

Implementació de la tecnologia blockchain a l'operació de la planta pilot de purificació d'aigua regenerada, destinada a la recàrrega d'aqüífers d'abastament per la fiabilitat en la lectura i processament de la informació

Blockchain 4SDG: Grup Ca'n Tovell

Antoni Bergas Galmés

UNIVERSITAT POLITÈCNICA DE CATALUNYA

antonio.bergas@upc.edu

Guillem Pascual Martí

UNIVERSITAT OBERTA DE CATALUNYA

guillempascual@uoc.edu

Inès Sunyer Guiscafré

UNIVERSITAT DE GIRONA

u1952353@campus.udg.edu

8 de març de 2022



Resum

Al llarg de les darreres dècades s'ha produït un augment poblacional exponencial i, en conseqüència, una intensificació en l'explotació dels recursos hídrics per a usos consumptius i no consumptius. També per l'efecte del canvi climàtic es preveuen a curt i llarg termini, estacions més seques i amb menys pluges, cosa la qual fa disminuir els recursos hídrics que es troben a l'abast humà. Així mateix, durant els darrers anys les noves tecnologies han suposat una incipient revolució en la transferència d'informació i la seguretat. És per això que es pretén implementar la tecnologia blockchain a una planta pilot purificadora d'aigua regenerada que està destinada a la recàrrega d'aquífers a Roses, Catalunya, per tal d'abastir d'aigua potable a la població. La implementació d'aquest tipus de tecnologia permetrà la fiabilitat i seguretat en la lectura i processament de la informació de la planta, així com assegurar la traçabilitat, validesa i immutabilitat de totes les dades recopilades. A través de la implementació de la tecnologia Hyperledger Fabric a la planta es podrà aconseguir una blockchain híbrida (pública-privada) amb un cost econòmic i consum energètic baixos.

Abstract

Over the last few decades, there has been an exponential increase in population and, consequently, an intensification in the exploitation of water resources for consumptive and non-consumptive uses. Also due to the effect of climate change, shorter and longer-term seasons with less rainfall are forecast, which reduces the water resources available to humans. Also, in recent years, new technologies have led to an incipient revolution in the transfer of information and security. That is why it is intended to implement blockchain technology in a pilot plant for purifying regenerated water that is intended to recharge aquifers in Roses, Catalonia, in order to supply drinking water to the population. The implementation of this type of technology will allow the reliability and security in the reading and processing of the information of the plant, as well as ensure the traceability, validity and immutability of all the data collected. Through the implementation of Hyperledger Fabric technology in the plant it will be possible to achieve a hybrid blockchain (public-private) with a low economic cost and energy consumption.

Índex

1	Introducció	5
2	Blockchain	7
2.1	Smart Contracts	8
2.2	Algoritme de consens	9
2.2.1	Proof of Authority	10
2.2.2	Proof of Stake y Proof of Elapsed Time	11
2.2.3	Proof of History (PoH)	12
2.2.4	Proof of Work i Prog Proof of Work	12
3	Anàlisi del problema i necessitats	13
3.1	Economicitat, seguretat i sostenibilitat	14
3.2	Com s'aconseguirà?	15
3.3	Blockchain pública	16
3.4	Blockchain privada	17
3.5	Blockchain híbrida	19
4	Hyperledger	21
4.1	Ledger compartit	22
4.2	Smart contracts	23
4.3	Privacitat	24
4.4	Algoritmes de consens	25
4.4.1	Raft (Understandable Distributed Consensus)	26
4.5	Casos d'implementació de la tecnologia Hyperledger Fabric	28
5	Implementació	29
5.1	Descripció de la planta pilot purificadora	29
5.2	Desenvolupament de la blockchain	31
5.2.1	Entorn	31
5.3	Interacció a la blockchain	32
6	Prova de concepte	36
6.1	Xarxa d'Hyperledger Fabric	36
6.2	Chaincode	37
6.3	API i aplicació web	38
7	Extensió del projecte	42
8	Conclusions	43

Índex de figures

1	Diferència entre una ledger centralizada i una ledger distribuïda.	8
2	Anàlisi del funcionament d'un smart contract.	9
3	Descripció del funcionament d'un algoritme de consens.	10
4	Comparativa entre Proof of Work i Proof of Stake.	11
5	Evolució del preu de la criptomoneda Bitcoin.	15
6	Diferències entre diferents tipus de blockchains.	19
7	Descripció de l'estructura d'una blockchain híbrida.	20
8	Temps d'execució, latència i rendiment d'Ethereum i Hyperledger Fabric, de manera respectiva	22
9	Escalabilitat per a Hyperledger Fabric, Ethereum i Parity.	23
10	Descripció de l'estructura d'Hyperledger Fabric.	24
11	Demostració de com Hyperledger Fabric permet la privacitat de dades.	25
12	Avaluació per a dues organitzacions.	26
13	Descripció visual del procés del protocol Raft.	28
14	Esquema general del funcionament de la planta pilot purificadora amb els respectius processos de tractament de l'aigua i sondes, així com els paràmetres fisico-químics que mesura cada una d'elles. Els paràmetres mesurats en l'aigua depenen del procés en el que es trobi aquesta.	30
15	Rangs desitjables de l'aigua pels principals paràmetres: cabalímetre, conductivitat elèctrica, amoni, carboni orgànic total i potencial REDOX, mesurats amb els diferents tipus de sondes, segons la localització de l'aigua a la planta.	31
16	Visualització del procés que realitza la funció automatitzada per la revisió dels hashes.	36
17	Pàgina d'inici des de la vista d'un membre de les Aigües de Catalunya.	40
18	Vista completa concreta de l'amoni. Una gràfica i l'històric de transaccions.	41
19	Vista detallada concreta de l'amoni. Una gràfica i l'històric de transaccions.	42

1 Introducció

S'estima que avui en dia més de la meitat de l'aigua dolça en el món es troba destinada a l'ús humà, sigui de forma consumptiva o no consumptiva. Així mateix, es creu que en l'avanç dels anys aquesta despesa serà major, ja que també s'estima que durant els trenta anys vinents la població mundial haurà augmentat en un terç de la que hi ha actualment. En conseqüència, es produirà una intensificació en la utilització dels recursos hídrics que condueix a la necessitat i obligació de buscar una millora en la gestió de l'aigua. A més, els efectes del canvi climàtic seran molt visibles al llarg d'aquest segle XXI i limitaran encara més l'accés a l'aigua a tota la població [1].

A causa de l'augment de la temperatura, associat al canvi climàtic, a Catalunya es preveu una disminució dels dies de pluja i, per tant, un augment dels dies de sequera persistents. Aquest fet provocarà escassetat en els recursos hídrics, sobretot durant les èpoques estivals [2]. Això provoca una clara necessitat de recuperar la molècula d'aigua que es perd quan es fa servir aigua no potable per consum humà.

Espanya és un dels països d'Europa que més estrès hídric presenta, és a dir, que la demanda d'aigua excedeix les possibilitats d'extracció d'aquesta al país. A més, a aquest fet se li ha de sumar que l'any 2006 només un 10,8% de l'aigua residual depurada es reutilitzava a l'estat espanyol (Prats-Rico, 2016). Tenint en compte dades de l'any 2012, l'aigua reutilitzada va passar a ser un 22% (AEAS, 2012). Per tant, el percentatge d'aigua reutilitzada a Espanya en 6 anys ha augmentat el doble, en un 11,2%. Això pot fer veure que aquest percentatge augmentarà al llarg d'aquests anys vinents. [3][4]

És per aquest conjunt de motius que en un món de cada vegada més conscienciat i bolcat per la sostenibilitat, es considera necessària una millor gestió de l'aigua que es fa servir perquè aquesta pugui ser: (1) Reutilitzada o (2) Potabilitzada per a consum humà. A partir de la idea d'aigua regenerada en sorgeix posteriorment la idea d'aconseguir-ne aigua purificada, és a dir, potable pel consum humà. S'ha de tenir present que l'aigua residual és el tipus d'aigua que es troba més lluny de complir el rang de tolerància necessari per a poder ser consumida pels humans. És per això que requereix uns tractaments molt específics i complexos que requereixen ser monitorats de forma contínua i precisa per tal que aquesta pugui ser purificada correctament. [5]

En aquest context, l'any 2008, una empresa denominada Orange County Water District (OCWD) situada al comtat d'Orange County (Califòrnia, EUU), va posar en marxa la planta purificadora d'aigua regenerada més gran del món a causa de la falta de recursos hídrics potables per la població del comtat. Aquesta aigua és destinada a omplir els aqüífers de la conca subterrània del comtat, cosa la qual també evita la intrusió salina. [6]

Així és com el Consorci d'Aigües Costa Brava de Girona, una mica a tall d'inspiració a partir del OCWD, posa a la pràctica aquesta idea per Catalunya. El projecte es tracta de la construcció d'una planta pilot de purificació d'aigua regenerada destinada a la recàrrega d'aqüífers de Roses. Així mateix, l'Agència Catalana de l'Aigua (ACA) ha disposat un ajut econòmic elevat al Consorci per tal de poder assolir el projecte i aconseguir abastir a la població de l'EDAR de Roses [7].

Dins aquest marc sorgeix un altre projecte o repte que ofereix la possibilitat de col·laboració amb estudiants universitaris a través d'un concurs: 2a edició de Blockchain 4SDG [8], aigua neta i sanejament, promogut pel Centre Blockchain de Catalunya (CBCat) [9]. Aquest repte també compte amb altres institucions i empreses col·laboradores, tals com el Consorci d'Aigües Costa Brava de Girona, la Universitat de Girona (UdG) [10], l'Agència Catalana de l'Aigua [11] i la Universitat Pompeu Fabra (UPF) [12].

El concurs consisteix en 17 reptes basats en els diferents SDG (Sustainable Development Goals). Aquests, van ser creats i desenvolupats pels Estats Membres de les Nacions Unides l'any 2015 com a eix central de l'Agenda 2030 pel Desenvolupament Sostenible [13]. Així doncs, el repte d'aquesta 2a edició és en referència a l'objectiu 6 dels SDG: Aigua neta i sanejament, per promoure una millora en la qualitat de l'aigua mitjançant la reducció de la contaminació, utilització eficient dels recursos hídrics i protecció dels ecosistemes relacionats amb l'aigua.

Per tal d'aconseguir-ho, es planteja un propòsit: la implementació de la tecnologia blockchain a la planta pilot purificadora de Roses per tal d'assolir fiabilitat, traçabilitat i transparència en la lectura i processament de la informació. D'aquesta manera s'obtindrà més sostenibilitat no només en el tractament de les aigües, sinó també amb la utilització de les noves tecnologies emergents, tals com la blockchain, per tal d'implementar una planta pilot més innovadora que permetrà unir els dos mons en un de sol.

Per tant, aquest repte és un projecte de generació de nous recursos locals per millorar l'abastiment d'aigua i garantir als municipis recurs en moments de manca de recursos hídrics o sequeres que es puguin produir a mig o llarg termini fruit del canvi climàtic.

Finalment, cal fer especial esment a que la creació d'una planta pilot purificadora d'aigua regenerada amb la implementació de la tecnologia blockchain amb suposaria un gran avenç tecnològic que permetria començar a fer ús de mètodes alternatius que difereixen molt dels mètodes utilitzats fins ara, com ara que l'aigua depurada sigui abocada directament al mar o a rius [14]. Això demostra que, clarament, es requereixen noves metodologies que permetin poder recuperar la molècula d'aigua i aconseguir reutilitzar-la per evitar perdre-la.

2 Blockchain

Blockchain o cadena de blocs es pot entendre de dues maneres. Una forma simple d'explicar el concepte és imaginant-la com una eina que serveix per crear una base de dades descentralitzada o distribuïda, on tots els usuaris tenen accés a la informació i es garanteix que aquesta sigui segura, fiable, traçable i immutable. Per contra, de forma més complexa, la blockchain es pot definir com una estructura matemàtica, on es construeix una llibreta de registre, anomenada ledger, on les transaccions que s'incorporen a la base de dades hi queden enregistrades. Les transaccions realitzades s'ordenen seqüencialment i de forma immutable utilitzant els nodes (ordinadors) com a agents validadors i els blocs com a unitat d'emmagatzematge, permetent que aquesta informació sigui traçable i inequívoca.

Per tant, es pot pensar en la blockchain com una cadena de blocs, com el seu propi nom indica, que contenen informació diferent entre ells. Per aconseguir que la informació que s'emmagatzema a cada bloc sigui immutable cada un d'ells, està enllaçat a un hash, és a dir, una seqüència de símbols creats a partir de la informació que hi ha en el bloc a través de processos criptogràfics. A més, cada bloc que conforma aquesta cadena, a part del seu propi hash, conté també el hash del bloc anterior. D'aquesta manera, si es pretén modificar la informació d'un bloc, el seu hash canvia i també canvien els hashes de la resta de blocs posteriors a aquest. Cal tenir present també que una de les normes de la blockchain és que la cadena de blocs més llarga és la més vàlida i per això és extremadament complicat modificar la informació de la blockchain. Per fer-ho, el node que pretén canviar la informació, ha de competir contra la resta de nodes i crear blocs a un ritme superior per aconseguir formar la cadena més llarga, fet que és quasi impossible actualment.

Per contra, si es tracta de la ledger, aquesta informació no és immutable. És a dir, tenint en compte que a la ledger hi queden enregistrades les noves transaccions, també s'hi poden fer modificacions de transaccions anteriors. Per això es diu que és mutable. Llavors, el que realment és immutable a la ledger és l'ordenament en el qual s'han produït les transaccions i modificacions. D'aquesta manera, qualsevol canvi en la ledger quedarà sempre anotat i és pràcticament impossible que es pugui falsificar la informació.

