EAPC blog

Diàleg Blockchain – Mònica Sabata

29 d'octubre de 2019

Relatoria duta a terme per Mònica Sabata, Can Jaumandreu, Universitat de Barcelona

El proppassat 18 de juny el Govern va aprovar l'Estratègia Blockchain de Catalunya amb la voluntat de situar Catalunya com a país capdavanter en l'ús i el desenvolupament de les tecnologies de registre distribuït. És en aquest marc on es contextualitza aquest nou diàleg organitzat per l'Escola d'Administració Pública amb la col·laboració de la Universitat de Barcelona. I és que davant de les paraules de l'HC Jordi Puigneró afirmant que "Catalunya serà digital, o no serà", l'Escola va tenir la voluntat d'impulsar un nou espai de diàleg (donat que el 4 d'octubre de 2018 ja va obrir-ne un sobre ciberseguretat) que permetés als servidors públics prendre consciència del que implicarà aquesta nova estratègia governamental.

Com no podia ser d'altra manera, el diàleg es va organitzar amb dues persones expertes en la matèria: d'una banda, el Sr. Alfonso Egio, desenvolupador sènior a l'i2CAT i, de l'altra, el Sr. David Ferrer, Secretari de Telecomunicacions, Ciberseguretat i Societat Digital, Departament de Polítiques Digitals i Administració Pública. La jornada buscava plantejar els principals reptes que implica aquesta tecnologia que permet mantenir un registre de transaccions permanent, immutable i cibersegur, sense necessitat d'intermediaris o de cap autoritat central, i la utilitat d'una base de dades distribuïda, descentralitzada i encriptada que garanteix les transaccions, les fa irrevocables i transparents.

Però, comencem pel principi i definim de què estem parlant. **Què és la blockchain?**

Tal com ens va explicar el Sr. Alfonso Egio, **la blockchain** és una base de dades distribuïda on cada node guarda una còpia exacta de la mateixa base de dades i no es pot ni modificar ni reescriure. Per escriure aquestes dades cal fer una signatura criptogràfica amb una clau privada que cadascú conserva. Quan parlem de blockchain no parlem d'ocultar informació sinó que parlem de certificar. La base de dades accepta transaccions, les valida perquè siguin signades pel propietari legítim i les reescriu a sobre d'un registre. Però com s'arriba a la conclusió de que el registre és vàlid? Es fa passant una prova de treball, que és com un trencaclosques criptogràfic, que no serveix per a res més que per garantir que pocs agents poden escriure de forma molt ràpida a la cadena i en puguin alterar el seu comportament. A més, cal afegir que hi ha blockchains de caràcter públic i privat, qüestió que més tard reprendrem. En tot cas, però, cal tenir clar que la blockchain és una tecnologia -o eina- que, de forma senzilla, pot facilitar processos o la solució de problemes que podrien ser molt complicats o costosos. Ara bé, també cal considerar que no cal aplicar blockchain a tot arreu.

Per resumir, el Director general d'Innovació i Economia Digital, el Sr. Daniel Marco, present al diàleg, va afirmar que: "la blockchain és un registre, és un sistema transaccional, on estàs intercanviant valors digitals. Per això, és a tot arreu on hi hagi transaccions on la blockchain i la seva immutabilitat tenen sentit".

"La blockchain ha significat un canvi de paradigma" que, segons el Sr. Egio, ha significat que els avenços criptogràfics que es van fer durant els anys setanta, ara s'hagin posat al dia a través de l'aparició de les criptodivises i que, de fet, puguin permetre guanyar privacitat, control i empoderament amb coses i dades que la ciutadania va perdre o regalar sense adonar-se'n. Per exemple: una companyia com Facebook o LinkedIn no podria controlar la nostra identitat digital si estiguéssim utilitzant un sistema d'aquest estil.

Ara bé, i amb paraules del Sr. David Ferrer, "**cal tenir clar que blockchain no vol dir només criptomonedes o només mineria. Quan ho aterrem a l'entorn de l'administració pública, vol dir desintermediar**", cosa que significa treure actors que estan al mig de dos o més que volen intermediar. Ara bé, i seguint amb les reflexions del Secretari, **cal tenir en compte la potència que té blockchain i també la dificultat i la immaduresa tecnològica que encara és inherent a la mateixa tecnologia**.

