Universitat Autònoma de Barcelona

Dipòsit digital de documents de la UAB

This is the **published version** of the bachelor thesis:

Rams Satué, Eric; Herrera-Joancomartí, Jordi, dir. Estudi de la criptomoneda Helium. 2021. (958 Enginyeria Informàtica)

This version is available at https://ddd.uab.cat/record/248504

under the terms of the BY-NC-ND license

Estudi de la criptomoneda Helium

Eric Rams Satué

Resum– La motivació principal d'aquest treball és demostrar que l'ús de la tecnologia blockchain és compatible amb l'àmbit de la tecnologia IoT podent substituir als proveïdors de serveis tradicionals. D'aquesta manera es pot veure el resultat d'aplicar aquesta tecnologia en una xarxa relativament nova explicant els punts principals en els quals es basa aquesta xarxa. Durant el desenvolupament d'aquest estudi es pot observar que encara que Helium es basi en la tecnologia blockchain, aquesta funciona d'una manera molt diferent comparada amb altres criptomonedes necessitant un algoritme propi per poder funcionar correctament. Al mateix temps aquest projecte presenta una nova manera de veure el funcionament de les xarxes IoT i com poder donar més poder als propietaris dels dispositius.
Paraules clau– Blockchain, Data Credits, Helium, HNT, Hotspot, IoT, LoRaWAN, Proof of Coverage, Token, Transaccions

Abstract– The main motivation of this project is to demonstrate that the use of blockchain technology is compatible with the field of IoT technology by replacing traditional service providers. In this way, the result of applying this technology to a relatively new network is appreciated by explaining the main points on which this network is based. During the development of this study, it can be observed that although Helium is based on blockchain technology, it works in a very different way compared to other cryptocurrency by using its own algorithm to work properly. At the same time, this project introduces a new point of view of how IoT networks work and how to give more power to the owners of the devices.

Keywords– Blockchain, Data Credits, Helium, HNT, Hotspot, IoT, LoRaWAN, Proof of Coverage, Token, Transactions

1 Introducció

L'augment de l'ús de la tecnologia blockchain en els darrers anys és inqüestionable. Aquest ús ve justificat per la possibilitat de fer servir aquesta tecnologia en molts sectors com el financer, el polític, l'habitatge, etc [1]. Possiblement l'aplicació de la tecnologia blockchain més coneguda és en l'ús de criptomonedes com Bitcoin i Ethereum [2, 3].

Quan parlem de blockchain és inevitable parlar de criptomonedes encara que no necessàriament ha de ser així. Podem diferenciar tres tipus de criptomonedes: les de reserva de valor, els security tokens i els utility tokens [4]. Criptomonedes com Bitcoin, Zcash o Monero pertanyen al primer grup, altres com Sia Funds, Bcap i Science Blockchain pertanyen al segon grup [5, 6, 7] i finalment altres com Filecoin, BAT i HNT pertanyen al tercer grup [8, 9, 10]. Pel que fa a la criptomoneda que s'estudia en aquest treball, es tracta d'un utility token. Un utility token permet l'accés futur a un producte o servei d'una empresa [11]. Un cop entès el propòsit d'aquest tipus de criptomonedes recalco que en aquest treball s'estudia el funcionament de la criptomoneda Helium però centrant-nos més en com funciona la blockchain que fa servir aquesta criptomoneda.

Helium es defineix com una xarxa de miners distribuïda i descentralitzada que proporciona connectivitat sense fils de gran abast per a dispositius IoT utilitzant la xarxa LoRaWAN. L'objectiu principal és que els miners proporcionin cobertura en tots els llocs possibles dels diferents països del món tal que els usuaris de la xarxa puguin enviar informació entre els seus dispositius. Aquesta xarxa seria una alternativa als proveïdors de serveis tradicionals en cas de voler transmetre informació entre dispositius però amb la diferencia que en aquesta xarxa es paga per la quantitat d'informació transmesa.

Aquest projecte es basa en tres pilars: l'ús de la tecnologia blockchain per poder enregistrar de manera fiable i segura tota la informació que es transmet per la xarxa, l'ús de l'algoritme *Proof of Coverage* per poder verificar que els dispositius estan col·locats en la localització on ells diuen estar i l'ús de la xarxa sense fils LongFi que combina el protocol LoRaWAN amb la blockchain d'Helium de manera que qualsevol dispositiu compatible amb LoRaWAN pugui transmetre dades per la xarxa Helium. En aquesta xarxa diferenciem dos actors: els miners que guanyen HNT

• E-mail de contacte: eric.rams@e-campus.uab.cat
• Menció realitzada: Tecnologies de la Informació
• Treball tutoritzat per: Jordi Herrera Joancomartí (DEIC)
• Curs 2020/21

(Helium Network Token) per proporcionar cobertura i per transmetre la informació dels usuaris i els usuaris que gasten DC (Data Credits) per poder enviar una certa quantitat d'informació. Per tant, existeixen dues monedes en aquesta xarxa, els HNT i els Data Credits.

2 Estat de l'art

Com s'ha esmentat abans, la tecnologia blockchain i les criptomonedes estan experimentant un fort increment en el seu ús. No obstant, Helium es va fundar al 2013 quan la tecnologia blockchain tenia uns índexs de popularitat molt més baixos que en l'actualitat. Aquest fet unit amb la poca infraestructura disponible per dispositius IoT, com per exemple sensors per la digitalització de ciutats (smart cities), van proporcionar la idea de poder millorar la infraestructura disponible i la capacitat de comunicació dels dispositius IoT, poden esdevenir la referencia en el sector d'IoT.

Aquest projecte va ser fundat l'any 2013 per Shawn Fanning, Amir Haleem i Sean Carey amb l'objectiu de poder connectar dispositius d'una forma més senzilla a l'existent en aquell moment. La directiva actual està formada per Amir Haleem (CEO), Marc Nijdam (CTO) i Frank Mong (COO), tots tres amb més de 20 anys d'experiència en el sector tecnològic. La seva idea a l'hora de crear aquest projecte consistia en poder connectar molts dispositius de baix consum que transmeten una baixa quantitat de dades i que es troben a una gran distancia entre ells. D'aquesta manera Helium es va convertir en la primera xarxa P2P sense fils del món. Sens dubte és un projecte orientat a dispositius IoT i que gràcies a la connectivitat LoRA s'aconsegueix comunicar dispositius a grans distancies, encara que recentment s'està estudiant utilitzar altres protocols sense fils com el 5G, 4G o WiFi per poder interactuar amb la blockchain i conviure al mateix temps amb la tecnologia LoRa.

La xarxa va començar a estar operativa al juliol de 2019 (la mainnet) permeten als dispositius començar a transmetre les primeres dades d'aquesta xarxa. Durant el mes de febrer, els desenvolupadors d'Helium van penjar a la pàgina web un llistat d'objectius per aquest any. Entre ells destaquen l'aprovació del HIP 25, començar a utilitzar la figura dels validadors, la creació d'una testnet, introduir la possibilitat de realitzar la multi-signatura i millorar l'eina *Console*.

3 Objectius

L'objectiu principal d'aquest treball és entendre el funcionament d'aquesta xarxa, les seves característiques, quins avantatges i inconvenients representa respecte a altres criptomonedes, com està estructurada i determinar la usabilitat i fiabilitat de la xarxa. Es busca comprovar i verificar que l'ús d'aquesta xarxa és l'opció més adequada per poder interconnectar dispositius d'IoT.

Com aquest projecte es pot estudiar des de molts punts de vista, aquest està centrat en l'apartat de blockchain però explicant de manera breu altres apartats perquè es pugui entendre tot el treball ja que totes les parts que conformen aquesta xarxa es troben relacionades.

