Introducción al modelo de servicios distribuidos con IOTA.

Javier González Sánchez

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Criptomonedas

Nombre Profesor/a responsable de la asignatura

Víctor García Font

04/06/2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Introducción al modelo de servicios distribuidos con IOTA.*
Nombre del autor:	*Javier González Sánchez*
Nombre del consultor/a:	*Nombre y dos apellidos*
Nombre del PRA:	*Nombre y dos apellidos*
Fecha de entrega (mm/aaaa):	06/04
Titulación::	MISTIC
Área del Trabajo Final:	*Criptomonedas*
Idioma del trabajo:	*Español*
Palabras clave	*Criptomonedas, IOTA, modelo distribuido.*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

Este trabajo consta de una introducción a los modelos de servicios desde la creación de internet, pasando por los modelos centralizados, descentralizados y llegando al modelo distribuido que plantea IOTA.

Se ha hecho hincapié en el análisis de Bitcoin para asentar las bases de un modelo de servicios descentralizado autónomo y ciertamente afianzado y aceptado en internet.

Posteriormente se presenta IOTA como modelo distribuido, detallando el concepto principal que da forma a la criptomoneda como es el Tangle. Tras esta explicación se detalla la arquitectura y protocolo que forma esta criptomoneda.

Se comprueba como IOTA puede ser una solución fiable para las comunicaciones certificadas entre máquinas a futuro, puesto que está en un estado inicial de desarrollo que cuenta con desventajas.

Abstract (in English, 250 words or less):

Contents

Tabla de ilustraciones

Glosario

Moneda Virtual. Moneda no física utilizada a través de internet.

Criptomoneda. Es una moneda basada en la resolución de problemas matemáticos y el uso de cifrados.

Bitcoin. Nombre de la unidad de moneda, la red y el software de este ecosistema de gestión autoreglado de finanzas.

BTC. Nombre corto de Bitcoin.

Cadena de bloques (Blockchain). Plataforma encargada de registrar transacciones mediante protocolos distribuidos de consenso basados en bloques.

Bloque. En Blockchain es una estructura de datos que almacena un grupo de transacciones y se enlaza a la cadena de bloques apuntando al bloque anterior.

Nodo. Elemento software que proporciona los protocolos de conexión y funciones que permiten colaborar en una red distribuida.

Internet de las cosas. Red de comunicación entre los dispositivos del día a día.

IOTA. Tecnología de contabilidad distribuida que permite comunicar máquinas para intercambiar información y valores.

DLT o Distributed Ledger Technology. Definición de tecnología en red que permite la gestión de una economía distribuida.

DAG. En español Grafo Acíclico Dirigido es una estructura de datos basada en un grafo sin ciclos, dirigido y con múltiples enlaces en cada nodo.

Tangle. Un libro de contabilidad distribuido con forma de DAG que almacena toda la información de transacciones de la red IOTA.

Punta. En IOTA se refiere a las transacciones insertadas en el tangle pendientes de aprobación, que también puede ser denominada transferencia final o en inglés, tip.

Trinary. En español trinario es un sistema numérico con base 3.

Trytes. Conjunto de caracteres compuesto por el alfabeto latín en mayúsculas y el número 9, constando de 27 valores diferentes.

Trit. Puede tener los valores 0, 1 o -1.

Winternitx one-time signature. En el texto se encuentra como firma de un uso es un esquema de firmas que es usado para autorizar un gasto desde una dirección IOTA.

IRI, IOTA Reference Implementation. En español Implementación de referencia IOTA está escrita en Java y configura un nodo completo con toda la lógica que necesita para formar parte de la red e interactuar con ella. Tiene una API que permite conectarse a usuarios ligeros.

Semilla en IOTA. En inglés seed es la clave privada maestra de IOTA. Con ella se generar otras claves privadas y públicas.

Selección de punta. Algoritmo usado para la elección de transacción punta a validar.

Prueba de trabajo en IOTA, PdT. Proof of Work en inglés es un puzle computacionalmente difícil de resolver, en IOTA usan Hashcash.

1. Introducción

1.1 Contexto y justificación del Trabajo

Hoy en día existen muchos dispositivos conectados como ordenadores y teléfonos inteligentes que conectan contra servidores centralizados para el intercambio de información.

Existen dispositivos que hoy en día están en nuestras vidas y manejan información, captada habitualmente en el uso de un individuo o captada por sensores de manera pasiva, que son una importante fuente de información que podría ser relevante para el conocimiento individual o global y sin embargo no tienen la posibilidad de ofrecer esa información a terceros, o que si intercambian esta es contra servidores del propio fabricante del dispositivo.

IOTA es una plataforma de consenso distribuida que quiere involucrar a los dispositivos de la IoT en el intercambio de información de manera descentralizada, dando la posibilidad a que todos los dispositivos de un entorno puedan estar conectados y trabajar de manera colaborativa.

Como tecnología nueva requiere de un estudio para poder conocer cuáles son sus usos y sus limitaciones para conocer cuál es su proyección a futuro.

1.2 Objetivos del Trabajo

El documento trata de extraer de IOTA la siguiente información:

- Fundamentos y bases de IOTA.
- Características principales.
- Privacidad y seguridad.
- Aplicaciones en estudio.
- Identificación de posibles casos de uso.

1.3 Enfoque y método seguido

El enfoque seguido es estudiar los principales artículos académicos y libros de IOTA, sus predecesores y competidores en el mundo de las comunicaciones distribuidas.

Dando importancia a un análisis crítico y objetivo será necesario comparar las características de IOTA con la principal plataforma de consenso distribuida más madura e importante del momento como es Bitcoin.

Con este enfoque y método se pretende obtener un documento académico de estudio sobre IOTA que sirva de base en siguientes investigaciones.

1.4 Planificación del Trabajo

La planificación del trabajo no está solamente ligada a las PEC, sino que hacemos revisiones de manera habitual basándonos en hitos.

Por el momento, la planificación del trabajo en función de las PEC ha sido:

PEC 1: Entrega de índice con los temas a tratar.

PEC 2: Entrega del trabajo maquetado con información del Bitcoin.

PEC 3: Entrega del trabajo con la información de IOTA.

Además, hacemos revisiones periódicas según se avanzan hitos menores que los de la entrega de las PEC para ir haciendo un trabajo sólido.

1.5 Breve sumario de productos obtenidos

Se ha obtenido un conocimiento de las alternativas que existen para la emisión y recepción de información en internet, pasando del sistema centralizado, al descentralizado con Bitcoin y llegando al que pretende ser distribuido, IOTA.

1.6 Breve descripción de los otros capítulos de la memoria

2. Modelos de comunicación en internet.

Para comenzar a hablar de criptomonedas y sus modelos en red es importante conocer cuáles son los precedentes del intercambio de información a través de internet.

2.1. Introducción a las comunicaciones a través de internet

Nuestra sociedad está sometida a un cambio en el paradigma en que se desarrollan las gestiones y el tratamiento de la información. Hemos pasado de la gestión en papel a la gestión electrónica y con ella la creación de un modelo que relaciona al individuo con las entidades corporativas, monetarias y estatales que tiende a realizarse de manera lo más flexible y rápida posible, utilizando para ello las comunicaciones a través de internet.

Para la realización de cualquier gestión e intercambio de información a través de internet es necesaria la existencia de entidades que puedan verificar el origen, la información, y el destino de una transferencia de información para que pueda ser contemplada como válida.

Durante el desarrollo de internet las corporaciones y estados han empezado a comunicarse con los individuos a quienes prestan servicios a través de internet, creando el modelo de comunicación centralizado.

2.2. Modelo centralizado

Definición

El modelo centralizado es el más usado en internet cuando se quiere realizar transferencia de información con el fin de realizar gestiones.

Este modelo se basa en la creación de entornos centralizados localizados en una ubicación lógica de internet que ofrecen servicios a los usuarios. Es decir, si un usuario necesita hacer una determinada acción sobre un servicio web tiene que dirigirse a la URL de ese servicio, dependiendo así el éxito de la operación de la entidad que ofrece ese servicio.

En las comunicaciones se suele utilizar el modelo cliente-servidor, que es como se denomina al modelo que conecta a múltiples usuarios de un servicio contra los servidores que sirven ese servicio.

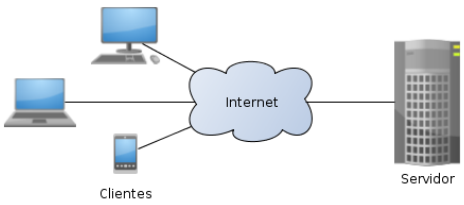

Ilustración 1. Modelo centralizado de cliente-servidor

Toda comunicación sobre un servicio requerirá verificar las comunicaciones que realizan los usuarios, así como verificar datos del propio usuario para identificarle unívocamente en el servicio si este lo requiere. Esta verificación es uno de los motivos de la existencia de este modelo, ya que cada entidad dará servicios a usuarios diferentes.

Otro de los motivos de la aplicación de este modelo ha sido la necesidad de almacenar información y centralizarla para el acceso de ella por parte de la entidad. La entidad podrá manejar los datos una vez los tiene en su poder.

Problemas del servicio centralizado

Que los servicios estén publicados en internet genera problemas de disponibilidad y seguridad que las entidades deben tener en cuenta.

Existen muchos motivos por los que un servicio pudiera quedar inaccesible en internet, como son la consulta masiva de un servicio, así como problemas técnicos en los servidores que los hospedan.

La seguridad es otro punto para tener en cuenta pues tiene que evitar que haya accesos no autorizados y fuga de información que pudiera comprometer los datos de los usuarios del servicio.

Estos dos problemas podrían darse en cualquier modelo, pero un sistema centralizado está mucho más expuesto que en un caso en el que hubiera una gestión distribuida por el hecho de que se sabe cómo acceder a ese servicio. Precisamente las entidades distribuyen en distintos servidores ubicados físicamente en distintos sitios para que haya una redundancia ante una falta de disponibilidad, así como utilizar dispositivos de seguridad como Firewalls para proteger las conexiones frente a usos maliciosos.

2.3. Modelo distribuido

Definición y características

En internet existe modelos distribuidos que permiten el intercambio de información entre pares de manera que no existen servidores centralizados a los que tengas que dirigirte para conseguir información.

Uno de ellos es el modelo de red entre pares P2P, en inglés Peer-to-peer, que no utiliza ni clientes ni servidores fijos.

Las principales características del P2P es que todos los nodos son iguales y se comportan de igual manera entre sí, actuando cada uno como cliente y servidor respecto al resto y sin necesidad de clientes ni servidores fijos.

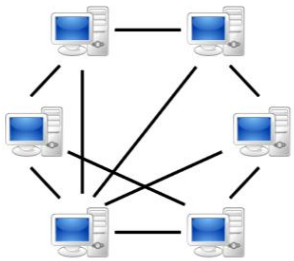

Ilustración 2. Red entre pares (P2P)

Un método distribuido como este se utiliza para la transmisión de información no solo entre dos pares, sino que, si la información está en muchos nodos, el nodo receptor puede descargar la información con un mayor ancho de banda limitada solo por la suma del ancho de banda de los usuarios que le sirven la información. Esto proporciona una alta disponibilidad del servicio dado que puede conseguirse a través de múltiples nodos.

Al no tener un servidor centralizado ninguna entidad influye en esa transmisión, solo intervienen los pares involucrados, por lo que se consigue una independencia sobre las entidades.

La seguridad no puede ser valorada igualmente que en el modelo centralizado, pues precisamente el único servicio que tienen los nodos de la red es de compartición de información y no servicios que requieran de verificación por parte de una entidad.

