Estudi de la blockchain de Polkadot

Alex Binué Sampedro

Resum— Polkadot, és un projecte de codi obert, desenvolupat per la Fundació Web3, llançat al Maig del 2020. És tracta d'un protocol compartit que busca la possibilitat que les blockchains puguin operar de manera conjunta, és a dir, busca crear una xarxa unificada, formada per l'agrupació de diferents blockchains. Es tracta d'una cadena multi-chain, escalable, col.laborativa i heterogènia. Està formada per dues components claus, el primer anomenat cadena de relleus, en anglès *relay chain* el qual la seva funció és interactuar amb cadenes fragmentades, que s'executen de forma paral.lela, conegudes com a *parachains*.

Paraules clau— Polkadot, Blockchain, multi-chain, DOT, escalabilitat, Relay Chain, Parachains, NPoS, BABE,GRANDPA, Layer 1, Layer 2, Layer 0, Substrate, Sharding, fees, slots, bridges, validators, nominators, collators, ERA, VRF, prova de validació, arbre de Merkle, hash, candidate receipt, erasure coding, auction.

Abstract— Polkadot is an open source project, developed by the Web3 Foundation, launched in May 2020. It is a shared protocol that seeks the possibility that blockchains can operate together, that is, it seeks to create a unified network, formed by the grouping of different blockchains. It is a multi-chain chain, scalable, collaborative and heterogeneous. It consists of two key components, the first called relay chain,whose function is to interact with fragmented strings, which run parallelly, known as parachains.

Index Terms— Polkadot, Blockchain, multi-chain, DOT, escalability, Relay Chain, Parachains, NPoS, BABE, GRANDPA, Layer 1, Layer 2, Layer 0, Substrate, Sharding, fees, slots, bridges, validators, nominators, collators, ERA, VRF, proof of validity, Merkle tree, hash, candidate receipt, erasure coding, auction.

1 Introducció - Context del treball

En aquest document es presenta el treball dut a terme per investigar sobre l'estudi de la blockchain de Polkadot, els mecanismes d'integració de les parachains i la seva comunicació.

La criptomoneda Polkadot és una blockchain de nova generació que intenta promoure un ecosistema multi-chain, és a dir, un entorn heterogeni on puguin coexistir diferents cadenes o Blockchains.

Impulsada per DOT, la moneda nativa de la xarxa i mitjançant aquesta, l'ecosistema de Polkadot intenta resoldre molts dels problemes i limitacions que tenen avui en dia *les blockchains*, com l'escalabilitat, la capacitat de mantenir el seu rendiment a mesura que augmenta la seva mida, i la seguretat, entre d'altres.

- *E-mail de contacte: alex.binue@uab.cat*
- *Menció realitzada: Tecnologies de la Informació*
- *Treball tutoritzat per: Jordi Herrera Joancomartí (departament)*
- *Curs 2021/22*

Polkadot a més de ser una blockchain pública, es tracta d'una blockchain *permissionless*, fet que garanteix, un marc de seguretat i interoperabilitat a totes les xarxes connectades, les quals poden tenir els seus propis ecosistemes, màquines virtuals i consens totalment independent de la *relay chain* [1].

2 Objectius

Com ja s'ha esmentat anteriorment, l'objectiu del projecte és estudiar la blockchain de Polkadot així com el mecanismes d'integració dels diferents components, donant èmfasi en la integració de les diferents cadenes de blocs, les *parachains*, en una cadena central, coneguda com a *Relay Chain*. Tot aquest estudi s'aconsegueix mitjançant la recerca online de webs, documents, articles d'opinió i vídeos explicatius.

A partir d'aquest estudi, podrem aprofundir i desenvolupar un conjunt de conceptes que ens ajudaran a entendre que, com i perquè existeix cadascun dels mecanismes, components, protocols i estructures de Polkadot.

2.1 Objectius principals

El treball consistirà en dues parts, un marc teòric i un marc pràctic

Per aconseguir la finalitat del projecte, s'han planejat un conjunt d'objectius principals a desenvolupar:

- Introducció i estructura a Polkadot
- Característiques i funcionament de la Relay Chain de Polkadot.
- Protocol de Consens
- Block Production: BABE i Finality Gadget: GRANDPA.
- Parachains, parathreads i Bridges.
- Protocol d'interoperabilitat i comunicación entre aplicacions cross-chain XCMP.

Per altra banda, el marc pràctic, consistirà en la implementació d'una Blockchain amb la finalitat que pugui ser una Parachain integrada a la Relay Chain mitjançant Substrate, un Framework modular i flexible que facilita la creació d'una Blockchain personalitzada, que permet combinar diferents components predefinits i desenvolupar una lògica empresarial deixant tota la resta del treball al *Framework*.

Per tant, de forma resumida, els objectius de la part pràctica seran els següents:

1. Instal·lar Substrate a la nostra VM.

2. Preparar el nostre node de Substrate utilitzant un template node.

3. Executar el node Blockchain, aquesta serà la nostra Parachain.

4. Transferir fons d'un compte a un altre, per assegurarnos que la nostra Blockchain esta funcionant [2].

3 METODOLOGIA

A l'hora d'escollir la metodologia a aplicar en aquest projecte, se'ns plantegen diverses alternatives. Per una banda, podem escollir una metodologia més tradicional, com pot ser la metodologia de cascada, on els projectes s'executen seguint un ordre seqüencial: **Iniciació > Planificació** > **Execució** > **Mesurament**, seguint una sola direcció i sense possibles canvis. El problema d'aquesta metodologia, i per la qual han sorgit de noves, és el fet que, s'ha de fer una fase de captura de requeriments molt elevada i a la vegada ha de ser única, ja que després ja no es pot tornar enrere per fer canvis. Aquesta metodologia és idònia, per a projectes on ja es té una gran quantitat d'experiència amb el producte en qüestió i quan tens la certesa que els requisits no canviaran, proporcionant així un entorn amb unes condicions estables i conegudes [3].

En el nostre cas, com que tot està en continu canvi, desenvolupament i que mai podem assegurar que tot sortirà segons el que estava previst, escollirem les metodologies àgils com a metodologia per a aplicar. Aquestes metodologies es caracteritzen per ser adaptatives i flexibles, és a dir, no són reticents als canvis, ja que els canvis es consideren successos esperats i que s'han de tractar amb normalitat. Amb això aconseguirem reduir les probabilitats de fracassar ja sigui per subestimar costos, temps o funcionalitat.

Optarem doncs per utilitzar Scrum com a metodologia a seguir per a dur a terme tot el procés de desenvolupament del TFG. Els avantatges d'escollir aquesta metodologia, per exemple, són: la dinàmica que permet reorganitzar i afegir noves funcionalitats, el fet d'oferir una millora en cada sprint, poder dissenyar abans de desenvolupar codi, entre d'altres. Per això considerem que aquesta opció és més adient respecte els avantatges que ens poden oferir les altres metodologies.

Tenint en compte les fases o condicions que estableix la metodología escollida, s'ha detallat un ordre cronòlogic que es durà terme, per a desenvolupar el pla de projecte, mostrant les setmanes de duració de cada tasca, les tasques crítiques, els milestones i les tasques independents mitjançant l'eina *click up* [3].

4 ESTAT DE L'ART

Existeixen projectes com Bitcoin o Ethereum inicialment desenvolupats amb una sola capa, **Layer 1** (blockchain de Bitcoin/Ethereum) on a mesura que ha evolucionat el mon de les criptomonedes, han hagut de desenvolupar una segona capa en la seva *blockchain*, per problemes d'entre d'altres d'escalabilitat, **Layer 2**. En la **Layer 2** s'executen diferents operacions que no necessàriament han de quedar registrades en la blockchain, sinó que només es guarda l'estat inicial i l'estat final del conjunt d'operacions executades.

Polkadot en aquest sentit és un avançat respecte a la resta, mitjançant la fragmentació (model de sharding) juntament amb la seva arquitectura diferencialista, Relay Chain – Parachain, ha aconseguit desenvolupar un ecosistema on precisament hi ha una **Layer 1**, la *Relay Chain*, envoltada d'un conjunt de *parachains* que funcionarien com una **Layer 2**. Tot això fa funcionar a Polkadot com un protocol de **Layer 0**, protocol que uneix múltiples blockchain especialitzades en una xarxa unificada i escalable.

Desenvolupant aquesta separació de capes, s'aconsegueix per exemple reduir els problemes d'escalabilitat, augmentant la capacitat i la velocitat de les transaccions a la **Layer 1**. És a dir, fan el protocol molt més escalable en tots els sentits.

