UNIVERSITAT POLITÈCNICA DE CATALUNYA

FACULTAT D'INFORMÀTICA DE BARCELONA

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

FIB

Blockchain-based authentication of IP addresses

Autor: Ismael Julià Reifs

Especialitat: Enginyeria del Software

Director: Alberto Cabellos Aparicio
Subdirector: Jordi Paillissé Vilanova

Tutor: Ferran Sabate Garriga

Data: 19/06/2018

Descripció

En aquest projecte s'escolleix i estableix un sistema software capaç d'assignar adreces IP amb una seguretat acceptable, comprovant quins problemes sorgeixen en la seguretat i quins són evitables partint d'eines actuals que desenvolupen la mateixa tasca. Per realitzar aquest treball utilitzarem la *Blockchain* de IOTA[1], fent un estudi de les estructures de dades i algorismes que té i com podem adequar-los al nostre context, per així finalment arribar a una conclusió de si la proposta que fem té prou potencial per ser una solució efectiva en l'assignació d'adreces IP.

Descripción

En este proyecto se escoge y establece un sistema software capaz de asignar direcciones IP con una seguridad aceptable, comprobando qué problemas surgen en la seguridad y cuales son evitables partiendo de las herramientas actuales que desarrollan la misma tarea. Para realizar este trabajo utilizaremos la *Blockchain* de IOTA, haciendo un estudio de las estructuras de datos y algoritmos que tiene y como podemos adecuarlos a nuestro contexto, para así finalmente llegar a una conclusión de si la propuesta que hacemos tiene suficiente potencial para ser una solución efectiva en la asignación de direcciones IP.

Description

In this project we choose and establish a software system that will be able to assign IP addresses with an acceptable security, checking the problems that may appear in the security and which ones can be avoided with the actual tools that develop the same task. In this project we will use the IOTA's *Blockchain*, and we will elaborate a research of the data structures and algorithms that it has and how we can adapt them in our context, in order to conclude if our proposal has the sufficient potential to be an effective solution in the assignment of IP addresses.

Índex

1. Introducció i contextualització

Aquest és un treball de fi de grau (TFG) realitzat en el Grau d'Enginyeria Informàtica cursat a la Facultat d'Informàtica de Barcelona, i desenvolupat conjuntament amb col·laboració del Departament d'Arquitectura de Computadors.

El projecte es basa en la *Blockchain* o tecnologia *ledger* distribuïda(DLT), impulsat i desenvolupat primerament per Bitcoin [2], per tal de tenir un mètode de comptabilitat. Aquest projecte ha sorgit a partir d'una investigació prèvia, feta pel director i subdirector d'aquest projecte, juntament amb altres investigadors, sent l'únic document que presenta formalment una proposta en l'àmbit IP en la data d'inici del projecte. La motivació per realitzar-lo ha sorgit pel fet que Bitcoin no està regulat per una autoritat central, així que són els mateixos usuaris els que poden dictar i validar les transaccions que s'envien per rebre béns o serveis, eliminant qualsevol tercera persona involucrada que aporti veracitat a la transacció, fet que comporta que es pugui produir un ambient de desconfiança entre les entitats involucrades, ja que pot usar-se sense la necessitat de certificats digitals i control centralitzat, en canvi s'utilitzaran medis que proporciona la *Blockchain* per arribar a un consens de forma distribuïda.

Per tant, aquest treball té com a punt de partida entendre les principals funcionalitats de la *Blockchain* i poder-les usar en un camp concret d'Internet. Específicament busca donar una nova solució a l'assignació d'adreces IP a partir d'un projecte amb una *Blockchain* pròpia que va sorgir l'any 2017, anomenat IOTA i que presentarem més endavant.

L'objectiu és comprovar quins aspectes positius i negatius en la seguretat aporta aquesta nova tecnologia comparada amb les tecnologies convencionals que desenvolupen la mateixa tasca i usar aquesta nova forma d'enviament d'informació a partir de transaccions per tal de poder fer l'assignació d'adreces IP. Per tal d'arribar al nostre propòsit, caldrà partir d'un anàlisi de com funciona actualment la *Blockchain*, primerament introduint Bitcoin i després IOTA, per tal de conèixer el per què de l'elecció d'aquest última *Blockchain* i quins mètodes, estructures de dades i seguretat ens ofereix per realitzar el nostre propòsit. Després de conèixer bé com funciona aquest sistema, usarem les funcionalitats de les que disposa adaptant-lo al nostre estudi, de tal forma que crearem un petit software per comprovar com seria el funcionament de les assignacions IP a un usuari o un grup d'usuaris en concret, amb una seguretat d'acord amb el propòsit del projecte.

A partir d'aquesta introducció, el següent pas és definir els diferents actors implicats en el projecte. Dit això passem a la següent secció, on seran identificats.

1.1 Actors implicats

Com aquest projecte es basa en un estudi d'una nova tecnologia, no es pretén que sigui utilitzat com un sistema per realitzar una certa tasca, sinó que el que es pretén és que els beneficiaris n'utilitzin per crear o analitzar una proposta semblant o igual a la seva. Una vegada realitzat aquest treball podrà servir de recolzament tant en l'àmbit d'investigació com empresarial, les parts beneficiades seran:

Desenvolupador principal És l'única persona que desenvoluparà el projecte, i s'encarregarà d'assolir les fites d'aquest, fent la seva respectiva documentació, software i presentació.

Investigadors Ha sorgit un gran interès per part dels equips d'investigadors per tractar problemes encara no resolts o optimitzar els existents a partir d'aquesta tecnologia, el fet de poder interconnectar persones en un camp específic, pot ser pensat també com una forma d'interconnectar el pensament i idees per tal de trobar solucions des d'una altra perspectiva, és a dir, tenir una nova proposta encara no provada per resoldre un mateix problema i pensar si realment usant el punt de vista que ofereix la *Blockchain* ajudaria a resoldre'l o avançar i desenvolupar un sistema més competent que l'actual, independentment de que l'estudi que realitzin sigui de la mateixa temàtica d'aquest treball o no.

Empreses Hi ha diverses empreses en múltiples sectors que estan analitzant si aquesta nova tecnologia podria ser desenvolupada per oferir el mateix que els productes actuals però amb més seguretat i millor funcionalitat. L'interès per trobar fonts fiables i que expliquin clarament què poden i què no poden fer resultaria molt atractiu en el cas que vulguin donar un salt a la *Blockchain*.

Emprenedors Els facilita una introducció a la *Blockchain* i els orienta a poder fer un estudi o projecte igual o semblant en el context d'Internet, o si simplement volen conèixer més sobre aquesta tecnologia, ajudant-los a tenir una idea d'aquesta amb la possibilitat de que la puguin adaptar en un futur. La *Blockchain* pot ser usada en quasi totes les temàtiques, ja que no només es tracta de fer una transacció de valor monetari, sinó que es pot adaptar el *token* a un projecte en concret fent altres usos, com per exemple en sistemes que controlen la cadena de subministrament. Aquest fet està ajudant a que grups d'emprenedors estiguin enfocant el seu nou projecte en aquesta nova tecnologia, ja que no podrien competir amb les empreses que dominen actualment el mercat segons en quina temàtica, això ajuda tant a crear oportunitats per a nous projectes com a avançar la tecnologia.

Ara que ja hem definit de què es tractarà el projecte, quins són els objectius i les persones involucrades en el mateix, és un bon moment per passar a la secció de l'estat de l'art, on explicarem la base teòrica en la que es sustenta el treball.

1.2 Estat de l'art

La *Blockchain* o DLT ha començat a ser popular des de l'aparició de Bitcoin l'any 2007. Es presenta com una base de dades criptogràfica segura que guarda les diferents transaccions dels *tokens* d'una adreça a una altra i que no és editable (aquest punt serà tractat amb més detall a la secció 1.2.2). Un punt a destacar és que aquesta base de dades és compartida mitjançant els nodes amb una còpia, és a dir, ningú podrà apropiar-se individualment d'ella. Això suposa una innovació en la informació registrada i distribuïda que elimina la necessitat d'una entitat per facilitar els intercanvis digitals i la confiança entre elles, ja que soluciona el problema dels generals bizantins [2]. La *Blockchain* resulta ser una combinació de tecnologies existents però aplicades d'una nova forma, en concret de tres: la xarxa P2P [3], la criptografia de la clau

privada [4] i un protocol [5] que governi els incentius. El resultat és un sistema per transaccions digitals.

La confiança és un judici entre diferents entitats, i en el món virtual, determinar aquesta confiança acaba consistint en aprovar una identitat (autenticació) i aprovar els permisos (autorització). En el cas de la tecnologia *Blockchain*, la criptografia de la clau privada ens dóna una eina per tal d'assolir els requeriments d'autenticació. La possessió d'una clau privada és personal, evitant que una persona hagi de compartir informació confidencial que d'una altra forma es requeriria per fer una transacció. En aquest punt ens adonem que autentificació no és suficient, necessitem autorització, la qual necessita una xarxa P2P com a punt de partida, a més a més de reduir el risc de centralització o fallades.

Aquesta xarxa distribuïda també s'ha de comprometre amb el manteniment dels registres coneguts com a blocs i la seguretat de la xarxa de transaccions, ja que l'autorització de les transaccions és el resultat de que tota la xarxa aplica les seves regles pròpies, el protocol *Blockchain*, encarregat de validar nous blocs.
Per realitzar els intercanvis anteriorment esmentats és necessari d'un bé digital que es pugui intercanviar per un altre bé o per un servei, en la *Blockchain* d'aquesta moneda se'n diu *token*. Hi ha una gran varietat de *tokens* en el mercat digital actual [6], on els més populars són Bitcoin i Ethereum.

La descentralització i la seguretat que aporta aquesta nova tecnologia és un dels principals motius que han impulsat la realització d'aquest treball. Les eines actuals que són usades per fer assignacions IP contemplen un gran ventall d'atacs i proporcionen la seguretat que els usuaris i empreses desitgen, però a partir d'aquí volem comprovar si aquesta nova tecnologia de la Blockcahin té prou potencial per poder contrarestar alguns problemes existents, tant en la seguretat com en l'ús de les tecnologies convencionals referent al context de les adreces IP.

En el nostre cas la millor forma de començar és definint les nocions bàsiques del primer projecte que va aparèixer en la *Blockchain*, Bitcoin. Dit això procedim a fer-ho a la següent secció.

1.2.1 Nocions essencials de la *Blockchain* Bitcoin

Per tal de fer una correcta introducció a la *Blockchain*, es farà un resum del funcionament bàsic a continuació:

Tot comença quan un node d'un usuari vol fer una transacció, és a dir, una transferència de valor entre un origen i un o diversos destinataris. Quan s'envia, aquesta es transmesa per la xarxa *Blockchain* i recopilada en una estructura de dades que té com a nom blocs. Aquesta estructura, que es pot entendre com un arxiu que guarda les dades de les transaccions, és semblant a les pàgines d'un llibre on es registren les transaccions d'accions de borsa. Els blocs s'organitzen dins de la *Blockchain* com una seqüència lineal al llarg del temps, conegut com cadena de blocs i amb el propòsit de confirmar quines transaccions de la xarxa són vàlides. Per fer-ho, hem d'incloure un nou element, en aquest cas el miner. Es tracta d'un altre node, però que en aquest cas col·labora en processar les noves transaccions i afegir-les als blocs per tal de que posteriorment siguin acceptats pel conjunt d'usuaris (consens). La forma en que fa aquest procés és fent un *Proof of Work* (PoW) de tota les dades que contenen els blocs per tal de ser considerats vàlids.

La feina del PoW és de resoldre computacionalment una espècie de trenca-closques, que variarà en dificultat depenent de l'estat en el que es trobi la *Blockchain* i el total d'usuaris miners. Una vegada que s'ha validat el bloc pel miner, passa als altres nodes, fins que entre tots arriben a un consens de que aquest bloc és certament vàlid. L'incentiu d'aquest procés, és que cada miner que participa en el PoW d'un bloc, rep a canvi una quantitat de Bitcoins, que en aquest sistema de la *Blockchain* representarien les taxes a pagar per fer la transacció. Tot això suposant que el bloc on estava inclosa la transacció enviada s'ha validat correctament per tots els nodes, arribant a tenir les 6 confirmacions necessàries (cada bloc que es genera després d'aquest és una confirmació). Després de la sisena confirmació es considera que ja ha estat completament validada, per tant, des d'aquest moment queda inclosa a la *Blockchain* per sempre, sense poder patir modificacions. Gràcies a que aquesta transacció no està encriptada, es pot buscar en la *Blockchain*, així podem saber d'on s'han rebut els diners i a on s'envien, ja que una de les propietats que té és que les transaccions estan vinculades entre elles.

En la següent secció es farà una introducció bàsica al funcionament de Bitcoin, per tal de tenir una base per quan es parli posteriorment de transaccions, adreces i de claus públiques i privades.

1.2.2 El funcionament de Bitcoin

Prenent com a exemple Bitcoin, la representació de la moneda és una entrada a la base de dades, que enregistra una transacció monetària. En el cas d'un banc, tant la persona A com la persona B serien propietàries d'un compte i s'identificarien amb un número de compte. A Bitcoin qualsevol persona pot generar un parell de claus criptogràfiques públiques i privades que poden servir per a crear un equivalent a un compte bancari (Figura 1), el qual denominarem direcció Bitcoin, aquesta identificarà de forma única al propietari d'un compte, sent aquest compte el *hash* de la clau pública generada.

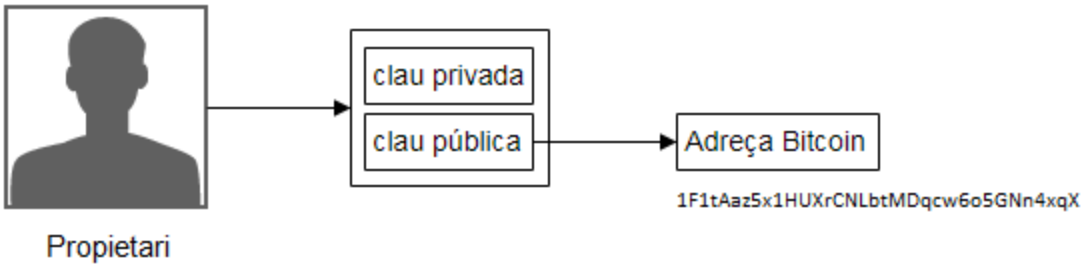


Figura 1: Identificació d'un compte

Com s'ha explicat anteriorment, Bitcoin no és un actiu tangible, sinó que és una transacció que es registra en un llibre anomenat *Blockchain*. Aquesta transacció bàsicament, manté l'origen dels ingressos amb una direcció Bitcoin i assigna els enviaments amb una altra direcció.

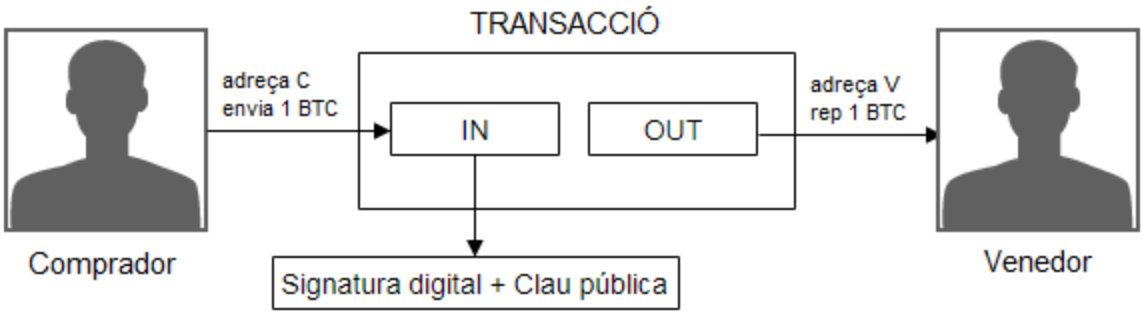


Figura 2: Esquema bàsic d'una transacció

Per garantir la propietat dels Bitcoins, tota transacció s'ha de firmar digitalment amb la clau privada de l'usuari que envia una quantitat de diners. Després, la firma, juntament amb la clau pública seran incloses a la transacció (Figura 2). Això permet que qualsevol persona pugui validar que els Bitcoins transferits són realment de la propietat del remitent.