Limitaciones de las redes entre pares

La implantación de este modelo no ha llegado por el momento a todos los ámbitos de los servicios, limitándose habitualmente a compartir ficheros o retransmisión de contenido en tiempo real.

El protocolo no se ha usado para implantar servicios por parte de entidades debido a que los nodos no son controlados por estas y existe la dificultad de que en caso de que establecieran servicios en este modelo, estos pudieran ser vulnerados, o se hicieran un uso abusivo del mismo por nodos que pudieran ser maliciosos.

El problema de ofrecer un servicio en una red distribuida haciendo que todos los nodos se pongan de acuerdo en las decisiones, evitando ellos mismos por consenso el posible uso fraudulento o la confirmación de la realización del servicio, aun estando la red compuesta por nodos maliciosos o no fiables, se denomina problema de los generales bizantinos.

Este problema se ha estado estudiando durante años para resolverse de manera eficiente y no ha sido hasta hace poco cuando se ha propuesto una idea que se ha popularizado para ofrecer servicios a través de redes distribuidas.

Fue entonces cuando nació el Bitcoin.

3. Introducción a Bitcoin

3.1. Historia

La idea de Bitcoin fue inventada en 2008 por un individuo anónimo bajo el pseudónimo de Satoshi Nakamoto en la publicación de un trabajo titulado *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008). El año siguiente, en 2009, Nakamoto desarrolló su idea en un proyecto de código abierto en el que comenzaron a participar más desarrolladores, consiguiendo así la creación, desarrollo y mantenimiento de su proyecto.

Años más tarde Nakamoto abandonó el desarrollo del proyecto delegándolo en el grupo de desarrolladores que habían estado trabajando con él.

Bitcoin destacó entre otros proyectos contemporáneos de criptomonedas porque fue el primero en encontrar solución al denominado *Problema de los generales bizantinos* (Pérez-Solà, 2014), que, en pocas palabras, consiste en conseguir el acuerdo o consenso global en una red no confiable.

3.2. Red de comunicaciones

El protocolo de Bitcoin forma una red superpuesta a internet, conectando los nodos que la constituyen mediante el modelo de red de pares. Una red en la que todos los nodos pueden ofrecer y consumir servicios colaborando en el consenso.

Los nodos se conectan a la red y consecuentemente a otros nodos a través de peticiones DNS con una semilla a servidores predeterminados que facilitan direcciones IP de nodos asociados.

Además, cuando un nodo nuevo quiere conectarse con un nodo activo lo hace de la siguiente manera:

- Envío de versión del cliente software.
- Verificación del nodo activo y viceversa.
- Envío al nodo activo de su dirección.
- El nodo activo le envía su lista de direcciones conocidas.

Todas estas conexiones que se realizan entre nodos no están cifradas por defecto y será necesario utilizar servicios de terceros para proteger la privacidad de nuestra conexión.

Una vez sabemos cómo conecta un nodo y forma parte de la red, vamos a tratar la identificación de usuarios y la validación de emisión de las transacciones de un usuario, que hemos visto se hacen en el apartado 3.2.

3.3. Características generales

Bitcoin es una red de comunicaciones distribuidas basada en nodos en la cual estos emiten, validan y almacenan transacciones, formando un registro público distribuido.

Un nodo puede ser utilizado por un usuario para sustentar la red, para realizar transacciones o para ambas, a través de lo que denominaremos su dirección de Bitcoin.

Cuestión de claves

Los usuarios de Bitcoin necesitan poder ser identificados unívocamente y poder autorizar la emisión de sus transacciones. Para responder a estas necesidades cada usuario tiene una clave privada que podrá utilizar para la generación de claves públicas que identificarán cada una de sus direcciones Bitcoin con las que posteriormente podrá operar. Una vez generada al menos una dirección de Bitcoin el usuario puede firmar con su clave privada la emisión de cuantías en transacciones a otra dirección de Bitcoin, bien suya o de otro usuario que haya compartido su dirección de Bitcoin previamente con él.

Una vez que conocemos de la existencia de las claves, podremos entrar a definir las transacciones.

3.4. Transacciones

Ciclo de vida de una transacción

Una transacción es una emisión de una operación económica de una dirección Bitcoin a otra.

Una aproximación simplificada y abstracta podría resumirse en los siguientes puntos:

- La emisión de transacciones viene dada por los usuarios de la red que deciden hacer operaciones con una cuantía sobre otro usuario.
- La validación de esa transacción se realiza conjuntamente a otras, resolviendo un nodo la prueba de trabajo del bloque que las contiene, diciéndose que el nodo ha minado el bloque.
- El nodo que ha conseguido resolver la prueba del trabajo del bloque que contiene un conjunto de transacciones, recibe una gratificación en forma de valor de Bitcoin.
- El bloque resuelto apuntará al bloque anterior formando ahora parte de la conocida como cadena de bloques, que se dedica a almacenar el histórico de transacciones verificadas con el minado.

Para facilitar la compresión se ha adaptado la siguiente imagen (Bitcoin transaction, 2018) al idioma español:

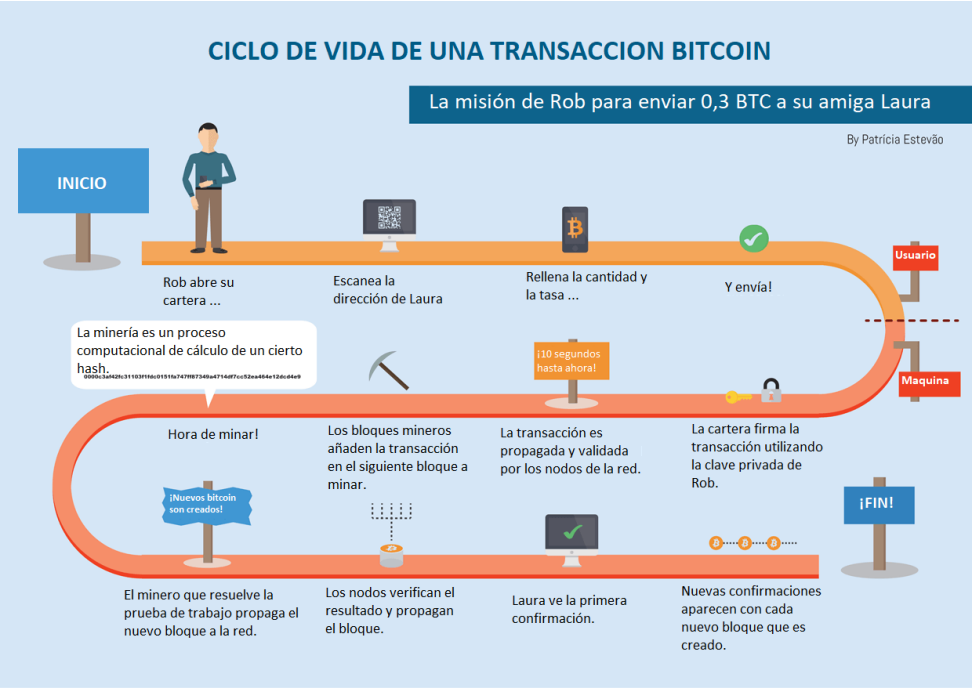

Ilustración 3. Ciclo de vida de una transacción de Bitcoin

Una vez conocido el ciclo de vida de una transacción se van a explicar los contenidos de una transacción y la relación que tienen estos con otras transacciones.

Estructura de una transacción

Las transacciones están vinculadas entre ellas para verificar su procedencia y validez, como introducción a lo que se explicará digamos que cada transacción recibida por una dirección de Bitcoin se referenciará a la transacción del emisor para poder consultar su validez.

Cada transacción se firma con la clave privada del emisor y consta de una cabecera que tiene un identificador hash único, una lista de entradas y otra de salidas de BTC, que serán transacciones previas entrantes y transacciones salientes, respectivamente, de una determinada dirección de Bitcoin propiedad de un individuo.

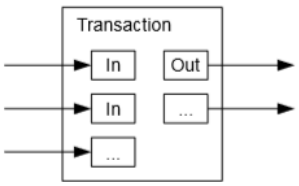

Ilustración 4. Representación abstracta de una transacción

Un *elemento de entrada* siempre contendrá la clave pública del emisor de la transacción, el identificador hash que apunta a la operación donde este emisor fue receptor y la cuantía de la transacción.

Un *elemento de salida* está compuesto por el valor que el emisor quiere transmitir a su receptor, la dirección BTC de dicho receptor, el cambio de la transacción que se le devolverá al emisor en caso de ser menor la cantidad emitida a la que recibió y está referenciada en el input del emisor y la tarifa de transacción.

Esta implementación consigue evitar algunas de las posibles situaciones que pudieran producir el doble gasto por parte de un usuario puesto que el receptor de una transacción siempre podrá comprobar la transacción de la que provienen sus BTC verificando que no ha sido gastado previamente. Cabe recalcar que no es el único mecanismo que ayuda a evitar el doble gasto, véase Prueba de Trabajo.

Se ha visto la relación que existe entre las transacciones, pasemos a ver cómo se registran estas en la red comprendiendo la estructura en la que se almacenan: la cadena de bloques.

3.5. La cadena de bloques

La cadena de bloques es una estructura de datos compuesta de bloques relacionados con su predecesor que almacena el histórico de transacciones validadas de Bitcoin.

Un bloque está referenciado a través del identificador hash de la cabecera del bloque anterior, creando una red interconectada de bloques en forma de pila donde cada bloque referencia a su predecesor hasta llegar al bloque inicial o génesis. Toda esta cadena de bloques es almacenada en cada uno de los nodos mineros que sustentan la red.

El bloque

Un bloque está formado por transacciones de los participantes en las redes y contiene una cabecera con campos, de los cuales uno es un identificador hash que permite identificarle unívocamente y otro de ellos referenciar a su bloque anterior.

Según se comenta en el apartado Structure of a Block (Antonopoulos, 2016), cada bloque contendrá un número variable de transacciones, que pueden llegar alcanzar y sobrepasar las 500, dependiendo del tamaño también de estas.

Los nodos mineros son los encargados de elegir las transacciones que formarán un bloque. En esta operación el bloque almacena a la transacción en su interior registrando la hora a la que se ha añadido.

Para que un bloque forme parte de la cadena será necesario llegar a validar este a través de un consenso de la red Bitcoin.

3.6. Minería y consenso

Cuando la transacción entra en un bloque, este necesita ser minado para su verificación.

El minado se basa en la resolución de una prueba de trabajo del bloque (Proof of Work, (Nakamoto, 2008)) que ha de ser resuelta computacionalmente por los nodos mineros, denominados así por su rol, que compiten entre ellos para conseguir ser los que resuelven exitosamente esta prueba.

El tiempo de resolución medio de cada bloque suele ser 10 minutos sea cual sea la potencia actual de la red Bitcoin, debido a que existe un algoritmo de reajuste de la dificultad de la prueba de trabajo.

Una vez se mina o se resuelve la prueba de trabajo de un bloque, este propaga el bloque para que el resto de nodos mineros verifique su trabajo, añadiéndose dicho bloque a la cadena de bloques en caso de ser validado por el resto de nodos, llegando a lo que se denomina el consenso distribuido.

Este consenso mayoritario está representado por la cadena más larga que corresponde a la cadena con más capacidad de cómputo empleada desde los inicios, tal y como se describe en el apartado Proof-of-Work (Nakamoto, 2008).

La honestidad de la red dependerá, tal y como se comenta en el apartado *Simplified Payment Verification* (Nakamoto, 2008), de que los nodos mineros honestos sigan proveyendo la mayor parte de la potencia de cómputo a la red, esta se mantendrá segura.

