de Sia es competir con las soluciones de almacenamiento existentes. Se considera una competencia directa con los principales proveedores de almacenamiento en la nube, como Amazon, Google y Microsoft. Debido a su naturaleza descentralizada, Sia puede ofrecer tasas de almacenamiento competitivas. Los archivos almacenados en la red Sia se dividen en 30 segmentos cifrados, con cada segmento cargado en un host único para su redundancia. Los acuerdos entre cargadores y anfitriones se registran en la cadena de bloques de Sia y se aplican mediante contratos inteligentes. Siacoin actúa como el método de pago en la red, con arrendatarios que pagan a los anfitriones utilizando SC, y anfitriones que bloquean SC en contratos inteligentes como garantía.

Skynet, la compañía detrás de Sia y Siacoin, ha anunciado varios productos construidos sobre la red Sia, incluido SiaStream, una aplicación de transmisión de medios basada en la nube, y la red Skynet, su red insignia de entrega de contenido e intercambio de archivos. Además, cada transacción relacionada con el almacenamiento en la red Sia está sujeta a una tarifa de

3,9%, que se distribuye a los titulares usando la segunda criptomoneda de la compañía, Siafund.

3. Golem (https://www.golem.network)

Golem (GNT) es similar a Siacoin, pero con la idea de combinar todos los recursos de los participantes en una única máquina virtual, que puede usarse para resolver problemas de gran coste computacional, como los que se encuentran en Big Data o Machine Learning. Otro ejemplo de uso es el renderizado. Los participantes que proporcionen recursos son recompensados por ello.

En abril de 2016 se anunció el Proyecto Golem, liderado por Golem Factory. La red lanzó su *mainnet* el 10 de abril de 2018. Golem Network es una red de cómputo descentralizado; una nueva forma de distribuir potencia informática a demanda. Crea una red *peer-to-peer* donde los usuarios se unen en igualdad de condiciones para comprar y vender potencia de computación, dividiendo las tareas complicadas en subtareas más pequeñas en la red. En Golem no hay autoridad central y ningún usuario es más o menos importante que otro. Se necesita GNT o Golem Network Token para pagar los cálculos en la red. Esta es la moneda que impulsa el mercado. Como solicitante, se puede establecer una oferta por una cantidad de GNT que se estará dispuesto a pagar para que se complete la tarea. Como proveedor, se ganaría GNT al cumplir con las tareas de los solicitantes. El sistema permite establecer los propios umbrales de precio mínimo y máximo en la configuración.

Resumen

Siempre se debe ser critico ante un modelo de negocio rentable. Ya que, si así fuere, no se tardaría demasiado tiempo que en otros jugadores entren al negocio para capturar el valor excedente y llegar a un nuevo equilibrio. Así la tecnología también podría seguir complejizando el modelo, incrementando las barreras de entrada y restringiendo el acceso a jugadores con menos poder de inversión o conocimiento técnico. Como se ha visto la minería de criptomonedas ofrece distintas alternativas de abordaje. Y aunque el concepto de minería

está muy radicado al aporte computacional y protocolos de consenso PoW, se ha visto que con el paso del tiempo la tecnología blockchain va ganando terreno en su uso, dándole la posibilidad a los usuarios que formen parte del negocio, permitiéndoles ser proveedores y clientes al mismo tiempo, y una oportunidad de rentabilizar ingresos a través de la descentralización de la oferta de servicios.

Conclusiones

En el presente trabajo se ha explicado cómo la tecnología blockchain nació para corregir las imperfecciones de la internet moderna y cómo la red de bitcoin se creó para corregir las imperfecciones del sistema financiero mundial aportando, en ambos casos, sus propiedades intangibles como la descentralización, seguridad, inmutabilidad y anonimato. Con ella también nacieron los agentes validadores y la minería de criptomonedas bajo un nuevo concepto de modelo de negocio, captando en la última década una creciente adopción por parte de devotos tecnológicos con ganas de invertir capital y generar rentabilidad bajo su ecosistema.

Se debe entender que minar criptomonedas no es una actividad estable, depende de muchos factores intrínsecos propios de su tecnología, como así también, de factores externos provenientes del mercado y hasta de las propias regulaciones de los Estados. Si bien la euforia por adquirir equipos de minería ha venido creciendo en estos últimos años, es importante entender en qué estadio se encuentra cada proyecto criptográfico, sea bitcoin o cualquier otra *altcoin*, para no caer en la trampa de querer incrementar el capital de forma efímera en proyectos que no tengan fundamentos sólidos o se encuentren en su etapa final de desarrollo.