Hem de fer èmfasis en un punt, i és que les transaccions no existeixen per si mateixes, és a dir, cada entrada a una transacció és un punter a una transacció anterior. En resum, l'entrada usada en una transacció és el resultat d'una transacció anterior, ja que la *Blockchain* emmagatzema aquesta llista vinculada de transaccions, per aquest fet, qualsevol Bitcoin enviat pot rastrejar-se fins al seu origen, on poden haver-hi transaccions amb múltiples fonts d'entrada i de sortida per entre mig.

Finalment hem d'esmentar que els clients de la xarxa Bitcoin posseeixen una còpia de la *Blockchain*, que és pública i accessible per a qualsevol persona per tal d'aportar una transparència en aquesta moneda virtual, fet que genera un contacte més proper amb el sistema.

Ara que ja sabem de forma bàsica com funciona Bitcoin, podem comentar alguns dels problemes que sorgeixen en aquesta *Blockchain*, i alguns dels motius per els quals s'ha plantejat fer aquest treball amb la *Blockchain* de IOTA.

Problema de l'escalabilitat

És degut a la quantitat de transaccions que la xarxa Bitcoin pot processar, degut a que els registres (blocs) en la *Blockchain* estan limitats en mida i freqüència. La capacitat de transacció de la xarxa Bitcoin està limitada per la creació de blocs, que en mitjana és de 10 minuts i la mida màxima del bloc. Aquests dos factors restringeixen el rendiment de la xarxa, on la capacitat màxima de processament de les transaccions està estimada entre 3.3 i 7 transaccions per segon.

Temps

És degut a l'activitat a la xarxa i les taxes que s'han de pagar als miners per tal de processar els blocs. Quantes més transaccions s'han de processar, més temps triga cada una. Això és degut a que hi ha un nombre finit de miners que poden processar cada bloc, com també hi ha un nombre finit de transaccions que es poden incloure a cada bloc. Els miners, prioritzen les transaccions que tinguin una taxa o recompensa més elevada, degut a això, moltes d'elles triguen més en ser processades ja que l'incentiu dels

miners és el benefici.

Com hem mencionat anteriorment, la creació d'un bloc és de 10 minuts, però generalment es necessiten 6 confirmacions dels miners abans que es processi, així que estem parlant d'un temps aproximat d'una hora per transacció. Degut a la popularitat que ha guanyat avui dia Bitcoin, el temps ha incrementat de 30 minuts per confirmació a 16 hores en casos extrems.

Taxes

Les taxes s'eleven cada vegada més, i és un problema, ja que no facilita les micro-transaccions degut a que es pot arribar a pagar més de taxa que de quantitat transferida.

Fork

Degut al problema d'escalabilitat que hem parlat anteriorment, es requereixen fer canvis sobre el funcionament de la xarxa Bitcoin, aquest és un procés que s'anomena *fork*. El *fork* presenta alguns problemes, sobretot pels usuaris, ja que el pitjor cas és quan la *Blockchain* es divideixi en dos i causa confusió de cap a on s'han d'enviar els *tokens* o monedes virtuals.

- ***Hard fork*** quan la *Blockchain* es separa en dues incompatibles *chains*. Això és degut a que dues o més conjunts de regles estan intentant governar el sistema.

- ***Soft fork*** quan hi ha un canvi de regles que permet crear nous blocs reconeguts com a vàlids per versions anteriors del sistema.

Havent definit el funcionament i els principals problemes de Bitcoin, el líder d'aquest camp en aquest moment, farem un petit incís en el document d'investigació en la següent secció, posteriorment com s'ha realitzat l'elecció del sistema per desenvolupar el projecte i els avantatges d'utilitzar-lo.

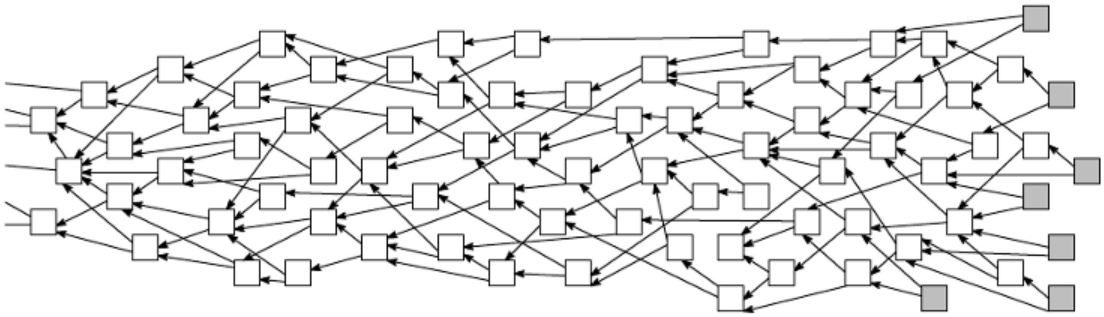
1.2.3 Proposta de projecte d'investigació, elecció i avantatges en utilitzar IOTA

Com s'ha esmentat en la introducció del projecte, partim d'un estudi ja realitzat, però en aquest cas, afegint un valor ja que també fem un estudi i un anàlisi posterior dels resultats obtinguts amb la *Blockchain* de IOTA. Partim de la proposta inicial del document d'investigació "*An analysis of the applicability of Blockchain to secure IP addresses allocation, delegation and bindings*" [7] que tracta d'analitzar la seguretat d'assignar, vincular i delegar direccions IP en una *Blockchain*, a partir d'entitats desconegudes entre si i tenint com a algorisme de consens el *Proof of Stake* (PoS). En el seu anàlisi es refereixen al PoW com a una forma d'usar el poder computacional per fer segura la *Blockchain*, ja que ha estat provat en programes financers, però no sempre el poder computacional dels participants en una *Blockchain* va lligat amb l'interès de voler que aquesta funcioni correctament. Partint d'aquí és on comencen a definir-se la possibilitat d'atacs. Per això posteriorment fan una proposta utilitzant PoS, on els participants amb més *tokens* tenen més probabilitat de confirmar els blocs, partint d'aquí les entitats que tenen més *tokens* tenen més control de la *Blockchain*. La raó d'utilitzar aquesta algorisme de consens és que per un atacant, el fet de tenir més *tokens*, en aquest

cas, adreces, és molt més complex que no pas el d'acumular poder computacional, ja que l'algorisme PoS no pot ser afectat per recursos externs a la pròpia *Blockchain*.

A partir d'aquest raonament vam començar a discutir quins algorismes de PoS es podrien utilitzar en aquesta aplicació. Després d'investigar els projectes NXT [8], NEO [9] i IOTA vam esbrinar que IOTA tenia un algorisme PoW, però en comparació amb els altres va ser el més atractiu pel fet que utilitzava una nova estructura de dades diferent a una cadena de blocs, i per tant, funcionava amb un mecanisme molt diferent, resolent els problemes de temps i escalabilitat, així que vam decantar-nos per aquest, deixant de banda l'algorisme de PoS, ja que va ser el que vam veure amb més potencial per ser estudiat.

A més a més, en comparació amb NEO i NXT, IOTA estava molt més ben documentat i tenia una API pels desenvolupadors, afavorint la presa en contacte i anàlisi posterior en el nostre context, i si és o no pitjor opció que altres que usen PoS.



Partint d'aquesta petita síntesis, farem una introducció a IOTA i quins són els seus avantatges abans de procedir amb el seu funcionament bàsic.

IOTA [10] usa el Tangle per tal de guardar les transaccions, que es basa en un protocol asíncron en una xarxa P2P, representat per un graf directe acíclic, on no hi ha blocs, ni cadenes, ni miners. Degut a això funciona de forma bastant diferent a les altres *chains*.

Al no haver-hi miners, cada participant en la xarxa que vulgui fer una transacció ha de participar en el consens de la xarxa aprovant dues transaccions anteriors, aquest fet aconsegueix que tota la xarxa assoleixi un consens amb l'estat actual de les transaccions aprovades. D'aquesta forma podem visualitzar el Tangle de IOTA com indica la Figura 3.

Figura 3: Tangle de IOTA

Font: https://iota.readme.io/docs/what-is-iota

On:

- Els quadres grisos representen els *tips*, transaccions referenciades però no aprovades.
- Els quadres blancs representen els *sites*, transaccions referenciades i aprovades.

Alguns dels principals avantatges que té aquest projecte són els següents:

- L'alt rendiment de transaccions de IOTA, gràcies a la validació paral·lela de les transaccions, a més de que es poden confirmar sense límit en un interval determinat
- No té taxes per transaccions
- No té miners, cada participant col·labora activament en el consens
- Usa funcions de *hash* que són immunes a les futures màquines quàntiques

Posteriorment es farà una introducció al funcionament de IOTA basant-nos en el seu *whitepaper* [11] i en una guia d'introducció per a desenvolupadors [12].

1.2.4 Funcionament bàsic de IOTA

Com en el cas de Bitcoin, tot comença quan es vol fer una transacció. Primer de tot cal que el node que envia creï un *bundle*, que representa una estructura de dades on es poden incloure diverses transaccions d'entrada i diverses de sortida, és a dir, varies transaccions dels comptes d'origen i destí. Una vegada creat el *bundle*, comença el procés de selecció de dues transaccions encara no aprovades en el Tangle de IOTA, conegudes com *tips* (aquest procés de selecció s'ha de fer per cada transacció inclosa). En aquest procés es podria seleccionar només un *tip* a aprovar, però llavors la probabilitat de que la transacció inclosa en el *bundle* s'aprovi disminueix, ja que el que es vol és contribuir a fer més estable i segur el Tangle, per tant, quantes més transaccions no aprovades es seleccionen, més dret té un usuari d'incloure les seves.

Encara que s'hagi contemplat aquesta possibilitat, normalment els nodes seleccionen dues transaccions, pel motiu que s'ha esmentat anteriorment. El procés de selecció dels *tips* es diu *tip* Selection i l'algorisme de selecció de les transaccions enviades pel node (les que estan incloses en el *bundle*) es diu Monte Carlo Markov *chain* Algorithm (MCMC). Per tal de verificar les transaccions escollides pel MCMC, cada transacció ha de comprovar les transaccions directament o indirectament referenciades per aquesta (*tips* i *sites*), a partir del procés de validació. Si una transacció es afegida sense verificar les transaccions referenciades, cap altre transacció posterior referenciarà a aquesta en el cas de que sigui invàlida, ja que el procés de validació no s'ha portat a terme i per tant hi pot haver aquesta possibilitat. Per tal de referenciar correctament als *tips*, el node ha de fer un PoW d'una dificultat menor a la de Bitcoin i que serveix majoritariament per evitar el spam més que per la seguretat del Tangle. Després de fer-lo la transacció ja pot ser enviada a tots els nodes veïns per tal d'arribar a un consens de que la transacció és vàlida.

En comparació amb la *Blockchain* de Bitcoin, en el Tangle, els nodes no paguen taxes per realitzar transaccions. Una de les característiques principals en el funcionament de IOTA, és que un node ha de participar en la propagació de les transaccions, ja que d'una altra forma, els seus veïns es donarien compte ràpidament que el node en sí no vol col·laborar amb la resta de nodes a fer que es segueixin els mètodes creats per un bon funcionament del Tangle. D'aquesta forma el tractaran com un node lazy, que més tard serà esborrat de la llista dels veïns i abandonat, fent que no pugui tornar a enviar transaccions.

A continuació definirem què són és un *snapshot* de IOTA i com afecta al rendiment de la *Blockchain*, ja que

serà imprescindible entendre-ho per quan haguem de modificar el projecte al nostre context.

1.2.5 *snapshot* de IOTA

Un *snapshot* [22] és un mètode que utilitza IOTA per tal de reduir la mida de la base de dades del Tangle, eliminant totes les transaccions i deixant únicament els registres de les adreces dels usuaris amb els seus corresponents saldos, on les adreces sense cap saldo també seran eliminades. Aquelles adreces que queden seran utilitzades com adreces del gènesis, és a dir, com a adreces confiables. Una vegada el *snapshot* s'ha fet, és possible que s'hagin de demanar els *tokens* del Tangle antic (abans del *snapshot*) per transmetre'ls al nou, diem que és possible, perquè aquest mecanisme manual només es necessita quan hi ha grans canvis en el disseny del protocol de IOTA. Tot el que hem explicat es fa de forma manual i concretant un data en concret, però es preveu que en el futur es faci automàticament.

Ara que ja tenim una base teòrica suficient dels elements que ens basarem per fer el projecte, és el moment per definir quin serà l'abast d'aquest, on inclourem també els requeriments per realitzar-lo i les solucions a possibles obstacles.

2. Abast del projecte

2.1 Objectius

El projecte que es pretén desenvolupar es basarà en l'assignació d'IPs i la seguretat. Per fer-ho, utilitzarem l'algorisme de consens PoW, i no el que es presenta com a opció principal en el document, el *Proof of Stake*, ja que PoW és amb el que treballa IOTA, un sistema diferent a la *Blockchain*, i que per tant, té uns altres mecanismes de protecció.

Els objectius d'aquest projecte són diversos. Primer de tot es tracta d'entendre bé la *Blockchain*, en el seu projecte inicial, és a dir, Bitcoin. El següent punt serà entendre quins són els mecanismes usats en la xarxa per aconseguir una seguretat òptima en les transferències de *tokens* abans de entrar en l'estudi de IOTA.

Un cop havent acabat l'etapa anterior, el següent objectiu és l'estudi de les estructures i funcionalitats dins de la *Blockchain* de IOTA per fer les assignacions IP al Tangle, veient com canvien les estructures internes i els mecanismes per realitzar les transaccions. Gràcies a això podrem començar a definir les dades que volem incloure en la nostre adaptació i la dificultat de fer-ho.

Després arribarà l'objectiu principal del projecte, el de fer una modificació al projecte existent de IOTA, per tal de definir un seguit de proves que s'usaran per garantir la correctesa de les funcionalitats que hem de provar i per avaluar el sistema fent un anàlisi del seu funcionament i posteriorment una comparació amb les eines actuals que desenvolupen la mateixa tasca. D'aquesta forma podrem concloure si aquest sistema podria ser prou òptim per ser estudiat i desenvolupat, o si bé aquesta adaptació no ens aporta cap avanç en el direccionament IP des del punt de vista de la funcionalitat i seguretat.

Finalment, com a subobjectiu, es comprovarà si el PoW de IOTA ofereix una millor protecció i funcionament que l'algorisme de consens PoS del qual s'ha fet l'anàlisi i proposta en el document d'investigació previ.

A continuació donarem pas als requeriments necessaris per la realització del projecte.