El mantener nodos honestos es uno de los principales fines que se trata de alcanzar con el medio de incentivos a los nodos mineros.

3.7. Emisión de moneda e incentivos

La red realiza el trabajo de emitir la moneda bajo el único criterio de minado de bloques, será necesario minar un bloque y que lo valide el resto de la red para recibir el incentivo en forma de BTC, así se consigue que la red se mantenga.

Inicialmente el incentivo era de 50 BTC y cada 4 años se divide entre 2, siendo a futuro quizás un problema para motivar a los nodos mineros a seguir trabajando.

A pesar de ser el único método de emisión de moneda, no es el único método de incentivar el sustento de la red por parte de los mineros, sino que existe el incentivo que representa la tarifa de transacción opcional.

Los mineros pueden tener en cuenta las tarifas de las transacciones para dar prioridad a estas para ganar dinero por el trabajo que invierten.

Es importante conocer que esta economía tiene un límite de moneda en circulación marcado en 21.000.000 BTC, que será el número total de monedas que podrá tener esta economía.

Cuando se llegue a la emisión del último BTC, los nodos mineros no tendrán un incentivo por mantener la red consensuada y según la implementación actual deberán recibir los incentivos de las comisiones en las transacciones, algo que se empieza a ver hoy por hoy, pudiendo discriminar entre las transacciones para elegir las que mayor comisión les ofrezcan.

Estado de emisión de la moneda

En cuanto al inicio de la emisión de la moneda (Bloques #0, 2009), los primeros 50 BTC fueron emitidos a la vez el día 3 de enero de 2009 y algo más de 9 años más tarde el día 12 de abril de 2018 existen cerca de 17.000.000 (Bitcoins in circulation, 2018).

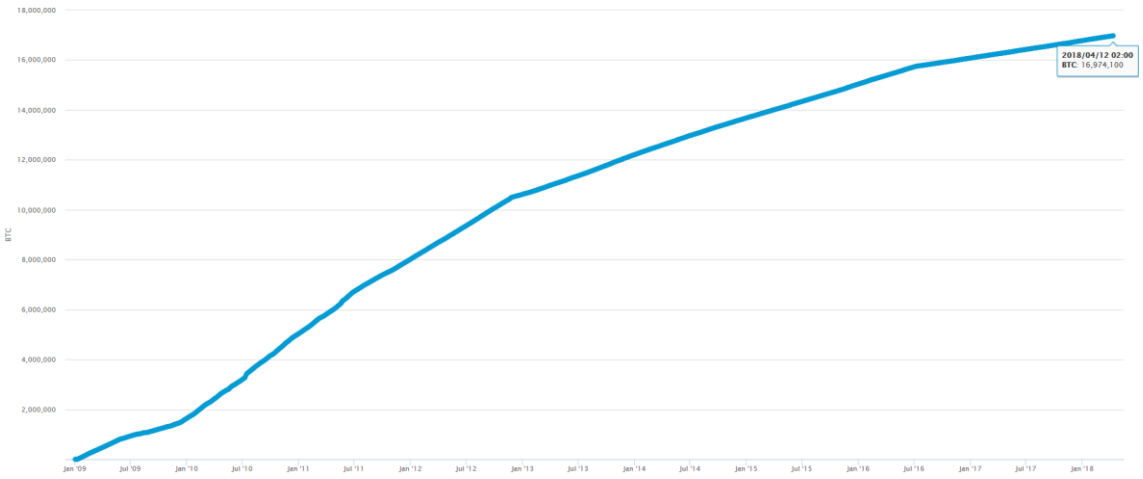

Ilustración 5. Bitcoins en circulación.

Según se puede observar en la Ilustración 3, la emisión de moneda cada vez es menor debido a que cada 4 años se reduce la recompensa por minar un bloque a la mitad.

Para facilitar el uso de la moneda existen decimales para el BTC, denominados mBTC correspondiendo con 1000 partes de 1 BTC.

3.8. Puntos fuertes y limitaciones

Bitcoin permite ofrecer servicios descentralizados

La red es capaz de validar transacciones legítimas de nodos que también lo son a pesar de la existencia de nodos ilegítimos que traten de hacer un uso fraudulento o ilegítimo de la red. Esto permite utilizar el sistema distribuido para ofrecer servicios por una entidad dada.

Bitcoin es una red distribuida accesible

Bitcoin es una red descentralizada y distribuida que valida transacciones y mantiene copias accesibles del histórico de las mismas en distintos nodos repartidos por la red.

Esto implica que ninguna entidad centraliza e interviene la información, siendo esta accesible por los involucrados en cada una de las transacciones y por nadie más.

3.9. Limitaciones

Bitcoin es una red difícilmente escalable

La dificultad con la que se inserta un nuevo bloque en la cadena será de 10 minutos (3.7. Minería y consenso), siendo un valor medio en una red en la que el número de usuarios no está limitado ni tampoco el número de transacciones que puede hacer cada uno.

Añadiendo además que, cada bloque contiene un número máximo de transacciones (3.6. La cadena de bloques) se obtiene que la red es capaz de hacer 7 transacciones[1] por segundo (Croman, y otros, 2017), algo que no es viable en una implantación global de esta tecnología.

Bitcoin es una red dependiente de la energía

La red Bitcoin depende de la capacidad de cómputo de todos sus nodos mineros que para competir entre ellos están en constante aumento de la potencia del hardware necesario para escalar los recursos de los nodos. La capacidad de cómputo entonces está sujeta a una fuente de energía eléctrica que se incrementa con la capacidad.

Esto representa un problema para tanto para el sustento de la red a futuro como para el bajo coste de las transacciones.
El sustento de la red depende de que se incentive a los nodos mineros de manera que tengan una ganancia respecto a los incentivos (ver punto 3.7) que ofrece la red frente al coste energético.

Para combatir la posible devaluación de la ganancia de los mineros que además podría verse disminuida por otros motivos (ver punto 3.7), será necesario que los usuarios apliquen subidas en las tarifas de transacciones que irán incrementándose de media en función al coste energético, pudiendo llegarse a un punto en el que no salga rentable la transferencia de pequeñas cantidades de dinero.

[1] El número de transacciones ha aumentado sensiblemente con el despliegue de la mejora denominada SegWit.

Ya existen estudios que avisan de este problema (Jacquet & Mans, 2018) y tratan de proponer alternativas al uso de la energía como base de criptomonedas, siendo IOTA una de las propuestas.

Hardware mínimo para operar transacciones

Por cada transacción cada nodo debe descargarla y verificarla a través de algoritmos de criptografía. Esta operación requiere de una potencia mínima de cómputo de todos los nodos participantes.

4. IOTA

En el desarrollo de las tecnologías de comunicación distribuidas, tras pasar por el modelo de cadena de bloques de Bitcoin, llega el Tangle de IOTA, un sistema que promete acabar con las limitaciones de Bitcoin y ofrecer soluciones de conectividad para las IOT.

4.1. Historia

Creada en 2015 y mantenida en la actualidad por la fundación sin ánimo de lucro del mismo nombre Fundación IOTA (Sonstebo, 2017), registrada oficialmente como fundación en 2017 con sede en Alemania y dirigida por David Sonstebo, IOTA es una tecnología de libro contabilidad distribuida de código abierto enfocada a resolver el problema de comunicación entre máquinas del Internet de las cosas.

El libro de contabilidad distribuida está basado en el Tangle, idea concebida por el doctor en matemáticas Serguei Popov, quien publicó las primeras versiones del documento en 2015, estando en la actualidad por la versión 1.4.2 del día 19 de Febrero, que será la que contemple este documento.

La implementación de la idea a código fuente de distintos lenguajes de programación vino por parte de Sergey Ivancheglo y Dominik Schiener, informáticos de profesión que forman aun parte importante en el desarrollo actual del proyecto.

IOTA está en una fase inicial de su implantación siendo una red que actualmente está compuesta principalmente por nodos de la fundación, que con la refactorización del código y nuevas actualizaciones pueden realizar operaciones sobre la red para corregir posibles problemas en la red o reducir el número de transacciones para liberar espacio de almacenamiento del libro de contabilidad distribuido.

Esto da a entender que es una red descentralizada que aspira ser una red distribuida con el paso de tiempo y la madurez del proyecto.

4.2. El Tangle

Tangle es una red que ideó Serguei Popov para resolver el problema del consenso en una red de comunicaciones distribuidas entre máquinas o nodos sin necesidad de servicios centralizados de verificación de transacciones.

Una definición de Tangle podría ser la de una red de transacciones emitidas por nodos participantes, en la que la validación de la propia red depende de estos nodos, que para emitir una transacción deberán validar dos transacciones ya existentes en la red. Este esquema

pretende quitar de la ecuación a los servicios de validación centralizados que abundan en internet, así como los nodos de validación distribuidos en Blockchain.

El hecho de que una transacción cree una relación de validación con otras dos previas hace que el crecimiento de la red siga una línea de tiempo desde la primera transacción hasta la última.

La estructura de datos con el conjunto de las transacciones se denomina Grafo Acíclico Dirigido o GAD (Weisstein, n.d.). Las propiedades de un GAD son, la inexistencia de ciclos entre transacciones, la inserción de los nodos en base al tiempo y que cada nodo puede estar conectada a varias por varios aristas o flechas, creando un grafo conexo de transacciones.

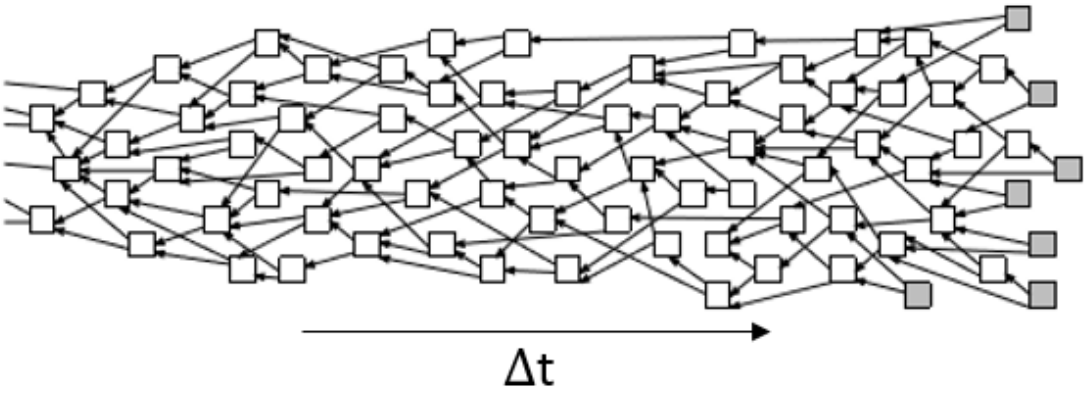

Ilustración 6. Incremento del GAD en función del tiempo

La no existencia de ciclos está dada porque una transacción no puede validarse a sí misma, es decir, no puede crear una relación de validación sobre sí misma.

En la Ilustración 7 se ha representado un GAD en el que las cajas son las transacciones emitidas por los nodos participantes en la red, mientras que las flechas representan la validación entre transacciones. La flecha se origina en la transacción que crea el vínculo de validación con la transacción destino de la flecha.

