Guia sobre les tecnologies de llibre major distribuït, blockchain i les entitats locals

Impulsem la societat del coneixement
al servei de tots els municipis

LOCALRET

Redactada per Ignacio Alamillo, Doctor en Dret, Advocat, CISA, CISM, COBIT5-f i ITIL v3-f, per encàrrec del Consorci LOCALRET.

Barcelona, juny de 2019.

Índex

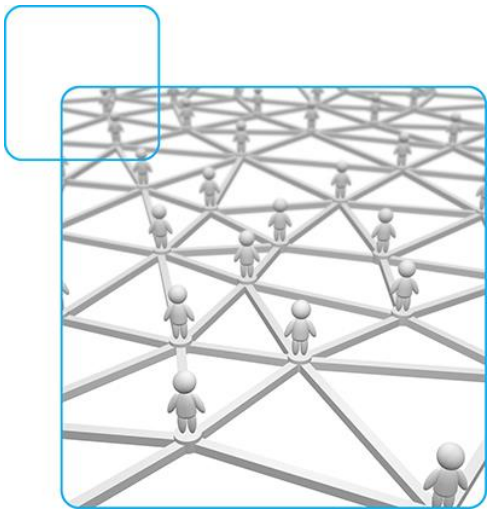
1

1. Una breu introducció a les tecnologies de llibre major distribuït

Les tecnologies de llibre major distribuït (*distributed ledger technologies*, en anglès) i, en particular, la tecnologia de cadenes de blocs (o *blockchain*, en anglès), que es basen en la criptografia de clau pública, permeten la creació d'un registre inalterable i gestionat de forma absolutament descentralitzada, que permet noves aplicacions fins ara impensables, amb un potencial transformador fora de tot dubte.

Pel que ara ens interessa, autors com Swan (2016) caracteritzen la tecnologia de cadenes de blocs com un protocol de software i un llibre major distribuït per registrar transaccions, que pot actuar com a substrat computacional a escala global per al processament de qualsevol tipus d'activitat digitalitzada.

Aquesta autora assimila, de forma gràfica, una cadena de blocs "com un document gegant de full de càlcul interactiu de Google que qualsevol persona pot veure a petició, en què administradors independents (miners) verifiquen i actualitzen constantment el llibre per confirmar que cada transacció és vàlida", indicant que "es denomina cadena de blocs perquè es publiquen seqüencialment blocs o lots de transaccions a un llibre major, de forma que es crea una cadena de blocs", resultant "la creació d'una xarxa segura en la qual es pot, de forma independent, confirmar cada transacció com única i vàlida sense la intervenció d'un intermediari centralitzat, com un banc, govern o altra institució".



Des d'aquesta perspectiva, es tracta d'un sistema que ja no es basa en la confiança entre les parts, sinó en el funcionament del propi sistema de cadenes de blocs, el qual es basa en tècniques de consens matemàtic.

Cal notar que aquests sistemes empren tecnologies de signatura digital molt semblants a les utilitzades per la signatura electrònica de documents, pel que podrà considerar-se com un sistema de signatura electrònica avançada, quan s'empri per a la prestació del consentiment, o de segell electrònic, quan l'empri una persona jurídica.

Des d'un punt de vista més abstracte, la tecnologia de cadenes de blocs permet l'actualització de tots els nodes d'una xarxa en un entorn de computació distribuïda amb l'estat actual del món, fet que permet conferir un estat compartit de confiança a un sistema distribuït; és a dir, que **quan es registra una actuació emprant aquestes tecnologies, el que realment succeeix és que aquest registre és realitzat en una gran quantitat d'ubicacions diferents, en lloc d'en una única ubicació centralitzada, pel que podem considerar que aquest registre és verdader**.

En definitiva, ens trobem davant d'un sistema en el que podem escriure qualsevol informació que vulguem, emprant un node específic de la xarxa; des d'aquest

1

moment, l'esmentada informació es copiarà a tots els nodes restants de la xarxa, pel que cap d'ells podrà eliminar aquesta informació de forma unilateral. Únicament amb el concurs d'un gran nombre de nodes es podria eliminar una inserció a la xarxa en qüestió, resultant necessari confiar en cap d'ells en particular, i que es consideri que una inserció d'informació que s'ha estès dins de la xarxa sigui considerada "verdadera".

Això no significa, per descomptat, que la informació en si mateixa sigui veritable, sinó que és veritat que es va escriure aquesta informació, i no una altra informació diferent. De la mateixa manera succeeix quan s'empra la signatura electrònica avançada basada en certificat electrònic per autenticar un document privat: el contingut del document resulta atribuïble al signant, amb independència que el contingut esmentat sigui verídic o no. Per exemple, quan es realitza i se signa una declaració falsa, el document és autèntic perquè és imputable al signant, però el seu contingut és fals. El mateix succeeix, en el fons, amb les tecnologies de registre distribuït.

