Seguridad en la Internet de las cosas. Estudio de IOTA para el Internet of Things

Montse Sorrius Martí

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Área del trabajo final

Nombre Consultor: Víctor García Font
Nombre Profesor responsable de la asignatura: Víctor García Font

Fecha Entrega: 04/06/2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Seguridad en la Internet de las cosas. Estudio de IOTA para el Internet of Things.*
Nombre del autor:	*Montse Sorrius Martí*
Nombre del consultor/a:	*Víctor García Font*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	04/06/2018
Titulación::	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC).*
Área del Trabajo Final:	*TFM - Seguridad en el Internet de las cosas.*
Idioma del trabajo:	*Castellano*
Palabras clave	*Criptomonedas, IOTA, tangle, blockchain, IoT*

Resumen del trabajo:

Después del bitcoin se han creado muchas criptomonedas. Estas monedas virtuales han ido despertando el interés del público en general, con la posibilidad de llevar a cabo diferentes tipos de operaciones comerciales, compra/venta en el sector inmobiliario, servicios o incluso establecimientos que dejan pagar con criptomonedas.

El TFM pretende hacer un estudio general de criptomonedas y blockchain, profundizar en el estudio de IOTA para el Internet of Things, analizar su tecnología, características y vulnerabilidades.

La principal innovación de IOTA es el tangle, un nuevo libro contable distribuido, en lugar del blockchain que utilizan criptomonedas como bitcoin.

En este trabajo se realiza una comparación entre de ambas tecnologías, blochchain y el tangle, donde se observan muchas similitudes. En ambos casos son sistemas inmutables, con pruebas de trabajo PoW y utilizando una estructura de datos P2P. Por otro lado, la red tangle presenta ventajas como las transacciones con cero comisiones, es una red ligera y escalable. Estas son características importantes para IoT, ya que los dispositivos requieren un sistema de bajo consumo de recursos y la capacidad de emitir nano transacciones.

Tras el análisis de IOTA, se han estudiado los ataques basados en DAG, que pueden llegar a dividir la red tangle y validar transacciones de doble gasto, así como otras vulnerabilidades del sistema ya rectificadas.

Se han estudiado algunos casos de uso de la criptomoneda IOTA, como la implementación en el sector industrial, entidades gubernamentales o en el uso diario como extensión de navegadores web.

En resumen, dado que hay muchos proyectos en desarrollando, la red IOTA tiene que madurar y crecer en número de transacciones para poder evaluar su evolución y demostrar su correcto funcionamiento e implementación.

Abstract:

Many cryptocurrencies have been created after bitcoin. These virtual currencies have been awakening the interest of the general public, with the possibility of carrying out different types of commercial operations, buying / selling in the real estate sector, services or even at establishments that allow paying with cryptocurrencies.

The TFM intends to make a general study of cryptocurrencies and blockchain, to deepen the study of IOTA for the Internet of Things, analyze its technology, characteristics and vulnerabilities.

The main innovation of IOTA is the tangle, a new distributed accounting book, instead of the blockchain that uses cryptocurrencies like bitcoin.

In this piece of work, a comparison is made between both technologies, blockchain and tangle, where many similarities are observed. In both cases they are immutable systems, with PoW work tests and using a P2P data structure. The tangle network presents advantages such as transactions with zero commissions, and it is a light and scalable network. These are important features for IoT, since the devices require a low resource consumption system and the ability to issue nano transactions.

After the IOTA analysis, DAG-based attacks have also been studied, which can divide the tangle network and validate double-spending transactions, as well as other rectified system vulnerabilities.

Some cases of the use of the IOTA cryptocurrency have been studied, like the implementation in the private sector, government entities, in daily use as an extension of web browsers.

To summarize, as there are many projects being developed, the IOTA network has to still mature and grow in number of transactions in order to be able to evaluate its evolution and demonstrate its correct functioning and implementation

Índice

1.0 Introducción

1.1 Contexto y justificación del Trabajo

El concepto o idea de criptomoneda fue descrita por primera vez por Wei Dai, en 1998, donde propuso la idea de crear un nuevo tipo de dinero descentralizado. La primera criptomoneda que se creó fue el bitcoin en 2009 [1].

Después del bitcoin se han creado muchas criptomonedas. Estas monedas virtuales han ido despertando el interés del público en general, en especial cuando aumentó el valor de cotización del bitcoin en abril de 2013. En 2010 el precio del bitcoin no alcanzaba el dólar, pero en abril del 2012 un bitcoin tenía un valor aproximado de cinco dólares y transcurrido un año subió a un valor aproximado de 130 dólares [1].

Existe un número creciente de individuos que utilizan las criptomonedas para realizar operaciones comerciales. Esto incluye negocios como restaurantes, compra/venta en el sector inmobiliario, bufetes de abogados y servicios de Internet populares como Namecheap[1], Wordpress[2], Reddit[3] y Flattr[4]. Por otro lado, también existen empresas y entidades que se lanzan a crear sus propias criptomonedas.

La criptomoneda IOTA es presentada como la criptomoneda para el Internet of Things (IoT) de ahí sus siglas. IoT hace referencia a cualquier objeto conectado a la red. Objetos que generan gran cantidad de datos que existe la posibilidad de monetizar. La principal innovación de IOTA es el tangle, un nuevo libro contable distribuido (Distributed Ledger Technology, DLT en inglés), escalable, ligero y que permite realizar transferencias sin comisiones.

Un libro contable distribuido es donde se anotan todas las transacciones que suceden en la red. Esta tecnología debe aportar seguridad en cualquier tipo de transacción entre usuarios sin la necesidad de intermediarios. En el caso de IOTA, el libro contable distribuido que soporta esta tecnología es conocido como tangle (*enredo* en español) por la manera como se enlazan las transacciones.

IOTA según sus creadores también es conocida como la columna vertebral del IoT, ya que IOTA pretende dar una economía autónoma a las maquinas a través del tangle. Esta tecnología tal como hemos mencionado, permite liquidar transacciones con coste cero. Los dispositivos pueden intercambiar cantidades bajo demanda, así como almacenar información de forma segura, intercambiar datos de sensores y verificar los datos del tangle

[1] https:www.namecheap.com/
[2] https://wordpress.org/
[3] https://www.reddit.com/
[4] https://flattr.com/

[2]. Todas estas operaciones se realizan de forma autónoma, es decir que las transacciones de maquina a máquina se hacen sin intermediarios.

Imaginemos un frigorífico inteligente, donde el usuario configura qué productos deben estar siempre disponibles. Probablemente mediante sensores la nevera detectará que falta leche y automáticamente realizara un pedido al supermercado. Esta operación se realizará sin intermediarios.

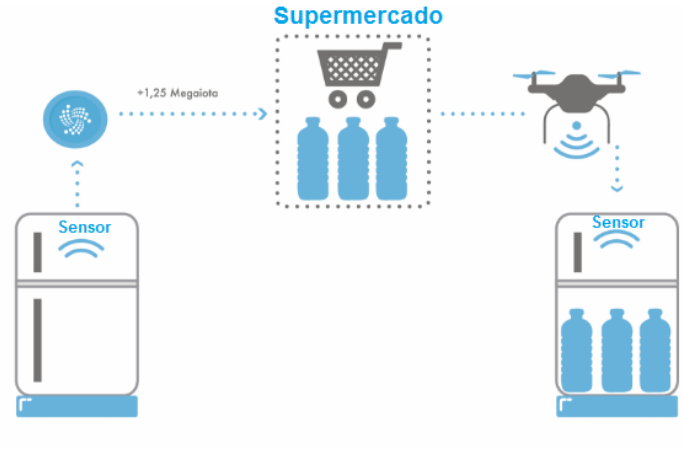

Fig. 1- Ejemplo gráfico transacción autónoma de un frigorífico.

IOTA ha reunido la participación de más de 20 organizaciones globales, así como Microsoft[5], Bosch[6], Fujitsu[7], o incluso grupos de investigación de universidades de todo el mundo [3]. Por otro lado, según las predicciones de IOTA durante la próxima década se esperan más de 75 millones de dispositivos conectados, interactuando entre sí, generando datos, dando lugar a la era de los datos, que podrán ser comercializados [4].

Por este motivo he considerado interesante estudiar la criptomoneda IOTA para el Internet of Things y ampliar los conocimientos relacionados con blockchain. Para ello, este trabajo pretende profundizar en IOTA, empezando por su origen, sus características, formación, como funciona, colaboradores, estudio a nivel de seguridad y posibles actividades actualmente.

1.2 Objetivos del Trabajo

Este trabajo final de Máster dispone de un objetivo general que consiste en el estudio de IOTA para el Internet of Things. Este tiene un carácter meramente teórico.

El proyecto se ha basado en los siguientes puntos:

1. Estudio general de criptomonedas y blockchain:

[5] https://www.microsoft.com/es-es
[6] http://es.bosch-automotive.com/es/internet/parts/startpage_1.html
[7] http://www.fujitsu.com/es/

- Estudio y documentación de la historia y fenómeno de las criptomonedas.
- Documentación de conceptos básicos relacionados con las criptomonedas.
- Estudio y documentación de la IoT.

2. Objetivo principal: estudio en profundidad de la criptomoneda IOTA, centrándonos en los siguientes puntos.
    - Estudio y documentación del origen e historia de IOTA, así como su vinculación con el IoT.
    - Estudio de las características y conceptos técnicos relacionados con IOTA (e.g. tangle, PoW, validación de transacciones, etc).
    - Empresas colaboradoras.
    - Estudio de implementaciones y casos de uso.
    - Estudio de la situación actual y expectativas de evolución.
3. Estudio a nivel de seguridad:
    - Estudio de la integridad, confidencialidad, problemas de seguridad y vulnerabilidades.
    - Estudio de limitaciones.

1.3 Enfoque y método seguido

Este TFM se va a centrar en el estudio, investigación y documentación de la criptomoneda IOTA, vinculada con IoT, la tecnología utilizada, así como su relación con blockchain y posibles aplicaciones en diferentes ámbitos. Al encontrarnos en un Máster de seguridad informática, se prestará especial atención en los aspectos relacionados con la seguridad, y vulnerabilidades publicadas.

En la primera fase, ante la falta de conocimiento, se hacen tareas de búsqueda y documentación sobre las criptomonedas. Una vez estudiada su historia se profundiza en conceptos básicos para comprender su funcionamiento.

En la segunda fase se procede al análisis de la criptomoneda IOTA. Desde su historia, características, funcionamiento, conceptos técnicos, soporte y vinculación con grandes multinacionales.

Una vez comprendida la parte más técnica de IOTA, se realiza un estudio y análisis a nivel de seguridad.

Finalmente, se han buscado casos prácticos del uso e implementación de la criptomoneda, así como el análisis del estado actual y expectativas de evolución.

Para llevar a cabo este proyecto se ha buscado obtener el conocimiento necesario, para realizar la investigación, así como documentar y adjuntar los conocimientos adquiridos, para que el lector, pueda adquirir los conocimientos necesarios.

1.4 Planificación del Trabajo

Para la planificación de este trabajo final de Máster, se ha elaborado un diagrama de Gantt, donde se divide temporalmente el proyecto en cuatro secciones.

Inicialmente la fase de planificación, la segunda y tercera fase son de investigación y búsqueda de información, en la cuarta fase se elabora la memoria y conclusiones, y finalmente se realiza la presentación.

Para elaborar el diagrama de Gantt, se han estudiado los principales puntos del proyecto y elaborado una tabla:

Actividades	Inicio	Duración	Fin
PAC1- Requisitos del trabajo	21-feb	20	12/03/2018
Contexto y justificación del Trabajo	21/02/2018	5	25/02/2018
Objetivos del Trabajo	26/02/2018	5	02/03/2018
Enfoque y método seguido	03/03/2018	5	07/03/2018
Planificación del Trabajo	08/03/2018	5	12/03/2018
PAC2 -	13/03/2018	28	09/04/2018
Estudio y documentación General Criptomonedas	13/03/2018	7	19/03/2018
Origen de las criptomonedas	13/03/2018	7	19/03/2018
blockchain	13/03/2018	7	19/03/2018
IoT	20/03/2018	3	22/03/2018
3.Introducción a IOTA	23/03/2018	7	29/03/2018
Orígenes	23/03/2018	7	29/03/2018
Fundación	23/03/2018	7	29/03/2018
Tecnología: características y descripción técnicas (TANGLE)	30/03/2018	11	09/04/2018
Cero comisiones	30/03/2018	11	09/04/2018
Empresas colaboradoras	30/03/2018	11	09/04/2018
PAC3 -	10/04/2018	28	07/05/2018
Seguridad de IOTA	10/04/2018	18	27/04/2018
Limitaciones	28/04/2018	5	02/05/2018
Implementaciones y Casos de uso	03/05/2018	5	07/05/2018
PAC4 Memoria final, conclusiones	05/05/2018	38	04/06/2018
Situación actual y evolución conclusiones	05/05/2018	5	10/05/2018
Redacción de la memoria	11/05/2018	20	31/05/2018
Conclusiones	01/06/2018	4	04/06/2018
PAC5 Presentación	05/06/2018	6	11/06/2018

Tabla. 1 - Diagrama de Gantt.

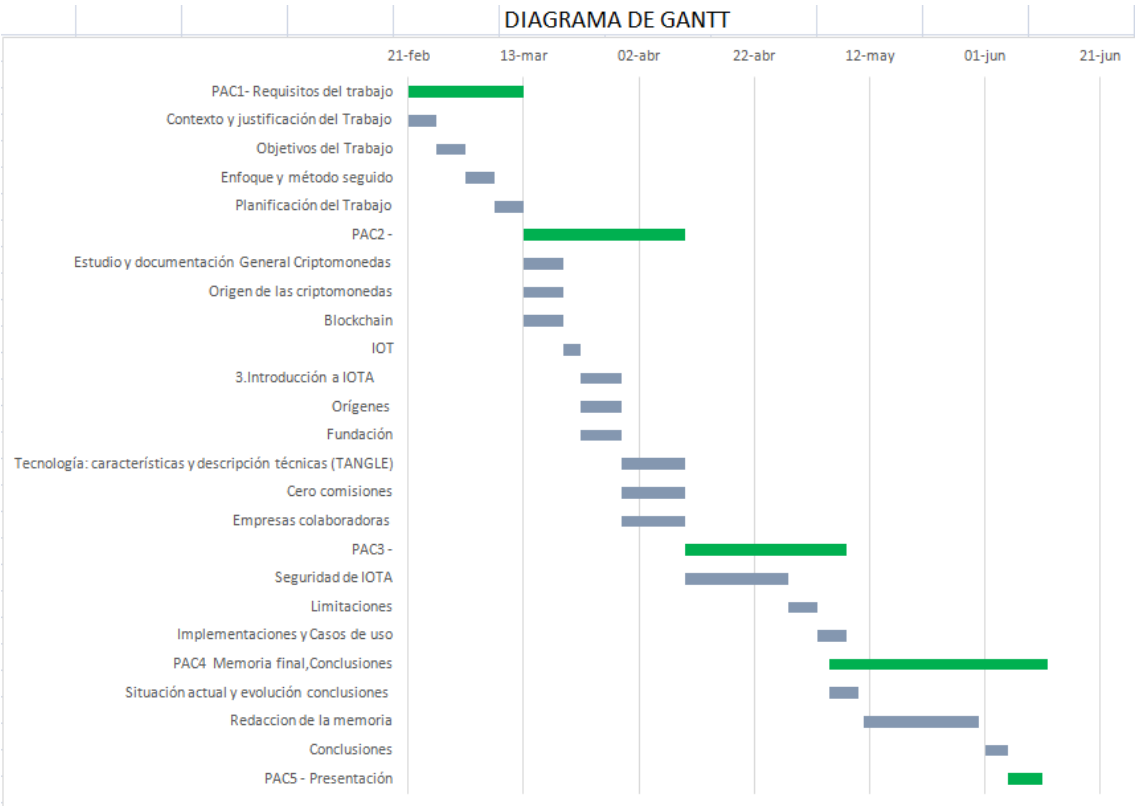

Fig. 2- Diagrama de Gantt.

1.5 Breve descripción de los otros capítulos de la memoria.

- Introducción: En la primera parte de la memoria, se describe el contexto y justificación del trabajo, así como sus objetivos, método de trabajo y toda la planificación.

- Criptomonedas: Resumen general del estudio de las criptomonedas, su historia, conceptos básicos importante, así como el análisis del blockchain y estudio de IoT.

- Introducción a IOTA: Documentación del estudio de IOTA, su historia, fundación IOTA, característica de funcionamiento como el tangle y conceptos más técnicos.

- Seguridad de IOTA: Resumen del estudio de las vulnerabilidades de IOTA, integridad, problemas de seguridad, así como posibles ataques detectados.

- Casos de uso: Resumen de casos prácticos, actualmente en fase de pruebas o proyectos en desarrollo.

- Conclusiones: Resumen de los conocimientos aprendidos, reflexión sobre los objetivos planteados y su desarrollo, así como el análisis crítico de la planificación del proyecto y las posibles líneas abiertas de investigación.

- Glosario: Listado de términos y acrónimos utilizados durante la memoria.

- Bibliografía: Listado de referencias bibliográficas utilizadas dentro de la memoria.

2.0 Criptomonedas

2.1 Origen de las Criptomonedas.

Las criptomonedas son sistemas de pago a través de la red, basadas en un sistema peer-to-peer, utilizando un elemento de seguridad basado en la criptografía. El valor se transfiere sin intermediarios y de manera electrónica.

El concepto de criptomoneda fue descrito en 1998 por Wei Dai, con la idea de la descentralización del dinero, utilizando como sistema de control la criptografía [1].

La primera criptomoneda fue el bitcoin, creada en 2009 por el desarrollador Satoshi Nakamoto [5]. Con un sistema descentralizado de igual a igual para verificar transacciones y permitiendo el intercambio de forma electrónica y anónima, sin depender de intermediarios.

Hasta el momento se han creado nuevas criptomonedas, con diferentes finalidades y aunque con atributos similares tienen características que las diferencia. Algunos ejemplos son: la criptomoneda Namecoin[8] creada para intentar descentralizar DNS, Litecoin[9] basada en Scrypts y muchas otras, pero no todas han sido exitosas, así que han ido también desapareciendo [6].

En sus últimos casi 10 años de existencia, las criptomonedas han ido ganando popularidad en el público en general y medios [7]. En el año 2013 bitcoin toma un valor de 200USD, y a finales del 2017 llega a un valor aproximado de 20.000USD [6].

Entre las características principales que hacen populares a las criptomonedas se pueden destacar: se garantiza la seguridad, integridad, tienen alcance global sin fronteras, dificultad de trazado y son descentralizadas.

2.2 Blockchain y conceptos clave

Blockchain significa “cadena de bloques”, nació formando parte de la creación del bitcoin, ya que es una estructura de datos que utiliza bitcoin y que sustenta toda su estructura. Su potencial más allá de las transacciones financieras permite una amplia diversidad de usos, entre ellos en la administración pública o el internet de las cosas, tal como veremos en los siguientes puntos.

La transferencia de datos digitales se realiza con una codificación compleja y de manera segura, descentralizada, distribuida en múltiples nodos independientes entre ellos que registran y validan la información. Una vez

[8] https://namecoin.org/
[9] https://litecoin.org/es/

introducida la información no podrá ser borrada, debido a su sistema de bloques, únicamente pueden añadirse nuevas operaciones [8].