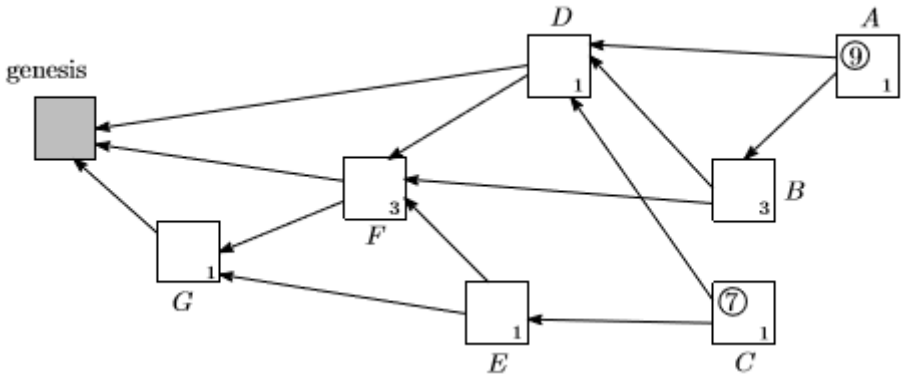

Ilustración 7. Ejemplo de Grafo Acíclico Dirigido del Tangle

El grafo siempre se verá en un formato de línea de tiempo de izquierda a derecha, estando la transacción origen en el extremo izquierdo, denominado transacción génesis, en el derecho las transacciones sin validar denominadas transacciones finales o puntas y en el centro habitualmente las validadas.

Entre estas transacciones podrían encontrarse las transacciones milestone[2] emitidas por la figura del coordinador, que discutiremos en la sección de protocolo.

En la Ilustración 7 vemos la relación de validación existente entre las transacciones del Tangle, donde podemos analizar el caso de ejemplo que ilustra y ver que la transacción A valida directamente las transacciones B y D e indirectamente valida las transacciones D, F, G y la transacción génesis. Esta forma de validación encadenada permite que se cree una historia de transacciones o libro de cuentas distribuido en el que las transacciones que se validaron quedarán referenciadas por las transacciones emitidas posteriormente a ellas.

A continuación, se muestra un diagrama que resume los pasos requeridos por un nodo para la emisión de una transacción.

[2] Transacción milestone o traducida a español hito se refiere a la transacción que emite el coordinador con valor cero.

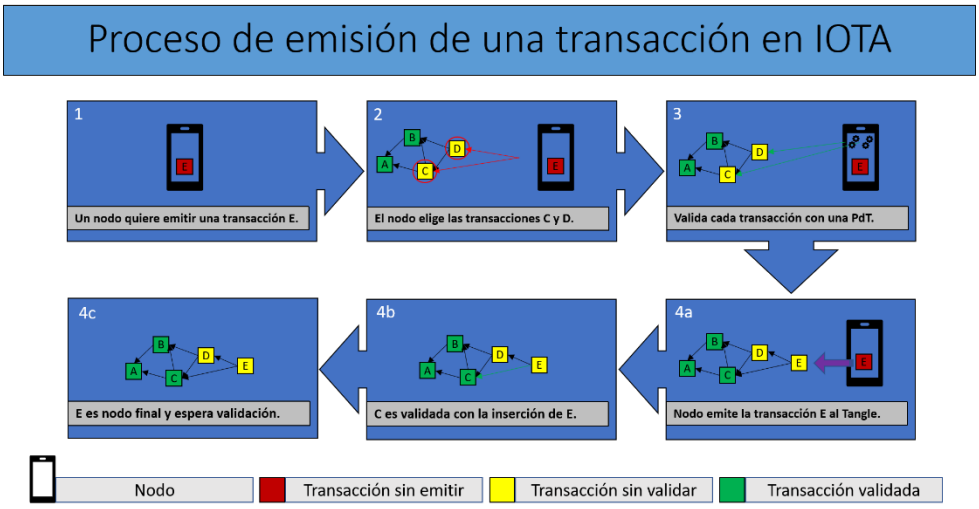

Ilustración 8. Emisión de una transacción

La definición del consenso es distinta en Bitcoin, y es que no existe un nodo con un rol de validador que necesite de un gran tiempo de cómputo para resolver una prueba de trabajo que valide las transacciones, y no es porque no exista una prueba de trabajo, sino porque ésta es menos costosa y es asumible por nodos de computación menores como ordenadores de sobremesa normales. El consenso en IOTA llega por el trabajo comunitario de todos los nodos en su labor de validación de transacciones.

Una transacción utilizará fondos previamente validados en otras transacciones y serán referenciados por el nodo que realiza dicha transacción. Solo tendrá que comprobar la existencia de estas transferencias y validar la última mediante una prueba de trabajo[3]. Es decir, la validación del grafo según pasa el tiempo, crea lo que se denomina consenso. No se tiene que repetir la prueba de trabajo de ningún nodo ya validado con la prueba de trabajo, tan solo comprobar[4] que el resultado de la prueba es correcto.

Cuando un nodo debe elegir qué transacciones debe validar utiliza los denominados algoritmos de selección de punta que veremos posteriormente. Estos algoritmos utilizan métricas de los nodos para resolver el camino que un nodo tomará para llegar al nodo final a validar.

[3] Prueba de trabajo o Proof of Work es un problema matemático al que es retado un nodo para la validación de una transferencia.
[4] Realizar la prueba de trabajo es mucho más complejo computacionalmente hablando que comprobar que el resultado de una prueba es correcto.

4.2.1. Las métricas del Tangle

Las métricas del Tangle vienen explicadas en la sección *Weights and more* del artículo The Tangle (Popov, 2018).

El *peso* en una transacción es proporcional a la suma de trabajo que el nodo emisor invierte dentro de ella, siendo más importante una transacción con un gran peso que una con menor peso.

El peso es generado a través de la ejecución de algoritmos de selección de transacciones finales, dando más importancia a la transacción que más veces ha sido validada por el resto de los nodos y pudiendo dejar a la transacción con menos validaciones aislada, quedando huérfana y no siendo tenida en cuenta como transacción válida en las futuras validaciones del Tangle y consecuentemente no aceptada.

El *peso acumulado* de una transacción se define como la suma del peso de la transacción más los pesos de los elementos del conjunto de transacciones que aprueban la transacción directa o indirectamente. Esta métrica aumenta en función de su cercanía con el nodo origen, teniendo más peso las transacciones más antiguas pues obtienen más aprobaciones.

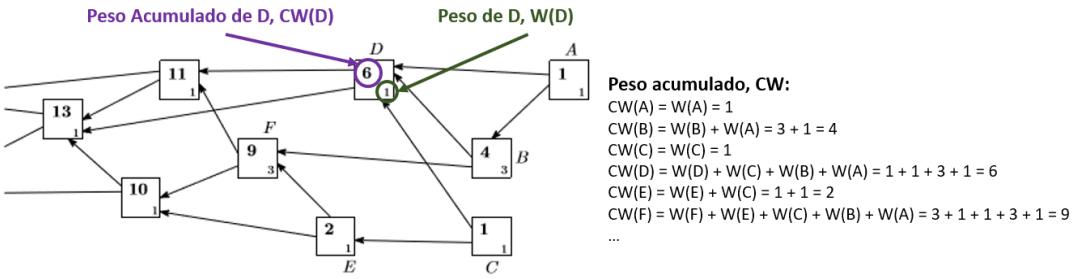

Ilustración 9. Peso y Peso acumulado en un Tangle

La *altura* es la cantidad de transacciones que se atraviesan en el camino más largo hasta el génesis.

La *profundidad* es la cantidad de transacciones que se atraviesan en el camino inverso más largo hacia algún nodo final.

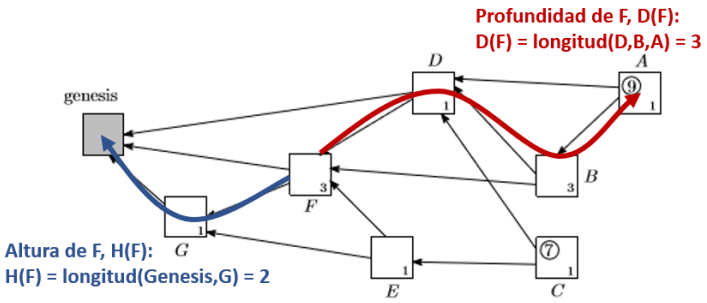

Ilustración 10. Métricas de Altura y Profundidad

4.2.2. Método de selección de transacciones

El método de selección de puntas o transacciones sin aprobar viene dado por un algoritmo estadístico denominado Markov Chain Monte Carlo o MCMC (Robert & Casella, 2012), cuyo cometido es crear una distribución equilibrada, en este caso dentro de la red conectada de IOTA, disminuyendo el tiempo de aprobación de transacciones nuevas y disminuyendo la probabilidad de elegir nodos deshonestos.

El algoritmo se basa en recorrer partes del Tangle realizando caminos aleatorios[5], con lo que en MCMC se denomina un caminante aleatorio, desde una transacción X a una transacción Y, donde X es una transacción con una profundidad dentro de un rango arbitrario, Y es una transacción punta a la que X llega aleatoriamente y se cumple el requisito de que Y puede aprobar X directa o indirectamente, siendo Y una transacción candidata para ser elegida para su validación por las nuevas transacciones entrantes en el Tangle.

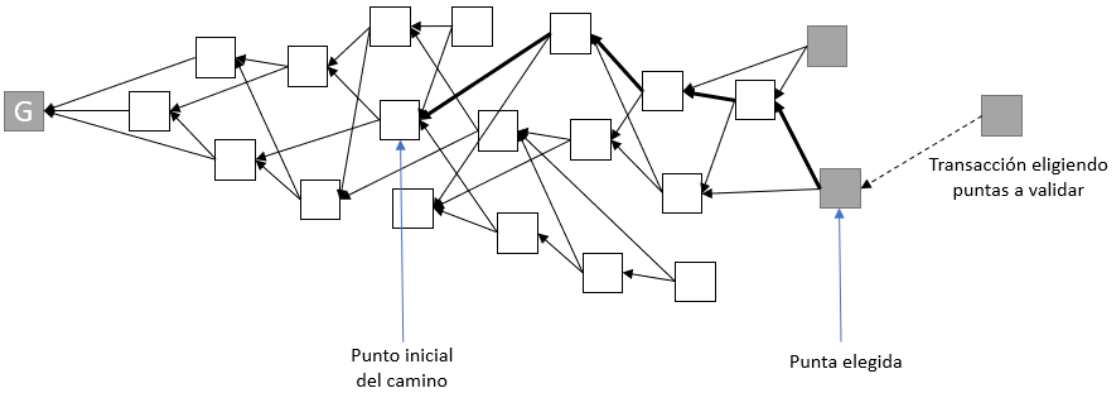

Ilustración 11. Elección de punta mediante camino aleatorio

Así, si el algoritmo detecta que se llega a una transferencia punta por debajo o encima de un umbral mínimo y máximo de tiempo establecido respectivamente, descartará ésta por

[5] Caminos aleatorios o Random Walk son algoritmos usados ampliamente en el entorno de la estadística, en este caso destinados a la elección de las dos transacciones que un nodo debe validar.

considerar que no es de un nodo honesto, consiguiendo que en el primer caso se descarten las transacciones punta lentas como candidatas a validar o en el segundo caso se descarten transacciones que puedan crear o alimentar Tangles paralelos[6].

Con este método, además, se disminuye el tiempo de elección de punta evitando el cálculo del peso acumulado del Tangle entero, tan solo se calculará desde la transacción inicial que apuntaba el caminante aleatorio.

4.2.3. Prueba de trabajo

Para validar una transacción será necesario realizar una prueba de trabajo. La prueba de trabajo consta de la resolución de un problema de cálculo matemático que implica conseguir un hash de manera aleatoria como resultado o *nonce*[7]. En esta prueba de trabajo existe un requisito de entrada y es que haya un número de ceros al final del valor que deberá ser como mínimo igual al peso de la transacción o como se denomina de manera formal Magnitud de Peso Mínimo.

Por ejemplo, si existe una transacción con peso uno, el hash que se deberá generar como prueba de trabajo contendrá al menos un cero al final.

