ACTIVIDAD C1: DOMINIO

GRANJA MINERA DE CRIPTOMONEDA

MOISÉS FRUTOS PLAZA

CONTEXTO

Las granjas mineras de criptomonedas se situan dentro del contexto del sistema abierto, democrático, y descentralizado de las monedas criptográficas digitales como Bitcoin, Ethereum, u otras criptomonedas alternativas, que aportan a la sociedad en internet un valor real, sirviendo como alternativa a las monedas físicas reales que suelen ser cerradas, centralizadas, y muy poco, o nada, democráticas.

La primera moneda criptográfica en hacer su aparición fue Bitcoin en el año 2009 y fue creada por un programador, o grupo de programadores, desconocido con el sobrenombre de ***Satoshi Nakamoto*** (*https://bitcoin.org/en/about-us*). Dicha moneda digital nació con el afán de convertirse en la moneda de internet, en la que ningún gobierno o entidad central ejerciera un control arbitrario sobre ella. Todas las transacciones serían públicas y transparentes a todos los usuarios, aunque las cuentas de los mismos serían anónimas. Se podría enviar dinero digital de una persona en una parte del mundo a otra sin tener que pasar por intermediarios, ya que la red es global y descentralizada. La red es mantenida por nodos repartidos por todo el mundo. Pero ¿cómo una transacción puede ser segura y sobre todo ser inmutable de modo que nadie "haga trampa"? ¿Quien vigila que eso sea así? La propia red cuando se realiza una transacción va generando confirmaciones, lo que vienen a ser que nodos y ordenadores clientes por el que la transacción pasa es analizada y verificada por estos contra lo que se denomina una **cadena de bloques común (Blockchain)** a toda la red (https://bitcoin.org/en/how-it-works). Cuando varias transacciones son realizadas y verificadas con éxito se crea un nuevo bloque encriptado. El bloque es enviado a los mineros para que éstos calculen su número de hash, a partir del número de hash del bloque anterior, el cual ya es seguro y autenticado por la cadena de bloques. Cuando uno de los mineros obtiene un nuevo número de hash que cumple con el patrón exigido por la cadena de bloques, éste nuevo número de hash es aceptado y asociado al nuevo bloque, y éste pasa a formar parte de la cadena de bloques. Debido a la **prueba de trabajo (Proof of Work)** que el minero ha realizado para hallar el nuevo número de hash correcto (cosa que hoy en día requiere millones de intentos, ya que cada vez que un nuevo bloque se adhiere a la cadena de bloques, ésta aumenta de forma intencionada la dificultad del patrón del nuevo hash) se le premia con una cantidad de monedas en recompensa. A este fenómeno es lo que se le denomina minar moneda criptográfica.

En resumen, todos los mineros obtienen el nuevo bloque encriptado a través de la red, todos intentan encontrar un nuevo número hash que asociarle para que sea aceptado por la cadena de bloques común a todos, el primero que logra conseguirlo obtiene la recompensa y logra "minar" el bloque. Si alguien logra otro hash correcto pero llega tarde, aunque sea por un microsegundo, su trabajo se declara **huérfano (Orphan)** y no obtiene la recompensa.

Este tipo de minería ha dado a lugar a que cuanto más potencia de procesamiento tienes, más intentos de hallar un nuevo hash correcto tienes por segundo aumentando en gran medida las posibilidades de que uno de tus mineros sea el que encuentre el hash correcto y te lleves la recompensa. De ahí que nacieran las granjas mineras. Las granjas mineras suelen estar compuestas por naves enormes repletas de mineros haciendo calculos de hashing las 24 horas del día, 365 días al año en busca de obtener las recompensas de los nuevos blosques que van apareciendo para distintos tipos de monedas. Se puede decir que albergan auténticos clústeres de supercomputación. La gente común, que no puede competir contra semejantes monstruos de la computación, suelen organizarse en **pools** de minería para que entre todos los usuarios se pueda sumar una gran potencia de cómputo. Estos pools reparten **shares** entre todos los mineros participantes y cuando se logra encontrar un hash para el nuevo bloque, se reparte la recompensa según los shares que cada minero tuviera en ese momento. Los shares se obtienen de forma proporcional al cómputo aportado por cada minero (https://dash.suprnova.cc/index.php?page=statistics&action=pool).