També dota a la **Layer 2** la capacitat de processar i executar transaccions de forma molt més rapida a la vegada que redueixen la carrega de la **Layer 1**, i pel general, tenen unes *fees* molt més baixes [4].

5. LA BLOCKHAIN DE POLKADOT

5.1 Origen

La història de Polkadot té una forta vinculació i associació a una altra criptomoneda, Ethereum. El seu fundador és el Dr. Gavin Wood, que va ser un dels directors de capacitació i desenvolupament principal d'Ethereum. Va desenvolupar el llenguatge de programació dels Smart Contracts, Solidity.

Tot i que Ethereum s'ha convertit en la segona *blockchain* més utilitzada al món després de Bitcoin, amb una capitalització de més de $330 bilions, tanmateix, aquest enorme creixement i gran potencial no va ser suficient per a Wood, qui va decidir abandonar el projecte per buscar nous reptes. Considerava que Ethereum havia esdevingut una xarxa que competia per dominar el món de la blockchain que cada vegada abastava més multitud.

Volia crear un nou ecosistema *multi-blockchain* que servis com a pont per altres blockchains, eliminant aixi el que Wood considera com un conjunt de sistemes legals, independents i aïllats d'Internet. Una de les principals raons que volia abordar amb Polkadot era intentar moure a la gent cap a un ecosistema menys criptonacionalista, on tinguéssim moltes cadenes diferents operant sobre un sistema comú, i intentar reduir la idea que si ets part d'una, no pots ser part d'una altre, una cosa que considerava molt freqüent en l'ecosistema de les criptomonedes especialment arrel dels seus problemes amb el món de Bitcoin.

Així va succeir, quan el 2016, va involucrar-se en el desenvolupament i la construcció d'una *blockchain* més fragmentada que la d'Ethereum, i a l'octubre del mateix any va publicar el *white paper* de Polkadot [5].

5.2 Token DOT

El token natiu de Polkadot és DOT, un token inflacionari amb una emissió actual de 987,579,319 DOT**.** El preu actual del token és de 9$ a 20 de Juny de 2022, amb una capitalització de 18,363,247,802$ [6].

No s'utilitza simplement com un token amb valor al mercat i per pagar les *fees* de les transaccions, sinó que manté el funcionament correcte de tota la xarxa i compleix tres funcions claus en l'ecosistema de Polkadot:

-**Governança:** Els usuaris que posseeixen els tokens de Polkadot exerceixen un control complet sobre el protocol de la plataforma. Tots els privilegis que són exclusius per als miners en altres plataformes, s'atorguen als participants de la Relay Chain, coneguts com a DOT *holders*, inclós la capacitat de gestionar esdeveniments excepcionals, com actualitzacions i correccions de protocols. Aquest fet és una característica molt usual de les xarxes que utilitzen Proof of Stake com a protocol de validació.

-***Staking***: La segona funció del token DOT serà facilitar el mecanisme de consens que utilitza Polkadot. Perquè la plataforma funcioni i permeti que es realitzin transaccions vàlides a través de les parachains, s'incentiva l'ús correcte de tokens DOT als posseïdors mitjançant la teoria de jocs. Polkadot confiarà que els usuaris exerceixin un paper actiu en el sistema, de forma que, posaran en risc els seus DOTs, el que es coneix com *staking*, per dur a terme aquestes funcions, de forma que una participació incorrecta es considerarà com un desincentiu i suposarà una pèrdua de participació. D'altra banda, els participants amb un comportament que contribueixi al correcte funcionament de la xarxa rebran un incentiu mitjançant una política de recompensa que atorga el sistema.

La quantitat de DOT requerida per participar en la xarxa pot variar segons l'activitat realitzada, la duració del *staking* i el nombre total de DOT *staked*.

-***Bonding***: Aquesta funció s'encarrega d'afegir noves *parachains* a la relay chain, vinculant aquest token com una unió, *bonding* en anglès, amb la nova *parachain*. DOT es bloqueja durant el període de bonding i es retorna a l'usuari que ha fet la unió després que transcorri la durada de l'enllaç i s'elimini la *parachain*.

D'aquesta forma aconseguim dues coses, incentivar als usuaris validadors a actuar amb honestedat al tenir un interès financer en l'autenticitat del procés de verificació i validació i alhora permetre eliminar aquelles *parachains* obsoletes o que no s'utilitzin enllaçades al sistema, de forma que, no només elimina la parachain sino també els tokens vinculats a ella [7].

5.3 Estructura

La idea de la xarxa de Polkadot es pot representar mitjançant la figura 1:

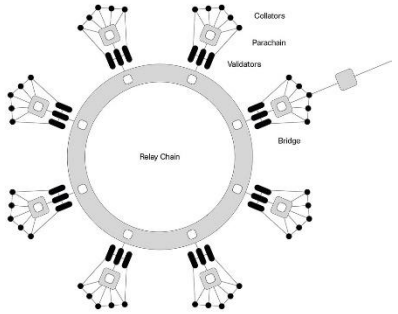

Figura 1. Estructura general de Polkadot.

L'ecosistema de Polkadot està format per 3 peces claus:

***Relay Chain*:** És l'eix central de la xarxa de Polkadot i s'encarrega entre d'altres de garantir la seguretat de les *parachains* i és responsable d'intercanviar missatges.
Parachain: És una blockchain independent de la *relay chain*, però connectada a la xarxa principal, proporciona els blocs per la *relay chain*.
***Bridges*:** Serveix com a blockchain per a certes aplicacions descentralitzades i també actua com a pont per connectar serveix externs o altres *blockchains*. [8].

5.4 Relay Chain de Polkadot

Molts projectes estan treballant per construir arquitectures *relay* on la comunicació es *two-way*, permetent així la interoperabilitat entre cadenes, mitjançant un enllaç central anomenat *relay chain*. Les *relay chain* són *blockchains* que funcionen com a node central pels altres membres, les *blockchains* connectades. Els membres poden aprofitar la informació de les altres cadenes enviant missatges que passen a través de la *relay chain*, que s'encarrega de fer un seguiment de l'estat de totes les cadenes connectades i de la seva comunicació, i en certes situacions poden atorgar privilegis en el control dels actius. Les arquitectures *relay chain* són molt eficaces en entorns en els quals les cadenes tenen certes característiques com la capacitat de multisignatura i un protocol de consens ràpid.

Les funcions de la *relay chain* són mínimes i per així només conte un nombre reduït de transaccions de diferents tipus que incloeixen interaccions amb el mecanisme de governança, les subhastes de *parachains*, més endavant en parlarem i el procés de participació en NPoS, Nominated Proof Of Stake. La relay chain té un nombre limitat *d'slots* o ranures per a les parachains. L'objectiu de Polkadot és anar augmentat aquest espai fins arribar a 1000 slots, i a llarg termini, es vol introduir un nou concepte anomenat nested Relay Chain, que ens permetrà arribar a un nombre il·limitat de parachains per desenvolupar

així un entorn quasi infinit i altament escalable .

6. El Mecanisme De Consens

En el món Blockchain, el procés de crear un bloc de transaccions i afegir-lo de forma definitiva a la cadena principal s'anomenat segellat o minat. Quan un bloc queda segellat, la informació que conté pasa a formar part de la cadena principal, i es torna immutable i inalterable. El protocol de consens és el mecanisme que regula la forma com els nodes que fan el segellat de blocs arriben a un acord per poder fer-ho i així incorporar el bloc a la cadena. Perquè l'estat d'una *blockchain* segueixi desenvolupant-se i avançant, tots els nodes de la xarxa han d'estar d'acord i arribar a un consens. És la forma en què els nodes d'una xarxa descentralitzada poden estar sincronitzats entre si. No és més que l'acceptació de tots els membres de la xarxa blockchain que la informació que hi ha en aquesta és correcta i no ha patit cap manipulació, ni té dades errònies o duplicades.

Per evitar que s'afegeixin blocs incorrectes a la blockchain, cadascun d'aquests blocs necessiten estar revisats i confirmats, aquest procés succeeix en totes les *blockchains* i la primera en implementar-ho i utilitzar-ho va ser Bitcoin (PoW).