Respecto a otras criptomonedas como Bitcoin, el nonce utilizado es menor[8] y la complejidad para obtenerlo viene impuesta por cada transacción, no por la potencia de cómputo de la red. Es decir, que en la red no se impone una dificultad equiparable a la potencia de cómputo de la red para mantener una tasa de transacciones estable.

Con la aplicación de la prueba de trabajo, se tratan de evitar varios problemas que pudieran poner en apuros a la red. Con el requisito de tener que realizar dos pruebas de trabajo de dos transacciones para poder emitir una transacción, se hace más compleja la aplicación a la red de ataques de spam, denegación de servicio o de recibir un ataque Sybil[9] (Douceur, 2002).

Este algoritmo se denomina Curl y es similar al usado en Hashcash, siendo ambos algoritmos de hashes que dado un valor de complejidad, el cálculo a realizar será más o menos complejo,

[6] Los Tangles paralelos se utilizan en escenarios de ataque a la red.
[7] Nonce es como se denomina comúnmente a los resultados de las pruebas de trabajo.
[8] El nonce está formado por un hash de 81 caracteres, como se detallará en la sección de Protocolo.
[9] El ataque Sybil consiste en tratar de convertir una red p2p honesta en deshonesta por parte de algún participante.

sin embargo teniendo el resultado del cálculo es muy sencillo comprobar su validez computacionalmente hablando.

4.2.4. Escenarios de ataque

En el Tangle existen diversos escenarios de ataque con el fin de hacerse con el control de la red, ya sea para dar prioridad a sus comunicaciones y transacciones o para permitir el doble gasto de un recurso económico. Se han extraído algunos casos del apartado Possible attack scenarios del documento The Tangle (Popov, 2018).

Un escenario de doble gasto sería en el que un usuario de la red emitiera dos transacciones referenciando un mismo recurso económico. Una de las transacciones se la haría a una segunda cartera suya, mientras que la otra la haría a un vendedor que le ofrece algo a cambio.

El vendedor recibe la transacción y envía el producto, momento en el cual el atacante tratará de usar la potencia de cómputo para emitir muchas transacciones de poco peso que aprueben la transacción hecha a su otra cartera.

Para que el proceso del doble gasto pudiera iniciar su carrera al éxito, el primer paso sería que una vez llegada la transacción al vendedor y éste haga el envío, el usuario eligiera validar dos transacciones antiguas en el Tangle que no tengan referenciada la transacción al comerciante en el Tangle a validar.

Con la potencia de cómputo adecuada y la generación de gran cantidad de transacciones, el usuario podrá crear una rama o subtangle que invalide la contraria siempre y cuando consiga un peso acumulado similar al del Tangle original, quedando la rama con la transacción al vendedor huérfana, perdiendo ésta toda validez ya que el vendedor tratará de retirar su nuevo balance y en el nuevo Tangle no estará referenciado.

Este es un problema para el IOTA debido a que hoy por hoy no existen muchos nodos y podría existir la situación, en que una entidad externa pudiera hacerse con el control del Tangle y meter así transacciones con doble gasto.

Para evitar este escenario el flujo de transacciones de los nodos honestos deberá ser mayor a la de los usuarios maliciosos y por ello en la actualidad, existen unos nodos coordinadores de la fundación Tangle que emiten transacciones con el único objetivo de validar transacciones y mantener un flujo constante y suficientemente alto para no permitir estos tipos de ataque.

Otra opción derivada de este ataque sería que un usuario malicioso formara una cadena denominada parásita que vaya aprobando de vez en cuando transacciones antiguas del Tangle

principal, a la vez que crece aprobando transacciones que el mismo puede estar emitiendo con distintas carteras. Una vez la suma de todos los pesos del Tangle fueran mayor en su red que en la red principal, podría darse que los participantes de la red del Tangle principal tomen la cadena del usuario malicioso como principal.

La solución que pudiera existir para este ataque y que ha adoptado el Tangle es el uso del ya conocido algoritmo de selección MCMC. Que la elección de nodos se haga de la manera más equilibrada posible consigue evitar estos tipos de ataque, puesto que evitan la creación de grandes ramas o cadenas alternativas de transacciones, pues la rama del usuario siempre tendría un peso acumulado menor que las ramas principales del Tangle.

El último escenario explicado en el documento, denominado el ataque de división[10], habla de un tipo de ataque que trata de partir el Tangle en dos: el Tangle principal y su propio Tangle. Esto lo hará tratando de mantener un balance entre ambos mientras se incrementan. El ataque funcionaría incluso con el algoritmo de selección de puntas MCMC.

Para defender este ataque con MCMC debería establecerse la posición inicial del camino aleatorio con una profundidad mayor a la normal, así será probable que se puedan elegir transacciones anteriores a la división y romper la igualdad mantenida por el atacante.

Otra defensa posible sería que la red tuviera una capacidad de cómputo mayor que el atacante y ser capaz de emitir un flujo mayor de transacciones vacías.

4.3. Arquitectura

La red IOTA consta de una arquitectura software que interconecta los dispositivos electrónicos inteligentes que denominamos nodos, permitiendo a estos realizar transacciones, como se ya vio en la parte del Tangle.

A continuación, se puede observar una representación gráfica de un grafo de transacciones generado aleatoriamente que muestra.

[10] Ataque de división es más conocido como Splitting Attack.

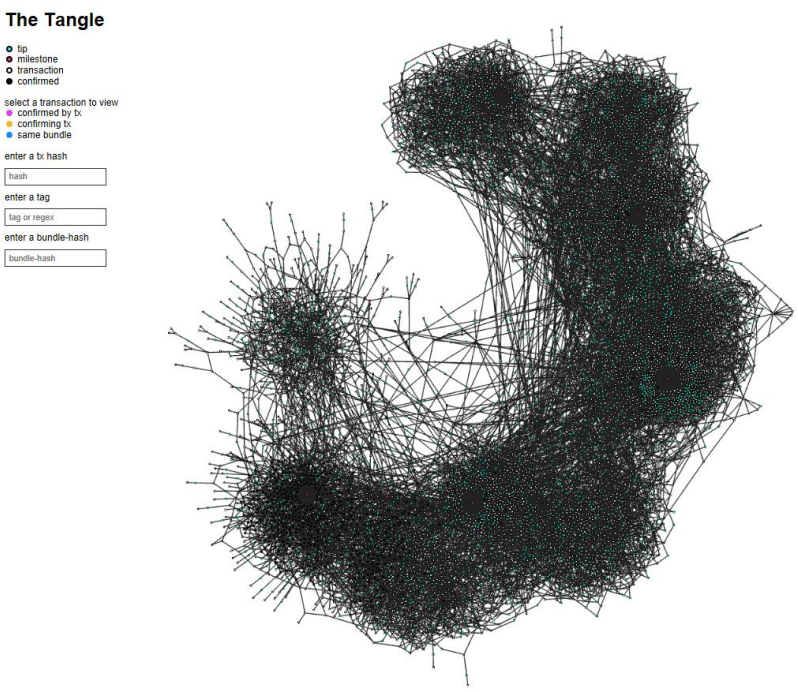

Ilustración 12. Simulación de conexión de cerca de 10.000 transacciones aleatoriamente generadas

Normalmente en la representación de IOTA se muestra este grafo obviándose de manera habitual la representación de los nodos.

En la siguiente imagen puede observarse como una red distribuida de nodos forma un Tangle en base a transacciones. El Tangle en realidad está almacenado entero o en parte dentro de cada uno de los nodos que se representan.

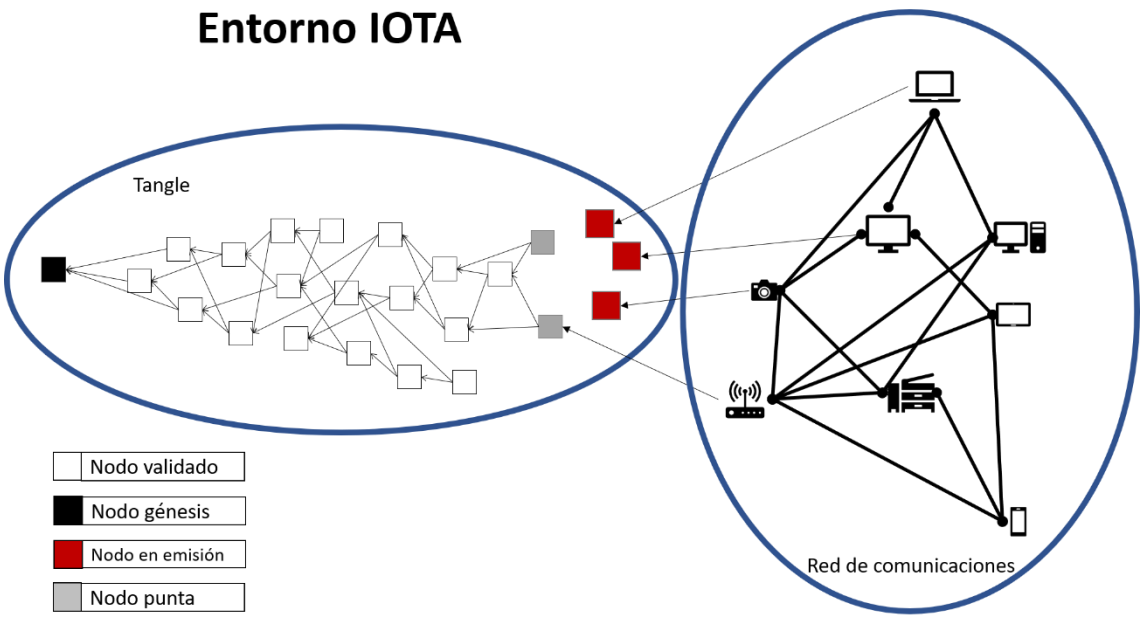

Ilustración 13. Representación de red de comunicaciones IOTA formando el Tangle.

Estos nodos son instancias software instaladas en sistemas electrónicos conectados a la red. Estas instancias dan a los nodos la lógica necesaria para mantener las comunicaciones entre ellos, para realizar y regular las operaciones sobre las transacciones de la red IOTA, siendo autosuficientes en todas las tareas, dejando atrás el uso de entidades en el caso del sistema centralizado y de los mineros en la cadena de bloques de Bitcoin.

Un usuario en esta red es una persona o entidad que opera sobre algún nodo de manera unívoca a través de un identificador que se denomina semilla. Un usuario podrá tener las cuentas que quiera.

Para la realización de transferencias por los usuarios, el nodo cuenta con una cartera, que es una interfaz que se encarga de retirar la información de un usuario en el libro de cuentas distribuido y darle los mecanismos necesarios para completarla.

4.3.1. Los nodos

Las funciones principales del nodo se centrarán en la gestión de las comunicaciones y de las transacciones de la red.

Vamos a ver cuáles son las funciones principales que tienen para realizar la operativa de gestión de transacciones.

Emisión de las transacciones al Tangle una vez preparada en el nodo para que pueda entrar en el proceso de validación a través de la difusión a todos los nodos.

Anunciar las direcciones[11] *del monedero* al Tangle para comprobar que no haya colisión con anteriores direcciones.

Recepción de transacciones del resto del Tangle por el método de difusión entre nodos con la finalidad de almacenar todas las transacciones difundidas por el resto de nodos, creando una copia[12] de parte del Tangle. Es decir, recibirá todas las transacciones emitidas por el resto de nodos, incluso las transacciones que tengan al usuario del nodo como receptor.

Consulta de fondos de una cuenta en el Tangle, buscando todas las claves publicadas en el Tangle de dicha cuenta.

