Blockchain per l'educació

Joan Manel Arcas Sanz

Resum— La tecnologia *Blockchain* o de cadena de blocs va sorgir com a suport de la xarxa de monedes virtuals Bitcoin, però amb la recent aparició dels Smart Contracts existeix la possibilitat de crear infinitud d'aplicacions que funcionin de manera distribuïda i sense la necessitat d'entitats intermediàries. En aquest article es presenta una introducció a la tecnologia Blockchain, des dels seus inicis amb Bitcoin fins a l'actualitat amb la utilització dels *Smart Contracts*. Posteriorment es comparen algunes de les plataformes Blockchain més utilitzades actualment com són Ethereum o Hyperledger, per a finalment mostrar una solució en l'àmbit de l'educació: emmagatzematge d'expedients acadèmics utilitzant la tecnologia *Blockchain* i els *Smart Contracts*.

Paraules clau— Cadena de blocs, contracte intel·ligent, Ethereum, Quorum, distribuït, consens, educació, expedients acadèmics.

Abstract— Blockchain technology emerged as a support for the Bitcoin cryptocurrency network, but with the recent appearance of Smart Contracts there is the possibility to create infinity of applications that work in a distributed way and without the need for intermediate entities. This paper presents an introduction to the Blockchain technology, from its beginnings with Bitcoin to the present day with the use of Smart Contracts. Subsequently, some of the most commonly used Blockchain platforms are compared, such as Ethereum or Hyperledger, to finally show a solution in the field of education: storage of academic records using Blockchain technology and Smart Contracts.

Índex Terms— Blockchain, Smart Contract, Ethereum, Quorum, distributed, consensus, education, academic records.

1. Introducció

L'ANY 2009, amb l'aparició dels Bitcoins, va néixer també una nova tecnologia anomenada Blockchain. Una Blockchain és com un gran llibre de comptabilitat distribuït on s'apunten totes les transaccions de la xarxa, de manera que aquestes queden ordenades en el temps sense poder ser modificades posteriorment. Una transacció en aquest cas no és res més que un intercanvi d'informació entre dos nodes de la xarxa.

Tot i que inicialment va ser creada i utilitzada majoritàriament com a suport de xarxes de cryptomonedes com la de Bitcoin, la recent incorporació dels Smart Contracts a les xarxes Blockchain ha fet que cada dia més persones i empreses estiguin interessades en incloure aquesta tecnologia com a base de les seves aplicacions.

Aquests Smart Contracts o contractes intel·ligents són simplement codi que es pot executar a la Blockchain, permetent fer aplicacions tan diverses com votació electrònica, emmagatzematge distribuït, mètodes de finançament o controls d'identitat, entre de molts altres.

En aquest article es mostra una aplicació de Blockchain més enllà de les cryptomonedes utilitzant els Smart Contrats en l'àmbit de l'educació: un sistema per a les universitats que permet l'emmagatzematge d'expedients acadèmics de manera distribuïda.

1.1. Objectius

L'objectiu d'aquest projecte és, primer de tot, estudiar i investigar la tecnologia Blockchain, les seves característiques principals, els tipus, els protocols que utilitza i la més recent incorporació dels Smart Contracts per la creació d'aplicacions. En segon lloc, provar algunes de les plataformes disponibles actualment per la creació i utilització de Blockchains. D'aquestes plataformes es compararan algunes de les seves característiques i, segons una sèrie de requeriments, es triarà una per a finalment presentar una implementació d'una solució Blockchain per a l'emmagatzematge d'expedients acadèmics.

1.2. Motivació

La motivació a l'hora de dur a terme aquest projecte ha estat poder arribar a entendre com funciona la tecnologia Blockchain, quin és l'estat actual d'aquesta i a quina velocitat avança, poder provar diferents de les plataformes disponibles que existeixen i finalment implementar un sistema real funcional.

És usual escoltar la paraula Blockchain normalment seguida de "Bitcoin", però la veritat es que aquesta tecnologia té infinitud d'altres aplicacions, i donat que és una tecnologia relativament jove, cada cop s'afegeixen més casos d'us on Blockchain és una millora respecte a sistemes més tradicionals.

- *E-mail de contacte: drumsjuanma@gmail.com*
- *Menció realitzada: Tecnologies de la Informació.*
- *Treball tutoritzat per: Jordi Duran Cals (DEIC)*
- *Curs 2016/17*

2. METODOLOGIA

La metodologia seguida per la realització del projecte ha estat una metodologia àgil Scrum. Donat que es partia d'una base de coneixement sobre la matèria molt escassa, era difícil planificar amb exactitud les diferents etapes i tasques a realitzar. La metodologia Scrum permet una planificació distribuïda en diferents intervals (o Sprints) de llargada variable, facilitant així projectes on tant els requeriments com els objectius a curt termini són variables, com era el cas.