Quan no s'arriba a un consens segons les normes estipulades que nodes i miners estableixen per incloure i validar la informació d'un bloc dintre de la *blockchain*, es donen situacions que produeixen bifurcacions en la cadena. La funció més important del consens és evitar situacions en les quals la informació en la cadena sigui inconsistent amb les regles definides per ella mateixa. Per exemple, en una *blockchain* d'una criptomoneda, el consens evita la doble despesa, situacions en què una persona utilitza una quantitat de criptomonedes per realitzar una transacció de compra i després de fer-ho, reverteix el procés manipulant la informació del bloc on es troben les transaccions anteriors, eliminant la informació del bloc on es troba registrada la transacció i així poder tornar a gastar aquestes criptomonedes [9].

6.1 Nominated Proof of Stake

En els sistemes de PoS (Proof of Stake) tradicionals, participar en el procés de producció de blocs depèn en gran manera de la quantitat de tokens en possessió, en lloc de la potència computacional. Tot i que els desenvolupadors de PoS són grans defensors d'una participació equitativa de forma descentralitzada, la majoria de projectes acaben esdevenint projectes amb alguns nivells d'operacions centralitzats on per exemple, el nombre de validadors amb poder de participació és limitat. Com a conseqüència, aquests validadors acaben sent els més rics i influeixen en la xarxa PoS, ja que són els més apostats. A més, el nombre de candidats per mantenir la xarxa que tinguin coneixements i equipament necessaris també és limitat, raó per la qual els sistemes amb un gran nombre de validadors tendeixen a formar agrupacions per reduir la variància dels seus ingressos i obtenir beneficis de l'economia d'escala. Una manera de reduir aquest comportament és permetent la formació de diversos grups a la cadena i donar la possibilitat als titulars dels tokens de votar, fent dipòsit, perquè els validadors els representin.

Polkadot implementa NPoS (Nominated Proof-of-Stake) com a mecanisme per seleccionar el conjunt de validadors que poden participar en el protocol de consens. Està dissenyat amb els rols de *validators* i *nominators*, per maximitzar la seguretat de la cadena. Qualsevol usuari que estigui interessat a mantenir la xarxa pot executar un node validador.

Els validadors assumeixen la funció d'afegir nous blocs a la blockchain (BABE), validar els blocs de les *parachains*. Els nominadors poden recolzar als validadors seleccionats amb la seva participació, *staking* i poden aprovar candidats en els quals confien i recolzar-los també amb els seus tokens [10].

6.2 Rols en el sistema de consens

Per a un correcte funcionament del mecanisme de consens, NPoS està format per 4 rols que doten d'autonomia a l'ecosistema [11].

-Validadors (en anglès *Validators*): Produeixen blocs per la Relay Chain i l'asseguren a través del *staking* de DOTs tant propis com dels ***nominators***. Validen les dades, blocs de les parachains i les proves de validació, PoV, dels ***Col·lectors*** en consens amb altres validadors, veure figura 2. A canvi reben recompenses de participació.
Per ser un *validator* has de tenir uns requeriments tècnics, de hardware, mínims per poder executar el teu node.

Figura 2. Estructura dels *Validators* dintre de l'ecosistema de Polkadot.

-Nominadors (en anglès *Nominators*): Són els encarregats d'escollir validadors confiables per fer *Staking* dels seus DOTs, veure figura 3. Vinculen la seva participació a ***validators*** particulars, per ajudar a estar entre els validadors més actius i així poder produir blocs per la *Relay Chain*. Els nominators seran recompensats amb una part de la participació obtinguda pel ***validator.*** Cal dir que els nominators no han de tenir la potència de càlcul dels *validators*. Per participar en el procés de selecció només han de tenir una participació de 120 DOT, el que es considera com *minimum bond*.

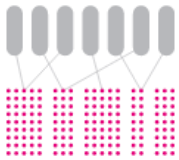

Figura 3. Estructura dels *Nominators* dintre de l'ecosistema de Polkadot.

-**Col.lectors (en anglès *Collators)***: Són nodes complets presents tant en una *parachain* com en la *relay chain*. Els collators actuen com un node complet per a una parachain en particular, el que significa que retenen tota la informació necessària per crear nous blocs i executar transaccions de la mateixa manera que els miners ho fan a la cadena de blocs PoW (Proof of Work), veure figura 4. Recopil.len i executen transaccions per crear un bloc sense segellat i el proporcionaran juntament amb una prova de validació, PoV, a un o més validadors responsables de proposar un bloc de la parachain. També poden enviar i rebre missatges d'altres *parachains* utilitzant el protocol d'intercanvi de missatges XCMP.

Figura 4. Estructura dels *Collators* dintre de l'ecosistema de Polkadot.

-**Pescadors (en anglès *Fishermen)***: Fan un monitoreig de la xarxa i informen del mal comportament als ***validators***, veure figura 5. Els ***collators***, o qualsevol altre node complet de la Parachain, pot actuar com a ***Fishermen*** . Necessiten tenir DOTs en stake per funcionar, com a mecanisme anti-spam, sinó podrien fabricar alertes invàlides.

Figura 5. Estructura dels *Fishermen* dintre de l'ecosistema de Polkadot.

6.3 Funcionament

És possible nomenar a un *validator* mitjançant interfície d'usuari de Polkadot-JS, veure figura 6. Un *nominator* pot nomenar fins a 256 *validators*, però només 16 poden ser escollits. Una vegada els *validators* són seleccionats, les nominacions estaran actives durant la següent *ERA* (~24h) . Per cada 24-hores, una *ERA*, el sistema escollirà 297 *validators*. El treball que desenvoluparan els *validators* serà molt complex, hauran d'executar operacions costoses, garantir una alta capacitat de resposta en les comunicacions i construir una reputació confiable amb els altres validators. També hauran dipositat els seus DOTs, juntament amb els DOTs dipositats pels nominators en el seu favor, veient-se reduït aquest dipòsit (*gets slashed*), cada cop que es desvien de les seves funcions.Al contrari se'ls pagarà bé quan compleixen les normes i segueixen les regles. Qualsevol node que pugui ser capaç d'executar les tasques, es pot oferir públicament com a *validator*. Fins al moment, el node *validator* amb menys quantitat de participació triat a la xarxa ha sigut de 1,75M de DOT mitjançant el recolzament d'uns 18.000 *nominators*.

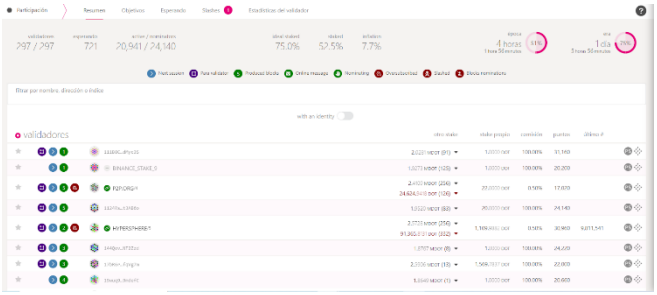

Figura 6. Interfície d'usuari de Polkadot on es poden veure els llistats de *validators*.

Per una altra banda, el sistema anima a qualsevol titular de DOT a participar en el procés com a *nominator*. Com a *nominator*, publiques una llista de candidats a *validators* segons la teva confiança, posant una quantitat de DOTs en dipòsit per donar-li support. Si algun d'aquest *validators* és escollit, el nominator comparteix amb ell tant els beneficis com les sancions rebudes, segons el % de DOT en dipòsit. A diferència dels *validators*, la quantitat de nominators que poden participar són il.limitats. Sempre que un *nominator* sigui honest amb la seva elecció i només doni suport als *validators* amb bones pràctiques de seguretat, el seu dipòsit tindrà un risc molt baix de perdre diners i proporcionarà una font continua d'ingressos [12].

Aquesta relació *nominator-validator* produeix un vincle de seguretat molt elevada. Permet al sistema escollir *validators*, que tinguin una gran quantitat de DOTs com a suport, molt més gran que una entitat que es pugui presentar de forma única i suprimint així els de stake més reduït. Tot això provoca, per exemple, que per a una entitat maliciosa sigui impossible ser escollida com a *validator*, ja que hauria de tenir una reputació i una confiança molt elevada, i estar preparada per a patir moltes pèrdues del dipòsit de DOTs, cada cop que intenti atacar al sistema i aquest respongui reduint la seva quantitat de DOTs, fet que, resultarà quasi impossible de succeir.

6.3.1 Selecció dels *validators*

A diferència d'altres projectes que utilitzen PoS, on els validadors es trien per la seva capacitat de dipòsit, és a dir, per la quantitat de monedes que posen ells mateixos com a suport, Polkadot otorga la capacitat als *validators* escollits de tenir el mateix poder per votar i decidir en el protocol de consens. El sistema ho fan repartint el dipòsit entre els *validators* seleccionats de la manera més uniforme possible, respectant sempre les preferències dels *nominators*.