Entonces, ¿es un buen momento para ingresar en el negocio de la criptominería? Lo importante es que, a nivel mundial, cada vez se registran más transacciones y transferencias en criptomonedas favoreciendo el crecimiento de su ecosistema. Aunque en la actualidad la respuesta a dicha pregunta no sea exacta, el sentimiento del inversor dependerá de cómo fluctúe el precio de la criptomoneda en el mercado.

Desde la óptica del negocio, y en base a lo expuesto en el presente trabajo, se podría concluir que es un buen momento para incursionar en este modelo de negocio ante la amplia disponibilidad de hardware a precios descontados. Si bien es verdad que la cotización de Bitcoin se encuentra en niveles bajos e inmerso en un escenario de *bear market* afectando la rentabilidad de los mineros, entendiendo su diseño deflacionario, se puede suponer que, llegado al próximo evento de *halving*, el precio volvería a tomar impulso, quedando en manos de los mineros la decisión de su producción y distribución. Este entendimiento de la realidad se puede extrapolar a otros proyectos *altcoins*,

especialmente en Ethereum que, tras el derrumbe de su cotización, también han bajado mucho los precios de sus rigs (equipos), lo que genera una buena oportunidad de entrada. Desde la óptica del inversor también se pudo comprender cuáles son las estrategias a corto y largo plazo para los ahorristas de criptomonedas. Los inversores independientes adoptan la criptominería como una apuesta a mediano y largo plazo, mientras que hacer trading sería la mejor forma de generar estos activos en el corto, ya que permite hacer una buena diferencia a partir de las altas fluctuaciones de precios. Aquellos mineros que vienen llevando la actividad desde épocas tempranas, principalmente los que trabajan bajo el formato industrial, coinciden que no es un buen momento para minar, dadas las desfavorables condiciones que se obtienen de combinar las principales variables que afectan al proyecto, como el precio de las *altcoins*, la curva de dificultad y el costo energético. Aunque el negocio a nivel industrial no sólo se encuentra en la minería, sino en la creación de nuevas verticales, focalizándose en la investigación y desarrollo de nuevas tecnologías que les permitan suplir y rentabilizar las necesidades del futuro.

En el caso de la minería de Ethereum, se ha realizado el análisis de un proyecto real de minería doméstica, llegando a la conclusión de que este negocio es sumamente rentable, por lo tanto, el que posea los equipos debería seguir en la actividad. Sin embargo, ingresar desde cero en estos momentos parecería ser un movimiento arriesgado, entendiendo que en el corto plazo se prevé un cambio en su protocolo de consenso que impedirá seguir desarrollando esta actividad en su formato tradicional. Cuando esto ocurra, un posible escenario podría impulsar a los mineros a migrar a otros proyectos alternativos bajo el protocolo PoW. Sin embargo, sería muy difícil anticipar un cálculo de rentabilidad ya que dependerá de la capacidad que tengan los proyectos *altcoins* existentes en el mercado de absorber todo el *hashrate* o potencia instalada ociosa remanente tras el *merge* de Ethereum. Otro posible escenario a tener en cuenta, en caso de que los inversores no puedan ubicar sus equipos de minería, será desarmarlo y vender sus componentes como hardware de computación, dado que las GPUs son altamente demandadas por la industria de los video juegos o diseño gráfico. Es decir, se tendrá la posibilidad de minimizar el costo hundido en un mercado secundario. Caso que para Bitcoin no aplicaría, dado que sus equipos son exclusivos para la actividad y no tienen otro uso. En síntesis, no hay mejor frase que aplique al inversor que *"DYOR" - Do Your*

Own Research, donde deberá analizar los proyectos y establecer estrategias de negocio si quiere generar una rentabilidad duradera sobre su inversión.

