CloudMiner

Proyecto de Sistemas Informáticos
2013-2014
Facultad de Informática
Universidad Complutense de Madrid

Autores:
Juan Arratia
Arturo Pareja García
Tomás Restrepo Klinge

Director:
Jose Luis Vázquez Poletti

Índice general

Autorización

Los abajo firmantes, matriculados en la asignatura Sistemas Informaticos de la Facultad de Informatica, autorizan a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines academicos, no comerciales y mencionando expresamente a sus autores, tanto la propia memoria, como el codigo, la documentacion y/o el prototipo desarrollado durante el curso academico 2013-2014.

Juan Arratia

Arturo Pareja García

Tomás Restrepo Klinge

Agradecimientos

Resumen

CloudMiner es un proyecto cuyo objetivo principal es conseguir un mejor aprovechamiento del hardware existente, consiguiendo un beneficio económico mediante el uso de cripto-monedas virtuales. La idea principal es crear un "cloud" de recursos, compuesto por distintas máquinas con arquitecturas potencialmente distintas. Este "pool" será monitorizado en tiempo real por la aplicación, permitiendo al usuario comenzar/parar el 'minado' en cualquier momento en cualquiera de las máquinas disponibles, asimismo dándole información respecto al estado actual de estas. Se pondrán a disposición opciones adicionales, tales como aadir o quitar recursos (bajo arquitecturas y SSOO soportados). Adicionalmente, se podrá usar inteligencia artificial basada en estadísticas, consiguiendo un cierto nivel de automatización de la aplicación. Estas estadísticas también se harán visibles al usuario, para ayudar en la toma de decisiones.

Palabras clave: Cloud, Bitcoin, Monedas virtuales, Minería

Abstract

CloudMiner is a project that aims for a better exploitation of the existing hardware, achieving economical benefit through the mining of virtual crypto-currencies. The main idea is to create a cloud-computing resource pool, composed by diverse machines under potentially different architectures. This pool will be monitorized in real-time by the application, enabling the user to start/stop mining at any given point on any of the available machines, also providing information on their current status. Additional options will be available, like adding or removing resources (supported architectures). Artificial Intelligence based on statistics may be used in order to allow automated control of the mining cloud. This statistics are also visible to the user, to aid decision taking.

Keywords: Cloud, Bitcoin, Virtual currencies, Mining

Capítulo 1

Introducción

1.1. Divisas electrónicas, Bitcoin

1.1.1. Fundamentos

El fenómeno del dinero electrónico se está extendiendo para dar soporte a las actividades que se desarrollan en el ciberespacio. Una de las primeras actividades virtuales que incluía el concepto de divisa virtual fue SecondLife, una red social en la que los usuarios podían interactuar entre sí en el mundo virtual que definía. Con la implantación de una moneda virtual, Linden Dollar, los usuarios podían adquirir objetos y posesiones virtuales. Para obtener crédito se podían realizar actividades en el juego o bien recurrir a cambiar dinero real por créditos del mundo virtual. Suponía el primer paso en la creación de productos virtuales por los que los usuarios estaban dispuestos a pagar. Este modelo se popularizó rápidamente y empezaron a surgir juegos multijugador online donde los jugadores podían acceder a objetos, misiones o mejoras mediante la compra de créditos.
Con la explosión del uso de internet, la utilización de medios virtuales de pago también se ha generalizado para facilitar las operaciones y obtener una mayor seguridad en las transacciones. El objetivo es reducir los riesgos asociados a proporcionar a un desconocido los datos bancarios personales. Así, servicios como PayPal o Google Wallet, entre otros muchos, proporcionan un monedero virtual con el que se pueden realizar pagos en infinidad de servicios de todo tipo prestados en la red.

Sin embargo, en ciertos entornos se ha hecho necesario ir un paso más allá con objeto de alcanzar el anonimato total en las transacciones. En este contexto, donde el anonimato de la red resulta imprescindible para los artífices de ciertas actividades, surgen las denominadas divisas electrónicas. Se trata de activos equivalentes al dinero en metálico, dado que no identifican

al poseedor y no queda constancia de las operaciones que éste lleva a cabo.

Para poder analizar con cierto detalle el funcionamiento de las divisas electrónicas, tomamos a partir de ahora como caso particular el Bitcoin.