[11] Las direcciones del monedero son cadenas alfanuméricas que apuntarán el balance de valor de IOTAs que un usuario tiene registrado en el Tangle. Se trata en la sección Cuentas y claves en IOTA.
[12] Se habla de copia de parte del Tangle porque existe la posibilidad que el nodo esté conectado a la red de manera que no le llegaran todas las transacciones y no pudiera recomponer el Tangle completo.

Método de selección de puntas que permiten elegir las transacciones a validar antes de poder emitir una transacción en el Tangle.

La enumeración de estas funciones será suficiente para entender las características principales de IOTA y el protocolo que hay tras ella.

Para disponer de estas funciones, los nodos deben tener unas características básicas que cumplir, como son la posibilidad de ubicar a cada nodo de manera unívoca en la red y que tengan la capacidad de cómputo necesaria para resolver las pruebas de trabajo.

A pesar de no distinguir entre distintos roles en cuanto a que las máquinas tengan distintos cometidos, sí que existen dos tipos de instalación de nodos en función de su capacidad de procesado y de reconocimiento único en la red.

Si un nodo no tiene la capacidad de cómputo necesaria para resolver las pruebas de trabajo, no conseguirá nunca emitir transacciones y en caso de emitir algunas pocas podrá ser tomado como un nodo perezoso y no elegido por los algoritmos de selección.

Los nodos, además, necesitan establecer una comunicación entre iguales en la red de manera unívoca a través del protocolo TCP/IP, es decir, con direccionamiento IP público si consideramos la red pública y no de privada en un test. Por desgracia en la actualidad los proveedores de servicios ofrecen a los pequeños clientes direccionamiento dinámico de IP, que cambia la dirección IP del usuario según pasa el tiempo. Conseguir una dirección IP privada tiene un coste que no es asumible para crear una plataforma distribuida de comunicación gratuita.

Por estos motivos existe la posibilidad de habilitar una API[13] en los nodos completos para que los nodos que no cumplen o alguno de los requisitos o ninguno, puedan interactuar con la red IOTA.

A este tipo de nodos sin capacidad de cómputo se les instala un software denominado cartera ligera[14], delegando las funciones de su cartera al nodo al que se hayan conectado.

Existen en internet listas de nodos completos públicos[15] que permiten a las carteras ligeras interactuar contra la red principal.

---

[13] Application Programming Interface es un conjunto de operaciones software que ofrece una librería para ser utilizado por otro software.

[14] Cartera ligera o Light Wallet en inglés se refiere a las instalaciones software que mantienen los datos principales de un usuario en un dispositivo de uso cotidiano.

[15] Se puede consultar un ejemplo de listas de nodos en http://iotasupport.com/lightwallet.shtml

Por el motivo de la delegación de funciones, es inevitable pensar que, si un usuario o entidad tendrá multitud de nodos de tipo de cartera ligera, sería conveniente que estas entidades tuvieran un nodo completo para delegarle las tareas a un nodo conocido.

4.3.2. El nodo coordinador

Al igual que existen nodos de los usuarios, debido a motivos de seguridad expuestos en los escenarios de ataque, también existen nodos propiedad de la fundación IOTA denominados coordinadores.

El rol de estos nodos es simplemente emitir transacciones de valor 0 cada dos minutos utilizando los algoritmos de selección de puntas recomendados para todos los nodos para así conseguir tener un flujo de transacciones constante, que ofrezca fortaleza ante los ataques explicados y para minimizar el número de transacciones de nodos honestos sin validar.

4.4. Características generales

IOTA aspira a convertirse en una red de comunicaciones capaz de proveer una infraestructura distribuida de comunicaciones segura entre iguales, que permita la comunicación autónoma y gratuita de los dispositivos inteligentes y conectados a internet que están emergiendo en la vida cotidiana, como pueden ser los vehículos y electrodomésticos.

Estos dispositivos inteligentes serán denominados en IOTA como nodos, que se comunican entre ellos formando la conocida estructura de red entre iguales o Peer to Peer.

Cuando hablamos de comunicación autónoma nos referimos al intercambio de información entre los nodos a través de transacciones sobre la red sin la mediación de los, tan necesarios hoy día, servidores que se encargan de validar nuestra información a través de sus servicios. Los participantes mismos de la red IOTA son capaces de validar las transacciones de otros nodos en la red mediante una prueba de trabajo sencilla computacionalmente hablando. Estas validaciones se hacen a través de las comunicaciones cifradas que hacen de esta red segura.

La validación en cadena de todas las transacciones y las dependencias entre ellas crean el Tangle, obteniendo con el proceso un consenso entre todos los nodos que forman la red.

Las principales características de IOTA son la descentralización, escalabilidad y transacciones libre de tasas.

4.4.1. Principales características de IOTA

La descentralización está motivada por la validación no centralizada que realizan entre los nodos, pudiendo hacer la validación de una transacción cualquier nodo completo.

La propiedad de la escalabilidad viene dada por el hecho de que para emitir una transacción se validen dos previamente, esto quiere decir que según se incrementa la tasa de transferencias se incrementa también la ratio de validaciones. Otro factor en la escalabilidad es la aprobación una a una de las transacciones, en detrimento de Bitcoin que aprueba las transacciones por conjuntos de ellas, denominados bloques.

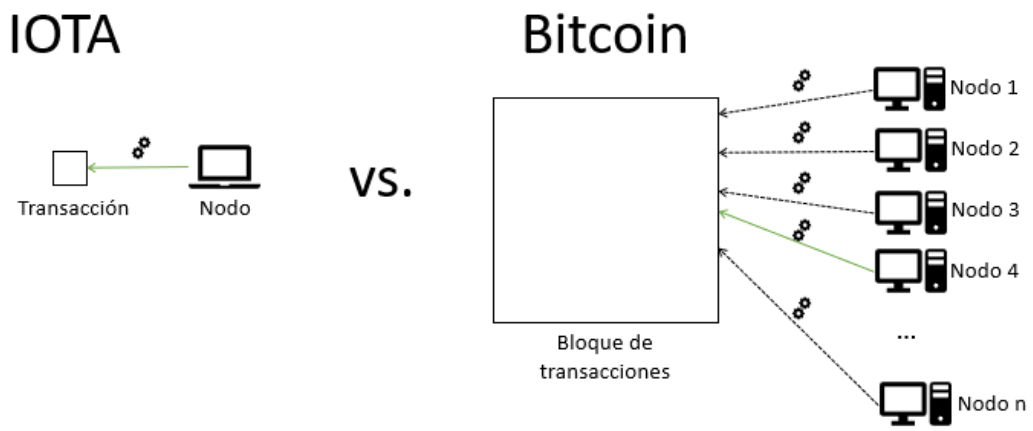

Ilustración 14. Validación de transacciones en IOTA y Bitcoin

En Bitcoin se validan por bloque y en IOTA se hace una a una, como se puede observar en la ilustración 14.

La inexistencia de tasas en las transacciones está motivada igualmente por la necesidad de validar el doble de transacciones que se quieran emitir, no existiendo así tarifas con las que premiar a los nodos, pues ya mantienen el consenso de la red por necesidad.

Tal y como se puede observar en estas tres características, la clave está en la validación propuesta por el Tangle.

4.4.2. Consenso entre iguales

El consenso se basa en la validación de una transacción por parte de múltiples nodos, haciendo una transacción tan fiable como el número de validaciones exitosas que han realizado el resto de los nodos.

La premisa exacta de este consenso es que un nodo debe validar dos transacciones previas antes de poder insertar la suya en el libro de contabilidad, formando una red de transacciones validadas, donde cada transacción debió validar otras y estas a su vez a otras.

En este modelo se eliminan la validación descentralizada que tiene el Bitcoin y la validación centralizada de los servicios típicos de internet, en detrimento de la validación de transacciones entre todos.

Este cambio tiene varias implicaciones, siendo la primera que en IOTA no existe una fuerte dependencia energética, debido a que no hay nodos mineros compitiendo por minar los bloqueos que en muchos casos contienen las mismas transacciones, realizando trabajos similares compitiendo por ser los primeros.

Una implicación más de eliminar los nodos mineros es que se elimina también el sistema de retribución por el mantenimiento de la red y la necesidad de cobrar una tarifa por cada transacción, dando a IOTA una de sus principales características: la gratuidad de la red.

4.4.3. Libro de contabilidad gratuito

El libro de contabilidad distribuido y consensuado se hace además gratuito. No existen tasas de transacción por los motivos que hemos visto.

Lo que si existe es la capacidad de intercambiar valores económicos, creando una economía virtual que es validada y almacenada en el libro de cuentas distribuido que forma el Tangle.

Otra característica de esta tecnología es que se pueden hacer intercambios de información entre nodos utilizando las ventajas que ofrece la validación distribuida, y es que una transacción puede marcarse con valor cero, pudiendo usar el campo mensaje en este caso para la inserción de la información que se quiera transmitir. Existe un módulo denominado Mensaje de Autenticación Enmascarado[16] que saca provecho de esta opción dando opciones de cifrar los mensajes.

4.4.4. La moneda

La moneda de IOTA es una criptomoneda que tiene un valor y permite que los usuarios de la red puedan intercambiar dicho valor entre ellos. Cuando hablamos de moneda de IOTA hay que tener claro que no son monedas numeradas, sino que son valores que se almacenan en la red de transacciones a través de un valor entero positivo y que estarán asignados a algún usuario.

[16] Masked Authenticated Messaging es un protocolo que permite añadir mecanismos de cifrado y autenticación a los mensajes.

La totalidad de las monedas de IOTA fueron generadas en el momento de la emisión de la primera transacción, siendo un valor constante y no modificable sin la posibilidad de generar nuevas monedas IOTA bajo ningún método.

La cantidad de monedas emitidas es de 2.779.530.283.277.761[17], pudiendo representarse con el sistema métrico decimal, lo que serían algo más de 2 Peta IOTA.

4.5. Protocolo

En este apartado se va a explicar la implementación técnica de IOTA, detallando las estructuras de datos y las comunicaciones que hacen posible su uso, tal y como se detalla en la documentación online del proyecto (Schiener, 2017).

4.5.1. Cuentas y claves en IOTA

Cuando un usuario quiere abrir una cuenta lo primero que debe hacer es tener una semilla, que le permita crear las direcciones o claves privadas para la realización de transacciones.

La semilla es la única vía de acceso a la cuenta del usuario y consecuentemente a sus fondos y se representa como una cadena de trytes[18]. Esta semilla puede tener tres longitudes distintas asociadas dependiendo de la seguridad[19] que queramos aplicar: baja, media y alta.

En todas las comunicaciones que se ve involucradas, se usa por defecto la seguridad alta, pudiendo negociarse otra más baja.

Una vez el usuario posee una semilla podrá crear un índice de públicas llamadas direcciones.

La creación de todas estas semillas y claves se hará siempre en el lado del cliente, motivo por el cual es importante que se tengan en cuenta medidas de seguridad tales como no generar estas por terceros y no hacer públicas ni semilla ni claves privadas.

IOTA usa en su modelo de privacidad firmas de una sola vez que permite tener un listado de las firmas utilizadas para que no se reutilicen.

4.5.2. La estructura de una transacción

Veamos la estructura de una transacción tal y como se muestra en la documentación online de IOTA (IOTA Fundation, 2018).

---

[17] El número total monedas IOTA se calcula con la fórmula (3^33-1)/2=2.779.530.283.277.761

[18] El alfabeto de Trytes es un conjunto de caracteres mayúsculas formado por el alfabeto latín y el número nueve que se utiliza habitualmente en IOTA para la generación de cadenas y hashes y puede encontrarse referenciado en las mismas como “trinary”.