Mientras tanto la tecnología seguirá evolucionando y las posibilidades de invertir y generar ingresos minando criptomonedas, ya sea como minero PoW, validador PoS o bien conformando parte de una infraestructura que ofrezca servicios operativos en blockchain, cada vez serán más accesibles y variadas. Si bien el presente trabajo se focaliza en analizar la minería PoW de bitcoin y Ethereum como modelo de negocio, siendo que juntos representan el 60% de toda la capitalización del mercado (compuesto por más de 20.000 monedas/proyectos), también se revisaron otras alternativas de minería o generación de criptoactivos que el inversor no debería descartar a la hora de analizar sus posibilidades.

Minar criptomonedas ha puesto en evidencia que, desde la génesis de bitcoin, se ha venido gestando la idea de un modelo de negocio donde uno puede ser productor y consumidor al mismo tiempo. Tanto el *PoW (Proof of Work)* como el *PoS (Proof of Stake)* generan pruebas irrefutables de que hay personas que intervienen en ambos lados del mostrador, y eso lo podemos ver en una infinidad de aplicaciones en función de las múltiples propuestas de valor de criptomonedas existentes. Es a partir de la evolución de la descentralización que empezamos a identificar muchas opciones alternativas a la minería tradicional. Las posibilidades que ofrece esta tecnología son infinitas y sin duda viene a instalar un cambio de paradigma.

A partir de la incursión en el uso de las criptomonedas, todos estarían en condiciones de empezar a tener un rol más activo en múltiples procesos de producción y decisión sobre gobernanza de proyectos. En caso de ser un inversor, aconsejaría iniciarse en la criptominería dado que es sumamente importante involucrarse y aprender en un ecosistema que seguramente regirá nuestros usos y costumbres en el futuro cercano, donde los modelos cooperativos blockchain avancen sobre las estructuras cotidianas y la tecnología pueda ser el motor de este cambio potencial mediante la construcción de una nueva infraestructura digital que facilite nuevos casos de usos emergentes.

Referencias

Academy, B. (28 de 11 de 2018). Difference between blockchain and bitcoin.

Academy, B. (12 de 2018). Proof of Work (PoW) vs. Proof of Stake (PoS).

Alizart, M. (2020). *Criptocomunismo.* La Cebra.

Ammous, S. (2018). *The Bitcoin Standard.* John Wiley & Sons Inc.

Binance Academy. (29 de Dic de 2019). ¿Qué es la Tecnología Blockchain? Guía Definitiva.

Cryptonixworld. (s.f.). Obtenido de https://cryptonixworld.com/

Glassnode. (06 de 06 de 2022). *insights.glassnode.com.* Obtenido de https://insights.glassnode.com/the-week-onchain-week-23-2022/

Gralla, P. (2007). *Cómo funciona Internet.* ANAYA MULTIMEDIA.

José Luis Cáceres, CEO NWC10Lab . (Febrero de 2022). *https://www.youtube.com/c/NWC10*. Obtenido de https://www.youtube.com/watch?v=p9acQBbgoDc

Nakamoto, S. (2008). *Bitcoin P2P e-cash pape.*

Ng, F. (10 de 06 de 2022). *Cointelegraph.* Obtenido de https://es.cointelegraph.com/news/global-bitcoin-adoption-to-hit-10-by-2030-blockware-report

Perez, C. (21 de 01 de 2021). *Coiquora.* Obtenido de https://coinquora.com/que-es-apostar-es-rentable-apostar-mejores-monedas-pos/

Pietrzak, B. C. (2009). *La cadena de bloques de Chia Network.*

Platzi. (2020). *https://platzi.com/clases/1317-inversion-criptomonedas/12109-blockchain-10-20-30/.*

POA Network. (Noviembre de 2018). *Medium.* Obtenido de https://medium.com/poa-network/poa-network-how-honey-badger-bft-consensus-works-4b16c0f1ff94

Rojas, M. R. (2018). *Guia para Minar Bitcoin y Criptomonedas.* CreateSpace Independent Publishing Platform.

Russo, C. (2020). *The Infinite Machine: How an Army of Crypto-hackers Is Building the Next Internet with Ethereum.* HarperCollins B and Blackstone Publishing.