Cada bloc de cada blockchain està format per l'agrupació d'un conjunt de transaccions, les quals emmagatzema i de les quals en conté tota la informació necessària. Cal remarcar que cada blockchain tindrà més o menys transaccions emmagatzemades depenent dels algoritmes i processos amb els quals es crea cada blockchain, per exemple, els blocs de la blockchain de Bitcoin contenen unes 2.000 transaccions cada un, que equivalen a 1 MB.

El funcionament general de la blockchain es regeix per no tractar-se d'un sistema centralitzat on tota la informació es troba en un mateix lloc i es troba

gestionada pel mateix òrgan, sinó que més aviat tot el contrari. La blockchain es caracteritza per ser informació descentralitzada o distribuïda en diferents ubicacions, és a dir, situada a molts de nodes de forma simultània i que la informació que conté és accessible per qualsevol usuari que hi tingui accés. Per això es diu que la blockchain és un sistema de registre veritablement públic i fàcilment verificable. Els nodes són qui realment validen les transaccions i creen els blocs. Tot comença quan un node rep una transacció i a través del que es coneix com gossip protocol envia aquesta informació a la resta de nodes. Així, es decideix l'ordre d'execució de les transaccions que van arribant i gràcies a l'algoritme de consens cada node executa totes les transaccions de forma ordenada. Per això es diu que els nodes realment són rèpliques i cada un d'ells té una còpia de les transaccions validades. També s'ha de tenir present que al cor d'una xarxa blockchain hi ha una ledger distribuïda que enregistrarà totes les transaccions que es fan. Aquest conjunt de fets són els que fan que la blockchain i la ledger siguin tan traçables i immutables. [15] [16]

Finalment, cal remarcar que en termes generals existeixen dos tipus de blockchains: les públiques i les privades, que presenten característiques que les fan similars, però sobretot que les fan diferents. Aquestes s'explicaran més detalladament més endavant.

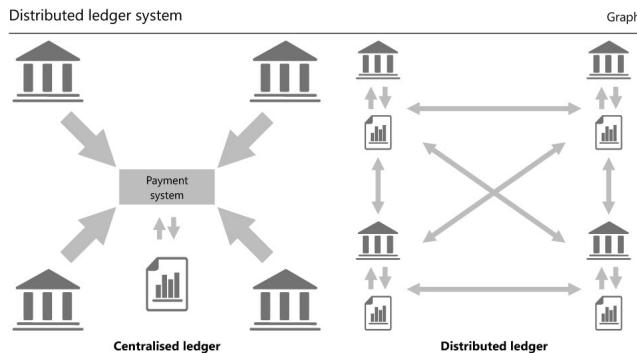


Figura 1: Diferència entre una ledger centralizada i una ledger distribuida.

[17] [15] [18]

2.1 Smart Contracts

Per donar suport a l'actualització continuada de la informació a la blockchain i per habilitar tota una sèrie de funcions de la ledger, com ara transaccions o consultes, una blockchain pot utilitzar smart contracts per proporcionar un accés

controlat a la ledger. És a dir, un smart contract és un programa informàtic que facilita, assegura i fa complir un acord que queda enregistrat entre dues o més parts.

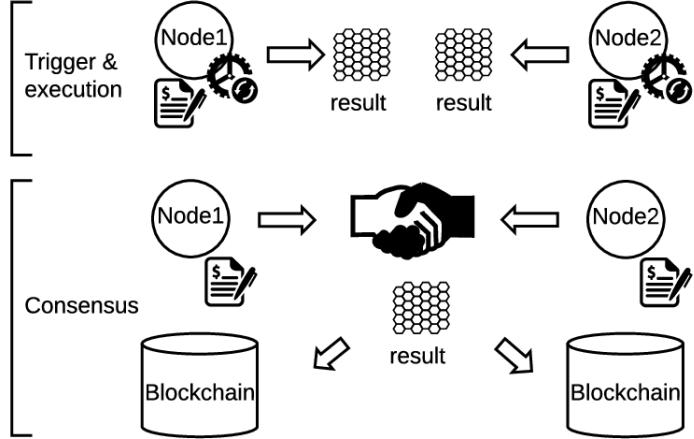


Figura 2: Anàlisi del funcionament d'un smart contract.

Els smarts contracts també es poden redactar per permetre als participants executar determinats aspectes de les transaccions automàticament i tenir en compte diferents variables acordades entre els participants del contracte. També es soLEN empar per codificar la informació i reduir la mida (bytes) de les transaccions.

Els smart contracts són específics d'algunes blockchains i tenen múltiples aplicacions tecnològiques. Una de les seves aplicacions més famoses actualment és el registre de NFT's (None Fungible Tokens). S'han popularitzat perquè l'ús de smarts contracts permet tenir un registre de la possessió dels NFT's i, a més, permeten crear condicions especials com per exemple que el creador dels NFT's s'apropiï del 10% del valor d'aquest cada vegada que canvia de propietari. [18]

2.2 Algoritme de consens

Un algoritme de consens és un mecanisme que permet als ordinadors o usuaris coordinar-se en un entorn distribuït per tal de garantir que tots els agents partícents en el sistema blockchain puguin posar-se d'acord respecte a una font única de veritat. Per tant, suposa un procés que manté les transaccions de la ledger sincronitzades a tota la xarxa i garanteix que aquestes transaccions, a mesura

que van arribant al sistema de forma seqüencial, pugui ser validades i aprovades en aquest mateix ordre de priorització. La informació nova rebuda i aprovada quedarà enregistrada a la blockchain i a la ledger, la qual s'actualitzarà. [19] [20]

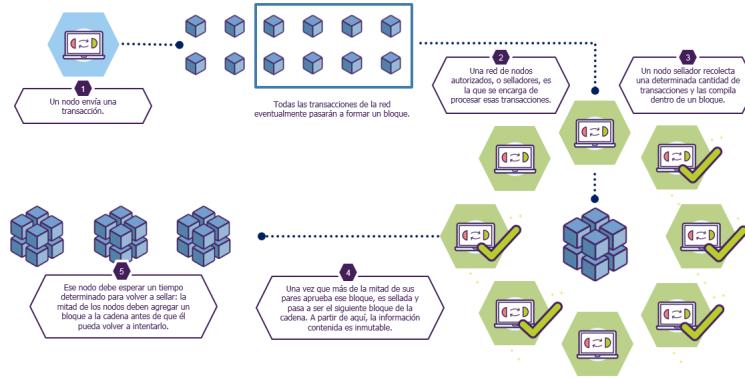


Figura 3: Descripció del funcionament d'un algoritme de consens.

Alguns dels exemples dels algoritmes de consens més utilitzats avui en dia tant en les blockchains públiques com privades són:

2.2.1 Proof of Authority

Proof of Authority (PoA) és un tipus d'algoritme de consens on els usuaris validadors de les transaccions posen en joc la seva pròpria reputació per tal d'efectuar correctament les transaccions. És a dir, aquest model es basa en la desaparició de l'anonymitat rere la validació de les transaccions, per tant, com a mínim un altre usuari ha de conèixer la identitat de l'altre. És per això que es tracta d'un model basat en la limitació dels validadors involucrats, que consten com a entitats confiables, i que han estat acceptats per participar-hi. Com que se sap la identitat dels validadors a través d'una certificació digital, la seguretat de la validació de les transaccions recau sobre aquest fet. És el model més utilitzat en les xarxes privades, ja que aquestes empreses poden mantenir la privacitat mentre aprofiten els beneficis de la tecnologia blockchain. [19] [21]

2.2.2 Proof of Stake y Proof of Elapsed Time

Proof of Stake (PoS) és un algoritme de consens que depèn de la inversió del validador a la xarxa i del temps que hi porta. És a dir, es basa en la idea que com més criptomonedes té el validador i com més temps porti a la xarxa, més possibilitats té de ser elegit a l'atzar per validar les transaccions. Per tant, s'entén que aquests validadors seran als que els hi tocarà més vegades validar i, conseqüentment, més tenen a perdre si s'equivoquen o realitzen frau. Això és el que genera en aquest cas la seguretat a l'hora que executin bé la seva tasca.

Aquest sistema pot portar a una centralització indesitjada. És per això que apareix Proof of Elapsed Time per solucionar-ho. Aquest mètode intenta seleccionar al validador que sigui el primer a completar un bloc després d'esperar un temps aleatori determinat. Essencialment, és un mètode similar a Proof of Work però sense els grans requisits de consum energètic. Per assignar aleatoriament aquest temps d'espera i certificar que el validador ha esperat el temps corresponent cal un entorn de computació segura.[19] [22] [23]



Figura 4: Comparativa entre Proof of Work i Proof of Stake.

2.2.3 Proof of History (PoH)

Proof of History (PoH) és un algoritme de consens complementari al Proof of Stake, que pertén accelerar el procés de consens proporcionant eines per la codificació del temps en ell mateix dins la cadena de blocs. Permet als nodes confiar en les marques temporals dels blocs i verificar criptogràficament el moment i l'ordre de l'ocurrència dels missatges o esdeveniments que tenen lloc a la xarxa. D'aquesta forma s'evita que els validadors hagin de comunicar-se entre ells per acordar els sucessos en funció del temps, evitant els colls de botella del PoW i reduint el temps de consens. [24] [25] [26]

Proof of History se basa en Verifiable Delay Functions (VDF), un concepte criptogràfic que permet la validació de transaccions sense potència computacional. Aquest pocés no permet el processament en paral·lel i facilita conèixer quant de temps s'ha tardat en resoldre el VDF. D'aquesta forma, el pas del temps està clarament definit i interpretat a la blockchain. [27] [24] [28] [29] [25]

2.2.4 Proof of Work i Prog Proof of Work

Proof of Work (PoW) és dels algoritmes de consens més utilitzats avui en dia. El seu sistema de funcionament és molt segur, però gasta molta d'energia a causa del gran esforç que requereix la seva prova. El Proof of Work consisteix en la resolució de problemes computacionals com a procés de completació de transaccions. Els usuaris que competeixen per acabar els primers aquestes transaccions s'anomenen miners i obtenen recompenses cada vegada que solucionen una de les dificultats presentades abans que la resta. Aquest algoritme de consens s'empra per validar transaccions i per afegir nous blocs a la blockchain.

El problema computacional resideix en trobar un conjunt de símbols aleatoris que es troben definits per un algoritme, el qual modifica la seva dificultat dependent de la situació de la blockchain. Aquest algoritme de consens requereix un consum energètic elevat, ja que per descobrir els nombres associats s'empren ordinadors amb targetes gràfiques potents i aquests consumeixen molta energia. A més, un dels inconvenients principals del PoW és que si un dels nodes aconsegueix reunir el 51% de la potència de processament, pot falsificar i modificar transaccions. Encara que sigui una treta difícil, no és impossible. A les blockchains grans públiques és complicat que aquest fet succeeixi, però les blockchains petites que fan ús de PoW són poc segures. Un exemple és la blockchain de Bitcoin, en aquesta hi ha un nombre limitat de Bitcoins (21.000.000). D'aquests, n'hi ha un percentatge en circulació i un altre que està en reserva, ja que quan es crea un bloc, s'ha de recompensar als nodes que ho han permès (els que han resolt el problema computacional) i s'empren els Bitcoins en reserva per pagar-los-hi la feina. Això implica que cada vegada hi ha menys Bitcoins. Per això, per dificultar la seva adquisició, l'algoritme generador del conjunt de símbols

aleatoris és cada vegada més complex.

ProgPoW és una evolució de PoW que intenta compensar el poder de les ASICs (processadors destinats a l'execució del PoW), on es calcula PoW canviant l'algoritme perquè sigui necessari tenir una targeta gràfica. Encara que el ProgPoW és més segur que el PoW, implica un major consum d'energia perquè no pot fer servir els ASICs, sinó que requereix rigs de targetes gràfiques potents, que gasten més d'energia [30] [19] [31]

3 Anàlisi del problema i necessitats

Totes les problemàtiques presentades i possibles solucions esmentades a la introducció sobre els recursos hídrics i la seva gestió, fa que la creació de la planta pilot purificadora de Roses i la implementació de la tecnologia blockchain en el seu funcionament siguin una prioritat. La complementació d'una planta purificadora amb el sistema blockchain suposa un avanç molt important en la millora de la gestió dels recursos hídrics en el món.

Així i tot, s'ha de tenir en compte que implementar aquesta tecnologia blockchain implica certes complicacions i precisa que certes autoritats superiors autoritzades disposin d'accés a aquest sistema per tal de validar i verificar les dades que entraran a la blockchain. És a dir, de forma breu, la idea és que la blockchain funcioni de forma automatitzada, analitzant i emmagatzemant les dades entrants de la planta purificadora. Però, aquestes dades podran ser visualitzades de forma pública, a través d'una pàgina web. A més, en cas que es produueixi alguna incidència (detecció per part de la blockchain de dades que no són correctes segons valors predeterminats) es notificarà als usuaris corresponents perquè la problemàtica es pugui resoldre. Finalment, la solució de la incidència serà verificada per les entitats superiors autoritzades.

En aquest cas, les autoritats superiors autoritzades serien, per exemple: l'Agència Catalana de l'Aigua (ACA), l'Agència de Protecció de la Salut Pública, el Consorci d'Aigües Costa Brava de Girona o l'ajuntament de Roses. Per contra, els usuaris corresponents fa referència a la persona o persones encarregades de la planta capaces de proporcionar una solució immediata a la incidència detectada.

