Estudi de la criptomoneda Sia

Albert Cabrerizo López

30 de Juny del 2018

Resum– Una criptomoneda és un actiu digital, dissenyat per a ser utilitzat com a mitjà d'intercanvi, que utilitza tècniques criptogràfiques per a controlar la generació de monedes, verificar-ne la transferència i assegurar les transaccions. Ara bé, dotar a una criptomoneda d'una utilitat que la diferenciï de la resta no és gens fàcil, ja que són molts els casos de criptomonedes que no aporten cap innovació. Altrament, NebulousLabs sembla que ho ha aconseguit creant Siacoin. Siacoin és la criptomoneda darrera la plataforma d'emmagatzematge descentralitzat Sia. És gràcies a aquesta criptomoneda que s'assoleix una descentralització completa donant control absolut a l'usuari final. En aquest treball es realitzarà una investigació transversal sobre la plataforma Sia per a coneixer el funcionament d'aquesta.

Paraules clau– Criptomoneda, Blockchain, Sia, Siacoin, emmagatzematge, descentralitzat

Abstract– A cryptocurrency is a digital asset designed to be a medium of exchange using cryptographic techniques to control the generation of coins, securing the transfer of assets and verifying the transactions. However, It is difficult to develop a useful cryptocurrency with a differential functionality because there are a lot of cases where there are no improvements. By contrast, NebulousLabs has achieved this goal by developing Siacoin. Siacoin is the cryptocurrency behind Sia's decentralized storage platform. Thanks of this cryptocurrency there is a full decentralization, giving absolute control to the end user. In this article a cross-sectional research will be carried out on Sia's platform to understand how it works.

Keywords– Cryptocurrency, Blockchain, Sia, Siacoin, storage, decentralize.

1 Introducció

Una criptomoneda és un actiu digital, dissenyat per a ser utilitzat com a mitjà d'intercanvi, que utilitza tècniques criptogràfiques per a controlar la generació de monedes, verificar-ne la transferència i assegurar les transaccions. Aquest tipus de moneda no es troba sota el control de cap tercera entitat com seria el govern o els bancs en el cas de les monedes convencionals, sinó que utilitza un control descentralitzat que funciona a través de la blockchain, una mena de base de dades pública i distribuïda on es registren totes les transaccions.

La primera criptomoneda en aparèixer va ser el Bitcoin l'any 2009, on a partir d'aquí sorgiren una gran quantitat d'altres criptomonedes freqüentment anomenades altacoins (alternative coin). Moltes d'aquestes altacoins només volen ser una altre moneda digital més, però també en sorgeixen que volen aportar noves funcions i/o solucions a problemes reals de les persones, com per exemple les criptomonedes que permeten emmagatzematge descentralitzat.

Les criptomonedes d'emmagatzematge descentralitzat apareixen gràcies a la quantitat d'espai d'emmagatzematge desaprofitat que hi ha arreu del món en les computadores personals. Així doncs, el que es busca és crear una xarxa amb dos usuaris principals, els hosts i els clients. Els hosts seran usuaris que oferiran els seu espai d'emmagatzematge a canvi de rebre una certa quantitat de criptomonedes. I els clients seran els usuaris que pagaran aquesta quantitat de criptomonedes per emmagatzemar les seves dades en els hosts. D'aquesta manera es pot aconseguir una alternativa a les plataformes d'emmagatzematge conegudes com són Dropbox, Drive o Amazon S3.

En aquest article s'examina concretament la moneda Siacoin de la plataforma d'emmagatzematge descentralitzat Sia impulsat per NebulousLabs. En l'apartat (II) es presentarà l'anàlisi previ a l'inici de la recerca sobre aquesta criptomoneda on es van analitzar les tres possibles candidates a ser analitzades. L'apartat (III) explica de forma general

• E-mail de contacte: albertcabrerizo@gmail.com
• Menció realitzada: Tecnologies de la Informació
• Treball tutoritzat per: Jordi Herrera Joancomartí (dEIC)
• Curs 2017/18

els diferents components de la plataforma Sia. En l'apartat (IV) s'entra en detall en el funcionament de la criptomoneda Siacoin, així com explicar el tipus de blockchain que proposa. En l'apartat (V) s'explicarà el procés d'emmagatzematge descentralitzat. L'apartat (VI) es presentarà la criptomoneda Siafund, que és la moneda secundària de la plataforma Sia. Finalment en l'apartat (VII) s'extreuran les conclusions a les que s'ha arribat.

1.1 Objectius

L'objectiu general d'aquest treball és entendre el funcionament del sistema d'emmagatzematge descentralitzat Sia per així saber com s'utilitza la criptomoneda i com es gestiona a nivell tècnic l'emmagatzematge de dades. Per assolir aquest objectiu s'han plantejat diferents subobjectius. El primer és entendre el funcionament general de la plataforma. el segon és entendre el tipus de blockchain i el detall de les transaccions. El tercer és analitzar el tipus de "proof of work" que utilitza. El quart és analitzar com es verifica que un host guarda la informació. El cinquè és extreure estadístiques sobre la utilització de la plataforma. I finalment el sissè és comparar la informació extreta de diferents fonts per conèixer la seva veracitat.

1.2 Metodologia

Per a entendre el funcionament de la plataforma primerament s'analitzaran tots els punts que tracta el *whitepaper* de Siacoin. També es farà una recerca sobre que diu la comunitat de la plataforma. Després es farà un anàlisis dels documents que l'equip desenvolupador té penjats en el seu GitHub per a saber quina informació es pot extreure per a assolir els coneixements esperats sobre la plataforma.

El detall de les transaccions es podrà entendre gràcies al codi en GO del repositori de GitHub, així es sabrà quina estructura segueixen i quins tipus de transaccions es poden trobar. Per a una visió més precisa s'arribarà al més baix nivell possible d'anàlisis amb la blockchain en local.

S'indagarà en el paquet de "Consensus" de Github gràcies al qual es podrà obtenir informació sobre el "Proof of work" que utilitza Siacoin. També s'analitzarà com es verifica que un host manté les dades que el client hi ha emmagatzemat.

Per a obtenir estadístiques sobre el funcionament de la xarxa, a través del entorn NodeJS, s'utilitzaran les APIs de Siastats.info i Explorer.siahub.info. Es farà correr un node de Sia en un entorn Linux on tindrà sincronitzada la blockchain. Mitjançant crides a la API que ofereix la plataforma es podrà accedir a la informació guardada a la blockchain. Així es podran comparar les dades obtingudes des de tercers i directament sobre la blockchain.

2 Estat de l'art

Per tal de decidir quina de les criptomonedes s'analitzarà, s'ha realitzat una comparativa de plataformes d'emmagatzematge descentralitzat, centrat en analitzar superficialment tres de les plataformes amb més renom que utilitzen la tecnologia blockchain per tal d'oferir aquest tipus d'emmagatzematge. El que s'ha buscat és identificar quina d'aquestes plataformes és més interessant per a un anàlisis més profund de la seva tecnologia. Aquestes plataformes són Siacoin, Storj i FileCoin.