2.2 Requeriments

Aquest projecte està fitat per tenir una càrrega de treball per desenvolupar-se amb quatre mesos de dedicació, començant el dia 30/01/2018 i acabant el dia 28/05/2018, per tant, aquest és el marge de temps que disposem per fer-ho. Per una altra banda necessitarem un pressupost per poder disposar del personal necessari per realitzar el projecte, en aquest cas, un enginyer del software, dos enginyers de xarxes i un product manager que vetllarà per la correctesa de la documentació del projecte fins que finalitzi la primera etapa del TFG. Els costos associats a aquest personal estaran inclosos en la secció de costos del projecte, juntament amb les hores dedicades a cada tasca. Per últim, cal dir que aquest treball tindrà una bona qualitat, ja que s'està desenvolupant rigorosament a partir de documentació d'investigació com també de les principals fonts d'informació de les tecnologies implicades, entenent-les i aplicant aquests coneixements en els objectius plantejats, per tal d'aconseguir els millors resultats possibles.

Ara que sabem de què hem de disposar per començar el projecte, és un bon moment per presentar els possibles obstacles i solucions que ens podem trobar en el transcurs del desenvolupament del treball.

2.3 Possibles obstacles i solucions

Durant el projecte poden sortir certes dificultats que afectin al seu desenvolupament i modifiquin la seva planificació. A continuació es defineixen els possibles problemes que s'han identificat:

Manca d'informació del sistema IOTA

Es pot necessitar informació d'alguna de les funcionalitats implementades per a una millor comprensió, però com aquest projecte és relativament nou, pot ser difícil de trobar informació específica.

Primera alternativa:

- Fer una recerca exhaustiva d'informació, tant en fòrums de desenvolupadors com en articles fets per usuaris explicant parts del sistema.

Segona alternativa:

- Contactar amb els desenvolupadors i que ens puguin facilitar la comprensió d'alguna característica del programa en la que hi hagi dubtes.

Errors en la implementació del software

En l'etapa on s'ha d'adaptar el context del nostre projecte a la *Blockchain* de IOTA poden sorgir errors inesperats degut a algun comportament del programa del que partim (GUI de IOTA), no previst anteriorment.

Primera alternativa:

- Fer una recerca exhaustiva d'informació, tant en fòrums de desenvolupadors com en articles fets per usuaris explicant parts del sistema.

Segona alternativa:

- Pot ser que no es pugui solucionar amb els coneixements que s'obtenen de l'estudi de la *Blockchain* IOTA, no es pugui contactar amb un expert o la recerca d'informació no ajudi. La solució serà no fer la implementació del software i incloure un anàlisi teòric complet del seu funcionament en el cas que estigués implementat correctament el sistema, i basant-nos en això, raonar si realment és una opció viable al programari tradicional d'assignació d'IPs des d'una perspectiva de funcionalitat i protecció a atacs.

Tenint les solucions als possibles problemes que ens podem trobar al llarg del desenvolupament del projecte, introduirem els següents tres apartats, que es basaran en els mètode de treball per realitzar el projecte, les eines que s'utilitzaran per guiar-nos en el seu desenvolupament i com es validarà cada fase.

2.4 Mètode de treball

La feina realitzada es farà seguint la planificació definida en el diagrama de Gantt, on a més d'haver-hi les tasques a realitzar, també estaran inclosos els diversos lliurables. En cada etapa del treball el director i subdirector faran de guies del següent pas a realitzar, és a dir, guiaran el projecte a la següent etapa quan l'anterior hagi assolit l'objectiu que es pretén.

Com la major part del treball es basa en buscar i raonar sobre la documentació del sistema IOTA, serà primordial fer recerca en papers i webs de desenvolupadors per tal de trobar una informació fiable. En el cas de que no sigui suficient o que no s'ajusti del tot a les necessitats dels nostres objectius, es realitzaran cerques tant a fòrums com a webs no oficials però fiables per tal de garantir l'assoliment de totes les feines previstes a temps.

Pel que fa el desenvolupament del codi s'aplicarà un desenvolupament guiat per proves (TDD) sempre que es vegi factible, ja que seran després les usades per garantir que el que volem provar s'està realitzant satisfactòriament i fer posteriorment l'anàlisi funcional i comparatiu.

Per últim, el feedback que aportarà tant els directors del projecte com el tutor de GEP serviran per corregir i/o adequar algunes tasques per millorar-les, així després de fer-ho, es podrà seguir fent la següent tasca

sabent que tota la feina realitzada anteriorment és correcta, aportant seguretat i confiança en la feina ja feta.

2.5 Eines de seguiment

Quan es generi codi, es gestionarà a través de Github, per poder tenir un control de versions i canvis en el desenvolupament del mateix, on es podran incloure també les proves realitzades i els resultats obtinguts. Per una altra banda es tindrà el director i subdirector del projecte per tal d'aconseguir un rendiment idoni i per fer propostes de la feina a fer.

Tant el progrés del document com el del codi es seguirà amb un diagrama de Gantt per veure el progrés segons la planificació inicial, i per especificar la feina a fer durant tota l'etapa de duració del treball per tal d'arribar correctament als terminis d'entrega sense imprevistos, ja que en aquest diagrama hi haurà el temps necessari per fer els diversos lliurables del treball que estan inclosos a l'Atenea fins el dia del torn de lectura del projecte.

2.6 Validació

Es tindran reunions setmanals amb el cap de projecte per resoldre qualsevol dubte i/o enfocar el treball en una direcció concreta a mesura que s'avança el seu desenvolupament. Una altra forma de validació serà amb l'ajuda del tutor de GEP, el qual ajudarà a fer i estructurar el document de la millor forma possible a partir d'un feedback, que posteriorment serà utilitzat per reescriure o incloure nova informació requerida en el treball.

Ara que ja tenim el mètode de treball que se seguirà, és un bon moment per passar a la planificació del projecte, que tractarà les taques i els recursos necessaris per tal d'arribar satisfactòriament a la data d'entrega del treball.

3. Planificació temporal

L'objectiu d'aquest apartat és el d'encaminar el projecte i fixar les diferents dades i fases per les que passarà, començant el dia 30/01/2018 i acabant el dia 28/05/2018 (4 mesos), sent aquest el dia de la lectura del TFG. Tant els lliurables com la documentació del projecte, a més de les reunions setmanals, es requeriran 396 hores (17 dies), amb una mitjana de 4.5 hores diàries.

Aquest és un projecte d'investigació, però bastant fitat en el context que es tracta. El cap de projecte anirà revisant les diverses fites d'aquest, però s'hi aniran afegint de noves amb cada coneixement après, sempre partint d'un estudi realitzat anteriorment com a base. Per tant, la metodologia més adequada per treballar seria una que sigui interactiva i incremental. El principal motiu per realitzar aquest treball amb aquesta metodologia és que s'haurà d'anar iterant amb cada coneixement nou, adaptant-lo al motiu principal del projecte i als coneixements que es vagin adquirint en cada pas de la investigació.

En el projecte, cadascuna de les iteracions començaran en cada nova reunió amb el cap de projecte. Després de fer un repàs de les tasques a realitzar es prendrà en consideració les dificultats i mètodes alternatius per a realitzar la propera iteració. Cada reunió encaminarà més el projecte cap al seu propòsit, partint d'una idea bàsica a una de més específica i detallada, afegint en cada pas una millora, en aquesta cas, un plantejament i raonament millors del sistema a desenvolupar en contrast amb el que teníem prèviament.

A continuació es llistaran la sèrie d'elements que s'utilitzaran per realitzar el TFG.

3.1 Recursos utilitzats per la realització del projecte

Per dur a terme el projecte s'utilitzarà un ordinador de sobretaula amb connectivitat a internet. S'utilitzarà Google Chrome com a navegador i Google Drive per incloure les idees destacades en el transcurs de l'aprenentatge, la posterior elaboració dels lliurables i document final del projecte.

Per una altra banda també s'utilitzarà un telèfon mòbil per realitzar el vídeo de la presentació preliminar, el Dropbox per compartir el vídeo, Eclipse per desenvolupar el codi, la API de IOTA, Atenea i El Racó de la FIB per fer el lliurable del document final. Per la realització de les taques d'aquest treball, caldrà a més a més la col·laboració del cap de projecte i el subdirector, per tal de fer de guies tasca rere tasca en les diverses reunions presencials.

En la següent secció es farà un recull de les tasques que constarà el projecte i dels objectius que es volen aconseguir.

3.2 Tasques a realitzar

3.2.1 Familiarització amb la *Blockchain*

- **Informació sobre la *Blockchain***: El primer pas en aquest projecte és aprofundir en l'estudi de la *Blockchain* des de la seva base. L'objectiu és conèixer el per què es va crear, i a partir d'aquí fer un estudi més exhaustiu del que permet fer, és a dir, quines funcionalitats aporta aquesta nova tecnologia i quins problemes té tant en el present com en el futur, per si podria ser o no una millora de les tecnologies convencionals en quasi tots els àmbits.

- **Informació sobre conceptes en la seguretat d'Internet**: Després d'haver aprofundit en l'estudi de la *Blockchain* s'hauran d'aprendre conceptes nous en la seguretat a internet, d'entre ells com a més importants: la criptografia de clau pública i privada, funcions de *hash*, certificats digitals i funcions criptogràfiques.

- **Cerca d'informació sobre Bitcoin (introducció)**: A partir de la base apresa en els conceptes

d'Internet ens centrarem en conèixer com funciona el primer projecte dedicat a la tecnologia *Blockchain*, Bitcoin, en les seves estructures internes, processos i seguretat, per tal de tenir un coneixement més extens i poder raonar més endavant una elecció de sistema per tal d'adaptar el projecte.

Recursos utilitzats:

- **Recursos humans**: cap de projecte i subdirector per guiar en l'aprenentatge i resoldre dubtes sobre la *Blockchain* i Bitcoin.
- **Recursos hardware**: ordinador de sobretaula.
- **Software**: Google Chrome per buscar la informació i Google Drive per documentar.

3.2.2 Contacte amb la proposta del projecte, recerca i anàlisis de candidats

- **Anàlisi de la proposta del document informatiu**: Tenint una base sòlida ja adquirida de com funciona una *Blockchain*, en aquest cas Bitcoin, el següent pas serà entendre què és el que proposa fer el cap de projecte. Per fer-ho, caldrà analitzar cada punt del document informatiu An analysis of the applicability of *Blockchain* to secure IP addresses allocation, delegation and bindings inclòs en la bibliografia, on es presenta una proposta de com es podria realitzar l'assignació d'IPs usant *Blockchain*.

- **Cerca de projectes comparables amb IOTA**: Juntament amb la tasca anterior, i el coneixement de la *Blockchain* Bitcoin, es buscaran projectes que puguin ser comparables amb les funcionalitats de IOTA, i si algun d'ells està prou documentat i desenvolupat per tal de ser utilitzat com a plataforma per desenvolupar el projecte, descartant en aquest cas IOTA.

- **Recopilació d'informació de la *Blockchain* IOTA**: Després de tenir clara la proposta del document informatiu i havent fet la cerca d'altres projectes comparables amb IOTA, es començarà a recopilar tot tipus d'informació sobre la *Blockchain* de IOTA, començant per el paper de la seva web oficial, per tal d'entendre bé com funciona i quines eines té per protegir-se d'atacs.

- **Definició de l'abast i contextualització**: Després d'entendre mínimament el seu funcionament es podrà procedir a fer el document de la Definició de l'abast i contextualització, englobant alguns dels punts més importants del que s'ha après en les tasques anteriors.

Recursos utilitzats:

- **Recursos humans**: cap de projecte i subdirector per guiar en l'aprenentatge i resoldre dubtes sobre la *Blockchain* i Bitcoin.
- **Recursos hardware**: ordinador de sobretaula.

- **Software**: Google Chrome per buscar la informació i Google Drive per documentar.

3.2.3 Investigació a fons de la *Blockchain* IOTA i comparació amb altres *chains*

- **Anàlisi de IOTA**: Després d'haver fet una introducció a la *Blockchain* de IOTA, es farà un anàlisi més a fons, començant per la generació d'adreces, fins arribar a entendre les seves estructures internes i processos que utilitza per tal d'emmagatzemar i transmetre la informació entre les diverses entitats. També s'analitzaran els possibles atacs, i com fer-los front recolzant-nos amb tot el que hem après anteriorment, fent en aquest punt un estudi més exhaustiu.

- **Documentació de la planificació temporal**: Després de tenir clar com funciona el sistema sobre el qual construirem el nostre projecte i havent fet la documentació de l'abast i contextualització serà un bon moment per fer la planificació temporal, així tindrem una organització i temps a dedicar en cada tasca per tal de portar el projecte al dia fins la seva finalització.

- **Anàlisi de l'algorisme de consens de IOTA en comparació amb altres *chains***: Sabent d'una forma bàsica com funciona IOTA i havent fet un anàlisi, es buscaran altres projectes de la *Blockchain* que utilitzen el mateix algoritme de consens *Proof of Work* (PoW) i d'altres que usin *Proof of Stake* (PoS) per comparar la decisió que prenen cadascun d'ells a l'hora d'aprovar una transacció, veient en aquest cas quin seria millor en aquest punt o quines conclusions hi podem extreure.

- **Documentació de la gestió econòmica i sostenibilitat del projecte**: Després d'haver realitzat la documentació de la planificació temporal es començarà a fer el de la gestió econòmica i sostenibilitat del projecte.

Recursos utilitzats:

- **Recursos humans**: cap de projecte i subdirector per guiar en l'aprenentatge i resoldre dubtes sobre la *Blockchain* IOTA.
- **Recursos hardware**: ordinador de sobretaula.
- **Software**: Google Chrome per buscar la informació i Google Drive per documentar.

3.2.4 Preparació de la presentació, documentació i revisió del projecte de la fase GEP

- **Preparació de la presentació preliminar**: Ara que ja tenim els tres documents principals, es prepararà un guió i s'utilitzarà el mòbil per gravar la presentació de com a màxim 4 minuts. Després es crearà un document amb l'enllaç del vídeo al Dropbox.

- **Preparació de la documentació final de la fase GEP**: Just després d'haver preparat la presentació preliminar es revisarà el feedback dels tres entregues lliurades i es farà tot el possible per corregir les mancances i/o errors en aquests, formant així un document que els inclogui ja revisats i modificats.

- **Elaboració del plec de condicions**: juntament amb la preparació de la documentació final es començarà a elaborar el plec de condicions, on es pretén descriure el projecte, les competències tècniques escollides, i la justificació de si s'adeqüen a l'especialitat triada.

- **Preparació del** PowerPoint **de la presentació oral:** es realitzarà un PowerPoint de la presentació oral de 5 minuts de durada, on s'exposarà el treball realitzant durant les quatre setmanes del curs, servint com a document de partida per la defensa final del TFG. Aquesta tasca s'elaborarà conjuntament amb la preparació del document final i el plec de condicions.

Recursos utilitzats:

- **Recursos humans**: cap de projecte i subdirector per guiar en l'aprenentatge i resoldre dubtes sobre la *Blockchain* IOTA.
- **Recursos hardware**: ordinador de sobretaula i el mòbil.
- **Software**: Google Chrome per buscar la informació i Google Drive per documentar.

3.2.5 Adaptació del projecte IOTA al nostre context i finalització del projecte

- **Definició de les dades per adaptar el nostre projecte a IOTA i anàlisi**: Ara que ja tenim clar com funciona l'algorisme de consens de IOTA i hem fet la comparació amb altres *chains*, serà el moment de definir les dades per fer l'adaptació del nostre projecte a la *Blockchain* de IOTA, juntament amb un anàlisi per veure els canvis que es produeixen en l'estructura original.

- **Elaboració del software i proves**: Tenint clar les dades que hem de representar i els canvis que succeeixen en l'estructura original, es procedirà a realitzar el software juntament amb les proves per veure el funcionament.