Aquesta és la llista de tots els punts que s'han estudiat durant el treball:

- Objectius i estructura de la xarxa
- Tecnologia de xarxa utilitzada (LoRaWAN)
- Components de la xarxa: Hotspots, Usuaris i Helium Network Servers
- Rols dels Hotspots
- L'algoritme Proof of Coverage (PoC)
- L'Helium Consensus Protocol
- Comparació del Proof of Coverage amb el Proof of Work
- HNT i Data Credits: Tokens i principis econòmics de la blockchain
- Explicació general de la blockchain d'Helium
- La blockchain d'Helium: Blocs, epochs, transaccions i chain variables
- State channels: Enviament de dades als servidors
- Oracles i fees
- Comptes, wallets i criptografia

A llarg d'aquest informe final es fa un resum dels punts més importants. El estudi complet amb tots els detalls queda reservat pel dossier final.

Per tal de poder verificar aspectes com l'estructura d'un bloc i d'una transacció o altra informació s'ha fet servir la blockchain API proporcionada per Helium.

4 Metodologia

Per fer l'estudi d'aquesta criptomoneda s'ha decidit que el més adequat és fer servir una metodologia que faci una revisió dels avanços produïts cada una o cada dues setmanes per poder mantenir un control de la feina feta fins un cert moment i poder verificar que s'estan complint les dates fixades inicialment o si es necessari fer una replanificació. També és necessari que sigui aplicable a un grup de treball d'una sola persona.

Tenint en compte aquests requisits s'ha decidit utilitzar la metodologia Scrum. Scrum es caracteritza per fer entregues parcials i de manera constant del producte final. És útil quan es necessita obtenir resultats aviat i els requisits estan poc definits. D'aquesta manera, s'ha pogut fer l'estudi de manera progressiva amb petites entregues. Donada la dificultat de definir de manera exhaustiva els punts que s'estudien en aquest treball degut a que canvien constantment i a que contínuament s'afegeixen noves funcionalitats a la xarxa aquesta metodologia proporciona força flexibilitat.

En Scrum existeixen 3 rols importants: el Product Owner, el Scrum Master i el equip de desenvolupament. El Product Owner és l'encarregat de maximitzar el valor del treball de l'equip de desenvolupament i de parlar amb el client. El Scrum Master s'encarrega de que les tècniques Scrum s'apliquin correctament i tracta d'eliminar els impediments o inconvenients que sorgeixen en un sprint. Per últim, l'equip de desenvolupament s'encarrega de realitzar totes les tasques que el Product Owner desitgi. Com aquest treball és d'una persona, els tres rols seran executats per la mateixa.

A continuació, s'explica de manera detallada la planificació que s'ha dut a terme durant la realització del treball:

Cada dues setmanes es produeix una iteració amb l'excepció que en cas que hi hagi una entrega de l'informe de seguiment o informe final enmig d'alguna iteració llavors el sprint s'escurça per acabar just el dia abans de l'entrega. El primer dia de cada iteració es fa una selecció de requisits que consisteix en escollir les tasques que es duran a terme en aquest sprint. Aquestes tasques es troben en un tauler creat en la plataforma Trello, podent-hi afegir, suprimir o modificar tasques en cas que sigui necessari. Després es fa una planificació per distribuir les tasques durant aquest sprint.

Cada dia que s'ha fet alguna tasca del projecte, s'han hagut de respondre a tres preguntes (reunió de sincronització): *¿Què he fet des de l'última reunió de sincronització?*, *¿Què faré avui en el projecte?* i *¿Quins problemes tinc o em puc trobar per fer aquesta tasca?*.

Finalment l'últim dia de la iteració es fa una revisió de totes les tasques realitzades durant el sprint corresponent i una retrospectiva per comprovar que s'està avançant adequadament i veure quins problemes han sorgit durant el desenvolupament del sprint.

5 Resultats

Un cop definits tots els punts que s'estudiaran en aquest treball, s'ha fet un únic document on es recullen tots els punts esmentats anteriorment. Aquest document s'ha estructurat de manera que el lector pugui comprendre el funcionament de la xarxa Helium i la seva blockchain amb un nivell de coneixement força acceptable. En aquest cas, aquest document seria el punt central del estudi i conformaria gran part del dossier final.

5.1 Tecnologia de xarxa utilitzada - LoRaWAN

Una de les bases del projecte Helium és la connectivitat que utilitzen els seus components: LoRaWAN. Tant els sensors com els Hotspots utilitzen la tecnologia LoRaWAN per comunicar-se i enviar-se dades entre ells. LoRa es defineix com una tecnologia sense fils que fa servir una modulació en radiofreqüència patentada per Semtech. Destaca per tenir una alta tolerància a les interferències i una alta sensibilitat per rebre dades (-168db), baix consum (la vida útil de les bateries és de l'ordre d'anys), gran abast (entre 10 i 20 km) i baixa velocitat de transferència de dades (255b/s). Unes característiques que s'adapten força bé al camp d'IoT.

Aquest protocol necessita tres components: els gateways, els nodes i el network server. Els gateways són els encarregats de rebre i enviar la informació als nodes i els nodes són els dispositius finals (sensors per exemple) que reben i envien les dades de la xarxa. El network server sol estar gestionat per una entitat però en el cas d'Helium no es així. Un principi d'Helium és ser una xarxa descentralitzada, per tant el network server no pot estar gestionat per una organització. Cadascú té la possibilitat de tenir el seu LoRaWAN Network Server (LNS) i evitar dependre d'un únic LNS gestionat per una sola entitat.

5.2 Components

Aquesta xarxa té 3 components principals: els dispositius dels usuaris de la xarxa que envien i reben dades contínuament, els dispositius que fan servir els miners per poder cobertura als dispositius dels usuaris anomenats "Hotspots" i els routers (Helium Network Server) que són les aplicacions d'Internet que compren les dades xifrades dels Hotspots. Per poder fer servir la xarxa Helium per enviar dades entre dispositius es necessari que els dispositius compleixin els requisits especificats en el document LoRaWAN Specification v1.02 elaborat per l'entitat LoRA Alliance. Normalment aquests són sensors IoT, dispositius de baix consum els quals envien una quantitat petita de dades. D'altra banda tenim els dispositius que donen cobertura a aquesta xarxa: els Hotspots. Els Hotspots al seu torn fan les funcions de Packet Forwarder i d'Helium Miner. El Packet Forwarder seria la part encarregada de interactuar amb les freqüències de ràdio que emeten els sensors i rebre els paquets que aquestes transporten. En canvi, l'Helium Miner s'encarrega d'encaminar els paquets al router apropiat fent servir microtransaccions negociades via libp2p. Per últim, tenim els routers. Els routers, també anomenats LoRaWAN Network Servers per xarxes LoRa (*Helium Network Servers* en el cas de la xarxa Helium), són els encarregats de rebre els paquets provinents dels dispositius i gestionar les respostes per aquests quan sigui convenient. Per poder enviar informació entre els dispositius, un usuari/companyia necessita un Organizationally Unique Identifier (OUI). Els OUIs són identitats registrades en la blockchain d'Helium. Aquests són necessaris perquè un usuari de la xarxa pugui rebre paquets d'un dispositiu final. Però, no és obligatori tenir un OUI. Existeix la possibilitat de tenir el teu propi OUI o utilitzar-ne un gestionat per un tercer, com per exemple *Console* operat per Helium Inc. Cada LoRaWAN Network Server (LNS) d'Helium té un Organizationally Unique Identifier (OUI). Amb aquest identificador únic es pot registrar cada LNS en la blockchain.

La figura 1 ens mostra de forma gràfica com interaccionen els components de la xarxa Helium.

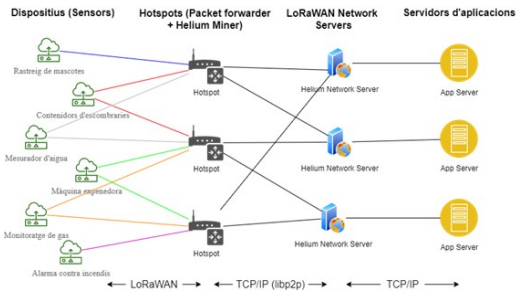

Fig. 1: Estructura de la xarxa Helium

Com s'ha esmentat abans els Hotspots fan la funció de Packet Forwarders i d'Helium Miners. Aquestes dues parts poden ser construïdes independentment de manera que no estiguin incloses en el mateix dispositiu.