En aquest tipus de plataformes la idea principal és que donat un arxiu que es vol emmagatzemar de forma distribuïda, aquest s'ha de trossejar, xifrar i repartir cada tros en diferents nodes. Després s'apliquen "Erasure Codes" que mitjançant la replicació de les dades permeten recuperar l'arxiu sense la necessitat que tots els hosts es trobin online.

Siacoin crea un marketplace [1] on els hosts s'ofereixen establint un preu que els clients hauran de pagar per tal d'utilitzar-los, així els clients poden decidir en quins hosts volen que s'emmagatzemin les seves dades. Aquests hosts seran triats segons preu i disponibilitat. Els contractes que es formen entre client i host per recollir els detalls del pacte es registren a la blockchain. Per tant els contractes generats es converteixen en transaccions esperant a ser seleccionades i col·locades en blocks per part dels miners i finalment el block ser col·locat en la blockchain pròpia de la plataforma de Siacoin. Una vegada el contracte es trobi en la blockchain les condicions d'aquest es podran actualitzar segons interessos dels clients i hosts.

FileCoin també crea un Marketplace [2], concretament dos: un mercat d'emmagatzematge i un altre de recuperació. Els dos tenen la mateixa estructura però un disseny diferent, el mercat d'emmagatzematge permet als clients pagar als "Storage Miners" per emmagatzemar les dades, mentre que el de recuperació permet als clients pagar als "Retrieval Miners". En els dos mercats, tant clients com miners poden proposar els seus preus o acceptar les ofertes. La primera idea de FileCoin va ser utilitzar els SmartContracts de la plataforma de Ethereum però finalment ha decidit implementar la seva pròpia blockchain per tal d'emmagatzemar els contractes entre clients i miners. FileCoin funciona sobre el protocol InterPlanetary File System (IPFS) [4] dissenyat per a crear un sistema de fitxers distribuït en una xarxa p2p.

Storj no crea cap Marketplace, sinó que estableix uns preus fixes pels clients i uns guanys també fixes pels hosts. És Storj qui s'encarrega de distribuir les dades en els hosts que troba oportú i gràcies a la plataforma Ethereum crea els SmartContracts que permetran als hosts cobrar per emmagatzemar les dades. L'accés a la plataforma Storj no és descentralitzat ja que aquest implementa un element anomenat "Bridge" que actua com un servidor d'accés al sistema. Segons Storj Labs [3], qualsevol podria fer funcionar el seu propi Bridge per facilitar l'accés a la xarxa, però de moment l'únic utilitzable és el que manté Storj Labs.

Veient les característiques esmentades de cada plataforma es discriminarà la plataforma de Storj, ja que el que es vol dur a terme és un estudi d'una plataforma d'emmagatzematge descentralitzat amb un ús coherent de la tecnologia blockchain. Storj, a l'utilitzar els Bridges com a porta

d'accés, centralitza part de la seva estructura i s'allunya de les característiques desitjades.
Tant Siacoin com FileCoin utilitzen la blockchain d'una forma coherent pel sistema que volen crear. Pel que fa a FileCoin, el protocol IPFS que utilitza pot ser una eina interessant i útil per a la distribució de les dades. També ho és el funcionament de la blockchain, mentre que els miners de Siacoin utilitzen la "Proof of work" mitjançant potència de còmput per a trobar el block següent en la blockchain, FileCoin està en contra de la potència de càlcul desaprofitada, per tant opta per realitzar la "Proof of Spacetime", [2, 6.2] bàsicament el que vol aconseguir és que la probabilitat de que la xarxa (el conjunt de nodes de la plataforma) esculli un miner per crear el nou block sigui proporcional al seu emmagatzematge en ús en comparació amb el de la resta de la xarxa. Així s'aconseguirà que els miners inverteixin en emmagatzematge en comptes de potència de còmput.
El inconvenient de FileCoin és que actualment la plataforma no és funcional, ha rebut inversió però encara no s'ha desenvolupat una plataforma útil. Per tant, com que en aquest treball es vol realitzar un estudi sobre la blockchain de la plataforma, en el moment de realitzar-lo FileCoin no és una bona opció.
En resum, la plataforma triada per a realitzar el estudi en profunditat és Sia. Aquesta sí que és funcional actualment i a part és una plataforma totalment descentralitzada. En el cas que el equip de desenvolupament que la impulsa desaparegués, la plataforma seguiria funcionant sense cap inconvenient.

3 Visió general de la plataforma Sia

Sia és creada com una plataforma d'emmagatzematge descentralitzat. Els desenvolupadors, NebulousLabs, han volgut convertir els usuaris finals en els responsables dels seus propis arxius sense haver de confiar en terceres companyies que els gestionin sense cap mena de control. Per aconseguir aquest propòsit han utilitzat la tecnologia blockchain per a crear una pròpia criptomoneda, Siacoin, per a poder fer realitat aquesta descentralització.
En aquesta plataforma es troben diferents tipus de participants: clients, hosts i miners, com es pot observar a la figura (1). Els clients i hosts només intervenen en l'àmbit de l'emmagatzematge descentralitzat utilitzant Siacoin com una moneda per a comprar i vendre serveis o simplement per a fer transferències de monedes. Els miners són el motor que fa funcionar la criptomoneda, mantenen el consens en la blockchain fent que es pugui "confiar" en el sistema.

Els clients són els usuaris interessats en emmagatzemar dades al cloud i els hosts són els interessats en emmagatzemar les dades dels clients. Per a connectar aquestes dues parts Sia crea un marketplace on els hosts es poden anunciar i establir un preu d'emmagatzematge i d'ample de banda. Els clients poden seleccionar els hosts que vulguin utilitzar creant contractes amb ells. En aquests contractes tant el client com el host inclouran una certa quantitat de Siacoins. Els clients ho faran per pagar el servei d'emmagatzematge i d'ample de banda utilitzat, i els hosts per a crear confiança i incentivar-los a mantenir les dades dels clients disponibles si volen obtenir benefici. Durant el període del contracte els hosts hauran de demostrar que segueixen mantenint les dades dels clients, si no són capaços de demostrar-ho perdran