Cuando se habla de criptografía, se conocen principalmente tres formas tradicionales, que se utilizan de manera combinada o individual, para la trasferencia de datos o comunicaciones P2P sólidas y seguras:

- Cifrado con criptografía simétrica: Para este tipo de cifrado solo se utiliza un clave para cifrar y descifrar, esta clave la tiene que conocer el emisor y el receptor. El principal problema de seguridad de este cifrado se encuentra en el intercambio de claves, ya que cuando se envía puede ser interceptada.

- Cifrado con criptografía asimétrica: Este sistema utiliza dos claves: la clave pública (que se difunde a cualquier persona) y la clave privada (que no se debe revelar nunca). Para enviar un mensaje el remitente utiliza la clave pública del destinatario, cifrar el mensaje, utilizando un algoritmo simétrico con esta clave pública. Una vez cifrado envía el mensaje y únicamente el destinatario utilizando su clave privada, puede descifrar el mensaje.

- Firma Digital basada en criptografía asimétrica: La firma digital permite al receptor verificar la autenticidad del origen de la información, así como su integridad, es decir, si el mensaje ha sido modificado desde su generación. Para ello el remitente cifra el resumen del mensaje con su clave privada obteniendo así su firma digital. Manda al receptor los datos originales junto la firma digital. El receptor descifra la firma digital con la clave pública del emisor y verifica que este mensaje coincide con el mensaje original.
  Resumen de mensaje (en ingles *digest*), con función hash sobre datos: Las funciones hash son operaciones matemáticas que realizan un resumen de un mensaje.

Con blockchain se ofrece una manera segura de mantener una estructura de datos distribuida, o lo que entendemos como un registro o libro de cuentas, de cierto tipo de información y que nunca pueda ser manipulada, es decir que los datos no se puedan modificar.

Como funciona blockchain:

La cadena de bloques, está formada por bloques, cada bloque contiene información codificada de transacciones en la red y dos apuntadores hash. Estos apuntadores indican cual es el bloque que le precede “prev hash” y por otro lado el hash del propio bloque “block hash” que será utilizado por el siguiente bloque para indicar el bloque que le precede, y así sucesivamente, quedando todos los bloques enlazados por los apuntadores hash.

Cuando se envía una transacción a la red, esta quedara registrada en el bloque de blockchain. Los mineros agrupan las transacciones en una estructura criptográfica de apuntadores hash llamada árbol Merkle, debido a su inventor

Ralph Merkle. Esta estructura agrupa los bloques de información en pares y genera un hash por cada bloque de datos. Los hashes generados vuelven a ser agrupados en pares y se genera un nuevo hash que a su vez se agrupa con otro y se repite hasta alcanzar el “root hash”, o raíz del árbol Merkle. El root hash permite recorrer cualquier punto del árbol para verificar si las transacciones están incluidas o incluso si los datos han sido manipulados. Por otro lado, tenernos e “Block hash”, que se registra como dirección del bloque actual, y permite enlazar los bloques del blockchain. Véase la siguiente imagen para comprender el contenido de un bloque de la cadena de bloques [9], [10].

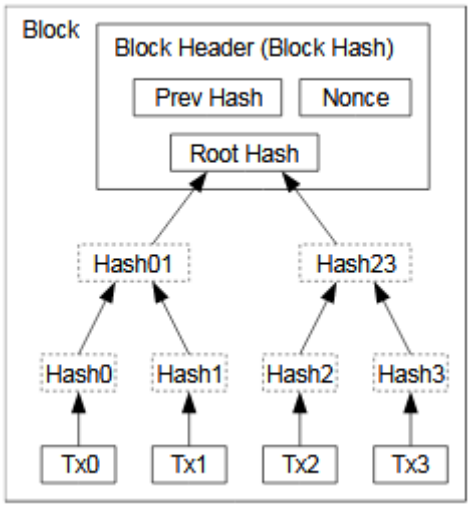

Fig. 3- Estructura del Merkle Tree [9].

Para decidir el curso de la cadena de los bloques se utiliza el algoritmo de consenso. En el caso de muchas criptomonedas como bitcoin, utiliza PoW, Proof of work. El concepto prueba de trabajo (PoW), consiste en implementar un trabajo computacionalmente costoso.

El elemento ‘nonce’ del diagrama anterior es un número aleatorio que encuentran los mineros a través de PoW, que se utiliza para construir el nuevo bloque.

Cuando se crea un bloque a través del sistema de PoW, el minero va probando diferentes nonce hasta que se encuentre el adecuado, es decir, que necesita un nonce que al hacer el hash del bloque encuentren un valor hash de todo el bloque menor a la dificultad de minado propuesta. Esta es una operación repetitiva, donde el minero va probando diferentes nonce hasta encontrar el adecuado. Para realizar estas operaciones, los mineros necesitan potentes maquinas, con capacidad de cómputo para repetir una y otra vez dicha operación de comprobación.

El minero que descubre el nonce adecuado, es decir que encuentra una solución, validada el bloque, lo sella y recibe una recompensa fija por bloque minado, y una comisión de las transacciones entre usuarios [11].

La recompensa de cantidad fija de bitcoin varía según la fecha en que se mine el bloque, ya que influye la cantidad de bloques que se hayan generado antes, a lo que se le denomina 'halving'.

Se le llama halving a la reducción de la recompensa a la mitad por la creación de un nuevo bloque. Esto lo realiza el protocolo de forma automática y es inevitable. En 2009, el protocolo otorgaba 50 BTC al minero que descubriera un nuevo bloque, así hasta 210.000 bloques, donde llegado el momento se reduciría la recompensa a la mitad (unos cuatro años aproximadamente), en noviembre de 2012, los 50 BTC de recompensa pasaron a 25 BTC**.** Este valor se mantuvo durante otros cuatro años, hasta julio de 2016, cuando volvió a reducirse a la mitad, 12,5 BTC que se ofrecen como recompensa en la actualidad [12].

Una vez validado el bloque, este queda registrado de forma permanente en esa cadena de bloques, sin poder ser modificado sin alterar antes todos los bloques que están relacionados con él. Si modificamos cualquier dato de un bloque, los bloques siguientes también quedarían invalidados, ya que a partir del bloque modificado los hashes dejan de coincidir. Por otro lado, hay que tener en cuenta que existe una réplica de la cadena de bloques en los otros nodos de la red. Por lo tanto, si modificamos algún bloque de la cadena, los otros nodos detectarían dicha modificación.

Tal como hemos mencionado los bloques enlazados cuentan con un puntero hash que enlaza al bloque anterior, además de la marca de tiempo y los datos de las transacciones, como información pública. La cadena de bloques no revela la identidad de los usuarios, pero permite controlar la trazabilidad de esas transacciones. Si hablamos de bitcoin, la trazabilidad permite saber el camino que ha seguido el bitcoin de una cartera con su dirección origen y al llegar a la cartera de otro con su dirección destino, únicamente mostrando sus direcciones origen y destino, nunca mostrando sus identidades.

Este complejo mecanismo de minería, recompensa y validación es el principio básico de la mayoría de las blockchains que aseguran pagos correctos y por otro lado mantienen la integridad de los datos, ya que una vez que el sistema lo aprueba, los valores o la información no se pueden alterar.

Si hablamos de bitcoin, en los blockchains se están utilizando comisiones (en inglés *fee*) de transacciones para evitar que se envíe spam a la red.

En la siguiente imagen podemos ver la relación de comisiones en los últimos meses. Si observamos este último mes de abril las transacciones de bitcoin tienen un promedio entre 0 y 1,5 dólar [13]. Estas comisiones son establecidas por el remitente en cada transacción. Los mineros tienen el incentivo de incluir las transacciones con comisiones más elevadas, ya que así aumenta su recompensa. Para priorizar las transferencias con comisiones más elevadas se genera una rivalidad entre usuarios.

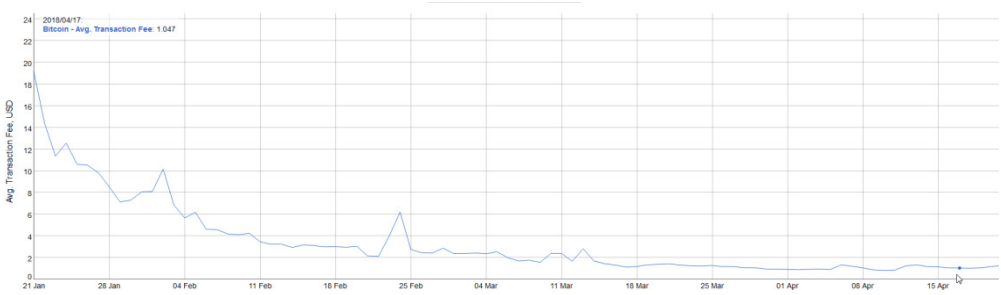

Fig. 4- Gráfica comisiones de bitcoin.

Más allá de la economía, sus características han hecho que diferentes sectores se interesen en la adaptación a sus necesidades. Desde validación de contratos, sistema de control en las cadenas de manipulación de alimentos de grandes superficies, empresas de seguros y contratos [14].

Existen muchos proyectos actualmente abiertos en diferentes áreas:

- **Registro de propiedades**: el gobierno de Suecia en colaboración con ChromaWay[10] han puesto a prueba una plataforma basada en contabilidad distribuida, con el objetivo de agilizar el proceso de bienes del país. Esta aplicación marca con una huella digital única en cada propiedad, solo se registra en papel en su primera venta. La cadena de bloques se encarga de resguardar, verificar y modificar los datos de cada compra. Este proceso es más rápido, menos costoso que el habitual, ya que elimina los intermediarios y gestiones a papel habituales. Este sistema permite consultar toda la historia de una propiedad por medio de una interfaz sencilla [15].

- **Almacenamiento en la nube**: normalmente los servicios de almacenamiento están centralizados en un proveedor específico, pero la empresa Storj[11] quiere descentralizar este servicio para mejorar la seguridad y reducir la dependencia de ese proveedor de almacenamiento [16].

  Storj es una plataforma de almacenamiento descentralizada y de código abierto, basada en la tecnología P2P y blockchain. Esta mantiene los datos distribuidos a través de una red descentralizada, los datos están divididos y encriptados para evitar el acceso. Las claves están en posesión de cada usuario, y no de una compañía central. A cambio de ofrecer espacio de almacenamiento para la red, los usuarios reciben pagos en su propia criptomoneda.

- **Música**: La distribución musical podría sufrir toda una revolución si se lograra implantar un sistema basado en la cadena de bloques para

[10] https://chromaway.com/
[11] https://storj.io/

gestionar su reproducción y distribución. Spotify[12] está apostando fuerte por su propia cadena de bloques ante problemas con los pagos de derechos de autor, “royalties” [17].

La startup Mediachain[13] ha creado una base de datos P2P que permite registrar, identificar y seguir la distribución online de los trabajos, como podría ser la música. La gestión de la música con la cadena de bloques actúa como certificado de la propiedad y permite conocer todas las transacciones a las que se ha sometido la canción.

Este proyecto no fue pensado únicamente en el ámbito musical, sino en cualquier trabajo u obra distribuida por internet.

Utilizando la tecnología de blockchain Spotify pretende conseguir atribuir a cada obra musical una gestión más detallada para atribuir a cada canción, su creador, propietario, y datos relevantes sobre derechos de autor para poder hacer los pagos de royalties correctamente.

- **Seguridad social y sanidad**: Se podría generalizar a todos los servicios públicos, pero en la sanidad pública o privada un sistema de cadena de bloques serviría para registrar todo tipo de historiales médicos, y mantener por completo la privacidad en el historial médico de cada persona, al mismo tiempo que facilitar el intercambio de documentos entre proveedores de salud o incluso las aseguradoras. Actualmente ya existen startups que están trabajando para sacar plataformas tecnológicas a nivel de blockchain sanitario: GemOs Health[14], HealthCombix[15], iSolve[16],etc [18].

Hay muchos proyectos que se encuentran en pleno desarrollo o fase de pruebas. Podemos ver que se están aplicando en diferentes ámbitos; a nivel público, en la industria, gestión documental, etc.

2.3 IoT

El IoT (en inglés, Internet of Things), se refiere a una red global de dispositivos, que interactúan con diferentes fines entre sí. El objetivo principal de IoT es hacer que los dispositivos se comuniquen entre sí y, en consecuencia, se conviertan en dispositivos mucho más inteligentes e independientes.

IoT es un concepto que fue introducido por Kevin Ashton en 1999, pero que en sí no era nada novedoso, ya que se refiere a la interconexión de dispositivos con una red global, la cual ya se utilizaba con anterioridad, sólo que para la interconexión se utilizaban circuitos cerrados de radio o de TV [19].

[12] https://www.spotify.com/
[13] http://www.mediachain.io/
[14] https://gem.co/
[15] https://healthcombix.com/
[16] http://www.isolve.com/

El Internet of Things permite que los ordenadores interactúen con elementos de la vida real como pueden ser un frigorífico, una estación meteorológica, y ganen independencia de los seres humanos. La capacidad de conectar dispositivos con capacidades limitadas de CPU, memoria y energía significa que IoT puede tener aplicaciones en casi cualquier área.

En el pasado CES 2015 se habló del IoT, en el que cada dispositivo es un aparato inteligente y todos se comunican a través de Internet. Como podrían ser un teléfono inteligente, macetas inteligentes, ventiladores, persianas, etc., Pero se ha avanzado tanto tecnológicamente, que ya no se cuestionan si es posible, sino, si se debería digitalizar todo. Dubravac en el certamen de CES 2015 hablo de su visión general del mundo, en la que hay comunicación entre productos y servicios, como una comunicación beneficiosa e omnipresente, poniendo como ejemplo el intercambio de información entre un cepillo de dientes y el dentista [20]. Esta información, pero, debe enviarse a la red utilizando algún método seguro y rentable, como nos puede ofrece IOTA.

Fig. 5- Ejemplo del Internet de las cosas.

Hewlett Packard[17] realizo un estudio en 2015, donde expuso que el 70% de dispositivos IoT tienen vulnerabilidades de seguridad en sus contraseñas, así como problemas de cifrado de los datos. Por otro lado, menciono que el 50% de aplicaciones móviles no encriptan las comunicaciones [21].

Karsperky lab[18] realizo unas pruebas en objetos conectados al IoT y consiguió acceder a cámaras de vigilancia de bebes, o incluso se obtuvo la clave de la Wifi de una cafetera [22].

Tal como se observa hay una tendencia de aumento de dispositivos IoT. Pero no todos están conectados de forma segura. Los datos que podemos encontrar en estos dispositivos, son de uso cotidiano, hábitos de usuarios, información de consumo o tendencias, información personal y valiosa para muchas empresas. La forma de disminuir su accesibilidad, proporcionar seguridad de gestión, es con una encriptación y cifrado de datos, como propone IOTA.

[17] https://www.hpe.com/
[18] https://www.kaspersky.es/

3.0 Introducción a IOTA

3.1 Orígenes de IOTA

David Sønstebø, Sergey Ivancheglo, Dominik Schiener, y el Dr. Serguei Popov fundaron IOTA en 2015. El proyecto está dirigido por David Sønstebø, experimentado en negocios y tecnología. Serguei Popov experto en matemáticas, que aporto los conocimientos necesarios para el desarrollo del tangle. Sergey Ivancheglo y Dominik Schiener que programaron posteriormente el tangle.

Todos los fundadores de IOTA (David Sønstebø, Sergey Ivancheglo, Serguei Popov, Dominik Schiener), son conocedores de la tecnología blockchain antes de empezar con el proyecto IOTA. Por ejemplo; Sønstebø formó parte de pruebas con Blockchain, Dominik Schiener empezó como minero y trabajando en empresas relacionadas con blockchain y el sector financiero [23].

Según una entrevista a Dominik Schiener, empezaron a explorar las blockchain para IoT por dos motivos, el potencial de las IoT y el desarrollo de un microprocesador de computación distribuida llamado “Jinn” [24].

El proyecto Jinn, trata del desarrollo de un microprocesador basado en la lógica ternaria. Este procesador estará diseñado para colocar en cualquier dispositivo IoT de baja potencia. Se desconocen muchas características, ya que actualmente sigue en desarrollo y no hay información pública.

Ante el conocimiento de las limitaciones de blockchain, desarrollaron un nuevo protocolo conocido como tangle basado en un gráfico acíclico dirigido (DAG) que se especializa en IoT, y que explicaremos en los siguientes puntos.

IOTA organizó un “crowdsale” en diciembre de 2015, momento en el que se realizó toda la emisión de moneda, distribuida entre todos los participantes de la crowdsale. El evento recaudó 1,337 bitcoin para el desarrollo del proyecto. Con el fin de incentivar a los cofundadores y el creciente equipo de desarrolladores. La comunidad IOTA se unió para donar una cantidad significativa de recursos para la fundación.

La fundación IOTA es una fundación sin ánimo de lucro, con sede en Alemania. Además de su financiación original, la fundación recibe apoyo de subvenciones gubernamentales y contribuciones corporativas, muy parecido a la fundación Linux[19].

En 2016 se anunció la fundación IOTA y, desde entonces, creció en número de colaboradores, proyectos y experiencia. Es en el verano del 2016 cuando IOTA entró en pruebas open-beta.

[19] https://getgnulinux.org/es/

La comunidad IOTA financió posteriormente "The Big Deal" a través de donaciones. Este acuerdo ayudaría a establecer numerosas colaboraciones corporativas en el ámbito del IoT.

La comunidad mostró su compromiso estableciendo el "Club de Inversores" con su enfoque en financiar más proyectos centrados en la comunidad y cultivando el ecosistema de manera sostenible.

El objetivo de IOTA es lanzar un mercado de datos donde las organizaciones puedan comercializar y monetizar datos. Según la firma, se generan más de 2,5 quintillones de bytes de información diariamente, y la cifra registra un crecimiento exponencial mensualmente. Aun así, casi el 99% se pierde porque no existe un modo seguro para intercambiar esta información [2].

David Sønstebø en sus declaraciones a Reuters[20] aseguró que *"Cualquier tipo de datos se puede monetizar. Si tiene una estación meteorológica que recolecta datos del viento, la temperatura, la humedad y la barometría, por ejemplo, puede venderla a una entidad que esté haciendo una investigación sobre el clima*" [25].

IOTA, establece su sede en Berlín, y ofrece una tecnología diseñada especialmente para el Internet de las Cosas (IoT), pero también aplicable a otras áreas, como, el intercambio de datos.

3.3 Fundación IOTA:

La fundación IOTA es una organización sin ánimo de lucro situada en Alemania que coordina y financia el desarrollo de la tecnología y del ecosistema de IOTA.

La fundación IOTA está formada por personas, con conocimiento, talento y con un historial reconocido, las cuales realizan trabajos para la fundación de manera organizada y pública.

Actualmente los miembros de la Fundación son el fundador de IOTA David Sønstebø, Dominik Schiener, Serguei Popov, Sergey Ivancheglo, Gianluigi Popov y Per Lind.