5.2.1 Hotspots

Helium Inc va ser el primer fabricant de Hotspots capaços de minar HNT (Helium Token) i proveir cobertura LoraWAN. Actualment, Helium Inc ja no fabrica Hotspots.

La intenció era la de poder donar un primer impuls a la xarxa i que després s'unissin altres fabricants. Finalment, després de l'aprovació del HIP 19 s'han afegit diversos fabricants aprovats per la comunitat d'Helium [12]. A dia d'avui, aquests són els fabricants operatius: Nebra, SyncroB.it, RAK/CalChip, EasyLinkin/Bobcat i Kerlink. La majoria d'aquests dispositius estan formats per una Raspberry Pi 3/4 i un mòdul concentrador LoRa

Afegir que per tal de guanyar HNT s'ha d'adquirir algun dels Hotspots de la llista anterior. Si et montes el teu propi Hotspot (Packet Forwarder + Helium Miner) llavors no tindràs la capacitat de minar HNT encara que compleixis totes les condicions per poder minar.

5.2.2 Rols

Un dels components més importants d'aquesta xarxa són els Hotspots. Els Hotspots s'encarreguen de proporcionar cobertura als dispositius dels usuaris finals i d'entregar les dades als Helium Network Servers corresponents. La manera de compensar i incentivar als miners a complir aquesta tasca és donant Helium Tokens (HNT) als miners. Però, un Hotspot no només pot guanyar HNT fent la funcionalitat de gateway. Aquests poden participar en diferents activitats imprescindibles pel correcte funcionament de la xarxa i en cadascuna d'aquestes activitats els Hotspots tenen un rol diferent. Recalcar que un Hotspot pot tenir més d'un rol alhora, tot depèn de les circumstancies en les que es troba.

Un Hotspot pot guanyar HNT si forma part d'algun d'aquests rols:

- PoC Challenger
- PoC Challengee
- Witness
- Consensus Group
- Security
- Network Data Transfer

El PoC Challenger es tracta del Hotspot que ha creat un PoC challenge amb èxit i l'ha penjat a la blockchain. Aquest PoC challenge és necessari per poder desenvolupar l'algoritme Proof of Coverage correctament.

Els PoC Challengees són els Hotspots que han transmès un paquet de PoC creat per un Challenger després de ser seleccionats per ell.

Els Witnesses són els Hotspots que observen el seu entorn en busca d'algun paquet de PoC (beacon) transmès per part d'algun Challengee que vulgui confirmar la seva posició.

El Consensus Group són un grup de 16 Hotspots seleccionats prèviament i que van canviant contínuament. Aquests són recompensats amb HNT per validar i pujar les transaccions a la blockchain.

El Security Group està format per Helium Inc. i altres inversors que posseeixen Security Tokens. Aquest grup guanya HNT per haver fet una inversió prèvia al començament d'aquest projecte i confiar en el seu desenvolupament.

Per últim, també es pot guanyar HNT encaminant dades provinents de sensors LongFi, sensors pertanyents a la xarxa Helium. Actualment no hi ha moltes transaccions d'aquest tipus degut a que la infraestructura encara està creixent.

5.3 Blockchain

El fet de descentralitzar la xarxa d'Helium té un inconvenient important: com mantenir de forma activa la infraestructura i poder atraure a nous usuaris. Si això es fes de forma centralitzada el sistema seria ben fàcil, la companyia faria pagar una quota als seus clients per fer servir la seva infraestructura i així poder mantenir la xarxa actual i obtenir beneficis. Però tenint en compte que els Hotspots que donen cobertura a la xarxa pertanyen a diferents persones no es poden repartir els beneficis econòmics de la mateixa manera que amb un sistema tradicional. Per recompensar a cada usuari de forma justa, clara i còmoda es va decidir adoptar la tecnologia blockchain per poder enregistrar els moviments que es produeixen en la xarxa de forma fiable. Si un Hotspot transmet més dades que un altre, aquest guanyarà més recompenses i per tal de demostrar-ho es podrà veure a la blockchain tot el treball que ha realitzat. Afegir que les adreces de la blockchain es troben pseudoanonimitzades pel que sempre es podran veure les accions dels usuaris però sense afectar a la seva privacitat.

Els conceptes bàsics que conformen la blockchain d'Helium són: els blocs, les epochs, les transaccions i les chain variables. A continuació s'explicaran aquests conceptes.

5.3.1 Blocs i Epochs

Els blocs estan formats per un conjunt de transaccions i es minen en un termini fixat de temps indicat en la chain variable *block time*. Actualment el block time és de 60000 mil·lisegons (60 segons). Això significa que cada bloc tarda en ser minat aproximadament 60 segons.

Un bloc està format pels següents camps: la versió, la altura (height), el hash del bloc anterior, les transaccions (guardades com un arbre de Merkle) i la signatura del Consensus Group corresponent a la epoch en què es va crear el bloc.

Aquest es un exemple de com es veuen tots els camps d'un bloc fent servir l'API.

```
ericrams@ubuntu:~$ GET https://api.helium.io/v1/blocks/793898
{"data":{"transaction_count":85,"time":1617808509,"snapshot_hash":"","prev_hash
":"QWFB5XJMpFz1eWYRr0GPSTrKdgN35pAvvyOSkUHDh78","height":793898,"hash":"uiot-Fl
xZkMHgxopbzK3L7Lf_PXuMt--rDhxjDwEGM4"}}ericrams@ubuntu:~$
```

Fig. 2: Bloc vist des de l'API d'Helium

Una epoch és el temps en el què un grup de Miners són escollits per formar part del Consensus Group. Tal i com està definit en la chain variable *election interval* una epoch són 30 blocs.

D'aquesta forma cada 30 blocs un nou Consensus Group és escollit. Al final de cada epoch es distribueixen tots els HNT, a diferencia d'altres sistemes com Bitcoin que reparteixen les recompenses en cada bloc. En el cas del Consensus Group aquestes recompenses són distribuïdes fent servir una transacció de tipus *rewards*.

5.3.2 Transaccions

Actualment, la blockchain d'Helium té 20 tipus diferents de transaccions però només unes poques són utilitzades habitualment, com per exemple *poc receipt* i *poc request*. En canvi, altres només s'han fet servir un cop i ja no serveixen per res més. A continuació, es citen algunes de les transaccions més importants:

- **data credits:** Aquesta transacció crema HNT per convertir-los en Data Credits seguint el preu actual que marquen els oracles.
- **payment:** Transacció per fer un pagament des d'un wallet a un altre.
- **poc request:** Transacció pujada per un miner amb la intenció d'iniciar un challenge.
- **poc receipt:** Transacció resultant d'un challenge enviat a la xarxa un cop s'ha completat.
- **state channel open:** Obre un nou canal d'enviament de dades entre un Hotspot i un router d'Helium (OUI).
- **state channel close:** Tanca un canal d'enviament de dades entre un Hotspot i un router d'Helium (OUI).
- **consensus group**: Marca l'elecció d'un nou Consensus Group per a la propera epoch.
- **chain vars:** Serveix per modificar una chain variable. Només els usuaris que coneguin la master key poden pujar aquesta transacció a la blockchain.

Totes les transaccions poden ser vistes en detall fent servir l'Helium Blockchain Explorer o l'API. En aquest cas, es mostra un exemple de com es veu una transacció de tipus *poc request* fent servir l'API.

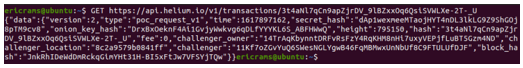

Fig. 3: Exemple de transacció poc request vista des de l'API d'Helium

5.3.3 Chain variables

Les Chain Variables, també conegudes com *chain vars*, són una sèrie de paràmetres de configuració de la blockchain d'Helium. Les Chain Variables defineixen alguns paràmetres com per exemple el temps en el que es mina un bloc, el temps que dura una epoch, el nombre mínim de targets en un PoC challenge, etc. Per poder modificar alguna chain variable és necessari pujar una transacció de tipus *chain vars* indicant la chain variable a canviar, el seu nou valor i una signatura de la chain variable master key. Evidentment, només els desenvolupadors tenen aquesta master key.