El problema principal de la blockchain resideix en generar un sistema fiable en el qual diferents entitats autoritzades puguin validar i verificar la informació. També és interessant que aquesta tecnologia permeti la traçabilitat de les dades i mesures que es van agregant com a solucions a les incidències. Es pretén implementar un sistema que contingui els valors dels diferents paràmetres fisioquímics correctes i, en cas que es detectin dades per sobre o per sota d'aquests valors establerts, que es puguin emetre automàticament avisos o alarmes als usuaris corresponents. [8]

La solució que es vol aplicar és la tecnologia blockchain, però s'ha de tenir present que hi ha moltes formes diferents d'implementar aquesta tecnologia i que s'ha d'escollar l'opció més segura, sostenible i econòmica.

3.1 Economicitat, seguretat i sostenibilitat

Seguretat: Pel que fa a la seguretat, les blockchains empren funcions criptogràfiques per transformar les dades de qualsevol bloc en una sèrie de símbols i signes amb una longitud fixa. D'aquesta manera, si la informació d'un bloc canvia, el seu hash propi també ho fa. Com que aquest bloc conté el hash del bloc anterior també, la cadena quedará invalidada. A més, el concepte de descentralització permet que la informació que existeix en una blockchain estigui compartida per diferents nodes, de forma que si un d'ells la pretén modificar no ho pugui aconseguir en la majoria de casos (depèn del consens que usa la blockchain). Prèviament, ja s'ha parlat dels diferents algoritmes de consens i s'han explicat alguns dels exemples més coneguts. Veient que hi pot haver casos concrets on la seguretat es pot veure malmenada, en la majoria de circumstàncies la blockchain és una tecnologia segura que de cada cop ho és més, amb la creació de nous algoritmes i sistemes que permeten que les transaccions que es realitzen siguin les més segures possibles. Per tant, el que es buscarà en aquest projecte és crear un sistema el més segur possible, sobretot determinat per l'algoritme de consens.

Sostenibilitat: Pel que fa a la sostenibilitat, aquest és un altre concepte que aporta tema de debat en el món de les blockchains, ja que depenen de l'algoritme de consens es requerirà més o menys d'energia per validar les transaccions correctament, cosa la qual a petita escala no té per què suposar una problemàtica molt gran, però que a mitjana i gran escala sí que ho és. Als inicis de la creació de la blockchain i del Bitcoin, amb un funcionament total d'aquesta moneda del PoW, els pocs usuaris que van començar a treballar-hi no consumien molta energia. Amb el transcurs dels anys, el Bitcoin ha tingut de cada cop més renom i el preu d'aquesta moneda digital ha patit un augment exponencial dràstic (Figura 5). Així, de cada vegada més usuaris utilitzaven el PoW i, com s'ha esmentat anteriorment, és un dels algoritmes de consens que més energia consumeix.

Tot això ha arribat fins al punt en què hi ha països en els quals s'han fet estudis per estimar la petjada de carboni que suposa l'ús excessiu i tan massiu del PoW. És així com l'estudi de Jiang et al., (2021) [32], va concloure a través de simulacions que s'espera a la Xina per l'any 2024 un consum anual energètic de la cadena de blocs de Bitcoin d'un màxim de 296,59 TWh i la generació de 130,50 milions de tones mètriques d'emissió de carboni. A més, l'estudi també focalitza que a escala internacional, aquesta producció d'emissions superaria la producció total anual d'emissions de gasos d'efecte hivernacle de la República

Txeca i Qatar.

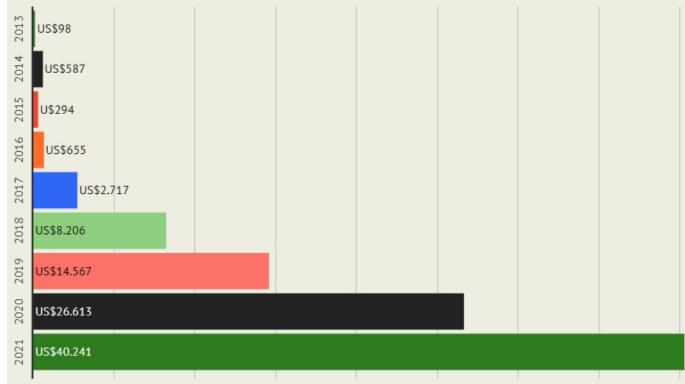


Figura 5: Evolució del preu de la criptomonedra Bitcoin.
[33]

Per tant, el problema del consum tan exagerat d'energia recau principalment en el tipus d'algoritme de consens que es faci servir i, com més s'ha pogut comprovar, el PoW és dels pitjors en aquest aspecte. És per això que en aquest projecte es pretén trobar un sistema de consens que sigui el més sostenible possible i evitar despeses energètiques elevades.

Economicitat: L'eficiència econòmica d'un sistema és una característica rellevant a l'hora de decidir implementar un sistema o altra pel que fa a la tecnologia blockchain. Alguns dels projectes principals de les blockchains públiques actualment són les criptomones Bitcoin o Ethereum, tot i que presenten la problemàtica de requerir una despesa elèctrica elevada i, per tant, tenen un rendiment econòmic baix. Així mateix, hi ha altres tipus de blockchain públiques que busquen solucions més econòmiques, tot i que avui en dia les millors opcions en termes d'economicitat són les blockchains privades o híbrides (públic-privades).

3.2 Com s'aconseguirà?

Per aconseguir aquesta implementació d'una tecnologia blockchain segura, sostenible i econòmica a la planta purificadora, es crearà una blockchain híbrida que farà servir un sistema de distribució de ledgers determinat: Hyperledger Fabric. D'altra banda, per tal que la blockchain sigui híbrida, ha de contenir una part privada i una part pública. La part privada serà la blockchain de creació pròpia on, cada vegada que s'hi formi un nou bloc (que contindrà entre

5.000 i 10.000 transaccions), es formarà també un nou hash associat a aquest bloc. L'algoritme de consens que es farà servir serà Raft. La part pública es basarà en la blockchain ja existent Solana, seleccionada pel fet de tractar-se d'una blockchain molt econòmica i amb un algoritme de concens determinat molt segur i sostenible: Proof of History (PoH). Llavors, cada vegada que es formi un nou bloc a la privada, es publicarà el hash d'aquest mateix a la pública (Solana) per tal de formar una còpia del que s'ha fet a la privada. Així, en cas que es produeixi una alteració o modificació d'alguna dada a la blockchain privada, com que el hash del bloc modificat canviaria, aquest no coincidiria amb el hash còpia que es trobarà a Solana. D'aquesta manera, es podria determinar si s'han produït modificacions.

Així és com, tenint en compte tot el conjunt de les opcions seleccionades, es podrà aconseguir una blockchain segura, sostenible i econòmica que es detallarà millor durant la resta del projecte.

3.3 Blockchain pública

Una blockchain pública és una xarxa de base de dades d'infraestructura pública, és a dir, que qualsevol usuari té llibertat d'unir-s'hi sense haver de sol·licitar permís. Els participants que es troben dins la xarxa poden participar en la validació de les transaccions (a través dels algoritmes de concens), a més de poder-les visualitzar. Les principals blockchains públiques actualment són les criptomonedes Bitcoin i Ethereum, tot i que també n'existeixen d'altres amb prou renom com ara MATIC, Solana, DogeCoins, Omi... .

Per tant, les blockchain públiques serveixen per a ús públic, com bé diu el seu propi nom, i s'hi pot tenir accés a través d'aplicacions als ordinadors o als mòbils. Requereixen una transparència absoluta i una descentralització total. Els usuaris de les aplicacions són animats per aquestes mateixes a comprovar o revisar algunes transaccions amb l'objectiu que de rebin a canvi alguna recompensa en forma de criptomoneda. D'aquesta forma, la blockchain s'enforteix i de cada vegada hi podrà haver usuaris més interessats en aquest sistema, cosa la qual farà augmentar el valor de la criptomoneda en qüestió.

Així mateix, els principals avantatges que ofereixen les blockchains públiques són:

- La transparència. Cada participant té la llibertat de veure o obtenir còpies de les transaccions, les quals es troben totalment distribuïdes.
- L'accessibilitat. Qualsevol usuari es pot unir a la xarxa de nodes i a l'historial de transaccions i informació.
- La descentralització. Per ser xarxes públiques, tots els membres exercei-

xen els mateixos drets, no hi ha comptes amb major o menor poder o de caràcter especial, a més que tampoc poden alterar el registre de transaccions).

- La immutabilitat. No hi ha cap usuari amb la capacitat de manipular la informació que ja ha estat enregistrada a la blockchain, per tant, és molt segura.

Per contra, algunes de els principals desavantatges són:

- Alt consum energètic. Actualment, la majoria de xarxes públiques utilitzen el Proof of Work (PoW), cosa la qual fa que l'energia utilitzada sigui molt elevada i poc sostenible.
- La traçabilitat. Les transaccions poden ser rastrejades en cas que una wallet (cartera) vagi associada directament a un participant. Així, es podran veure tots els moviments i transaccions realitzades, tot i que en molts casos no suposa un problema, ja que les wallets són anònimes.
- Les comissions. Els miners, els usuaris que duen a terme la validació de les transaccions, exigeixen una retribució a canvi d'assegurar la xarxa, de manera que els usuaris que vulguin registrar una transacció o informació hauran de pagar una comissió que anirà a parar a aquests.

Algunes de les millors opcions de blockchain públiques avui en dia en termes d'econòmicitat i sostenibilitat són Solana, Cardano, Terra o Polygon, que emprén protocols de consens més sostenibles que el PoW i les seves transaccions són més barates que les d'altres blockchains.

[34] [35] [36] [37]

3.4 Blockchain privada

Les blockchains privades són aquelles que admeten participants que han estat convidats prèviament a la xarxa, de forma que hi ha una entitat controladora que assigna i permet que els participants realitzin accions com transaccions o creació de blocs. Són xarxes convenientes per organitzacions, entitats, empreses o negocis, ja que requereixen tenir un accés limitat i privat a la blockchain. Les operacions que es fan són validades pels mateixos participants. Per tant, les blockchains privades són un sistema dissenyat per organitzacions, de forma que només hi tenen accés determinats usuaris i aquests poden tenir rols concrets. Així i tot, s'ha de tenir present que l'econòmicitat i sostenibilitat de les blockchains privades depenen del seu protocol de consens.

Els principals avantatges que ofereixen les blockchains privades són:

- Rendeixen millor. Acostumen a ser blockchains més petites que les públiques i aquest fet provoca que el rendiment i la velocitat de les seves operacions sigui major i que hi hagi una disponibilitat superior a la mateixa xarxa.
- Més confiables. A les xarxes públiques els participants mantenen l'anonimat, mentre que a les privades s'identifica qui és cada un d'ells.
- No hi ha comissions. Els creadors dels blocs no desenvolupen la seva feina buscant un incentiu econòmic, sinó que ho fan per formar part de la xarxa. Per aquest motiu no necessiten una retribució.

D'altra banda, els majors desavantatges són:

- No està descentralitzada. Els registres es troben a un accés tancat i és administrat per una sola entitat.
- No és immutable. El conjunt de nodes es poden posar d'acord per alterar les transaccions i les dades registrades a la blockchain.
- Seguretat. Tot i que ser blockchains petites i no anònimes pot suposar un avantatge, també pot suposar un inconvenient, ja hi ha menys nodes i això suposa que hi hagi més control, és a dir, que la seva seguretat es veu reduïda. Així mateix, també cal remarcar que depenen del tipus d'algoritme de consens que s'utilitzi aquesta seguretat s'incrementarà o es reduirà.

Per exemple, pel que fa als algoritmes de consens Proof of Work o Proof of Stake, aquests no tenen sentit en una organització privada, ja que és més fàcil que amb aquests es posseeixi més del 50% del control de la xarxa, és a dir, diferents persones que poden col·laborar per canviar la informació. En canvi, hi ha altres proves com el Raft o Proof of Elapsed Time que s'adequen millor a aquests tipus de sistemes, pel fet que empra l'aleatorització com a eina per desenvolupar els protocols de validació.

[36]

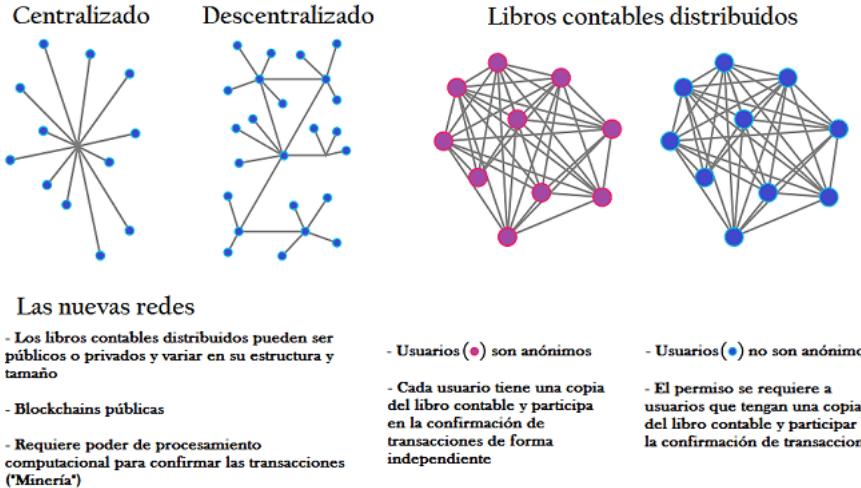


Figura 6: Diferències entre diferents tipus de blockchains.