¿Porqué comentar lo de los pools si el dominio va sobre las granjas mineras? Porque las propias granjas mineras suelen diversificar su campo de negocio. No centran toda su potencia de cómputo en buscar el nuevo hash y llevarse toda la recompensa porque a veces puede llevar días, semanas o incluso meses encontrar la recompensa. Por lo que parte de su cómputo lo redirigen hacia pools que consideran prometedores. Acumulan todos los shares posibles y cuando el pool obtiene la recompensa, la granja se lleva un gran porcentaje de la misma aunque no toda, pero por lo menos se lleva algo de forma más **regular en el tiempo**.

Otra forma que las granjas mineras tienen de ganar dinero es alquilar sus mineros, o equipos de cómputo, mediante contratos de alquiler, en el que el arrendatario paga una cantidad inicial y luego le paga además ciertas comisiones por mantenimiento de los equipos y gastos de electricidad, obteniendo el arrendatario toda la parte sobrante como "dinero minado". A éste fenómeno se le conoce como **Cloud Mining** o Minería en la nube (https://www.genesis-mining.com/). Y poco a poco se va extendiendo más y más a lo largo del mundo.

Pero ¿para qué se quiere tener a disposición tanto dinero digital si al final lo que interesa es tener dinero real? Como ya se ha comentado antes el dinero digital por sí mismo aporta un valor a la sociedad en internet, ya que sirve para poder comprar artículos físicos o digitales en varios negocios electrónicos que aceptan este tipo de moneda, como por ejemplo Dell, Paypal, Expedia (https://www.coinbase.com/clients?locale=es), o Steam (http://www.theverge.com/2016/4/28/11525482/bitcoin-steam-valve-bitpay). No obstante, hay **casas de cambio (exchangers)** interesadas en cambiar el dinero digital por dinero real a costa de unas importantes comisiones como, por ejemplo, hacen Payza (https://www.payza.com/) o Cex.io (https://cex.io/). Por lo que el negocio, de llevarse a cabo con una buena estrategia puede llegar a ser rentable.

1. OBJETIVOS DE NEGOCIO

1. **Aumentar la producción de Satoshis diarios**, o lo que es lo mismo, ganar el mayor dinero posible, ya sea digital o real.
2. **Alcanzar y superar el ROI (Return On Investment)**, o **Retorno de la Inversión**, lo antes posible.

2. FACTORES CRÍTICOS DE ÉXITO

1. Que la producción de dinero diaria de los mineros, o **Revenue**, sea mayor que el gasto por el consumo eléctrico y mantenimiento de los mismos.
2. Alargar la vida útil de los equipos para maximizar su producción en el tiempo.

3. INDICADORES

1. **Producción** (o Revenue): **2 millones de Satohis diarios ó 0.02 BTC** producidos a las 23:59H.
2. **Gasto diario**: **5 €/día**. Es lo que se estima que cuesta mantener los mineros en correcto funcionamiento las 24 horas del día.
3. **Consumo Eléctrico**: Se estima un consumo eléctrico de **24 kWh** al día a las 23:59H. Este indicador se va incrementando a cada hora, y según su franja horaria costará más o menos, también dependiendo de la tarifa eléctrica contratada.
4. **Inversión Total**: **5000€ iniciales + Gasto Diario de 5€**. Este indicador tiene en cuenta todos los gastos efectuados hasta la fecha ya sea tanto en la compra de equipos como en consumo eléctrico, y mantenimiento de los mismos.
5. **ROI**. Porcentaje **negativo** de lo que que queda pendiente hasta alcanzar el ROI, o bien si se ha superado. Se empieza con un **-100%**. El negocio empieza a ser rentable cuando este porcentaje ya es positivo.
6. **Temperaturas**: Los mineros comenzarán con **35ºC** de temperatura de promedio. Estos indicadores muestran las temperaturas alcanzadas por los mineros en tiempo real. Los mineros están sometidos a mucho estrés, si uno de ellos alcanza una temperatura de **85ºC** hay que hacer una parada técnica para alargar su vida útil. Normalmente la parada técnica suele durar **5 minutos** (ver acciones).
7. **Frecuencia de Recepción de Trabajos**. Se espera que la frecuencia sea de **10 trabajos por minuto** como mínimo. Este indicador debe medir con qué frecuencia los mineros están recibiendo trabajos. Esto se hace sobre todo cuando se está minando hacia un pool y éste puede estar fuera de servicio.