5.3.4 HNT i Data Credits

Helium fa servir dos tipus de tokens: HNT (Helium Token) i Data Credits (DC). Els HNT són la recompensa que es dóna als Hotspots per exercir alguns dels rols explicats anteriorment. En canvi, els Data Credits només es fan servir per pagar les fees de les transaccions, usualment per les transaccions d'enviament de dades.

Com s'ha esmentat anteriorment els Hotspots guanyen HNT per donar cobertura però aquests tokens també son utilitzats pels usuaris de la xarxa Helium per poder enviar i rebre dades dels seus dispositius IoT. Per fer això es necessària una conversió d'HNT a Data Credits. Els DC s'obtenen "cremant" HNT (conversió HNT a DC).

Actualment, la xarxa d'Helium té com objectiu produir 5.000.000 d'HNT mensualment. Si tenim en compte que una epoch són 30 blocs, en un mes hi ha 1460 epochs. I si es produeixen 5.000.000 HNT per mes llavors en cada epoch es generen 3424,6575 HNT. És important recalcar que les recompenses sempre es reparteixen al final de cada epoch, a diferencia d'altres blockchains com la de Bitcoin.

En la figura 4 s'explica com estan distribuïdes les recompenses d'acord amb el HIP 10 que és la distribució utilitzada actualment [13].

Reward Type	Percentage	HNT Earned by Reward Type
PoC Challenger	.95%	32.53427
PoC Challengees	5.31%	181.849446
Witnesses	21.24%	727.397784
Consensus Group	6%	205.4796
Security Tokens	34%	1164.3844
Network Data Transfer	*Up to 32.5%*	*Up to 1113.0145*
Total	**100%**	**3424.66**

Fig. 4: Taula de distribució dels HNT entre els diferents rols

Aquesta distribució va canviant al llarg dels anys donant cada cop més pes al Network Data Transfer i reduint el pes dels altres rols.

Pel que fa als participants de l'algoritme PoC (Challengers, Challengees i Witnesses), aquests guanyaran el nombre d'HNT proporcionals al nombre d'esdeveniments en els quals hagin participat respecte al total d'esdeveniments de cada epoch. De manera similar, les recompenses que obtindrà cada Hotspot que participi en el Network Data Transfer seran proporcionals a la quantitat de dades que hagin transferit respecte al total de cada epoch.

Els Hotspots que participin en més d'un rol guanyaran les recompenses corresponents a cadascun d'aquests rols al final de cada epoch.

Però, hi ha un problema. Aconseguir una sincronització entre els temps en què es mina un bloc i el temps que dura una epoch és una tasca dificultosa. Per aconseguir-ho, Helium fa servir un mecanisme anomenat *proration* per assegurar l'objectiu de 5.000.000 HNT.

La clau per aconseguir això consisteix en què els HNT produïts depenen dels blocs produïts i no del temps consumit en minar un bloc. Conseqüentment, si els blocs tarden molt en ser minats llavors la producció d'HNT es veurà reduïda de manera proporcional.

Destacar que quan la producció d'HNT es veu reduïda degut a la lentitud en la que surten els blocs, l'impacte és equitatiu per tots els participants en activitats relacionades amb la distribució d'HNT a excepció dels membres del Consensus Group.

5.3.5 Principis econòmics de la blockchain

La blockchain d'Helium es basa en 3 principis de caire econòmic: una quantitat màxima limitada d'HNT, el sistema Burn-and-Mint i les Net Emissions.

El màxim d'HNT es troba fixat en 223.000.000 HNT des d'aprovació del HIP 20. En realitat, el màxim d'HNT fixat inicialment era de 240.000.000 HNT però com en el primer any de la blockchain només es van produir 43.000.000 HNT dels 60.000.000 HNT previstos inicialment hi ha 17.000.000 HNT que s'han perdut per sempre. La blockchain d'Helium està programada per fer un halving cada dos anys.

D'altra banda, el sistema burn-and-mint es basa en la relació entre els HNT i els Data Credits. Un DC sempre val el mateix, 0,00001 dòlars o el què es el mateix 1 dòlar sempre equivaldrà a 100.000 DC. En el cas de l'HNT, aquest també té un preu en USD però aquest preu va variant en funció del que marquin els oracles. L'objectiu d'aquest sistema és què el subministrament de HNT respongui a les tendències d'ús de la xarxa, de forma que quan es troba l'equilibri, la quantitat d'HNT roman estable mes a mes.

Per poder entendre millor aquest sistema posarem 2 exemples:

Exemple 1: Imaginem que el preu actual de l'HNT és d'1 dòlar. Sabem que el preu del DC sempre és de 0,00001 dòlars. Llavors, si cremem 1 HNT llavors obtindrem 100.000 DCs (1/0,00001).

Exemple 2: Ara imaginem que un usuari de la xarxa Helium necessita 50.000 DCs al mes per poder enviar dades als seus sensors. Com sempre, el preu del DC és de 0,00001 dòlars i el preu actual de l'HNT és de 2 dòlars. Si cremem 1 HNT obtindrem 200.000 DCs, el doble que en el exemple anterior. Per tant si volem 50.000 DCs, només necessitem 0,25 HNT (50.000/200.000).

Si el preu de l'HNT puja, es necessitarà cremar menys HNT per obtenir el mateix nombre de DCs. En canvi, si el preu de l'HNT baixa, es necessitarà cremar més HNT per obtenir el mateix nombre de DCs.

L'últim principi econòmic són les Net Emissions. Aquest concepte va ser introduït en el HIP 20 i encara no s'ha activat [14].

Si fem un repàs a tot el que hem vist fins ara, podríem arribar a la conclusió de que si la blockchain està cremant HNT contínuament i el nombre d'HNT està limitat llavors en algun moment la blockchain podria quedar-se sense.

Per poder evitar aquesta situació existeixen les Net Emissions. El seu objectiu és quantificar el nombre d'HNT què es fan servir per ser transformats en DCs i afegir aquest nombre d'HNT al nombre d'HNT que s'havien de donar en un principi en una epoch. Si per exemple es cremen 10 HNT en una epoch llavors la blockchain afegirà 10 HNT al sistema de recompenses inicial.

Però, hi ha un inconvenient. Si tots els HNT cremats son substituïts per uns de nous llavors les Net Emissions anul·larien la deflació provocada pel Burn and Mint. Per evitar que passi això, el nombre d'HNT que són restaurats via Net Emissions per epoch està limitat. Si el nombre d'HNT cremats supera aquest límit llavors hi haurà una reducció en el nombre total d'HNT.

Aquest límit està fixat en el 1 per cent d'HNT que es donen per epoch. Com actualment es donen 3424,66 HNT per epoch, llavors el límit està situat en 34,24 HNT. Si el nombre de DC generats durant una epoch no supera els 34,24 HNT llavors els HNT restants seran repartits entre els participants del PoC. Però, si es cremen més de 34,24 HNT en una epoch determinada, el sistema BME pot iniciar-se de nou per desinflar l'oferta d'HNT i augmentar el seu preu fins assolir l'equilibri.

5.3.6 State channels

Per tal d'efectuar l'enviament de dades dels dispositius a la seva destinació final es necessita obrir un state channel.

Els state channels són canals oberts pels 2 extrems oberts per un OUI operator. Amb una transacció de tipus *state channel open*, l'operator gasta 2 cops el nombre de Data Credits disponibles per ser gastats en aquest canal. Addicionalment, la quantitat de blocs fins que el canal desaparegui es troba fixada (block expiration). Un cop el canal s'ha obert, Hotspots i OUIs ja poden transferir dades pel canal. Primer, el hostpot ofereix transmetre un paquet a l'OUI operator però el hostpot no mostra el payload del paquet, només ensenya certes metadades. Després, l'OUI operator decideix si comprar el paquet o no. En cas afirmatiu, la oferta es signada i el paquet es entregat del hostpot a l'OUI operator. Totes les ofertes signades són afegides al "banner" del state channel, el que permet al dispositiu poder confirmar que se li recompensarà durant el temps de vida del state channel. Això és possible fins i tot si altres hotspots tenen les seves transaccions afegides al mateix banner.