El que veritablement diferencia ambdós casos té a veure amb una de les particularitats més singulars del document electrònic, i consisteix en la possibilitat de realitzar infinites còpies idèntiques d'aquest, totes elles amb la condició d'original **i** de forma simultània.

En efecte, imaginem que redactem un contracte en un fitxer PDF i el signem electrònicament. En paper seria original l'exemplar físic en què es conté la signatura, i donada la impossibilitat de duplicar-lo, necessitarem, almenys, dos exemplars, cadascun d'aquests signats per ambdues parts, per formalitzar el contracte (que, per aquest motiu, se signa "per duplicat exemplar"), tenint cadascun d'ells aquesta condició de forma exclusiva. Altrament, en l'esmentat suport electrònic i format PDF, únicament és necessari signar un exemplar, que pot ser reproduït infinites vegades a través de la simple còpia del corresponent fitxer informàtic, comunicació, per exemple, quan s'emmagatzema en un disc dur o suport portable, quan es remet per correu electrònic o es carrega en un servei d'emmagatzematge de fitxers en el Núvol (motiu pel qual, a més, haurà d'abandonar-se l'avui ritualista menció al "per duplicat" en benefici de "l'exemplar únic electrònic").

L'exemple que s'acaba d'esmentar mostra un dels avantatges de signar electrònicament un document, però també dona bona mostra d'una de les seves limitacions, que pot intuir-se ràpidament. I és que no és un mecanisme útil per aquells casos en què la transferència d'un valor es produeix mitjançant l'entrega d'un document.

En efecte, **les tecnologies de llibre major distribuït permeten, per primer cop en la història, aplicacions com la realització d'endossos** –inclús en blanc–, **facilitant, d'aquesta manera, tant la implementació de títols-valors electrònics de tota mena**, o la implantació eficient i inalterable de registres jurídics i administratius inalterables, en especial aquells en els que es recullen transferències d'actius o assignacions d'atribucions.

Fins a l'aparició d'aquestes tecnologies, l'enfocament per la informatització (avui parlaríem, segurament, de la digitalització) dels títols-valors de tot tipus consistia en la substitució de l'ús del títol corresponent per la seva "anotació en compte"; és a dir, per l'anotació en un registre centralitzat de les titularitats i les seves ulteriors modificacions. D'aquesta manera ha succeït en els mercats secundaris, en les

1

transferències dineràries i en altres operacions de pagament, o en els títols de transport.

No obstant això, i com ja hem avançat, amb les tecnologies de llibre major distribuït, ara disposem de la capacitat de realitzar electrònicament transferències de títols, mitjançant el seu endossament electrònic, eliminant, així, la necessitat d'aquests registres centralitzats.

Però no és únicament en aquest àmbit en el que s'han proposat aplicacions de les tecnologies de llibre major distribuït. Malgrat el que s'acaba d'indicar, aquesta tecnologia permetria la implantació de garanties d'autenticitat en les bases de dades centrals, impedint la modificació indetectable dels registres que les contenen.

Finalment, resulta absolutament ineludible referir-se a la possibilitat d'implementar, a través de les tecnologies de llibre major distribuït, sistemes de traçabilitat de tota mena d'objectes, tant del món electrònic, com del món físic, mitjançant la tècnica de la *tokenització*, en especial quan els *tokens* representen propietats.

Cal dir, ja, que a causa de les exigències d'aplicació de la normativa de protecció de dades, normalment tots els usos dels sistemes de cadenes de blocs impliquen que els documents o escrits, o dades a transmetre o protegir amb aquesta tecnologia es trobin fora de la cadena de blocs; és a dir, que el que es registra a la cadena de blocs no és la dada en si mateixa (que es troba fora del sistema), sinó únicament el seu resum criptogràfic.

D'aquesta forma, es pot garantir que el document o dada no ha estat modificat, però sense donar publicitat al seu contingut, i amb la possibilitat de donar compliment a les normes de protecció de dades, en especial el dret a la supressió.

1.1. Terminologia essencial

Tot i que existeixen diversos vocabularis que es refereixen a les tecnologies de registre distribuït i a la blockchain, resulta especialment interessant el treball de normalització que està realitzant el Comitè Tècnic 307 de l'Organització Internacional de Normalització (ISO), que empra els següents termes:

- Un **llibre major** (*ledger*) és un magatzem d'informació que conserva registres finals i definitius (immutables) de transaccions.

- Un **llibre major distribuït** (*distributed ledger*) és un llibre major que es comparteix i se sincronitza de forma distribuïda.

- Una **tecnologia de llibre major distribuït** (*distributed ledger technology*) és una tecnologia que permet l'operació i l'ús de llibres major distribuïts.

- Una **cadena de blocs** (blockchain) és un llibre major distribuït (*distributed ledger*) amb blocs confirmats i validats, organitzats mitjançant vincles criptogràfics, en una cadena seqüencial que només permet addicions.