3.5 Blockchain híbrida

Les blockchains híbridas sorgeixen de la unió d'una blockchain privada i una pública. Més concretament, en aquest projecte consisteix en la creació d'una blockchain privada que envia informació a una blockchain pública perquè la primera sigui més segura. Com en el cas de les blockchain privades, les blockchain híbridas són permissionades, és a dir, que requereixen permís per poder entrar-hi o unir-s'hi i executar diferents funcions dins d'aquesta.

Són ideals per a empreses, organitzacions o negocis que vulguin tenir una capa de seguretat addicional en la seva blockchain privada. A més, aquest tipus de sistema té grans aplicacions perquèaprofita els avantatges dels dos tipus de blockchains sense patir els seus desavantatges. Són una molt bona opció a l'hora de contemplar o desenvolupar un sistema d'emmagatzematge d'informació basat en blockchain, perquè permeten aconseguir un sistema més econòmic i sostenible alhora que segur, sempre que es contemplin els protocols adequats.

La idea d'aquest projecte de forma més detallada és crear una blockchain privada on cada bloc sigui capaç de guardar entre 5.000 i 10.000 transaccions i que aquestes quedin també enregistrades en una ledger. Cada bloc de nova creació tindrà un hash determinat que s'enviarà a la blockchain pública, per tant, es formarà una còpia de la transacció que s'ha realitzat a la blockchain privada. Així mateix, una modificació en la privada farà que els hashes en ambdues no coincideixin en aquell bloc i això podrà fer determinar que s'ha produït una

alteració de les dades.

Com bé s'ha esmentat, la blockchain privada serà de creació pròpia, però la blockchain pública que es farà servir per crear aquest sistema serà Solana, ja que per les característiques d'aquest projecte és la que resulta ser més econòmica i sostenible. Això es deu al fet que Solana no requereix potència computacional per validar les transaccions perquè fa servir el PoH (Proof of History) com a algoritme de consens i que el preu per transacció és molt baix actualment: 0.00025 dòlars [25].

Tot i això, cal esmentar que hi ha altres alternatives a l'hora d'escol·lir quina blockchain pública és la millor opció, com ara per exemple MATIC o Terra que també són molt sostenibles, encara que el seu preu per transacció és més elevat que el de Solana i per això s'ha decidit escollir aquesta darrera blockchain. Un punt a tenir en compte és que el sistema de blockchain híbrida s'ha escollit amb la finalitat de complir amb el requisit d'econòmicitat, ja que el mateix projecte publicat a una blockchain pública podria costar entre 5.000 i 10.000 euros mensuals depenent del valor de les criptomonedes, tot i emprar monedes econòmiques com són Solana o MATIC.

Finalment, cal esmentar que un sistema híbrid ha estat l'elecció més coherent a l'hora de crear una blockchain, ja que es poden tenir tots els beneficis que aporta cada tipus de blockchain i evitar-ne els perjudicis, a més d'aconseguir més seguretat en el sistema. Això permet assolir una tecnologia més segura, econòmica i sostenible.

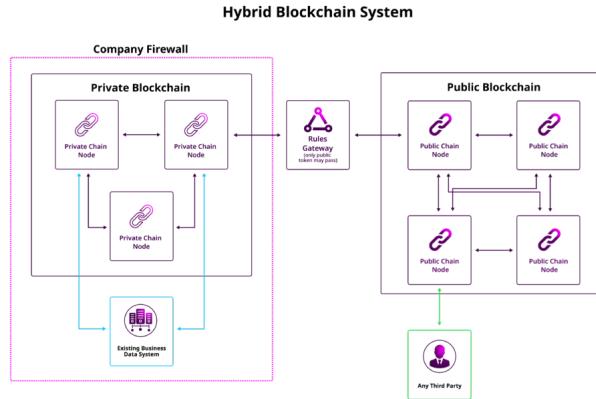


Figura 7: Descripció de l'estructura d'una blockchain híbrida.

4 Hyperledger

La Fundació Linux va fundar el projecte Hyperledger el 2015 per avançar en les tecnologies de cadena de blocs entre sectors. En lloc de declarar un únic estàndard de cadena de blocs, fomenta un enfocament col·laboratiu per desenvolupar tecnologies de cadena de blocs mitjançant un procés comunitari, amb drets de propietat intel·lectual que fomenten el desenvolupament obert. Hyperledger Fabric és un dels projectes blockchain d'Hyperledger.

Com altres tecnologies blockchain, té una ledger, utilitza smart contracts i és un sistema pel qual els participants gestionen les seves transaccions. On Hyperledger Fabric es diferencia d'alguns altres sistemes blockchain és que és privat i està autoritzat. En lloc d'un sistema obert sense permís que permet que identitats desconegudes participin en la xarxa (que requereixen protocols com ara PoW per validar les transaccions i assegurar la xarxa), els membres d'una xarxa d'Hyperledger Fabric s'inscriuen a través d'un proveïdor de serveis de membres (MSP) de confiança. Hyperledger Fabric també ofereix diverses opcions connectables. Les dades del ledger es poden emmagatzemar en diversos formats, els mecanismes de consens es poden intercanviar i sortir i s'admeten diferents MSP. Hyperledger Fabric també ofereix la possibilitat de crear canals, cosa que permet a un grup de participants crear una ledger independent. Aquesta és una opció especialment important per a xarxes en què alguns participants poden ser competidors i no volen que les transaccions que realitzin puguin ser visibles per tots els participants, com ara per exemple, un preu especial que s'ofereix a alguns participants i no a altres. Si dos participants formen un canal, aquests participants, i cap altre, tindran còpies del ledger d'aquest canal. [38] [39] [40]

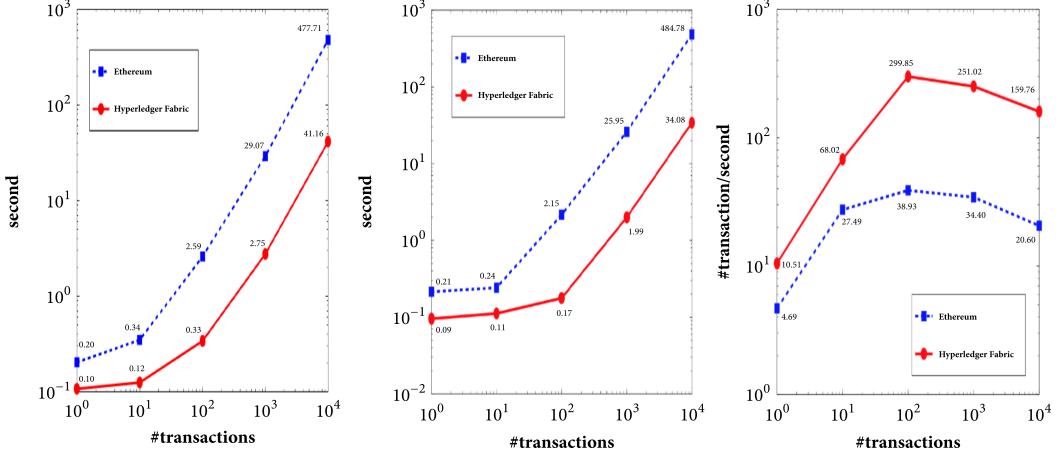


Figura 8: Temps d’execució, latència i rendiment d’Ethereum i Hyperledger Fabric, de manera respectiva

La ledger compartida Hyperledger Fabric té un subsistema de registre que consta de dos components: l’estat general i el registre de transaccions. Cada participant té una còpia de la ledger a cada xarxa d’Hyperledger Fabric a la qual pertany. El component d’estat general descriu l’estat de la ledger en un moment determinat (és la base de dades de la ledger). Per contra, el component del registre de transaccions s’encarrega de registrar totes les transaccions que han donat lloc al valor actual de l’estat general (és l’historial d’actualitzacions de l’estat general). La ledger, doncs, és una combinació entre la base de dades de l’estat general i l’historial del registre de transaccions [20]. La ledger té un magatzem de dades reemplaçable per a l’estat general. De manera predeterminada, aquesta regista els valors abans i després de la base de dades de la ledger que utilitza la xarxa blockchain.

4.1 Ledger compartit

Hyperledger Fabric té un subsistema de registre que consta de dos components: l’estat general i el registre de transaccions. Cada participant té una còpia del ledger a cada xarxa d’Hyperledger Fabric a la qual pertany.

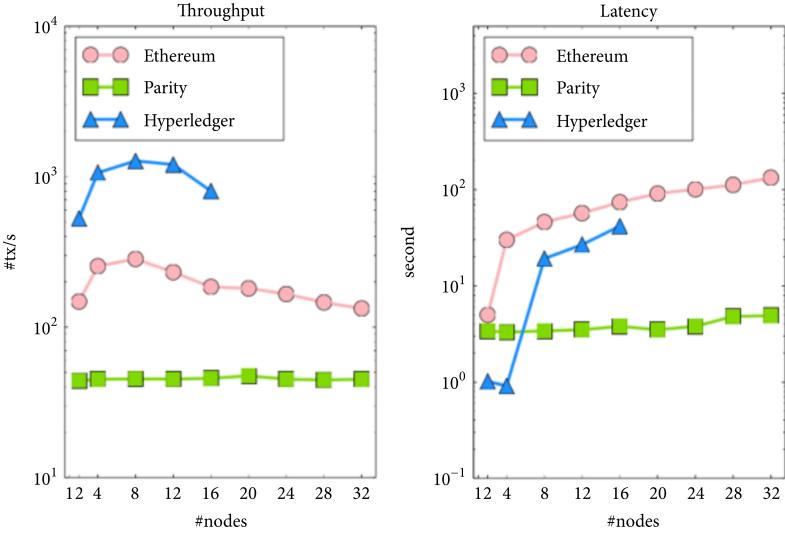


Figura 9: Escalabilitat per a Hyperledger Fabric, Ethereum i Parity.

El component d'estat general descriu l'estat del ledger en un moment determinat (és la base de dades del ledger). El component del registre de transaccions registra totes les transaccions que han donat lloc al valor actual de l'estat general (és l'historial d'actualitzacions de l'estat general). El ledger, doncs, és una combinació de la base de dades de l'estat general i l'historial del registre de transaccions.[38]

El ledger té un magatzem de dades reemplaçable per a l'estat mundial. De manera predeterminada, aquesta és una base de dades de la botiga de valors-clau de LevelDB. El registre de transaccions no ha de ser connectable. Simplement, registra els valors abans i després de la base de dades del llibre major que utilitza la xarxa blockchain. [41]

4.2 Smart contracts

Els smart contracts, anomenats 'chaincode' en el context d'Hyperledger Fabric, són convocats per una aplicació externa a la cadena de blocs quan aquesta aplicació necessita interactuar amb la ledger. En la majoria dels casos, el codi en cadena només interactua amb el component de base de dades de la ledger (estat general) i no amb el registre de transaccions. El codi en cadena es pot implementar en diversos llenguatges de programació. Actualment, s'admeten Go, Node.js i el codi de cadena Java per programar el temps d'execució, latència i rendiment d'Ethereum i Hyperledger Fabric, de manera respectiva [38].

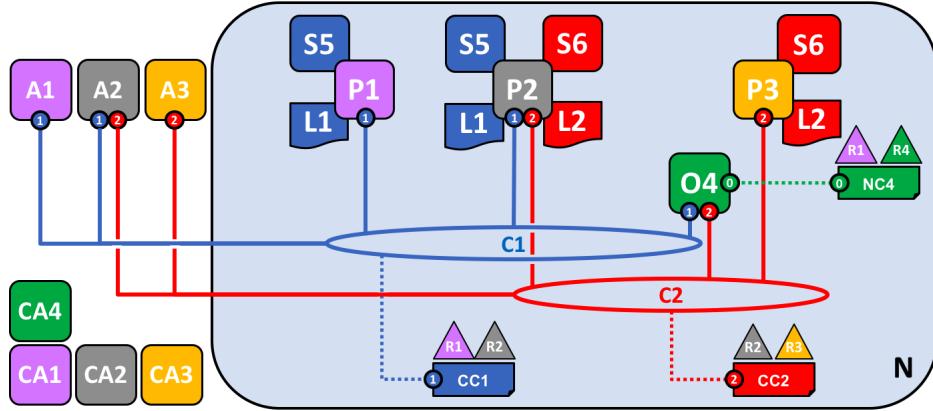


Figura 10: Descripció de l'estructura d'Hyperledger Fabric.

4.3 Privacitat

Ja es coneix que Hyperledger Fabric permet la construcció de ledgers distribuïdes. D'aquesta forma, diferents organitzacions que componen la xarxa de nodes poden interactuar entre elles a partir d'una ledger distribuïda. Així, aquestes entitats poden compartir informació entre elles sense que sigui visible per les altres organitzacions, fent servir canals determinats. És interessant per la comunicació entre entitats, ja que no sempre es vol compartir tota la informació.

En funció de les necessitats d'una xarxa de nodes, els participants d'aquesta, poden ser extremadament sensibles a la quantitat d'informació que comparteixen. Per a altres xarxes, la privadesa no serà una de les principals preocupacions. En canvi, Hyperledger Fabric admet xarxes on la privadesa és un requisit operatiu clau, així com xarxes que són completament obertes.