En algunes ocasions, l'OUI operator pot pujar la transacció de tipus *state channel close* abans del bloc d'expiració fixat en la transacció *state channel open* corresponent.

Aquesta transacció també mostra quants Data Credits es cremaran en nom dels hotspots participants. En cas que un Hotspot no sigui recompensat de manera adequada, aquest pot presentar una disputa durant un "temps de gràcia" (10 blocs després del tancament del canal) fent servir les ofertes signades com a prova. Per poder obrir una disputa, el Hotspot ha de pujar una transacció de tancament de canal *(state channel close)* alternativa.

Si no hi ha cap disputa, la meitat de la inversió inicial i qualsevol crèdit restant són retornats a l'OUI operator. En cas contrari, la inversió completa es congela i, en cas de disputa, es paga la quantitat apropiada de Data Credits cremats als Hotspots que guanyin la disputa.

Per últim, si l'operator no tanca l'state channel abans del bloc d'expiració llavors s'acceptaran tancaments per part de tots els participants durant el temps de gràcia. Si encara i així, l'OUI operator no tanca el canal, perdrà tota la inversió.

5.4 Oracles i fees

5.4.1 Oracles

La blockchain d'Helium fa servir un sistema d'oracles per fixar el preu de canvi de USD a HNT i així poder fer la conversió d'HNT a Data Credits. Es tracta d'un sistema de preus descentralitzats basat en l'ús d'oracles de la Maker Foundation [15].

Per definir el preu, 9 oracles fixen el preu de canvi de forma periòdica. Un cop la blockchain té suficient dades sobre el nou preu, aquesta calcularà un nou preu HNT/USD que

romandrà vàlid fins que un cert nombre d'oracles presentin nous preus diferents al actual provocant una revisió del mateix.

Aquests 9 oracles estan formats per empreses, organitzacions i persones: 7 membres anònims pertanyents a la comunitat d'Helium, Helium Inc i Decentralized Wireless Alliance (DEWI). Els noms dels membres s'han decidit mantenir-los anònims per evitar intents externs d'extorsió o xantatge. En canvi, les claus publiques dels 9 HNT Price Oracles estan publicades en l'apartat "Documentation" de la pàgina web d'Helium.

Cada 10 blocs (aproximadament cada 10 minuts) la blockchain intentarà establir un nou preu HNT/USD.

Aquests són els passos per establir un nou preu de la criptomoneda: Primer, la blockchain busca nous preus que hagin pujat els Oracles fent servir una transacció de tipus *price oracle submission*. Un enviament de preu vàlid és qualsevol transacció del tipus que hem vist anteriorment que hagi estat pujada a la blockchain en les últimes 25 hores i porti més d'una hora penjada. Això permet a la blockchain calcular una mediana final de 24 hores alhora que manté un buffer en el que guarda les entrades de preu atípics (outliers) en els darrers 60 minuts.

Si hi ha suficients enviaments de preu vàlids en una finestra de 24 hores, un nou preu serà establert. Perquè això passi, és necessari que la majoria d'oracles ((N/2)+1) hagin pujat un preu durant la finestra. Seguint la fórmula anterior, es necessiten com a mínim 5 dels 9 oracles per canviar el preu. En cas contrari, no es calcula un nou preu. Si hi ha almenys 5 nous preus, es procedeix a ordenar els preus en una llista de menor a major i s'agafa la mediana com a preu vàlid. Per exemple, si tenim 7 enviaments de preu vàlids i els ordenem de menor a major quedant així: 0.20 USD, 0.22 USD, 0.235 USD, 0.238 USD, 0.25 USD, 0.27 USD, 0.45 USD. La blockchain seleccionarà 0.238 USD com a preu vàlid fins que un nou preu sigui establert (10 blocs com a molt aviat).

Per poder pujar un nou preu per l'HNT, és necessari penjar una transacció del tipus *price oracle submission* signada per una clau privada associada a una de les 9 claus publiques pertanyents als oracles. Actualment, els oracles fan servir l'Helium Wallet CLI per pujar aquestes transaccions.

5.4.2 Fees

Per poder fer una transacció d'enviament de dades a la blockchain d'Helium és necessari pagar unes fees en Data Credits per pujar-la. Aquests Data Credits es generen cremant una certa quantitat d'HNT. Gràcies a un sistema anomenat "Implicit Burn", els usuaris no necessiten subministrar els DC manualment per pagar les fees. En cas que l'Helium wallet que s'utilitzi per enviar la transacció contingui suficients HNTs per poder pagar la transacció incloent les fees, alhora de produir-se el canvi d'HNT a DC, en aquest ja se inclouran els Data Credits per pagar les fees.

En la següent taula es mostren la quantitat de fees en Data Credits que s'han de pagar en cada tipus de transacció:

Crida l'atenció que la transacció per enviar HNT tingui un cost variable pel que fa a les fees. Aquest cost es basa en la mida de la transacció en bytes. Un cop la mida és calculada, s'aplica un multiplicador de 5000x. Un exemple d'una transacció típica d'enviament d'HNT d'un wallet a un altre seria així:

Fee Type	Fee Description	Cost (DC)	Cost ($USD)
Send HNT	Transferring HNT from wallet to wallet	`Variable`	`Variable`
Transferring Device Packet Data	Fee paid by device owner when sending or receiving sensor data. Metered per 24 bytes.	`1`	`$.00001`
Add Miner	Fee paid to add Miner to the blockchain. (**Only applies to non-Helium Hotspots.)**	`4000000`	`$40`
Assert Miner Location	Required when asserting a Gateway's location. (The **first two assertions** for Helium Hotspots are paid by Helium, Inc.)	`1000000`	`$10`
Purchasing a blockchain OUI	Buy an OUI from the Helium blockchain	`10000000`	`$100`
Purchasing a blockchain Subnet	Buy a Subnet from the Helium blockchain	`10000000`	`$100`

Fig. 5: Taula amb els costos de les fees de cada tipus de transacció

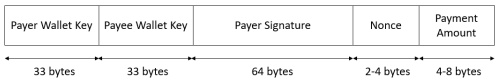

Fig. 6: Composició d'una transacció d'enviament d'HNT

Si sumem la mida de tots els camps, en total tenim 139 bytes (agafem 3 bytes pel nonce i 6 bytes pel payment amount). Cada 24 bytes s'ha de pagar 1 DC (igual que amb una transacció per enviar dades entre dispositius). Per tant, si volem enviar 139 bytes necessitem 6 Data Credits (139 / 24 = 5,79). Per últim, s'aplica el multiplicador de 5000x i com a resultat obtenim que el cost en fees de la transacció és de 3000 DC.

5.5 Proof of Coverage

L'objectiu d'aquest algoritme és verificar que els Hotspots es troben on ells afirmen estar. Si especifiquem més, es tracta de assegurar que els Hotspots proporcionen cobertura a la xarxa Helium en una zona concreta.

L'èxit de la xarxa Helium recau en la quantitat de cobertura que proporcionen els miners als dispositius dels usuaris finals. Un objectiu tant específic necessita un algoritme propi. D'aquesta necessitat neix aquest algoritme.

La blockchain fa servir un mecanisme anomenat "PoC Challenge". Les dades generades per les proves fetes als Hotspots, s'emmagatzemen en la blockchain d'Helium i serveixen com a prova que certs Hotspots estan proporcionant cobertura. Podríem definir el challenge com la unitat de treball del PoC.

En aquest procés participen 3 rols que ja s'han anomenat anteriorment: El Challenger, el Transmitter (o Challengee) i el Witness.