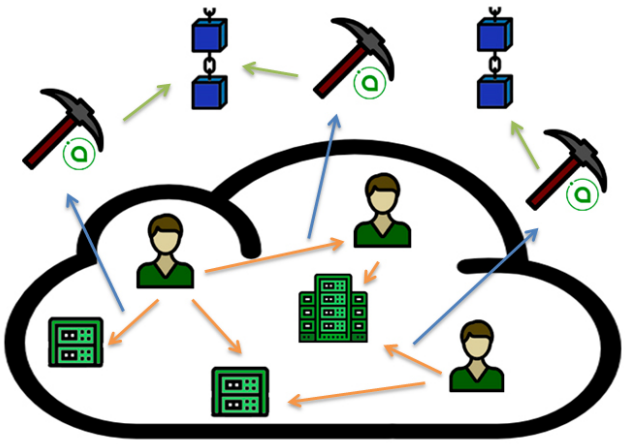

Fig. 1: *Big picture* de la plataforma

les Siacoins que han afegit en el contracte i el client recuperarà les seves.
En la plataforma de Sia apareix la criptomoneda secundaria Siafund. Aquesta criptomoneda ha estat creada per a finançar el projecte. Els desenvolupadors en comptes de preminar una gran quantitat de Siacoins han decidit crear aquesta moneda secundaria per aconseguir encara més descentralització i no tenir un gran poder sobre el preu de Siacoin en el mercat. Per als propietaris de Siafunds aquesta moneda actua com un actiu, ja que el 3,9% de les Siacoins gastades en els contractes finalitzats satisfactòriament es reparteixen proporcionalment entre tots els posseïdors de Siafunds.
La funció dels miners és crear blocks amb les transaccions que creen els diferents usuaris de la xarxa. Recullen les transaccions de la xarxa p2p, validen que són correctes i les afegeixen al block que volen crear. Una vegada tenen el block hauran d'aplicar-li una funció hash diverses vegades per a obtenir el hash vàlid del block. Aquestes operacions requereixen d'un ús intensiu dels recursos hardware dels que disposen amb la despesa en electricitat que suposa. El que els incentiva a realitzar aquesta tasca és la recompensa per trobar un hash vàlid per al block per poder-lo afegir a la blockchain i les comissions que paguen els usuaris als miners en les transaccions de Siacoins.
Siacoin ha estat creada com una moneda inflacionària per a incentivar l'ús d'aquesta i evitar que certs participats vulguin mantenir-ne una gran quantitat per a futures pujades de preu. Per tant permanentment es crearan Siacoins en cada block afegit a la blockchain. Totes les decisions sobre l'estructura de la criptomoneda han estat triades conscientment per a que sigui beneficiosa per l'emmagatzematge descentralitzat i no com a mitjà d'especulació.

4 Siacoin

Siacoin és la criptomoneda de Sia. Aquesta és divisible en 10^{24} unitats anomenades Hastings. La raó d'aquesta unitat tant petita (si es compara amb el Satoshi que és una 10^{-8} part d'un Bitcoin) és que la finalitat de la plataforma és l'emmagatzematge descentralitzat, per tant en el sistema hi haurà una gran quantitat de micropagaments entre hosts i clients. A tot això, a més demanda d'espai d'emmagatze-

matge per part dels clients, més pujarà el valor de la moneda i els desenvolupadors han volgut que aquesta segueixi sent accessible per a tothom encara que el valor incrementi.

4.1 Blockchain

El concepte de blockchain apareix per primera vegada en el *whitepaper* de Bitcoin [10]. El que planteja és portar en un entorn descentralitzat i distribuït una base de dades amb tres requisits: qualsevol participant del sistema pot afegir informació, tothom és capaç de llegir-la i ningú ha de poder eliminar o modificar la informació. Per a que el sistema funcioni i per tant no tingui mancances de seguretat es parteix de la presumpció que tot individu que participarà és malintencionat i per tant no hi pot haver confiança, així s'han d'adoptar una sèrie de mesures per a que es compleixin els requisits esmentats. Aquí és on entra en joc la criptografia, ja que utilitzada de la forma correcta es pot comprovar que ningú pot enganyar o que efectuar un atac és massa costós per a que sigui profitós per a l'atacant.

4.1.1 Tipus de Blockchain a Sia

La blockchain creada per Sia utilitza el model de Unspent Transaction Output (UTXO). UTXOs s'anomenen les adreces que encara no han gastat les monedes, per tant per efectuar un pagament vàlid els inputs de la transacció han de ser UTXOs. Així, una vegada contruida i analitzada la blockchain en un node local, només faran falta els UTXOs per saber si una certa adreça pot gastar els Siacoins que hi té.
Per a les funcions hash s'utilitza l'algoritme blake2b que dona una sortida de 256 bits. S'ha triat aquest ja que és diferent del SHA-2 utilitzat per Bitcoin evitant així que miners amb molts recursos de la xarxa de Bitcoin puguin atacar la xarxa de Siacoin.
El protocol que determina si un block generat és vàlid és similar al de Bitcoin, el miner haurà de trobar un hash del block amb una quantitat establerta i variable de zeros en l'inici del hash. Aquesta quantitat de zeros ve determinada segons la dificultat de trobar un block en aquell moment. La dificultat de trobar un block en un cert instant de temps depen de la mitjana de temps de block dels 1000 anteriors blocks. Els nodes de la xarxa augmentaran o disminuiran aquesta dificultat per consens per a mantenir un temps de generació de block estable.
El temps de generació d'un block és de 10 minuts i la mida màxima d'aquest és de 2MB. Les transaccions no tenen mida màxima sempre que càpiguen dins el block. L'identificador del block es calcula:

$$IdBlock = (PaIdBlock + 64bitNonce + T + BMR)$$

On el PaIdBlock és l'identificador del block predecessor, els 64 bit Nonce són els bits lliures que el miner pot modificar per a trobar el hash del block vàlid, la T és un Timestamp del moment de creació del block i el BMR és el Block Merkle Root que s'obté creant un Merkle tree on les fulles estan formades pels outputs del miner i els hash de les transaccions del block.
A diferència de Bitcoin on hi ha un màxim de monedes que la xarxa pot generar, a Sia no hi ha un límit de Siacoins, aquestes seran generades per sempre. El que si que canvia en el temps és la recomença que reben els miners. La recompensa en Siacoins per minar un block i afegir-lo a la blockchain ve donada per la següent fórmula:

Si $Recompensa > 30.000$:
$Recompensa = (300.000 - hblock)$
Sinó: $Recompensa = 30.000$

On hblock és l'altura del block. Es pot veure de forma gràfica en la figura (2).

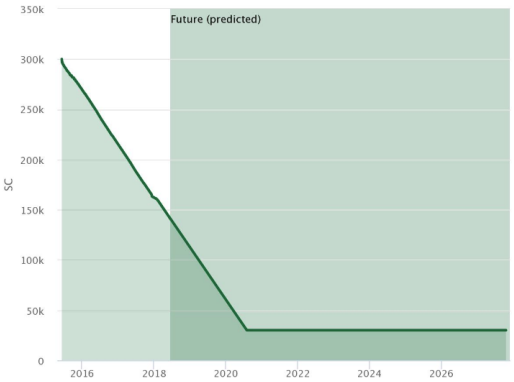

Fig. 2: Generació de Siacoins al llarg del temps

La blockchain s'emmagatzema a disc mitjançant una base de dades escrita en Go. Aquesta forma part del projecte BoltDB on s'ha creat un tipus de base de dades que funciona per clau/valor. Aquesta s'estructura per buckets etiquetats, els quals permeten agrupar les dades a conveniencia per a una lectura ràpida.

4.1.2 Consens

El consens en la blockchain és una de les parts més importants d'aquesta, ja que com s'ha comentat anteriorment el sistema ha de poder funcionar correctament en un entorn hostil. El consens és l'acord entre els diferents individus que participen en el sistema en relació a com s'actuarà davant les dades que s'han d'inserir en la blockchain, per tant quines seran vàlides i quines incorrectes. En un sistema on no es confia en els demés individus s'ha de provar que el que s'està fent és correcte. Apareixen diferents mètodes com poden ser Proof of Work (PoW) o Proof of Stake (PoS).