A pesar de que la fundación es el órgano central de IOTA, el esfuerzo tras el proyecto sigue estando centrado en la comunidad. Esto significa que cualquiera puede ayudar a promover IOTA y asegurar su éxito, formen parte de la fundación o no [2].

La comunidad dono el 5% de la oferta total de IOTA, para que la fundación realizara los trabajos de desarrollo [26].

[20] https://es.reuters.com/

Trabajos que hace la fundación:

- Asistir a conferencias relacionadas con el Internet de las cosas y la blockchain, así como participar activamente en hackathons.
- Entrega de recompensas por desarrollo en colaboración con grandes 'holders' de IOTA.
- Iniciar el desarrollo del cliente core en C y RUST.
- Ser capaces de fortalecer la marca y aumentar la concienciación de IOTA en todas las capacidades.
- Involucrar a empresas y organizaciones, especialmente aquellas enfocadas a Internet de las cosas y la blockchain.
- Ser la organización pública detrás de IOTA.

Según una publicación de principios de 2018, la fundación lanzará el ecosistema alrededor de IOTA para acelerar su desarrollo y adaptación como un proyecto de código abierto. Esta será una plataforma de la comunidad de desarrolladores, startups, o incluso aficionados de todo el mundo que trabajan para la descentralización, podrán aprender, colaborar, construir, desarrollar e incluso intercambiar ideas [27].

3.4 Empresas colaboradoras

El mercado de datos fue creado por la fundación IOTA en colaboración con más de 40 empresas como iniciativa de innovación. El objetivo es llegar a construir un mercado de datos sobre un libro distribuido, utilizando IOTA, teniendo en cuenta las limitaciones legales y técnicas. Ya que actualmente existe una legislación reguladora que limita el comercio de datos libremente.

IOTA anunció de manera oficial la colaboración con diferentes entidades, empresas o instituciones, que participan en una serie de ejercicios de innovación tecnológica con la red tangle de IOTA**.**

Participantes de todos los sectores e industrias están participando. Empresas como Microsoft, Fujitsu, Deutsche Telekom[21], Bosch, PwC[22], Schneider Electric[23], Accenture Orange[24] y muchos más han desplegado sensores que venden directamente los datos en el mercado. Las empresas que participan en el proyecto proporcionan datos de su industria. La finalidad es habilitar un mercado de datos muy diverso y abierto, que incentive el flujo libre de información entre estas entidades.

Además de Microsoft, IOTA lleva a cabo experimentos similares de “liderazgo intelectual” con varias otras compañías. “Ya hemos comenzado a realizar actividades con varias de las compañías enumeradas y pronto

[21] https://www.telekom.com/en
[22] https://www.pwc.es/
[23] https://www.schneider-electric.es/es/
[24] https://www.accenture.com/

publicaremos los primeros resultados", comentó Schiener, miembro de IOTA [6].

Si buscamos información, son muchas las entidades gubernamentales, multinacionales, universidades, asociaciones y entidades interesadas en IOTA. IOTA pública en su página oficial hechos relevantes, como nuevos colaboradores, proyectos o incluso personas que se unen para colaborar con la fundación [28]. Recientemente vemos publicada la noticia sobre su asociación con ITIC[25] para trabajar en bancos de pruebas de vehículos autónomos.

3.5 Tecnología: características y descripción técnicas.

IOTA se centra inicialmente en servir como la columna vertebral del Internet de las cosas (IoT).

Los fundadores de IOTA, con la experiencia adquirida a lo largo del tiempo e implicación en diferentes proyectos tecnológicos, así como el conocimiento en las primeras tecnologías de blockchain, les hizo pensar que debían empezar de cero para satisfacer las demandas del internet de las cosas. Así pues, nació el tangle.

Este innovador protocolo, el tangle, da lugar a nuevas características, únicas, como son: cero comisiones, escalabilidad, transacciones rápidas, transferencia segura de datos y muchas otras características que veremos a continuación.

El usuario y el validador (minero, staker, etc.) dejan de ser diferentes personas como en el caso de blockchain. Por otro lado, IOTA no requiere de equipos muy potentes para la realización de los cálculos, y por tanto disminuye el consumo de energía de la minería, o incluso el riesgo de la centralización en la validación.

Para realizar una transacción de IOTA, es necesario que el dispositivo que envía la nueva transacción confirme otras dos transacciones de la red. Para la confirmación de estas, el dispositivo realiza una PoW de baja dificultad. Estos problemas matemáticos podrían ser realizados por casi cualquier dispositivo moderno, tanto portátiles como teléfonos.

La PoW en IOTA no debe compararse con la utilizada en cadenas de bloques tradicionales. Es directamente comparable a Hashcash, con una dificultad muy baja y que tiene dos propósitos: prevenir el spam y los Sybil-attacks (ocurre cuando un sistema distribuido es corrompido por una misma entidad que controla distintas identidades de dicha red). La PoW en IOTA puede incluso ser exteriorizada de pequeños dispositivos ligeros a dispositivos con más capacidad de carga computacional [2]. Analizaremos la prueba de trabajo en la sección 3.5.5.

[25] http://www.itic-sc.com/

3.5.1 Características:

3.5.1.1 Cero comisiones:

Fig. 6- Representación de una transacción con cero comisiones.

Con IOTA se consigue un consenso sobre la validez de las transacciones sin la participación de ningún minero, y por tanto no hay honorarios de transacción a pagar**.**

IOTA permite realizar cualquier transacción, de valor incluso muy pequeño, sin ningún tipo de comisiones de transacción para el remitente o el destinatario.

Las blockchains más comunes no pueden evitar cobrar un mínimo de comisión, ya que, por su diseño, es necesario compensar los trabajos de minería, y por lo tanto de consenso y protección de la red.

IOTA, al no tener operaciones mineras, ni bloques, ni tarifas de transacción, la seguridad y el consenso de la red no se distribuyen entre mineros. Tal como hemos mencionado, validadores y usuarios, son el mismo usuario que realiza la transacción [2].

3.5.1.2 Infinitamente escalable:

Para enviar una transacción es necesario que el usuario valide dos transacciones en el tangle. Por tanto, cuantos más usuarios, más número de transacciones y más validaciones.

IOTA fue diseñado para permitir la liquidación transaccional a escala. El consenso es paralelo a el hecho de enviar una transacción, y no se hace en intervalos (por bloques) secuenciales de lotes como en blockchain.

Tal como se puede deducir, cuanta más gente utiliza IOTA, más transacciones referenciadas y directamente confirmadas. Las tasas de confirmación mejoran, así como los tiempos de confirmación, a diferencia de blockchain. Véase la sección 3.5.2.1 para comprender como se realiza una transacción y como son referenciadas las transacciones.

El tangle está asegurado por el poder de hash actual de la red, ya que este poder de hash es el que añade peso acumulado al tangle legítimo. Los nodos de IOTA sólo hacen PoW cuando emiten transacciones, y por tanto la seguridad de tangle depende de la frecuencia de transacciones y la cantidad de PoW por transacción. Como la red de IOTA es todavía pequeña, y el número de transacciones es bajo, el equipo de IOTA ha establecido un nodo de confianza al que llama 'Coordinador' o 'Coo'.

El coordinador es el responsable de decidir el estado de tangle, y proteger la red frente ataques del 34%. Este tipo de ataque lo explica IOTA en su “White paper” [29] y lo explicaremos en el siguiente bloque del proyecto. Pero para comprender rápidamente este tipo de ataque, si se realiza una transacción con un peso acumulado lo suficientemente alto podría convencer al algoritmo MCMC para seguir una ruta no deseada del tangle. Véase el apartado 3.5.2.1 para comprender el peso y algoritmo MCMC.

El coordinador actúa como vigilante para el crecimiento correcto del tangle y hace un control contra ciertos ataques, para verificar que no se están incumpliendo las reglas de consenso al crear nuevas transacciones. Según IOTA este permanecerá encendido hasta que la actividad en el tangle sea suficiente para que pueda evolucionar sin ayuda, en cuyo punto el “coordinador” permanecerá apagado.

IOTA no está limitada a nivel computacional, ya que no existe la minería. Pero no hay constancia que el tangle funcione de manera segura sin el “coordinador”. De hecho, explicaremos como un ataque DDoS satura la red, y deja de funcionar correctamente, en el siguiente bloque.

Así pues, actualmente no podemos hablar de escalabilidad en una red pequeña de IOTA. Por otro lado, queda por demostrar si IOTA es infinitamente escalable cuando la actividad en el tangle sea lo suficiente grande como para prescindir del coordinador.

Tal como hemos mencionado anteriormente, una de las características principales de las criptomonedas, es la descentralización. Actualmente con el coordinador funcionando no podemos hablar de una distribución descentralizada de IOTA.

3.5.1.3 Transacciones rápidas:

Tal como hemos visto en la escalabilidad, cuantas más transacciones, más rápidamente se confirmará cada transacción. A medida que IOTA se aproxime a un uso masivo, los tiempos de transacción se reducirán, y es posible que se aproximen al tiempo de propagación de la red. Así pues, los tiempos de transacción son inversamente proporcionales al número de transacciones en el tangle [2].

Uno de los aspectos más destacados de IOTA es la velocidad de transacción. La encriptación en IOTA es a través de código ternario, mucho

más eficiente que el código binario (se explica más detalladamente en la sección 3.4.2), pero sin embargo esto podría dar complicaciones de cómputo o sobrecarga de los dispositivos existentes, actualmente todos los sistemas y computadoras están desarrolladas en sistemas binarios, lo que obliga a los sistemas y equipos a realizar una contante conversión de datos a código binarios para ser procesados [30].

Si la red tangle es lo suficientemente grande, ayudará a aumentar la velocidad de propagación, pero actualmente la utilización del código ternario se muestra como un obstáculo. Se entiende que por ello IOTA tiene un proyecto de investigación para desarrollar un procesador ternario, que mencionaremos en la siguiente sección, pero aún tiene que demostrar su eficacia y correcta funcionalidad en la práctica.

3.5.1.4 Oferta monetaria fija:

Todas los IOTA que existen fueron creados en el llamado bloque génesis. La oferta monetaria total es de 2.779.530.283.277.761 de monedas en circulación, 132 veces superior al número máximo al que podrá llegar bitcoin, 21.000.000. Nunca aumentará o disminuirá ya que no se puede minar. Su cantidad está optimizada para la computación ternaria $((3^{33-1}) / 2) = 2.779 \times 10^{15}$ [2].

3.5.1.5 Prueba cuántica:

IOTA utiliza firmas basadas en hash en lugar de criptografía de curva elíptica (ECC). Las firmas basadas en hash son mucho más rápidas que ECC y simplifican el proceso de firma y verificación, reducen la complejidad general del protocolo tangle [31].

La criptografía de Curva Elíptica (ECC) es un tipo de criptografía de clave pública que requiere claves más pequeñas, y al mismo tiempo ofrece un nivel de seguridad equivalente [32]. Este tipo de criptografía ha sido apenas usada hasta ahora, pero el hecho de que requiere claves más pequeñas que otros sistemas de clave pública lo hace un buen candidato para aplicaciones donde los requisitos de tamaño de memoria son más exigentes. Bitcoin utiliza ECC para manejar con facilidad las claves públicas para la criptografía.

Las firmas basadas en hash son mucho más rápidas que las firmas de criptografía de curva elíptica. Es por eso que en lo referente a velocidad el tangle es muy rápido.

Inicialmente IOTA utilizo la función hash Curl diseñada especialmente para IoT, pero al detectar que las firmas podían falsificarse fácilmente, los desarrolladores cambiaron rápidamente la funciona hash por Kerl (versión ternaria de Keccak).

IOTA utiliza el esquema de firma única de Winternitz (W-OTS) ligeramente modificado para ternario y basadas en hash. Este tipo de firma permite usar la clave privada una única vez. W-OTS utiliza una función unidireccional *f* :

$$f :\{0,1\}^n \rightarrow f :\{0,1\}^n$$

Y una función hash *g :*

$$g :\{0,1\}^* \rightarrow \{0,1\}^n$$

Selecciona un parámetro de Winternitz W ≥ 2, que es la cantidad de bits que se deben firmar simultáneamente.

Cuando los usuarios crean un monedero de IOTA, deben ingresar una clave privada de 81 caracteres de extensión. Debido a sus características IOTA recomienda generar las claves privadas, a las que llama semillas, dentro de la propia GUI de IOTA[26] o ejecutando un código en Linux[27] u OSX[28].

El índice, es un número entero que especifica que clave derivar de la semilla, donde subsemilla = hash (semilla +índice). Al generar una clave publica, tiene la opción de elegir entre tres modelos de seguridad (81-trit, 162-trit y 243-trit), que afectan a la longitud de los paquetes de transacción. La clave pública se calcula aplicando *f* a cada cadena de bits en $2^W - 1$ tiempos de clave privada, así pues, se deriva de la semilla y el nivel de seguridad [33].

Los usuarios deben tener en cuenta que no deben reutilizar las claves privadas que se han utilizado ya que al realizar una operación se revela parte de la clave privada. La seguridad de los fondos disminuye rápidamente si vuelven a firmar nuevas transacciones con la misma clave, ya que podría ser utilizada por otro usuario.

Las firmas basadas en hash no sólo son mucho más rápidas que ECC, también simplifican en gran medida el proceso de firma, verificación y reducen la complejidad general del protocolo Tangle [2].

3.5.2 Tangle:

La principal innovación detrás de IOTA es el tangle. Se trata de una novedosa arquitectura distribuida, basada en un DAG (Directed Acyclic Graph).

DAG, es un sistema de almacenamiento que se caracteriza porque los enlaces entre los elementos siempre van en una dirección y acíclico porque no se pueden crear bucles dentro de la estructura.

[26] https://iotasupport.com/gui-download.shtml
[27] https://getgnulinux.org/es/
[28] https://support.apple.com/es-lamr/macos

El tangle se programa en ternario, desviación del código binario, que utiliza tres dígitos -1,0 y 1, por lo tanto, 3 estados en total. En la actualidad todos los sistemas y equipos computacionales están desarrollados en sistemas binarios. Pero hay que mencionar que el tangle puede trabajar bajo los dos sistemas de códigos, tanto binario como ternario.

Los beneficios de ternario van más allá del rendimiento computacional en comparación al binario. Otras áreas en la que brilla el ternario, son las redes neuronales artificiales y la lógica de la inteligencia artificial. Tal como hemos mencionado el ternario es de base 3, más cercana al número "e", base de los logaritmos naturales, que tiene un valor aproximado de 2,71. A diferencia del código binario en base 2 [34].

Si ponemos un ejemplo sencillo, con 18trits, se podrían representar cualquier cosa entre -387.420.489 y 387.420.489, para poder representar este intervalo en binario, serían necesarios 29bits.

Podemos ver a continuación un ejemplo de ternario en Java, donde se puede apreciar que el código es mucho más corto, y por tanto e reducen considerablemente las líneas de programa.

En este ejemplo se utilizará la condición "If" para verificar si un número es mayor a 50:

```
public static void main(String[] args) {
    int numero = 5;
    if(numero > 50){
        System.out.println("Es mayor a 50.");
    }else{
        System.out.println("Es menor o igual a 50.");
    }
}
```

Ahora con ternario:

```
public static void main(String[] args) {
    int numero = 5;
    System.out.println(numero > 50 ? " Es mayor a 50."
            : " Es menor o igual a 50.");

}
```

Con ternario se simplifican los tipos de datos, reduce las instrucciones condicionales o incluso operaciones básicas por el hecho de eliminar el signo.

Es necesario mencionar que, en la década de los años 50, en Rusia se construyeron algunas computadoras experimentales utilizando ternario, llamados Setun[29] [35] [36].

[29] https://en.wikipedia.org/wiki/Setun

El código ternario se puede considerar más eficiente en cuanto al consumo de energía que el código binario, pero para ello es necesario un cambio de computadoras. IOTA está diseñada para IoT, motivo por el cual es muy importante equilibrar el uso eficiente de la energía y, al mismo tiempo, tener capacidad de cómputo para asegurar el sistema.

Tal como hemos mencionado existe el proyecto Jinn, y tratan de desarrollar un procesador de lógica ternaria optimizado, de bajo coste, pocas dimensiones y eficientes en el consumo de energía a la hora de realizar cálculos. Pero actualmente tal como hemos mencionado IOTA permite el uso de ambos sistemas, ternario y binario.

Tangle en su núcleo, sigue teniendo los mismos principios que blockchain: una base de datos distribuida, una red P2P con mecanismo de consenso y validación. Pero, como principal diferencia la estructura de IOTA es tangle que se basa tal como hemos mencionado en un gráfico acíclico dirigido (DAG) y la forma de lograr el consenso no depende de los mineros.

En IOTA no hay “bloques” en el sentido clásico. En su lugar, una sola transacción que hace referencia a dos transacciones pasadas. Esta referencia de transacciones se considera como una certificación: con su transacción se validan directamente dos transacciones anteriores, e indirectamente también se validan unas subsecciones del tangle [37].

La red está formada por nodos que emiten transacciones. Toda la red de participantes es directamente responsable del consenso general, es decir que está involucrado en la aprobación de transacciones. Así IOTA consigue que el consenso no esté desacoplado del proceso de transacción, es una parte de él, y es lo que permite a IOTA escalar sin tarifas de transacción.

3.5.3 Proceso de una transacción de IOTA:

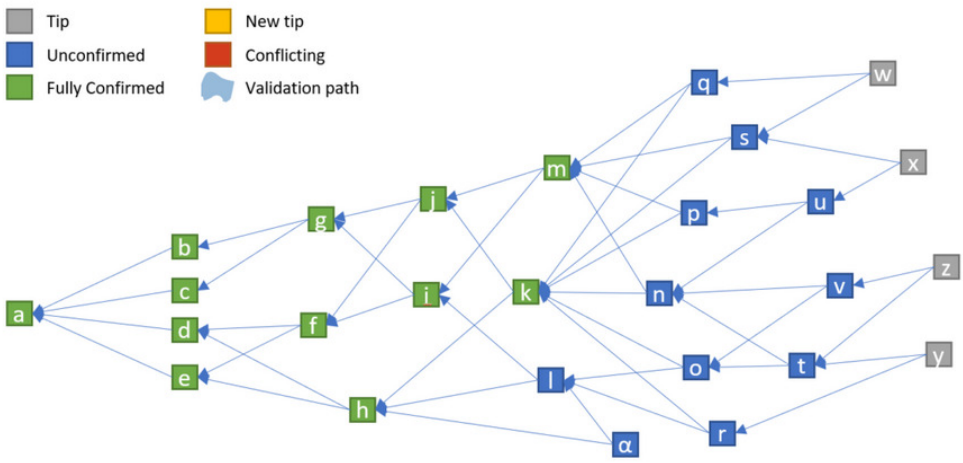

Fig. 7- Representación gráfica de tangle [38].

En este ejemplo gráfico de tangle, sé representa la red de transacciones donde podemos diferenciar:

- Bloques verdes: transacciones que ya están confirmadas por la red con gran nivel de seguridad.
- Bloques azules: transacciones en las que todavía no estamos seguros de su plena aceptación.
- Bloques grises: consejos, tips, transacciones no confirmadas.

El objetivo de cualquier transacción es que sea verde, es decir, confirmada y aceptada por toda la red.

IOTA no crea una secuencia sincronizada de bloques con varias transacciones como en el blockchain.