Així doncs, finalment el projecte s'ha dividit en quatre Sprints:

- Estudi i investigació de la tecnologia Blockchain. Veure i entendre l'estat de l'art de la tecnologia, característiques, protocols, arquitectura, etc.
- Estudi i prova de diferents plataformes Blockchain. Primer contacte amb la tecnologia i proves dels primers Smart Contracts.
- Tria d'una de les plataformes per la realització de l'aplicació d'emmagatzematge d'expedients i aprenentatge del llenguatge de programació d'aquesta. Posada en marxa, configuració de la Blockchain i aprenentatge d'aquesta.
- Desenvolupament de l'aplicació. Codificació del Smart Contract i de la interfície.

3. ESTAT DE L'ART

3.1. Història

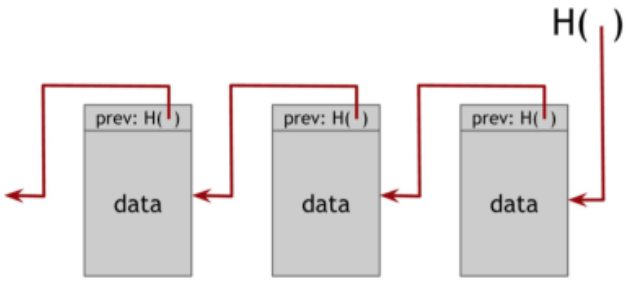
L'any 2008 un usuari d'internet amb el sobrenom de Satoshi Nakamoto va publicar un article a on descrivia el protocol Bitcoin. Mesos més tard, a principis de gener del 2009, la xarxa P2P de Bitcoin va entrar en funcionament com a experiment de moneda virtual. [1]

Més enllà de la pròpia moneda virtual, es va descobrir la capa o la tecnologia sota la qual funcionava la xarxa: les Blockchains o cadenes de blocs. Aquesta tecnologia pot ser separada de la xarxa Bitcoin per a utilitzar-se en multitud d'àmbits diferents.

Al llarg dels últims anys han sorgit altres xarxes i aplicacions Blockchain més enllà de l'ús de cryptomonedes. Avui en dia s'estima que la majoria d'institucions financeres importants del món estan investigant sobre aquesta tecnologia, i durant aquest 2017 aproximadament un 15% dels bancs ja l'utilitzin en les seves transaccions. [2]

3.2. Definició i característiques

Una Blockchain o cadena de blocs és una base de dades distribuïda en la que una sèrie de nodes hi afegeixen transaccions. Aquestes transaccions s'agrupen en blocs, i cada cop que s'afegeix un nou bloc aquest queda enllaçat amb l'anterior amb un punter hash.



Il·lustració 1- Estructura de la cadena de blocs

La tecnologia Blockchain té una sèrie de característiques principals [3]:

- **Descentralitzada**: No existeix la necessitat d'una entitat central de confiança, sinó que els nodes es comuniquen *peer-too-peer* (node a node).
- **Distribuïda**: Tots els nodes de la xarxa posseeixen una còpia exacta de la informació emmagatzemada en tot moment.
- **Immutable**: Cada bloc de la Blockchain apunta al bloc anterior amb un apuntador hash, pel que si un dels blocs és modificat, els apuntadors no coincidiran.
- **Anònima**: Els nodes s'identifiquen mitjançant únicament la seva clau pública, pel que la identitat a la xarxa no està relacionada directament amb cap entitat física.
- **Consens**: Cada transacció enviada ha de ser verificada per la resta de nodes de la xarxa abans de ser emmagatzemada a la Blockchain.

3.3. Tipus de Blockchain

Existeixen vàries maneres d'organitzar els diferents tipus de Blockchain. Una manera simple pot ser diferenciar les públiques, on qualsevol persona es pot unir, i les privades, on només un grup de persones determinat pot fer-ho. Tot i així, amb els diferents avanços que s'han produït en la tecnologia, una manera més acurada seria diferenciar entre els permisos d'escriptura i de lectura per separat [4].

Control de lectura:

- ***Fully Open***: Tothom pot veure i llegir el contingut de la Blockchain.
- ***Partially transparent***: Tothom pot veure el contingut de la Blockchain, però aquest es troba encriptat.
- ***Closet***: Només un grup determinat d'entitats pot veure el contingut de la Blockchain.

Control d'escriptura:

- ***Permissioned***: Tothom pot realitzar transaccions i, si la plataforma ho permet, utilitzar Smart Contracts.
- ***Permissionles***: Només un grup d'entitats pot fer transaccions i utilitzar Smart Contracts.

3.4 Protocol de Consens

Un protocol de consens és aquell que serveix per a posar d'acord una sèrie de nodes d'una xarxa distribuïda en algun tema en concret. En aquest cas, el protocol de consens serveix perquè tots els nodes de la xarxa verifiquin que les transaccions produïdes són vàlides i es generin els nous blocs corresponents.

Alguns d'aquests protocols també serveixen per premiar a aquells nodes que estiguin realitzant aquestes tasques a canvi de, per exemple, cryptomonedes de la xarxa Blockchain corresponent. Aquesta recompensa és necessària normalment quan la xarxa és pública, i es coneix amb el nom de "mineria". En el cas de xarxes privades no és necessari recompensar als usuaris, ja que se suposa que existeix una motivació de mantenir la Blockchain verídica i estable. A més a més, com en aquestes xarxes privades els usuaris que accedeixen són coneguts, no fan falta protocols tant segurs, ja que existeix una capa externa de seguretat.