Sia utilitza el mètode de PoW construït en base a equihash [11]. Aquest algoritme està basat en el problema generalitzat de l'Aniversari [12], per tant està àmpliament estudiat per científics i criptògrafs. Gràcies a això es pot assegurar que una optimització exitosa per part de certs nodes de la xarxa seria molt difícil d'aconseguir. L'algoritme blake2b que utilitza la plataforma és quasi 2x més ràpid que el SHA-2, per tant una bona opció per a clients lleugers de la plataforma.
Els algoritmes de PoW que utilitzen les criptomonedes es poden classificar entre els que poden ser implementats per hardware mitjançant Application-Specific Integrated Circuit (ASIC) i els que no.
L'algoritme blake2b juntament amb el de Bitcoin són dels que es poden implementar per hardware. Per això mateix, l'equip de NebulousLabs té pensat llençar un

ASIC propi anomenat Obelisk a mitjans de 2018. Aquest aparell promet un hashrate (nombre d'operacions hash per segon) de 550 GH/S. Per als algoritmes de PoW que no es poden implementar específicament per hardware s'utilitzen targetes gràfiques per a realitzar el treball.
El fet de poder desenvolupar dispositius específics per a realitzar el treball pot tenir aspectes positius i negatius segons el punt de vista.

Des del punt de vista dels miners pot ser tant positiu, ja que el hashrate per segon és alt en comparació a minar amb CPU o GPU obtenint avantatge davant d'altres usuaris de la xarxa, com negatiu ja que han de gastar una certa quantitat de diners en hardware específic per a una criptomoneda fent impossible el minat en una altre a no ser que s'utilitzi el mateix algorisme de hash.

Des del punt de vista de la criptomoneda és positiu, ja que s'aconsegueix fidelitat amb els miners de la plataforma que no migraran a minar una altre moneda si el preu d'aquesta fluctua.

Un altre aspecte positiu és que es minimitzen els possibles atacs del 51% a la plataforma. Qualsevol miner o grup que assoleixi una capacitat de minat superior al 51% de la xarxa pot ser un possible atacant al sistema generant *forks* o *double-spends* en la blockchain, però si aquests han hagut d'invertir una gran quantitat de diners per adquirir hardware específic per a minar i superar aquest 51% de poder de minat esmentat seran reticents a realitzar atacs a la plataforma ja que això faria baixar el valor de la criptomoneda fent que no amortitzessin el hardware adquirit.

Les criptomonedes que s'han de minar mitjançant GPUs es troben més desprotegides davant d'aquests tipus d'atacs. Qualsevol entitat en el món amb una alta capacitat de còmput pot ser un possible atacant podent ser entitats que no estan contemplades en el sistema ja que podrien no estar exercint com a miners. S'han trobat diferents casos en criptomonedes emergents com Krypton o Shift on la xarxa té poca capacitat de còmput i entitats com 51crew hi han realitzat atacs [13].

La part negativa d'utilitzar ASICs per part de les criptomonedes és el control que tenen les empreses que desenvolupen aquests dispositius ja que són els verdaders coneixedors del hashrate que hi ha a la xarxa (podrien amagar la quantitat real de dispositius distribuïts) i així realitzar estratègies per a treure'n profit.

4.2 Transaccions

Per al funcionament de la plataforma de Sia es necessiten diferents tipus de transaccions. Això és així ja que el seu propòsit principal és el de esdevenir com a plataforma d'emmagatzematge descentralitzat. Per tant dins d'aquest entorn es necessitaran crear transaccions de pagaments de Siacoins, de creació de contractes entre clients i hosts o anuncis de nous hosts a la xarxa, entre d'altres.
Sia utilitza la mateixa estructura de dades per a totes les transaccions. Així doncs certs camps simplement es trobaran buits segons l'acció que s'estigui duent a terme. Per exemple, una transacció de pagament de Siacoins d'una adreça a una altra no necessita omplir el camp de FileContract.
Com s'ha mencionat en el punt 4.1.1 les transaccions de Siacoins segueixen el model UTXO. Per tant quan s'estigui creant una transacció de Siacoins el camp SiacoinInputs apuntarà al camp SiacoinOutputID provinent d'una altra transacció (Apèndix, 1). Si la quantitat de Siacoins que es tenen en una adreça és superior a la que es vol pagar en una altre adreça, es crearà més d'un SiacoinOutput on un serà el que es vol pagar a l'adreça destí i l'altre el canvi que es tornaria el propietari a una adreça del seu domini. En la figura (3) s'aprecia el detall dels camps de SiacoinInputs i SiacoinOutputs.

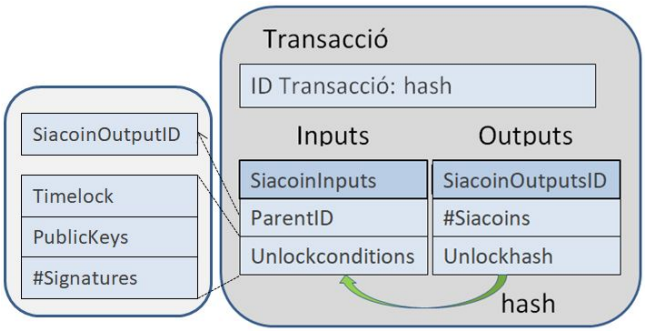

Fig. 3: Detall d'una transacció

L'estructura de SiacoinOutput està format per tres paràmetres. El primer és el SiacoinOutputID que es calcula fent el hash dels diferents camps de la transacció (menys les signatures) i un índex amb domini en la transacció. El segon camp és on s'indiquen el nombre de Siacoins que conté. L'últim camp és on es troba el "unlockhash" que és el hash de les "unlockConditions". Pel que fa als *Inputs*, el camp de SiacoinInput consumeix un SiacoinOutput, per tant està format per un "parentID"que apunta al SiacoinOutputID i per les "unlockConditions".

Les "unlockConditions" estan formades per tres camps, el "timelock"que és l'alçada de block de quan s'ha generat el SiacoinOutput, una llista de claus públiques i el nombre de signatures requerides per a gastar els Siacoins.

Tenint en compte els tres camps de les "unlockConditions", un SiacoinOutput només podrà ser gastat si es compleix que el block on es vol introduir la transacció és més gran que el "Timelock", la signatura pertany a una de les adresses del llistat de claus públiques i s'afegeixen tantes signatures com marqui el darrer camp.

5 Emmagatzematge de fitxers

Sia crea una sèrie de procediments per aconseguir una gestió de l'emmagatzematge totalment descentralitzada. El procés comença com es veu en la figura (4) (Procés 1) amb la necessitat dels hosts d'anunciar-se a la xarxa. La forma amb la que s'anuncien és creant transaccions afegint en el camp de ArbitraryData el protocol d'anunci (Apèndix, 2). Aquest es basa en una estructura de dades precedida per

la paraula "HostAnnouncement", seguida de la direcció IP pública i la clau pública, tot codificat en base64. En la figura (5) es pot veure la descodificació del camp de ArbitraryData de la transacció (Apèndix, 5). Amb aquest protocol els clients podran trobar hosts disponibles i així crear contractes d'emmagatzematge i transferir els arxius.