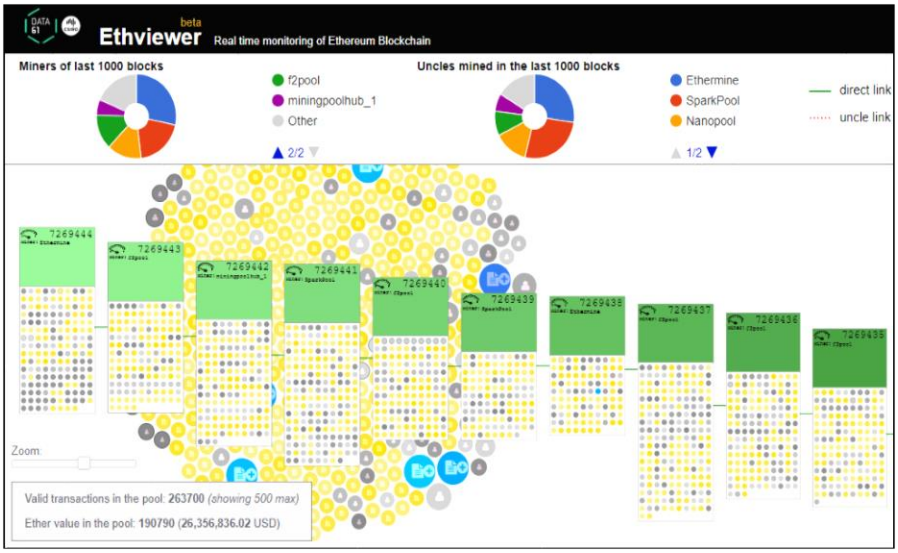
1

- Un **bloc** és una estructura de dades que compren dades de transaccions i una capçalera de bloc.
- Una **confirmació** és un estat d'una transacció o d'un bloc que es dona quan s'ha arribat a consens sobre la seva inclusió a un sistema de llibre comptable distribuït.
- Una **validació** es un estat d'una transacció o d'un bloc que es dona quan s'han comprovat i satisfet les seves condicions exigibles d'integritat.

1.2. Una visió gràfica de la cadena de blocs

Com s'ha indicat anteriorment, aquestes tecnologies es basen en la construcció de cadenes criptogràfiques de blocs que asseguren les transaccions.

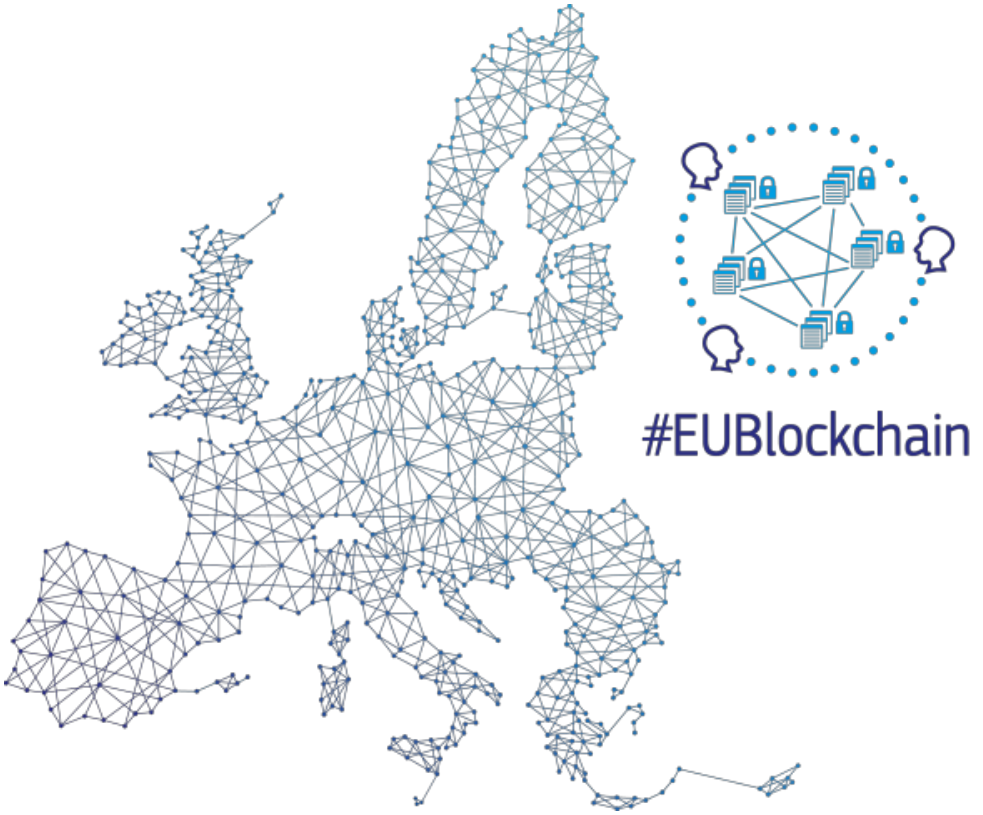
Potser resulta més fàcil comprendre millor el funcionament de la tecnologia mitjançant algun dels sistemes de visualització d'una xarxa, com en el cas de la xarxa Ethereum.