A continuació es detallen alguns dels protocols de consens més utilitzats [5]:

3.4.1. Prova de Treball (PoW)

La probabilitat de minar un bloc i per tant obtenir la recompensa corresponent depèn del "treball" fet pel node. Aquests treballs solen ser càlculs matemàtics difícilment executables però fàcilment verificables. Amb aquest protocol evitem que un possible atacant pugui crear més d'un node en una mateixa màquina per realitzar un atac sense cap cost.

3.4.2.Prova de Participació (PoS)

Es basa en la suposició que el nombre de cryptomonedes que un node posseeix equival a l'interès que aquest té per verificar i corregir el bon funcionament de la xarxa. Es per això que com més cryptomonedes es posseeix, més probabilitats de minar un bloc hi ha, i per tant, d'aconseguir la recompensa corresponent.

3.4.3.Practical Byzantine Fault Tolerance (PBFT)

Aquest protocol soluciona el problema del *Byzantine Fault Tolerance* [6] o dels generals bizantins, en el qual s'exposa el cas en què un conjunt de sistemes informàtics han de posar-se d'acord en un tema concret, però existeix la possibilitat que algun dels sistemes no sigui fiable.

En aquest cas, aquest protocol està dissenyat per a xarxes Blockchain privades, on no hi hagi cap recompensa per la mineria de blocs més enllà de mantenir la xarxa segura. En l'algorisme s'especifica un nombre màxim de nodes *Bizantins* f (nodes no fiables) on f=(N-1)/3, i N és el nombre de nodes validadors de la xarxa. [7]

3.4.4. Vulnerabilitats

Una de les vulnerabilitats que presenta Blockchain és l'anomenat "atac del 51%". Si es modifica un bloc entremig del Blockchain, els enllaços hash no coincidiran i s'hauran de tornar a crear. Per fer això, els blocs posteriors han de ser re-minats per a incloure-hi els nous hashs que s'han de tornar a calcular. En el cas llavors que un atacant volgués modificar un valor pel seu benefici i intentés reconstruir la cadena modificada calculant els hashs, hauria de tenir el control de com a mínim el 51% del recurs que utilitzi el protocol de consens, per tal que pugui reconstruir la cadena a una velocitat superior a la que aquesta es genera [8].

Aquesta vulnerabilitat afecta principalment a les plataformes que utilitzen prova de treball o prova de participació, però tot i així és una situació difícilment realitzable, donat que significaria tenir el 51% de la potència computacional o el 51% de les cryptomonedes de tota la xarxa.

3.5. Smart Contracts

Un Smart Contract o contracte intel·ligent és un programa informàtic que facilita, assegura, fa complir i executa acords registrats entre persones i organitzacions. Un Smart Contract té validesa de per sí, sense dependre d'una tercera autoritat de confiança donat la seva naturalesa: un codi visible per tothom que no es pot modificar a l'existir sobre la tecnologia de Blockchain [9].

En definitiva, un Smart Contract no es res més que codi que s'executa en la Blockchain, i que per tant té totes les característiques d'aquesta tecnologia. El llenguatge de programació en el que s'escriu i la quantitat de diferents funcionalitats per les quals es poden utilitzar depenen de la plataforma a la qual s'utilitzin.

Els Smarts Contracts són actualment un dels conceptes més atractius i utilitzats juntament amb les Blockchains, ja que permeten afegir funcionalitats molt diverses a aquesta tecnologia. Entre d'altres coses, els Smart Contracts poden rebre i enviar cryptomonedes, reaccionar a events o executar operacions matemàtiques.

Actualment s'utilitzen per aplicacions tan diverses com vot electrònic, plataformes de *crowdfunding*, emmagatzematge distribuït, traçabilitat de processos, etc.

3.6. Avantatges i Desavantatges

La tecnologia Blockchain proporciona una sèrie d'avantatges davant d'altres actualment més utilitzades. A continuació es detallen alguns d'aquests avantatges i desavantatges [10]:

3.6.1. Avantatges

- **Seguretat**: L'autenticació mitjançant firmes digitals permet assegurar la identitat dels nodes. A més a més, les dades romanen immutables un cop emmagatzemades en la Blockchain i agrupades en blocs enllaçats entre si, el que permet mantenir la traçabilitat de la informació.
- **Robustesa**: Al ser una tecnologia descentralitzada, tota la informació està replicada a tots els nodes de la xarxa. Això fa que la pèrdua o la corrupció de les dades sigui pràcticament impossible de produir-se.
- **Transparència**: Tota la informació emmagatzemada a la Blockchain és visible per a tots els nodes de la xarxa. A més, cada transacció registrada per un node

ha de ser prèviament validada per la resta.
- **No necessitat d'intermediaris:** La comunicació es produeix directament entre nodes de la xarxa sense la necessitat d'una entitat central de confiança. Això, a més a més, abarateix el cost donat que no calen intermediaris.