Per explicar aquesta darrera afirmació convé tenir en compte que el 2008 es va començar a desplegar el bitcoin i és, encara avui, un entorn que encara s'està desenvolupant. No en va, encara hi ha qüestions tècniques pendents de resoldre com ara el model de governança, el qual és necessari per desplegar-ho com a solució corporativa. Per això, encara s'estan fent proves i no es pot desenvolupar del tot.

Tanmateix, mentre es desenvolupa, convé tenir clara una qüestió cabdal: **en la blockchain no hi ha intermediaris** i, per tant, el que abans es feia a través d'un sistema d'informació habitual i implicava que resoldre una problemàtica concreta podia ser molt costós i complex, ara -amb la blockchain- esdevé molt més simple. Això és així, perquè tal i com va explicar Egio a l'inici del diàleg, és una base de dades distribuïda en que cada cop que algú fa una transacció, tots els altres nodes registren un apunt i, per tant, tots s'acaben vinculant amb operacions matemàtiques que fan que sigui molt confiable i transparent que el registre que no ha estat alterat. Per això, Ferrer resumia **la blockchain com un notari descentralitzat**.

Un dels elements importants que aporta la blockchain, malgrat hi hagi diverses aproximacions (per exemple, Hyperledger o Ethereum o d'altres), és que hi ha solucions que permeten crear blockchain a través de tecnologia existent. Això significa que cada vegada que afegeixo una nova entrada en la blockchain, el programa desencadena un comportament per calcular i fer operacions diverses. És a dir, entres en una nova dimensió que pot ser gairebé una aplicació. Són, per tant, solucions que venen de fàbrica que si haguessis d'implementar serien molt costoses. .

I si ho portem a l'administració pública?

Portat a l'administració pública, el que implica és que la desintermediació -independentment de la blockchain que s'utilitzi- **ens interpeꞑa al fet que hi hagi una transformació digital real del procés**. Per exemple, amb la blockchain no pots emular un procés de subvenció.

Així doncs, a les administracions, i amb paraules del secretari Ferrer "ens permet desenvolupar una solució o un procés de manera molt més senzilla per bé que al mateix temps, l'administració ha de plantejar com presta o desenvolupa aquest servei".

I què ha fet l'administració catalana?

L'any 2018, es va crear un grup de treball transversal amb representació de molts Departaments per veure quina aproximació s'havia de fer des de l'administració de la Generalitat per fer quelcom amb la blockchain. El grup de treball fou ampli. Per això, cada Departament va enviar les persones que van voler a colꞑaborar i al mateix temps es va comptar amb experts que van dinamitzar-lo i contribuir-hi. A l'actualitat, aquest grup ja ha finalitzat els seus treballs bo i complint la seva tasca principal, la qual era plantejar quins són els reptes que blockchain ens implica en l'àmbit corporatiu, posar les bases per poder adoptar una estratègia blockchain i, finalment, pensar a quines qüestions pròpies de l'administració es podria aplicar aquesta tecnologia.

Per això, es poden assenyalar dues conclusions:

– Primera: calia mecanitzar o protocolaritzar a través d'un programa o d'una eina la detecció de les oportunitats de la Generalitat per implementar un entorn o proves pilot en l'entorn de blockchain.

– Segona: a més, com a administració, calia dotar-nos d'un entorn tecnològic que permetés tenir una metodologia i una plataforma tecnològica per començar a testejar i provar.

Un cop es va acabar el grup de treball, es va aprovar l'estratègia de blockchain de Catalunya que té diverses dimensions:

– Sectorial

– Desenvolupament d'empreses vinculades a la tecnologia blockchain, que permetessin que a Catalunya es desenvolupessin startups o empreses vinculades a la tecnologia blockchain i que, al mateix temps, tinguessin una metodologia o proposta que permetés desenvolupar-lo dins de la mateixa administració.

Sobretot, però, cal tenir en compte que amb la Blockchain -que com hem afirmat és una base de dades- **és vital que les dades que s'emmagatzemin siguin amb el vist-i-plau de la GDPR perquè quan estan inscrites no es poden esborrar**.

En quins àmbits es podria aplicar la blockchain?