Il·lustració 1. Visualització de la cadena de blocs de la xarxa Ethereum, amb l'aplicació Ethviewer (disponible a http://ethviewer.live/)

2. Les possibilitats d'ús de la blockchain al sector públic

La blockchain es considera una tecnologia de tipus disruptiu, que podria oferir **oportunitats d'innovació en el procediment administratiu, incloent-hi el local**. L'interès per l'ús d'aquestes tecnologies en el sector públic es palesa en la important Declaració sobre Cooperació en una Associació de Blockchain Europea (*Declaration creating the European Blockchain Partnership*), signada el 10 d'abril de 2018 per vint-i-un Estats membres de la Unió Europea, incloent-hi l'Estat espanyol, i a la que posteriorment s'han adherit sis Estats més.



Il·lustració 2. Representació gràfica d'una blockchain al Mercat Únic Digital (font: https://ec.europa.eu/digital-single-market/en/blockchain-technologies)

A la Declaració, els estats signataris reconeixen el potencial de la *blockchain* per a la transformació dels serveis públics digitals a la Unió Europea, es comprometen a treballar de forma conjunta per aconseguir realitzar el potencial dels serveis basats en *blockchain* en benefici dels ciutadans, la societat i l'economia, i estableixen objectius concrets per a l'Associació.

2

Especialment interessant resulta la visió, continguda a la Declaració, relativa a que "els serveis basats en blockchain tenen el potencial per permetre serveis digitals descentralitzats, de confiança, centrats en l'usuari, i estimular nous models de negoci que beneficien la nostra societat i l'economia", per la qual cosa considera que "aquests serveis crearan oportunitats per potenciar els serveis tant en el sector públic com el privat, en particular fent un millor ús de la informació del sector públic alhora que preserven la integritat de les dades i proporcionen un millor control de les dades dels ciutadans i organitzacions que interactuen amb les administracions públiques, reduint el frau, millorant el manteniment de registres, l'accés, la transparència i l'auditabilitat, dins i fora de les fronteres".

L'Observatori i Fòrum de Blockchain de la Unió Europea (2018) considera el valor de les cadenes de blocs per a la creació de confiança en la informació i els processos en situacions en què hi ha grans quantitats de parts interessades o usuaris, molt heterogenis, i també per a la creació de pistes fiables d'auditoria de la informació, permetent la compartició i privacitat de les dades.

Es tracta d'una visió que es complementa amb el possible lideratge europeu en aquest àmbit, en la que destaca amb força la previsió de la creació d'una Infraestructura Europea de Serveis de Blockchain.

2.1 La identitat autosobirana en les relacions amb el sector públic

Un dels casos d'ús interessant de les tecnologies de registre distribuït es refereix a la denominada identitat auto-sobirana (*self-sovereign identity*, en anglès), que és aquella creada i gestionada per cada persona individualment, sense la intervenció de terceres parts.

Com ha indicat Allen (2016), aquestes identitats han d'atendre a les següents característiques: existència de la identitat d'una persona independentment d'administradors o proveïdors d'identitat; control per la persona de les seves identitats digitals; accés complet per les persones a les seves dades; transparència dels sistemes i algorismes; persistència de les identitats digitals; portabilitat de les identitats digitals; interoperabilitat de les identitats digitals; compliment de l'economia de dades; i protecció dels drets de la persona.

En un sistema d'identitat autosobirana basat en tecnologies de registre distribuït, l'usuari pot obtenir testimoni de dades d'identitat, produïts per entitats que els han verificat, per, posteriorment, poder crear al·legacions d'identitat en les que presentarà, a tercers, les dades que requereixi per acreditar la seva identitat o altres atribucions.

A diferència, doncs, dels sistemes que més s'empren en l'actualitat en el procediment administratiu electrònic, com Cl@ve, en què intervé un proveïdor d'identitat en cada autenticació, en aquests sistemes d'identitat auto-sobirana, aquesta intervenció desapareix.

En efecte, en el sistema Cl@ve, la identificació se sustenta en un procés en què participen diverses entitats: en primer lloc, l'interessat es connecta al servei electrònic ofert per l'Administració i selecciona autenticar-se mitjançant Cl@ve. Aquest servei reenvia l'interessat a la pàgina web del servei Cl@ve, on es produeix l'autenticació

2

(per exemple, mitjançant contrasenya o doble factor d'autenticació). Un cop autenticat, a l'interessat se li entrega un codi únic i se'l reenvia, de nou, al servei al que necessita accedir, havent d'entregar-li l'esmentat codi com a prova. A continuació, el servei pregunta a Cl@ve sobre la identitat de l'interessat, per a la qual cosa li envia aquest codi, i rep una resposta, en forma de document en XML, amb les dades d'identitat de la persona que ha lliurat el codi. Finalment, es concedeix l'accés.