3.6.2. Desavantatges

- **Delay**: Existeix un cert temps de retard entre que s'emet una transacció fins que aquesta es valida i s'inclou en un nou bloc. Aquest temps variarà depenen de la plataforma i la configuració utilitzada.
- **Escabilitat**: La Blockchain emmagatzema totes les transaccions de la xarxa i tots els nodes miners requereixen descarregar-se la sencera. Això fa que la quantitat d'informació emmagatzemada sigui elevada i en continu creixement.
- **Privacitat:** El fet que tota la informació sigui visible per a tots els nodes de la xarxa fa que hi hagi una manca total de privacitat en les dades. En quant als nodes o usuaris, tot i que només s'identifiquen per la seva clau pública, seguint el rastre de les diferents transaccions és relativament fàcil descobrir la identitat d'aquests.

4. Emmagatzematge d'expedients acadèmics

4.1. Problema

Cada universitat és responsables d'emmagatzemar i gestionar els expedients acadèmics dels seus alumnes. Aquesta tasca és relativament senzilla fins al moment en què un estudiant requereix canviar d'universitat, temporalment o indefinidament.

Donat que cada universitat pot utilitzar un sistema diferent per a gestionar les seves dades, el procés de transferència d'un expedient pot generar problemes, a més del simple fet que la informació queda distribuïda entre els diferents centres.

4.2. Solució proposada

Una possible solució a aquest problema és la utilització d'una Blockchain i d'Smart Contracts per a l'emmagatzematge dels expedients acadèmics. Amb aquesta tecnologia, un mateix estudiant podria tenir unificats els diferents expedients acadèmics dels diferents centres als que ha estat en una mateixa plataforma, i les universitats podrien comunicar-se entre si més fàcilment i d'una manera estandarditzada. A més a més de tot això, la informació emmagatzemada estaria distribuïda, pel que s'evitarien els problemes de possibles pèrdues de dades.

4.3. Requisits

L'aplicació proposada es basa principalment en una Blockchain privada utilitzada inicialment només per les universitats, amb la qual a través dels Smart Contract poder emmagatzemar els expedients acadèmics dels alumnes.

Per dur a terme aquesta funcionalitat, a banda dels requisits específics que tingui l'aplicació, hi ha una sèrie de característiques les quals ha de complir la plataforma Blockchain utilitzada:

- **Permissivitat**: els expedients acadèmics són, òbviament, uns documents sensibles que no tenen perquè ser visibles per tothom. És per això que cal que la Blockchain tingui un control d'accés perquè només una sèrie d'usuaris o entitats tinguin accés a la informació (en aquest cas les universitats).

- **Smart Contracts**: Com ja s'ha mencionat anteriorment, el funcionament de l'aplicació es basa en Smart Contracts, els quals permeten gestionar la informació emmagatzemada i mantenen un format estàndard de les dades. Per tant és necessari que la plataforma permeti la utilització d'aquests.

- **Protocol de Consens**: En plataformes obertes i públiques com per exemple Bitcoin, el protocol de consens, a més a més, serveix per protegir a la xarxa de possibles atacs.

  En una xarxa privada on els nodes són coneguts (existeix un control d'accés) no és necessari un protocol de consens així, ja que es considera que tots els nodes són confiables.

5. Plataformes Blockchain

Prèviament al desenvolupament de l'aplicació, s'han provat algunes de les plataformes Blockchain disponibles avui en dia per a familiaritzar-se i per a poder escollir-ne la més adient als requisits anteriorment mencionats.

5.1. Ethereum

Ethereum és una plataforma descentralitzada creada l'any 2014 que utilitza la tecnologia Blockchain i permet la creació de Smart Contracts. A l'igual que Bitcoin, Ethereum compta amb una cryptomoneda pròpia anomenada Ether. Aquesta moneda es genera d'una manera similar als Bitcoins, a través de mineria amb *Proof of Work*, però pot ser utilitzada per la utilització de Smart Contracts.

Aquests Smart Contracts es desenvolupen en llenguatges d'alt nivell (LLL, Serpent o Solidity, el més utilitzat). Aquest codi és necessari compilar-lo i passar-lo a EVM bytecode (Ethereum Virtual Machine bytecode) i finalment desplegar-ho a la Blockchain.

Ethereum, tot i ser una plataforma pública, permet la implementació de xarxes privades gracies a la fàcil configuració del seu codi. Això ha donat lloc a què multitud de desenvolupadors utilitzin Ethereum per la implementació de llibreries i aplicacions, així com modificacions i millores d'aquesta. [11]

5.2. Hyperledger

Hyperledger és una plataforma de Blockchain de codi obert que pretén ser la base tecnològica d'empreses amb la utilització de Blockchain. La idea principal és la de subministrar estàndards i protocols per donar suport a la utilització d'aquesta tecnologia, utilitzant un protocol de consens propi i diferents mòduls amb funcionalitats tan diverses com l'emmagatzematge o el control d'accés.

A diferencia d'altres Blockchains, Hyperledger està enfocada únicament a xarxes privades per empreses, pel que no hi ha una implementació pública i no té una cryptomoneda pròpia. [12]

5.3. Eris

Eris és una plataforma per a desenvolupadors implementada per la companyia Monax centrada en la creació d'aplicacions sobre les Blockchains en àmbits empresarials. Aquesta plataforma ofereix kits de desenvolupament de software (SDKs) per la ràpida creació d'aplicacions, de manera modular i senzilla.