La blockchain es pot aplicar en molts àmbits. Per exemple:

– A l'economia en general.

– En els certificats dels bancs.

– En l'utilització de credencials.

– En l'atorgament de les subvencions. Podries tenir un sistema basat en blockchain per a la presentació de sol·licituds. Aquest fet permetria guanyar transparència. En el cas de les subvencions el que més canviaria seria el procés d'atorgament i de resolució. Per exemple: els ajuts als menjadors escolars. Si es transferissin directament al compte de la família, com controles que han estat utilitzats per als menjadors? Per resoldre-ho i tenint en compte que els diners serien finalistes, es podria generar un actiu que garantís que l'ajut només pot ser utilitzat al menjador escolar. Es podria evitar que fossin gastats en altres qüestions i s'evitarien els intermediaris, com per exemple els bancs.

– Amb l'Identicat: la Generalitat possibilitarà que cada individu es pugui crear una identitat digital. Quan l'usuari estigui identificat es generarà un *claim* i es podrà identificar si aquest *claim* és de l'usuari o no. Es pot plantejar perquè la Generalitat no tindrà cap dada perquè es podrà fer des d'una blockchain pública.

– En la traçabilitat de residus.

– En la traçabilitat animal (per saber per on ha passat el bestiar, per exemple).

Un altre concepte important: la blockchain pública vs la blockchain privada

Des del punt de vista de les característiques de blockchain, com ara la resiliència, la transparència, la immutabilitat, la robustesa... és molt difícil que si una blockchain té, per exemple, 7000 nodes, es pugui atacar de manera prou poderosa com perquè sigui trencat tot al mateix temps.

Ara bé, portat al terreny de l'administració pública, es generen preguntes que són fruit de la manera en que es funciona i sobre com estan organitzades les administracions. Ens referim, per exemple, als dubtes que puguin sorgir per part de les assessories jurídiques. Per exemple: on està la informació?; estan aquí o a fora?; si la informació aplica o no?

Per això, si a l'actualitat es plantegés una estratègia de blockchain de la Generalitat caldria, potser, plantejar-ho a través d'una empresa privada o pública o híbrida. Però el que està clar és que **cal fer-ho des d'un entorn controlat**.

Altres qüestions que sorgiren durant el debat:

– La blockchain es pot utilitzar per a la gestió dels transplantaments o la cessió d'autoritzacions que permetin accedir a les dades mèdiques?

Les dades mèdiques són dels pacients i, per tant, l'administració només les guarda. Estònia va trobar la solució amb una targeta digital que identifica a tots els ciutadans i, per això, quan un ciutadà va al metge, s'autoritza a l'accés al registre sanitari. Per tant, aquest no seria un tema de blockchain sinó un tema d'aproximació a la dada única i de posar el ciutadà al centre, enlloc de posar-hi a l'administració.

En el cas dels transplantaments, l'aproximació que es fa a l'actualitat a l'OCATT, és per compartir els registres de les analítiques de les diàlisis que estan fent els pacients. En aquest context, els laboratoris que les fan, poden facilitar les dades a l'administració, creuar-ho de forma anònima i així, accelerar el procés i la presa de decisió de si el pacient és idoni o no per a un transplantament. Aquí sí que s'ha pogut fer una aproximació amb blockchain, la qual accelera molt el procés i en conseqüència, permet, per exemple, estalviar molts diners en diàlisi. Però **no es tracta de guardar dades a la blockchain sinó que es tracta de guardar referències a les dades**.

A partir d'aquí, segons David Ferrer, el gran repte serà que **"quan es puguin començar a fer desplegaments importants de blockchain a l'administració caldrà fer una transformació de la manera de treballar, de molts dels procediments i dels processos que s'han utilitzat fins ara".**

I quins terminis hi ha per fer-ho? I com afectarà als servidors públics en el seu dia a dia?

Ara per ara, segons Ferrer, encara hi ha molts clarobscurs en la seva aplicació i una realitat tossuda: la legislació va pel darrera de la tecnologia. Per això, en algun moment caldrà posar la legislació que doni les garanties per fer-ho de manera segura.