En la imagen anterior, cada bloque representa una transacción y las flechas que salen de cada transacción apuntando hacia otras dos representan la aprobación de las dos transacciones previas. La transacción génesis se encontraría fuera del diagrama por su lado izquierdo, y las transacciones más nuevas, llamadas “puntas” (tips) en el “White paper”, se encuentra a la derecha, coloreadas de color gris.

Cuando miramos la imagen, la diferencia principal de los bloques verde y azul, es que los bloques verdes son indirectamente referenciados por todos los bloques grises. Esto significa que, para cada transacción confirmada, hay una ruta directa que conduce a ella desde una punta [38].

3.5.3.1 Agregar una transacción al tangle:

Cuando un nodo quiere agregar una transacción al tangle “1”, el nodo realiza los siguientes pasos:

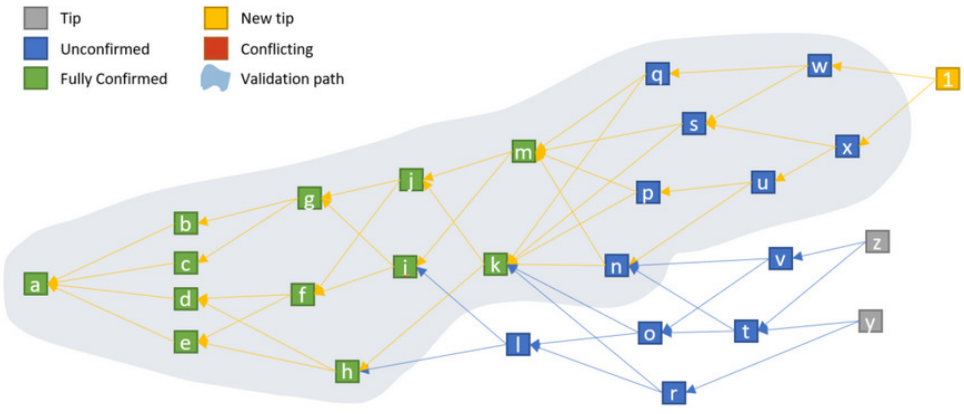

Fig. 8- Representación gráfica de tangle, se añade una transacción [38].

1. El nodo firma las entradas de la transacción con sus llaves privadas. Un nodo debe elegir cuál de sus direcciones usar para la transferencia y finalmente construir el paquete.

2. El nodo elige dos transacciones para aprobar, según el algoritmo MCMC (cadena de Markov Monte Carlo). Este selecciona al azar dos consejos (es decir, las transacciones no confirmadas), que serán referenciadas (branchTransaction y trunkTransaction). La primera opción natural para escoger una transacción sería escoger las tips donde se alcanza el máximo de peso acumulado (véase sección 3.5.4 para entender el concepto peso acumulado). Pero hay nodos egoístas que actúan así muchas transacciones nuevas aprobarán las mismas dos tips al mismo tiempo, por lo que habrá demasiada competencia entre ellos para su aprobación posterior. Por lo tanto, incluso un nodo egoísta tendría que usar algún algoritmo de aprobación aleatoria de la tip.

MCMC es un algoritmo que tiene que ser ejecutado cada vez antes de que enviara la transacción.

El algoritmo se describe de la siguiente manera:

Sea Hx el peso acumulado, considere todas las transacciones con un peso acumulado entre W y 2W (donde W es razonablemente grande, a elegir). Para ello el nodo selección un número “n”, por ejemplo 10 de profundidad en la tangle, y se realizaran caminatas aleatorias independientes y discretas "hacia las tips" (es decir, la transición de x a y es posible si y aprueba x). Las dos caminatas aleatorias que lleguen primero a la tip fijada indicarán nuestros dos tips a aprobar. Las probabilidades de transición de los paseos se definen de la siguiente manera: si y aprueba x (nosotros denotamos este y --> x), entonces la probabilidad de transición Pxy es proporcional a exp − α(Hx − Hy), es decir:

$$P_{XY} = exp\left(-\propto (H_X - H_Y)\right)\left(\sum_{Z:Z\to X} exp\left(-\propto (H_X - H_Y)\right)\right)^{-1}$$

donde $\propto > 0$ es un parámetro a elegir (puede iniciarse p. ej. con α = 1).

Estos consejos se seleccionan de manera no determinista. La idea es que como menor sea la diferencia del peso acumulado entre las transacciones que puede elegir, menor será la diferencia del peso acumulado final de esta transacción [29].

3. El nodo verifica si estas dos transacciones no están en conflicto y no aprueba las transacciones conflictivas. Verifica la firma de esa

transacción, la PoW y asegura que no estén en conflicto con ninguna transacción anterior.

4. Para que un nodo emita una transacción válida, el nodo debe resolver un rompecabezas criptográfico mucho más fácil a los de la cadena de bloques de bitcoin. Esto se logra encontrando un nonce, que es un hash de 81-tryte, tal que el hash de ese nonce concatenado con algunos datos de la transacción aprobada tiene una forma particular. Cada transacción debe tener un nonce para que sea aceptada por la red.

El nonce es seleccionado por una función de prueba de trabajo para satisfacer un hash de transacción final que termina en el número de ceros dictados por el usuario. Profundizaremos en la sección 3.5.5 sobre la prueba de trabajo.

5. El usuario finalmente agrega su nueva transacción haciendo referencia a las dos transacciones elegidas.

Una vez realizados estos puntos, la transacción será transmitida a la red. Otros usuarios realizarán transacciones, elegirán nuestra transacción en el proceso de selección y la validarán. De esta forma se consigue una validación colaborativa global de la tangle.

Al mismo tiempo, antes o después otros usuarios pueden agregar transacciones en posiciones diferentes, y no crear ningún conflicto.

Cuando hablamos de validar, o aprobar una transacción, el nodo que hace la validación debe partir de las dos transacciones que está validando y seguir todas las rutas en orden inverso hasta la transacción del génesis, asegurándose de que nunca encuentra una contradicción (por ejemplo, un doble gasto, saldo insuficiente o cosas parecidas). Si hay una contradicción, escogerá otro par de transacciones para aprobar.

Como podemos ver en la siguiente imagen, al agregar una nueva transacción ”2” esta valida gran parte de las transacciones que ya fueron validadas por la transacción “1”, además de otras que no estaban en la ruta de la validación de la transacción “1”. Si se superponen las dos rutas de validaciones, podemos ver como algunas transacciones únicamente se han validado una vez y otras se han validado en estas dos transacciones.

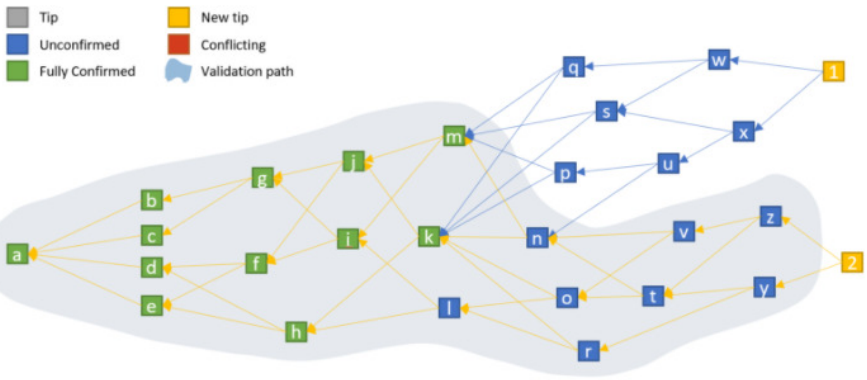

Fig. 9- Representación gráfica de tangle, se añade una segunda transacción [38].

Si observamos la siguiente imagen, “n” se ha vuelto verde, confirmada y validada por todos los tips. Las próximas transacciones vinculadas a “1” y “2”, continuaran confirmando la transacción “n”.

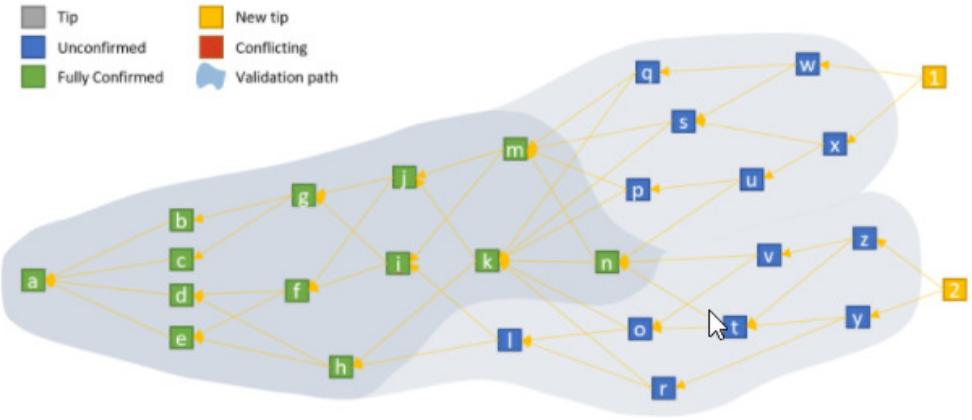

Fig. 10- Representación gráfica de tangle, confirmación y validación [38].

Así pues, transcurrido un tiempo, cuando una transacción se ha adentrado en el tangle, existe una ruta directa o indirecta desde cualquiera de las últimas tips hasta ella, y como en el caso de la transacción “n”, se considera confirmada, se volverá a referenciar y validar por cada transacción.

Cabe destacar que el tangle puede contener transacciones conflictivas. Los nodos no tienen que llegar a un consenso sobre qué transacciones válidas que tienen derecho a estar en el tangle, lo que significa que todas pueden estar enredadas. Sin embargo, en el caso de que haya transacciones conflictivas, los nodos deben decidir qué transacciones quedarán huérfanas. Para ello utilizan el llamado algoritmo Markov-Chain Monte Carlo (MCMC). Veremos a continuación que es el peso de una transacción [38].

3.5.4 Peso de una transacción

El nivel de confianza de una transacción se decide mediante el algoritmo de selección de propinas, que seleccionan las transacciones para la confirmación de acuerdo con su peso acumulado. Como más alto es el peso acumulado más probable que la punta sea elegida.

Para determinar cuando el nivel de confianza es seguro, hablamos del intervalo de confianza, este intervalo calcula el nivel de aceptación de una transacción por el resto de la red de la siguiente forma:

- Se ejecuta el algoritmo de selección de tips 100 veces (MCMC), y se verifica cuántos de esos 100 consejos de ruta a seguir en el tangle aprueban la transacción.

- El número que obtenemos, es el intervalo de confianza, y se expresa en tanto por ciento, para tener el intervalo de confianza.

El peso de una transacción es proporcional a la cantidad de trabajo que el nodo emisor invirtió en él. El peso se adjunta a una transacción a través de un número entero positivo, número que se puede leer al leer la información de la transacción y el paquete en el que se encuentra.

El peso acumulativo, es el propio peso de la transacción más la suma de los pesos propios de todas las transacciones que aprueban nuestra transacción directa o indirectamente [39].

En la siguiente imagen podemos observar cómo funciona el algoritmo.

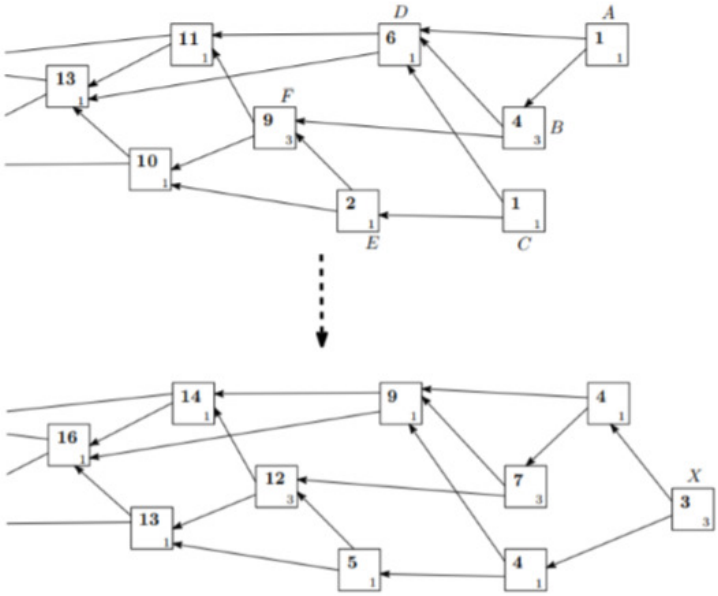

Fig. 11- Representación gráfica del algoritmo de trabajo de tangle [29].

Cada transacción o tip está representada con un recuadro, donde podemos observar dos números, el peso de la propia transacción en la esquina inferior derecha. El número más grande del recuadro representan los pesos acumulados.

Por ejemplo, la transacción F es directamente o indirectamente aprobado por las transacciones A, B, C, E. El peso acumulado de F es 9 = 3 + 1 + 3 + 1 + 1, que es la suma del propio peso de F y los propios pesos de A, B, C, E.

Cuando llega una nueva transacción, por ejemplo “x”, con un peso “3”, el peso acumulado de todas las tips del tangle aumenta en 3.

En general, la idea es que una transacción con un peso mayor es más "importante" que una transacción con un peso menor.

3.5.5 Proof of Work (PoW)

Antes de emitir una transacción, un nodo debe realizar una prueba de trabajo (PoW). Esto significa que una función hash se debe calcular una y otra vez, mientras que cada vez se incrementa un nonce hasta que se cumpla un determinado criterio, tal como Hashcash introdujo el concepto.

Hashcash, es una prueba de trabajo que se propuso originalmente como mecanismo para combatir el correo spam o para evitar la denegación de servicio en varios sistemas, en mayo de 1997. El beneficio original de usar Hashcash es la protección de denegación de servicio (DDoS) [40].

El beneficio original de usar Hashcash es la protección de denegación de servicio. En el tangle, si no había trabajo necesario para emitir transacciones, un atacante podría dividir fuertemente la red mediante él envió de transacciones conflictivas o spam. Para una atacante es mucho más fácil enviar una gran cantidad de transacciones sin realizar ninguna PoW, y los nodos deberían transmitir todas estas transacciones, esto se asemejaría a un ataque DDoS contra toda la red.

Pero si el nodo es capaz de darse cuenta de que el atacante no ha realizado un trabajo necesario, se abstiene de transmitir las transacciones. Esto significa que además de evitar la denegación de servició, Hashcash provoca el mecanismo de PoW que hace posible la integridad y defiende al tangle de los ataques, como el doble gasto, que se estudian en la sección 4.

Blockchain funciona de manera diferente. El propósito de PoW en el Blockchain es mantener constante el número de bloques por segundo. Esta se logra bajando el número de hashes aceptables. En el tangle, sin embargo, se supone que debe asegurarse de que la red no se sature de transacciones que no se puedan gestionar, y evitar así la denegación de servicio.

El PoW de IOTA no es mejor o peor que el PoW de bitcoin, es diferente su propósito. Para Bitcoin, es una forma de definir la verdad, es decir que, si

resuelves un bloque más rápido que nadie, este bloque será la verdad una vez validado. En IOTA encontrar un nonce adecuado permite adjuntar una transacción al tangle, no permite decidir cuál es la verdad, ya que para establecerse el camino correcto del tangle y no validar transacciones incorrectas, al enviar nuevas transacciones y utilizar el algoritmo MCMC para la selección de tips, no validaría transacciones que colisionan, como es el caso del doble gasto.

Es evidente que la dificultad de PoW de bitcoin es mucho mayor que la dificultad de IOTA, suponiendo un gasto mucho más energético elevado, respecto al relativamente económico de IOTA.

En conclusión, PoW en el tangle es solo un mecanismo de protección que casi no tienen impacto en el consenso, como es el caso de bitcoin, así pues, para IOTA el PoW tiene tres propósitos:

- Protección DDoS.
- Protección contra el doble gasto.

3.5.6 Transacciones Offline:

La red IOTA es asincrónica. En general, los nodos no necesariamente ven el mismo conjunto de transacciones. Tangle permite la ramificación fluida y volver a la red, así pues, IOTA hace posible que unos conjuntos de dispositivos se ramifiquen y continúen realizando transacciones en un entorno fuera de línea, es decir sin conexión.

Un ejemplo claro, es dentro de una intranet de una compañía, o en una interrupción de internet.

Poder realizar transacciones sin conexión es una característica importante en el mundo de IoT donde se espera una comunicación asíncrona.

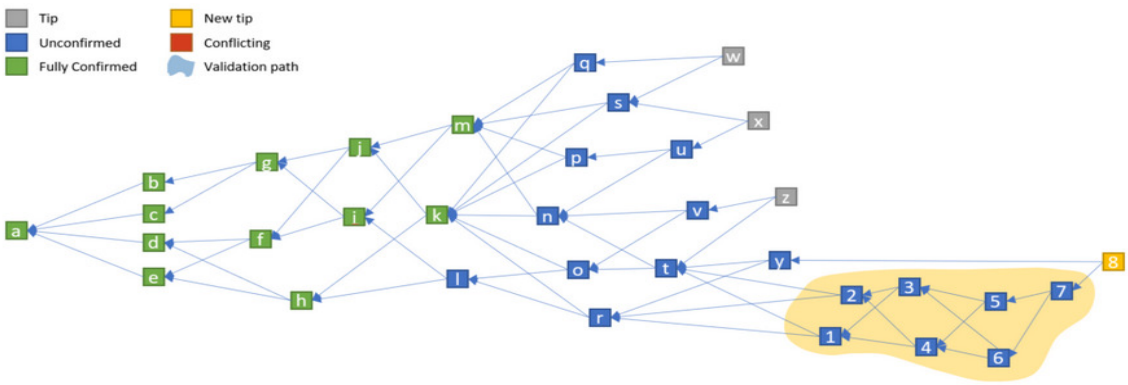

Fig. 12- Representación gráfica de tangle, con transacciones fuera de línea [38].

Si analizamos el ejemplo de la figura 10, las transacciones “1” y “2” son las primeras que se realizan fuera de línea, pero conectadas a las dos últimas dentro del tangle online “t y r”. La red tangle fuera de línea puede seguir creciendo, las siguientes transacciones fuera de línea, se envían apuntando a dos transacciones anteriores fuera de línea, y una vez se quiere sincronizar con el tangle principal, la última transacción fuera de línea “8” fusiona la offline tangle con una transacción de la tangle online. Para que el tangle fuera de línea y la tangle principal se puedan fusionar, no deben entrar en conflicto, es decir que las transacciones existentes no pueden estar en conflicto. Las próximas transacciones que se conecten con la transacción número ocho incluirán todas las transacciones fuera de línea en su ruta de validación.

Si hablamos de un entorno fuera de línea, como podría ser un hogar, un entorno empresarial (intranet), un vehículo sin conexión a internet, etc. Con IOTA los datos y transacciones son seguras incluso en un entorno fuera de línea, ya que al intentar fusionar el tangle fuera de línea con al tangle principal si existe una transacción en conflicto, la fusión no sería posible. El tangle fuera de línea no podría volver a validar transacciones del tangle principal, y este tangle fuera de línea no tendría un índice alto de validación, y por tanto finalmente quedaría abandonado [38].