Una de les característiques principals d'Eris, és que no funciona sota cap Blockchain específica. De fet, podem considerar-lo com una implementació d'un node Blockchain el qual és capaç d'interactuar amb diferents plataformes simultàniament. Tot i que inicialment va ser creada com un *fork* d'Ethereum (implementant l'Ethereum Virtual Machine), poc a poc són més les plataformes les quals poden funcionar conjuntament amb Eris.

5.4. Quorum

Quorum [13] és un projecte desenvolupat per JP Morgan, el banc més important d'Estats Units. Està basat en la Blockchain d'Ethereum, amb una implementació d'aquesta xarxa de manera privada.

Les principals diferencies entre Quorum i Ethereum són que Quorum no utilitza moneda pròpia (ja que està enfocat a xarxes privades), utilitza un protocol de consens propi i afegeix una capa de privacitat extra.

5.5. zCash

Zcash [14]és una cryptomoneda desenvolupada amb el protocol Zerocoin [15] que ofereix una capa de privacitat, mantenint en l'anonimat el remitent, el receptor i el contingut (nombre de cryptomonedes en aquest cas), mantenint la credibilitat i la consistència de la Blockchain.
Això s'aconsegueix utilitzant el protocol zero-knowledge proof [16] o la seva variant non-interactives zero-knowledge proof [17], els quals permeten als nodes validadors validar les transaccions sense la necessitat de tenir informació sobre el contingut d'aquestes. Aquest mètode, tot i disminuir el rendiment i el nombre de transaccions per segon que pot suportar la xarxa, permet mantenir l'essència de les Blockchains mantenint en privat als usuaris i les seves accions, alhora que es verifica la credibilitat d'aquestes.

En definitiva, zCash aplica una millora donant una capa de privacitat a les Blockchains. Tal com es cita a l'article oficial de zCash, *'Bitcoin is HTTP for Money; zCash is HTTPS'*. [18]

5.5.1 ZoE (zCash on Ethereum)

ZoE és el projecte de la incorporació del protocol utilitzat a zCash *zk-SNARKSs* per al desenvolupament d'una xarxa de cryptomonedes completament anònima a Ethereum. Això permet no només poder crear un sistema de cryptomonedes secret, sinó aplicar aquest anonimat als Smart Contracts, permetent als usuaris utilitzar i cridar les diferents funcionalitats dels Smart Contracts de manera anònima i privada.

Per desgracia, actualment el projecte encara segueix en desenvolupament, i s'espera que zCash afegeixi el seu protocol no només a Ethereum, sinó a altres plataformes com hyperledger.

5.6 Comparació

A continuació es mostra una taula on es comparen les característiques mencionades anteriorment, necessàries per la implementació de l'aplicació, juntament amb altres com per exemple la disposició d'una bona documentació, o la dificultat d'implementació que suposen:

	Ethereum	Hyperledger	Eris	Quorum	zCash
Smart-Contracts	Si	Si	Si	Si	No
Protocol de consens	PoW	BFTA	BFTA	Voting	PoW
Permisivitat	Private	Private	Private	Private	Public
Learning curve	Easy	Hard	Medium	Easy	Hard
Code-complete	Si	Si	Si	Si	Si
Bona documentació	Si	No	Si	Si	No
Funcionalitats adicionals	No	Si	Si	Si	Si

Taula 1 Comparació de plataformes Blockchain

Aquesta taula ha estat realitzada després d'haver analitzat i provat cadascuna de les plataformes que hi apareixen (Ethereum, Hyperledger, Eris, zCash i Quorum). En el següent apartat es detalla el perquè de la tria de Quorum com a plataforma Blockchain pel desenvolupament de l'aplicació d'emmagatzematge.

6. QUORUM

Quorum és una plataforma que es basa en Ethereum, però que hi afegeix una capa extra amb una sèrie de funcionalitats addicionals.

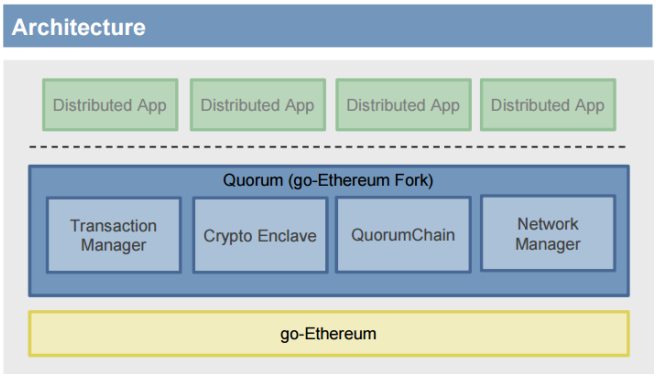
Primer de tot i partint dels requisits mencionats anteriorment, Quorum és una plataforma permissiva (té un control d'accés que controla els nodes que s'hi poden afegir a la xarxa), permet la utilització de Smart Contracts (utilitza la Ethereum Virtual Machine) i utilitza un protocol de consens basat en votació molt simple, on un o més nodes són els encarregats de crear els blocs i la resta simplement verifica que siguin correctes.