Per fer aquesta selecció Polkadot implementa dos conceptes clau per desenvolupar un procés de selecció eficient que ofereixi seguretat i una representació justa, conceptes que es poden aplicar en qualsevol blockchain que fa servir NPoS.

Al primer se'l coneix com a *proportional justified representation* [21] i és un mètode desenvolupat pel matemàtic Suec Lars Edvard Phragmén, per triar als membres del parlament

del seu país. La idea principal d'aquest mètode aplicat a la xarxa de Polkadot, és assegurar que cap node o pool de nodes estigui sobrerepresentat ni subrepresentat pels *validators* escollits, sempre mantenint la proporcionalitat.

Suposem que necessitem escollir 4 *validators* pel sistema, n=4 , la propietat de representació justa (fair representation) es tradueix en la regla que qualsevol nominator que tingui un total stake/N ha de tenir garantit que almenys un dels seus *validators* de confiança sigui escollit.

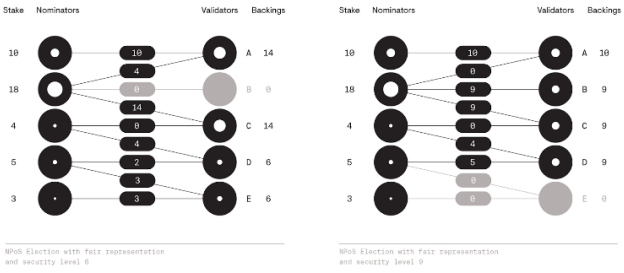

Figura 7. Exemple de les possibles distribucions que faran obtenir un determinat nivell de seguretat i on s'aplicara el concepte de *proportional justified representation*

L'altre concepte molt important a tenir en compte és la seguretat, si un *nominator* aconsegueix tenir dos o més *validators* de la seva confiança, s'ha de distribuir el dipòsit de manera que el total del dipòsit que reben els *validators* sigui el més equilibrat possible per tal d'aconseguir fer que sigui el més difícil possible per a un conjunt d'adversaris obtenir un *validator* escollit, i això només ho podran fer si obtenen un suport molt elevat. Per tant, el nivell de seguretat del resultat d'una elecció s'aconseguirà com la quantitat mínima de suport que ha de tenir qualsevol *validator* escollit.

Com podem observar en la figura 7, el resultat d'escollir l'opció de la dreta obté un major nivell de seguretat i clarament ho aconsegueix dividint la participació dels *nominators* en suport als *validators* d'aproximadament la mateixa mida [13].

6.4 GENERACIÓ I FINALITZACIÓ DE BLOCS

6.4.1 BABE

BABE (*Blind Assignment for Blockchain Extension*) és el mecanisme de producció de blocs que s'executa entre els nodes validators i determina els autors de nous blocs. En aquest mecanisme, el temps es divideix en èpoques, *epochs*. Cada *epoch* es divideix al seu temps en unitats de temps més petites anomenades *slots*, de 6 segons de durada, 2400 *slots* formen una *epoch*, la qual cosa fa que les *epoch* tinguin una durada de 4 hores. Un bloc és produït en cada *slot*.

Al principi de cada *slot*, tots els *validators* seleccionats participen en una loteria per determinar per quin *slot* seran els encarregats de produir el bloc. Executen una funció (VRF) que utilitza com a input d'entrada els següents paràmetres:

- ***The "secret key" sk_v/j:*** Cada validator té la seva propia parella de claus de firma pública-privada, creada especificament per aquest procés.
- ***An epoch randomness value r_m,*** que es el hash dels valors obtinguts de l'execució del VRF dels blocs en l'època anterior a l'últim (N-2), per la qual cosa l'aleatorietat passada afecta a l'aleatorietat actual pendent (N)
- **El número *d'slot sl_k*.**

L'output genera dos valors: el **RESULTAT** (el valor random) i una **PROVA** (de que el valor aleatori s'ha generat correctament), veure Figura 8. Com que aquest procés es determinista, ja que es basa en dades de la cadena de blocs d'epoques anteriors, altres *validators* han de poder verificar-ho, és per això que es crea aquesta prova, que juntament amb la clau pública del *validator*, es pot comprovar que ha sigut correctament generat [17].

$$\mathsf{VRF}_{\mathsf{sk}_j^v}(r_m||sl_k) \rightarrow (d, \pi)$$

Figura 8. Fòrmula per al càlcul del VRF.

El **RESULTAT** es compara amb un llindar, *threshold*, definit en la implementació del protocol, veure figura 9. Si el valor és menor que aquest llindar, llavors el *validator* que obtingui aquest valor esdevindrà un candidat viable per la producció de blocs per aquell *slot*. Posteriorment, el validator intentara crear un bloc i l'enviarà a la xarxa juntament amb la **PROVA** i el **RESULTAT.** Aquestes assignacions inicialment es troben en secret, només conegudes pels *validators* assignats i es quan volen reclamar públicament aquell slot per produir un bloc, quan es fan públiques.

Slot i	VRF output
1	37
2	72
3	14
4	42

Threshold = 20

We can make a block

Figura 9. Exemple dels possibles resultats d'executar VRF i els possibles guanyadors.

Degut a aquest mecanisme d'aleatorietat, diversos *validators* podrien ser candidats per al mateix slot. En altres casos, un slot podria estar buit (situacions que es poden minimitzar incorporant més validators a la xarxa de Polkadot). Aquestes situacions es gestionen utilitzant els següents mecanismes:

-Multiple validators per slot: Quan es produeixen situacions on es seleccionen múltiples *validators* per produir blocs en un slot determinat, tots els *validators* produiran els seus blocs i els transmeten a la xarxa. El mecanisme que utilitza Polkadot, el mateix que Bitcoin, el qual depèn de la topologia i la latencia de la xarxa, guanya el validator el qual el seu bloc arribi primer a la major part de la xarxa. Ambdues cadenes es continuaran construint individualment fins que la finalització s'activi utilitzant el protocol ***GRANDPA*** i resolgui aquesta bifurcació.

-No validator selected in slot: una ranura pot romandre aparentment sense blocs quan cap *validator* ha generar un número pseudoaleatori suficientment baix com per ser productor de

blocs per aquell *slot*. Aquesta situació s'evita executant un algoritme secundari de selecció de *validator* d'estil *round-robin* en segon pla. Els validators seleccionats per produir blocs a través d'aquest algoritme sempre produeixen blocs. Aquests blocs secundaris s'ignoren si el pel mateix *slot* es produeix un bloc primari d'un *validator* seleccionat per VRF.

Per tant, cada *slot* té un autor principal i un secundari. Els *primary slot leaders* son assignats de manera random, i com que aquesta funció és random, BABE executa un round-robin per assignar a aquests blocs un *secondary slot leaders* [14].

6.4.2 GRANDPA

GRANDPA (*GHOST-based Recursive Ancestor Deriving Prefix Agreement*) és el mecanisme de finalitat que s'implementa per la Polkadot *Relay Chain*, que garantitza que un bloc estigui en la cadena de blocs canònica. Funciona en un model de xarxa parcialment asincrona on hi hagi ⅔ dels nodes honestos.

Tan aviat com ⅔ dels *validator*s donguin fe d'una cadena que conté un determinat bloc, tots els blocs que condueixen a aquest es finalitzen a la vegada [19].

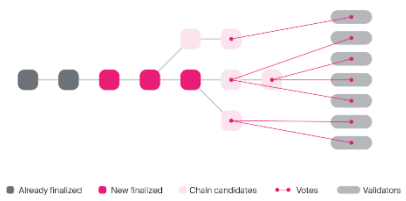

Figura 10. Simulació del procés de finalització, GRANDPA, amb els seus respectius vots.

GRANDPA arriba a acords (votacions) sobre les cadenes de blocs en comptes dels blocs. Com podem veure a la figura 10, representa el procés de votació aplicant GRANDPA per cadascun dels *validators*, el qual emet el seu vot un cop aplicat aquest criteri, la cadena amb més vots serà la cadena que es finalitzarà. La qual cosa accelera de manera enorme el procés de finalització, inclus en circumstàncies de particions de les xarxes a llarg termini o fallades del sistema. El protocol va aplicant vots transitivament i l'algoritme GRANDPA troba el número de bloc més alt amb un número suficient de vots per ser considerat definitiu. Aquest procés permet finalitzar diversos blocs en una ronda, reduint així el coll d'ampolla que en altres casos obstaculitza altres dispositius de finalitat de la blockchain.