[19] Los niveles de seguridad se codifican con 81 trits el bajo, 162 el medio y con 243 el alto.

Una transacción IOTA es codificada con un hash de 2673-trytes, constando de los siguientes campos:

Hash: Cadena de 81-trytes única de la transacción.

Fragmento de mensaje de firma (Signature Message Fragment): Cadena de 2187-trytes que puede contener en caso de existir un valor asociado a la transacción, la firma de la clave privada del emisor, de lo contrario podría ser un valor nulo representado con el carácter “9” o un valor mensaje que se quiera transmitir.

Dirección (Address): Cadena de 81 trytes que en caso de ser una salida[20] será la dirección del destinatario y del emisor de la transacción en caso de ser una entrada[21].

Valor (Value): Valor entero cuantificado en IOTAs que se transfiere.

Marca de tiempo (timestamp): Valor entero que representa la fecha de la transacción.

Índice actual (currentIndex): Valor entero con el índice de transacción en el paquete.

Último índice (lastIndex): Valor entero con el número total de transacciones en el paquete.

Paquete (bundle): Cadena de hash de paquete de 81 trytes usada para identificar un paquete que agrupa campos de transacción que deben validarse de manera única para evitar inconsistencias. Los campos son el destinatario, el emisor, la firma del emisor y el valor sobrante de la transacción que será enviado de vuelta al emisor. Una transacción puede contener múltiples entradas y salidas.

Transacción Trunk (trunkTransaction): Cadena de 81 trytes que representa la primera transacción aprobada con esta transacción.

Transacción Branch (branchTransaction): Cadena de 81 trytes que representa la segunda transacción aprobada con esta transacción.

Nonce: Cadena con un hash de 81 trytes conseguido a través de una prueba de trabajo y necesario para formar parte de la red.

Una transacción real se vería como en el siguiente cuadro.


```
{
"hash":"IPQYUNLDGKCLJVEJGVVISSQYVDJJWOXCW9RZXIDFKMBXDVZDXFBZNZJKBSTIMBKAXHFTGETEIPTZGNTJK",
"signatureMessageFragment":"99999999999999999…",
```


[20] Output o salida es una cantidad de valor IOTA que le llega a un destinatario en una transacción.
[21] Input o entrada es la cantidad de valor IOTA que el emisor pone en la transacción para emitir un valor.

```
"address":"A9RGRKVGWMWMKOLVMDFWJUHNUNYWZTJADGGPZGXNLERLXYWJE9WQHWWBMCPZMVVMJUMWWBLZLNMLDCGD
J",
"value":0,
"tag":"99999999999999999999999999",
"timestamp":1482522289,
"currentIndex":0,
"lastIndex":0,
"bundle":"TXEFLKNPJRBYZPORHZU9CEMFIFVVQBUSTDGSJCZMBTZCDTTJVUFPTCCVHHORPMGCURKTH9VGJIXUQJVHK
",
"trunkTransaction":"99999999999999999999999999999999999999999999999999999999999999999999999
9999999999",
"branchTransaction":"99999999999999999999999999999999999999999999999999999999999999999999999
99999999999",
"nonce":"99999999999999999999999999999999999999999999999999999999999999999999999999999999”
}
```


Ilustración 15. Objeto transacción en formato diccionario

4.5.3. Emisión de una transacción

Los pasos que ha de realizar un nodo para la emisión de una transacción constan, de la firma de esta, de la selección de dos transacciones previas y la realización de la prueba de trabajo de cada una de ellas.

A modo resumen se podría decir que los pasos son:

- Firma de la transacción a emitir.
- Elección de transacciones a validar.
- Validación de las transacciones mediante prueba de trabajo.

El primer paso será la creación de una transacción por parte del usuario, rellenará sus campos y confirmará la emisión de la transacción asociándola a una dirección.

Una vez firmada la transacción, el siguiente paso es elegir dos transacciones pendientes de validar del libro de contabilidad mediante un algoritmo de selección.

Como tercer y último paso, el nodo deberá validar las transacciones elegidas mediante la realización de una prueba de trabajo por cada una de ellas, almacenando en los campos trunkTransaction y branchTransaction las direcciones de las transacciones validadas y el campo resultado de la prueba de trabajo, el nonce.

Estos tres pasos componen la emisión de una transacción y la validación de transacciones previas, que no es lo mismo que el ciclo de vida de la transacción que se trataba de emitir pues quedará el paso de validación, teniendo otro nodo que repetir estos mismos pasos.

Para la realización de transacciones se realizará bajo la estructura de datos denominada paquetes, explicando en el siguiente paso el proceso de firma, que quizás a estas alturas sea el más desconocido, puesto que la elección de transacciones y la realización de prueba de trabajo se han cubierto.

4.5.4. Paquetes

Los paquetes son estructuras virtuales que permiten la asociación de transacciones de entrada y salida con transacciones de información permitiendo la emisión de una transacción.

Un usuario guarda sus fondos en un índice de direcciones que deberán ser referenciadas para poder utilizar dichos fondos en alguna transacción. Esto quiere decir que, para la emisión de una transacción, será necesario crear varias transacciones de entrada que referencien direcciones con fondos y al menos una transacción de salida que referencie la dirección receptora y el valor de la transacción.

El paquete es un conjunto de transacciones que el usuario que incluye la transacción objeto de la operación y transacciones auxiliares. En el Tangle se verán como distintas transacciones referenciadas por un mismo paquete, siendo una estructura atómica a nivel de validación de la transacción objeto. En caso de no aprobarse alguna de las transacciones que forman el paquete, de nada valdrá la validación del resto.

Los campos de las transacciones que las relacionan en un paquete son los de índice, último índice del paquete y el hash del paquete.

El flujo principal para crear un paquete en el paso previo para la emisión de una transacción con valor IOTA asociado, sería el siguiente:

1. Creación de transacción de salida. Se inserta el valor a traspasar y la dirección del destinatario.
2. Inserción de transacciones de entrada. Se necesitará obtener todas las direcciones del usuario del libro de cuentas hasta que la suma de ellas iguale o supere el valor de la transacción de salida. Por cada transacción de entrada se crea una transacción de valor cero denominada transacción de información que almacene una de las partes de la firma.
3. Creación de transacción de devolución o reembolso. En caso de que las direcciones entrantes necesarias sumen un valor mayor al que se quiere emitir en la transacción de salida, deberá crearse esta transacción de reembolso que tendrá como destinatario una nueva dirección nuestra.

4. Validación del paquete. En este paso se enumeran las transacciones por sus campos índices y se indica cual es el número total de todas en cada una de ellas. Una vez referenciados, se genera un hash a través del algoritmo de Kerl[22], que tomará como entrada una a una las transacciones del paquete y sus datos.
5. Firma de transacciones entrantes. La firma de transacciones entrantes es el motivo por el cual hemos creado una transacción vacía asociada a cada una de estas transacciones. A partir de la semilla y el índice y utilizando el Generador de Fragmentos de Firma se generarán para cada transacción salientes una firma en dos partes, ubicando la primera parte en la transacción de entrada y la segunda en su transacción asociada.

A partir del recurso web (Lu, 2018), se ha creado la siguiente ilustración que enumera y detalla los pasos que se siguen para generar el paquete de una transacción.

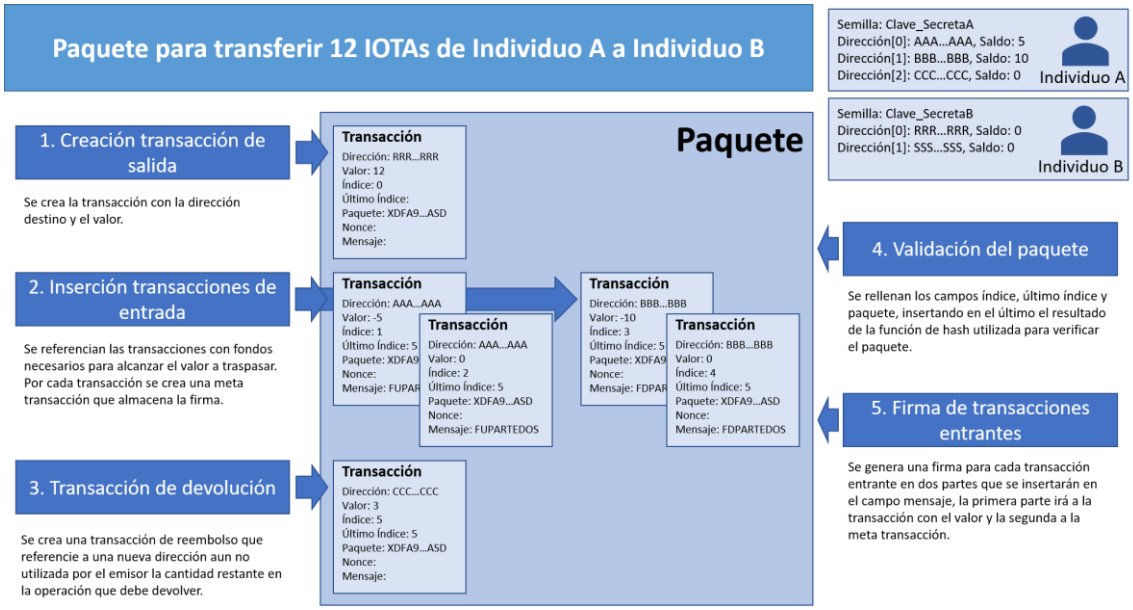

Ilustración 16. Paquete de una transferencia

4.5.5. Gestión de claves

Para poder acceder a la red se necesita una clave denominada semilla. La semilla es una clave privada maestra con la que se generan las claves privadas y públicas para lo que podría denominarse una cuenta de usuario, siendo la clave única de autenticación.

[22] El algoritmo de Kerl es una función hash basada en SHA-3.

Una vez autenticado el usuario podrá revisar su balance de valor IOTA, y deseará emitir o recibir transacciones en su cuenta de usuario, para ello usará el concepto de direcciones que son claves públicas derivadas de la semilla, el nivel de seguridad y el índice de clave.

El usuario compartirá con otros usuarios su dirección en ese momento en caso de querer recibir transacciones. Todo valor de IOTA que reciba el usuario se guardará en la dirección.

Sin embargo, cuando un usuario realice una transacción, deberá cambiar de dirección dónde almacenar el balance de su valor posterior a la transacción.

La reutilización de direcciones puede crear un problema de seguridad para el usuario, debido a que en la emisión de transacciones con valores IOTA asociadas, se firman las transacciones con unas firmas que se derivan directamente desde la semilla. Si un usuario reutilizara de manera sistemática las direcciones, un tercero podría seguir el historial de transacciones y obtener todas sus firmas, pudiendo probar semillas que aplicando el mismo algoritmo de firmas de transacciones coincidieran en el resultado de esas firmas, viéndose así comprometidos sus fondos.

Para solucionar este problema, IOTA plantea el uso de firmas o direcciones de una sola vez de Winternitz[23], implementando un esquema de generación de direcciones determinista utilizando un índice y una semilla para su cometido.

El esquema permite a los usuarios crear direcciones que se pueden reconstruir tan solo con la semilla, el índice y el nivel de seguridad, permitiendo que la operación aplicada ofrezca siempre el mismo resultado. Esto permitirá a un usuario con su semilla, poder buscar su histórico en el libro de cuentas sin la necesidad de almacenar ninguna información en local más que su semilla.