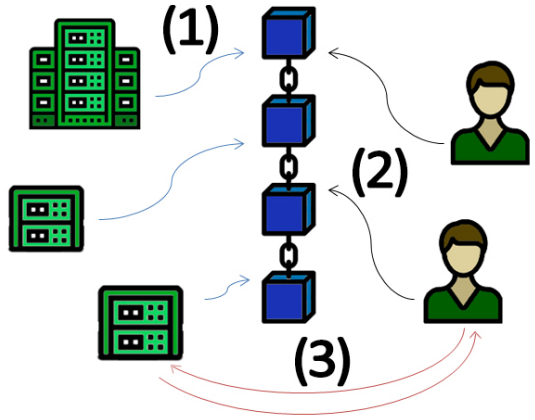

Fig. 4: HostAnnouncement, Allowance i Canal

En aquest sistema els hosts cobren per espai d'emmagatzematge i per ample de banda utilitzat. Això incentiva a molts usuaris o empreses que disposen de màquines operatives 24 hores set dies a la setmana a oferir el espai extra dels seus discs durs, ja que no suposa un increment significatiu en el preu de l'electricitat gastada el fet de tenir el dimoni de Sia gestionant l'emmagatzematge de fitxers. Com que tot el sistema s'ha pensat per tal que pugui ser el màxim de transparent per a l'usuari que l'utilitza, aquest no haurà de dedicar una gran quantitat de temps extra a gestionar els processos d'emmagatzematge i transferència de dades.

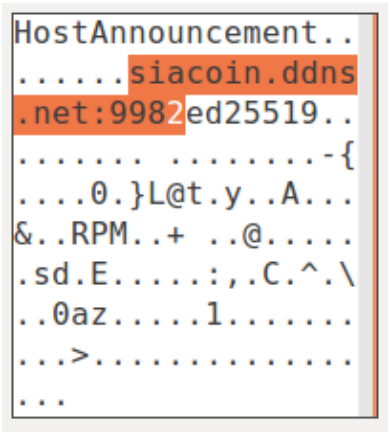

Fig. 5: Descodificació del camp ArbitraryData

Ara bé, a un nivell més baix que el de l'usuari estàndar s'hi troben un seguit de protocols d'intercanvi de transaccions per a gestionar tot el sistema. Seria un greu problema d'escalatge que tota la informació que s'han de transferir el client i el host es fes a través de la blockchain. Per aquest motiu Sia crea un canal de pagament/transferència entre el client i el host utilitzant el protocol Lightning Network [9]. Amb aquest protocol, per norma general, només queden registrades a la blockchain dos transaccions, la primera, el primer FileContract i la segona el últim FileContractRevision. En la figura (4) aquest canal està representat pel procés (3). A continuació s'entrarà en detall en els diferents passos per a dur a terme el emmagatzematge.

5.1 Allowance

Per tal de poder crear contractes d'emmagatzematge entre el client i el host, prèviament el client ha d'assignar una certa quantitat de Siacoins per a aquesta comesa. Sia anomena allowance a aquest tràmit. El client ha de decidir la quantitat de Siacoins que es dedicaran a comprar espai d'emmagatzematge. D'aquesta quantitat 1/3 part és utilitzada per a crear contractes amb 50 hosts diferents amb una durada de 13 setmanes. Els 2/3 restants es guardaran per a crear futurs nous contractes o per a les despeses d'ample de banda utilitzat per a pujar i baixar els arxius. Aquesta acció queda reflexada en la figura (4) (Procés 2) on els clients exploren la blockchain per a trobar els anuncis de hosts per a després contactar amb ells.

Els 50 hosts els tria el node de Sia automàticament basant-se en una puntuació estimada segons el preu, temps del host a la xarxa i espai lliure d'aquest. Per ara el nombre de hosts i la tria no es pot fer manualment, però en futures versions l'equip de NebulousLabs promet que serà possible triar totes les variables segons la necessitat de cada client.

Si el temps establert en els contractes finalitza i el client no ha pujat cap arxiu a la xarxa, totes les Siacoins menys les *fees* del allowance seran retornades al client. La forma de pagament al host s'explicarà en el punt 7. Les *fees* que ha de pagar el client són el 3.9% de l'allowance i el 3.9% de les monedes que posa el host en el contracte anomenades *collateral locked*. El *collateral locked* serveix per a incentivar el host a complir amb el contracte, ja que en el cas de no fer-ho aquestes Siacoins que ha dipositat es perdrien.

5.2 File contracts

Sia utilitza el terme File Contract per referir-se als SmartContracts. En altres tipus de plataformes on s'utilitzen SmartContracts, com Ethereum [5], la idea és que qualsevol els pugui crear per tal de desenvolupar aplicacions descentralitzades. L'equip de NebulousLabs ha pensat que el fet que cadascú dissenyés els seus SmartContracts portaria inevitablement a errors i possibles falles de seguretat. Per tant, Sia soluciona aquest problema creant un format únic de file contract.
La creació d'un File Contract passa per una prèvia negociació entre el client i el host fora de la blockchain. En la figura (6) el procés (1) mostra que el client i el host s'envien l'un al altre els diferents requeriments de cadascú per a la formació d'un nou contracte. Això ho fan seguint un protocol de comunicació per a finalment en el procés (2) pujar el File Contract signat per les dues parts a la blockchain. El reste de comunicació la faran a través d'un canal fora de la blockchain com es veu en el procés (3).

Entre els camps dels quals està format el File Contract (Apèndix, 3) es troba el hash de l'arrel de l'arbre de Merk-

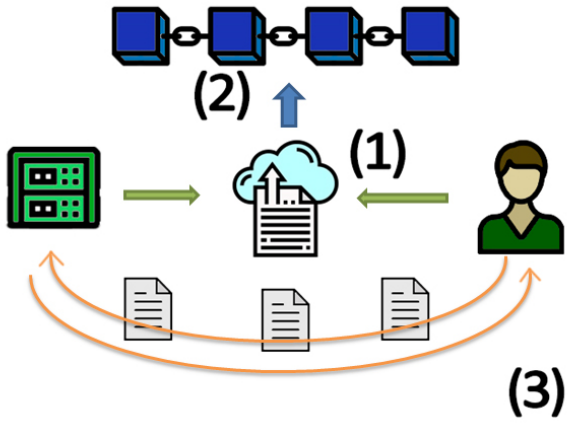

Fig. 6: Protocol de creació del File Contract

le [6] del fitxer. L'arbre de Merkle simplifica la localització de les dades emmagatzemades i facilita la validació d'aquetes. En la creació del file contract el client especifica la durada del contracte, el *challenge frequency* i els paràmetres de pagament. El *challenge frequency* és la freqüència en la que el host ha de fer els Proof of Storage (comentats en la secció 5.4). Els paràmetres de pagament defineixen la quantia en monedes que es desbloquegen per prova vàlida, els que es bloquegen per prova invàlida i el màxim nombre de proves que es permeten fallar. Durant el període de temps que es manté actiu, el File Contract por rebre alguna actualització de les condicions inicials. Aquestes modificacions quedaran reflexades en una revisió del contracte. Aquesta revisió del contracte farà referència al contracte inicial i augmentarà el camp de RevisionNumber (Apèndix, 3) creant un històric de versions d'aquest contracte. Quan finalitza la durada del file contract aquest es pot renovar o no. Si no es renova, tant el host com el client reben les Siacoins desbloquejades per cada part i el host ja pot alliberar l'espai d'emmagatzematge ocupat pels arxius del client que a partir d'aquest moment ja no rebrà cap penalització. D'altra banda, si es renova, a ulls de l'usuari pot semblar una ampliació del contracte creat prèviament, però segons el protocol que es segueix aquest contracte queda finalitzat i s'inicia el procés de creació d'un nou contracte desde zero. Això comporta que s'han de tornar a abonar les *fees* d'aquesta acció.