En canvi, **en un sistema d'identitat autosobirana, donat que l'interessat ja posseeix les dades d'identitat i els altres atributs autenticats pels emissors, degudament enllaçats en la xarxa de nodes, per identificar-se enfront de tercers, ja no necessita de la intervenció dels emissors**.

Cal preguntar-se sobre la possibilitat d'emprar aquests sistemes per a la identificació en el procediment administratiu, a efectes dels quals hem de remetre'ns al règim contingut en l'article 9 de la Llei 39/2015, d'1 d'octubre, del Procediment administratiu comú de les administracions públiques (d'ara endavant, LPAC).

Tot i que el règim de la LPAC, com indica el preàmbul de la Llei, es troba alineat amb el Reglament (UE) núm. 910/2014, del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior, i pel que es deroga la Directiva 1999/93/CE (d'ara endavant, Reglament eIDAS), el mateix és suficientment neutral com per permetre l'ús d'altres sistemes d'identificació electrònica, inclús malgrat que no trobin encaix en l'esmentat Reglament de la Unió.

En aquest sentit, l'epígraf 2 de l'article 9 de la LPAC autoritza que "els interessats podran identificar-se electrònicament davant les administracions públiques a través de qualsevol sistema que disposi d'un registre previ com a usuari, que permeti garantir la seva identitat", essent admissibles diversos tipus de sistemes:

"a) Sistemes basats en certificats electrònics reconeguts o qualificats de signatura electrònica expedits per prestadors inclosos a la «Llista de confiança de prestadors de serveis de certificació». A aquests efectes, s'entenen compresos entre els esmentats certificats electrònics reconeguts o qualificats els de persona jurídica i d'entitat sense personalitat jurídica.

b) Sistemes basats en certificats electrònics reconeguts o qualificats de segell electrònic expedits per prestadors inclosos en la «Llista de confiança de prestadors de serveis de certificació».

c) Sistemes de clau concertada i qualsevol altre sistema que les administracions públiques considerin vàlid, en els termes i condicions que s'estableixin".

En tot cas, cal notar que el requisit legal ve referit a l'existència d'un registre previ d'usuari, fet que, en el cas de la tecnologia de registre distribuït, es compleix perfectament per part de l'emissor.

I pel que fa als sistemes esmentats en la LPAC, les dues primeres possibilitats es basen en l'ús de certificats de signatura electrònica (en el cas de persona física) o de segell electrònic (en el cas de persona jurídica). En el cas de les tecnologies de registre distribuït, i donat que l'actuació dels interessats mitjançant les mateixes se sustenta, com s'ha avançat, en la signatura digital, resultaria possible expedir els corresponents certificats (fet que s'ha denominat com una infraestructura de clau

2

pública descentralitzada), però no és comú que això succeeixi, pel que, en general, s'haurà d'acudir a la tercera possibilitat, sempre que l'Administració consideri aquest sistema vàlid.

Per això s'haurà d'estar a allò que s'estableix en el Reial decret 3/2010, de 8 de gener, pel que es regula l'Esquema nacional de seguretat en l'àmbit de l'Administració electrònica (d'ara endavant, ENS) i, concretament, a les normes de seguretat aplicables a la identificació i autenticació d'usuaris, que són més o menys estrictes en atenció al nivell de seguretat exigible al sistema (nivell que és determinat considerant l'impacte o dany que es produiria en cas d'una suplantació d'identitat, en allò que estem ara analitzant).

Com pot veure's en l'epígraf 4.2.1 de l'Annex II de l'ENS, "les parts que intervenen s'identificaran d'acord als mecanismes previstos en la legislació europea i nacional en la matèria, amb la següent correspondència entre els nivells de la dimensió d'autenticitat dels sistemes d'informació als que es té accés i els nivells de seguretat (baix, substancial, alt) dels sistemes d'identificació electrònica previstos en el Reglament (UE) núm. 910/ 2014, del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior, i pel que es deroga la Directiva 1999/93/CE:

– Si es requereix un nivell BAIX en la dimensió d'autenticitat (annex I): Nivell de seguretat baix, substancial o alt (article 8 del Reglament núm. 910/2014)

– Si es requereix un nivell MITJÀ en la dimensió d'autenticitat (annex I): Nivell de seguretat substancial o alt (article 8 del Reglament núm. 910/2014)

– Si es requereix un nivell ALT en la dimensió d'autenticitat (annex I): Nivell de seguretat alt (article 8 del Reglament núm. 910/2014)".