Primer, el Challenger crea un challenge i el puja a la blockchain. En el cas del Challenger, els Hotspots solen emetre challenges aproximadament 1 cop cada 240 blocs. Per crear un challenge, el Challenger genera un parell de claus publiques i privades efímeres. Un hash SHA256 de la clau pública i privada són pujats a la blockchain juntament amb el hash del bloc actual, com un PoC Request. Si la sol·licitud és vàlida i acceptada per la blockchain, el hash del bloc on apareix el PoC Receipt es combina amb el hash de la clau pública efímera i la identitat del Challenger per

generar una entropia verificable. Un nombre aleatori uniforme generat a través d'aquesta entropia és utilitzat per a seleccionar qui serà el Transmitter.

Després de crear el challenge packet, aquest és lliurat al Trasmitter a través de la xarxa Peer-to-Peer d'Helium. L'objectiu del Transmitter és poder demostrar que ell està donant cobertura a la xarxa en la posició on va dir inicialment que estava. El Transmitter rep el challenge packet, desxifra la capa més externa utilitzant la seva clau privada i la clau pública efímera (aquest clau publica efímera apareix en el paquet de PoC i el Hotspot que rep aquest paquet pot inspeccionar la blockchain buscant un PoC Receipt amb el SHA256 corresponent de la clau efímera), i immediatament transmet el paquet resultant (beacon) a la xarxa d'Helium. Aquest paquet no té un receptor assignat i qualsevol Hotspot que es trobi geogràficament a prop el pot veure i reportar l'existència d'aquest paquet a la blockchain. En cas que algun Hotspot vegi algun beacon dintre del seu rang, aquest adquireix el rol de "Witness" i serveix per confirmar la posició del Transmitter.

Una vegada que el Challenger té el conjunt complet de receipts de PoC dels Witnesses i del Transmitter, o el temps transcorregut des que el repte va ser emès ha passat el límit, el PoC Challenge es considera complert. En aquest punt, el Challenger puja el PoC Receipt com una transacció a la blockchain per ser verificada pel Consensus Group actual. Com que els passos donats pel Challenger per construir i completar la prova són deterministes i fàcilment reproduïts, els membres del Consensus Group poden verificar la legitimitat de la prova. Concretament, el Challenger revela la clau efímera secreta que va utilitzar tant per obtenir la PoC request original com per xifrar cada capa del paquet del challenge. Aquesta informació crucial, que s'ha ocultat fins que es publica el receipt, permet la recreació de l'entropia determinista.

5.6 Helium Consensus Protocol

Totes les transaccions vistes anteriorment no són pujades directament a la blockchain per part dels Hotspots sinó són pujades i verificades pels membres de l'Helium Consensus Group.

L'Helium Consensus Protocol està basat en una variant del HoneyBadgerBFT (HBBFT) protocol [16]. L'HBBFT és un protocol de difusió atòmica asíncron dissenyat perquè un grup de nodes coneguts pugui arribar a un consens sobre enllaços poc fiables. En el cas d'Helium, es forma un Consensus Group (CG) d'Hotspots. La seva missió consisteix en rebre transaccions encriptades i arribar a un acord per poder ordenar aquestes transaccions abans de formar un bloc i afegir-lo a la blockchain. HBBFT es basa en un esquema de seguretat conegut com threshold encryption. Utilitzant aquest esquema, les transaccions es xifren amb una clau pública compartida i només es poden desxifrar quan el Consensus Group treballa conjuntament per desxifrar-les. El fet d'utilitzar el threshold encryption permet al Consensus Protocol d'Helium aconseguir transaccions resistents a la censura.

Com s'ha esmentat anteriorment, un nou Consensus Group es escollit en cada epoch. Actualment es trien 16 membres per formar part de cada Consensus Group, tal i com es troba definit en la chain variable *num consensus members*. A partir de l'aprovació del HIP 16, tots els Hotspots que es trobin actius poden ser escollits per formar part del Consensus Group [17]. Aquests són seleccionats a l'atzar encara que hi ha certes variables que fan que aquesta aleatorietat no sigui pura.

Un filtre geogràfic és aplicat per assegurar que hi hagi una diversitat d'ubicacions adequada per part dels Hotspots. La blockchain d'Helium utilitza un sistema anomenat H3 (Hexagonal Grid) per fer una representació geoespacial de la xarxa [18]. Actualment, la resolució H4 és la triada com a filtre per escollir els diferents Hotspots d'un Consensus Group.

En cada elecció per formar part del Consensus Group es produeix una migració de només un subconjunt dels membres del CG existent durant una sèrie de epochs. Concretament, cada Consensus Group nou que es forma manté 12 dels 16 membres anteriors. 4 membres són seleccionats per formar part del nou Consensus Group i els altres 12 provenen de l'anterior. Això es fa per fer premiar als membres del CG que han demostrat una bona actitud i capacitat per minar blocs i distribuir HNT.

Un cop seleccionat, un Hotspot pot formar part de fins a quatre CG consecutius. Els membres del CG que proporcionin un baix rendiment és més probable que siguin expulsats abans d'arribar a les 4 epochs consecutives. Per últim, una vegada que un Hotspot és expulsat d'un CG, no podrà elegir-se per formar part d'un altre grup fins que els altres 15 membres del seu grup quedin eliminats (això serien 4 epochs).

Un altre fet important que succeeix durant l'elecció del nou Consensus Group és la generació de claus distribuïdes per iniciar la creació d'una threshold encryption key (TPKE). Aquesta TPKE és una primitiva criptogràfica que permet a qualsevol Hotspot de la xarxa encriptar transaccions amb una master public key de forma que els membres del Consensus Group hagin de treballar conjuntament per desencriptar-les. Els Hotspots van pujant noves transaccions constantment. A mida que van arribant, cada membre del Consensus Group agafa un subconjunt aleatori i reenvia aquestes transaccions als altres membres del grup després d'haver-les desencriptat parcialment amb la seva part de la master public key.

Al final de cada epoch, les recompenses són distribuïdes pel Consensus Group a les adreces dels wallets que les hagin aconseguit participant en els diferents rols.

6 Conclusions

Helium és l'exemple perfecte de com fusionar la tecnologia blockchain i la xarxa d'IoT per poder oferir una xarxa a nivell global diferenciada del sistema tradicional ofert pels proveïdors de serveis. Amb unes petites modificacions dels components tradicionals que composen una xarxa LoRa han estat capaços de descentralitzar-la i poder involucrar a persones de tot el món a participar-hi ja sigui donant cobertura a la xarxa amb un Hotspot o adquirint sensors per enviar les seves dades a través d'aquesta innovadora xarxa. No obstant això, dissenyar aquesta xarxa no ha estat gens fàcil. S'ha hagut de crear un nou algoritme conjuntament amb la blockchain per poder assegurar la cobertura de la xarxa. També ha estat clau la decisió d'escollir LoRa com a tecnologia de xarxa degut als seus avantatges respecte a les

altres opcions com per exemple la llarga distancia del seu senyal. Adaptar els dispositius perquè siguin compatibles amb la xarxa d'Helium també ha estat més fàcil gracies a la connectivitat LoRa.

Confeccionar una nova blockchain ha significat dissenyar nous blocs, transaccions, variables i definir aspectes bàsics del seu funcionament com el temps en que es mina cada bloc, la criptografia utilitzada i els tokens a fer servir.

Finalment, es va decidir utilitzar 2 tokens: l'HNT per un ús general i els Data Credits per pagar les fees de les transaccions. Aquests tokens es troben en equilibri gràcies a certes polítiques econòmiques com un nombre màxim d'HNT, el Burn-and-mint i les Net Emissions. Aquests principis treballen conjuntament per mantenir el valor de la criptomoneda i assegurar la supervivència d'aquesta entre la gran varietat de criptomonedes que existeixen a dia d'avui.

És important recordar que l'objectiu d'aquesta moneda no és esdevenir una reserva de valor sinó convertir-se en una xarxa d'IoT que apliqui la tecnologia blockchain per poder transmetre informació mitjançant l'ús de transaccions.