A més a més d'això, la tria de Quorum és deguda principalment a una sèrie de característiques addicionals que incorpora [19]:

- El protocol de consens està codificat en un Smart Contract en la mateixa Blockchain. Això permet que en un futur es pugui modificar aquest mètode de consens d'una manera molt fàcil en cas que es volgués. A més a més, aquest protocol no consumeix pràcticament recursos, a diferencia de la prova de treball utilitzada a Ethereum.

- Incorpora un sistema de transaccions que permet la comunicació entre dos o més nodes de la xarxa de manera privada. Un altre cop mes, quan ens referim a transaccions significa també Smart Contracts o qualsevol informació emmagatzemada a la Blockchain. Això significa que cada node de la xarxa comparteix un estat públic amb tota la resta de nodes, però també emmagatzema un estat privat, el qual variarà segons aquestes transaccions privades.

Aquestes funcionalitats juntament amb la base de Quorum estan desenvolupades en quatre mòduls afegits a Ethereum. Això permet aprofitar els avantatges d'Ethereum, afegint de manera modular altres funcionalitats, i garanteix que cada cop que Ethereum tingui una actualització de versió i afegeixi noves funcionalitats, Quorum podrà actualitzar-se de manera senzilla per tal que no es quedi obsolet.



Il·lustració 2- Arquitectura de Quorum

Aquests quatre mòduls són els següents:

- **Transaction Manager**: encarregat del funcionament de les transaccions privades.
- **Crypto Enclave**: encarregat de la gestió de claus per a les transaccions privades entre parelles o grups de nodes.
- **QuorumChain**: Smart Contract on està codificat el funcionament del protocol de consens de *Voting*.
- **Network Manager**: encarregat del control d'accés a la xarxa Blockchain.

Tot i que aquestes funcionalitats addicionals no seran necessàries inicialment pel desenvolupament de l'aplicació, sí que permeten moltes altres funcionalitats per a possibles implementacions futures (sobretot en termes de millorar la privacitat del sistema).

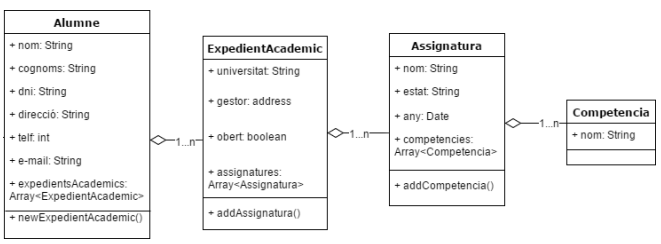
7. RESULTATS

El resultat final de la realització d'aquest projecte és un sistema que connecta diferents universitats i permet emmagatzemar tota la informació acadèmica dels alumnes de manera distribuïda. Aquesta informació només pot ser modificada o afegida pel node (universitat) que hagi creat l'expedient, però és visible per la resta de nodes. En el cas que alguna altra entitat necessiti poder escriure en la fitxa acadèmica d'un alumne de la qual no en té permís, la universitat propietària és l'encarregada de concedir aquests permisos.

El sistema està compost per 3 elements:

- Una Blockchain muntada sobre la plataforma de Quorum. Aquesta Blockchain té un control d'accés pel qual només una sèrie de nodes pre-configurats poden connectar-s'hi i permet la utilització de Smart Contracts.

- Un Smart Contract codificat en el llenguatge de Solidity, el qual permet emmagatzemar totes les dades personals i acadèmiques dels alumnes, i permet controlar el permís d'escriptura en aquests expedients. La informació està organitzada tal com es mostra a continuació, de tal manera que un Smart Contract emmagatzema la fitxa acadèmica d'un alumne, el qual té n Expedients acadèmics, cadascun dels quals està format per n Assignatures, les quals tenen assignades una sèrie de competències.



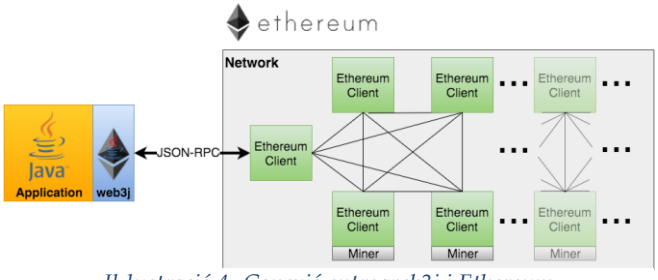
Il·lustració 3- Organització de la información emmagatzemada

Aquest Smart Contract permet organitzar la informació d'una manera ordenada i estandarditzada, i a més a més permet controlar quin node de la Blockchain té el poder de modificar o afegir informació dins de l'expedient acadèmic d'un alumne. Aquest control d'escriptura s'aconsegueix emmagatzemant, juntament amb cada expedient acadèmic, l'adreça de la Blockchain del node que l'ha creat, i només permetent al propietari d'aquesta adreça cridar les funcions corresponents.