D'aquesta manera, i a diferència del que succeeix en la LPAC, realment en l'ENS sí que trobem un alineament general dels sistemes d'identificació que poden ser admesos per les administracions públiques amb el Reglament eIDAS, però, únicament, en allò que fa referència a les exigències de seguretat que han de complir aquests sistemes, i no a altres qüestions que podrien resultar més conflictives, com les relatives a la interoperabilitat, ja que el Reglament eIDAS aposta, en l'actualitat, per una xarxa de sistemes com Cl@ve, i no per sistemes d'identificació basats en tecnologies de registre distribuït.

Donat que un dels fonaments tècnics de les tecnologies de registre distribuït és, com ja hem esmentat, l'ús de signatures digitals, amb caràcter general podem considerar que aquests sistemes permetran complir sense cap mena de dificultat els criteris del Reglament eIDAS per al nivell substancial, pel que es podran emprar en la majoria de supòsits de procediment administratiu.

Òbviament, l'Administració que implementi aquest tipus de servei d'identificació ha de conservar l'al·legació d'identitat que li ha transferit l'interessat, podent verificar-la en el moment que ho necessiti a través de la consulta a la xarxa. En realitat, en termes de valor probatori, es tracta d'un sistema tan bo com el que es basa en un certificat qualificat o en Cl@ve, sempre que l'emissor apliqui les degudes exigències en el moment de produir els testimonis d'identitat que entregarà a l'interessat.

2

Molt interessant resulta la previsió de l'article 9.3 de la LPAC, en virtut del qual "en tot cas, l'acceptació d'algun d'aquests sistemes per l'Administració general de l'Estat servirà per acreditar davant de totes les Administracions Públiques, excepte prova en contra, la identificació electrònica dels interessats en el procediment administratiu".

Aquest article, que ha estat declarat constitucional en la STC 55/2018, de 24 de maig (malgrat que amb un vot particular en contra), permet estendre a totes les administracions públiques l'ús d'un sistema d'identificació que hagi estat prèviament admès per l'Administració general de l'Estat, fet que podria facilitar l'adopció de determinats sistemes basats en tecnologies de registre distribuït, com en el cas del sistema Alastria ID.

Un fet similar succeeix en el cas de la identificació de les administracions, en aquest cas regulada en la Llei 40/2015, de 1 d'octubre, de Règim jurídic del Sector Públic (d'ara endavant, LRJSP), a excepció del supòsit de la identitat de la seu electrònica, que, per altra banda, no es realitza – almenys a dia d'avui – mitjançant tecnologies de registre distribuït.

En aquest cas, la normativa és molt parca i es limita a autoritzar, per a la identificació, l'ús de sistemes de segell electrònic avançat basat en certificat electrònic qualificat, però sense restringir la possibilitat d'ús d'altres tipus de sistemes, pel que resulta perfectament factible.

2.2. Signatura i segell electrònics basats en tecnologies de registre distribuït

Com ja s'ha indicat anteriorment, aquestes tecnologies es basen en l'ús de signatures digitals produïdes mitjançant la corresponent clau privada que té el signant, sigui aquest l'interessat o l'Administració.

Per aquest motiu, ens hem de plantejar la possibilitat d'emprar aquests sistemes a efectes de signatura en el procediment administratiu –en aquells casos en què sigui exigible, conforme a la previsió de l'article 11 de la LPAC– o en altres relacions electròniques amb les administracions públiques regides per la seva normativa sectorial corresponent; signatura que haurà de resultar conforme al règim establert en l'article 10 de la LPAC, i en els articles 42 i següents de la LRJSP.

En aquest sentit, l'article 10.1 de la LPAC autoritza que "els interessats podran signar a través de qualsevol mitjà que permeti acreditar l'autenticitat de l'expressió de la seva voluntat i consentiment, així com la integritat i inalterabilitat del document", complementant, d'alguna manera, la definició de signatura electrònica continguda en l'article 3.10 del Reglament eIDAS, en virtut del qual es defineix com "les dades en format electrònic annexes a altres dades electròniques, o associades de manera lògica amb elles, que empra el signant per signar", en un enfocament d'encertada neutralitat tecnològica, que permet perfectament l'ús de qualsevol tecnologia que pugui satisfer els requisits legalment establerts.

2

De fet, si atenem a la definició de la signatura electrònica avançada continguda en l'article 3.11 del mateix Reglament eIDAS, aquesta ens condueix a l'article 26 del Reglament, que estableix els requisits que la mateixa ha de complir:

"a) estar vinculada al signant de manera única;

b) permetre la identificació del signant;

c) haver estat creada emprant dades de creació de la signatura electrònica que el signant pot utilitzar, amb un alt nivell de confiança, sota el seu control exclusiu, i

d) estar vinculada amb les dades signades amb la mateixa, de manera que qualsevol modificació ulterior d'aquestes sigui detectable".