1.1.2. Origen del Bitcoin

Bitcoin fue concebido en 2008 por una persona (o grupo de personas) bajo el seudónimo "Satoshi Nakamoto". La creación de la primera aplicación para operar con Bitcoins también se le atribuye. Sin embargo, existen dudas sobre la nacionalidad e incluso sobre la existencia real de esta persona y hay múltiples especulaciones sobre su identidad real.

Bajo este seudónimo se publicó también un libro que propone un sistema de transacciones electrónicas que no depende de la confianza, sino que permite realizar transferencias de forma directa sin la necesidad de un intermediario. Al contrario de la mayoría de las monedas, el Bitcoin no está respaldado por ningún gobierno ni depende de la confianza en ningún emisor central, sino que utiliza un sistema de prueba de trabajo para impedir el doble gasto y alcanzar el consenso entre todos los nodos que integran la red.

Desde que se puso en funcionamiento en 2009 el sistema ha ido ganando popularidad gracias a las características de anonimato con las que permite realizar transacciones comerciales y al interés especulativo que ha despertado la evolución de su cotización al cambio con monedas reales.

1.1.3. Seguridad

La seguridad de la mayoría de las criptomonedas (y en particular de Bitcoin) reside en la utilización de técnicas de criptografía para la protección del saldo del usuario. La firma y la verificación de las solicitudes de transacción se realizan mediante técnicas de criptografía de clave pública.

Para hacer operaciones es necesario distribuir la clave pública de forma generalizada para que cuando se le remita información a un destinatario éste pueda comprobar que la información es válida, correcta y que corresponde a información que sólo ha podido ser generada por una persona que posee la clave privada.

El proceso por el que se aplica la clave privada a la información que se va a transferir se denomina firma y consiste en obtener un número que depende de la información a transmitir y de la clave privada. El receptor, a partir de la información recibida y la clave pública del usuario, obtiene un nuevo número que, si coincide con el enviado, permite validar la autenticidad y fiabilidad de la información.

Una vez garantizada la seguridad del saldo del usuario, el sistema también debe asegurar que las transacciones son correctas y que el poseedor de un saldo no puede gastarlo más de una vez. Para ello se utilizan técnicas de sellado temporal con las que se registra el momento exacto en el que se solicita una transacción de bitcoins. Los nodos de procesado tienen en cuenta estos valores para determinar cuándo una transacción es válida o no.

1.1.4. Protocolo

Direcciones

Todo participante de la red Bitcoin tiene una cartera electrónica que contiene un número arbitrario de claves criptográficas. A partir de la clave pública, se obtiene la dirección Bitcoin, que funciona como la entidad remitente y receptora para todos los pagos. Su clave privada correspondiente autoriza el pago solo para ese usuario. Las direcciones no tienen ninguna información sobre su dueo, son generalmente anónimas y no requieren de ningún contacto con los nodos de la red para su generación.

Las direcciones son secuencias alfanuméricas aleatorias de 33 caracteres de largo, en formato legible para personas, como puede verse en este ejemplo: 1LtU9rMsQ41rCqsJAvMtw89TA5XT2dW7f9. Utilizan una codificación en Base58, que resulta de eliminar los siguientes seis caracteres del sistema Base64: 0 (cero), I (i mayúscula), O (o mayúscula), l (L minúscula), + (más) y / (barra). De esta forma, se componen únicamente de caracteres alfanuméricos que se distinguen entre sí en cualquier tipo de letra. Las direcciones Bitcoin también incluyen un checksum de 32 bitsNota 4 para detectar cambios accidentales en la secuencia de caracteres.

Transacciones

Los Bitcoins contienen la dirección pública de su dueo. Cuando un usuario A transfiere algo a un usuario B, A entrega la propiedad agregando la clave pública de B y después firmando con su clave privada.31 A entonces incluye esos bitcoins en una transacción, y la difunde a los nodos de la red P2P a los que está conectado. Estos nodos validan las firmas criptográficas y el valor de la transacción antes de aceptarla y retransmitirla. Este procedimiento propaga la transacción de manera indefinida hasta alcanzar a todos los nodos de la red P2P.