3.6 Tangle vs blockchain:

IOTA al utilizar el protocolo tangle es bastante diferente de las “cadenas de bloques”, protocolo blockchain.

Tal como hemos visto IOTA utiliza tangle que se basa en un gráfico acíclico dirigido (DAG). Las transacciones se procesan en paralelo con la validación, dando lugar a un alto rendimiento. El tangle va creciendo con el aumento de transacciones y IOTA se vuelve cada vez más rápido y seguro validando transacciones.

A diferencia de blockchain, tangle tiene escalabilidad y las transacciones no tienen coste. En blockchain existe la figura del minero y el usuario que realiza la transacción, donde la validación de dicha transacción se consigue en la cadena de bloques. Los mineros compiten entre sí en un intento de agregar el siguiente bloque y ganar así su recompensa. En IOTA todos los participantes de la red aprueban dos transacciones al generar su transacción, permitiendo así el coste cero, y eliminando la figura del minero.

Desde otro punto de vista, si no existe un incentivo económico para los nodos, como en blockchain, porque hay que utilizar IOTA. Si no hay incentivos, actualmente es difícil que el tangle de IOTA crezca, ya que a pesar de permitir micropagos, IOTA está diseñado para IoT y actualmente la mayoría son proyectos en desarrollo, pero no implementados definitivamente.

Para que una transacción se confirme en la cadena de bloques, transcurre el tiempo necesario para la creación del siguiente bloque. Tiempo que ha aumentado con el tiempo debido a la dificultad de la creación de nuevos

bloques. Tangle no tiene restricciones temporales, incluso permite los pagos asíncronos, por lo que no hay limitaciones temporales en la finalización de la transacción.

Si hablamos de la integridad de las transacciones, en ambos casos no pueden alterarse una vez publicadas en la red. Con blockchain, una validado el bloque, no puede ser alterado, ya que cada nodo contiene una copia de la cadena de bloques y por otro lado tal como hemos mencionado anteriormente el bloque contiene el hash del bloque anterior, así pues, si se modifica un bloque, todos los hashes subsiguientes se alterarían también. De lo contrario, un nodo instantáneamente podría ver que el hash es incorrecto. Del mismo modo que en el tangle, los hashes almacenados en la transacción de aprobación se vería alterados.

Tal como hemos comentado, cabe destacar que incluso fuera de línea es posible crear transacciones en IOTA, con blockchain al necesitar los mineros para la validación y creación de bloques, las transacciones no pueden tener lugar fuera de la cadena ya que es necesario garantizar que no se pueden gastar dos veces el mismo dinero.

El tangle se programa en ternario que es una desviación del código binario tradicional. El Ternario es mucho más eficiente que el binario y proporciona algunas mejoras significativas en la funcionalidad. Cabe destacar que se puede ejecutar tanto en sistemas binarios como ternarios.

En cuanto a la descentralización, con blockchain si podemos hablar de un sistema descentralizado como en el caso de bitcoin. El tangle de IOTA depende del coordinador, motivo por el cual, mientras la red no sea lo suficientemente grande y deje de funcionar el coordinador, no podemos hablar de una red tangle descentralizada, característica muy importante para las criptomonedas. Hablamos del coordinador en la sección 4.6.

4. Seguridad de IOTA

Como muchas tecnologías nuevas, IOTA tiene sus propias vulnerabilidades de seguridad. Al ser una criptomoneda que no se basa en el protocolo blockchain, tiene su conjunto de problemas de seguridad, muchos de ellos relacionados con el protocolo de verificación basado en DAG y otros exclusivos en la implementación por parte de IOTA.

Los principales ataques en un sistema basado en tangle son, sin duda, aquellos basados en la selección de peso y en cómo se aprueban nuevas transacciones si hay un conflicto. Por otro lado, existen las vulnerabilidades críticas en la función hash de IOTA. También hay otros posibles ataques que han tenido lugar y que veremos en los siguientes puntos.

El "White paper" [29] explica ataques basados en DAG, explicaremos a continuación posibles ataques, todos ellos dirigidos a realizar un doble gasto. Veamos un ejemplo de doble gasto para poder comprender mejor los posibles ataques.

4.1 Doble gasto:

Como se ha mencionado anteriormente cuando se realiza una transacción, cada transacción contiene información del formato "el origen transfiere a destino 10iotas". El aprobador es el que tiene que asegurarse de que emisor tiene realmente esas 10iotas, y por tanto que la transacción que quiere aprobar es válida.

Un doble gasto, en ingles *doble spending*[30], es un intento de transferir el mismo saldo dos veces, es decir, que se le prometió al receptor original, pero que también se enviará a un segundo receptor. El emisor intenta gastar el mismo dinero más de una vez, dando lugar al que llamamos doble gasto.

Si un remitente con un importe determinado, intenta realizar dos transacciones de dicho importe, una de las dos transacciones no será validada ya que si así fuera el saldo del remite tendría que ser negativo.

El intento de doble gasto ira obteniendo sus primeras confirmaciones, pero tarde o temprano sucederá que ambas transacciones en conflicto estén en la ruta de validación de una transacción. Esta transacción que intenta validar ambas transacciones anteriores, detectara el conflicto, y volvería a seleccionar los consejos del algoritmo MCMC hasta que encuentre que no están en conflicto para asegurarse de que su transacción se convierta en una transacción válida. Los usuarios que a continuación realizan transacciones pueden tener solo una de estas transacciones conflictivas en su ruta de validación [38].

[30] https://es.wikipedia.org/wiki/Doble_gasto

Esto da lugar a dos rutas en el tangle, donde ambas no pueden ser aprobadas. Una de las dos ramas del tangle crecerá y será más pesada que la otra, y la más ligera será abandonada. Todas las transacciones subsiguientes asociadas a la rama del tangle abandonada (ya que no pudieron ver el conflicto) también serán abandonadas.

Desde la perspectiva de los receptores ambos ven la transacción, pero solo uno de ellos recibe la cantidad transferida.

Esto implica que una transacción, aunque tenga algunos aprobadores, podría formar parte de una rama del tangle que será abandonada. Para asegurarse de que su transacción está confirmada, el destinatario tiene que esperar a que la confianza de confirmación sea lo suficientemente alta, tal como está explicado en el apartado 3.5.4.

Veamos un ejemplo:

En la siguiente imagen Alice tiene 5i, he intenta gastar su dinero más de una vez. La casilla representa una transacción donde se anota el saldo en la cuenta de Alice, Charlie y Bob, antes y después de que la transacción se llevara a cabo. Dicho saldo se expresa junto al número como “i”, de IOTAs. Antes de realizar las transacciones Alice tiene 5i, transfiere esta cantidad a Bob, y este pasa a tener 5i y Alice se queda con 0i. A su vez Alice realiza la misma transacción a Charlie.

Estas dos transacciones no se podrán tratar como transacciones válidas, y por tanto no se podrá tener una transacción futura aprobando ambas transacciones realizadas por Alice, ya que tendríamos un saldo negativo en la cuenta de Alice.

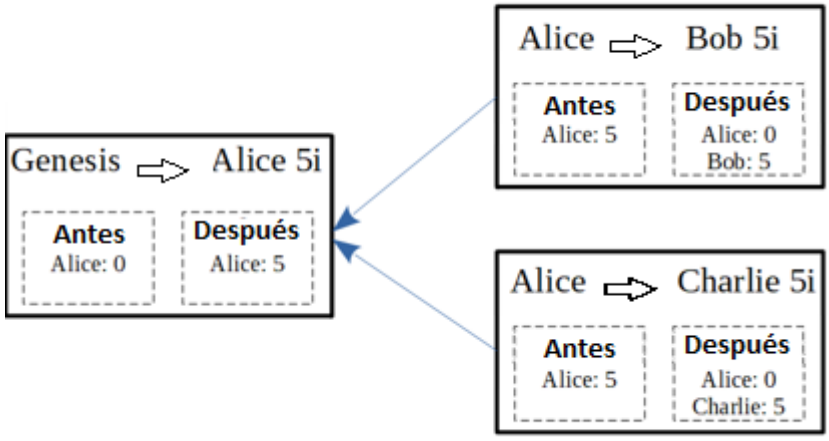

Fig. 13- Representación gráfica transacción de doble gasto.

Tal como hemos visto anteriormente, el algoritmo MCMC decide la ruta a seguir en el tangle. En este caso una de las dos rutas del tangle que han generado las dos transacciones se hará mucho más grande tomando más peso, y la otra ruta tendrá un peso más ligero. El peso acumulado de esta transacción decidirá cual se quedará en el tangle como válida. Si uno de las

dos rutas se estanca, finalmente, la transacción quedará huérfana y será abandonada, es decir dejara de crecer, sin formar un consenso de validación sobre dicha transacción.

En el caso de Charliei y Bob ambos ven la transacción, pero uno de ellos no recibe la cantidad transferida. Una transacción no puede considerarse confirmada inmediatamente después de su emisión, aunque tenga algunas aprobaciones, ya que podría formar parte de una rama del tangle que será abandonada. Por este motivo, para asegurar una transacción, es necesario esperar a que la transacción esté confirmada por un número alto de confirmaciones de la transacción, es decir, que el nivel de confianza sea lo suficientemente alto, tal como hemos explicado en el apartado 3.5.3.

Una vez que la transacción alcanza un umbral de confianza alto, es muy poco probable que se determine que no es una transacción válida y no tenga derecho a estar en el tangle.

Hasta aquí, podemos suponer que el doble gasto se ha realizado de forma involuntaria, pero si se realiza de manera intencionada se podría considerar un ataque como podremos ver en los siguientes puntos [39].

4.2 Ataque de peso grande simple / 34%:

El ataque de peso grande simple es conocido en inglés como *Simple Large Weight Attack / 34%-Attack.*

Si el remitente dispone de suficiente poder computacional, puede tratar de emitir muchas transacciones para aumentar el peso acumulado de la ruta del tangle con la operación de doble gasto, y llegando a abandonar la ruta legitima del tangle.

Si recordamos el ejemplo anterior Alice al tratar de hacer dos transacciones, da lugar a una bifurcación en el tangle, por un lado, el tangle principal con la transacción original y por otro lado la rama del tangle donde se encuentra la transacción de doble gasto y que por tanto crea una ruta alternativa al tangle principal que llamaremos sub-tangle.

Una vez aceptada la transferencia original, el atacante, si dispone de suficiente poder computacional, emitirá tantas transacciones como pueda, tratando de aumentar el peso acumulado del sub-tangle que contiene en la ruta la operación de doble gasto.

Si en algún momento la sub-tangle del atacante supera el peso acumulado del tangle principal, entonces el ataque de doble gasto será exitoso. Si eso no sucede, entonces la transacción de doble gasto no será aprobada por otros (ya que el tangle principal con la transacción original adquirirá más peso acumulativo y esencialmente todas las nuevas tips lo aprobarían indirectamente), por lo que quedará huérfana.

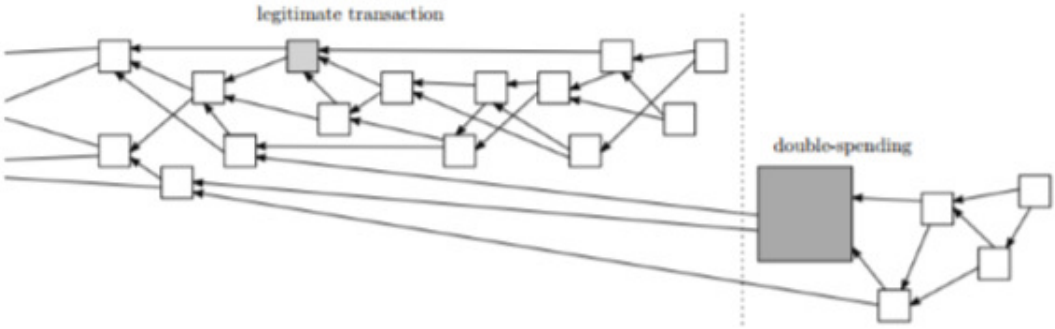

Fig. 14- Representación gráfica Simple Large Weight Attack [29].

Básicamente este ataque se reduce a tener más de un tercio, el 34%, de la potencia total de hashing, para que las nuevas tips con el algoritmo MCMC tiendan a validar el sub-tangle y no el tangle principal.

De esta forma podría conseguir que toda la red de IOTA crea en dicha transacción de doble gasto, y continúe la ruta por la nueva sub-tangle con la operación de doble gasto, una ruta no deseada [41].

En la siguiente figura, podemos ver un ejemplo real. Alicia dispone de un importe 5 en su cartera. Alicia envía una transacción por la compra de un ordenador de importe 5 a Bob. Por otro lado, envía una transacción de doble gasto por la compra de un aspirador de importe 5 a Charlie, creando una nueva rama del tangle principal, es decir, sub-tangle que contiene la transacción de doble gasto. Al aceptar la transacción del tangle principal, Bob envía el portátil. Alicia recibe el artículo, y emitirá tantas transacciones como pueda al sub-tangle, tratando de aumentar el peso acumulado.

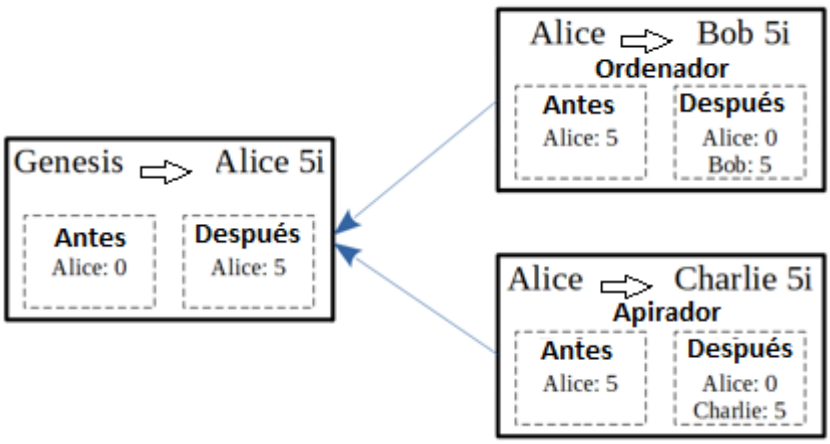

Fig. 15- Representación gráfica doble gasto.

Si Alicia consigue en algún momento que la sub-tangle con la transacción de doble gasto supere el peso acumulado del tangle principal, entonces el ataque de doble gasto será exitoso. En este caso el tangle principal

seria abandonado. La transacción de importe 5 por la compra del aspirador será validada. Charlie enviará el producto y recibirá el dinero de la transacción, pero Bob sin embargo no recibirá el dinero y ya habría enviado el ordenador [39], [29].

4.3 Cadena parasito:

La cadena de parasito, conocida en inglés como *parasite chain,* esta también mencionada en el White paper de IOTA. *Es m*uy similar al ataque anterior, en este caso, para poder realizar un doble gasto se crear una rama en el tangle paralela al tangle principal, que llamaremos también sub-tangle. Como en el caso anterior el atacante emite una transacción al tangle principal, la cual es validada. Posteriormente la intención es enviar una transacción de doble gasto en la sub-tangle. En este tipo de ataque la sub-tangle se convertirá de manera eventual en el tangle principal, dejando abandonada la transacción legítima del que era anteriormente el tangle principal.

Esta rama que llamamos sub-tagle tendrá más peso acumulado que el tangle principal. La diferencia en este ataque, es que el sub-tangle se basa en el tangle principal, haciendo referencia ocasionalmente a él. Esto permite alcanzar un peso acumulado mayor, es decir que las tips toman la suma de su peso propio y el peso de todas las transacciones validadas directa o indirectamente, siendo el peso acumulado superior.

Como en el caso anterior Alicia realizara un doble gasto en el sub-tangle. Pero en este caso a diferencia del anterior, Alicia volverá a emitirá transacciones al sub-tangle tratando de aumentar el peso acumulado, pero estas transacciones aleatoriamente harán referencia al tangle principal, es decir que enviara una transacción que validara una transacción del sub-tangle y la otra del tangle principal.

Si hablamos de una tip honesta, su peso acumulado, es el trabajo de toda la tangle principal, y en una tip de la sub-tangle paralela se podría sumar el trabajo del tangle principal y el realizado por toda la sub-tangle.

El atacante, Alicia puede añadir transacciones a esta sub-tangle ganando peso. Si gana suficiente peso, las nuevas transacciones al utilizar el algoritmo MCMC podrían escoger las tips de la sub-tangle y validar así las transacciones del sub-tangle, el cual tiene una transacción de doble gasto, y el ataque de Alicia tendría éxito, ya que la red se dividirá en dos, y ambas ramas crecerían.

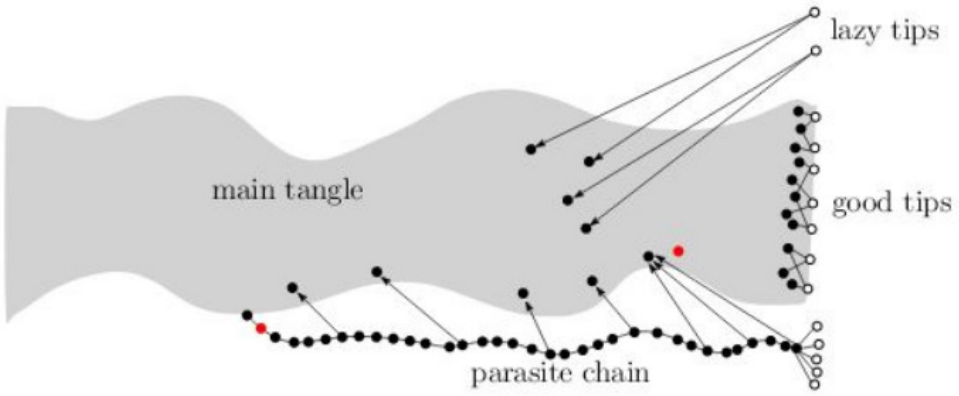

Fig. 16- Representación gráfica parasite chain [29].

En la imagen anterior, podemos visualizar como la sub-tangle, llamada cadena parasito, en ingles *parasite chain,* está haciendo ocasionalmente referencia al tangle principal.

Las tips que validan transacciones más nuevas tendrán un peso acumulado mayor, debido a la existencia de todas estas transacciones intermedias que suman peso. Es por este motivo que será más probable que estas tips se seleccionen en futuras validaciones de nuevas transacciones [29].

Este ataque de doble gasto basado en una cadena parasito es difícil que tenga éxito, cuando se utiliza la selección de tips con el algoritmo MCMC, teniendo en cuenta que la tangle principal tiene más poder de dispersión que el atacante, y en consecuencia más peso acumulado. Así pues, las nuevas transacciones que utilizan el algoritmo MCMC tendrán la tendencia a escoger tips del tangle principal. Si los usuarios no utilizan el algoritmo MCMC y la sub-tangle.

4.4 Ataque de división

Spliting attack en Ingles, es un ataque mucho más complicado y que combina los anteriormente descritos.

En este caso, como en los casos anteriores se genera una sub-tangle, pero el atacante no necesita estar realizando continuamente transacciones. El objetivo es equilibrar la sub-tangle con la tangle principal en cuanto a peso acumulado y de esta forma la mitad de la red cree en la sub-tangle y la otra mitad en el tangle principal, y así consigue dividir la red. Su intención no es superar el peso acumulado como en los dos ataques descritos anteriormente.