Els sistemes basats en tecnologies de registre distribuït emprades per a la identificació, com en el cas d'Alastria ID, permeten el compliment de tots aquests requisits, constituint signatura electrònica avançada. En efecte, l'ús de la signatura digital per a l'actuació garanteix la vinculació de la signatura amb el signant (donat que únicament el signant posseeix la clau) i amb el document signat (donat que la signatura incorpora el resum de la transacció a la que s'ha enllaçat el document); mentre que el control exclusiu de la clau ve garantit per les mesures de seguretat de l'aplicació de l'usuari. Finalment, el sistema d'identitat auto-sobirana garanteix la identificació del signant.

Per la seva banda, l'epígraf 2 del mateix article 10, en certa manera anàleg a l'article 9.2 ja analitzat, regula que "en el cas que els interessats optessin per relacionar-se amb les administracions públiques a través de mitjans electrònics, es consideraran vàlids a efectes de signatura:

a) Sistemes de signatura electrònica reconeguda o qualificada i avançada basats en certificats electrònics reconeguts o qualificats de signatura electrònica expedits per prestadors inclosos en la «Llista de confiança de prestadors de serveis de certificació». A aquests efectes, s'entenen compresos entre els esmentats certificats electrònics reconeguts o qualificats els de persona jurídica i els d'entitat sense personalitat jurídica.

b) Sistemes de segell electrònic reconegut o qualificat i de segell electrònic avançat basats en certificats electrònics reconeguts o qualificats de segell electrònic inclosos en la «Llista de confiança de prestadors de serveis de certificació».

c) Qualsevol altre sistema que les administracions públiques considerin vàlid, en els termes i condicions que s'estableixin".

Com pot constatar-se, malgrat que els dos primers supòsits no seran aplicables, donat que, normalment, no s'expediran certificats qualificats als usuaris d'aquestes tecnologies, el tercer supòsit permet a l'Administració fer ús d'aquestes tecnologies sense majors dificultats.

Quelcom similar succeirà en el cas de la signatura electrònica per part de l'Administració. En aquest aspecte, potser l'oportunitat més gran es troba en reforçar el sistema de signatura electrònica per a l'actuació administrativa automatitzada consistent en un Codi Segur de Verificació, previst en l'article 42.b) de la LRJSP.

2

L'alineació d'aquests Codis Segurs de Verificació amb les tecnologies de registre distribuït –o directament la substitució d'un sistema per l'altre– aportaria una garantia real amb la finalitat d'impedir un possible esborrat, i facilitaria la verificació dels Codis Segurs de Verificació, que podrien ser comprovats sense la intervenció de l'Administració que els va generar, incrementant-se la confiança en el sistema.

En allò que fa referència a les autoritats i treballadors i treballadores públiques, res en la LRJSP s'oposa a que l'Administració pugui establir un sistema de signatura electrònica basat en tecnologies de registre distribuït.

En tot cas, i com ja hem vist en el supòsit de la identificació electrònica, tant en el cas de la signatura dels interessats com de l'Administració, s'haurà d'estar al que disposi l'ENS en relació amb l'ús de la signatura electrònica, en funció de la categoria de seguretat del sistema d'informació en qüestió. Concretament, l'epígraf 5.7.4 de l'Annex II de l'esmentada norma imposa límits que poden impedir l'ús de sistemes de *blockchain*, únicament en el nivell alt, pel que, en general, podran emprar-se en la immensa majoria de relacions amb les administracions públiques.

2.3. La representació electrònica

En íntima connexió amb les necessitats d'identificació i signatura electròniques, que s'acaben d'exposar, trobem l'acreditació de les facultats de representació d'un tercer.

Tal i com autoritza l'article 5.4 de la LPAC, "la representació podrà acreditar-se a través de qualsevol mitjà vàlid en Dret que deixi constància fidedigna de la seva existència", pel que podria, perfectament, plantejar-se la possibilitat d'emprar també, per a aquesta finalitat, la tecnologia de registre distribuït, donat que, en el fons, ens estem referint a atributs d'una persona.

En efecte, sistemes com el ja indicat d'Alastria permetrien l'obtenció d'un poder notarial, per exemple, i la seva *tokenització* a efectes de transferència a l'Administració per part de l'interessat, pel que haurà de produir-se la corresponent còpia electrònica autèntica d'acord amb les previsions de l'article 17 bis.3 de la Llei del Notariat de 28 de maig de 1862, incorporat per l'article 115 de la Llei 24/2001, de 27 de desembre, de Mesures fiscals, administratives i de l'ordre social.

És més, pot emprar-se el propi sistema de *blockchain* per a la concessió de l'apoderament, electrònicament, que serà entregat a l'apoderat, trobant-nos davant d'un apoderament que ja no serà *apud acta*, sinó endossat amb base a la xarxa.