6.5 Resolució de Forks

Fins ara, GRANDPA finalitza cadenes i BABE crea nous blocs. Algunes de les cadenes de BABE poden tenir *forks* (bifurcacions) degut a que podem tenir diferents autors per un mateix *slot*.

La primera regla per escollir la millor cadena per estendre és simple: BABE ha de construir sobre una cadena que hagi estat finalitzada per GRANDPA.

Per tant, la millor selecció de cadenes en BABE és aquella on de tots els forks disponibles, els *validators* escolleixen la cadena més llarga amb més blocs primaris després de l'últim bloc finalitzar per GRANDPA, la canonical blockchain.

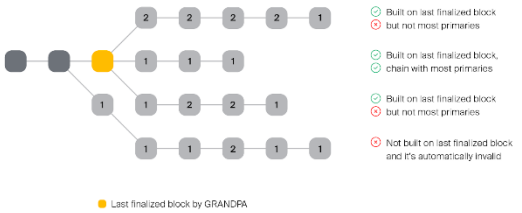

Figura 11. Exemple de la regla de selecció de la millor cadena per diferents forks en BABE.

Com podem veure en la Figura 11, els blocs en negre són blocs finalitzats, el bloc groc és l'últim bloc finalitzat per GRANDPA, per tant aquesta és la canonical blockchain. Els blocs marcats amb un "**1**" són blocs primaris i els blocs amb un "**2**" són blocs secundaris.

A partir d'aquí podem extreure les següents conclusions si apliquem GRANDPA.

De totes aquestes cadenes, la segona cadena es considera la cadena canónica. Encara que tingui menys altura que la 1 i la 3, es construeix utilitzant la major quantitat de blocs primaris i serà la que tingui més vots a GRANDPA [15].

7. PARACHAINS

Una *parachain* és una estructura de dades específica d'una aplicació que és globalment coherent i validable pels *validators* de la *relay chain*. Agafa el seu nom del concepte *parallelized chains* que s'executen en paral.lel amb la *relay chain*. Les *parachains* són *blockchains* connectades a la xarxa de Polkadot. Com altres *blockhains* són màquines d'estat on cada parachain té el seu propi estat, executa un conjunt de transaccions d'estat anomenat bloc i aconsegueix així un nou estat [16].

7.1 Block Creation of Parachain

El procés de creació de blocs de les *parachains* comença pels *parachains collators*. Els *collators* són similars als *validators* en altres xarxes, però aquests no necessiten proporcionar seguretat perquè Polkadot ja s'encarrega d'això.

Cada *parachain* en Polkadot tindrà un conjunt de *validators* de la *relay chain* que accepten i validen els seus blocs, però aquests *validators* no es queden fixats en una sola *parachain*, sinó que un cop fet el seu treball, troben una nova *parachain* on validar blocs gràcies a *BABE*.

Els *validators* utilitzen l'output aleatori que genera *BABE* (el mateix que assigna un *slot* de producció) per determinar quina *parachain* hauran de validar. Un cop el *validator* coneix aquesta *parachain*, busca un *collator* d'aquesta *parachain* i estableix una connexió amb ell. Cada *validator* assignat a una *parachain* importa la funció de transició d'estats correcta per validar la *parachain*. Ara que els *collators* i *validators* comparteixen una connexió, el *collator* podrà enviar un bloc a un dels *validators*.

En resum:

- **Una *parachain* selecciona un *collator* per enviar un bloc a la *Relay Chain*.**

- **Polkadot assinga un conjunt de *validators* (*BABE*) a aquesta *parachain* i**
- **Els *collators* i *validators* estableixen una connexió per enviar un bloc.**

7.2 Block Preparation of Parachain

En el moment que un *validator* rep un bloc, primer comprovarà que el bloc segueix les normes de transició d'estat de la *parachain*.

L'estat d'una parachain és emmagatzemat en un arbre de *Merkle*. Cada punt de dades de l'arbre està format per una clau i un valor per exemple, la clau podria ser un ID del compte i el valor la quantitat de tokens que posseeix. Cada parell de dades es representa amb un *hash* i es converteix en una fulla d'un arbre. Per construir les branques, les fulles adjacents es concatenen i es torna a fer un *hash*, convertint dos parells de dades en un. El procés continua, reduint el nombre total d'elements a la meitat cada vegada, fins que l'arbre en té un únic valor *hash* per representar tota la base de dades, que serà l'arrel estat, veure figura 12.

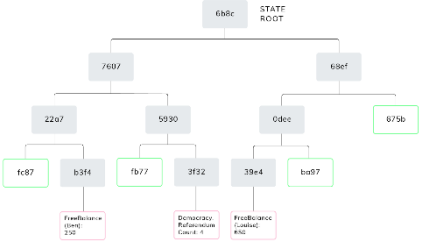

Figura 12. Exemple de validació de transició d'estat.

L'arbre de *Merkle* té una propietat molt interessant: si un valor canvia, es pot verificar aquest canvi només mirant els nous valors i el camí en l'arbre al qual afecta.

Si ens basem en aquesta propietat, un validator podrà verificar una transició d'estat sense tenir accés a l'estat sencer. Només necessita:

-El bloc (llista de transicions d'estat)

-Els valors de la base de dades de la parachain que modifica el bloc i

-Els *hashes* dels punts no afectats de l'arbre.

Aquest conjunt d'informació constitueix la prova de validesa. Com que els hash tenen una longitud fixa no importa la llargada dels valors que no es modifiquen, el *hash* és capaç de representar-los.

Polkadot no garanteix un estat vàlid, Polkadot garanteix una transició d'estat vàlida, que no és el mateix. Els *validators* de Polkadot no inspeccionen cada valor de la parachain, només aquells que han estat modificats, assegurant-se que la modificació és vàlida. Quan una cadena s'uneix a Polkadot, aquest comprova l'estat amb el qual arriba, i és quan s'executa totes les transaccions sota els paraigües de la seguretat de Polkadot, quan té un estat vàlid.

Una vegada el validator té aquesta prova de validesa (PoV) juntament amb el bloc, s'envia aquesta informació a la resta de validators que estan assignats a la parachain. Quan més de la meitat de validators estan d'acord en el fet que el bloc representa una transició d'estats valida, comencen a preparar per anunciar la seva validesa. Per anunciar aquesta validesa, construeixen un *candidate receipt* que formarà part del bloc de la *relay chain* (aquest *candidate receipt* és el que anirà al bloc de la *relay chain*) i un *erasure coding* que s'enviarà a tots els validators de la xarxa .

7.3 Candidate receipt.

En el procés de validació d'una parachain, la informació intercanviada entre els *collators* i els *validators* és molt gran. Aquesta prova de validació (PoV) conté un bloc sencer, si això ho multipliquem per les 100 *parachains* de Polkadot, seria una quantitat molt gran de dades a emmagatzemar. És per això que Polkadot necessita alguna cosa més petita que representi aquestes dades a la *relay chain*: els *candidate receipt.*

Un *validator* construeix un candidate receipt per un bloc de la parachain mitjançant la signatura de:

- **L'ID de la *parachain*.**
- **L'ID del *collator* i la seva signatura.**
- **Un *hash* del *candidate receipt* del bloc pare.**
- **Un *hash* del bloc.**
- **Un *Merkle root* amb tots els missatges.**
- **Un *Merkle root* del *erasure coding* del bloc**
- **L'arrel estat (*state root*) de la *parachain* abans d'executar el bloc.**
- **L'arrel estat (*state root*) de la *parachain* després d'executar el bloc.**

Encara que sembli una gran quantitat d'informació, en realitat és una quantitat molt més petita que la prova de validació (PoV) feta al començament del procés de validació del bloc de la parachain, això és degut al fet que cada ítem té una llargada fixa. L'ID de la *parachain* i el *collator* són simplement números, la resta són *hashs* (el *Merkle root* és un *hash* d'un *hash* d'un *hash*…).

Qualsevol mètode per representar un conjunt d'informació en una quantitat en una mida constant proporciona un avantatge d'escalabilitat. Aquest sistema pot anar escalant mitjançant el *push* de més i més informació mentre que la mida de la informació afegida a la *relay chain* es manté de forma constant.

El *hash* del *receipt* del bloc pare ens assegura que aquest rebut/comprovant (receipt) s'està construint i es basa en la cadena correcta. De totes maneres, els estats de les arrels de les *parachains* i el *hash* del bloc permet que qualsevol pugui verificar aquesta transició d'estat obtenint la prova de validació (PoV = bloc + actualitzacions de l'*state tree*) .