- **Comparativa entre IOTA i els sistemes tradicionals**: Després d'haver realitzat el software, les proves i entenent la seguretat que ens proporciona IOTA, és un bon moment per fer una comparació amb les eines tradicionals que realitzen la mateixa tasca.

- **Anàlisi de les conclusions preses**: A partir de la comparativa amb els sistemes tradicionals es realitzarà un anàlisi de les conclusions preses en l'adaptació del context del projecte en la *Blockchain* de IOTA, amb l'objectiu d'exposar si adaptar aquest projecte o un de semblant a IOTA seria viable, si seria pitjor, o si caldrien més dades per tal de fer un anàlisi més exhaustiu.

- **Revisió del document final i preparació de la lectura de la fase final del TFG**: Juntament amb l'anàlisi de les conclusions es prepararà la documentació final i el torn de lectura amb tota la informació rellevant trobada durant el transcurs del projecte i l'extreta del mateix projecte.

Recursos utilitzats:

- **Recursos humans**: cap de projecte i subdirector per guiar en l'aprenentatge i resoldre dubtes sobre la *Blockchain* de IOTA.

- **Recursos hardware**: ordinador de sobretaula.

- **Software**: Google Chrome per buscar la informació, Google Drive per documentar, Dropbox per penjar el vídeo i Eclipse juntament amb l'API de IOTA per desenvolupar l'aplicació.

Seguidament farem un resum de les seccions que engloben les tasques, indicant les precedències entre elles i el temps dedicat a cadascuna. Per fer-ho, introduirem una taula (*taula 1*) en la següent secció.

3.3 Estimació de temps i seqüència de tasques

3.3.1 Temps estimat per tasca i precedències

Codi	Tasca	Hores	Dependències
R1	Reunió 1	1	-
T1	Informació sobre la *Blockchain*	12	-
T2	Informació sobre conceptes en la seguretat d'Internet	4	T1
R2	Reunió 2	1	-
T3	Cerca d'informació sobre Bitcoin (introducció)	24	T2
T4	Anàlisi de la proposta del document informatiu	8	T3
T5	Cerca de projectes comparables amb IOTA	8	T3
T6	Recopilació d'informació de la *Blockchain* IOTA	30	T4, T5
R3	Reunió 3	1	-
R4	Reunió 4	1	-
T7	Documentació de la definició de l'abast i contextualització	8	-

R5	Reunió 5	1	-
T8	Anàlisi de IOTA	45	T6
R6	Reunió 6	1	-
T9	Documentació de la planificació temporal	8	T7
T10	Anàlisi de l'algorisme de consens de IOTA en comparació amb altres *chains*	20	T8
R7	Reunió 7	1	-
T11	Documentació de la gestió econòmica i sostenibilitat del projecte	12	T9
R8	Reunió 8	1	-
T12	Preparació de la presentació preliminar	5	T11
T13	Preparació de la documentació final de la fase GEP	30	T12
T14	Elaboració del plec de condicions	8	T12
R9	Reunió 9	1	-
T15	Preparació del PowerPoint de la presentació oral	6	T12
T16	Definició de les dades per adaptar el nostre projecte a IOTA i anàlisi	25	T10
R10	Reunió 10	1	-
T17	Elaboració del software i proves	100	T16
R11	Reunió 11	1	-
R12	Reunió 12	1	-
R13	Reunió 13	1	-
R14	Reunió 14	1	-
R15	Reunió 15	1	-
T18	Comparativa entre IOTA i els sistemes tradicionals	10	T17
T19	Anàlisi de les conclusions preses	6	T18
T20	Revisió del document final i preparació de la lectura de la fase final del TFG	12	T18

Taula 1: hores estimades i precedències entre tasques

Seguidament, es mostraran les diverses tasques de les seccions definides anteriorment usant el diagrama de Gantt (Figura 4).

3.3.2 Diagrama de Gantt

Figura 4: diagrama de Gantt generat amb TeamGantt.

En la següent secció tractarem de com fer front als principals problemes que ens podem trobar a l'hora de fer el projecte i quins plans alternatius ens poden ajudar per tal de poder-lo finalitzar a la data prevista.

3.4 Possibles complicacions i alternatives

3.4.1 Manca d'informació del sistema IOTA

Es pot necessitar informació d'alguna de les funcionalitats implementades per a una millor comprensió, però com que aquest projecte és relativament nou, pot ser difícil de trobar informació específica.

Primera alternativa (Temps requerit de 10 hores):

- Fer una recerca exhaustiva d'informació, tant en fòrums de desenvolupadors com en articles fets per usuaris explicant parts del sistema.

Segona alternativa (Temps requerit de 4 hores):

- Contactar amb els desenvolupadors i que ens puguin facilitar la comprensió d'alguna característica del programa en la que hi hagi dubtes.

3.4.2 Errors en la implementació del software

En l'etapa on s'ha d'adaptar el context del nostre projecte a la *Blockchain* de IOTA poden sorgir errors inesperats degut a algun comportament del programa del que partim (GUI de IOTA) no previst anteriorment.

Primera alternativa (Temps requerit de 10 hores):

- Fer una recerca exhaustiva d'informació, tant en fòrums de desenvolupadors com en articles fets per usuaris explicant parts del sistema.

Segona alternativa (Temps requerit de 20 hores):

- La sobreestimació d'hores en l'última etapa és degut a aquest problema, ja que pot passar que no es pugui solucionar amb els coneixements que s'obtenen de l'estudi de la *Blockchain* IOTA, no es pugui contactar amb un expert o la recerca d'informació no ajudi. La solució serà no fer la implementació del software i incloure un anàlisi teòric complet del seu funcionament en el cas que estigués implementat correctament el sistema, i basant-nos en això, raonar si realment és una opció viable al programari tradicional d'assignació d'IPs des de una perspectiva de funcionalitat i protecció a atacs.

Tenint les possibles solucions a imprevistos, passarem a la següent secció, on es tractaran les dificultats i el termini per realitzar el projecte.

3.5 Finalització del projecte

Comprovant el diagrama de Gantt (figura 4) podem veure que el termini per acabar el projecte és suficient, ja que a hores d'ara, la major dificultat es troba en com aplicar algunes de les definicions del protocol IP a la *Blockchain* i construir el petit software amb la tecnologia de IOTA. Tenint en compte el marge temporal que hi ha des de la reunió 10 no es preveu que hi hagi cap problema per tal de presentar el projecte a la data acordada, ja que hi ha prou temps per poder solucionar qualsevol imprevist amb les alternatives proposades.

Havent fet la planificació, és un bon moment per començar a fer el càlcul de costos associats de totes les parts que formen el projecte i de possibles imprevistos. Dit això, passem a la següent secció.

4. Gestió econòmica

Aquesta secció es basa en calcular els costos de recursos humans, software, hardware i de possibles desviacions que puguin fer augmentar el cost total de desenvolupar el projecte.

Per facilitar el càlcul del cost dels conjunt de tasques, s'han definit les dos seccions següents:

4.1 Càlcul dels costos directes

A continuació es calcularan els costos relacionats amb les activitats de desenvolupament del projecte.

Primer de tot definirem els rols de les persones involucrades:

- Enginyer de software (junior) : aquest rol correspon a l'estudiant, ja que la seva feina serà la de desenvolupar i avaluar un nou sistema, el salari és de: 6.21€/h [13]. Aplicant els impostos d'un 23.6% en Seguretat Social: 4.75€/h.

- Enginyer de xarxes (sènior) : correspondrà al director i subdirector del projecte, els quals facilitaran a l'estudiant la coneixença d'aquest camp d'investigació, els seus salaris seran de: 15.96€/h [14]. Aplicant els impostos d'un 23.6% en Seguretat Social: 12.19€/h.

- Project Manager (sènior): correspondrà al tutor de GEP, que vetllarà per la correctesa de la documentació del projecte fins que finalitzi la primera fase del TFG. El seu salari és de: 16.96€/h [15]. Aplicant els impostos d'un 23.6% en Seguretat Social: 12.96€/h.

Els salaris associats a les tres titulacions anteriorment esmentades han estat extrets de la web salary.com adjuntada a la bibliografia.

4.2 Càlcul dels costos indirectes.

Seguidament es calcularan els costos que afecten al procés de desenvolupament.

Definim l'amortització dels aparells electrònics (ordinador i mòbil) utilitzant la següent fórmula:

$$Amortització = PD * \frac{DDP}{365 * \text{VU}}$$

On la definició de les variables és:

PD = preu del dispositiu.

DDP = dies d'ús durant 4 mesos de duració del projecte (laborals i no laborals).

VU = vida útil (en dies).

Per realitzar el càlcul anterior suposarem que l'ordinador té una vida útil de 5 anys, i el mòbil, una vida de 4 anys. Els dispositius esmentats s'utilitzen diàriament durant tot l'any.

Altres costos indirectes són els de l'electricitat i del internet.

El preu aproximat per KwH a Espanya és de: 0.12 €.

Els watts consumits per l'ordinador són: 200 W.

Les hores totals d'ús de l'ordinador són: 376 hores.

Per tant, el total de cost elèctric serà de:

$$0.2\,Kw * \frac{0.12€}{KwH} * 376h = 9.03€$$

El preu d'internet és de: 40 €/mes. Calcularem el cost basant-nos en les hores consumides per fer el projecte:

$$\frac{40€/mes}{30\,dies/mes} * \frac{376h\ de\ consum}{24\frac{hores}{dia}} = 20.89€$$

4.3 Costos del projecte

Ara que ja tenim els procediments per a calcular tant els costos directes com indirectes, es procedirà a realitzar els costos del projecte (Taula 1). En els costos directes consten les reunions amb el director i subdirector i les tasques que realitzarà l'estudiant. Per l'altra banda, en els costos indirectes es llisten els factors que es requeriran per realitzar el desenvolupament del projecte.

Costos directes				
Codi	**Tasca**	**Hores**	**Salari (€/hora)**	**Import total(€)**
R1	Reunió 1	1	29.13 (4.75 + 12.19 * 2)	29.13
T1	Informació sobre la *Blockchain*	12	4.75	57
T2	Informació sobre conceptes en la seguretat d'Internet	4	4.75	19
R2	Reunió 2	1	29.13	29.13
T3	Cerca d'informació sobre Bitcoin (introducció)	24	4.75	114
T4	Anàlisi de la proposta del document informatiu	8	4.75	38
T5	Cerca de projectes comparables amb IOTA	8	4.75	38
T6	Recopilació d'informació de la *Blockchain* IOTA	30	4.75	142.5
R3	Reunió 3	1	29.13	29.13
R4	Reunió 4	1	29.13	29.13
T7	Documentació de la definició de l'abast i contextualització	8	4.75	38
R5	Reunió 5	1	29.13	29.13
T8	Anàlisi de IOTA	45	4.75	213.75
R6	Reunió 6	1	29.13	29.13
T9	Documentació de la planificació temporal	8	4.75	38
T10	Anàlisi de l'algorisme de consens de IOTA en comparació amb altres *chains*	20	4.75	95
R7	Reunió 7	1	29.13	29.13
T11	Documentació de la gestió econòmica i sostenibilitat del projecte	12	4.75	57
R8	Reunió 8	1	29.13	29.13
T12	Preparació de la presentació preliminar	5	4.75	23.75
T13	Preparació de la documentació final de la fase GEP	30	4.75	142.5
T14	Elaboració del plec de condicions	8	4.75	38
R9	Reunió 9	1	29.13	29.13
T15	Preparació del PowerPoint de la presentació oral	6	4.75	28.5

T16	Definició de les dades per adaptar el nostre projecte a IOTA i anàlisi	25	4.75	118.75
R10	Reunió 10	1	29.13	29.13
T17	Elaboració del software i proves	100	4.75	498.75
R11	Reunió 11	1	29.13	29.13
R12	Reunió 12	1	29.13	29.13
R13	Reunió 13	1	29.13	29.13
R14	Reunió 14	1	29.13	29.13
R15	Reunió 15	1	29.13	29.13
T18	Comparativa entre IOTA i els sistemes tradicionals	10	4.75	47.5
T19	Anàlisi de les conclusions preses	6	4.75	28.5
T20	Revisió del document final i preparació de la lectura de la fase final del TFG	12	4.75	57
Total (costos directes)		**396**	**-**	**2246.7**
Factors		**Hores**	**Preu(€)**	**Import total (€)**
Electricitat (requeriment de 200W)		376 (396 – 15h de reunions – 5h d'ús del mòbil)	0.12 (KwH)	9.03
Internet		376	40 (mensuals)	20.89
Ordinador de sobretaula		376	-	78.90
Mòbil		5	200	16.44
Google Drive		-	0	-
Dropbox		-	0	-
Eclipse		-	0	-
Google Chrome		-	0	-
API de IOTA		-	0	-
Total (costos indirectes)		**381**	**200 (cost del hardware)**	**125.26**
Total (costos directes + indirectes)		2371.96 **€**		

Taula 2: Costos directes i indirectes

Seguidament es calcularà la contingència (Taula 3), que serà d'un 5%, ja que el nivell de planificació del projecte és alt i no es preveu cap desviació significativa.

Cost de contingència			
	Justificació	**Impacte en el cost(%)**	**Cost(€)**

	El nivell de planificació és alt	5	2371.96
Total	-	-	118.60

Taula 3: Cost de contingència

A continuació s'afegiran els costos (Taula 4) per possibles incidències en el projecte:

Costos per possibles incidències					
	Causes	**Solució**	**Risc(%)**	**Impacte en el cost(€)**	**Cost(€)**
	Manca d'informació del sistema IOTA	Cerca exhaustiva (7 hores)	20	33.25	6.65
		Contactar amb els desenvolupadors (4 hores)	10	19	1.9
	Errors en la implementació del software	Cerca exhaustiva (10 hores)	40	47.5	19
		Canviar la implementació del software per un anàlisi teòric complet del funcionament (20 hores)	20	95	19
Total	-	-	-	-	46.55

Taula 4: Costos per possibles incidències

Havent finalitzat amb el càlcul dels diferents costos, el cost total del projecte (Taula 5) serà el següent:

Cost total del projecte		
	Tipus de cost	**Cost(€)**
	Directe i indirecte	2371.96
	Contingències	118.60
	Incidències	46.55
Total	-	2537.11

Taula 5: Cost total del projecte

Després d'haver realitzat el cost del projecte, s'ha d'establir un control de costos, per tal de comparar i avaluar possibles desviacions.

4.4 Control del pressupost

Com s'ha esmentat en l'apartat *3.4 Possibles complicacions i alternatives*, pot haver-hi una desviació en la planificació prevista del projecte que pot ser deguda a una manca d'informació del sistema IOTA que sigui necessària per tal de poder fer un anàlisi, com també errors en la implementació del software.

El principal problema serà l'increment d'hores a treballar per a l'enginyer del software, ja que haurà de contactar amb els desenvolupadors i dedicar diverses hores a fer una cerca intensiva fins a trobar la solució de l'error, per això aquesta possible problemàtica ha estat inclosa en la taula anterior en el càlcul d'incidències.
S'ha estimat que tant per realitzar el prototip com per fer un anàlisi complert, s'utilitzaran el mateix nombre d'hores en el cas de no poder arreglar l'error a l'hora de la implementació. Per tant, la majoria del problemes sorgiran en l'última secció del projecte, quan s'hagi d'adaptar IOTA al context del treball, per això també s'ha reservat més temps, així es podrà actuar sense preses i dins del límit d'entrega.