Pel que fa als objectius que s'havien proposat al principi d'aquest projecte, aquests s'han complit amb éxit. S'ha aconseguit compendre el funcionament de la xarxa d'Helium, els seus objectius, la seva estructura i totes les parts que la composen. L'explicació dels diferents apartats de la memòria reflecteix el coneixement adquirit estant aquest resumit en l'informe final. L'únic objecitu marcat al principi del desenvolupament del projecte i que no s'ha aconseguit és la construcció d'un packet forwarder fent servir una Raspberry Pi 4 i un LoRa HAT. Això és pel fet que no va haver-hi suficient temps per poder fer aquesta tasca i també a l'elevat cost que suposava comprar el material per construir el packet forwarder.

7 Futures línies de treball

Al tractar-se d'una xarxa bastant nova hi ha molts canvis en el seu funcionament en un curt període de temps. El ritme de propostes i aprovacions de nous HIPs (Helium Improvement Proposoal) és molt alt i això permet modificar i afegir noves característiques a la xarxa. Un altre factor important és el limitat temps per fer el treball que t'obliga a adaptar els teus objectius de fins a quin nivell de detall es pot arribar. Algunes de les millores o ampliacions que es podrien dur a terme per millorar el treball són:

- Estudi sobre la figura dels validadors i el seu efecte sobre el Consensus Group.
- Estudi sobre la introducció de la tecnologia 5G en la xarxa d'Helium. Tant els Hotspots com els dispositius podrien fer servir aquesta tecnologia conjuntament amb LoRaWAN. S'hauria d'investigar com es faria la unió de la blockchain actual amb la tecnologia 5G o si es faria servir una blockchain nova.
- Construcció d'un packet forwarder per a poder comprovar de primera mà el funcionament de l'eina *Console* i fer proves del funcionament de la xarxa.
- Estudi sobre els Lights Hotspots. Els Lights Hotspots són una alternativa als Hotspots tradicionals amb la diferencia que la seva potència de càlcul és limitada, de manera que depenen del serveis del cloud per al minat.

8 Agraïments

Agrair sobretot la confiança i el suport que m'ha donat el meu tutor Jordi Herrera durant la realització del treball. Sens dubte, no hauria estat possible treure aquest projecte endavant sense els seus consells i el seu gran coneixement en el camp de la tecnologia blockchain. També vull agrair el suport que m'han donat els meus amics de la universitat amb qualsevol incidència que ha pogut sorgir. Per últim, agrair a la meva família tots els ànims que m'han donat en tot moment.

Referències

[1] FinTech, "Aplicaciones de la tecnología blockchain," 2021. [En línia]. Disponible: https://www.fintech.es/2016/10/aplicaciones-de-la-tecnologia-blockchain.html

[2] A. M. Antonopoulos, "Mastering bitcoin: Programming the open blockchain," 2017. [En línia]. Disponible: https://github.com/bitcoinbook/bitcoinbook

[3] G. W. A. M. Antonopoulos, "Mastering ethereum: Building smart contracts and dapps," 2018. [En línia]. Disponible: https://github.com/ethereumbook/ethereumbook

[4] Multicoin.capital, "New models for utility tokens," 2021. [En línia]. Disponible: https://multicoin.capital/2018/02/13/new-models-utility-tokens/

[5] "Sia tech," 2021. [En línia]. Disponible: https://sia.tech/

[6] "Blockchain capital," 2021. [En línia]. Disponible: https://blockchain.capital/

[7] "Science blockcahin," 2021. [En línia]. Disponible: https://www.science-inc.com/blockchain.html

[8] "Filecoin," 2021. [En línia]. Disponible: https://spec.filecoin.io/

[9] "Basic attention token," 2021. [En línia]. Disponible: https://basicattentiontoken.org/

[10] "Helium inc," 2021. [En línia]. Disponible: https://www.helium.com/

[11] A. bit2me, "Què és un utility token," 2021. [En línia]. Disponible: https://academy.bit2me.com/que-es-utility-token/

[12] "HIP 19" 2021. [En línia]. Disponible: https://github.com/helium/HIP/tree/master/0019-third-party-manufacturers

[13] "HIP10: Usage-based Data Transfer Rewards" 2020. [En línia] Disponible: https://github.com/helium/HIP/blob/master/0010-usage-based-data-transfer-rewards.md

[14] "HIP 20: HNT Max Supply" 2020. [En línia] Disponible: https://github.com/helium/HIP/blob/master/0020-hnt-max-supply.md

[15] "Introducing Oracles V2 and DeFi Feeds," 2019. [En línia]. Disponible: https://blog.makerdao.com/introducing-oracles-v2-and-defi-feeds/

[16] K. C. Andrew Miller, Yu Xia, "The honey badger of bft protocols," 2019. [En línia]. Disponible: https://eprint.iacr.org/2016/199.pdf

[17] "HIP16: Hex Density Based Transmit Reward Scaling" 2020. [En línia] Disponible: https://github.com/helium/HIP/blob/master/0016-random-consensus-group-election.md

[18] Andrew Allen, "Mapping the World with Hexagons," 2018. [En línia]. Disponible: https://blog.helium.com/mapping-the-world-with-hexagons-49f57d8b3df5

APÈNDIX

A.1 Transaccions

Aquestes tres figures representen les següents transaccions: una transacció de tipus *payment*, una transacció de tipus *poc receipt* i una transacció d'enviament de dades. Les 2 primeres imatges han estat extretes des de l'API d'Helium i la última des de l'explorer d'Helium ja que totes les dades d'aquesta transacció no cabien en una imatge.


```
ericrams@ubuntu:~$ GET https://api.helium.io/v1/transactions/CNacMt4TlKyLROe2mR6
gnVoU-WwoUJy2tNFNOnF72sE
{"data":{"type":"payment_v2","time":1619276988,"payments":[{"payee":"13ezUKMbiCR
peyxBxD35rXEg2e8FNzy79ocs1TTJhNwhjz7JvY2","amount":4297270640}],"payer":"144Uw17
vUDpZx6C9kr7c3CXGBXksnJie8yQudEjiFgq95WNTCtp","nonce":3,"height":817102,"hash":"
CNacMt4TlKyLROe2mR6gnVoU-WwoUJy2tNFNOnF72sE","fee":35000}}ericrams@ubuntu:~$
```