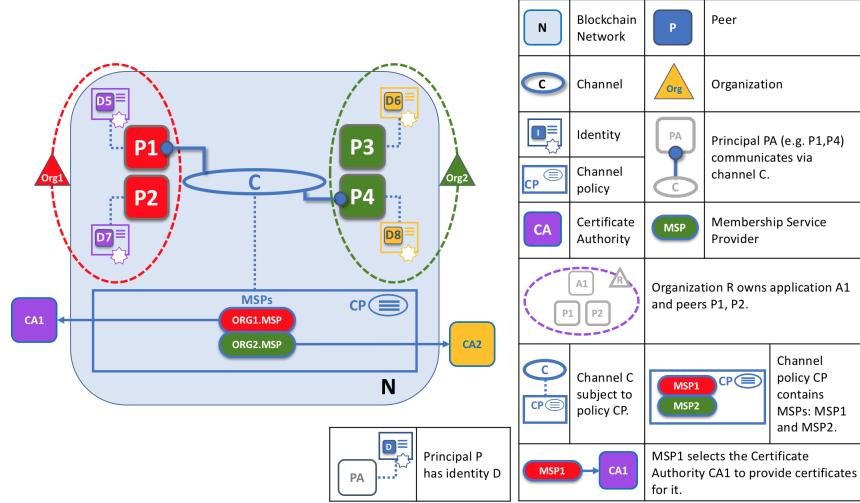


Figura 11: Demostració de com Hyperledger Fabric permet la privacitat de dades.

4.4 Algoritmes de consens

Les transaccions s'han d'escriure a la ledger en l'ordre en què es produeixen, encara que puguin estar entre diferents grups de participants dins de la xarxa de nodes. Perquè això succeeixi, s'ha d'establir l'ordre de les transaccions i s'ha de determinar un mètode per rebutjar transaccions defectuoses que s'han inserit a la ledger per error o de forma malintencionada. Aquesta és una àrea de la informàtica investigada a fons i hi ha moltes maneres d'aconseguir-ho, cadascuna amb diferents compromisos.

Per exemple, PBFT (Practical Byzantine Fault Tolerance) pot proporcionar un mecanisme perquè les duplicitats d'informació entre els nodes, es comuniquin entre elles per mantenir cada còpia, fins i tot en cas de corrupció. Per altra banda, a Bitcoin l'ordre passa a través d'un procés denominat mineria, on els ordinadors competidors (validadors de les transaccions) corren per resoldre un trencaclosques criptogràfic que defineix l'ordre sobre el qual es construeixen posteriorment tots els processos. Hyperledger Fabric s'ha dissenyat per permetre als usuaris de la xarxa seleccionar un mecanisme de consens que representi millor les relacions que existeixen entre els mateixos participants. De la mateixa manera que succeeix amb la privadesa, hi ha un espectre de necessitats: des de xarxes molt estructurades en les seves relacions fins a les que són més peer-to-peer (P2P), és a dir, amb nodes que es comporten d'igual a igual entre si.

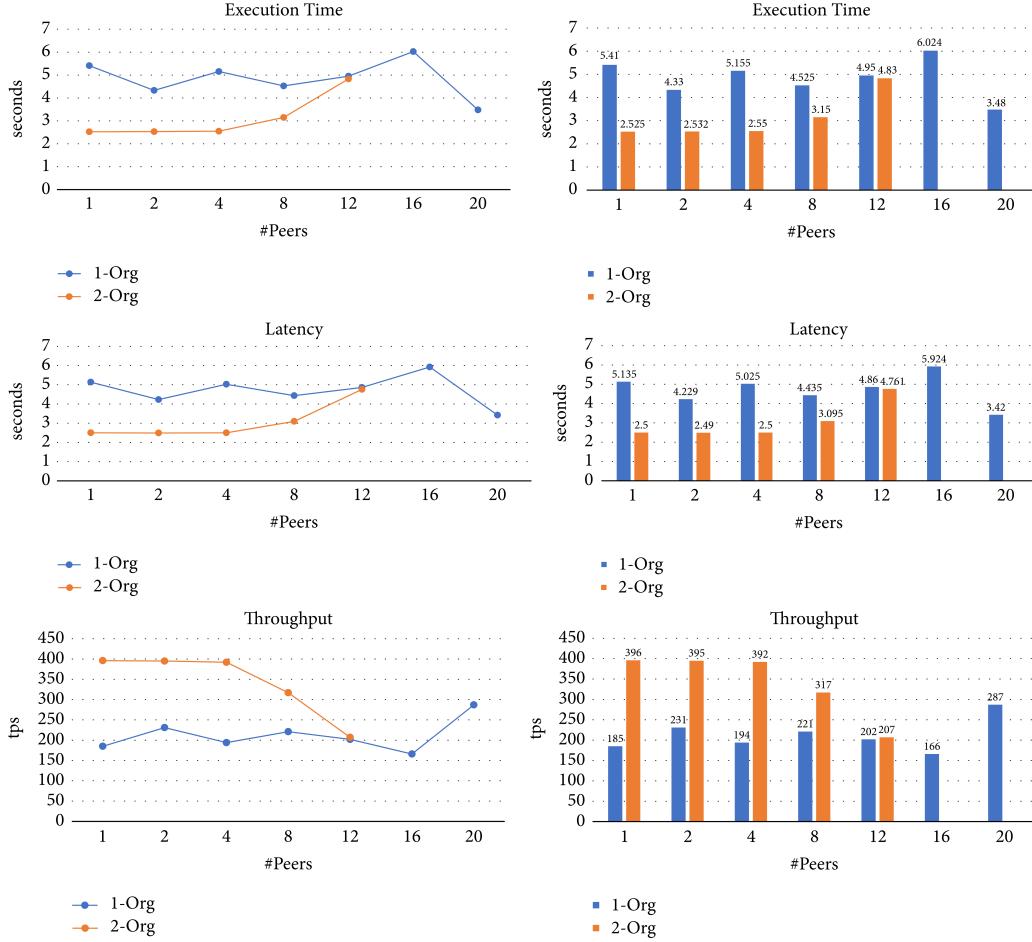


Figura 12: Avaluació per a dues organitzacions.

4.4.1 Raft (Understandable Distributed Consensus)[42]

Quan un sistema només té un node que actua com a base de dades, per una millor exemplificació es pot suposar que només emmagatzema un valor, la interacció i el consens entre un usuari que envia informació i el node que l'emmaigatzema és simple. Els problemes amb els consensos distribuïts apareixen quan s'afegeixen múltiples nodes.

Raft és un tipus d'algorisme de consens que segueix un protocol dissenyat per ser implementat en els consensos distribuïts. Dins el protocol Raft, un node pot constituir tres estats diferents: l'estat de seguidor, l'estat de candidat i

l'estat de líder. Hi ha un node líder que envia la informació a la resta de nodes, que són nodes seguidors. Així mateix, tots els nodes comencen en l'estat de seguidors, però quan aquests no reben informació del node líder poden assolir l'estat de candidat i transformar-se en candidats a líder. El candidat en qüestió sol·licitarà els vots dels altres nodes i aquests li responen amb el seu vot. Aquest fet es tracta d'una norma sistemàtica que només consta de decisions tècniques i automàtiques en el procés. Llavors, quan el node candidat rep la majoria de vots es converteix en el node líder. Aquest procés s'anomena selecció de líder i a partir d'aquest moment els canvis en el sistema es tramiten a través d'aquest. Per donar constància de la seva presència a la xarxa, tots els tipus de nodes emeten informació en forma de 'heartbeats'. Aquests es produeixen cada cert temps, normalment entre 150 i 300 mil·lisegons (ms).

Cada canvi de líder que es sol·licita és afegit com una entrada en el registre del nou node líder. Per confirmar l'entrada, el nou node líder replica la informació als nodes seguidors i espera fins que la majoria de nodes hagin enregistrat l'entrada i, una vegada aconseguit, es produeix l'acceptació del canvi de líder. Tot aquest procés es realitza de forma automàtica. Una vegada s'ha elegit un líder, s'han de replicar els canvis del sistema a tots els nodes i això es fa utilitzant el sistema de "heartbeats" que també s'empra en el procés d'adjuntar missatges d'entrada.

Primer de tot, un usuari envia un missatge al líder. En aquest protocol hi ha dos paràmetres de temps d'espera que controlen les eleccions. El primer és the election timeout, és a dir, la quantitat de temps que un seguidor espera fins a convertir-se en candidat i és un valor comprès entre 150 ms i 300 ms. Després d'aquest temps d'espera, el seguidor es converteix en candidat i comença un nou procés electoral. Així, es remet una sol·licitud a la resta de nodes per confirmar que la majoria l'interpreta com a líder, on el node receptor sempre votarà pel candidat i, posteriorment, es restableix el temps d'espera temporal dels nodes seguidors. Quan el node candidat aconsegueix ser el líder, els missatges que li arriben són enviats a la resta de nodes en intervals de temps específics determinats per un heartbeat i els seguidors responden a aquests. Aquest període electoral continuarà fins que un seguidor deixi de rebre 'heartbeats' i, d'aquesta manera, es podrà convertir en el candidat. Requerir la majoria de vots garanteix que només es pot escollir un líder per mandat. Si dos nodes esdevenen candidats al mateix temps, es pot produir una votació dividida, però gràcies al fet que 'the election timeout' és un valor comprès entre 150 i 300 ms, aquesta situació no perdurà en el temps. [43] [42]

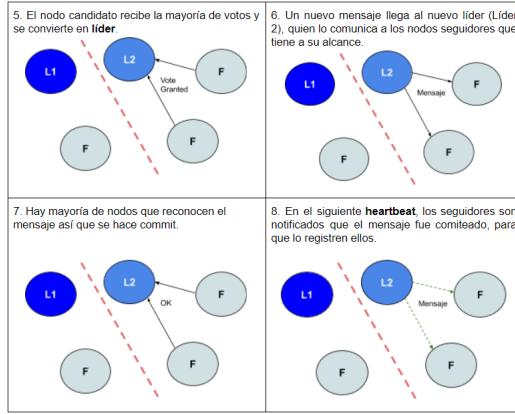


Figura 13: Descripció visual del procés del protocol Raft.

4.5 Casos d'implementació de la tecnologia Hyperledger Fabric

L'aplicació d'Hyperledger Fabric permet una millor traçabilitat dels productes. Així és com aquest sistema es va implementar a l'empresa Walmart, una corporació multinacional d'origen nord-americà que opera com una cadena de supermercats, magatzems de comestibles i tendes departamentals a preus molt baixos. Aquesta implementació de la tecnologia Hyperledger Fabric a la cadena de subministrament de l'empresa ha permès aconseguir la localització exacta de l'origen dels productes, a més de poder ubicar l'aparició de brots de mal estat en els productes. D'aquesta manera, no només s'ha pogut assegurar al client l'origen dels productes sinó que també s'ha pogut reaccionar davant la retirada de productes defectuosos amb més precisió i rapidesa. Així, l'origen dels brots produïts s'ha arribat a localitzar en menys de cinc segons, quan abans el procés durava setmanes.

Aquest sistema també es va implementar a l'empresa multinacional Honeywell, una companyia líder en tecnologia i fabricació que proporciona: productes i serveis aeroespacials, tecnologies de control per edificis, habitatges i indústries, sistemes de generació d'energia, productes químics especials, fibres, plàstics i materials electrònics [44]. Aquesta empresa va crear una pàgina web de venta de recanvis tecnològics basada en Hyperledger Fabric [0]. Amb l'aplicació d'aquest sistema, la companyia ha aconseguit reduir el temps de compra dels seus productes a segons i registren les peces venudes a la blockchain per millorar la traçabilitat d'aquestes.

Finalment, Deutsche Börse Group, una empresa organitzadora de mercat per

la negociació d'accions i altres valors, a més de proveïdor de serveis de transaccions [45], ha apostat també per la implementació d'Hyperledger Fabric per permetre transaccions en efectiu i realitzar transferències multijurisdiccionals de valors. [46] [47]

Falta esmentar, que hi ha altres projectes interessants, que estan desenvolupats a blockchains públiques, però que serien més eficients i obtindrien més rendiment si implementessin Hyperledger Fabric. Alguns d'aquests són el projecte d'ICO Costaflores [48] [49], el de MFarmer [50], el de la blockchain dedicada a l'agricultura [51] o les blockchains dedicades a la ramaderia. [52] [53]

5 Implementació

Com a resposta al projecte 'Blockchain 4SDG' i a fi d'assolir el control de la planta purificadora a través de la tecnologia blockchain, es descriurà primerament el funcionament general de la planta i, posteriorment, s'exposaran les dues implementacions paral·leles que es requereixen dur a terme:

- Desenvolupament de la blockchain
- Protocol a seguir pel correcte funcionament de la planta

5.1 Descripció de la planta pilot purificadora

Com es pot veure a la Figura 14, la planta purificadora consta de diferents dipòsits i processos. En resum, primerament l'aigua residual regenerada arriba al dipòsit de capçalera, on es localitzen quatre tipus de sondes principalment: cabalímetre, conductivitat elèctrica ($\mu\text{S}/\text{m}$), amoni ($\text{mg NH}_4\text{-N}/\text{L}$) i carboni orgànic total ($\text{mg TOC}/\text{L}$). A mesura que l'aigua surt d'aquest dipòsit, aquesta és cloraminada (addició de monocloramina) a fi d'evitar que el clor reacció amb la matèria orgànica i la consegüent generació de subproductes d'elevada toxicitat. Aquesta aigua arribarà al procés de microfiltració, que suposa el primer pas pel tractament de membrana amb l'objectiu de retenir sòlids en suspensió i soluts d'alt pes molecular. Tot seguit, l'aigua ha de passar per l'osmosi inversa a través de dos passos, que suposen el segon procediment del tractament de la membrana, en el qual es retenen els soluts de baix pes molecular (eliminació de l'amoni, el bor i les sals) i on es localitzen les mateixes sondes esmentades anteriorment. Posteriorment, l'aigua passa pel procés d'oxidació avançada (UV-AOP) on es dosifica peròxid d'hidrogen i travessa un reactor de llum ultraviolada perquè les possibles molècules que puguin trobar-se a l'aigua es degradin. En aquest cas, la principal sonda que es té en compte és la del potencial REDOX (mV). Tot

seguit, succeeix la filtració amb carbó actiu per retenir els fragments moleculars generats durant l'oxidació avançada. Finalment, l'aigua acaba al dipòsit de sortida on es produeix la remineralització d'aquesta, és a dir, la restitució de cations i anions. En aquest últim procés s'ubiquen també les mateixes sondes que en dipòsit de capçalera.