Per controlar el pressupost, al acabar cada tasca el pressupost serà actualitzat amb les hores efectives de feina, els costos dels recursos utilitzats i costos inesperats. A partir d'aquesta costos, es farà una comparació amb estimacions prèvies per tal d'obtenir indicadors que mostrin la quantitat de la desviació en comparació amb el pressupost inicial planificat. Per tal de portar aquest control s'utilitzaran les següents fórmules:

$$Cost\ de\ desviació = (CE - CR) * HR$$
$$Desviació\ en\ el\ consum = (HE - HR) * CE$$

On les variables definides són:

CE = cost estimat.
CR = cost real.
HR = hores reals.
HE = hores estimades.

El pressupost s'actualitzarà després d'acabar cada tasca, això ajudarà a determinar on ha ocorregut la desviació, ja que les hores i el cost dels recursos de cadascuna d'elles està definit. Com s'ha esmentat anteriorment, s'ha inclòs la possibilitat de que hi hagi una desviació (Taula 2 i Taula 3), així que el pressupost del projecte deixa un petit marge per possibles incidències.

Ara que ja tenim els costos, passarem a realitzar la secció de sostenibilitat del projecte, començant pel

domini en aquesta temàtica i acabant en un anàlisi de les variables de sostenibilitat del treball.

5. Sostenibilitat

5.1 Domini de la temàtica de sostenibilitat

Tenint l'apartat de costos definit, es procediran a tractar els aspectes sostenibles del projecte.

L'objectiu d'aquest punt és la d'obtenir informació sobre els nostres coneixements i competències pel que fa la sostenibilitat. Per fer-ho es tractaran les seves tres dimensions: social, mediambiental i econòmica.

Pel que fa a les causes, conseqüències i solucions respecte a la problemàtica social, econòmica i ambiental que esdevé de la sostenibilitat, no és un tema que m'és molt proper, però sé de que es tracta d'una forma bàsica. Al llarg dels anys en la facultat s'ha tractat mínimament aquesta competència i sé analitzar-la d'una forma suficient, ja que sempre s'ha partit d'un problema relacionat amb les TIC i s'ha hagut de preveure les conseqüències, algunes vegades sense solucions ja aplicades a elles, però sí amb problemes ja coneguts. Per una altra banda no tinc coneixença d'algunes de les tècniques usades, com per exemple la tècnica d'innovació, però sóc capaç d'aportar idees en un projecte per tal de fer-lo més sostenible. Tampoc conec els indicadors que s'utilitzen per mesurar l'impacte, però sé valorar i comprenc els costos ambientals al llarg del cicle de vida d'un producte, encara que moltes vegades en la proposta de projectes no tinc en compte tecnologies més sostenibles ni els efectes mediambientals que es poden generar a causa d'aquestes, com tampoc la problemàtica ni les conseqüències directes associades als serveis TIC. El que sí que comprenc, és que hi ha una necessitat d'introduir una justícia social, equitat, diversitat i transparència en els projectes TIC per tal de poder veure si realment contribueixen a millorar el bé comú de la societat, però a l'estar en constant desenvolupament de projectes de caire acadèmic no tinc en compte aquests factors, com tampoc els factors econòmics ni la viabilitat econòmica i comptabilitat amb les dimensions ambientals i socials de la sostenibilitat, com tampoc els principis deontològics. L'anàlisi que realitzo en aquesta temàtica és bastant superficial i després de valorar el coneixement propi, seria d'interès fer un canvi a millor i valorar en futur com es podrien fer projectes tenint més en compte la societat, els costos econòmics, la justícia, la transparència i els afectes ambientals o impactes del projecte a desenvolupar, ja que així respectaria més aquest assumpte i totes les seves implicacions en els futurs projectes en els que hi formi part.

5.2 Anàlisi de les variables de la sostenibilitat

A partir dels coneixements propis esmentats anteriorment, es procedirà a fer un anàlisi de les tres variables definides (Taula 6) en el context del nostre projecte.

	PPP	**Vida útil**	**Riscos**
Ambiental	Consum de disseny	Petjada ecològica	Ambientals
Econòmic	Factura	Pla de viabilitat	Econòmics
Social	Impacte personal	Impacte social	Social

Taula 6: Matriu de sostenibilitat

5.2.1 Variable ambiental

Els recursos que es necessitaran en les diverses fases del projecte seran recursos els quals la majoria ja eren utilitzats prèviament (ordinador, internet, mòbil, Google Drive, Dropbox, Eclipse, Google Chrome), l'únic nou serà la API de IOTA. La majoria d'aquests recursos (menys la API de IOTA i el mòbil), seran utilitzats durant tot el transcurs del projecte. Al primer cop d'ull no sembla que hagin de ser gaire contaminants, és a dir, no sembla que l'impacte ambiental al usar-los pugui ser greu, però si ens fixem en el total de CO2 generat durant el seu desenvolupament, 389 hores, consumint 0,2kW/h aproximadament, generem 61g de CO2 per hora, és a dir, un total de 23729g (quasi bé 24Kg de CO2 si comptem el mòbil i internet). Encara que no s'estigués realitzant aquest TFG, el consum i impacte ambiental seguiria produint-se, degut a que diàriament es fa un ús de quasi tots aquests recursos. Com aquest projecte no és resolt encara per cap altre, podrà millorar els posteriors, ja que tot el treball realitzat en aquest podrà ser un punt de partida per molts d'altres, disminuint la petjada ecològica, almenys, en una petita part, ja que no es requeriran d'alguns recursos ja utilitzats.

5.2.2 Variable econòmica

En aquest projecte existeix una avaluació de costos, tant de recursos materials com humans, on el cost final està ajustat al previst, ja que s'han tingut en compte únicament les hores requerides per desenvolupar-lo. El resultat serà un projecte viable en el cas que hagués de competir amb altres, ja que al ser únic en la temàtica que tracta i el cost que té, el fa ser un projecte amb un gran potencial. Per una altra banda, si estigués fet pel personal més qualificat i entès en aquesta tecnologia es podria reduir molt el temps per realitzar-lo, i per tant es requeririen de menys recursos, equilibrant o disminuint el seu cost. Al no haver-hi un producte completament funcional, sinó, un producte per experimentar, no s'han tingut en compte costos destinats a ajustos, actualitzacions i reparacions. Finalment, podrien produir-se escenaris que perjudicarien la viabilitat del projecte, en aquest cas seria l'anàlisi de comparació amb tecnologies ja existents que desenvolupen la mateixa feina, ja que el projecte podria ser descartat si és una pitjor solució que la que ja hi ha actualment.

5.2.3 Variable social

La situació política i social del país és bastant favorable en general, però no especialment pel que fa al sector del projecte, ja que al no haver-hi quasi gens de suport és difícil de poder-se fer notar en relació amb la competència tradicional ja establerta des de fa anys i el mateix passa en investigacions de la temàtica de xarxes. Des del nostre punt de vista, l'activitat que estem realitzant podria fer que millorés la situació actual, ja que hi ha una gran desconeixença sobre aquesta nova tecnologia, i de com pot aplicar-se per un bé comú en la societat, ja que al cap i a la fi, millora la qualitat de vida de les persones, ja que aquestes tenen més control de les seves pròpies accions.

Aquest treball es presenta com una oportunitat per canviar la forma en la que les persones poden gestionar les seves direccions de xarxa, sense la necessitat de creure o delegar aquesta feina a tercers. El prototip o experiment que es té en ment, és només una comprovació de si realment és prou potent per fer un canvi substancial en la societat.

Les companyies haurien d'adaptar-se o avançar els seus productes d'una forma que superessin aquesta proposta, però com ja s'ha dit anteriorment, aquest projecte és més aviat un model per completar, una

proposta per algú que pugui fer-la realitat. Així que de moment no es preveu que ningú surti perjudicat, encara que hipotèticament, si en un futur aquest TFG fos adoptat per una empresa amb potencial, i el desenvolupa de manera que arriba a ser una solució millor que l'existent, els col·lectius que es veurien perjudicats serien les empreses que treballen amb tecnologies tradicionals semblants.

A partir d'aquí és on començarem a desenvolupar el projecte basant-nos com hem dit amb la *Blockchain* de IOTA.

6. Problemàtica en la implementació del software i canvi en la planificació

D'acord amb la planificació del projecte, poden sorgir diverses complicacions en alguna etapa planificada. Això és el que ha passat en la part de la definició de les dades per adaptar el nostre projecte a IOTA degut a diversos factors que definirem a continuació.
Cal dir que aquest és un projecte relativament nou i la falta de documentació que hi ha en aquesta nova tecnologia és molt present, no només en la *Blockchain* IOTA, sinó en la majoria dels projectes enfocats a la *Blockchain*, fet que fa que qualsevol persona que vulgui iniciar-se en aquest món necessiti una corba d'aprenentatge molt més extensa que, per exemple si ho comparem en tecnologies més establertes en el desenvolupament de software.
Des de la nostra experiència trobem poca ajuda o informació relativa a una base d'on partir per començar a definir el nostre projecte, ja que IOTA no és un producte finalitzat i el que s'espera és un contribució per part del usuaris més que de l'empresa cap als desenvolupadors i investigadors, ja que no hi ha un interès molt generalitzat ni una retribució per la feina feta per part de l'empresa.

Partint d'aquesta base hem esbrinat com es fan les diferents funcionalitats de IOTA a partir del codi públic de la *chain*, el IOTA *reference implementation* (IRI) [17] i l'API de IOTA [18] que es pot trobar a GitHub per tal de pensar una forma de fer la nostre adaptació. La nostra idea principal ha estat descarregar aquesta API i modificar-la incloent un camp d'adreça per tal de que les transaccions no assignessin una quantitat monetària sinó adreces IP.
Aquest canvi en el codi s'ha desenvolupat amb èxit, però el problema ens l'hem trobat a l'hora de provar-lo. El projecte IOTA, com molts d'altres té una *testnet* privada (IRI privada amb monedes fictícies dedicada al test) per tal de que els desenvolupadors puguin provar atacs o possibles fallades en el sistema, així després poden intentar aportar una solució. El que no sabíem i que ha estat reafirmat per un col·laborador de l'equip de desenvolupadors del projecte ha estat que a l'incloure una nova transacció en el Tangle de IOTA, es realitza una comprovació en els camps no hagin estat modificats i que el conjunt d'atributs tinguin una mida específica en bytes. Per tant, el problema que ens vam trobar és que a l'hora d'incloure una nova transacció, aquesta era rebutjada, fent impossible la comprovació de la nostra implementació.

Degut a això vam discutir de modificar el codi de la IRI, però degut a la seva complexitat, falta de documentació i el temps disponible per realitzar el projecte vam decidir de no fer-ho, però en canvi, fer una proposta i un anàlisi complet del funcionament del sistema amb la nostra adaptació, així es tindria una base de la qual partir si en un futur es volgués modificar una gran part del codi, tant de l'API com el de la IRI privada. Parlem d'aquesta modificació com un apartat complex, ja que s'hauria de modificar fins al nivell de canviar com es fan les operacions en les adreces del usuaris, canviant en gran mesura els mecanismes i modificar el seu codi d'encriptació ja que el mecanismes de transmissió de dades variarien molt.

7. Arquitectura de IOTA

Per explicar la nostra proposta posteriorment hem d'entendre primer el mecanisme utilitzat per dur a terme una transacció en el Tangle de IOTA.

Així doncs, començarem explicant l'element més impotent del Tangle, la transacció.

7.1 Transaccions

Les transaccions de IOTA [16] estan incloses en un element que es diu *bundle*, una espècie de paquet, que serveix per enviar diverses transaccions juntes, partint d'aquesta base podem entendre una transacció com la mínima unitat transferida.

Index	Purpose	Value
0	Output. Recipient of the transaction	>0 (as defined by user)
1	First bundle entry that spends the entirety of the address input. This bundle entry also contains the first part of the signature (in the example case, it'll be the first half of **Alice's signature**)	<0 (spending of input)
2	Second half of Alice's signature.	0
3	Output. If there is a remainder (Alice didn't spend her entire balance at the respective key index), it will be sent to a remainder address.	>0 (input - output)

Figura 5: Estructura típica del *bundle*

Font: https://iota.readme.io/docs/bundles

Un dels punts clau del *bundle* és que produeix transaccions atòmiques, és a dir, o totes les transaccions incloses dins del mateix són acceptades pel Tangle o cap. Com podem veure en la figura 5 tenim una secció d'input, on és defineix d'on ve la quantitat aportada (en el cas que sigui 0 s'entén que el que es vol transmetre és un missatge i no una quantitat monetària). En les transaccions d'input és on estarà definida la quantitat que s'ha de restar de cada adreça de qui envia fins assolir l'output. En la majoria de casos són dos transaccions, tant en l'output com input, degut a que la signatura criptogràfica que identifica un input d'un usuari és massa gran per cabre en una única transacció. Això es fa actualment per donar una seguretat òptima a l'usuari, ja que com explicarem més endavant al fer una transacció es pot triar el nivell de seguretat que volem que tingui. Seguidament tenim la secció d'output, on podem definir quina és la quantitat que volem enviar i a on s'envia, a més de definir a on s'ha d'enviar la quantitat sobrant de l'input. Per tal de fer més entenedor el que hem explicat anteriorment i adaptar-ho al nostre context, explicarem a continuació cada part amb més detall.

7.1.1 Secció d'output

En aquesta secció hem de definir diverses parts:

- Quantitat a enviar i/o missatge
- Definició del destinatari
- Definició de l'adreça amb la quantitat sobrant

Primer de tot definirem la quantitat de IOTA's a enviar. Després d'enviar la quantitat, el conjunt de transaccions passaran a tenir una signatura que identificarà a la persona que envia i que estarà fragmentada en un camp específic en cadascuna de les transaccions de l'output.

Després tenim la definició del destinatari, on s'inclourà l'adreça o adreces del destinatari, a més d'incloure a on s'enviarà la quantitat sobrant si n'hi ha, ja que aquesta serà la diferencia entre l'input i output, és a dir, tota la quantitat que es desitja enviar menys tota la quantitat disponible de qui envia. Si no es defineix on s'ha d'enviar la quantitat sobrant, el propi sistema crearà una nova adreça a l'usuari que envia, per tal de tornar la quantitat sobrant.

En el cas de que no calgui una signatura de les transaccions, com es pot donar en el cas d'enviar només un missatge amb una quantitat d'input de 0, el propi camp on ha d'anar la signatura fragmentada podrà ser utilitzat per emmagatzemar el missatge. Per una altra banda, si és vol enviar una quantitat amb un missatge es compartirà el camp, i si no s'especifica el missatge o si no és necessari la signatura, el camp del missatge passarà a estar omplert de 9's. Es fa així degut a que el camp del missatge és de 2187 trytes, estant cada tryte en el sistema de numeració ternària tenint com a possibles valors -1, 0 i 1. Per una altra banda, com els missatges rarament són múltiples de 2187, l'espai sobrant serà omplert amb el número 9 per tal d'arribar a la mida esmentada anteriorment.

Per acabar de consolidar la part de l'output farem un petit exemple (figura 6) on es pugui recollir tot el que hem explicat en aquesta secció:

L'usuari A vol enviar 100 IOTA's a l'usuari B sense cap missatge, així que prepara la primera part del bundle, l'output.

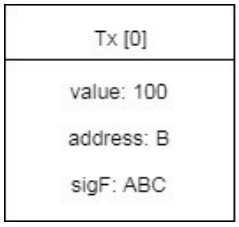


Figura 6: transacció d'output

Una vegada tenim clar de què consta un output, passem a la següent secció.