7.4 Erasure Coding

Abans d'enviar aquest *candidate receipt* a la cua de transaccions de la *Relay Chain* el *validator* que construeix aquest *candidate receipt* també ha de construir un *erasure coding* (esborrany) del bloc de la *parachain*.

L'*erasure coding* agafa un missatge, en aquest cas el bloc de la *parachain* i la prova de validació (PoV) i crea un conjunt de missatges més petits a partir dels quals es pot tenir la capacitat de reconstruir el missatge original aconseguint una fracció dels missatges. En el cas de Polkadot, el nombre mínim de missatges necessaris per reconstruir un bloc és igual al nombre total de *validators* dividit per 3. Per exemple, si Polkadot tingués 1000 *validators* i cadascú d'ells aconsegueix un *chunk* (a

Polkadot els missatges derivats d'aquesta fragmentació s'anomenen així), el nombre necessari de *chunks* per reconstruir aquest bloc seria de 334 [17].

Una vegada creats aquests *erasure coding chunks*, s'introdueixen dintre de l'arbre de *Merkle* del *validator* i s'envien als *validators* corresponents. Juntament amb aquests *chunks* també s'envia el *candidate recipt*, que és el que anirà realment al bloc de la *relay chain*. Aquest procés succeeix de forma simultània per a cada *parachain*, s'envia el *chunk* juntament amb el *candidate recipt* a cada *validator* i és inclós aquest últim en la *transaction queue* de la *relay chain*.

7.5 Relay Chain Block Construction

Els blocs de la *relay chain* són produits utilitzant *BABE*. *BABE* assigna *validators* de forma aleatòria per produir blocs en una ranura de temps determinada. El *validator* seleccionat haurà de provar que ha estat escollit per produir aquell bloc i crearà un bloc que inclou diversos *candidate recipients* de diverses *parachains*.

L'autor del bloc, que hagi guanyat el sorteig, només inclourà els *candidate recipients* que tenen un *candidate recipient* pare en el bloc de la *relay chain* anterior per assegurar-se així que aquella parachain sigui una cadena vàlida i només aquelles on el *validator* tingui un *erasure coding chunk* (els *validators* envien els *chunks* a tota la resta de *validators* de la xarxa) , assegurant així que es puguin realitzar comprovacions de disponibilitat i validesa en les properes rondes.

7.6 Final and Additional *Checks*

La comprovació de la disponibilitat dels *chunks* per part del *block author* assegura que Polkadot només inclourà blocs per als quals els *validators* hagin distribuït els seus trossos, pero no garanteix la seva validesa. En separar la producció de blocs ***(BABE)*** de la finalitat ***(GRANDPA)*** permet a Polkadot realitzar comprovacions addicionals després de produir un bloc però abans de finalitzar-lo. Polkadot té actors especials, els *fisherman*, que patrullen la *relay chain* en cerca de *candidate receipts* invàlids.

Una vegada el bloc és afegit a la *relay chain*, comença una fase de verificació. Aquesta fase de verificació consisteix en sol.licitar una quantitat suficient de fragments de *erasure coding chunks* per reconstruir el bloc codificat i una prova de validesa per validar la transició d'estat.

***Els** additional checks* són realitzats per *validators* assignats aleatòriament. El mínim nombre de *validators* per validar una *parachain* i proporcionar seguretat és de 14. Si en alguns casos s'assignen un nombre inferior de *validators*, com per exemple 10 a cada *parachain*, el sistema haurà d'assignar aleatòriament un mínim de 4 *validators* ocults.

Una vegada s'hagin obtingut la quantitat suficient dels *additional checks* en els *candidate receipt*, els *validators* finalment podran votar per bloc (i per extensió, els blocs previs) en GRANDPA. Tan aviat com un bloc tingui ⅔ de pre-commits els blocs s'inclourà en la cadena finalitzada.

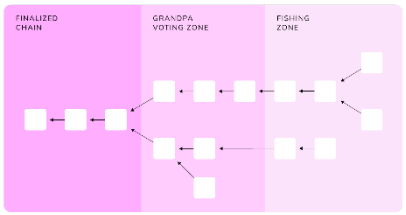

Figura 13. Procés de votació per a la finalització d'un bloc.

Si observem la figura 13, podem veure que hi ha 3 grans zones diferenciades. Com que els *validators* no poden votar blocs que no tinguin suficients *checks addicionals*, això crea tres zones a la *relay chain*: ***Finalized Chain***, ***the GRANDPA voting zone*** amb blocs vàlids i llestos per votar i ***the fishing zone*** on es troben els blocs que necessiten una validació. Totes aquestes validacions es produeixen en menys d'un minut des de que un bloc entra a la ***fishing zone*** fins que passa a la ***GRANDPA voting zone*** [18]**.**

7.7 Parachains Slots Auction

Polkadot suporta un nombre limitat de parachains, actualment es de 100. Com que el nombre és limitat hi ha diverses maneres d'assignar aquests *slots* a les *parachains*:

Governance granted parachains, or "common good" parachains → Són assignades pel sistema de governança *on-chain* de Polkadot i es consideren un bé comú per a la xarxa com els *bridges*. Es consideren cadenes a nivell de sistema o d'utilitat pública i no tenen un model econòmic, únicament ajuden a eliminar transaccions de la Relay Chain permetent un processament més eficient de les *parachains*. Tenen *slots* reservats per parachains que proporcionin aquests benefics a l'ecosistema.

Auction granted parachains → Són *parachains* concedides en subhastes, on qualsevol titular de DOT pot fer ofertes mitjançant els seus *tokens* o obtenir-los de la comunitat mitjançant la funcionalitat *crowdloan* .
Parathreads→ Tenen la mateixa API que les parachains, però estan programades per l'execució *pay-as-you-go* amb una subhasta per cada bloc [19].

8. Conclusions

Una vegada finalitzat el desenvolupament del projecte, podem afirmar doncs que aquest treball ens ha fet dur a terme una sèrie de conceptes una mica diferents dels que normalmente es treballen en l'àmbit informàtic.

Aquest projecte ens ha ajudat a adquirir una capacitat de lectura i anàlisis més extensa que la que probablement hauríem adquirit o ja tenim, dels treballs més pràctics. Aquesta capacitat ens ha permès entre d'altres aprofundir sobre els diversos temes que hem tractat mitjançant el qüestionament de diferents conceptes o el sorgiment de preguntes que ens han fet recapacitar i per conseqüència han necessitat una recerca per satisfer les nostres curiositats. En molta de la informació trobada, la dificultat no només ha estat a entendre la informació, si entenem per entendre el fet de poder traduir aquesta informació, sinó que a més després una de les grans dificultats

ha sorgit de saber com plasmar aquesta informació en el treball final de manera que fos comprensible.

Un altre dificultat, que potser és excepcional en el meu cas, és el fet de llegir diverses fonts d'informació, contrastarles i partir d'aquí elaborar l'explicació necessària sense deixar de banda cap informació fonamental de les fonts consultades en aquesta fusió, on la majoria de vegades la informació obtinguda era pràcticament igual, i la dificultat consistia a identificar el fet fonamental i diferencialista de l'altra font.

Respecte els objectius, podem afirmar amb èxit que s'han complert tots els fixats, encara que la part pràctica, per manca de temps i diversos problemes sorgits amb l'execució del SO, no s'ha pogut desenvolupar amb la totalitat que haguéssim volgut.

Si parlem del desenvolupament fet, gràcies a l'elaboració del document, podem concloure que Polkadot vol construir un entorn infinit, amb la inclusió de millers de *parachains* cadascuna amb la seva pròpia implementació i amb el seu funcionament, on la participació dels usuaris es necessària per a construir un entorn el més heterogeni possible. De fet, una de les idees en un futur de Polkadot, és que la relay chain passi a formar part de les parachains i actuï com aquesta, a més d'ampliar aquestes parachains a 1000. Podem entendre perquè es considera una blockchain heterogènia (multitud de cadenes desplegades i que treballen conjuntament), escalable (fragmentació en parachains), segura gràcies a l'ús de NPoS (Nominated Proof of Stake) i interoperable, ja que permet la comunicació entre *parachains*, o entre *parachains* i la *relay*, o entre qualsevol cosa que formi part del sistema de Polkadot (ús de *bridges*).