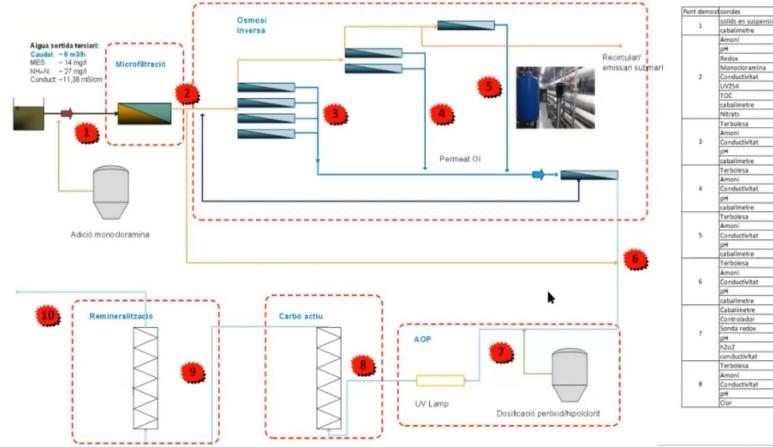


Figura 14: Esquema general del funcionament de la planta pilot purificadora amb els respectius processos de tractament de l'aigua i sondes, així com els paràmetres fisico-químics que mesura cada una d'elles. Els paràmetres mesurats en l'aigua depenen del procés en el que es trobi aquesta.

Llavors, segons la ubicació de l'aigua a la planta, aquesta passarà per un procés o altra. Així, els paràmetres fisicoquímics que ha de presentar l'aigua en cada moment seran diferents. Per això, les sondes seran les encarregades de determinar amb precisió els paràmetres que presenta l'aigua en cada moment del seu tractament, és a dir, el rang de valors típics i desitjables per cada tipus de sonda segons la localització de l'aigua a la planta. (Figura 16)

Ubicació	Rang de valors típics / desitjables per a cada tipus de sonda				
	Cabalímetre	Conductivitat elèctrica, $\mu\text{S}/\text{m}$	Amoni, mg NH4-N/l	Carboni orgànic total (TOC), mg/l	Potencial redox, mV
Dipòsit de capçalera	Nominal d'alimentació (x)	5.000 – 12.000	10 - 30	10 - 15	-
Microfiltració	-	-	-	-	-
Osmosi inversa, pas 1	0,8 x	< 500	< 5	< 3	-
Osmosi inversa, pas 2	0,6 x	< 100	< 1	< 1	-
Oxidació avançada (UV-AOP)	-	-	-	-	> 400
Remineralització - Dipòsit de sortida	Nominal producció (y)	< 500	< 1	< 1	-

Figura 15: Rangs desitjables de l'aigua pels principals paràmetres: cabalímetre, conductivitat elèctrica, amoni, carboni orgànic total i potencial REDOX, mesurats amb els diferents tipus de sondes, segons la localització de l'aigua a la planta.

5.2 Desenvolupament de la blockchain

Pel fet de requerir el projecte un disseny modular i escalable i a causa d'un entorn ple de diferents rols i permisos, així com necessitar un pretindre un projecte segur, sostenible i econòmic, es decideix implementar la blockchain emmarcada dins d'un entorn de tecnologia Hyperledger. Concretament, s'aposta per Hyperledger Fabric. A continuació, es defineix aquest entorn, determinat per Hyperledger, i es detalla la interacció amb la blockchain pròpiament.

5.2.1 Entorn

Com bé s'ha esmentat, les sondes són les encarregades de mesurar diferents paràmetres a l'aigua per poder tenir un control precís sobre la qualitat d'aquesta durant tot el tractament. Si les dades recopilades per les sondes entren dins del rang de qualitat d'aigua desitjable (que hauran estat prèviament establlits), aquesta aigua podrà ser transportada als aquífers corresponents per tal de recarregar-los.

Aquesta situació ha de ser validada per diferents organitzacions, entre les quals es fa especial esment a:

- Consorci d'Aigües Costa Brava de Girona
- Agència catalana de l'aigua (ACA)
- Salut pública

- Ajuntaments, cada un dels quals corresponen a una organització diferent
- Altres possibles entitats interessants pel control de la situació

Totes aquestes organitzacions, amb els seus respectius usuaris, es constitueixen dins el marc d'Hyperledger com a nodes que s'encarreguen de validar i verificar l'estat de les dades de la blockchain. A aquest conjunt de nodes, se li suma el node que es correspon al de la mateixa planta purificadora i que és la principal encarregada de transaccionar amb la blockchain.

Un node té un servidor de credencials (MSP) i serveix per afegir als usuaris amb els seus respectius credencials (clau pública i clau privada, una cartera digital o 'wallet'). Cada usuari d'una organització s'anomena 'peer'.

5.3 Interacció a la blockchain

S'escriu un smart contract (anomenat 'chaincode' en el context d'Hyperledger). Aquest passa per un procés d'aprovació per part de totes les organitzacions participants i s'encarregarà de regular totes les interaccions (o no interaccions) d'escriptura, computació o lectura de l'estat de les dades de la blockchain.

El 'chaincode' permet que el node corresponent a la planta enregistri dispositius, com seria en aquest cas les sondes o sensors, amb certa informació associada a aquests. A més, també ofereix un càlcul dinàmic per determinar els rangs desitjables dels paràmetres en funció de diverses variables introduïdes prèviament. Per exemple, el chaincode calcula els rangs en els quals es troba el procés d'osmosi inversa en funció del cabal. És a dir, com que prèviament s'hauran introduït a la blockchain els rangs (dinàmics i estàtics) desitjables de tots els sensors de la planta per cada moment del tractament, això suposaria una bona manera de poder detectar possibles incidències si els valors calculats en aquell moment no s'adequen dins del rang estableert prèviament.

Aquest 'chaincode' també ofereix la possibilitat de rebre la crida a una funció per part d'una vàlvula automatitzada i que serà la que rebrà la darrera ordre de 'GO / NO GO' en funció de la qualitat de l'aigua, és a dir, en el moment que es detecti una incidència en la qualitat de l'aigua o en un tractament, es produirà un enviament automàtic del senyal 'NO GO' perquè l'aigua no surti de les instal·lacions. Per determinar una correcta o no correcta qualitat de l'aigua a la sortida de la planta, es realitzarà una ponderació de totes les dades associades als dispositius de la planta (sondes, sensors) i aquestes seran validades per les organitzacions adscrites a la xarxa. Llavors, en el cas que el resultat esdevingués negatiu pel que fa als requisits de l'aigua, s'accionaria l'avís de 'NO GO' i s'enviaria una notificació als usuaris de les organitzacions participants. Així, aquella aigua no sortirà de la instal·lació vers la recàrrega.

Si la problemàtica detectada en l'aigua es pogués resoldre, aquesta es tornaria a condir cap a la capçalera del tractament si fos possible. Per contra, l'aigua que no pogués ser corregida pel que fa a la seva qualitat, seria abocada al mar via emissari submarí. D'aquesta manera, el sistema contemplarà un registre clar de què l'aigua aportada cap a la recàrrega d'aquífers compleix amb tots els requeriments establerts o, al revés, que en cas d'incidència no hi serà portada.

Per tal de portar un registre complet de totes les accions produïdes a la blockchain, el node de la planta pilot s'encarrega cada 20 minuts d'actualitzar els valors de les sondes, sensors, vàlvules i altres possibles dispositius de la planta mitjançant una crida a la funció del chaincode de la blockchain, per poder fer-hi canvis. Cada canvi s'anomena transacció i permet afegir nova informació a la blockchain.

Quan es fa una transacció i un valor no es troba dins el rang desitjable que prèviament ja s'ha determinat i deixat en constància, s'emet un senyal que arribarà en forma de notificació a totes les organitzacions corresponents a l'instant si així es configura. Per exemple, aquest avís es podria realitzar mitjançant correu electrònic o SMS.

Per tal de proporcionar una manera fàcilment accessible i comprensible per l'usuari, tant el que introduirà les dades com els encarregats de només validar-les, es disposa a les organitzacions una interfície d'usuari composta per dues parts. La primera part està conformada pel codi d'una API (Application Programming Interface) que actua com a intermediari entre la interfície i les cridades a les funcions de la chaincode. La segona part està composta per una aplicació web que facilita a l'usuari el registre i emmagatzematge de les seves credencials. Amb aquesta aplicació, l'usuari podrà visualitzar amb facilitat les dades de la blockchain, introduir noves dades (si té els permisos pertinents) i, en definitiva, interactuar amb la blockchain d'una manera àgil i senzilla.

El mètode de consens que s'ha escollit és el Raft, ja, per una banda, està dissenyat per blockchains que empren Hyperledger Fabric i, per altra banda, perquè permet que el projecte compleixi amb els requisits de seguretat, sostenibilitat i economicitat que tant es desitgen. És un algoritme de consens que es recolza sobre l'aleatorietat com a mecanisme de seguretat. Aquest factor és important, perquè així com en altres blockchains s'empra la capacitat de computació (PoW) o la capacitat econòmica (PoS), situacions on si es té més del 51% de la capacitat pot ser vulnerar la blockchain, en el cas del Raft, el node validador és el líder i és escollit a l'atzar emprant un sistema de 'heartbeats', com ja s'ha explicat anteriorment.

Amb aquest esquema format, es planteja que la planta purificadora sigui la principal emissora d'informació i que les sondes recaptin i enviïn informació cada 20 minuts. D'altra banda, la resta de nodes poden comprovar la informació,

que no és el mateix que modificar-la. Si es modifica quedarà enregistrat a la blockchain, de forma que es podrà saber que la informació ha estat alterada.

Llavors, es posaran per cas dues situacions. A la primera, se suposa que la qualitat de l'aigua és bona i que no es produeixen incidències en els rangs dels paràmetres desitjats. En aquesta situació, els nodes (organitzacions) i 'peers' (usuaris) que conformen la blockchain i que no són el node de la mateixa planta, tindran una funció de comprovació que les dades entrades pel node de la planta (sigui manual o automàticament) siguin correctes. És a dir, cada cert temps es prenen mostres manualment de l'aigua tractada per la planta purificadora, per comprovar que la seva qualitat és l'adequada i aquests resultats no només asseguraran que l'aigua tingui les característiques esperades, sinó que també es publicaran a la blockchain. Això permet fer una comparativa dels resultats obtinguts de forma manual i els resultats publicats per la mateixa planta en aquell mateix moment. Així, es podrà determinar si les dades entrades per la planta són les correctes, a més de poder aconseguir a llarg termini una base de dades ('big data') que contingui tota la informació enregistrada i que serà traçable, inalterable i fiable. En cas de detectar una incidència en l'aigua que la planta no ha detectat, a part de poder solucionar aquesta problemàtica també es podrà millorar el sistema blockchain amb nova informació que li permetrà ser més precisa.

Es considera també el cas en el qual hi hagi una organització que vulgui realitzar inspeccions ordinàries o extraordinàries sobre la qualitat de l'aigua de la planta. Per aquests casos, es redactaria una funció específica al chaincode disponible per aquestes organitzacions i, si la resta de nodes l'aproven, aquesta funció serviria per enregistrar els resultats de les inspeccions a la blockchain.

Com bé s'ha dit, les dades recollides tant d'una manera com d'altra es publicaran a la blockchain, la qual és la base de dades d'una pàgina web que es crearà. És a dir, totes les dades enregistrades a la blockchain seran publicades automàticament a aquesta pàgina web per facilitar la interacció entre la blockchain i el públic general, ja que la pàgina web serà completament pública i accessible per qualsevol persona, aconseguint un model totalment transparent. Dit això, cal esmentar que aquesta pàgina web serà un sistema dinàmic en el qual s'hi anirà publicant informació actualitzada de forma automàtica sobre la planta. També es remarca, però, que la pàgina inclourà funcions exclusives pels administradors, que seran usuaris autoritzats, com ara l'operari de la planta, les organitzacions corresponents o altres usuaris que es considerin pertinents.

Llavors, en aquesta pàgina web s'hi situaran els diversos processos de tractament de l'aigua i totes les sondes corresponents a cada un d'ells. D'aquesta manera, en clicar sobre un procés determinat (per exemple l'osmosi inversa) i un tipus de sonda concreta (per exemple la mesura de la conductivitat elèctrica), s'accedeix a un segon portal on es mostra un gràfic més gran i específic amb un historial de les transaccions. Aquestes presenten la informació que s'ha

enregistrat de la sonda des de la implementació del sistema fins a la darrera actualització, al present.