7.1.2 Secció d'input

Que consta de:

- Definir una quantitat per input
- Definir l'adreça per input
- Generar una signatura per input

En aquesta secció afegim un valor negatiu en cada input, que serà la quantitat a poder de IOTA's. Per un altra banda, ens dóna la possibilitat de que les nostres transaccions siguin més segures, per fer-ho, hem de multiplicar el camp de la signatura per cada nivell extra de seguretat. Per exemple, si volem incrementar la seguretat a nivell 3 la signatura tindrà un total de 3*2187 trytes, que comportarà més transaccions en l'input, conegudes com meta transaccions, que portaran cadascuna, un tros de signatura addicional, ja que cada transacció té un camp destinat per la signatura de 2187 trytes, així que en aquest cas tindríem 3 transaccions que portarien 3 trossos d'una mateixa signatura.

Per tal de veure-ho millor partirem de l'exemple anterior, però ara definint l'input:

L'usuari A vol enviar 100 IOTA's per satisfer l'output definit anteriorment, així que tria les seves adreces A1 i A2 amb una seguretat de nivell 2 per fer-ho.

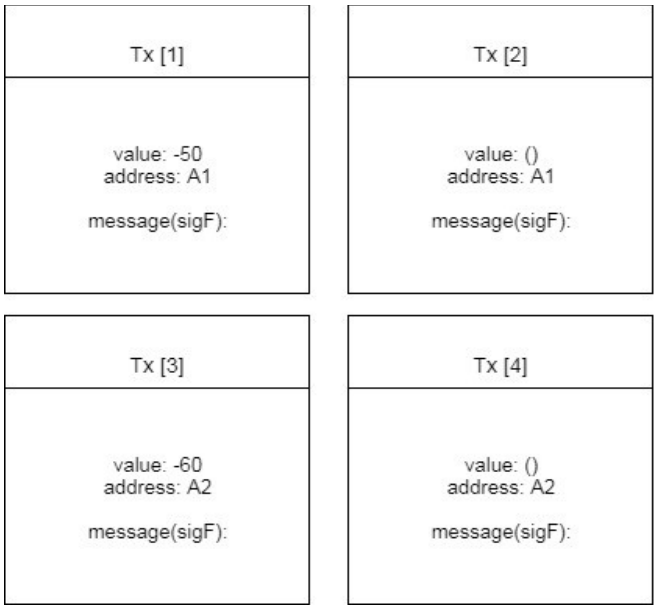


Figura 7: transaccions d'input

Com hem vist a la figura 7, hem generat 4 noves transaccions, ja que per una banda necessitem 100 IOTA's de les adreces A1 i A2, a més de que el nivell 2 ens requereix que per cada input afegim una meta transacció.

Dit això, encara ens queda per retornar la quantitat de IOTA's restant. Aquí hi hauria dos possibilitats.

La primera, afegir una nova transacció indicant a quina adreça s'ha de retornar la diferencia:

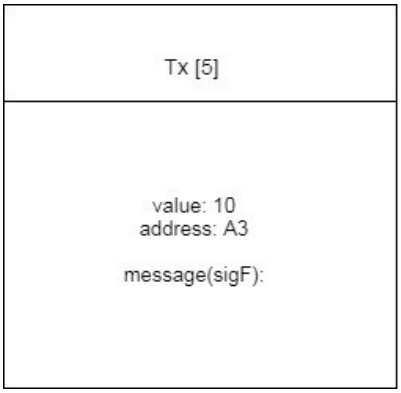


Figura 8: transacció dels IOTA restants

En la figura 8 hem especificat que els IOTA's que sobrin s'enviïn a l'adreça A3.

La segona forma de fer-ho seria no especificant cap transacció. Si escollíssim aquesta opció el propi sistema generaria una nova adreça per a l'usuari A, on enviaria els IOTA's restants.

Anteriorment hem vist com serien les estructures principals del *bundle* d'una forma bàsica, en la següent secció tractarem tota la informació que va inclosa dins de les transaccions i en l'estructura general del *bundle* fins arribar a realitzar la transacció.

7.1.3 Procés de finalització de les transaccions i construcció del *bundle*

En aquesta segona secció es necessari desplegar més camps de les transaccions que hem fet servir d'exemple anteriorment, així doncs les transaccions amb les que treballarem tindran el següent aspecte:

Figura 9: transaccions del *bundle*

Com podem comprovar en la figura 9, hem afegit diversos camps necessaris. Primer de tot tenim el TAG, que identifica una transacció en el Tangle, el *timestamp*, que indica en quin moment s'ha construït la transacció, i per últim els índexs per identificar la cadena de transaccions. A partir d'aquí generarem el *hash* del *bundle* a partir de les dades introduïdes i amb la funció Kerl *hash* els trits representats en cada camp són absorbits i validats per un *sponge constructor*, produint un output amb la mida desitjada (*hash* digest), que es pot entendre com si les dades fossin absorbides per una esponja i després espremudes generant l'output. La *sponge function* té dos fases, la primera, en que el missatge o contingut és comprimeix iterativament seguit d'una fase de espremut en el que el *hash* digest és extret d'una forma iterativa. Aquest algorisme ha estat realitzat per IOTA utilitzant la funció criptogràfica *estandard* keccak_384 com a base de la funció de compressió de dades.

A més a més, en el pas d'obtenir el *hash* del *bundle*, comprovarà si el *hash* obtingut és segur o no. En el cas de que no ho sigui, incrementarà el *tag* de la transacció amb índex 0 (*tail*) com podem veure en el la figura 10:

```
var normalizedHash = this.normalizedBundle(hash);
  if(normalizedHash.indexOf(13 /* = M */) != -1) {
   // Insecure bundle. Increment Tag and recompute bundle hash.
   var increasedTag = tritAdd(Converter.trits(this.bundle[0].obsoleteTag), [1]);
   this.bundle[0].obsoleteTag = Converter.trytes(increasedTag);
  } else {
   validBundle = true;
  }
```

Figura 10: codi de comprovació del *hash*

Com hem esmentat anteriorment, el *tag* serveix per buscar la transacció dins del Tangle per un valor específic, així que serà necessari que estigui actualitzat fins que el *hash* sigui prou segur.

Quan s'hagin validat tots els camps i es tingui un *hash*, serà el moment d'inserir-lo en cada transacció, quedant tal i com es mostra la següent figura 11:

Figura 11: transaccions amb el *hash* del *bundle*

El que hem de fer a continuació és signar les transaccions d'input amb la corresponent adreça o adreces de

clau privada que identifica l'usuari. Aquesta adreça l'aconseguirem a partir de la llavor de l'usuari A juntament amb el generador de claus, sent aquesta llavor l'encarregada de generar adreces i la part més important per la seguretat de l'usuari. A partir d'aquí utilitzarem el conjunt d'adreces de clau privada, per generar gràcies a la clau privada de cadascuna d'aquestes adreces i el *hash* del *bundle* les signatures de les transaccions. Aquest procés es farà de forma iterativa, és a dir, el generador utilitzarà la clau privada de cada adreça i el *hash* del *bundle* per fer la inicialització i posteriorment la construcció del fragment de la signatura de cada transacció.

Després d'haver fet aquest pas tindrem la figura següent:

Figura 12: Transaccions signades amb la clau privada

Com mostra la figura 12, una vegada tenim tots els camps omplerts menys el *nonce*, és l'hora d'enviar la nostra transacció al Tangle, ja que el *bundle* està construït.

7.2 Tangle de IOTA

En aquest punt necessitem obtenir dos *tips* (transaccions referenciades però no aprovades), un que es diu *branch* i l'altre que es diu *trunk*. Sabent que:

- *Trunk transaction*: string de 81 trytes, sent el *hash* de la primera transacció que ha estat aprovada

amb aquesta transacció.

– *Branch transaction*: string de 81 trytes, sent el *hash* de la segona transacció que ha estat aprovada amb aquesta transacció.

Per tal de fer-ho utilitzarem l'algorisme que utilitza IOTA, el Markov *chain* Monte Carlo (MCMC), per tal d'obtenir els dos *tips* que necessitem per referenciar la nostra transacció. L'algorisme abans mencionat ha estat creat per tal d'afavorir la selecció "aleatòria" dels *tips* però també com a mecanisme de seguretat per possibles atacs. Aquest últim punt el deixarem per més endavant. El funcionament d'aquest algorisme consisteix en repartir una sèrie de partícules (*random walkers*), en els *sites* (transaccions aprovades i referenciades) més propers a l'origen del Tangle, per tal de que vagin avançant pels diferents *sites* en direcció als *tips* d'una forma aleatòria, on els dos *tips* seleccionats pels dos primers *random walkers* són els candidats per ser aprovats.

Una vegada han estat seleccionats és l'hora d'omplir el *trunk*, *branch* i de trobar el *nonce*, realitzant un *Proof of Work* (PoW) en cada transacció del *bundle* per tal d'omplir aquest camp.
Com hem esmentat al principi d'aquesta secció, un *bundle* és una unitat atòmica de transferència en el Tangle, la qual cosa significa que es tindran els mateixos *tips* per cada transacció. Sabent això, recorrerem cada transacció en el *bundle* des de l'últim índex fins al primer, omplint el *trunk*, el *hash* del *branch*, el *timestamps* i fent per últim PoW per trobar el nonce i generar el *hash* de la transacció, per després validar el resultat del PoW. Després d'omplir els camps ens queda la següent figura:

Tx [0]	Tx [1]	Tx [2]
value: 100 address: B tag: TAG0 timestamp: currentTime() index: 0 lastIndex: 5 bundle: ARX... trunkTransaction: H1 branchTransaction: TRUNK_TIP nonce: POW1 message(sigF): SIG123123 hash: H0	value: -50 address: A1 tag: TAG1 timestamp: currentTime() index: 1 lastIndex: 5 bundle: ARX... trunkTransaction: H2 branchTransaction: TRUNK_TIP nonce: POW2 message(sigF): SIG123123... hash: H1	value: () address: A1 tag: TAG2 timestamp: currentTime() index: 2 lastIndex: 5 bundle: ARX... trunkTransaction: H3 branchTransaction: TRUNK_TIP nonce: POW3 message(sigF): ...123123 hash: H2
Tx [3]	**Tx [4]**	**Tx [5]**
value: -60 address: A2 tag: TAG3 timestamp: currentTime() index: 3 lastIndex: 5 bundle: ARX... trunkTransaction: H4 branchTransaction: TRUNK_TIP nonce: POW4 message(sigF): SIG123123... hash: H3	value: () address: A2 tag: TAG4 timestamp: currentTime() index: 4 lastIndex: 5 bundle: ARX... trunkTransaction: H5 branchTransaction: TRUNK_TIP nonce: POW5 message(sigF): ...124124 hash: H4	value: 10 address: A3 tag: TAG5 timestamp: currentTime() index: 5 lastIndex: 5 bundle: ARX... trunkTransaction: TRUNK_TIP branchTransaction: BRANCH_TIP nonce: message(sigF): SIG123124 hash: H5

Figura 13: Transaccions adjuntades al Tangle

Com podem veure a la figura 13, els camps de les transaccions ja estan emplenats. Si tot va com és d'esperar obtindrem el conjunt de trytes de la transacció, i el nostre *bundle* de transaccions passarà a formar part del Tangle, convertint-se en un conjunt de *tips*.

Ara que ja entenem de forma bàsica com es realitzen transaccions a IOTA, començarem per introduir la base de dades de IOTA.

7.3 Base de dades

7.3.1 RocksDB en el IRI de IOTA

La base de dades utilitzada per IOTA en el IOTA *reference implementation* (IRI) és la RocksDB [19]. On les columnes estan formades per famílies per tal de separar les metadades de les dades i per aconseguir escriptures atòmiques, on algunes d'elles utilitzen la operació de *merge* juntament amb l'operació *d'append* ",", ja que un valor pot contenir diversos ítems i es necessari separar-los.
Les diverses columnes que tenim en la aquesta base de dades són les següents:

Columna	Descripció	Key	*value*	Merged(si/no)
Default	Columna per defaut, no usada en el IRI	-	-	-
Transaction	Informació bàsica de la transacció	Transaction *hash*	Transaction(8019 trits, 2673 trits)	No
Transaction-metadata	La metadata de la transacció	Transaction *hash*	Transaction metadata	No
Milestone	Guarda el *hash* de la transacció de milestone a l'index	Milestone index (int, 4 bytes)	Transaction *hash*	No
stateDiff	Utilitzat en el milestone per fer un check del *snapshot*	Milestone *hash* (Transaction *hash*)	List([Transaciton *hash*, *value* Changed])	Yes
Address	Transaccions de les adreces	Address	List[Transaction *hash*]	Yes
Approvee	Els fills que referencien la transacció	Transaction *hash*	List[Transaction *hash*]	Yes
bundle	Grup de transaccions creades	Transaction *hash*	List[Transaction *hash*]	Yes
Tag	Atribut en la	TAG	List[Transaction	Yes

	transacció per tal de buscarla		*hash*]	

Taula 7: Columnes de la base de dades de IOTA

Partint de la taula 7, una particularitat que té IOTA és que els trytes-string del *transaction hash* són convertits a bytes abans de ser guardats en la base de dades ja que cada byte pot contenir 5 trits, així que podem reduir fins a un 60% l'espai fent aquesta conversió.

7.3.2 RocksDB i l'adaptació al nostre context

La rocksDB utilitza un *Log Structured Database Engine* per guardar les dades, ja que proveeix d'un accés indexat als fitxers podent inserir un gran volum de dades en un temps molt baix, mantenint-les en dos o més estructures separades, i estant cadascuna d'elles optimitzades i sincronitzades per fer-ho possible.

Per una altra banda, ens permet fer algunes operacions necessàries pel nostre context, d'entre elles: la divisió per columnes de famílies, per tal d'associar cada *key-value* en una família en concret, possibilitant operacions com *Write({column_family_1, key1, value1}*, l'operació de *merge* com una operació atòmica de *Read-Modify-Write*, *l'append*, i les bàsiques de get, *remove*, *set* i *add*. A partir d'aquest punt començarem a explicar com és l'arquitectura bàsica d'aquesta base de dades i quins mecanismes utilitza per fer les cerques.
En la rocksDB tenim una sèrie de fitxers amb el nom de log, els quals guarden els *updates* fets recentment, ja que cada *update* nou serà afegit al fitxer log utilitzat en aquell moment. Quan aquest fitxers arribar a una mida d'aproximadament 4MB, aquest es convertit en una taula ordenada (SST), i un nou fitxer log es creat per futurs *updates*, també una còpia de l'existent arxiu log es guardada en una estructura de memòria (*memtable*) per tal de ser consultada en cada *read*, per tal de que reflecteixin els *updates* fets.

Ara entrem en el tema de les taules ordenades. Aquestes guarden entrades ordenades per la *key*, on cada entrada és o bé un valor per la clau o bé un marcador de *delete* per la *key.*

Aquestes taules estan organitzades per nivells. La taula generada a partir d'un fitxer log s'inclou en el nivell 0, fins que aquest nivell té un total de 4 arxius. Quan això passa, tots els arxius del nivell 0 (que representen els que estan a memòria) són fusionats juntament amb tots els fitxers superposats del nivell 1 per produir una nova seqüencia d'arxiu de nivell 1 (crearem un nou nivell 1 d'arxius per cada 2MB de dades).