5.3 Upload, Download i replicació de fitxers

Cada arxiu que s'allotja en un host té un preu tant per l'espai/temps que ocupa com per l'ample de banda utilitzat per transferir-lo. D'aquesta manera, cada vegada que el client modifica els seus arxius allotjats es crea una comunicació entre el client i el host que s'envia a través del canal creat. Quan la comunicació finalitza i s'han fet els canvis pertinents en els arxius, es crea un FileContractRevision i queda registrat a la blockchain. Aquestes revisions de contracte actualitzen la quantitat de Siacoins, determinada en el Payout del contracte que rebrà el host i programen un nou Proof of Storage.

En la creació dels File Contracts s'ha vist que es construeix un arbre de Merkle per a localitzar i verificar les dades. Per a construir aquest arbre, el fitxer primer és dividit en múltiples parts de 40MB cadascuna com es pot observar en la figura (7)(Procés 1), després es xifra cada part en particular amb l'algoritme de xifratge de clau simètrica per blocks Twofish [7] com es veu en la figura (7)(Procés 2) i finalment es crea l'arbre de Merkle amb el hash de cada part en particular formant les fulles.

Les dades dels clients no només les emmagatzema un

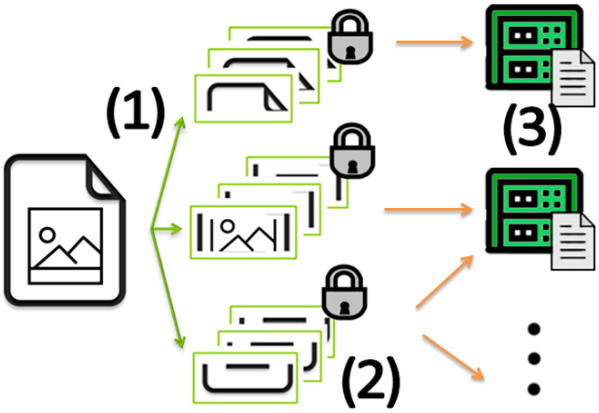

Fig. 7: Protocol de distribució de fitxers

únic host, per aconseguir una alta disponibilitat dels fitxers Sia utilitza *Repairing Reed-Solomon Codes* [8]. Cada part del fitxer es replica i es distribueix entre diferents nodes (7)(Procés 3). De forma estàndard utilitza una redundància de 3x i 30 hosts diferents, així només es necessiten 10 hosts disponibles en un moment donat per a recuperar l'arxiu original.
Per a pròximes versions del software client de Sia es pretén que aquests valors per defecte es puguin modificar i així obtenir la disponibilitat desitjada per a cada fitxer.

5.4 Proof of Storage

Res assegura que una vegada el File Contract s'ha creat i el client puja fitxers al host, aquest simplement elimini les dades o apagui la màquina i mai més torni a estar online. Per evitar que es donin aquests casos Sia utilitza el Proof of Storage representat en la figura (8). Bàsicament el que implica és que el host ha de demostrar diferents vegades durant el temps que duri el contracte que segueix allotjant les dades del client. D'aquesta manera pot anar desbloquejant les Siacoins del contracte que prèviament ha introduït ell com a collateral locked. El nombre de proves (*challenge frequency*) que ha de passar el host l'estableix el client.

Per a validar cada prova el host disposa d'un marge de temps anomenat *challenge window*, mesurat en blocks, d'aproximadament 24 hores. Aquest està determinat per dos blocks, la finestra d'obertura i la de tancament. La prova que ha de validar consisteix en generar una transacció amb l'identificador del contracte, un llistat de hashs de l'arbre de Merkle i una part de les dades que allotja representat en la figura (8)(Procés 1). Aquesta part és triada de forma aleatòria utilitzant el hash del block anterior de la finestra d'obertura del *challenge window*. Si la quantitat de fallades

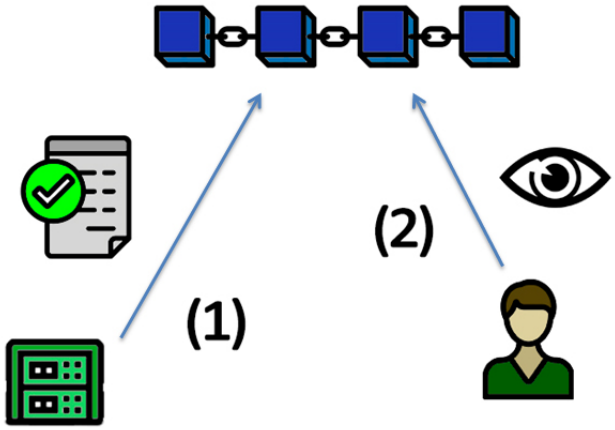

Fig. 8: Procés de Proof Of Storage

en les validacions sobrepassa un cert llindar el host perd tot el que havia introduït com a collateral locked i el Payout de Siacoins menys les *fees* són retornades al client.
Cada Proof of Storage és inclòs a la blockchain dins una transacció. El client o qualsevol persona amb accés a la blockchain pot comprovar la validesa del Proof of Storage, figura (8)(Procés 2). D'aqueta forma el client crea un FileContractRevision per actualitzar l'estat del File Contract. Aquest FileContractRevision queda registrat a la blockchain després d'haver intercanviat l'informació amb el host a través del canal de comunicació. D'aquesta manera qualsevol pot conèixer l'estat actual del File Contrat explorant la blockchain. Quan finalitza el contracte, l'última versió del File Contract queda registrat a la blockchain com a FileContractRevision amb l'últim *revision number*.