Cadena de bloques

Todos los nodos que forman parte de la red Bitcoin mantienen una lista colectiva de todas las transacciones conocidas, a la que se denomina la cadena de bloques. Los nodos generadores, también llamados mineros, crean los nuevos bloques, aadiendo en cada uno de ellos el hash del último bloque de la cadena más larga de la que tienen conocimiento, así como las nuevas transacciones publicadas en la red. Cuando un minero encuentra un nuevo bloque, lo transmite al resto de los nodos a los que está conectado. En el caso de que resulte un bloque válido, estos nodos lo agregan a la cadena y lo vuelven a retransmitir. Este proceso se repite indefinidamente hasta que el bloque ha alcanzado todos los nodos de la red. Eventualmente, la cadena de bloques contiene el historial de posesión de todas las monedas desde la dirección creadora a la dirección del actual dueo. Por lo tanto, si un usuario intenta reutilizar monedas que ya usó, la red rechazará la transacción.

Mining

La generación de bloques se conoce en inglés como mining y puede traducirse al espaol como extracción por analogía con la minería del oro. Todos los nodos generadores de la red están compitiendo para ser el primero en encontrar la solución al problema criptográfico de su bloque-candidato actual, mediante un sistema de pruebas de trabajo, resolviendo un problema que requiere varios intentos repetitivos, por fuerza bruta, no determinista, de manera que se evita que mineros con gran nivel de procesamiento dejen fuera a los más pequeos. De esta forma, la frecuencia de localización de cada bloque sigue una distribución de Poisson y la probabilidad de que un minero lo encuentre depende del poder computacional con el que contribuye a la red en relación al poder computacional de todos los nodos combinados, lo que permite que el sistema funcione de manera descentralizada. Los nodos que reciben el nuevo bloque solucionado lo validan antes de aceptarlo, agregándolo a la cadena. La validación de la solución proporcionada por el minero es trivial y se realiza inmediatamente.

La red reajusta la dificultad cada 2016 bloques, es decir, aproximadamente cada 2 semanas, para que un bloque sea generado cada diez minutos. La cantidad de Bitcoins creada por bloque nunca es más de 25 BTC, y los premios están programados para disminuir con el paso del tiempo hasta llegar a cero, garantizando que no puedan existir más de 21 millones de BTC.

Los mineros no tienen la obligación de incluir transacciones en los bloques que generan, por lo que los remitentes de Bitcoins pueden pagar voluntariamente una tarifa para que tramiten sus transacciones más rápidamente. Co-

mo el premio por bloque disminuye con el paso del tiempo, en el largo plazo todas las recompensas de los nodos generadores provendrán únicamente de las tarifas de transacción.

1.2. Rendimiento computacional de la minería

Las estrategias para la extracción de Bitcoins se han ido perfeccionando progresivamente. En los primeros meses de funcionamiento de la red era posible extraer en solitario con una CPU estándar y obtener un bloque y sus 50 BTC asociados con una frecuencia relativamente alta. Posteriormente, la aparición de software de minería adaptado a tarjetas gráficas, mucho más eficiente, desplazó completamente a las CPUs. La minería por GPUs se fue profesionalizando, con grandes instalaciones en países con energía barata, configuraciones personalizadas con uso generalizado de overclocking y sistemas especiales de refrigeración. Con el aumento sostenido de la dificultad, los mineros comenzaron a organizarse en grupos independientes (en inglés, pools) para extraer de manera colectiva, desplazando así a los mineros en solitario que podían tardar meses o incluso aos en encontrar un bloque de manera individual. El propietario del pool se lleva una comisión por encontrar un bloque. Los pools también compiten entre ellos para intentar atraer al mayor número de mineros.

Durante el ao 2013 se han comenzado a distribuir FPGAs y ASICs para extraer Bitcoins de manera más eficiente. Si con la minería con CPUs y tarjetas gráficas, el coste de explotación provenía fundamentalmente del gasto energético, la comercialización de equipos especializados de bajo consumo está desplazando las inversiones de los mineros hacia hardware más sofisticado, e indirectamente hacia la investigación necesaria para el desarrollo de estos productos.

El 30 de julio de 2012, en el bloque 191 520, la dificultad marcó un máximo histórico y superó por primera vez el valor de dos millones, con una potencia de procesamiento de 14 TeraHash/segundo. Un ao y medio después, en enero de 2014, la dificultad se multiplicó por 1000 hasta alcanzar prácticamente el valor de 2000 millones, con una potencia de procesamiento de 14 PetaHash/segundo (14 000 000 000 000 000 Hash/segundo).

1.3. Planteamiento del problema

1.4. Objetivos y alcance del proyecto

1.5. Situación actual de la fdi-UCM

1.5.1. Hardware existente - rentabilización

1.5.2. Desaprovechamiento de recursos

Consumo energético

otros. . . ??

1.6. Posibles ampliaciones