El atacante podría realizar una transferencia en la tangle principal y un doble gasto en la sub-tangle. Luego agrega transacciones según sea necesario para garantizar que tengan el mismo peso la tangle principal y la sub-tangle para mantenerlo dividido. Con ello espera que se realicen validaciones en ambas ramas. En este caso es mucho más complicado que los

anteriores, ya que el atacante tiene que estar pendiente y buscar el equilibrio entre ambas para conseguir así el doble gasto.

Como es de esperar, este es un ataque mucho más complicado que los anteriores, ya que el atacante tiene que estar constantemente buscando este equilibrio, para que ninguna de las dos divisiones se abandone.

Con este tipo de ataques, el atacante puede realizar un doble gasto esperando que ambos destinatarios de las transacciones den por validad la transacción y en este caso el atacante realizar un doble gasto.

Con un objetivo más complejo, podría existir la intención negar el servició al resto de la red. El atacante enviara un número “X” de transacciones conflictivas, dividiendo el tangle en “X” sub-tangles, cada una de las cuales empezaría acumular transacciones de otros usuarios. Con el tiempo el algoritmo de selección MCMC favorecería alguna de estas sub-tangles, transacciones en los otros sub-tangles quedarían huérfanas y tendrán que ser reenviadas, mientras el atacante enviara otro conjunto de transacciones conflictivas a esta sub-tangle dominante, repitiendo el proceso de dividir el tangle todo el tiempo que quiera. Como resultado gran parte de las transacciones nunca se confirmarán mientras dure el ataque, ya que los sub-tangles irán quedando huérfanos, y en ellos existirán transacciones conflictivas de doble gasto.

En blockchain también sucede algo parecido cuando dos mineros envían bloques aproximadamente al mismo tiempo. La diferencia, es que para un minero es muy difícil dividir la cadena de bloques repetidamente, ya que eso requeriría una gran potencia PoW. Con el tangle, en cambio, un atacante simplemente necesita la suficiente fuerza de ataque como para enviar un conjunto de transacciones simultáneamente [42], [29].

4.5 Problemas de la función hash Curl

La regla de oro de los sistemas criptográficos es " no desarrolle su propia criptografía" [43]. Se recomienda el uso de criptografías primitivas, bien comprendidas y probadas para construir un sistema. Las funciones de hash criptográficas, pasan por años de pruebas y pruebas antes de que se consideren lo suficientemente robustas como para usarlas en software crítico.

Una función de cifrado hash toma una cantidad arbitraria de entrada y produce resultados impredecibles con un tamaño fijo. La idea es que, dada una salida, es muy difícil encontrar una entrada que se corresponda con esa salida, y dada una entrada y salida, es muy difícil encontrar otra entrada que se corresponda con la misma salida. Cuando dos entradas se asignan a la misma salida, eso se llama “*colisión* “. Si en un sistema se encuentran colisiones fácilmente, significa que la función hash criptográfica está rota.

Las funciones de hash criptográficas son importantes para las criptomonedas por qué. Si se puede romper una función hash, también puede potencialmente romper las firmas de las transacciones, lo que significa que el

mecanismo utilizado para determinar si una transacción es un gasto válido y autorizado se ha roto. La integridad matemática que garantizan las criptomonedas depende de que esta relación sea segura.

IOTA desarrollo su propia función hash llama Curl, pero a mediados del 2017 un grupo de expertos (Ethan Heilman, Tadge Dryja, Madars Virza…) descubrió que la función hash Curl es vulnerable a una técnica bien conocida para romper funciones hash llamada "criptoanálisis diferencial" [44] que se utilizó para generar colisiones prácticas en esta nueva función hash desarrollada para IOTA.

Se utilizó una técnica para producir dos pagos en IOTA diferentes, pero con el mismo valor de hash, y por lo tanto la misma firma. Usando estas técnicas, un atacante podría falsificar firmas en los pagos de IOTA, y por tanto podría gastar los fondos de los usuarios, o posiblemente, los fondos de usuarios robados.

Una vez se descubrió la vulnerabilidad, se informó a los desarrolladores IOTA, estos decidieron cambiar la función hash Curl por la funciona hash Kerl (versión ternaria de Keccak) basada en SHA3 [45].

4.6 El coordinador

En una red madura, donde existe una cantidad considerable de transacciones pasando por el sistema, el doble gasto no es un riesgo, pero actualmente en la red IOTA no son suficientes las transacciones para que el sistema sea suficientemente robusto.

Para evitar el doble gasto IOTA establece un mecanismo voluntario y temporal, controlando así la red y evitar problemas de seguridad detectados: el coordinador.

Tal como hemos mencionado anteriormente el coordinador es un nodo de confianza que es el responsable de decidir el estado del tangle, y proteger la red frente ataques. Cada dos minutos la Fundación IOTA emite una transacción llamada "milestone" o "hito", y todas las transacciones aprobadas por ella se consideran con una confianza 100%.

Utilizando este mecanismo las transacciones de doble gasto nunca serían aprobadas en primer lugar.

Cuando la red tangle sea lo suficientemente grande, con un alto número de transacciones, la fundación cerrara el coordinador y dejara que la red tangle evolucione por sí sola.

Es necesario mencionar, que con el coordinador el tangle depende de la fundación IOTA, con sus transacciones esencialmente "garantizadas", y no actúa de manera descentralizada, sino que centraliza la confianza de la red tangle en el coordinador.

El coordinador es de código cerrado, y no se ha podido investigar en cuanto a código. Las transacciones emitidas por el coordinador se consideran garantizadas, pero existe el riesgo que un atacante se apodera del coordinador. Sin garantizar así las transacciones del coordinador, proporcionando un único vector de ataque muy grande para IOTA. Al ser el coordinador de código cerrado, no se puede verificar su veracidad, no se puede verificar si realmente si IOTA está controlando el coordinador, o es un atacante el que tiene el control.

Si un atacante se apodera de sus claves privadas puede emitir la transacción llamada “milestone” y hacerse con el poder de toda la red.

Actualmente el coordinador podría evitar algunos problemas causados por transacciones que colisionan como el doble gasto, pero sin él, un atacante podría haber dividido el tangle de IOTA en dos partes irreconciliables [46].

4.6 Otros ataques a IOTA

4.6.1 Phising

El termino phising es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. El estafador, conocido como phisher, utiliza técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza para que el ataque tenga éxito.

El pasado mes de enero un ciberdelincuente se apodero de casi 4 millones de dólares en IOTA [47].

Cuando los usuarios crean un monedero de IOTA, deben ingresar una clave de 81 caracteres de extensión. Hay varias formas de generar esta cadena aleatoria, pero una forma rápida para el usuario es utilizando un generador en línea, el cual no está recomendado por IOTA [23].

El atacante registró un dominio llamado iotaseed.io a mediados del año 2017, este dominio se publica como generador de claves privadas en línea de IOTA. Los usuarios se conectaban para obtener claves privadas para el monedero de IOTA, y el atacante las fue recolectando. Para ofrecer confianza, vinculo su página web a un repositorio de confianza, alegando que el sitio web ejecutaba el mismo código, cuando en realidad estaba modificado.

Transcurridos 6 meses, en enero de 2018, ejecuto el ataque, utilizo todas las claves privadas que había recolectado en su portal web enviando todo el dinero de estas cuentas a su propio monedero, con un daño estimado de casi 4 millones de dólares [48].

IOTA recomienda generar las claves privadas, a las que llama semillas, dentro de la propia GUI de IOTA[31] o ejecutando un código en Linux[32] u OSX[33]. Recuerda a los usuarios que guarden en un lugar seguro esta clave privada, ya que es posible perder los IOTA's. La clave privada es necesaria para recuperar el monedero en caso de pérdida [23].

4.6.2 Ataque DDoS satura la red tangle de IOTA

Ataque DDoS, en seguridad informática se conoce como un ataque de denegación de servicio, en ingles *Denial of Service.* Es decir que es un ataque a un sistema de red o equipos que causa que un servició o recurso sea inaccesible. Normalmente provoca perdida de conectividad a la red.

Tal como hemos mencionado anteriormente IOTA fue diseñada para ser infinitamente escalable. Pero en octubre de 2017 un ataque masivo DDoS genero una sobrecarga en el tangle de transacciones spam, y esta sobrecarga no se pudo gestionar por los nodos, hasta el punto que el tiempo de procesamiento de las transacciones tenía retraso y termino bloqueando la red tangle [49]. En IOTA, se conoce como spam el realizar transacciones sin valor, para evitar la inundación de spam por parte de un atacante, tal como hemos mencionado en la sección 3.5.5, PoW en el tangle se utiliza como protección, ya que obliga al remitente a realizar trabajo en cada transacción.

Actualmente la red tangle es pequeña, y el número de nodos no es suficientemente elevado para que la red funcione sin coordinador. Ésta falta de nodos hace que, al existir un número elevado de transacciones, como podría ser un ataque DDoS, no se puedan procesar de manera eficiente todas las operaciones.

En un futuro próximo, si aumentan el número de nodos y se descentraliza más la red tangle, una inundación de datos como un ataque DDoS podrá ser gestionada rápidamente como para mantener la red funcionando correctamente.

Este problema no es exclusivo de IOTA, ya que cualquier criptomoneda importante sin suficientes nodos en la red se encontrará con una saturación en la red frente a una inundación masiva de datos.

Actualmente existe el proyecto IOTA *Spam Fund* [34] que compensa a aquellos que realicen *spam* pagándoles una pequeña cantidad en IOTAs por cada transacción. Con este proyecto se pretende aumentar el número de nodos para fortalecer la red [50].

[31] https://iotasupport.com/gui-download.shtml
[32] https://getgnulinux.org/es/
[33] https://support.apple.com/es-lamr/macos
[34] http://iotaspam.com/

4.6.3 Cierre del coordinador temporalmente

Debido a un bug[35] a mediados de octubre del 2017, los desarrolladores de IOTA cerraron el coordinador. En consecuencia, el monedero oficial de IOTA no pudo aceptar confirmaciones de transacciones por unos días.

Bug es un término en inglés, cuya traducción literal es insecto, aunque en el argot de la informática tiene otro significado. Un bug, se puede referir a dos situaciones. La primera, el programa no se comporta según las intenciones del programador, su creador. La segunda, las intenciones del informático no satisfacen las expectativas razonables del usuario.

Según la publicación de IOTA no hay descripción clara del bug. Se puede considerar que, debido a errores o ataques, los desarrolladores de IOTA cerraron el coordinador para evitar consecuencias graves. Todas las transacciones fueron suspendidas y el tangle se mostró como una red congelada. Según IOTA la red no se cerró, y una vez reactivado el coordinador se volvió a la normalidad. Los saldos de las direcciones afectadas se transfirieron a direcciones controladas por IOTA y sus propietarios podían recuperar sus saldos sin riesgo una vez volvió la red a funcionar con normalidad.

Por parte de los usuarios, algunos informaron que su nodo permaneció operativo mientras el coordinador estaba cerrado, y algunas exchanges como Bitfinex[36], dejo de procesar transacciones, pero otras continuaron funcionando con normalidad.

En esta situación IOTA, en la que se desconoce el origen del bug, la fundación IOTA pudo cerrar el coordinador y evitar pérdidas de saldo de los usuarios, transfiriendo dichos saldos a cuentas controladas por los desarrolladores de IOTA. Así pues, se podría considerar que actualmente la red está bajo control, pero en dependencia del coordinador [51].

[35] https://es.wikipedia.org/wiki/Error_de_software
[36] https://www.bitfinex.com/

5. Casos de Uso

El principal producto de IOTA es MIOTA, actualmente la moneda digital del tangle, una moneda creada para la economía de la máquina, que ofrece soluciones con respecto a la tecnología de contabilidad distribuida como blockchain.

IOTA pretende ser la columna vertebral del sistema financiero del IoT. Además, también ha integrado otras funciones como mensajería segura y un mercado de datos. Estas características son parte de la economía de la máquina futura prevista por IOTA en las máquinas intercambian datos y pagos en tiempo real. Esto podría incluir desde un automóvil eléctrico que paga una estación de carga hasta sensores meteorológicos de todo el mundo que venden sus datos a científicos que trabajan en la predicción de patrones climáticos.

La característica principal de IOTA que lo hace adecuado para IoT es la falta de tarifas de pago.

Si bien hay muchos casos de uso teóricos para dicho sistema. La sección de "casos de uso" de la documentación de IOTA es escasa e inespecífica, y dice: "*El área de enfoque principal es obviamente Internet de las cosas, especialmente en áreas como Smart Cities, Infraestructura y Smart Grid*[37]*, Supply Chain*[38]*, Transportation and Mobility*".

Existe una enorme cantidad de organizaciones y especialistas individuales involucrados en el proyecto IOTA de todo el mundo, BOSCH que compró una gran cantidad de MIOTA recientemente y ha implantado un miembro de Robert Bosch Venture Capital [39](RBVC) en la junta de asesores de IOTA [52]. En el sector automovilístico Volkswagen también tiene un rol en la junta directiva de IOTA Foundation y es una compañía altamente motivada para integrar sistemas de IoT en sus productos de próxima generación. Por otro lado, cabe mencionar, como miembro del G20 afiliado del foro económico mundial, Julie Maupin [53], también es miembro de la Fundación IOTA.

Algunas de las utilidades actualmente consisten en utilizar el tangle de IOTA como un almacenamiento extremadamente seguro de información, y otros como una plataforma de mensajería segura de extremo a extremo. El gobierno holandés, por ejemplo, utiliza la red tangle para almacenar de forma segura y distribuir documentos legales sobre viviendas locales en la ciudad de Haarlem. Taiwán utiliza la tecnología y la experiencia de IOTA en IoT con el fin de mejorar la ciudad de Taipei[40], como capital de Taiwán en una ciudad inteligente moderna.

Veremos a continuación algunos de los ejemplos mencionados.

[37] https://es.wikipedia.org/wiki/Red_el%C3%A9ctrica_inteligente
[38] https://es.wikipedia.org/wiki/Cadena_de_suministro
[39] http://www.rbvc.com/en/rbvc/home/home.html
[40] https://es.wikipedia.org/wiki/Taip%C3%A9i

5.1 Aplicación de IOTA en la industria.

Recientemente, el Laboratorio de Máquinas-Herramienta e Ingeniería de Producción (WZL) de la universidad RWTH Aachen[41], anunció planes para buscar el uso industrial de IOTA.

Rheinisch-Westfaelische Technische Hochschule[42], es uno de los principales centros educativos de Alemania considerado como una de las dos mejores escuelas para estudios de ingeniería y ciencias.

La iniciativa es única en el mundo, concentrada específicamente en IOTA y la universidad está aceptando inscripciones de científicos y estudiantes que desean involucrarse en el estudio de IOTA y el Tangle.

IOTA ha atraído la atención de la universidad porque la tecnología Directed Acyclic Graph (DAG) del tangle ofrece la posibilidad de transportar y almacenar datos de manera segura, independiente del fabricante y de forma rápida. En comparación con la tecnología blockchain, IOTA permite transacciones sin coste y, por lo tanto, permite nano-pagos, es decir, la liquidación de cantidades muy pequeñas sin pérdidas.

Independientemente de la tecnología, DAG y Blockchain, creen en las posibilidades de tecnologías de contabilidad distribuida, especialmente en lo que se refiere a la economía máquina a máquina. Por lo tanto, antes de desarrollar este proyecto, en RWTH evaluaron con mucho interés diferentes DLT.

En RWTH Aachen University están investigando actualmente la “Internet de producción”, es decir el núcleo del internet industrial de las cosas, a la que llaman IoP (internet de producción). IoP describe una disponibilidad segura de la información en tiempo real en cualquier momento y en cualquier lugar.

En los procesos industriales, se generan gran cantidad de datos, datos precisos y continuos, que pueden proceder por ejemplo de sensores incorporados en las cadenas de producción, y que permiten almacenar automáticamente los datos y si posteriormente es necesario, utilizar estos datos almacenados para realizar estudios, con resultados que podrían detectar patrones de comportamiento.

WZL está trabajando en un proyecto en una máquina que realiza el corte fino de metal. Esta máquina lleva a cabo un proceso laborioso de producción, donde el metal se desenrolla de una bobina, se endereza, se aplana, procesa el material, etc. Este material final es adecuado para la producción de frenos, u otros materiales, que requieren que el producto final obtenido sea siempre idéntico. Para obtener un corte fino con precisión, influyen muchos factores,

[41] http://www.wzl.rwth-aachen.de/
[42] https://www.rwth-aachen.de/

como el material inicial, cortes, matrices, etc. motivo por el cual son necesarios costosos pasos de post-procesamiento. Para evitar estos pasos, es necesario capturar gran cantidad de datos del proceso de elaboración y combinados junto a cálculos de correlación obtener unos parámetros para llegar a establecer unos parámetros idóneas para obtener siempre un producto homogéneo y una producción perfecta.

Los datos que se toman en la producción provienen de sensores de fuerza, temperatura, que detectan las propiedades del material, etc. Se obtienen una cantidad elevada de datos, unos 10Gbit/s. Tal como hemos mencionado el objetivo es guardar todos estos datos y llegar a una correlación entre las mediciones para optimizar el proceso.

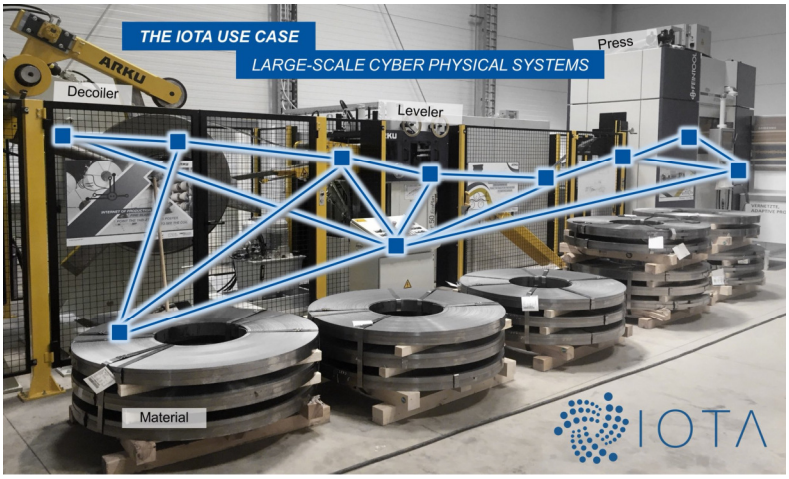

Fig. 17- Máquina en WZL.

En este contexto, IOTA se presenta de tal manera que en los estados del proceso, los pasos de producción y las propiedades de los componentes se mapean digitalmente en la red tangle, para cada componente producido por la máquina. Al mapear estos datos con el libro distribuido, se garantiza la integridad de los datos y la capacidad de llevar a cabo transacciones de datos que son tomados en la cadena de producción, de forma rápida y fluida.

Desde un punto de vista general, la implementación de IOTA en la industria puede aportar grandes beneficios. Podría facilitar la elaboración de patrones, permitir tomar decisiones predictivas en el proceso de producción, y optimizar la producción controlada. Cuando se habla de predicciones en la industria, en el punto más crítico se encuentran las predicciones de errores con un desencadenante fatal, o incluso de patrones que pueden mejorar el rendimiento o evitar ciertas pérdidas de tiempo en una producción en cadena.