6 SIAFUNDS

Siafund és la segona criptomoneda de Sia. Aquesta moneda ha estat creada únicament per a finançar el projecte de Sia. Els desenvolupadors de Sia en comptes de preminar una certa quantitat de monedes com es dona en altres plataformes van preminar 10.000 unitats de Siafunds. Així en diferents etapes del projecte s'han posat a la venda certes quantitats per tal d'aconseguir el finançament necessari.
Els posseïdors de Siafunds obtenen una recompensa per posseir-los, aquests reben la part proporcional en Siacoins provinent d'una pool de Siacoins, anomenada SFPool (SiafundPool), que es va omplint segons augmenten els File Contracts de la plataforma. Això és així ja que el 3,9% de Siacoins del payout d'un contracte van a parar a la *pool*. Aquesta *pool* el que fa és guardar el nombre total de Siacoins que s'hi ha transferit, perquè el que passa realment és que els Siacoins transferits són cremats (enviats a una adreça inaccessible). Un client per recaptar les Siacoins acumulades que li pertoquen ha de generar una transacció amb les Siafunds com a output amb destinació a una altra adreça, òbviament pot ser una adreça controlada per ell mateix en el seu propi wallet. Quan es genera una transacció amb SiafundOutputs es generen els Siacoins creant un SiacoinOutput amb el valor determinat per la següent funció:

$$Valor = ((SFPool - CS)/10.000) * \#SF$$

En el moment de ser generada la transacció la variable CS (ClaimStart) valdrà zero, per tant el SiacoinOutput tindrà la quantitat de monedes proporcionals a la possessió de Siafunds. Així el destinatari rebrà aquesta quantitat de Siacoins generada. Immediatament després la variable ClaimStart passarà a valer igual a la SiafundPool perquè el client no pugui reclamar Siacoins indefinidament. Quan la mida de la SiafundPool augmenta el client posseïdor de Siafunds pot repetir el procés per a cobrar les Siacoins que li pertoquen. Aquest usuari podria falsificar les variables de ClaimStart per a intentar obtenir més Siacoins de les que li pertoquen, però gràcies a les normes de consens que segueixen els nodes de la xarxa aquestes transaccions es denegarien.

7 CONCLUSIONS

Els objectius marcats per aquest treball s'han assolit quasi en la seva totalitat. Les excepcions es deuen al baix grau de maduresa de la plataforma Sia on components com l'Explorador de la blockchain no es troben enllestits. Això ha fet que l'abast del treball es limiti al coneixement teòric de la plataforma.
Sia es focalitza des d'un primer moment en l'emmagatzematge descentralitzat, per tant la criptomoneda Siacoin s'utilitza com una eina per a que aquest tipus d'emmagatzematge sigui possible. Convertint-se en un dels pocs projectes actuals que utilitzen la tecnologia blockchain de la forma per a la qual es va idear. Això s'ha vist quan s'ha comparat amb altres plataformes com Storj.
Siacoin és creada des de zero per NebulousLabs i segueix les pautes de Bitcoin utilitzant transaccions en forma de UTXOs i una funció hash implementable per hardware amb el benefici que això aporta a la criptomoneda en termes de seguretat contra atacs del 51%.
El punt clau de Sia és el marketplace on entren en joc hosts i clients. Agafant d'exemple la Lightning Network aconsegueix crear un flux de comunicació entre els anteriors sense saturar la blockchain de transaccions. Això sumat al sistema de pagament, pensat per premiar els hosts que mantenen les dades disponibles i castigar els que no, aconsegueix una plataforma fiable des del punt de vista del client on poder dipositar els seus fitxers.
La moneda secundaria Siafund ha estat ideada per obtenir finançament per part de l'equip desenvolupador. D'aquesta forma no s'ha fet un preminatge de Siacoins, sinó posant en venda certa quantitat de Siafunds esdevenint com actius del projecte que retornen uns interessos als posseïdors en forma de Siacoins.

7.1 Ampliacions futures

L'estat del projecte actual permet seguir la recerca en diferents possibles camins.
Donat que les transaccions de Siacoin segueixen el model de UTXO es podria seguir investigant com integrar la blockchain amb l'analitzador de dades BlockSci utilitzat en la xarxa Bitcoin. Això seria un avantatge si la mida de la blockchain arriba al que té ara Bitcoin (171GB). Ara bé, com que Siacoin emmagatzema la blockchain mitjançant una base de dades amb BoltDB s'haurien de fer proves de rendiment per a saber quina seria la possible millora.

A nivell de recerca sobre com està construida la plataforma Sia, es podria baixar a més baix nivell en cadascun dels apartats esmentats en el document. Això ajudaria a entendre millor els protocols que segueix en cadascuna de les accions que realitza.
Un altre punt important seria analitzar la blockchain emmagatzemada en local mitjançant BoltDB donat que la API de l'explorador que ofereix Sia no es troba fuincionant correctament.
Per últim, per donar un enfocament en l'àmbit professional, es podrien buscar solucions per a crear hosts de Sia de forma àgil mitjançant Docker en companyies proveïdores de servei i emmagatzematge al *cloud* per aprofitar l'espai d'emmagatzematge no utilitzat. Actualment hi ha un projecte planificat per a ser implementat a l'empresa Ilimit Cloud & Telecom.

7.2 Inconvenients trobats

L'objectiu inicial s'ha completat satisfactòriament juntament amb les subtasques d'anàlisis de la plataforma. On s'han trobat inconvenients ha estat a l'hora d'analitzar la blockchain en un node local. El node s'ha pogut crear, sincronitzar i interectuar amb la xarxa a través del client de Sia. Quan s'ha utilitzat l'explorador de la API que ofereix Sia per analitzar la blockchain les dades que s'obtenien no eren correctes o eren incompletes. A través de canals de comunicació com Reddit s'ha trobat que NebulousLabs anuncia que de moment l'explorador es troba inacabat. Per aquest motiu s'ha deixat de banda aquest objectiu i s'ha seguit aprofunditzant en la plataforma Sia.

AGRAÏMENTS

M'agradaria agraïr al meu tutor en Jordi Herrera per descobrirme aquest apassionant món de les criptomonedes.
A tots aquells que durant el camí m'heu donat ànims.
I especialment a la meva parella per confiar sempre en mi.

REFERÈNCIES

[1] D. Vorick and L. Champine, *Sia: Simple Decentralized Storage.* Boston, United States: Nebulous, Inc. , 2014. [Online]. Available: https://sia.tech/sia.pdf.

[2] Protocol Labs, *Filecoin: A Decentralized Storage Network.* San Francisco, United States: Protocol Labs. , 2017. [Online]. Available: https://filecoin.io/filecoin.pdf.

[3] S.Wilkinson and T.Boshevski, *Storj A Peer-to-Peer Cloud Storage Network.* Atlanta, Georgia, United States: Nebulous, Inc. , 2016. [Online]. Available: https://storj.io/storj.pdf.

[4] J.Benet, *IPFS - Content Addressed, Versioned, P2P File System.*United States, 2014. [Online]. Available: https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL 6X1o4k7zrJa3LX/ipfs.draft3.pdf.

[5] V.Buterin, *Ethereum White paper.* United States, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[6] R.CMerkle, *Protocols for public key cryptosystem.* IEEE Computer Society, 1980. Pages [122-133].

[7] B.Schneier, J.Kelsey, D.Ehiting, N.Ferguson, D.Wagner and C.Hall, *Twofish: A 128-Bit Block Cipher.* Minneapolis, United States, 1998. [Online]. Available: https://www.schneier.com/academic/paperfiles/paper-twofish-paper.pdf.