Cal mencionar que el conjunt de dades emmagatzemades és només una mostra triada per a realitzar una demostració i no equival al conjunt total que seria necessari guardar.

- Una interfície gràfica programada en el llenguatge Java. Per a poder comunicar l'aplicació amb la Blockchain, s'ha utilitzat la llibreria Web3j, una llibreria que permet la comunicació entre la Blockchain d'Ethereum i una aplicació escrita en Java. D'aquesta manera podem crear aplicacions que enviïn transaccions, creïn Smart Contracts o llegeixin de la Blockchain d'una manera senzilla a través de les funcions que ens ofereix la llibreria.

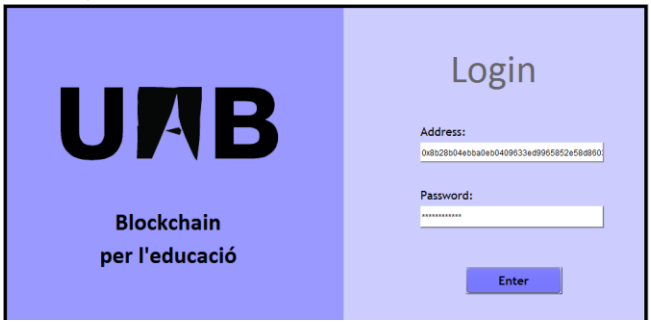
  Malgrat que web3j funciona per Ethereum, existeix una extensió per a Quorum, web3j-quorum. [20]



Il·lustració 4- Conexió entre web3j i Ethereum

Tot i que inicialment no estava previst el desenvolupament d'una interfície gràfica, donat que la planificació va ser millor de l'esperat, es va decidir fer una senzilla interfície per a realitzar la demostració i per a facilitar a l'usuari la introducció i la visualització de les dades.

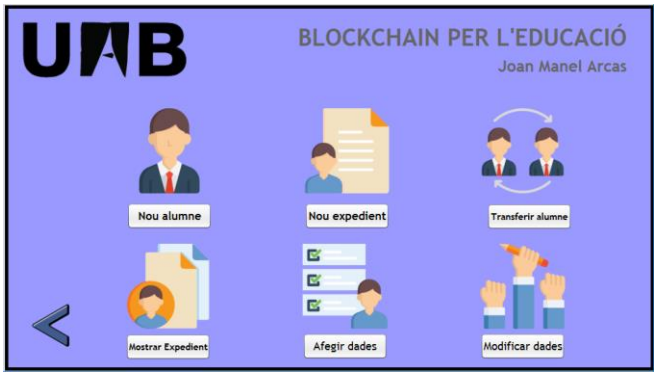
L'aplicació, doncs, inicialment demana uns credencials (l'adreça pública i la contrasenya), amb els quals es connecta a un node Blockchain de Qurum, el qual prèviament s'ha hagut de posar en marxa.



Il·lustració 5- Interfície: Login

A partir d'aquí, l'aplicació obre un menú amb les diferents funcionalitats que permet fer:

- Crear una nova fitxa d'alumne. Equival a desplegar un nou Smart Contract amb les dades personals d'un alumne a la Blockchain.
- Crear un nou expedient acadèmic en un alumne.
- Transferir un alumne a una altra universitat. Aquesta opció serveix per donar permís d'escriptura a una altra universitat per a crear un expedient en un alumne propi (permís per a crear un nou expedient, no per a modificar l'actual).
- Mostrar expedients i assignatures d'un alumne.
- Afegir noves assignatures a l'expedient d'un alumne.
- Modificar dades (personals, d'expedient o d'assignatures).



Il·lustració 5- Menú principal

8. TREBALLS FUTURS

El treball realitzat estableix una bona base d'un sistema no només per a emmagatzemar expedients acadèmics, sinó també per a automatitzar i estandarditzar molts processos que avui en dia es realitzen manualment a les universitats.

Un d'aquests processos podria ser el de la convalidació d'assignatures de diferents universitats i/o graus. A través d'un llistat de competències de cada assignatura que formessin una ontologia docent, es podria codificar un Smart Contract que automàticament comparés les competències i pogués determinar quines assignatures poden ser convalidades i quines no.

Una altra millora també podria ser afegir el rol de l'estudiant dins de la Blockchain, de manera que els estudiants poguessin veure els seus expedients sencers directament, fer sol·licituds a diferents universitats des de la mateixa plataforma, etc.

A més a més existeixen una sèrie d'aspectes, no de la funcionalitat en si, sinó de la tecnologia Blockchain, que encara han d'evolucionar i calen millorar. Un d'aquests és el tema de la privacitat. Com és evident, les dades acadèmiques dels alumnes és informació confidencial que no totes les universitats haurien de poder veure. Una possible millora temporal seria encriptar aquestes dades abans d'introduir-les a la Blockchain, i desenvolupar algun sistema

de transmissió de claus tal que les transferències d'expedients puguin ser efectives. D'altra banda, existeixen protocols i mètodes d'encriptació com el zero-knowledge proof o l'encriptació homomòrfica, els quals permeten obtenir privacitat en les dades alhora que es poden fer certes operacions i comprovacions amb elles. Aquestes tècniques, a dies d'ara, estan sent desenvolupades i acoblades a diferents plataformes Blockchain.