Anexos

I: Bitcoin P2P e-cash paper

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

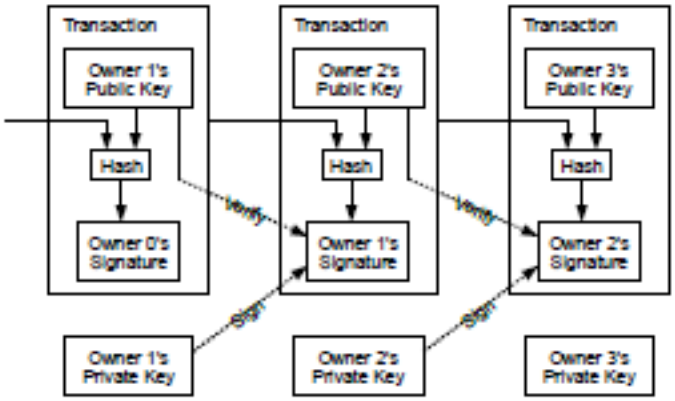
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

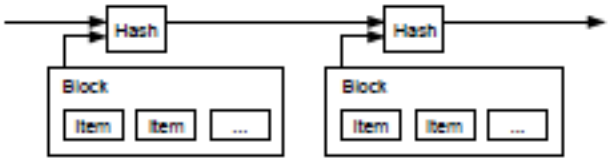


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

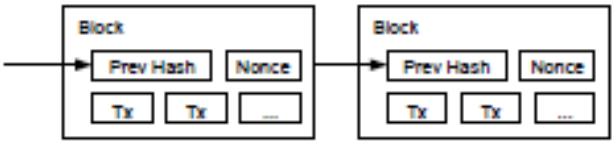
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

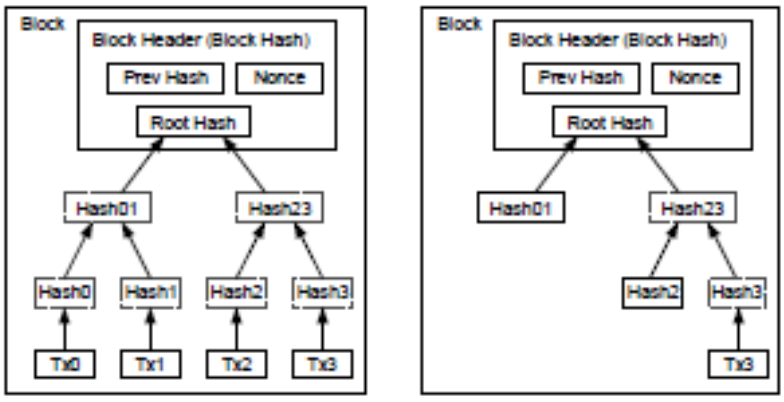
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



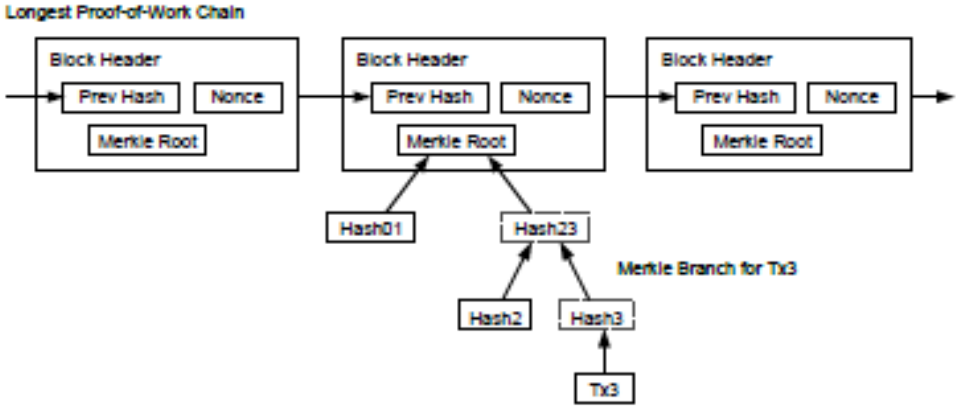
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

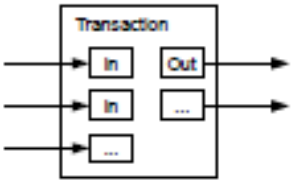
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

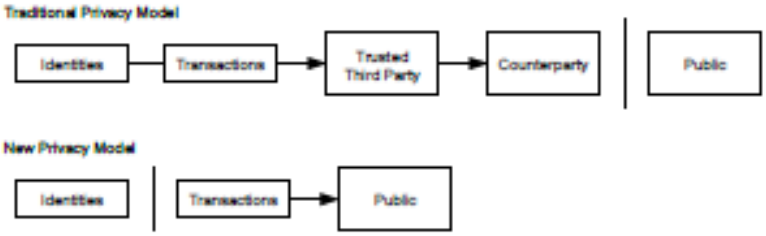
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