AGRAÏMENTS

Al tutor d'aquest Treball de Final de Grau, Jordi Herrera, tant pel que fa al suport, guia i ajut durant en el desenvolupament del projecte i per la seva docència a l'assignatura de Blockchain, que em va fer crear un interés pel món de les criptomonedes i sense això, aquest treball no hauria estat possible. A la meva família i amics pel suport incondicional des del primer dia i pels seus moments de desconnexió.

BIBLIOGRAFIA

[1] CoinTelegraph. ¿Qué es Polkadot?. [Online]. Available: https://es.cointelegraph.com/explained/what-is-polkadot.

[2] Substrate. Build a Local Blockchain. [Online]. Available: https://docs.substrate.io/tutorials/get-started/build-local-blockchain/.

[3] HMD. Módulo 0. Metodologías Ágiles Vs Metodologías Tradicionales. [Online]. Available: https://uv-mdap.com/programa-desarrollado/bloque-iv-metodologias-agiles/metodologias-agiles-vs-tradicionales/

[4] LemonWiki. Layer1vsLayer2. [Online]. Aavailable:https://wiki.lemon.me/layer-1-l1-vs-layer-2-l2-que-son-y-como-prometen-solucionar-la-escalabilidad-de-blockchain/.

[5] Protocol. An Ethereum co-founder is now on a crusade against 'crypto nationalism'. [Online]. Available: https://www.protocol.com/fintech/polkadot-ethereum-gavin-wood.

[6] CoinMarketCap. Today's Cryptocurrency Prices by Market Cap. [Online]. Available: https://coinmarketcap.com/.

[7] Polkadot. DOT Token. [Online]. Available: https://polkadot.network/dot-token/.

[8] [17] Wiki Polkadot. Architecture. [Online]. Available: https://wiki.polkadot.network/docs/learn-architecture.

[9] CoinTelegraph. Proof-of-stake vs. proof-of-work: Differences explained. [Online]. Available: https://academy.bit2me.com/consenso-criptomonedas/.

[10] Cevallos, Alfonso. How Nominated Proof-of-Stake will work in Polkadot. [Online]. Available: https://medium.com/web3foundation/how-nominated-proof-of-stake-will-work-in-polkadot-377d70c6bd43.

[11] Vangardem. 2.-Roles de Consenso. [Online]. Available: https://vangardem.gitbook.io/polkadot-espanol/glosario-1/untitled.

[12] Apriorit. Blockchain for Cybersecurity: Pros and Cons, Trending Use Cases. [Online]. Available: https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons.

[13] Cevallos, Alfonso. Overview of NPoS. [Online]. Available: https://research.web3.foundation/en/latest/polkadot/NPoS/1.%20Overview.html. Acessed: April. 12, 2022.

[14] Polkadot. Polkadot Consensus Part 3: BABE. [Online]. Available: https://polkadot.network/blog/polkadot-consensus-part-3-babe/.

[15] Sebastian Cripto. Consenso de Polkadot. [Online]. Available: https://polkadot.network/blog/polkadot-consensus-part-2-grandpa.

[16] Wiki Polkadot. Parachains. [Online]. Available: https://wiki.polkadot.network/docs/learn-parachains.

[17] Polkadot. The path of a parachain Block. [Online]. Available: https://polkadot.network/blog/the-path-of-a-parachain-block/.

[18] Wiki Polkadot. Bridges [Online]. Available: https://cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-two-how-consensus-works-1b2b2f3a2245.

[19] Seq. Polkadot — An Early In-Depth Analysis — Part Two — How Consensus Works. [Online]. Available: https://cointelegraph.com/blockchain-for-beginners/what-are-parachains-a-guide-to-polkadot-and-kusama-parachains.

APÈNDIX

A1. CREACIÓ D'UNA PARACHAIN- MARC PRACTIC

Parity, el desenvolupador de Polkadot i *substrate* (el marc blockchain que alimenta Polkadot), permet crear *blockchains* construïdes expressament mitjançant la composició de components personalitzats o preconstruïts. Aquests mòduls personalitzats, preconstruccions, s'anomenen *pallets*.

Els *pallets* es poden combinar fàcilment en *substrate* i cada *pallet* conté una lògica específica del domini, permetent afegir certes funcionalitats a una cadena basada en *substrate* , com Polkadot.

Mitjançant la interfície gràfica que ens proporciona l'eina de Substrate(https://substrate-starterkit.mvpworkshop.co/#/workspace) , podem crear la nostra *blockchain* a partir d'un conjunt de components predefinits que després executarem.

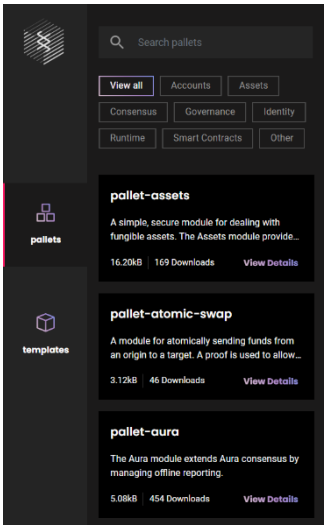

Figura 2. Llistat de *pallets*.

Primer de tot, haurem de seleccionar els *pallets* que volem per construir la nostra blockchain. Com podem veure en la imatge, els *pallets* són components bàsics que han de formar part de la nostra blockchain. Dintre del conjunt de pallets podem trobar de diferents tipus: ***accounts pallets***, ***assets pallets***, ***governance pallets***, ***consensus pallets***, veure figura 2.

Aquests *pallets* són necessaris quan es vol desenvolupar una blockchain, per exemple *l'asset pallet* ens permet tenir un mòdul senzill i segur per tractar actius fungibles. El mòdul ***Assets*** ens proporciona funcionalitat per a la gestió d'actius de classes fungibles amb un subministrament fix, incloent-hi: emissió d'actiu, transmissió d'actius, destrucció d'actius. La major part dels *pallets*, tenen dependències d'altre per proporcionar les seves funcionalitats a la *blockchain*, per la qual cosa per poder afegir un, s'ha d'afegir simultàniament tota la resta, veure figura 3.

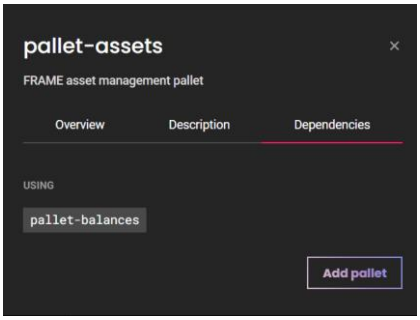

Figura 3. Dependències del *pallet-assets*.

De forma automatica, *Substrate* ens crea els 7 *pallets* que podem veure a continuació, aquests pallets són necessaris i són el mínim nombre de pallets que ha de tenir la blockchain per funcionar, no es poden eliminar, veure figura 4. Els *pallets* en qüestió són els següents:

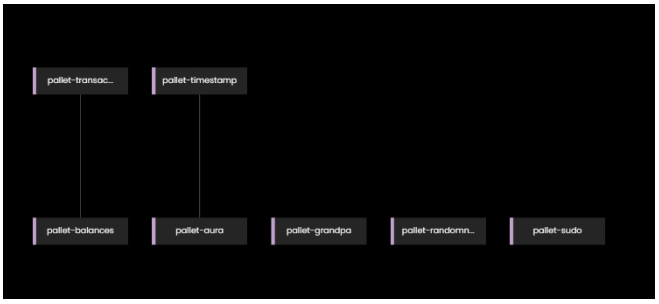

Figura 4. *Pallets* necessaris per a la construcció d'una blockchain.

Per a la nostra blockchain, afegirem els següents pallets: *pallet-assets*, en vermell, que com hem vist abans té una dependència del *pallet-ballances*, en color groc, d'igual forma que el *pallet-transaction*, color blau, del qual depèn el *pallet-ballances*, veure figura 5. Mitjançant amb la creació d'aquest conjunt de *pallets* el sistema serà capaç de mantenir un balanç de *tokens* de la blockchain així com l'intercanvi (enviament i recepció) de *tokens* entre diferents *accounts*.

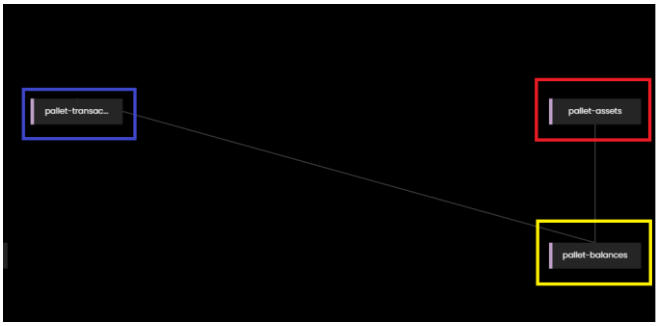

Figura 5. Dependències del *pallet-assets*.