La información en tiempo real puede permitir visualizar los procesos, realizar cambios para optimizar la producción, agilizar implementaciones o incluso adaptarse ante cambios en la producción en serie.

En este contexto, si se evalúa la idoneidad de las tecnologías actuales, la tecnología DAG desarrollada por la fundación IOTA presenta una mejor comunicación de maquina a máquina, autonomía de las maquinas, y seguridad

en las comunicaciones, IOTA no conoce tarifas de transacción y, por lo tanto, permite modelos comerciales que requieren el intercambio de nano pagos.

Con la implementación del tangle de IOTA se consigue una comunicación maquina a máquina rápida, transacciones de datos con garantía de integridad, proporcionan también identificadores rastreables y permite una cadena de suministro confiable. Por otro lado, cabe destacar que los clientes podrían disponer de la trazabilidad de los productos [54], [55].

5.2 Tecnología IOTA para la ciudad inteligente de Taipei

La Fundación IOTA, anuncia en enero de 2018 su asociación con la ciudad de Taipei para ayudar a alcanzar sus objetivos de ciudad inteligente.

Taipei busca convertirse en una ciudad inteligente utilizando el poder de la tecnología del libro contable distribuido (DLT). La ciudad ha optado por asociarse con IOTA, para proporcionar una serie de nuevas características tecnológicas para los habitantes. Taipei quiere ser una ciudad inteligente, para ello tiene en marcha una serie de proyectos, buscando mejorar la integridad de los datos y la autenticidad de los servicios públicos.

Un proyecto interesante en la ciudad es el de las “palmeras artificiales” que son sensores para tomar medidas sobre el estado del aire. Aibox[43] una compañía impulsada por Realtek[44] y ASUS[45], entre otras empresas especializadas en redes y sensores, se une a Taipei City e IOTA para crear árboles artificiales del tamaño de una palmera. Con estos sensores se puede detectar, analizar y promover información sobre la temperatura, luz, humedad, contaminación en el aire.

La ciudad de Taipei ya ha estado probando el sistema de sensores de "Airbox". Se han instalado cientos de pequeños sensores, que actualmente se encuentran en los hogares de la ciudad, y 150 escuelas. En la fase inicial todos estos sensores forman una red que recopila información, en la siguiente fase toda esta información se incluyó en una red tangle para facilitar toda esta información mediante una aplicación a los ciudadanos. Este proyecto permite una monitorización del aire en tiempo real con la tecnología IOTA.

En la siguiente imagen, podemos ver una captura del estado del aire en una zona concreta. El usuario que consulta la aplicación puede seleccionar cualquier zona del mapa y consultar contaminación, temperatura, etc. [56]

[43] http://www.airbox.es/
[44] http://www.realtek.com/
[45] https://www.asus.com/es/

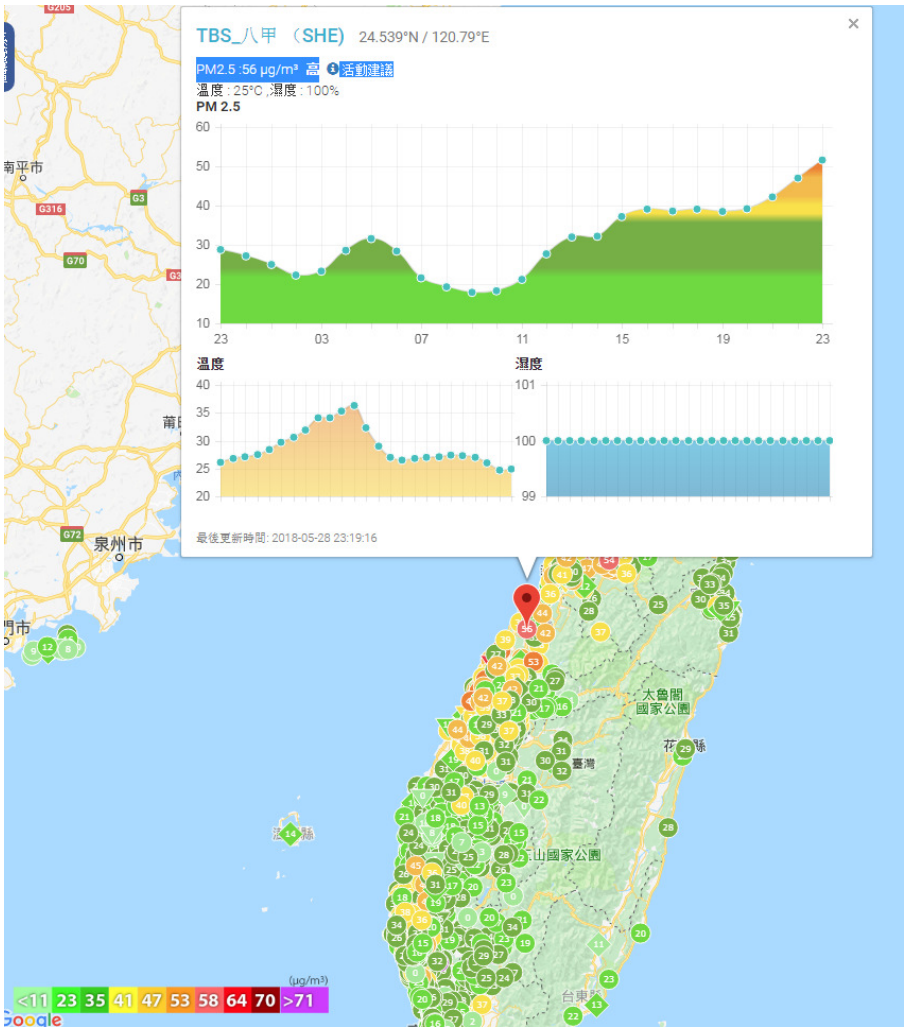

Fig. 17- Captura de la contaminación en tiempo real 28/05/2018 [57].

En este proyecto los datos de las palmeras se toman con sensores “lass airbox” que significa sistema de sensor de ubicación consciente.

El principal problema en este tipo sensores es la gestión de los datos obtenidos, por su alta cantidad y su integridad, ya que estos pueden ser fácilmente manipulados y es difícil validar su transmisión.

Para el intercambio de información, se utiliza los llamados “Flash Channels”. Estos son canales bi-direcionales en un tangle fuera de línea, que permite transacciones instantáneas con un alto rendimiento, es decir con un número elevado de transacciones sin esperar la validación en la red tangle pública de IOTA. Este canal solo permite dos transacciones en la red principal: abrir y cerrar. Cuando un sensor crea un canal, para enviar información, cada parte (emisor-receptor) deposita una cantidad igual de IOTA en una dirección multi-firma controlada por todas las partes. Se empieza a transferir las transacciones y no se necesita interactuar con la red hasta que se cierra el canal, que es cuando los saldos finales se publican en la red tangle. De esta forma el número de transacciones se reduce a dos.

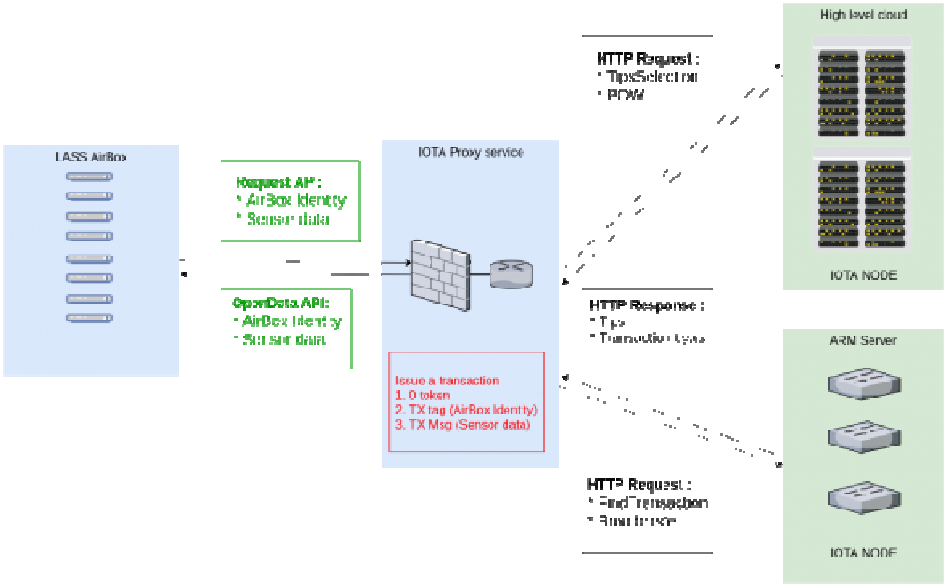

Fig. 18- Esquema comunicaciones sensores LASS [58].

Toda la información ambiental se toma con los sensores de Airbox y se envía con a través de los canales flash a los servidores cloud de Edimax[46], desde estos servidores está disponible la visualización en tiempo real la calidad del aire. Con la aplicación EdiGreen[47], los residentes de la ciudad pueden buscar información sobre la calidad del aire en cada base en cualquier momento.

En este caso con la implementación de IOTA, el tangle garantiza la integridad de los datos y disminuye el riesgo de ataques [58].

Otro proyecto en el que no profundizaremos, es la creación de tarjetas de identidad ciudadana construidas con la tecnología Tangle, llamadas tarjetas "TangleID". La creación de están tarjetas está diseñada para eliminar los riesgos de robo de identidad y fraude electoral, también proporciona un medio para rastrear el historial de salud proporcionando información de antecedentes médicos, y otros datos para los servicios relacionados con el gobierno, como intercambio de datos interurbanos.

La red de identificación digital estará basada en el tangle de IOTA, con la utilización de las tarjetas "TangleID", la identificación estará encriptada, nadie la puede copiar o suplantar.

Si se utiliza una base de datos normal, es posible que con un ataque se puedan a manipular datos o suplantar identidades. Utilizando IOTA se impide la modificación de datos, ya que una vez los datos se envían al tangle y se colocan en el libro mayor, no es posible su manipulación o eliminación.

[46] http://www.edimax.es/edimax/es/
[47] https://play.google.com/store/apps/details?id=com.edimax.airbox&hl=es

La esperanza es que este sistema basado en IOTA disminuya el robo de identidad y el fraude electoral, ya que únicamente cada usuario puede utilizar su Tangle ID, y no puede ser manipulado [56].

5.3 IOTA se utilizará para validar el proceso de identificación.

El municipio de Haarlem empezó en 2017 a desarrollar la solución tangle basada en IOTA para la administración de documentos legales.

Actualmente en muchos países del mundo hay que pasar por una oficina con todo tipo de documentación para demostrar que eres quien eres. Este tipo de procesos implican una pérdida de tiempo y tener que pagar una cantidad de dinero indeterminada para que se le haga entrega de un papel que certifica su identidad. La tecnología DLT es perfecta para hacer más fácil este tipo de servicio. La decisión de utilizar IOTA, fue tomada teniendo en cuenta el consumo de energía, costos de transacción y velocidad de transacción, son mucho más rápidos y menos costosos en IOTA que cuando se trabaja con blockchain por ejemplo.

El municipio de Haarlem[48] encargo a ICTU[49] y Xurux[50] desarrollar una prueba de concepto. Los ciudadanos entran en la web de Haarlem donde inicia sesión utilizando un sistema de gestión de identidad existente (DigID) para pedir un código QR al que llaman “claim”, verificable públicamente. Este código QR es conservado por el ciudadano y contiene información como dirección, numero de la seguridad social, y un hash (attesthah) de datos personales, así como una raíz. Este hash se almacena en IOTA tangle utilizando dicha raíz.

El ciudadano puede usar el QR para probar su ciudadanía a otros y validarla sin la necesidad de un tercero. Por ejemplo, en un registro de la propiedad, se puede demostrar la identidad de la persona con el código QR. Se escanea el QR para obtener la raíz y hash, el valor hash se recupera del tangle y compara con el almacenado en el código QR.

En la siguiente imagen podemos ver todo el proceso, donde Bruce pide su código QR “claim” al gobierno de Gotham, este genera el claim, se lo facilita y lo envía también al tangle. Si bruce quiere utilizar su QR para demostrar su identidad, muestra su QR a la entidad y esta entidad inicia el proceso de verificación del claim, que consiste en el escaneo del código QR. La entidad verifica si los datos del código QR son los mismos que existen en el tangle.

[48] https://www.haarlem.nl/
[49] https://www.ictu.nl/#
[50] https://xurux.nl/

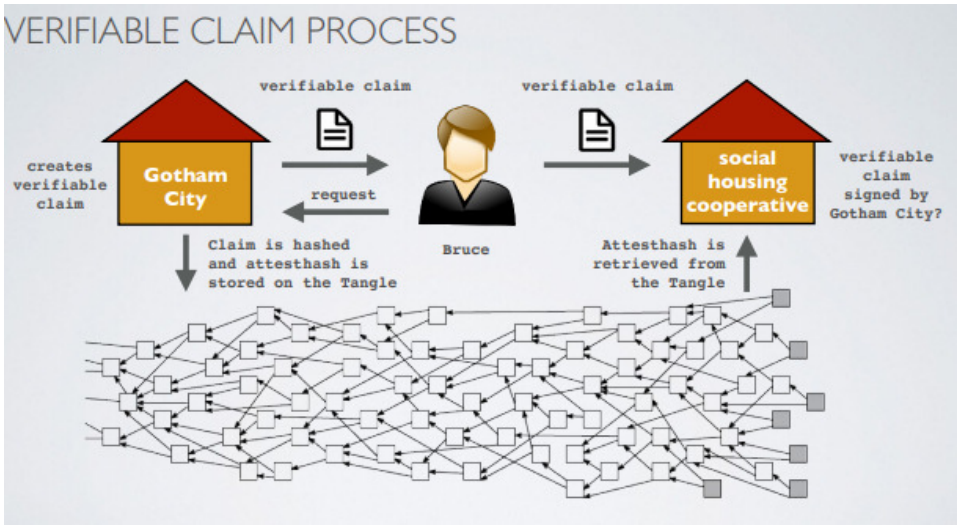

Fig. 18- Representación gráfica del proceso de identificación de un ciudadano [59].

La entidad pública no necesita tener ninguna conexión o interacción con el gobierno, ya que toda la información para validar la identidad está guardada en el tangle.

El software desarrollado por Xurux e ICTU garantiza la autenticidad de los documentos legales a través del tangle de IOTA, ya que la base de datos de los ciudadanos está integrada en el tangle.

Un ciudadano puede demostrarle a la corporación de vivienda que él o ella es un habitante de la ciudad de Haarlem. El ciudadano puede almacenar, autenticar y distribuir documentos gubernamentales sobre la vivienda, de forma segura, de forma rápida y sin la necesidad de visitar el ayuntamiento para recibir documentación oficial.

El software se lanza como un software de código abierto gratuito para uso de organizaciones gubernamentales y municipales que trabajan con extractos de registros públicos [59].

5.4 Sistema de propinas mediante Iota

Actualmente internet está lleno de webs con contenido interesante, pero la mayoría de estas webs, o creadores de contenido, no reciben ninguna remuneración por su trabajo. Tipiota[51] ha sido desarrollado para beneficiar a los creadores de buenos contenidos. De manera voluntaria el lector, si considera que el contenido es adecuado, y el creador merece una retribución monetaria por su trabajo, podrá dar propinas al creador de contenido con “Tipiota”, de ahí el termino tip=propina.

Tipiota es una extensión para los navegadores Chrome y Firefox que está actualmente en modo beta, pero en la que se está trabajando para que

[51] https://www.tipiota.com/

sea integrada y utilizada en la mayor cantidad posible de plataformas sociales. Una vez que la extensión haya sido ampliamente probada se comenzara la fase de expansión a plataformas sociales más grandes como Facebook[52], Twitter[53]y Youtube[54].

Para utilizar Tipiota, es necesario instalar la extensión en el navegador Chrome o Firefox. Una vez instalada la extensión el usuario tiene que entrar en el monedero de IOTA, para poder disponer de IOTA y poder dar propinas. La información de las claves privadas del monedero, nunca se envía a los servidores de Tipiota, así que preservan la seguridad del usuario. En el navegador aparecerá un botón o enlace “Tipiota” en aquellos sitios que soporta el sistema de propinas.

Si un usuario está leyendo un contenido interesante o que considera que el autor merece ser recompensado de alguna manera. Entonces todo lo que hay que hacer es clicar sobre el botón de “Tipiota” y se le abrirá una ventana que le pedirá que ingrese la cantidad de IOTAs que desea donar al autor y luego hacer click en “Tip now”. Esa cantidad de Miotas le llegará al autor instantáneamente sin ningún descuento de comisiones.

En la siguiente imagen podemos ver la extensión del navegador Chrome, y una vez instalada aparece un icono morado en la parte superior donde ya podemos iniciar sesión a nuestro monedero.

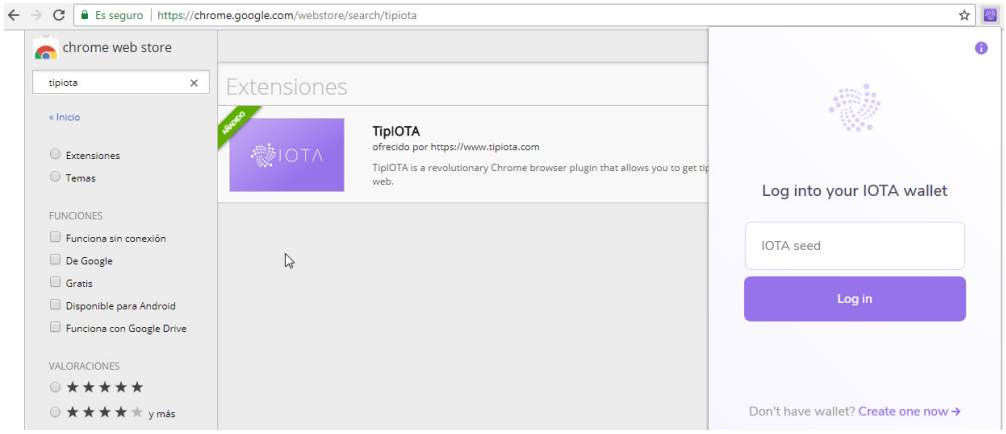

Fig. 19- La extensión de TipIOTA en el navegador Google Chrome.

Tipiota ilustra en su web como el usuario al dar propinar no envía su clave privada a los servidores de Tipiota. Tal como hemos mencionado anteriormente, es muy importante que la clave privada (semilla), el usuario la guarde de forma segura, ya que, si se tiene acceso a ella, es posible acceder a su monedero. Una vez se pierde la clave privada, no se puede recuperar el monedero y en consecuencia pierde los fondos.

[52] https://www.facebook.com/
[53] https://twitter.com/
[54] https://www.youtube.com/

Cuando el usuario da propina, la propina se combina con una dirección generada automáticamente y se envía a la dirección del propietario del contenido web. La propina se almacena en Tipiota y se envía un mensaje automático al destinatario donde aparece un número que corresponde a la dirección autogenerada, y única, para retirar el dinero.