Per fer un get(), la rocksDB accedeix a la *memtable* (taula de memòria) i als arxius SST per fer una cerca de la clau (com hem dit anteriorment aquests fitxers/taules estan organitzades per nivells). La compactació es realitzarà periòdicament, per tal de triar els arxius dels nivells alts i fusionar-los amb els de nivell baix. Com a resultat, els *key-values* seran moguts del nivell 0 cap a baix d'un *log-structured merge-tree* (LSM) de forma gradual. Aquesta compactació ordenarà els *key-value* i els dividirà en els fitxers. Gràcies a això, no farem un escaneig en cada fitxer SST mirant si la clau està en aquest rang, sinó que farem una cerca binaria basada en el fitxer FileMetaData.largest per tal de cercar un fitxer candidat que pugui contenir la clau que busquem. D'aquest forma reduirem la complexitat de O(N) a O(log(N)) en el millor cas (sent O(N) el pitjor cas en els nivells més inferiors), mantenint un temps d'inserció de O(1).

Una observació a aquest problema és que, després de construir l'arbre LSM, la posició d'una fitxer SST està fixat en un nivell, a més de que l'ordre relatiu dels fitxers del següent nivell també està fixat. Basant-nos en aquesta idea, podem realitzar una optimització que ofereix la RocksDB per tal de reduir el rang de la cerca binaria a partir de la cascada fraccional [20][21] ja que reduirem el rang de cerca. Si guardem una sèrie de llistes per separat, l'espai és O(N), però el temps per realitzar una consulta és de O(K log (N/K)), on N són els elements i K el nombre de llistes. On el cas pitjor és quan les llistes tenen la mateixa mida N/K, per això cada una de les cerques necessitem un temps de O(log (N/K)). Així doncs volem un mètode que combini un bon espai d'emmagatzematge i un temps de consulta adequat O(log N+K). Per fer-ho seleccionarem tots els elements de l'i-èssim *array* que no estiguin en l'anterior a aquest i els fusionarem, de forma que el primer *array* és el doble de gran, així podrem saber la informació de cada nou *array* que visitem abans de fer-ho utilitzant els punters generats. De forma més general, fem una consulta a partir d'una cerca binaria en la primera fila, i determinem a partir del resultat que ens doni la posició d'aquesta consulta en aquesta llista. Llavors, utilitzem aquesta posició per extreure el valor associat amb la posició del valor que busquem en la propera fila, ja que el valor associat amb la posició de la cerca en la primera fila apunta a una posició de la fila següent, que o bé és el valor que trobaríem amb la cerca binaria de la fila actual o està a un pas més lluny del valor correcte, fent una única comparació (aquest procés es repeteix fins trobar el valor). Degut a això fer la cerca en cada fila requereix una comparació, arribant com hem dit abans a un temps de O(log N+k) per cada cerca en k files.

Ara, passant aquesta solució a la RocksDB ens trobem amb una cerca binaria basada en el FileMetaData.largest per trobar el fitxer candidat. Llavors la *key* que busquem es comparada amb el fitxer anterior i el FileMetaData.smallest per tal de veure si cau en aquest rang. Si per exemple estem buscant la *key* 10 i el primer fitxer comença per la *key* 50, sabem que tindrem que baixar al següent nivell per tal de realitzar la cerca. Normalment s'hauria de fer una cerca binaria en tots el arxius del nivell dos però sabent que la *key* 10 es menor a la 50, i que només els fitxers amb un rang inferior a 50 podran contenir la clau fa que la cerca es redueixi notablement. En la rocksDB cada nivell l'espai té un factor multiplicatiu per 10, per tant, en el nivell més baix és on hi haurà més elements, però gràcies a aquesta solució les cerques es reduiran notablement a partir del primer nivell, ja que podrem fer una estimació d'on es localitzarà l'adreça que estem buscant en els nivells inferiors, reduint molt l'espai de cerca.

A continuació tractarem els aspectes més representatius de la seguretat en el sistema de IOTA, per saber a què ens enfrontem i quines són les solucions disponibles.

8. Seguretat

Un dels principals problemes de seguretat que han de combatre les *chains* és el atac del *double-spend* i el qual serà el motiu dels següents tres subapartats. Aquest tipus d'atac es descrit com qualsevol transacció que fa que una adreça arribi a un valor negatiu. Per exemple, el fet de gastar una mateixa quantitat monetària dos vegades, on el nostre context, enviar dues vegades la mateixa adreça.

Sabent això, comencem doncs a una explicació més precisa del MCMC, ja que serà la nostra eina per tal d'evitar aquests atacs.

8.1 El funcionament del Markov *chain* Monte Carlo (MCMC)

El principal motiu d'incloure aquest algorisme ha estat que utilitzant el *Random tip Selection Strategy* (una selecció dels *tips* de forma aleatòria) no podem protegir-nos contra aquest tipus d'atac, ja que fa que tots els *tips* tinguin la mateixa probabilitat de ser seleccionats.
El MCMC assegura que tots els *tips* són seleccionats de forma no-deterministica des del punt d'inici en l'interior del Tangle fins al *tip* seleccionat, on la ruta que es recorrerà es coneix com el *largest cumulative weight* que es basa en tindre en compte la suma de tots els pesos de les transaccions aprovades directament o indirectament de la qual partim, sent el pes el treball realitzat en el PoW. Per tant, aquest mecanisme és el recomanat per cada node que vulgui incloure una nova transacció, ja que ajuda a la seguretat del Tangle.

La forma d'actuar del MCMC és la següent:

Un node situa un nombre de *walkers*, per exemple 8, en una profunditat considerable del Tangle, utilitzant com a heurística que el nombre de pes acumulat (*cumulative weight*) estigui entre W i 2W, sent W un nombre no negatiu o per exemple el nombre de transaccions que s'han rebut en un rang de temps concret. Tenint la heurística, cada *walker* es mou avançant per una sèrie de *sites* referenciats fins arribar als *tips* a partir d'un càlcul probabilístic per decidir quin és el següent *site* on es situarà. Tot això tenint com a idea de que quan més petita sigui la diferencia entre els pesos acumulats del *site* on estem i el següent menys pes acumulat perdrà el *walker,* fent que l'elecció sigui més bona. Aquest procés es farà fins que dos *walkers* del conjunt arribin a dos *tips* per aprovar.

Sabent com funciona, passem a explicar quina seria l'actuació enfront d'un dels pitjors atacs possibles, el parasite *chain*.

8.2 Mètodes per evitar la parasite *chain*

Aquest atac comença quan usuari de forma secreta construeix un Tangle el qual conté una transacció que actuarà com a *double*-spend. Primer de tot enviarà una transacció legitima al Tangle principal, on es realitzà un pagament i esperarà que l'altre persona implicada accepti, mentre que el Tangle maliciós va referenciant transaccions del Tangle original per incrementar la notorietat del seu Tangle, incrementant el nombre de *tips* que aquest Tangle té en aquest moment. La idea que es té, es la de fer que els nodes afegeixin noves transaccions referenciant aquest Tangle maliciós, per tal que la branca no maliciosa del Tangle principal sigui abandonada. D'aquesta manera, s'esborrarà la transacció legítima i el receptor perdrà els diners. Com hem comentat anteriorment, davant d'aquest problema tenim la solució que ens ofereix el MCMC, ja que no seleccionarà cap *tip* de l'atacant amb una alta probabilitat degut a que el pes acumulatiu d'aquest Tangle maliciós és bastant baix i la probabilitat de que un del *walkers* caigui dins d'aquest Tangle també és bastant baixa. En el cas que caigués, seria abandonat més endavant degut al poc pes acumulat, per una altra banda si s'arribés a aprovar un *tip* maligne, arribaria un punt que succeiria un conflicte degut a l'estat del *snapshot* antic i el nou en la comprovació de la quantitat de *tokens* o adreces que té una usuari, així que tindríem un conflicte de transaccions perquè hi hauria un error degut a que el saldo d'un compte no pot ser negatiu. Per resoldre-ho, la branca on passa la incidència seria

abandonada i les transaccions ja aprovades en aquesta haurien de tornar a fer el procés per ser incloses al Tangle.

L'escenari anterior pressuposa que el Tangle origen té més poder computacional que el Tangle maliciós, ja que sinó l'atacant podria produir grans increments en el pes acumulat i prendria el control del Tangle origen. Per evitar això, IOTA continua utilitzant un mecanisme que s'anomena "el coordinador".

8.3 El coordinador de IOTA

El coordinador ha estat creat degut a que en IOTA hi ha pocs nodes i una atacant podria, amb relativa facilitat crear múltiples nodes i que aquests enviessin transaccions malignes. En aquest cas, si utilitzéssim el mètode de MCMC, hi hauria un alt percentatge de que aquestes transaccions fossin seleccionades. Per protegir el Tangle d'aquests atacs on es contempla que l'atacant té més d'un 33% de poder de computació, s'ha establert el mecanisme del coordinador (COO). Aquest és un node especial executat per la IOTA *Fundation* amb l'objectiu de validar directament o indirectament les transaccions, ja que crea *milestones* que no deixen de ser transaccions verificades com a ben intencionades per IOTA. L'ús d'aquest mecanisme no significa que la xarxa de IOTA sigui centralitzada, ja que els diferents nodes del Tangle segueixen verificant que el COO no trenqui cap de les regles de consens creant monedes no existents o aprovant atacs de *double-spending.* Aquest mecanisme continuarà sent utilitzat fins que el nombre de transaccions per segon arribin a un llindar, que de moment és desconegut, com també el pronòstic del moment en el que això succeirà, ja que depèn en gran part de la popularitat que aconsegueixi la *chain*.

9. IOTA i les adreces IP

Com sabem, el IPv6 està destinat a substituir el IPv4 d'Internet, a causa de l'assignació massiva de noves adreces IP, per tant hem optat de plantejar el nostre sistema pensant en el futur per tal de poder assignar aquestes IP's als diferents dispositius. El canvi més important que presenta la substitució de la que hem parlat anteriorment és la longitud de les adreces de xarxa, ja que passem a poder disposar de 128 bits, tenint a prop de 340 sextilions (2^{128}) adreces. La nostra proposta amb IOTA és la de tractar aquesta quantitat d'adreces com si fossin les monedes que utilitza per realitzar les transaccions, així doncs els canvis que hem inclòs i que inclourem més endavant estaran enfocats en com fer-ho possible.
IOTA utilitza la base de dades *key value* RocksDB, on els *keys* i *values* són *arrays* de bytes arbitraris ordenats per tal d'emmagatzemar les transaccions del Tangle, per poder discutir d'aquest tema abans de tot necessitarem saber quina és la seva estructura i com ens afecta en el nostre context.

9.1 Canvis en l'estructura de dades i comprovacions de IOTA

En la nostra adaptació canviem la quantitat positiva a enviar per adreces que han de seguir la nomenclatura del Internet Protocol Version 6 (IPv6), per fer-ho utilitzarem un *String* que tindrà el format hexadecimal de

les adreces IPv6 (b:b:b:b:b:b:b:b/X) on cada b correspon a 16 bits i X a la màscara. Fent-ho així, cada usuari tindrà diversos conjunts d'adreces IP, representats com a rangs, i per tant, la quantitat sobrant també passarà a ser una o diverses adreces que s'afegiran en el rang corresponent.

Per fer-ho haurem de modificar el camp de *value* per tal de que sigui un rang de *Strings* que representaran les adreces. Aquest canvi s'ha fet pensant, per una banda, perquè els usuaris només hagin de mirar quin és el primer i últim rang de cada paquet de rangs que tenen, per així facilitar-los la feina al fer les transaccions, ja que d'una altra manera haurien d'incloure cada adreça individualment juntament amb el prefix. D'aquest forma en cadascuna de les adreces d'un usuari hi haurà un conjunt de rangs, com paquets d'adreces que pugui gastar de forma fàcil i intuïtiva. Per una altra banda tenim que l'emmagatzematge en la base de dades és més senzill i no hem de realitzar cap pre-cerca per tal de trobar a quin prefix podem localitzar cadascuna de les adreces, a més de tenir-les ordenades facilitant els mètodes de cerca que hem esmentat anteriorment per tal de tenir un millor temps i per tant, una major escalabilitat del sistema.

Per una altra banda, la nostra proposta seria mantenir el format de columnes de famílies que hi ha a IOTA, però variant certs aspectes. Primer de tot, volem que la *key* de cada valor sigui una adreça codificada com a *BigInteger*, ja que una mateixa adreça IP no pot ser repetida en més d'una tupla. Així que la nostra forma de definir les dades serà de forma contraria a com estan definides a IOTA, ja que si utilitzem el valor (l'adreça) com a *key*, la principal informació que contindrà serà el *hash* de la transacció i el TAG. D'aquesta manera quan arribin diverses transaccions amb un rang d'adreces, cadascun d'aquests rangs seran descompostos en petites transaccions unitàries d'una sola adreça i compartint un mateix *hash* de transacció, per tal de que a l'hora d'identificar un rang tinguem enllaçats totes les adreces que conté. Previsiblement, la fase inicial d'aquesta proposta tindrà una gran quantitat de creació de noves tuples com adreces IPv6 utilitzades existeixen actualment, però les fases següents seran majoritàriament de cerca i modificació del camp origen i destí, referenciant nous intercanvis entre els usuaris d'aquest sistema. Per últim arribarem a la fase on haurem de reduir la base da dades utilitzant un *snapshot*, ja que depenent del nombre de noves adreces la mida prevista per emmagatzemar les dades serà massa gran, tant pels usuaris com pel sistema en si per tal de realitzar les cerques.

A partir d'aquí farem referència a les comprovacions realitzades per adaptar el nostre context al Tangle de IOTA.

El llenguatge que hem fet servir per realitzar els canvis és JAVA, així que a partir d'aquí totes les propostes estaran enfocades en aquest llenguatge de programació.

Per fer-ho, primer de tot utilitzarem la classe *Range* de la llibreria d'Apache per tal de definir la nostra estructura de dades de la següent forma:

```
1.  Range<String>range = Range.between(min,max); // range = [min..max]
```

D'aquesta forma, l'estructura dels saldos d'un usuari (input) i de les adreces a enviar (output) estaran definides així:

```
1.  private ArrayList<Range<String>> inputs;
2.  //inputs = ([min..max],[min..max],...)
3.
```

```
4.  private ArrayList<Range<String>> outputs;
```

Aquestes dos estructures les mantindrem ordenades de forma ascendent en relació amb els rangs d'adreces.

Una vegada definides quan vulguem crear una nova transacció haurem de fer un procés de comprovació per tal de que les adreces siguin vàlides:

```
1.  public static boolean IsIPv6(Range<String> rangeAddress) {
2.     IPAddress ip, ip2;
3.     if ((IPAddress.TryParse(rangeAddress.getMinimum(), out ip) && (IPAddress.TryParse(rangeAddress.getMaximum(), out
    ip2)) {
4.        return (ip.AddressFamily == AddressFamily.InterNetworkV6) && (ip2.AddressFamily == AddressFamily.InterNetwork
    V6);
5.     }
6.     else {
7.        return false;
8.     }
9.  }
```

Una vegada que hem comprovat les adreces, en el procés del *bundle* necessitarem saber si l'input satisfà l'output, és a dir, per saber si tenim les adreces que hem dit que volem enviar. Per fer-ho, una proposta de funció seria la següent:

```
1.  for(int i = 0; i < outputs.size()-1; ++i) {
2.              Range<String> actualRange = outputs.get(i);  //obtenim el primer output p.e [1...12] de la llista d'outputs
3.       int add = 0;  //g
4.       for(int j = 0; j < inputs.size()-1; ++j) {
5.            Range<String> spentRange = inputs.get(j);  //obtenim el primer input p.e. [1..10] de la llista d'inputs
6.            if(spentRange.contains(actualRange.getMinimum()+add)) {
7.                 if(spentRange.contains(actualRange.getMaximum())) {
8.                      j = inputs.size(); //conté tot el rang d'adreces, podem passar a comprovar el següent
9.                      add = 0;
10.                }
11.                else if(j.equals(inputs.size()-2)) {                    throw new IllegalSt
    ateException(NOT_ENOUGH_BALANCE_ERROR); //si estem a l'ultim rang i no hi és el que busquem, exc          }
12.                add = spentRange.getMaximum(); //per mirar el següent rang mirarem des del màxim rang anterior
13.           }
14.      }
15. }
```

En aquesta proposta comprovem que el nostre input satisfà l'output, és a dir, si el conjunt dels rangs dins de *l'ArrayList* de l'input queden inclosos dins de *l'ArrayList* de l'output.