Per contra, a la segona situació, es planteja la idea que la qualitat de l'aigua detectada per la planta no és bona, és a dir, s'ha percebut que algun o alguns paràmetres mesurats no entren dins del rang prèviament establert. En aquest cas, el senyal 'NO GO' s'activarà i es tancarà de forma automàtica la vàlvula de sortida d'aigua de les instal·lacions cap als aquífers. Tot seguit, s'enviarà un avís a l'operari de la planta i a les organitzacions corresponents per tal de notificar aquesta incidència a través d'un correu electrònic o SMS (és configurable), com s'ha mencionat anteriorment. Així, l'operari encarregat de solucionar la problemàtica detectada, resoldrà la incidència i l'enregistrarà de forma manual a la blockchain a través d'una funció del chaincode, la qual va enllaçada a la pàgina web. D'aquesta manera, la incidència passarà a formar part de la pàgina web automàticament. Posteriorment, quan aquesta incidència ja estigui resolta, l'operari tornarà a enregistrar a la blockchain que la problemàtica ha estat resolta i es remetrà una notificació de forma automàtica a les organitzacions corresponents (a través de correu electrònic o SMS també, per exemple) perquè aquestes estiguin assabentades.

Així, com bé s'ha comentat, la pàgina web també permetrà rebre incidències a través de l'operari i això permetrà que aquests puguin ser enregistrades per a accés de qualsevol usuari interessant, de la mateixa manera que també es podrà comprovar la resolució d'aquests. Per acabar, cal fer esment que aquest sistema permetrà deixar detallat a la pàgina web el moment exacte en el qual es realitzaran tots els registres: les publicacions de dades, les incidències i les solucions aportades.

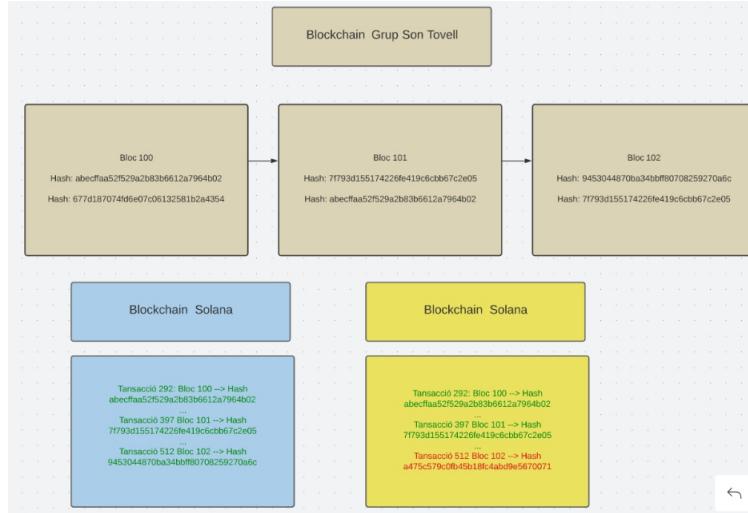


Figura 16: Visualització del procés que realitza la funció automatitzada per la revisió dels hashes.

6 Prova de concepte

En aquest apartat, es disposa una prova de concepte de la implementació d'aquest projecte. Tot el codi es troba disponible públicament al següent enllaç: <http://github.com/metabig/Can-Tovell-Blockchain>. Podem distingir quatre parts d'aquesta implementació: La xarxa que compon el conjunt de nodes on s'utilitza Hyperledger Fabric, el chaincode o smart contract, l'API i, finalment, l'aplicació web desenvolupada amb React. Aquest apartat requerirà coneixements tècnics per a una plena comprensió.

6.1 Xarxa d'Hyperledger Fabric

Per aquesta prova de concepte hem utilitzat la xarxa de test d'Hyperledger Fabric de la darrera versió. Concretament, iniciem la xarxa usant couchdb a una capa per sobre com a base de dades de l'estat de la blockchain. Una vegada comprovada la satisfacció dels requeriments de Hyperledger Fabric a la seva documentació oficial, a successió de comandes seria la següent:

```
#Baixeus les imatges de Docker necessàries
#Descàrrega de la xarxa de proves de teixit
```

```

curl -sSL https://bit.ly/2ysbOFE | bash -s
#Accés a la carpeta amb scripts útils
cd fabric-samples/test-network
#Crea un canal (anomenat "mychannel" per defecte)
#   Servidor de credencials msp (amb -ca)
#   Model de base de dades d'estats iguals: couchdb
./network.sh up createChannel -ca -s couchdb

```

En aquest punt, entre una llarga llista de logs se troba la llista de Dockers i la creació de tres organitzacions (nodes) i un usuari per cada organització. Tenim, llavors: peer0.org1.example.com, peer0.org2.example.com i orderer.example.com

6.2 Chaincode

S'ha creat el chaincode per a poder enregistrar, consultar, actualitzar i algunes operacions bàsiques pels dispositius i valors associats a ells. A continuació, es mostra un exemple del model d'un dels dispositius que s'enregistrarà amb la funció d'inicialització del chaincode. El chaincode està escrit amb el llenguatge javascript.

```

//Model
let device = {
  docType: type,
  id: id,
  name: name,
  value: value,
  deposit: deposit,
  unit: unit,
  min: min,
  max: max,
};
//Exemple
{
  id: "Conductivitat-01",
  name: "Conductivitat elèctrica",
  unit: "microS/m",
  value: 5234,
  deposit: "Dipòsit de capçalera",
  type: "sensor",
  min: 5000,
  max: 12000,
}

```

Aquest contracte, el qual es pot trobar complet al Github `./chaincode/lib/sensorUpdater.js` i la següent comanda, es demana l'aprovació de les altres organitzacions per a que aquest smart contract i en concret les seves funcions siguin el medi d'interacció amb la blockchain.

```
# Amb el nom sensorchain i la ruta absoluta del chaincode
# especificant javascript com a llenguatge seleccionat
./network.sh deployCC -ccn sensorchain -ccp \
/home/user/Can-Tovell-Blockchain/chaincode -ccl javascript
```

A partir d'aquest punt, una vegada invocada la funció per inicialitzar la ledger, es pot interactuar des de la terminal amb aquest smart contract de la següent manera:

```
# Obtenim en aquest cas l'històric de transaccions.
# En aquest cas no fa falta adjuntar credencials
# perquè és una acció pública.
peer chaincode query -C mychannel -n sensorchain -c \
'{"Args":["GetAssetHistory","Conductivitat-01"]}'
```

6.3 API i aplicació web

Es crea una API amb nodejs i el framework d'express perquè actuï com a intermediari entre l'aplicació web i la blockchain, aquesta api crearà la wallet per a un usuari de l'organització 1. En un cas ideal i en producció no seria l'API qui s'encarregui d'aquesta funció sinó que seria una extensió del cercador com MetaMask la que s'encarregaria de guardar les claus corresponents. Una vegada inicialitzada l'API que es troba a `./blockchain-gw-api` es crearà la carpeta `wallet` i s'executarà la funció `InitLedger` de la blockchain.

```
#Per iniciar l'API al port 8100 (per defecte)
npm install
npm run dev
```

A partir d'aquest punt, l'API ofereix diversos *endpoints* per a interactuar amb la blockchain. Exemples:

```
//Obtenció de l'històric de transaccions donat l'identificador del sensor.
GET localhost:8100/api/history/:id

//Publicació de sensors
POST localhost:8100/api/sensors
```

```

Content-Type: application/json

{
    id: "Conductivitat-01",
    name: "Conductivitat elèctrica",
    unit: "microS/m",
    value: 5234,
    deposit: "Dipòsit de capçalera",
    type: "sensor",
    min: 5000,
    max: 12000,
}

//Actualització del valor d'un sensor
PATCH localhost:8100/api/device/Conductivitat-01
Content-Type: application/json

{
    "value": 5566
}

```

Inicialització de l'API:

```

app.listen(8100, async () => {
    const wallet = await buildWallet(Wallets, walletPath);

    await enrollAdmin(caClient, wallet, mspOrg1);

    await registerAndEnrollUser(
        caClient,
        wallet,
        mspOrg1,
        org1UserId,
        "org1.department1"
    );

    await gateway.connect(ccp, {
        wallet,
        identity: org1UserId,
        discovery: { enabled: true, aslocalhost: true },
    });
    const network = await gateway.getNetwork(channelName);
    const contract = network.getContract(chaincodeName);
    await contract.submitTransaction("InitLedger");
});

```

Tot seguit, s'inicialitza l'aplicació web construïda amb React Framework que lleix i es classifiquen tots els dispositius registrats a la blockchain. A més a més, aquesta realitza un gràfic comprovant L'històric de transaccions de cada dispositiu. Per a inicialitzar aquesta aplicació web s'utilitzen les següents comandes:

```
npm install
npm start
```

Dit això, es mostren captures de pantalla per mostrar certs comportaments de l'aplicació web amb valors aleatoris.

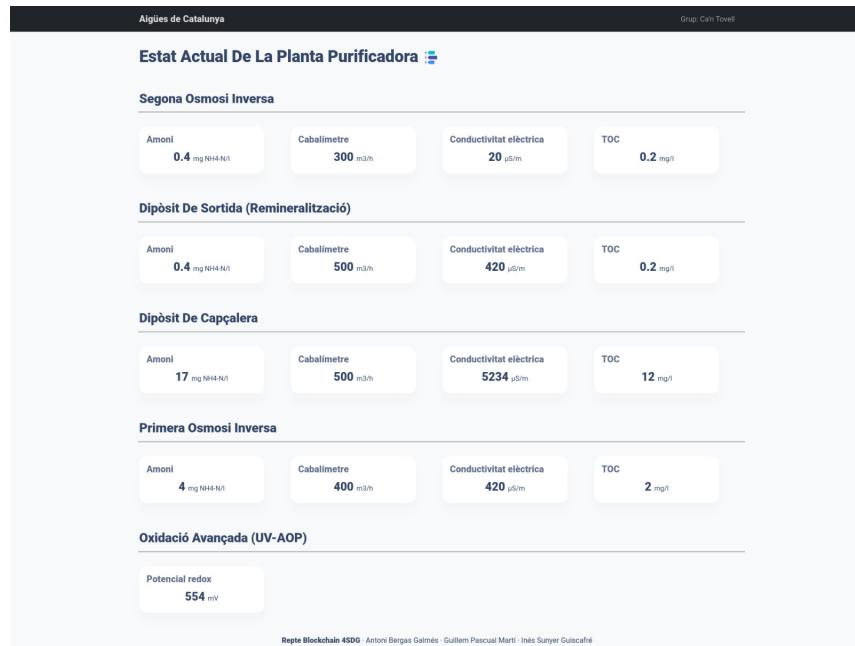
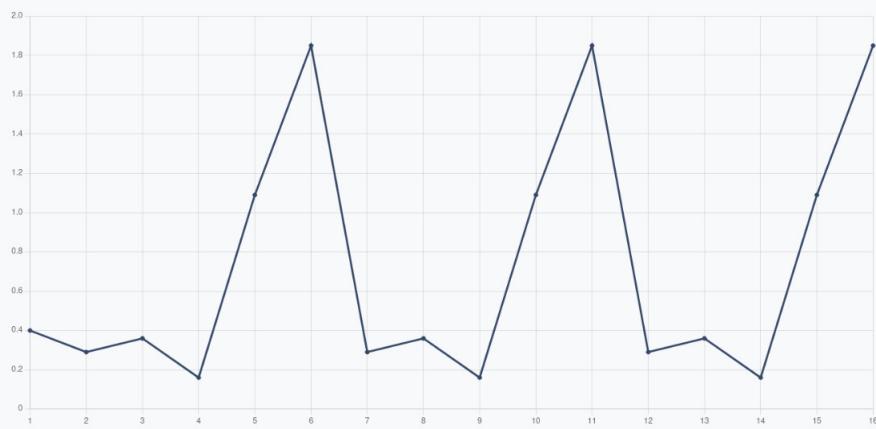


Figura 17: Pàgina d'inici des de la vista d'un membre de les Aigües de Catalunya.

Amoni



Històric de Transaccions

#	TxId	Data	Valor
16	1c020871755acfa2bc2377c083dd51cdcce9c2d72624001b5ad348549889b5c5	2022-03-05T00:53:52.000Z	1.85
15	3ce6f2be3e7ceaf64648963243526321e59c7dbaf53e14dd3acfcc9378ae21b	2022-03-05T00:53:52.000Z	1.09
14	6bb39d22ff801ab0b81852d41a7fcf06f045ef489c37b4c6e487dae9bf4fb9a287e	2022-03-05T00:53:51.000Z	0.16
13	cfc0ceacc750baa685f20d0ba7a6f6777ba0d4a5e7618efaa0f53239531dea	2022-03-05T00:53:50.000Z	0.36
12	7ffc1370851a5334e92e0e6de83dd2212bdfe5d0aa6ccca1766bbd6ea055951	2022-03-05T00:53:50.000Z	0.29
11	4475f035ff1212d271fe2ef6df63d91d7c9f91097519018b852732f3c0aa9bd3	2022-03-05T00:53:29.000Z	1.85
10	5356441308fb1595a635e51d2555b373c20603d48496cf24d6a3e9757a5f9e9f	2022-03-05T00:53:29.000Z	1.09
9	e0c123a4412cf3310722b1a259461f0141203abcf7ae30ab08006b72b271a	2022-03-05T00:53:28.000Z	0.16
8	609dc28d914d1d3d38bf072f65b9fe1f21fcba4d39edcc83943a175ec0a3cd44	2022-03-05T00:53:28.000Z	0.36
7	9bcb9d570439f1960e82304f1617f912c6623e5507df109ede0b0a2bec12b6	2022-03-05T00:53:27.000Z	0.29
6	649c2bcb630822a0a19d7180792d1c1607f55e601ea7b3233a8fee82457833a	2022-03-05T00:51:44.000Z	1.85
5	12074078cd54a231270ec136741788d00573c86dd39f630c74825028390d67fc	2022-03-05T00:51:44.000Z	1.09
4	86b96415ac8e3af3454ec731c72537cd9999d94d66bf9912c995a0f2bd88ef0	2022-03-05T00:51:43.000Z	0.16
3	8b2c184d1f912f05a77dc1f0a151cf539cf2b4adf11b63892bcc7dec5294c66	2022-03-05T00:51:43.000Z	0.36
2	14e920c0228bb978f5dfffa22dfbe7f5e59721699341d7ed56f769b88e3aa9b	2022-03-05T00:51:42.000Z	0.29
1	14bc80195d114d7b11585a6b8e9f541049395d05027121eddc675c07d61a60d1	2022-03-05T00:51:33.000Z	0.4

Repte Blockchain 4SDG - Antoni Bergas Galmés - Guillem Pascual Martí - Inés Sunyer Guiscafre

Figura 18: Vista completa concreta de l'amoni. Una gràfica i l'històric de transaccions.