9. Conclusions

Durant la realització d'aquest projecte he pogut entendre i aprendre el funcionament de la tecnologia Blockchain, així com provar diferents de les plataformes disponibles i arribar a fer un desenvolupament real que soluciona un problema. Un dels majors problemes principals que he tingut durant el projecte ha sigut la dificultat a l'hora de trobar informació al respecte, ja que la majoria de documentació es quedava en una visió molt general de la tecnologia, o estava ja bastant desactualitzada.

Al llarg de la realització d'aquest projecte he pogut comprovar a la velocitat a la qual es van incorporant noves funcionalitats i casos d'ús a la tecnologia. Probablement, la majoria de desavantatges que es mencionen a l'article tindran una solució en alguna de les plataformes en qüestió de mesos.

A nivell de l'aplicació d'emmagatzematge d'expedients, considero que no és només una primera solució a un problema actual, sinó que representa la base d'un nou sistema que permet infinitud de noves funcionalitats. Considero que l'aplicació de la tecnologia Blockchain a l'àmbit de l'educació es un cas d'ús clar, ja que compleix tots els requisits perquè Blockchain sigui millor que la utilització de sistemes tradicionals: un conjunt d'entitats diferents amb la necessitat d'interactuar entre si, compartir informació de manera regular i mantenir un històric dels successos.

En conclusió, la tecnologia Blockchain va néixer d'una xarxa de cryptomonedes, però definitivament té moltes més aplicacions de les que se li estan donant actualment. Si bé és cert que cada cop més empreses comencen a incorporar aquest nou sistema a les seves activitats, la majoria encara es troben en fase d'investigació, però molt probablement en poc temps es comencin a veure cada cop més aplicacions que l'utilitzin.

10. Agraïments

M'agradaria agrair al meu tutor Jordi Duran Cals per guiar-me durant tot el projecte, per aconsellar-me, i per les ganes i l'interès que ha tingut en aquest treball. També m'agradaria agrari al meu tutor d'empresa Carlos Mérida pels coneixements sobre la matèria i l'experiència que m'ha aportat.

11. Bibliografia

[1] Wikipedia, «Bitcoin,» [En línia]. Available: https://es.wikipedia.org/wiki/Bitcoin#Historia.

[2] V. Gupta, «Breve historia de 'blockchain' y del largo futuro que nos espera juntos,» 9 Març 2017. [En línia]. Available: http://hbr.es/tecnolog/497/breve-historia-de-blockchain-y-del-largo-futuro-que-nos-espera-juntos.

[3] Coursera, «Cryptocurrency,» 2017. [En línia]. Available: https://www.coursera.org/learn/cryptocurrency.

[4] J. Herrera, «Congrés de Seguretat Cognitiva i Blockchain,» Barcelona, 2017.

[5] Coindesk, «A (Short) Guide to Blockchain Consensus Protocols,» [En línia]. Available: http://www.coindesk.com/short-guide-blockchain-consensus-protocols/.

[6] M. Castro i B. Liskov, «Byzantine fault tolerance,» [En línia]. Available: https://www.google.com/patents/US6671821.

[7] IBM , «IBM Blockchain,» [En línia]. Available: https://console.ng.bluemix.net/docs/services/blockchain/etn_pbft.html.

[8] Investopedia, «51% Attack,» [En línia]. Available: http://www.investopedia.com/terms/1/51-attack.asp.

[9] A. Preukschat, Blockchain: la revolución industrial de internet, 2017.

[10] M. gates, BLOCKCHAIN, 2017.

[11] Ethereum, «A Next-Generation Smart Contract and Decentralized Application Platform,» [En línia]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[12] Hyperledger, «White paper,» [En línia]. Available: http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf.

[13] J.P Mogan, «Quorum. Advancing Blockchain Technology,» [En línia]. Available: https://www.jpmorgan.com/country/US/EN/Quorum.

[14] zCash, «Privacidad en el blockchain,» [En línia]. Available: https://z.cash/es/.

[15] Zerocoin, «Zerocoin Project,» [En línia]. Available: http://zerocoin.org.

[16] Wikipedia, «Zero-knowledge proof,» [En línia]. Available: https://en.wikipedia.org/wiki/Zero-knowledge_proof.

[17] C. Rackoff i D. R. Simon, «Non-Interactive Zero-Knowledge Proof of Knowledge and,» [En línia]. Available: https://link.springer.com/chapter/10.1007/3-540-46766-1_35.

[18] E. Ben-Sasson, A. Chiesa, C. Garman, M. G. Green, I. Miers, E. Tromer i M. Virza, «Zerocash: Decentralized Anonymous Payments from Bitcoin,» [En línia]. Available: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

[19] J. Morgan, «Quorum Whitepaper,» [En línia]. Available: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf.

[20] github, «web3j integration layer for JP Morgan's Quorum,» [En línia]. Available: https://github.com/web3j/quorum.