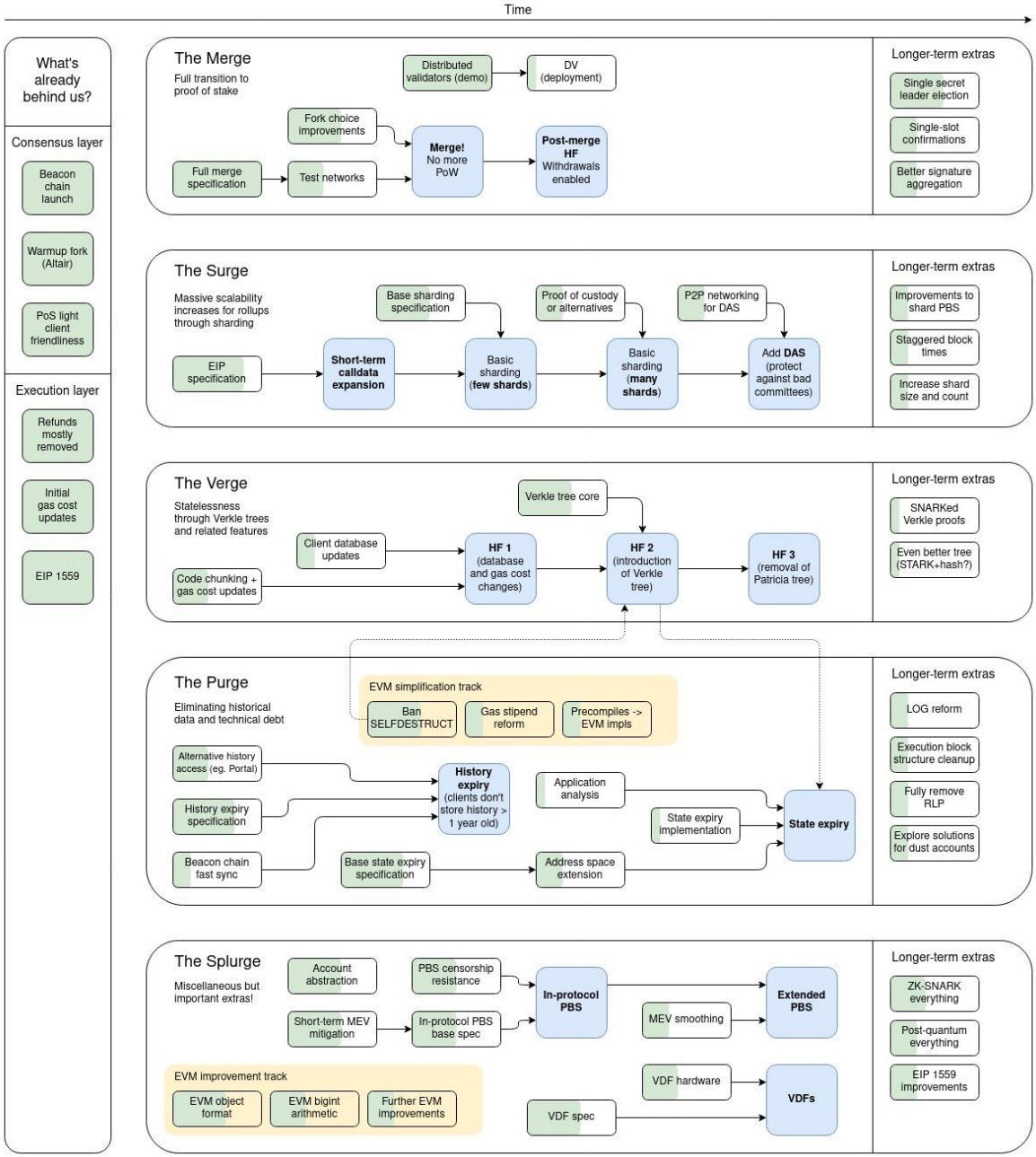
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

II: ETH 2.0 Road Map



III: Chia Network Future Roadmap