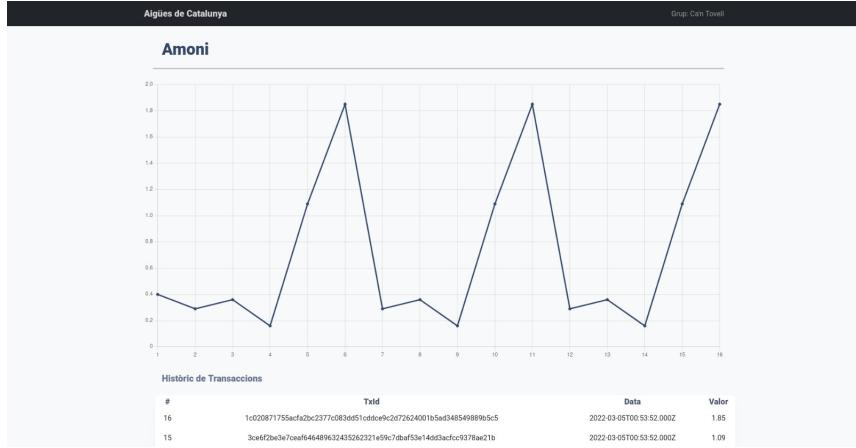


Figura 19: Vista detallada concreta de l'amoni. Una gràfica i l'històric de transaccions.

Per aclarir certs aspectes de la prova de concepte, s'exemplifica el recorregut de la dada en un cas concret. Un usuari pot actualitzar el valor d'un dispositiu des de la web, aquest construeix una request perquè amb la API es pugui interactuar amb la funció del chaincode d'actualitzar el dispositiu i, finalment, s'afegeixin dades a la blockchain. Una vegada fet això, quan la web realitzi la petició novament per obtenir les dades, l'API obtindria les dades actualitzades i faria possible la publicació de la web.

Una de les intencions de la creació d'aquesta API i aquesta aplicació web passaria perquè les organitzacions s'adaptin a l'entorn al seu gust de la manera més flexible possible, però que, com a mínim, comptin amb una base útil, versàtil i plenament funcional facilitant el seu desenvolupament posterior.

7 Extensió del projecte

Finalment, s'ha de comentar que hi ha una possibilitat per escalar la implementació del projecte del grup Ca'n Tovell aprofitant l'oportunitat que brinda el concurs A contrarellotge 2030, promocionat per l'Ajuntament de Girona. Aquesta extensió està plantejada per tenir sota control una petita zona de conflicte d'aigües, amb la finalitat de construir un mapa de la mateixa i poder conèixer els valors de l'aigua a cada punt d'aquest. És útil en cas que es vulgui fer un estudi de la zona o per determinar possibles mesures correctives o preventives.

La mateixa idea es pot implementar en un mapa més general d'aigües i,

cercant punts estratègics es poden fer servir per determinar quines són les zones més contaminades i cercar actuacions sobre aquestes, així com optimitzar la ubicació de plantes de tractament d'aigües residuals o prevenir l'arribada d'aigua molt contaminant a certes plantes de tractament per evitar que es rompin o es degradin parts d'aquestes, així com els filtres o les sondes.

8 Conclusions

Aquest projecte pretén no només demostrar la clara necessitat de la posada en marxa d'una planta purificadora d'aigua regenerada, sinó també del gran avenç que suposa la implementació de la tecnologia blockchain en aquesta.

La tecnologia blockchain que es vol implementar permet aconseguir els aspectes fonamentals: la seguretat, la sostenibilitat i l'economicitat, que s'aconsegueixen a través de la idea d'una blockchain híbrida Hyperledger Fabric, que permet crear un sistema traçable, fiable, sostenible i econòmic gràcies al fet que la blockchain pública que es farà servir és Solana i la blockchain privada és de creació pròpia.

Pel que fa a l'algoritme de consens, Raft, permet assolir molta seguretat en el procés. Tota aquesta xarxa permetrà que diferents nodes i usuaris puguin estar interconnectats dins la blockchain. Finalment, les dades de la planta purificadora seran publicades a la blockchain, que es troba enllaçada directe i automàticament a una pàgina web d'elaboració pròpia que permetrà transparència, ja que és d'ús públic, però només amb accés autoritzat dels administradors, que permetrà veure totes les dades que les sondes de la planta mesuren.

Referències

- [1] B. J. Robert, “Water in a changing world,” Aug 2001. [Online]. Available: [https://esa.journals.onlinelibrary.wiley.com/doi/abs/10.1890/1051-0761\(2001\)011\[1027:WIACW\]2.0.CO;2](https://esa.journals.onlinelibrary.wiley.com/doi/abs/10.1890/1051-0761(2001)011[1027:WIACW]2.0.CO;2)
- [2] [Online]. Available: <https://www.tethys.cat/sites/default/files/pdf/articles/8tethys-08-eng.pdf>
- [3] D. Prats-Rico, “La reutilización de aguas depuradas regeneradas a escala mundial: Análisis y prospectivas.” [Online]. Available: <https://revistaselectronicas.ujaen.es/index.php/atma/article/view/3292>
- [4] “Regeneració.” [Online]. Available: <https://aca.gencat.cat/ca/laigua/gestio-del-cicle-de-laigua/regeneracio/>
- [5] N. C. Chulluncuy-Camacho, “Tratamiento de agua para consumo humano.” [Online]. Available: https://revistas.ulima.edu.pe/index.php/Ingenieria_industrial/article/view/232
- [6] “History.” [Online]. Available: <https://www.ocwd.com/about/history/>
- [7] U.c, “Faran una planta pilot a roses per a la recàrrega d'aquífers - 09 des 2021,” Dec 2021. [Online]. Available: <https://www.elpuntavui.cat/societat/article/12-infraestructures/2067485-faran-una-planta-pilot-a-roses-per-a-la-recarrega-d-aqueifers.html>
- [8] “Blockchain4sdg,” Dec 2021. [Online]. Available: <https://www.cbc.cat/blockchain4sdg/>
- [9] “Pàgina d'inici - consorci d'aigües costa brava girona,” Jan 2022. [Online]. Available: <https://www.cacbgi.cat/es/>
- [10] “Universitat de girona.” [Online]. Available: <https://www.udg.edu/ca/>
- [11] “Inicio.” [Online]. Available: <https://aca.gencat.cat/es/inici/index.html>
- [12] “Noticias noticias.” [Online]. Available: <https://www.upf.edu/es/>
- [13] “Objetivos de desarrollo,” Oct 2019. [Online]. Available: <https://onu.org.gt/objetivos-de-desarrollo/>
- [14] “Situación actual de la vigilancia y control de vertidos.” [Online]. Available: <https://bit.ly/3MvxYsG>
- [15] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [16] [Online]. Available: <https://www.uria.com/documentos/publicaciones/5799/documento/art02.pdf?id=7875>

- [17] “White paper – distributed ledger technologies (dlt) and blockchain.” [Online]. Available: <https://www.cssf.lu/en/2022/01/white-paper-distributed-ledger-technologies-dlt-blockchain/>
- [18] L. W. Cong, “Nber working paper series.” [Online]. Available: https://www.nber.org/system/files/working_papers/w24399/w24399.pdf
- [19] Livia, “Algoritmos de consenso: La raíz de la tecnología blockchain,” Nov 2018. [Online]. Available: <https://101blockchains.com/es/algoritmos-de-consenso-blockchain/>
- [20] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, and A. Kerrouche, “Implementation of blockchain consensus algorithm on embedded architecture,” Apr 2021. [Online]. Available: <https://www.hindawi.com/journals/scn/2021/9918697/>
- [21] “Proof-of-authority consensus.” [Online]. Available: <https://apla.readthedocs.io/en/latest/concepts/consensus.html>
- [22] “On security analysis of proof-of-elapsed-time.” [Online]. Available: <https://www.scribd.com/document/444049756/On-Security-Analysis-of-Proof-of-Elapsed-Time>
- [23] [Online]. Available: <https://www.bitcoinpos.net/WhitePaperBPS.pdf>
- [24] “Validator requirements: Solana docs.” [Online]. Available: <https://docs.solana.com/running-validator/validator-reqs>
- [25] “Infraestructura escalable de blockchain: Más de mil millones de transacciones y contando: Solana: Build crypto apps that scale.” [Online]. Available: <https://solana.com/es>
- [26] “Proof of history,” Feb 2022. [Online]. Available: https://es.wikipedia.org/wiki/Proof_of_History
- [27] J. Vicent, “Proof of history: ¿qué es y cómo funciona?” Dec 2021. [Online]. Available: <https://cryptorobin.es/proof-of-history-que-es-y-como-funciona/>
- [28] “Description.” [Online]. Available: <https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-history>
- [29] “Proof of history,” Feb 2022. [Online]. Available: https://es.wikipedia.org/wiki/Proof_of_History
- [30] “Protocolos de consenso.” [Online]. Available: <https://bfa.ar/blockchain/protocolos-de-consenso>
- [31] [Online]. Available: <https://repository.psau.edu.sa/jspui/retrieve/4eeae047-64d2-4d01-938c-82059aa39e0b/PoSVsPoW.pdf>

- [32] S. Jiang, Y. Li, Q. Lu, Y. Hong, D. Guan, Y. Xiong, and S. Wang, “Policy assessments for the carbon emission flows and sustainability of bitcoin blockchain operation in china,” Apr 2021. [Online]. Available: <https://www.nature.com/articles/s41467-021-22256-3>
- [33] B. Linea, “La gráfica que muestra la evolución del precio del bitcóin desde 2013 a la fecha,” Nov 2021. [Online]. Available: <https://www.bloomberglinea.com/2021/07/29/la-grafica-que-muestra-la-evolucion-del-precio-del-bitcoin-desde-2013-a-la-fecha/>
- [34] “Algorant.” [Online]. Available: <https://www.algorand.com/es/resources/blog/algorands-leadership-in-blockchain-sustainability>
- [35] “Las 5 blockchains de 2021: Solana, cardano, terra, avalanche y polygon,” Dec 2021. [Online]. Available: <https://observatorioblockchain.com/blockchain/las-5-blockchains-de-2021-solana-cardano-terra-avalanche-y-polygon/>
- [36] [Online]. Available: <https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/24600/1/CP20.pdf>
- [37] [Online]. Available: <https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/20646/1/tg-mereles-ortellado.pdf>
- [38] “Blockchain network.” [Online]. Available: <https://hyperledger-fabric.readthedocs.io/es/latest/network/network.html>
- [39] “Hyperledger fabric,” Jun 2020. [Online]. Available: <https://www.hyperledger.org/use/fabric>
- [40] Pacoard, “Hyperledger blockchain + react that lets users manage smart home sensors and actuators.” [Online]. Available: https://github.com/pacoard/TFM_2017-18
- [41] E. Thieuleux, “Blockchain in supply chain : Applications and examples,” Oct 2021. [Online]. Available: <https://abcsupplychain.com/blockchain-supply-chain-examples/>
- [42] D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm.” [Online]. Available: <https://raft.github.io/raft.pdf>
- [43] “The raft consensus algorithm.” [Online]. Available: <https://raft.github.io/>
- [44] [Online]. Available: http://www.negociosdeseguridad.com.ar/articulos/030/RNDS_066.pdf
- [45] “¿qué es walmart? ¿a qué se dedica la empresa de walmart y cuál es su misión y visión? - objetivos walmart,” Mar 2021. [Online]. Available: <https://miracomosehace.com/que-es-walmart-dedica-empresa-walmart-mision-vision-objetivos-walmart/>

- [46] "Hyperledger fabric," Jun 2020. [Online]. Available: <https://www.hyperledger.org/use/fabric>
- [47] "Ibm anuncia proyecto de blockchain para la nube híbrida." [Online]. Available: <https://diarioti.com/ibm-anuncia-proyecto-de-blockchain-para-la-nube-hibrida/114688>
- [48] "Openvino project documentation." [Online]. Available: <https://docs.openvino.ai/latest/index.html>
- [49] Openvino, "Openvino/mtb18-token-crowdsale-dapp." [Online]. Available: <https://github.com/OpenVino/MTB18-token-crowdsale-dapp>
- [50] "The blockchain comes to agriculture," Oct 2018. [Online]. Available: <https://modernfarmer.com/2018/02/blockchain-comes-agriculture/>
- [51] "Blockchain technology in current agricultural systems: From techniques to applications." [Online]. Available: <https://ieeexplore.ieee.org/document/9159588>
- [52] Beefdaddy, Beefdaddy, K. DeCastro, and K. DeCastro, "Beefchain project documentation," Aug 2019. [Online]. Available: <https://beefchain.com/>
- [53] S. Bhatti, "White paper "blockchain application in beef supply chain"," Feb 2019. [Online]. Available: <https://www.linkedin.com/pulse/white-paper-blockchain-application-beef-supply-chain-sarosh-bhatti>