També afegirem un pallet de democràcia, en qüestió el *pallet-democracy*. Aquest *pallet* s'encarrega de l'administració del vot general de totes les parts que formen l'ecosistema. Qualsevol titular del token en el sistema pot votar en referèndum. El sistema de votació utilitza el vot de bloqueig de temps en permetre al titular de fitxes establir la seva convicció darrere

d'una votació. Els *pallets* en color blau són els *pallets* que s'han afegit per dependència directa del democracy, la resta són dependència dels *pallets* de color blau
.

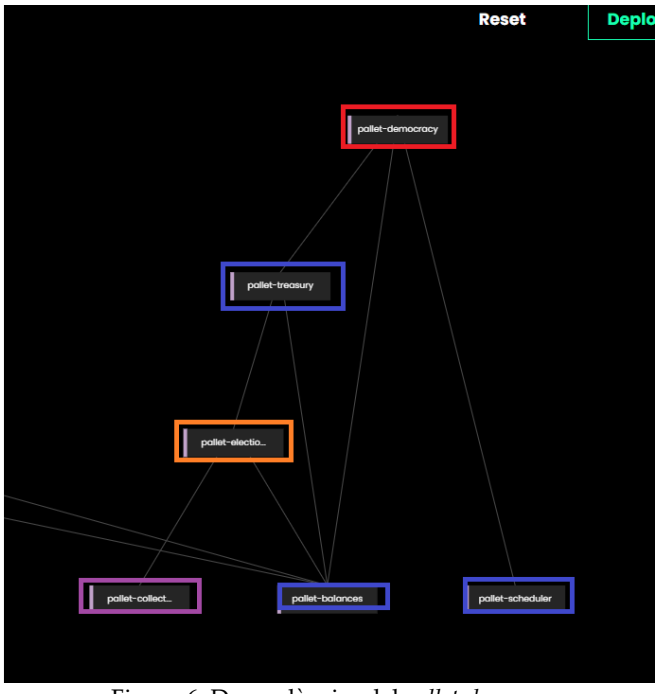

Figura 6. Dependències del *pallet-democracy*.

Per últim, també afegirem el *pallet-BABE*, amb aquest *pallet* podrem complementar el nostre sistema de consens juntament amb el *pallet-GRANDPA*, inclòs per defecte. Aquests *pallets* ens permet tenir un mòdul d'extensió de consens per al consens BABE que recull l'aleatorietat en cadena a partir de sortides VRF i gestiona transicions d'època.

Ara, mitjançant el conjunt de pallets seleccionats, tenim una *blockchain* que permet enviar, rebre, mantenir un balanç dels tokens dels usuaris i que té un sistema de governança *on-chain* juntament amb un protocol de consens i protocols per a la producció i finalització de blocs (BABE i GRANDPA).

Un cop creada la nostra *blockchain*, ja podem descarregar el nostre codi font disponible per executar i començar a posar en funcionament la *blockchain*, veure figura 7:

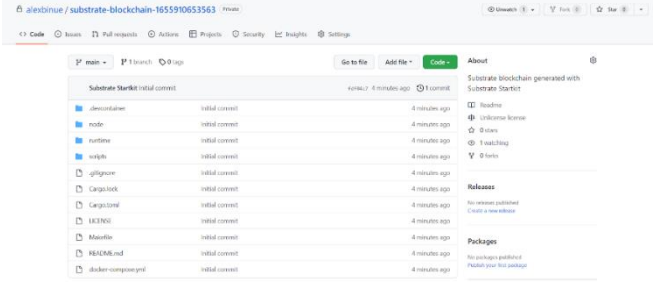

Figura 7. Esquelet de la *blockchain*.

El repositori es troba disponible i és accesible per tothom al següent enllaç:
https://github.com/alexbinue/substrate-blockchain-1655910653563.git

A2. GLOSSARI

CONCEPTE	DESCRIPCIÓ
PERMISSIONLESS	ES CONSIDEREN PERMISSIONLESS LES XARXES OBERTES A QUÈ TOTHOM QUE HI VULGUI PUGUI PARTICIPAR EN EL PROCÉS DE CONSENS QUE LA BLOCKCHAIN UTILITZI PER VALIDAR TRANSACCIONS I DADES.
LAYER 1	ÉS UN CONJUNT DE SOLUCIONS QUE MILLOREN EL PRÒPI PROTOCOL BASE PER FER QUE EL SISTEMA GENERAL SIGUI MOLT MÉS ESCALABLE.
LAYER 2	ES REFEREIX A UNA XARXA O TECNOLOGIA QUE OPERA A LA PART SUPERIOR D'UN PROTOCOL BLOCKCHAIN SUBJACENT PER MILLORAR LA SEVA ESCALABILITAT I EFICIÈNCIA
MODEL DE SHARDING	MODEL DE SHARDING HETEROGENI PER CONNECTAR DIVERSES BLOCKCHAINS EN UNA ÚNICA XARXA, DE MANERA QUE PUGUIN INTERCANVIAR DADES ENTRE SI I PROCESSAR TRANSACCIONS AMB SEGURETAT GARANTIDA
WHITE PAPER	UN DOCUMENT QUE SERVEIX DE GUIA PER EXPLICAR UN CONCEPTE DETERMINAT O LA SOLUCIÓ A UN PROBLEMA EN ESPECÍFIC, NORMALMENT AMB MOLTS TECNICISMES I AMB UNA CERTA COMPLEXITAT.
TOKEN	UNA UNITAT DE VALOR QUE UNA ORGANITZACIÓ CREA PER GOVERNAR EL SEU MODEL DE NEGOCI I DONAR MÉS PODER ALS SEUS USUARIS PER INTERACTUAR AMB ELS SEUS PRODUCTES, ALHORA QUE FACILITA LA DISTRIBUCIÓ I REPARTIMENT DE BENEFICIS ENTRE TOTS ELS SEUS ACCIONISTES
EMISSIÓ	ÉS LA QUANTITAT DE TOKENS QUE S'HA CREAT I PER TANT QUE CIRCULEN PER LA XARXA BLOCKCHAIN FINS AL MOMENT
STAKE	LA QUANTITAT QUE ES QUEDA BLOQUEJADA
CAPITALITZACIÓ	LA CAPITALITZACIÓ ES EL PREU TOTAL DE MERCAT DE LA CRIPTOMONEDA, I ES CALCULA APLICANT AQUESTA FÓRMULA: MARKET CAP = CURRENT PRICE X CIRCULATING SUPPLY
HOLDERS	MANTENEN LA SEVA INVERSIÓ INTACTA ESPERANT QUE EL VALOR DEL PRODUCTE FINANCER AUGMENTI ENCARA MÉS EN UN FUTUR.
SLASHED	PROCÉS MITJANÇANT EL QUAL UN VALIDATOR VEU REDUÏDES LES SEVES RECOMPENSES
ROUND ROBIN	ROUND-ROBIN ÉS UN ALGORITME DE PLANIFICACIÓ DE PROCESOS SIMPLES PER SELECCIONAR TOTS ELS ABSTRACTES EN UN GRUP DE MANERA EQUITATIVA I EN UN ORDRE RACIONAL, NORMALMENT COMENÇANT PEL PRIMER ELEMENT DE LA LLISTA FINS A ARRIBAR AL DARRER I COMENÇANT DE NOU DES DEL PRIMER ELEMENT
MECANISME DE FINALITAT (FINALITY GADGET)	UN DISPOSITIU DE FINALITAT PERMET QUE LES TRANSACCIONS ES COMPROMETIN SEMPRE DE FORMA OPTIMISTA
CADENA DE BLOCS CANONICA (CANNONICAL BLOCKCHAIN)	LA CADENA MÉS LLARGA AMB LA MAJOR QUANTITAT DE BLOCS PRIMARIS DESPRÉS DE L'ÚLTIM BLOC FINALITZAT PER GRANDPA
CROWDLOAN	QUALSEVOL PERSONA QUE HAGI REGISTRAT UNA PARACADENA POT CREAR UNA NOVA CAMPANYA DE CROWDLOAN PER A UNA RANURA DIPOSITANT UN NOMBRE DETERMINAT DE TOKENS
PAY-AS-YOU-GO	PAGAMENT PROGRESSIU, EN FUNCUÓ DE L'US.