El funcionament serà el següent:

Tenim dos *ArrayList*, un amb la llista d'outputs (el que volem enviar) i l'altre amb la llista d'inputs (el que tenim per gastar). Aquest mètode anirà obtenint cadascun dels inputs i comprovarà que els rangs satisfan tots els outputs. Si es troba que un rang de l'output queda inclòs dins d'un rang de l'input es passarà a comprovar el següent output, recorrent novament des del principi, altrament, utilitzarem la variable *add* per guardar el màxim trobat en el rang de l'input actual per tal que es tingui en compte en la propera iteració. Pot passar que s'obtingui l'últim rang dels inputs i encara no s'hagi satisfet un output en concret,

llavors es llançarà excepció ja que no hem trobat un rang de l'output inclòs en el i-èssim rang de l'input.

Finalment, quan el *bundle* i cada transacció hagin emplenats tots els camps, serà el moment de guardar la transacció. Per fer-ho convertirem cada adreça del rang en un BigInteger, per ser més fàcil de tractar utilitzant les llibreries de JAVA i més tard realitzar la seva inserció a la BD.

Una vegada tenint aquestes petites comprovacions i definicions de dades, les haurem d'ajustar a quasi cada mètode i classe de tot el sistema IRI de IOTA, variant la codificació de les transaccions, *bundle*, compressió, *snapshot* i encriptació de les dades. Per fer-ho, caldrà testejar mètode per mètode i anar pas per pas des de la creació d'una *wallet* amb els seus rangs d'adreces juntament amb les comprovacions que calen en cada etapa del procés d'incloure una transacció al Tangle, fins finalment arribar a la seva inserció a la base de dades i comprovar que al fer la desencriptació per modificar els valors nous i/o l'eliminació dels existents es realitza d'una forma correcte.

Una vegada tenim els principals canvis de paràmetres i quina seria la feina a realitzar, és necessari comentar com afectarà el nostre plantejament a l'escalabilitat del sistema quan es guardin de forma massiva cadascuna de les transaccions.

9.2 Escalabilitat

A IOTA una transacció ocupa 8019 trits, amb la seva transformació per reduir l'espai arribem a un total de 1604 bytes/transacció. Per una altra banda, tenim que els fitxers tenen una capacitat de 2MB, així que tindrem un total de 500 transaccions (aproximadament) per fitxer. Per exemple, guardant una quantitat de 5B d'adreces en transaccions necessitaríem aproximadament 7 TB d'emmagatzematge repartits entre els diferents nivells de la rocksDB i els diferents nodes del Tangle. Com IOTA no guarda les transaccions velles per tal de mantenir un Tangle d'una mida petita, seguirem el mateix mètode que utilitza del *snapshot*, triant quina informació del Tangle cal descartar per no tenir una base de dades massiva i centralitzada, ja que sinó seria impossible que cada usuari tingués una còpia. Així que a mesura que creixi el Tangle guardarem només la informació rellevant de les transaccions, en el nostre cas el *hash*, adreces, l'adreça (*key*) i la *milestone* de la tupla.

Com hem esmentat amb anterioritat, a IOTA es fa servir el TAG per identificar una transacció, però aquesta no ens diu res en el nostre context, ja que el que estem buscant és una adreça en concret. Per tant el nostre identificador o *key* en la base de dades serà l'adreça IP en si convertida en *BigInteger*, així podrem tenir els *keys* ordenats i la cerca serà molt més senzilla.

Una mesura de protecció que hem pensat a incloure és que al principi tindrem un cert rang d'adreces IP disponibles per tal d'anar-ne afegint depenent de la comunitat darrere el projecte, ja que la nostra capacitat d'emmagatzematge està relacionada amb el nombre total d'usuaris que en faran ús, i per tant, és impossible tindre totes les adreces IP disponibles des del principi. Llavors, a mesura que augmenti la popularitat del projecte, és podran incloure noves adreces IP. Per una altra banda, quan ens acostem a un llindar d'espai no sostenible per la majoria d'usuaris, es farà un *snapshot* del Tangle amb la informació necessària que hem comentant amb anterioritat per tal de reduir la mida i l'operativitat en ell.

A continuació, amb l'estudi que hem realitzat al llarg d'aquest projecte presentarem les conclusions que hem extret**.**

10. Conclusió

La principal motivació per fer aquest treball és de poder comparar quins aspectes positius i negatius en la seguretat ens aporta aquest nova tecnologia comparada amb les tecnologies convencionals que desenvolupen la mateixa tasca i utilitzar-la per poder fer assignacions IP. Al llarg del treball hem anat analitzant de mica en mica la tecnologia de la *Blockchain* fins centrar-nos únicament en el projecte de IOTA. A partir del que hem extret en el seu estudi teòric i la seva implementació pel context d'adreces IP no tenim prou informació per concloure de que pugui o no poder-se adaptar per tal de millorar el sistemes existents, però si que hi ha alguns punts a destacar del per què no el veiem del tot factible.

Primer de tot perquè el sistema de IOTA s'ha fet des de la base per un motiu en concret i amb unes estructures i mètodes quasi bé inamovibles pel que fa el canvi, ja que el projecte està completament integrat i no permet modificacions a nivell modular. A causa d'això qualsevol canvi que es vulgui plantejar enfocat en la seva estructura principal, passa per modificar gran part del mètodes que utilitza, i per tant, comporta una complexitat mitjana com hem comprovat en l'apartat 9.1, ja que els canvis en generals en l'estructura del *value* per adreces que hem tractat en la secció comporten una modificació en el funcionament de quasi cada classe, en múltiples funcionalitats i encriptacions, tant en les transaccions del *bundle* com en les adreces dels usuaris.

Des del principi vam pensar que al ser part de la *Blockchain* però no tindre les estructures de blocs podria aportar algun mecanisme nou per combatre els atacs, ja que la majoria de projectes que utilitzen PoW tenen el mateix problema que hem pogut comprovar amb aquest, però com en els altres ens trobem amb diversos problemes. Primer de tot la gran quantitat d'energia que es requerida per mantenir una quantitat de nodes verificant les transaccions a partir de l'algorisme de PoW, la centralització degut a l'acumulació del poder de *hash*, i la perillositat dels atacs que hem tractat anteriorment quan el COO desaparegui del Tangle, ja que llavors no hi haurà una entitat verificadora i que reguli el bon comportament dels usuaris. Però per una altra banda trobem algunes millores comparat amb alguns sistemes actuals que utilitzen PoW, ja que a IOTA no existeix un incentiu monetari per contribuir en el benestar del Tangle, sinó que els usuaris participen en aquest sistema per altre motius, com per exemple per tindre més control de les transaccions que envien. Per fer-ho no es requereix un sistema d'altes prestacions, ja que com hem explicat, al no haver-hi un gran incentiu, la competència amb els altres usuaris per contribuir en el *mining* no és tant ferotge, i també que disposa de mecanismes de defensa addicionals com el MCMC que ajuda a protegir el Tangle d'atacs futurs.

Per una altra banda, la seguretat que ens aporta el COO no sembla una mesura prou contundent i encertada per un projecte d'aquestes característiques, ja que quan en un projecte de la *Blockchain* s'inclouen aquest tipus de mecanismes "manuals" per la pròpia *chain*, sense una planificació ben realitzada de com poden canviar en el futur, deixa molts interrogants en quant a una utilització tan seriosa com seria l'assignació de direccions IP i una posada en funcionament a nivell global. Un altra dels problemes relacionats amb aquesta *Blockchain* i que hem pogut comprovar, és el possible atac del 33% de poder de

computació. No seria d'estranyar que grups maliciosos poguessin interferir i prendre control de la *chain* si es donés el cas.

Tanmateix, per poder valorar completament l'alternativa que hem proposat en la seva implementació, hauríem de disposar d'un petit prototip i veure el comportament a mesura que es va emplenant la base de dades fins a una mida considerable, ja que com indica l'anàlisi que hem realitzat podria ser un projecte del tot viable però necessitem saber fins a on pot arribar en relació a l'emmagatzematge d'adreces IP. Un dels punts clau seria comprovar l'efecte en el Tangle al realitzar transaccions modificant informació del *hashes* de les transaccions per veure el seu rendiment, però en principi el temps previst de cerca i inserció en l'anàlisi realitzat és adequat pel problema que estem tractant, com també les mesures proposades per poder controlar el creixement de la base de dades i que aquest no afecti el rendiment general del sistema.

Com a aspectes positius tenim que IOTA ens dona una gran escalabilitat i té un mecanisme de seguretat bastant diferent del PoW i PoS, a més de que amb la nostra proposta aconseguim una altra granularitat pel que fa l'emmagatzematge de les adreces de forma individual. Una altra punt es que ens alliberem de la centralització dels organismes que controlen cadascuna d'aquestes adreces i hi possibilitem més llibertat a les persones per poder-les gestionar còmodament. També tenim que si el sistema pogués aconseguir el llindar establert per treure el COO, aquest tipus d'implementació que proposem en aquest projecte podria ser contemplada, i en el cas d'èxit i amb un desenvolupament molt superior es podria arribar a un sistema més segur i recolzat per altres investigadors, fent-lo llavors possible en el context que tractem o extreure'n conclusions més realistes. Tot i que no s'ha explicat de manera extensa el tema del coordinador, aquest presenta un dubte a llarg termini per IOTA, ja que no sabem que podria passar si en el futur deixa d'existir, i si el fet de no ser-hi comportaria problemes a la seguretat del sistema.

Per últim, considerem que el nostre projecte té prou potencial per poder guardar les adreces IP fent servir la *chain* de IOTA. A partir d'aquí, el següent pas seria el de realitzar els canvis proposats per poder provar el model i el seu comportament, passant llavors a realitzar un estudi en ple funcionament. Depenent del resultat, és a dir, si realment és possible un bon funcionament en el Tangle de IOTA, es podrien comprovar els mecanismes de protecció, a més d'investigar o crear noves estructures que permetessin un millor temps de resposta tant en les consultes a la base de dades, ja que com hem demostrat en l'anàlisi teòric, el PoW presenta una millor escalabilitat i granularitat que el PoS, i aquesta característica és molt favorable en el context d'aquest treball, ja que necessitem el mínim temps possible entre transaccions tenint en compte la gran quantitat d'adreces IP que estem tractant.

11. Bibliografia

[1] IOTA Developers. IOTA Docs, [en línia]. Pàgina oficial de desenvolupadors de IOTA. Disponible en: https://dev.iota.org/ [2018, 12 de Febrer].

[2] Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, [en línia]. Web oficial de Bitcoin. Disponible en: https://bitcoin.org/bitcoin.pdf [2018, 1 de Febrer].

[3] Leslie Lamport, Robert Shostak, and Marshall Pease (1982). The Byzantine Generals Problem, [en línia].SRI International.
Disponible en: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf [2018, 1 de Febrer].

[4] Prof. Dr. Thorsten Strufe (2011). P2P networks lecture, [en línia]. Universitat tècnica Darmstadt. Disponible en: https://www.p2p.tudarmstadt.de/index.php?eID=tx_nawsecuredl&u=0&g=0&t=1523281475&*hash*=b459a3e75315e2632fc35add2df1d309121541bb&file=fileadmin/secured/P2P/p2pws10/Lecture_1_1.pdf [2018, 3 de Febrer].

[5] Security concepts - Symmetric cryptography, [en línia]. Web oficial de IBM. Disponible en: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html [2018, 3 de Febrer].

[6] Bitcoin protocol. Wiki oficial de Bitcoin, [en línia]. Disponible en: https://en.bitcoin.it/wiki/Protocol_documentation [2018, 3 de Febrer].

[7]Cryptocurrency Market Capitalizations, [en línia]. Disponible en: https://coinmarketcap.com/ [2018, 3 de Febrer].

[8] J. Paillisse, A. Rodriguez-Natal, V. Ermagan, F. Maino, Cisco Systems, A. Cabellos, UPC-BarcelonaTech (2017). An analysis of the applicability of *Blockchain* to secure IP addresses allocation, delegation and bindings, [en línea]. IETF Tools. Disponible en: https://tools.ietf.org/pdf/draft-paillisse-sidrops-*Blockchain*-01.pdf [2018, 9 de Febrer].

[9] NXT Wiki. What is NXT? , [en línia]. Disponible en: https://nxtwiki.org/wiki/Nxt_Wiki [2018, 10 de Febrer].

[10] NEO Developers. NeoContract *whitepaper*, [en línia]. Web oficial de NEO. Disponible en: http://docs.neo.org/en-us/sc/white-paper.html [2018, 11 de Febrer].

[11] Serguei Popov. The Tangle, [en línia]. Web oficial de IOTA. Disponible en: https://iota.org/IOTA_*whitepaper*.pdf [2018, 14 de Febrer].

[12] Dominik Schiener. IOTA Guide, [en línea]. Gitbook. Disponible en: https://domschiener.gitbooks.io/iota-guide/content/ [2018, 6 de Març].

[13] Junior Software Engineer Salary, [en línea]. Disponible en: https://www.payscale.com/research/ES/Job=Junior_Software_Engineer/Salary [2018, 18 de Març].

[14] Sr. Network Engineer Salary, [en línea]. Disponible en: https://www.payscale.com/research/ES/Job=Sr._Network_Engineer/Salary [2018, 18 de Març].

[15] Sr. Project Manager, [en línea]. Disponible en: https://www.payscale.com/research/ES/Job=Senior_Project_Manager%2c_IT/Salary [2018, 18 de Març].

[16] In depth explanation of how iota making a transaction, [en línia]. Disponible en: https://blog.louie.lu/2018/01/08/in-depth-explanation-of-how-iota-making-a-transaction/ [2018, 15 de Maig].

[17] IRI. IOTA Foundation, [en línia]. Repositori de la IRI. Disponible en: https://github.com/iotaledger/iri [2018, 25 de Maig].

[18] IOTA API. IOTA Foundation, [en línia]. Repositori de la API en JAVA. Disponible en: https://github.com/iotaledger/iota.lib.java [2018, 25 de Maig].

[19] RocksDB. Facebook, [en línia]. Base de dades RocksDB. Disponible en: https://github.com/facebook/rocksdb/wiki [2018, 24 de Maig].

[20] Fractional Cascading. Wikipedia, [en línia]. Fractional Cascading. Disponible en: https://en.wikipedia.org/wiki/Fractional_cascading [2018, 10 de Maig].

[21] Fractional Cascading. Computational Geometry Lab.Chapter 4 Fractional Cascading. Disponible en: http://cglab.ca/~morin/teaching/5408/notes/fractional_cascading.pdf [2018, 10 de Maig].

[22] IOTA *snapshot*. IOTA developer. IOTA *snapshot* and iri behind the scenes. https://blog.iota.org/the-april-29-2018-iota-*snapshot*-and-iri-1-4-2-4-behind-the-scenes-7e034babcd44 [2018, 20 de Maig].