Al mismo tiempo el usuario puede gestionar sus IOTAS, puede ver la cantidad que le han enviado y tiene la posibilidad de retirarlas a su monedero cuando quiera.

Tipiota se distingue de otros servicios similares en que es fácil de usar y por su escalabilidad a futuro sobre todo internet. De todas las criptomonedas disponibles actualmente han escogido IOTA porque como base del sistema es robusta, con cero comisiones y los desarrolladores han considerado que tiene potencial [60].

6. Conclusiones

Este TFM permite comprender la tecnología blockchain y tangle, así como profundizar en el funcionamiento y las características más importantes de IOTA. El tangle es un nuevo libro contable distribuido (DLT), escalable, inmutable, seguro, ligero y que permite realizar transferencias sin comisiones.

El tangle se muestra como una idea prometedora, ya que los dispositivos y maquinas requieren una forma eficiente en cuanto al consumo de recursos para emitir nano transacciones sin altos costes monetarios. En comparación con blockchain, estas son las ventajas del tangle. Sin embargo, en la comparación, de blockchain y tangle, son muchas las similitudes. En ambos casos hablamos de sistemas inmutables, que se basan en la prueba de trabajo (PoW) aunque con diferentes objetivos. Por otro lado, la estructura de datos, así como el rol de los nodos de la red P2P, son diferentes, en blockchain con el usuario y el validador (minero), mientras que en el tangle son la misma persona.

Aunque los objetivos de IOTA, y la tecnología del tangle parecen estar bien concebidos, hay ciertas advertencias de seguridad. En primer lugar, IOTA empezó a utilizar la función criptográfica diseñada especialmente para IoT, la función Curl, que tuvo que ser substituida por la funcion Kerl (versión ternaria de Keccak) al detectar que las firmas podían falsificarse fácilmente. Por otro lado, el enfoque trinario, ha planteado dudas sobre su optimización y agilidad.

El “White paper” de IOTA explica ataques basados en DAG. En el TFM se ha analizado como un atacante puede llegar a dividir la red tangle y realizar transacciones de doble gasto. Ante posibles ataques, y problemas de seguridad, la fundación IOTA pone en funcionamiento al coordinador como sistema de control, para garantizar el correcto funcionamiento del tangle.

Según los creadores de IOTA, cuando exista una cantidad considerable de transacciones en el tangle, no existirán los problemas de colisión y no serán un riesgo los ataques de doble gasto. Cuando en la tangle aumenten el número de transacciones, y la red sea lo suficientemente madura, la fundación cerrará el coordinador y la red tangle crecerá y evolucionada de manera descentralizada.

Tal como se ha analizado en el TFM, IOTA presenta unas características que la hacen adecuada para IoT. Ya que el tangle ofrece un sistema sin tasas de transferencia, ni mineros, integridad de los datos y fluidez de las transacciones. IOTA abre un sinfín de posibilidades, con un abanico muy diverso. En el TFM hemos podido detallar algunos proyectos de uso en la industria, implementado para convertir ciudades inteligentes, en instituciones gubernamentales para facilitar procesos, o incluso en nuestro día a día con extensiones en el navegador para valorar contenido web.

Actualmente son muchos los proyectos en desarrollo o fases de pruebas, pero dado que IOTA-Tangle es la única implementación existente de esta tecnología, el sistema aún tiene que demostrar su correcto funcionamiento con un alto número de transacciones y una red tangle grande.

7. Glosario

El diagrama de Gantt: es una herramienta gráfica cuyo objetivo es exponer el tiempo de dedicación previsto para diferentes tareas o actividades a lo largo de un tiempo total determinado.

P2P: Una red *peer-to-peer*, red de pares, red entre iguales o red entre pares (*P2P*, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

PoW: Un Sistema de prueba de trabajo o Sistema "POW" (del inglés *Proof-Of-Work system*), es un sistema que, para evitar comportamientos indeseados (por ejemplo, ataques de denegación de servicio o spam) requiere que el cliente del servicio realice algún tipo de trabajo que tenga cierto coste y que es verificado fácilmente en la parte del servidor.

Nonce: es un número aleatorio que encuentran los mineros a través de PoW, que se utiliza para construir el nuevo bloque.

Árbol hash de Merkle (en inglés *Merkle Hash Tree*) es una estructura de datos en árbol, binario o no, en el que cada nodo que no es una hoja está etiquetado con el hash de la concatenación de las etiquetas o valores (para nodos hoja) de sus nodos hijo.

Hackathon: Una hackathon o hackatón, es un término usado en las comunidades hacker para referirse a un encuentro de programadores cuyo objetivo es el desarrollo colaborativo de software, aunque en ocasiones puede haber también un componente de hardware. Estos eventos pueden durar entre dos días y una semana. El objetivo es doble: por un lado, hacer aportes al proyecto de software libre que se desee y, por otro, aprender.

Sybil-attacks: En seguridad informática un ataque Sybil ocurre cuando un sistema distribuido es corrompido por una misma entidad que controla distintas identidades de dicha red.

Spam: Se refiere al correo basura y mensaje basura, mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Hashcash es una propuesta realizada por Adam Back en 1997 para combatir el correo basura spam. Más recientemente Hashcash se conoce por su uso en Bitcoin.

8. Bibliografía

[1] Criptomoneda. Wikipedia. 17 mayo, 2018 [consulta: 21 febrero 2018] Disponible en: https://es.wikipedia.org/wiki/Criptomoneda

[2] *¿Qué es IOTA?* ©IOTA Support [consulta: 21 febrero 2018] Disponible en: https://iotasupport.com/whatisiota_es.shtml

[3] *IOTA (protocolo)*. Wikipedia. 21 abril, 2018 [consulta: 21 febrero 2018] Disponible en: https://es.wikipedia.org/wiki/IOTA_(protocolo)

[4] *IOTA estrena mercado descentralizado de datos global*. Noviembre, 2017 [consulta: 21 febrero 2018]. Obtenido de: https://www.criptonoticias.com/aplicaciones/iota-estrena-mercado-descentralizado -datos-nivel-global/

[5] *Bitcoin 101*. Thomson Reuters. Diciembre, 2014 [consulta: 13 marzo 2018] Disponible en: https://web.archive.org/web/20150227213409/http://thomsonreuters.com/business-unit/legal/digital-economy/bitcoin-101.pdf

[6] *Historia del dinero*. Andrés Tejero, CEO Fundador CriptoTendencia.com. Diciembre, 2017 [consulta: 13 marzo 2018] Disponible en: https://criptotendencia.com/2017/12/30/parte-v-historia-del-dinero-desde-el-trueque-hasta-las-criptomonedas/

[7] *Cryptocurrency*. James Surowiecki. Agosto, 2011 [consulta: 13 marzo 2018] Disponible en: https://www. technologyreview.com/ s/425142/cryptocurrency/

[8] *Blockchain, Smart Contracts y seguros*. Josep Celaya, Director Corporativo de Innovación de MAPFRE. Abril, 2017 [consulta: 13 marzo 2018] Disponible en: https://noticias.mapfre.com/blockchain-smart-contracts-seguros/

[9] Bitcoin White paper. Bitcoin Project 2009-2018 System. [consulta: 13 marzo 2018] Disponible en: https://bitcoin.org/bitcoin.pdf

[10] *Qué es una cadena de bloques (BLOCK CHAIN).* CriptoNoticias © 2015-2017. [consulta: 13 marzo 2018] Disponible en: https://www.criptonoticias.com/informacion/que-es-una-cadena-de-bloques-block-chain/

[11] *Prueba de Trabajo (PoW)".* Andrew Tar. Enero, 2018 [consulta: 13 marzo 2018] Disponible en: https://es.cointelegraph.com/explained/proof-of-work-explained

[12] *La minería de Bitcoin: nodos y recompensas.* Salva Lizana. 5 abril, 2018 [consulta: 13 marzo 2018] Disponible en: https://www.territorioblockchain.es/mineria-de-bitcoin-recompensas/

[13] *Bitcoin Avg. Transaction Fee historical chart*. [consulta: 13 marzo 2018] Disponible en:https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

[14] *¿Qué son las criptomonedas?* Gleen Marten. Abril, 2018 [consulta: 13 marzo 2018] Disponible en: https://ideacanal.com/que-son-las-criptomonedas/

[15] *Suecia concluye con éxito prueba de registro de* propiedad basada en blockchain. Isabel Pérez. Abril, 2017 [consulta: 13 marzo 2018] Disponible en: https://www.criptonoticias.com /aplicaciones/suecia-concluye-exito-prueba-registro-propiedad-basado-blockchain/

[16] *Storj creara una plataforma informática descentralizada en la nube con la supercomputadora de Sonm*. Emily Faria. Noviembre 2017 [consulta: 13 marzo, 2018] Disponible en: https://www.criptonoticias.com/aplicaciones/storj-creara-plataforma-informatica-descentralizada-nube-supercomputadora-sonm/

[17] *Spotify sí que cree en blockchain: así funciona Mediachain, la empresa que acaba de comprar.* Javier Pastor. 8 Mayo, 2017 [consulta: 13 marzo 2018] Disponible en: https://www.xataka.com/empresas-y-economia/spotify-si-que-cree-en-blockchain-asi-funciona-mediachain-la-empresa-que-acaba-de-comprar

[18] *Who Will Build the Health-Care Blockchain?* Mike Orcutt. Septiembre 15, 2017 [consulta: 13 marzo 2018] Disponible en: https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/

[19] *That 'Internet of Things' Thing.* Kevin Ashton cofounder and executive director of the Auto-ID Center. 22 junio 2009 [consulta: 20 marzo 2018] Disponible en: http://www.rfidjournal.com/articles/view?4986

[20] *CES 2015: The Internet of Things is Here, and It May Even Be Useful*. Marc Perton. 2017 [consulta: 20 marzo 2018] Disponible en: http://bigthink.com/think-tank/ces-2015-internet-of-things

[21] *Un estudio de HP revela vulnerabilidades del Internet de las Cosas*. Redacción Computing. 18 febrero, 2015 [consulta: 20 marzo 2018] Disponible en: http://www.computing.es/seguridad/informes/1079674002501/estudio-hp-revela-vulnerabilidades-internet-cosas.1.html

[22] *Sobreviviendo en el mundo IoT: Expertos de Kaspersky Lab exponen los riesgos de dispositivos domésticos inteligentes*. 5 noviembre, 2015 [consulta: 20 marzo 2018] Disponible en: https://latam.kaspersky.com/about/press-releases/2015_sobreviviendo-en-el-mundo-iot-expertos-de-kaspersky-lab-exponen-los-riesgos-de-dispositivos-domesticos-inteligentes

[23] *Un manual sobre IOTA.* ©IOTA Support. 21 mayo, 2017 [consulta: 23 marzo 2018] Disponible en: https://blog.iota.org/a-primer-on-iota-with-presentation-e0a6eb2cc621

[24] *Entrevista exclusiva a Dominik Schiener, para Japon*. 2 noviembre, 2017 [consulta: 23 marzo 2018] Disponible en: http://www.iotahispano.com/2017/11/02/entrevista-exclusiva-a-dominik-schiener-para-japon/

[25] *Blockchain network IOTA teams up with Microsoft, others on data marketplace*, Reuters. 28 noviembre, 2017 [consulta: 23 marzo 2018] Disponible en: https://www.reuters.com/article/us-blockchain-iota-cisco/blockchain-network-iota-teams-up-with-microsoft-others-on-data-marketplace-idUSKBN1DS2EE

[26] *IOTA SUPPORT.* ©IOTA Support [consulta: 23 marzo 2018] Disponible en: https://iotasupport.com/

[27] *IOTA ECOSYSTEM.* © 2018 IOTA Foundation [consulta: 23 marzo 2018] Disponible en:https://blog.iota.org/announcing-the-iota-ecosystem-339612656bc3

[28] *Anuncios IOTA*. ©IOTA Support [consulta: 23 marzo 2018] Disponible en: https://blog.iota.org/tagged/announcements

[29] White paper IOTA. IOTA Foundation. [consulta: 30 marzo 2018] Disponible en: http://iotatoken.com/IOTA_Whitepaper.pdf

[30] *Cryptographic vulnerabilities in IOTA*. 7 Septiembre, 2017 [consulta: 30 marzo 2018] Disponible en: https://medium.com/@neha/cryptographic-vulnerabilities-in-iota-9a6a9ddc4367

[31] *Firmas basadas en hash*. 18 julio, 2013 [consulta: 30 marzo 2018] Disponible en:https://www.imperialviolet.org/2013/07/18/hashsig.html

[32] Criptografía de curva elíptica. Wikipedia®. 25 diciembre, 2017 [consulta: 30 marzo 2018] Disponible en: https://es.wikipedia.org/wiki/criptograf%c3%ada_de_curva_el%c3%adptica

[33] *Post-Quantum Cryptography. © 2009 Springer-Verlag Berlin Heidelberg.* Diciembre 2008 [consulta: 30 marzo 2018] Disponible en: https://www.e-reading.club/bookreader.php/135832/Post_Quantum_Cryptography.pdf

[34] *Weird Number Bases.* © 2009-2015 DataGenetics. Diciembre 2015 [consulta: 30 marzo 2018] Disponible en: http://datagenetics.com/blog/december22015/index.html

[35] *The Balanced Ternary Machines of Soviet Russia.* Noviembre 2016 [consulta: 30 marzo 2018] Disponible en: https://dev.to/buntine/the-balanced-ternary-machines-of-soviet-russia

[36] *Operador ternario de java*. 22 febrero 2016[consulta: 30 marzo, 2018] Disponible en: http://programacionextrema.com/2016/02/22/operador-ternario-en-java

[37] *Data Security for the Internet of Things.* Andrew Shipilov, 19 abril, 2018 [consulta: 30 marzo 2018] Disponible en: https://knowledge.insead.edu/blog/insead-blog/data-security-for-the-internet-of-things-8911#kieyweekdlodigvl.99https://knowledge.insead.edu/blog/insead-blog/data-security-for-the-internet-of-things-8911

[38] *Transaciones, comfirmaciones y consenso de IOTA.* 7 noviembre, 2017 [consulta: 30 marzo 2018] Disponible en: http://www.iotahispano.com/ 2017/11/07/transacciones-confirmaciones-y-consenso-en-iota/

[39] *Tangle: una introduccion ilustrada*. Geronimo Patat. 17 marzo, 2018 [consulta: 10 abril, 2018] Disponible en: http://www.iotahispano.com/2018/03/17/tangle-una-introduccion-ilustrada-5ta-parte/

[40] *Hashcash*. Wikipedia®. 5 enero, 2018 [consulta: 10 abril, 2018] Disponible en: https://es.wikipedia.org/wiki/Hashcash

[41] Is a doublespending attack posible with IOTA? 10 julio, 2017 [consulta: 10 abril 2018] Disponible en: http://www.tangleblog.com/2017/07/10/is-double-spending-possible-with-iota/

[42] *How does IOTA protect against a DoS attack that continuously splits the tangle?* [consulta: 10 abril 2018] Disponible en: https://www.reddit.com/r/Iota/comments/73zyzj /how_does_iota_protect_against_a_dos_attack_that/

[43] *Why you don't roll your own crypto*. 10 diciembre, 2015 [consulta: 10 abril 2018] Disponible en: https://motherboard.vice.com/en_us/article/wnx8nq/why-you-dont-roll-your-own-crypto

[44] *Criptoanálisis diferencial.* Wikipedia. 4 enero, 2018 [consulta: 10 abril 2018] Disponible en: https://en.wikipedia.org/wiki/Differential_cryptanalysis

[45] *Actualizaciones y actualizaciones*. ©IOTA Support. 7 agosto, 2017 [consulta: 10 abril 2018] Disponible en: https://blog.iota.org/upgrades-updates-d12145e381eb

[46] *Peligro: Vulnerabilidades Criptográficas En IOTA*. Agosto 2017 [consulta: 10 abril 2018] Disponible en: https://steemit.com/blockchain/@xervantex/peligro-vulnerabilidades-criptograficas-en-iota

[47]*Phising de IOTA: 4$ millones robado por un hacker.* http://www.ibtimes.com/iota-phishing-scam-4-million-stolen-hacker-2646922

[48] *Los usuarios de criptomonedas de IOTA pierden $ 4 millones en ataque inteligente de phishing.* 29 enero, 2018 [consulta: 10 abril 2018] Disponible en: https://www.bleepingcomputer.com/news/security/iota-cryptocurrency-users-lose-4-million-in-clever-phishing-attack/

[49] *La red de IOTA lucha debido a la falta de nodos completos.* 22 noviembre, 2017 [consulta: 10 abril 2018] Disponible en:https://themerkle.com/iota-network-struggles-due-to-lack-of-full-nodes/

[50] *IOTA spam fund.* 31 mayo, 2016 [consulta: 10 abril 2018] Disponible en: http://iotaspam.com/

[51] IOTA:Coordinador abajo, precios arriba. Gabriel Jara. 30 octubre, 2017 [consulta: 10 abril 2018] Disponible en: http://www.iotahispano.com/2017/10/30/iota-coordinator-abajo-precios-arriba/

[52] *Bosch Group Has Purchased A Significant Amount Of IOTA (MIOTA) Tokens.* 19 diciembre, 2017 [consulta: 03 mayo 2018] Disponible en: https://oracletimes.com/bosch-group-has-purchased-a-significant-amount-of-iota-miota-tokens/

[53] *Welcome Julie Maupin to IOTA.* ©IOTA Support. 17 julio, 2017 [consulta: 03 mayo 2018] Disponible en: https://blog.iota.org/welcome-julie-maupin-to-iota-14b9ac92478f

[54] *Pressen information.* Reale Industrieanwendung mit IOTA. 06 abril, 2018 [consulta: 03 mayo 2018] Disponible en: https://www.wzl.rwth-aachen.de/ cms/www_content/de/dc5f626f19bbf8f1c125826700371c46/pressemeldung_iota.de.pdf

[55] *Big Data, IOTA y una gran aplicación en ingeniería de máquina herramienta*. Markus. 22 abril, 2018 [consulta: 03 mayo 2018] Disponible en: https://medium.com/coinmonks/big-data-iota-and-a-great-application-in-machine-tool-engineering-1b6210cf5129

[56] IOTA y Taipei firman asociación! Ezequie Outon. 30 enero, 2018 [consulta: 03 mayo 2018] Disponible en: http://www.iotahispano.com/2018/01/30/iota-y-taipei-firman-asociacion/

[57] PM2.5 OPEN DATA, 2017, 2018 © LASS Community / Academia Sinica. [consulta: 20 marzo 2018] Disponible en: https://pm25.lass-net.org/

[58] *Monitorización de contaminación con IOTA. Ezequie Outon.* 23 noviembre, 2017 [consulta: 03 mayo 2018] Disponible en: http://www.iotahispano.com /2017/11/23/monitorizacion-de-contaminacion-con-iota/

[59] *IOTA tutorial 22: Masked Authenticated Messaging Demo Verifiable Claims.* Mobilefish. 16 abril, 2017 [consulta: 03 mayo 2018] Disponible en: https://www.mobilefish.com/download/iota/verifiable_claims_part22.pdf

[60] *Tip anyone on any social media platform*. ©2018 Tip IOTA. [consulta: 03 mayo 2018] Disponible en: https://www.tipiota.com/