La consulta de fondos de un usuario se hace mediante la búsqueda de las direcciones en orden secuencial y ascendente con la suma de todas estas direcciones. La cartera no almacena las direcciones y sus valores localmente, sino que genera dichas direcciones cada vez que lo necesita en base al esquema de semilla e índices. Para iniciar la consulta del balance de una cuenta, se empezará buscando por la clave correspondiente al índice 0 del usuario que lo solicita, repitiendo esta búsqueda incremental aumentando el índice en 1, quedándose con la historia desde la dirección correspondiente al primer índice hasta el último que obtenga un resultado y así obteniendo el balance de la cuenta del valor acumulado de la historia. Dado

[23] Winternitz one-time signatures u W-OTS

este método, en caso de no haber anunciado una dirección al libro de cuentas en una transacción, el usuario podría perder el acceso a la dirección y con ella a sus fondos.

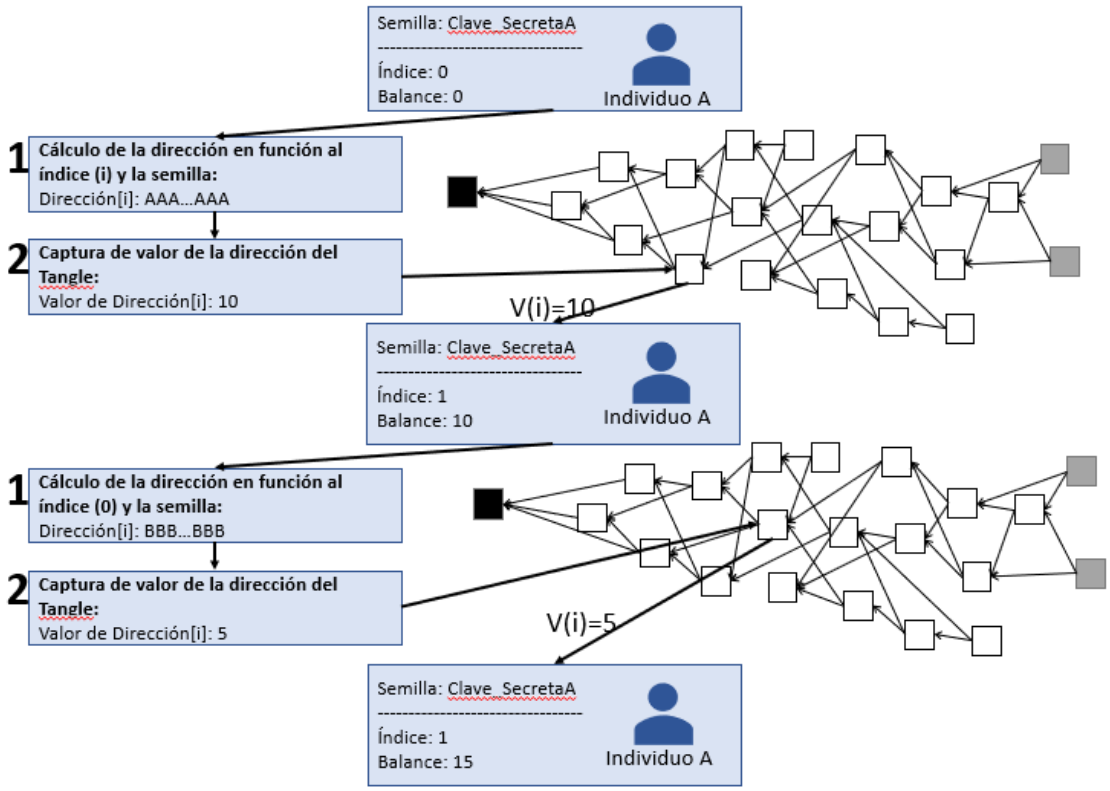

Ilustración 17. Consulta del saldo a un usuario con dos direcciones en su historial

En una transacción de valor mayor que cero IOTAs que se inserte en el libro de cuentas, que estará compuesta por un conjunto de entradas y salidas, las entradas corresponderán a las direcciones con fondos del usuario que sumen al menos el valor que se quiere transmitir. Las salidas a las direcciones del receptor de la emisión y del receptor del balance restante de la transacción, que será el usuario emisor. El balance restante, en caso de haberlo, se recibirá en la nueva dirección que el emisor creó con la emisión de la transacción. De esta manera, esta nueva dirección podrá ser reutilizada para recibir fondos de transacciones entrantes, pero no debería ser reutilizada en la emisión.

Actualmente, las carteras de IOTA permiten la generación de direcciones bajo este esquema, así como su publicación a la red.

Un paso que se ha de llevar a cabo cuando se genera una nueva dirección es que debe ser anunciada al libro de cuentas, pues existe la posibilidad que un usuario haya depositado sus fondos en la misma y de no estar la dirección registrada en la red podría no poder visualizar y recuperar dichos fondos, dado que todos los datos válidos se consiguen a través de la red y no de datos en local.

4.6. Particularidades

4.6.1. Instantánea

Por motivos de mantenimiento y con el fin de optimizar el Tangle cada cierto tiempo, se realiza una instantánea o Snapshot que borra todas las transacciones del Tangle con valor distinto de cero, dejando solo las transacciones con direcciones por valor de más de cero IOTAs.

Esto sucede porque existen direcciones que quedarán vacías de valor de IOTA, ya sea porque sea una dirección utilizada en una transacción y posteriormente quedando relegada con valor cero o en transacciones de comunicaciones de datos entre máquinas, que usan el campo del valor para transmitir mensajes.

Habiendo explicado anteriormente como se referencian los fondos a través de direcciones, no es de extrañar que se pierda la referencia a estos, debido que, si un usuario ha utilizado n direcciones, solo habrá quedado vigente la transacción n habiéndose borrado las n-1 direcciones.

Hoy por hoy las carteras no tienen la funcionalidad de buscar fondos en un conjunto incremental de direcciones que son cero, puesto que habrá que tenerlo en cuenta para hacer de nuevo la generación y adjuntado de claves a la Tangle hasta llegar a la transacción con valor.

Tras el mantenimiento se volverán a insertar direcciones en el Tangle de usuarios que emitan valores y tengan fondos asociados a su cuenta.

4.6.2. Pérdida de fondos

Ahora hablemos de la posibilidad de pérdida de visibilidad de los fondos de los usuarios, tal y como se explica en el artículo web (IOTA Hispano, 2017).

Han existido históricamente dos instantáneas que ha llevado asociadas otros trabajos como la implementación de una nueva función de PdT, obligando a los usuarios a actualizar su cartera a esta nueva implementación.

Dada la naturaleza intervencionista en estos primeros pasos de la plataforma, IOTA decidió asociar la propiedad de las transacciones con direcciones reutilizadas y de las transacciones de los sistemas que no habían realizado la actualización al nuevo sistema de prueba de trabajo.

Los usuarios afectados por la asignación de sus fondos por parte de IOTA, pueden reclamar los mismos con una aplicación.

5.1. Puntos fuertes

En esta sección recogemos los puntos fuertes de IOTA para poder hacer sitio en el mercado de las comunicaciones y crear lo que denominan la economía de las máquinas.

5.1.1. Comunicación libre

IOTA propone un protocolo de comunicación entre máquinas sin tarifas y basado en la seguridad que pretende ser un estándar en un mundo que está en plena expansión como es el entorno del internet de las cosas, donde no existe un referente claro. Así se pretende dar conectividad a los dispositivos a través de un protocolo gratuito.

5.1.2. Comunicación segura

La comunicación entra pares sobre sistemas de autenticación y cifrado hacen de la tecnología una candidata para establecer comunicaciones entre dispositivos.

5.1.3. Descentralización de los servicios

Se propone una alternativa distribuida para la publicación de servicios en internet entre pares, haciendo escalable la demanda y la oferta que plantea la inserción de todos los dispositivos del internet de las cosas como consumidores y generadores de contenido.

5.1.4. Pago por uso

Se permite el uso de la infraestructura para la compartición de recursos entre los dispositivos pudiendo fijar un valor monetario. Esto abre la veda de lo que denominan la economía de las máquinas, dónde una máquina calcule que necesite energía y pueda comunicarse con una que la genere, pudiendo realizar un pago con valor monetario por la energía.

5.1.5. Infraestructura gratuita

La infraestructura está mantenida por los nodos que emiten las transacciones debido a que tienen la obligación de validar dos transacciones previas. Esto hace que no se tenga que pagar a ninguna parte, consiguiendo una infraestructura gratuita.

5.2. Limitaciones

Las limitaciones de la plataforma por el momento están sujetas a su grado de desarrollo. En la actualidad IOTA está intervenido por la fundación y eso hace que los usuarios puedan no querer invertir

5.2.1. Red intervenida

La red está intervenida por la fundación, prueba de ella son la existencia de nodos coordinadores y nodos completos que aportan a la red y les ayuda a resolver los problemas que puedan surgir en momento puntuales en el desarrollo del proyecto. Esto es un punto negativo dado que existe un actor que puede modificar a su gusto el proyecto.

Bibliography

Antonopoulos, A. M. (2016). *Mastering Bitcoin* (2 ed.). O'Reilly. Retrieved from https://github.com/bitcoinbook/bitcoinbook/releases/tag/second_edition_print2

Bitcoin transaction. (2018, 03 3). Retrieved from Bitcoin Wiki: https://en.bitcoinwiki.org/wiki/File:Bitcoin-transaction-life-cycle.png

Bitcoins in circulation. (2018, 04 24). Retrieved from Blockchain: https://blockchain.info/es/charts/total-bitcoins?timespan=all&showDataPoints=true

Bloques #0. (2009, January 03). Retrieved from Blockchain: https://blockchain.info/block-index/14849

Croman, K., Decker, C., Ittay, E., Gencer, A. E., Juels, A., Kosba, A., . . . Wattenhofer, R. (2017). *On Scaling Decentralized Blockchains.* Retrieved from http://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf

Douceur, J. R. (2002, 01). *The Sybil Attack.* Retrieved from Microsoft Research: https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf

IOTA Fundation. (2018, 06 04). *The Anatomy of a Transaction*. Retrieved from IOTA Docs: https://iota.readme.io/docs/the-anatomy-of-a-transaction

IOTA Hispano. (09 de 11 de 2017). *Entendiendo el problema de Balance cero en la wallet IOTA*. Obtenido de IOTA Hispano: http://www.iotahispano.com/2017/11/09/entre-a-mi-wallet-y-tengo-balance-0-que-hago/

Jacquet, P., & Mans, B. (2018). *Green Mining: toward a less energetic impact of cryptocurrencies.* Retrieved from https://arxiv.org/pdf/1801.07814.pdf

Lu, L. (2018, 01 11). *In-depth explanation of how IOTA making a transaction (with pictures)*. Retrieved from Medium: https://medium.com/@louielu/in-depth-explanation-of-how-iota-making-a-transaction-with-picture-8a638805f905

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronica Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf

Pérez-Solà, C. (2014). *Bitcoins y el problema de los generales bizantinos.* Alicante: UAB. Obtenido de https://web.ua.es/en/recsi2014/documentos/papers/bitcoins-y-el-problema-de-los-generales-bizantinos.pdf

Popov, S. (2018). *The Tangle* (Vol. 1.4.2).

Robert, C., & Casella, G. (2012). A Short History of Markov Chain Monte Carlo: Subjective Recollections from Incomplete Data. Retrieved from https://arxiv.org/pdf/0808.2902.pdf

Schiener, D. (2017). *IOTA Guide.* Retrieved from Gitbook: https://legacy.gitbook.com/book/domschiener/iota-guide/details

Sonstebo, D. (2017, 11 14). *IOTA Foundation*. Retrieved from IOTA Blog: https://blog.iota.org/iota-foundation-fb61937c9a7e

Weisstein, E. (n.d.). *Acyclic Digraph*. Retrieved from Mathworld: http://mathworld.wolfram.com/AcyclicDigraph.html