Fig. 7: Composició d'una transacció de tipus *payment* vista des de l'API


```
ericrams@ubuntu:~$ GET https://api.helium.io/v1/transactions/3nVsRThiQydY8ySD7Lf
S3K7M4wOa3QKpnDgPkqzRuO0
{"data":{"type":"poc_receipts_v1","time":1619276988,"secret":"AC6HNlNy4HaHBp5u6l
FENddqQwJUWdJ1ryUMSUBhfNPeBO63YMCyfbuoCpA-1f22JsYEshUkY9gNhg8-AiOsi5gfcSNzfBB7iF
OOTEPieSadzuna2AXwhMzFbI95MpP2BXE","request_block_hash":"W-_JNILiRE4McoqKqU7oniX
u1lJ3oTs2Wt2LrIqUBpM","path":[{"witnesses":[{"timestamp":1619276608980957733,"sn
r":13.800000190734863,"signal":-72,"packet_hash":"F1-dgm5p0p8bgGh80LnO7JzmEbZn1K
Kf3heyePL5r14","owner":"14aRw5QQefHqDGFmEaicx6w4LNNdVS6r5ePeimtJxMJ5eVcbqn5","lo
cation":"8c2a1000b171dff","is_valid":false,"invalid_reason":"witness_too_close",
"gateway":"11WFpwfPDYPgaMbFV3gw7kFZtFdHBgAjtKF2RhXGYwNwKHLinJB","frequency":904.
5,"datarate":"SF9BW125","channel":3},{"timestamp":1619276608978349534,"snr":-5.5
,"signal":-112,"packet_hash":"F1-dgm5p0p8bgGh80LnO7JzmEbZn1KKf3heyePL5r14","owne
r":"13wxkek5EgS6MU5NSmfW5uzMHrniRdcSnJYGxG4k1M2qoq35e6o","location":"8c2a1000b09
edff","is_valid":true,"gateway":"11KYfGEwswmW2TZoVV187GSz5Ry6a9yoo9ZkL83hCHoW6Ub
Cqf7","frequency":904.5,"datarate":"SF9BW125","channel":3},{"timestamp":16192766
08913307076,"snr":-1.7999999523162842,"signal":-110,"packet_hash":"F1-dgm5p0p8bg
Gh80LnO7JzmEbZn1KKf3heyePL5r14","owner":"13JJAmn87e74xR24w6mWKZteHwPaBd1agV6hqJJ
q22bFFMKVzDe","location":"8c2a100724cd9ff","is_valid":true,"gateway":"11MuDjs5mE
cU3FDzw8PEr5f57zujFzdZ79DSjXXC5HArsZakqkc","frequency":904.5,"datarate":"SF9BW12
5","channel":3},{"timestamp":1619276608981663613,"snr":-8.0,"signal":-113,"packe
t_hash":"F1-dgm5p0p8bgGh80LnO7JzmEbZn1KKf3heyePL5r14","owner":"14CWV8cMpy7QtwNDW
VJL2vQBW574cZgqGqnZaJ1jcVQ4e5kTh8k","location":"8c2a1002834d9ff","is_valid":true
,"gateway":"112eM8YJSwZWUJoK9ySFssU5CvUqJc2ehQPnRghfNHrxn82nV33t","frequency":90
4.5,"datarate":"SF9BW125","channel":3},{"timestamp":1619276608994550268,"snr":11
.0,"signal":-42,"packet_hash":"F1-dgm5p0p8bgGh80LnO7JzmEbZn1KKf3heyePL5r14","owne
r":"14aRw5QQefHqDGFmEaicx6w4LNNdVS6r5ePeimtJxMJ5eVcbqn5","location":"8c2a1000b1
627ff","is_valid":false,"invalid_reason":"witness_too_close","gateway":"112dsrbZ
TgwesUQQ3by5t7WvuxL5gCUun8MajVK6Xx22FmjcudUF","frequency":904.5,"datarate":"SF9B
W125","channel":3},{"timestamp":1619276608915662908,"snr":-14.800000190734863,"s
ignal":-114,"packet_hash":"F1-dgm5p0p8bgGh80LnO7JzmEbZn1KKf3heyePL5r14","owner":
"13ZNCUTCV9g3vpFpsc1QXSxvcwXsqKVbJtUHWU947vw3TPDCCa8","location":"8c2a1008a0323f
f","is_valid":true,"gateway":"112qKKwpE1cZn6geen3kaikYKxMZA6HTMTRiMzdfsBrBqP7wfs
pP","frequency":904.5,"datarate":"SF9BW125","channel":3}],"receipt":null,"geocod
e":{"short_street":"17th Ave","short_state":"NY","short_country":"US","short_cit
y":"Queens","long_street":"17th Avenue","long_state":"New York","long_country":"
United States","long_city":"Queens","city_id":"cXVlZW5zbmV3IHlvcmt1bml0ZWQgc3Rhd
GVz"},"challengee_owner":"14aRw5QQefHqDGFmEaicx6w4LNNdVS6r5ePeimtJxMJ5eVcbqn5","
challengee_lon":-73.77536612818822,"challengee_location":"8c2a1000b1703ff","chal
lengee_lat":40.78547402051716,"challengee":"11EghwXxe3aExUdsiD4K4SRrMAFUndjEaqtA
BYZEREDpQSZsbuZ"}],"onion_key_hash":"dHk7A5uMPSaV8PAQR_OLrl79lylztq9ey0k76vvORdQ
","height":817102,"hash":"3nVsRThiQydY8ySD7LfS3K7M4wOa3QKpnDgPkqzRuO0","fee":0,"
challenger_owner":"14UVp55RsaF3yMhTYLnoe6BYiaedbLTt94BQwimRVBQP6yfF3do","challen
ger_lon":-122.26857260649282,"challenger_location":"8c28308f650ddff","challenger
_lat":37.895853340772774,"challenger":"11CR4h9vy59bNCXU5jssr9xYPpAw4iTvEKBiPoZY7
GzNapkoxFP"}}ericrams@ubuntu:~$
```


Fig. 8: Composició d'una transacció de tipus *poc receipt* vista de de l'API

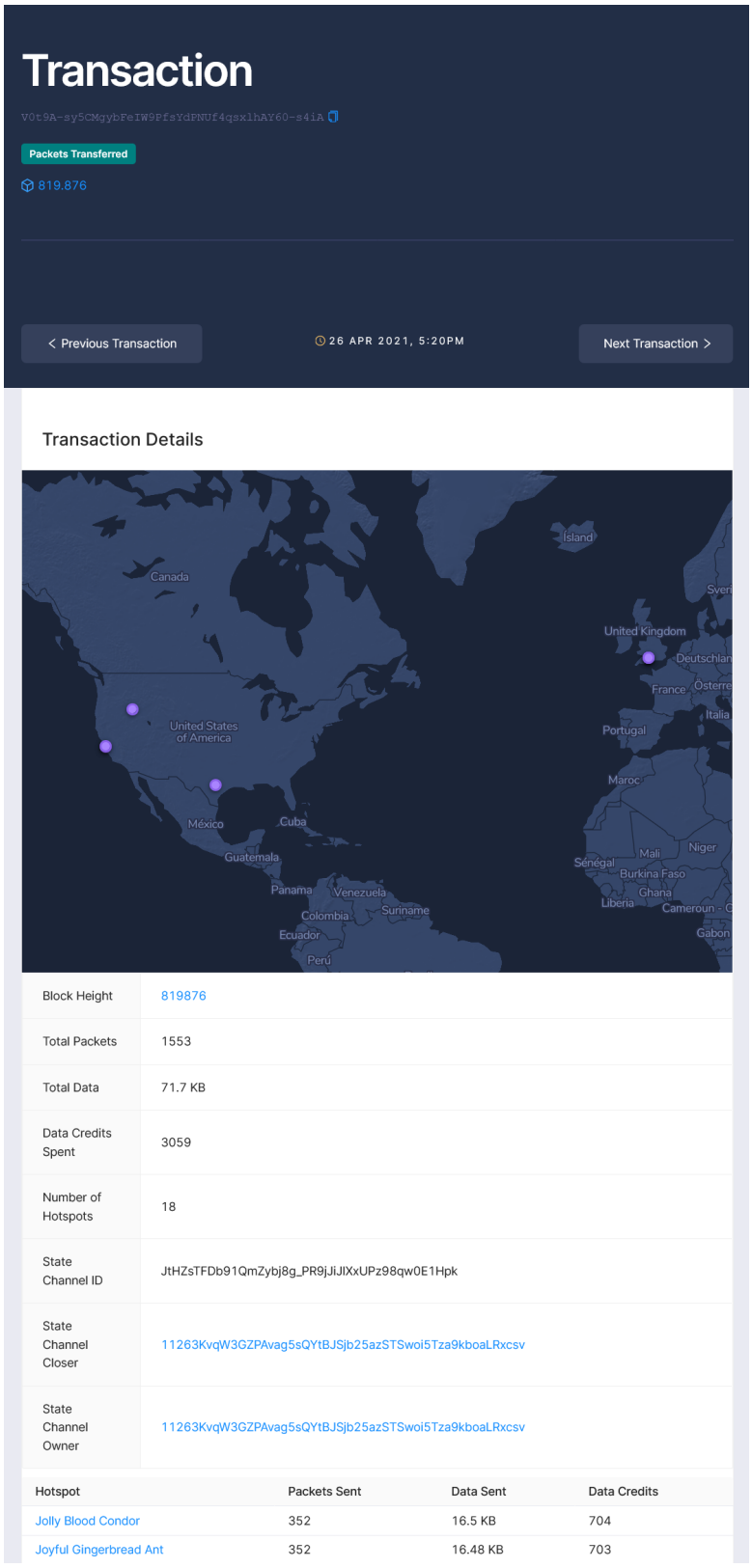

Fig. 9: Composició d'una transacció d'enviament de dades vista des de l'Helium Explorer