8. **Cotización** de la moneda que se esté minando. **1 BTC = 640 $** = 100000000 Satoshi, 1 ETH = 2000000 Satoshi, 1 EGC = 3700 Satoshi. El mercado de las monedas es muy cambiante y puede que una moneda que sea interesante de minar hoy mañana no lo sea.
9. **Dificultad** de hashing. **BTC = 150G (1G = 1 * 10^9)**. Este indicador muestra cuán difícil es encontrar un nuevo hash para una determinada moneda.
10. **Moneda más beneficiosa de minar**. Se espera al menos un **0.067%** de mínimo. Este indicador suele ser el ratio entre cotización / dificultad de hashing de dicha moneda. Cuanto más valga y a la vez más facil de minar sea mejor.

4. ACCIONES

1. Si la **producción es menor que el gasto** hay que **parar los equipos** o cambiar hacia el minado de una moneda más rentable si es posible (que no siempre es posible). Pero nunca aumentar la Inversión Total a mayor velocidad que el ROI.
2. **Si** uno de los mineros alcanza la temperatura de **85 ºC** tiene que **hacer una parada técnica** de **al menos cinco minutos** antes de poder continuar trabajando. De esta forma se alargará su vida útil y se maximizará su producción.
3. **Si** un minero recibe **menos de 10 trabajos por minuto** en un lapso importante de tiempo entonces se tiene que **cambiar de pool o de moneda**.
4. **Si el ratio cotizacion/dificultad** de una moneda **baja del 0.067% se comprueba** otra moneda que al menos cumpla la condición para **que los equipos pasen a minar la nueva moneda**. De este modo el ROI aumentará a mayor velocidad.
5. **Llegado** el día marcado, por ejemplo a **final de mes**, **intercambiar el dinero digital por real** o bien **reinvertirlo en mayor equipamiento**.

APÉNDICE: UNIDADES DE MEDIDA

- **THs, GHs, MHs, KHs ó Hs**: Velocidad a la que trabaja un minero. En realidad es el número de intentos de crear un hash por segundo. Según el algoritmo criptográfico de la moneda la unidad varía de Gigahash para SHA-256 (Bitcoin), por ejemplo, a Megahash para Dagger-Hashimoto (Ethereum). Si no ya, pronto se va a empezar a hablar de Terahash para SHA-256 ya que cada vez es más difícil de minar y su recompensa menor, pero los equipos son mucho más potentes.
- **Satoshi**: Es la unidad de medida de producción por excelencia dentro del gremio minero y equivale a 1*10^-8 BTC (Bitcoin). También es usada para las cotizaciones e intercambios de moneda en las casas de cambio.
- **W/Watts**: Unidad de consumo eléctrico de un minero una vez enchufado a la red eléctrica. En realidad son los vatios hora que consume.
- **€/kWh**:Precio del kilovatio hora que tenemos contratado en nuestra tarifa con nuestro operador de energía eléctirca. Puede variar según la franja horaria del día y/o según la tarifa.
- **ºC**: La temperatura se mide en grados centígrados o Celsius.
- **Trabajos Por Minuto**: En realidad no existe esta medida como tal en los actuales programas mineros, pero sí que te va mostrando a lo largo del tiempo si un trabajo ha sido aceptado, rechazado, o **stale** (llegado demasiado tarde). Si tras un buen tiempo, por ejemplo 5 ó 10 minutos, no se ha recibido ninguna notificación es que no se está recibiendo trabajos del pool, o bien hay problemas de conexión con el mismo. Una baja temperatura también es indicativo de que el minero está ocioso.