L'administració catalana aposta pel ***learning by doing:*** cal començar a "jugar" i testejar com es pot aplicar. Hi ha aproximacions senzilles que poden aportar molts beneficis i que, de fet, alguns Departaments ja estan provant. I és que quan fas aquests processos amb aquesta tecnologia evites molta feina i es continua essent molt garantista.

Una administració que utilitza blockchain és una administració més transparent?

Segons Ferrer, **"si ho preguntéssim als estonians ens dirien que sí"**. De fet, continua, **"ells mateixos ens van explicar que la transparència de l'administració estava directament vinculada a la qualitat democràtica"**. Ara bé, és més un concepte de com dissenyes l'administració que no pas de si la blockchain ajuda o no. És evident que ajuda i resolt problemes complexos. Malgrat això, la principal preocupació ha de ser la de posar el ciutadà al centre.

I Egio afegia, **"per defecte, una blockchain ha de ser perfectament auditable per a tothom. Per això, si és pública per a tothom, cal poder crear noves adreces i poder transaccionar de manera anònima"**. Ara bé, en aquest context **cal diferenciar entre seguretat i privacitat**. Per això és vital garantir que la informació privada està ben custodiada i que no hi accedeix ningú que no tingui autorització per fer-ho.

– Dos reptes que caldrà resoldre: els *smart contracts* i la regulació jurídica

L'administració pública es basa en procediments estandaritzats. És, en definitiva, un caldo de cultiu perfecte per establir *smart contracts*, per exemple. Tanmateix, sempre hi haurà d'haver una decisió final i per tant, sembla difícil de resoldre. Segons Egio, ja s'estan començant a generar models de negocis en què està previst qui haurà de prendre la decisió final.

Pel que fa a la regulació jurídica: des de la Secretaria s'està estudiant quins són els marges jurídics que tenim per desenvolupar blockchain. Per exemple, s'està treballant quin és l'entorn jurídic més procliu perquè les startups es puguin desenvolupar amb més facilitat.

– I finalment, quins són els reptes actuals en relació a la blockchain?

Per acabar el diàleg, el Sr. David Ferrer va esmentar els principals reptes de futur:

– Primer: superar la immaduresa tecnològica. Amb paraules de Ferrer **"això és un camí que ha començat a recórrer i anirà creixent. El que és bastant indubtable i, per això és bo ser-hi, és perquè no començar a entendre i a "jugar" amb aquestes tecnologies no ens ho podem permetre. No en va, en algun moment arribaran a tenir una certa maduresa i ens aportaran moltes coses a l'administració. Podrem fer coses noves i deixar-ne de fer d'altres".**

– Segon i el més gran: l'entorn jurídic. Quan es desplegui una solució caldrà que jurídicament sigui robusta.

– Tercer: tenir clar que no té gaire sentit començar pels problemes més complexes. Cal començar qüestions que permetin testejar i respondre les qüestions més bàsiques.

Per acabar, Mònica Sabata, moderadora del debat, va agrair als ponents i als assistents les aportacions i va desitjar que la jornada organitzada per l'EAPC servís per començar a entendre la importància de la blockchain i, al mateix temps -i parafrasejant al Secretari- per començar a "jugar".

Glosari vinculat al diàleg

– Bitcoin: és una criptomoneda descentralitzada creada per un autor anònim de pseudònim Satoshi Nakamoto. Està subdividida en 100 milions d'unitats més petites anomenades satoshis.És la moneda alternativa més utilitzada.

– Blockchain: és una base de dades distribuïda on cada node guarda una còpia exacta de la base de dades i no es pot ni modificar ni reescriure

– Mineria de blockchain

– Criptografia de clau pública

– Signatura criptogràfica

– *Smart contract*: un contracte intel·ligent és aquell que és capaç d'executar-se i fer-se complir per si mateix, de manera autònoma i automàtica, sense intermediaris ni mediadors.

– Tokenització: model virtual de recursos escassos o limitats i transferibles.

– Hash matemàtic: funció criptogràfica computacionalment tractable unidireccionalment, que genera una empremta de mida fixa a partir d'una entrada de dades arbitrària.

– Token: actiu criptogràfic.

BITCOIN, BLOCKCHAIN, CIBERSEGURETAT, CRIPTOMONEDES, DIGITAL, INNOVACIÓ, INTERNET, MÒNICA SABATA, RELATORIA