[8] V.Guruswami and M.Wootters, *Repairing Reed-Solomon Codes.* Minneapolis, IEEE Transactions on Information Theory, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7922614/.

[9] A. Wirdum, *Ünderstanding the Lightning Network, Part 1: Building a Bidirectional Bitcoin Payment Channel.* Bitcoin Magazine, 2017. [Online]. Available: https://bitcoinmagazine.com/articles/understanding-the-lightning-network-part-building-a-bidirectional-payment-channel-1464710791/.

[10] S.Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[11] A.Biryukow and D.Khovratovich, *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem.* [Online]. Available: https://www.cryptolux.org/images/b/b9/ Equihash.pdf.

[12] A.Biryukow and D.Khovratovich, *Birthday problem.* [Online]. Available: https://en.wikipedia.org/wiki/Birthday_problem.

[13] R.Campbell, *Krypton Abandons Ethereum for Bitcoin Proof of Stake Blockchain after 51% Attack.* [Online]. Available:https://www.ccn.com/krypton-ethereum-bitcoin-proof-of-stake-blockchain-after-51-attack/.

APÈNDIX

Estructures de dades

Camp	Descripció
SiacoinInputs	Volum de monedes Siacoin entrant, provenen d'un output, per tant és un Output ID. Línies tx [2-18]
SiacoinOutputs	Volum de monedes Siacoin sortint. Línies tx1[19-28]
FileContracts	Acord entre el proveïdor d'emmagatzematge i els seus clients. Línies tx1[29-51]
FileContractRevisions	Revisió d'un contracte existent. Línies tx1[52]
StorageProofs	Prova d'emmagatzematge. Línies tx1[53-63]
SiafundInputs	Volum de monedes Siafund entrant, provenen d'un output, per tant és un Output ID. Línies tx1[64-79]
SiafundOutputs	Volum de monedes Siafund sortint. Línies tx1[80-91]
Miner Fee	Recompensa del miner. Línies tx1[92]
ArbitraryData	Utilitzades per metadata i emmagatzematge d'estructures de dades com el "HostAnnouncement" codificades en base 64. Línies tx1[93-95]
TransactionSignatures	Signatures de clau pública. Línies tx1[96]

1.Estructura d'una transacció.

Camp	Descripció
Specifier	Camp de text amb la cadena: "HostAnnouncement". Línies tx1[93-95]
NetAddress	Direcció IP del host. Línies tx1[93-95]
PublicKey	Clau pública del host. Línies tx1[93-95]

2.Estructura del Host Announcement.

Camp	Descripció
FileContractId	Identificador del contracte. Línies tx1[29]
FileSize	Mida de les dades que es volen emmagatzemar. Línies tx1[31]
FileMerkleRoot	L'arrel de l'arbre de merkle creat a partir del particionat de les dades. Línies tx1[32]
WindowStart	Alçada de block on el host pot començar a emetre una proof of storage. Línies tx1[33]
WindowEnd	Alçada de block límit emetre una proof of storage. Línies tx1[34]
Payout	És la suma de ValidProofOutputs i MissedProofOutputs menys el 3,9% de fees que van a parar a la SiafunPool. Línies tx1[35]
ValidProofOutputs	Es creen SiacoinOutputs amb destí al host perquè ha superat les proves. Línies tx1[36-41]
MissedProofOutputs	Es creen SiacoinOutputs amb destí al client perquè el host no ha superat les proves. Línies tx1[42-47]
UnlockHash	Hash de les unlockConditions. Línies tx1[48]
RevisionNumber	Marca la versió del contracte. Línies tx1[49]

3.Estructura del File contract.

Camp	Descripció
ParentID	Identificador del contracte. Línies tx1[55]
Segment	Part de les dades que es mostren com a prova d'emmagatzematge. Aquest es tria de forma aleatòria. Línies tx1[56]
HashSet	Llistat de hashs del fitxer de l'arbre Merkle per verificar que el segment forma part de les dades originals. Línies tx1[57-61]

4.Estructura del Storage proof.

Transacció

```
"4b546dacff2ed0a... 256bits": {
     "siacoininputs": {
        "eed87bca77a35d03ea... 256bits": {
         "parentid": "eed87bca77a35d03e... 256bits",
         "unlockconditions": {
           "timelock": 0,
           "publickeys": [
              {
               "algorithm": "ed25519",
                "key": "ta5IazCP4... pubKey"
              }
         ],
         "signaturesrequired": 1
        }
      }
    },
    "siacoinoutputs": {
      "371d6a7ad10e3dce85... 256bits": {
        "value": "1804530529198723858443116000",
        "unlockhash": "f1d2b3fdbd3... 256bits"
      },
      "fddebd4bf6cd21ece1... 256bits": {
        "value": "93304717345703397243600",
        "unlockhash": "746d3d30931... 256bits"
      }
    },
    "filecontracts": {
       "eb328ca105bdde95... 256bits": {
        "filesize": 0,
        "filemerkleroot": "000000000000000... 256bits",
        "windowstart": 155685,
        "windowend": 155829,
        "payout": "10210453333333332691785169",
        "validproofoutputs": {
          "0788008d3ade937ed7... 256bits": {
            "value": "66052266666666625118503",
            "unlockhash": "a8664aecf812439... 256bits"
          }
        },
        "missedproofoutputs": {
          "0cc4dbd9e3e26d166cb71d... 256bits": {
            "value": "66052266666666625118503",
            "unlockhash": "a8664aecf812439... 256bits"
          }
        },
        "unlockhash": "076d53824d4885e3ae... 256bits",
        "revisionnumber": 0
      }
    },
    "filecontractrevisions": [],
    "storageproofs": {
       "eb328ca105bdde95... 256bits": {
         "parentid": "eb328ca105bdde95... 256bits",
         "segment": [15,205,24,93,169,...   ],
         "hashset": [
           "19ce32277baedbc5cd6... 256bits",
           "c197b62e5f194969520... 256bits",
           ...
         ]
      }
    },,
    "siafundinputs": {
     "6ec14e95b863508b3ac5497... 256bits": {
        "parentid": "6ec14e95b863508b3ac... 256bits",
        "unlockconditions": {
         "timelock": 0,
          "publickeys": [
            {
              "algorithm": "ed25519",
              "key": "eh51luVXO1b1H5... pubkey"
            }
          ],
          "signaturesrequired": 1
        },
        "claimunlockhash": "a544695cb2bfe0c... 256bits"
      }
    },
    "siafundoutputs": {
      "34dfdb1d7ac4a4136b043c9c2... 256bits": {
        "value": "221",
        "unlockhash": "3ff06fad9410... 256bits",
        "claimstart": "0"
      },
      "d5bb235950cf8309ce45f7a90... 256bits": {
        "value": "1",
        "unlockhash": "273dcb9f1184... 256bits",
       "claimstart": "0"
      }
    },
    "minerfees": null,
     "arbitrarydata": [
      "SG9zdEFubm91bmNl... encoded into byte slices"
    ],
    "transactionsignatures": null
},
```

5.Exemple d'una transacció (tx).
Dades extretes de la API de https://siahub.readme.io/v1.0/docs