2

2.4. Les comunicacions amb les administracions públiques

Tractant-se d'una xarxa de nodes que s'envien transaccions entre els mateixos, es pot perfectament plantejar l'ús d'aquesta tecnologia per a les comunicacions entre els interessats i les administracions públiques, i entre les pròpies administracions.

En aquest sentit, sobre aquestes xarxes es pot implementar qualsevol mecanisme de comunicació amb el sector públic.

Més concretament, aquestes comunicacions poden incloure:

- La presentació de documents i escrits al registre electrònic d'entrada de l'Administració, així com el lliurament dels corresponents rebuts de presentació.

- La remissió de comunicacions i de notificacions administratives als interessats, per part de les entitats del sector públic.

En tots dos casos, **l'ús de les tecnologies de cadenes de blocs permet l'assegurament de les evidències dels actes de comunicació**, incrementant les garanties del procediment

2.5. Assegurament dels llibres electrònics de registre i altres documents

Una altra de les aplicacions que poden ser transformades per l'adopció de la tecnologia de registre distribuït es refereix als llibres de registre (com els comptables, o els d'actes, decrets i resolucions), en els que, certament, **l'actual utilització de la signatura de les diligències pot ser substituïda per aquestes noves tecnologies de garantia**.

En el cas dels llibres comptables és necessari recordar –per posar únicament un exemple– que la Regla 15.2 de la Instrucció del model normal de Comptabilitat Local, aprovada per Ordre HAP/1781/2013, de 20 de setembre en atenció a allò previst en l'article 203.1 del Text refós de la Llei reguladora de les Hisendes locals, aprovat pel Reial decret Legislatiu 2/2004, de 5 de març, preveu que "les bases de dades del sistema informàtic on resideixin els registres comptables han de constituir suport suficient per a la gestió de la comptabilitat de l'entitat comptable, sense que sigui obligatòria l'obtenció i la conservació de llibres de comptabilitat en paper o per mitjans electrònics, informàtics o telemàtics", però sempre que s'estableixin les necessàries garanties d'autenticitat i integritat (Regla 39.2, en relació amb els justificants de les operacions i dels suports de les anotacions comptables i Regla 42.1, en relació amb la informació comptable).

2

En allò que fa referència als llibres d'actes, decrets i resolucions –dels que, per cert, s'ha oblidat completament el legislador tant de la LPAC com de la LRJSP– si partim de l'obligació de l'Administració pública d'emprar exclusivament mitjans electrònics en la seva actuació (sigui formalitzada o no), que resulta, com a mínim, dubtosa en el cas dels òrgans col·legiats de govern segons la disposició addicional vint-i-unena de la LRJSP, ha d'entendre's derogada la legislació reguladora dels llibres d'actes, decrets i resolucions en suport paper, en especial la continguda en el Reial decret 2568/1986, de 28 de novembre, pel que s'aprova el Reglament d'organització, funcionament i règim jurídic de les entitats locals, que, malgrat d'aplicació supletòria, continua essent una barrera clara a l'extensió d'aquest tipus d'instrument electrònic.

Sembla aclarir la qüestió el Reial decret 128/2018, de 16 de març, pel que es regula el règim jurídic dels funcionaris d'Administració local amb habilitació de caràcter nacional, quan, en els seu article 3, es refereix a la transcripció de les actes a llibres en suport paper o electrònic, indistintament, cal imaginar que en funció del que disposi el Reglament orgànic municipal.

En definitiva, l'ús de tecnologies de registre distribuït pot suposar una oportunitat real per a l'assegurament de la integritat dels llibres electrònics de registre.

2.6. Actuació administrativa automatitzada i Smart contracts

No podem tancar aquesta panoràmica d'usos de les tecnologies de registre distribuït sense referir-nos a la formalització electrònica i execució automatitzada de contractes i convenis administratius i altres actuacions administratives automatitzades emprant els anomenats contractes intel·ligents (*Smart contracts*), en condicions de fiabilitat, transparència i control per totes les parts interessades mai abans assolides.

Un contracte intel·ligent no és, però, realment un contracte, sinó que es refereix a un programa informàtic que executa una operativa prèviament descrita, en especial en l'àmbit dels contractes (Szabo, 1994), tot i que actualment s'utilitza aquesta expressió amb caràcter general, com per exemple en el cas del llenguatge *Solidity* de la xarxa Ethereum, que s'utilitza per a força tipus de propòsits, incloent-hi les compres a distància o les votacions electròniques.

En el sentit esmentat, el Comitè Tècnic 307 d'ISO defineix el contracte intel·ligent com el programa informàtic enregistrat a un sistema de llibre major distribuït en el qual es registra el consens sobre els efectes de qualsevol execució del programa en qüestió.

Des d'aquest punt de vista, cal recordar que l'actuació administrativa automatitzada es troba autoritzada per la LRJSP, norma que permet fàcilment l'adopció d'aquesta tecnologia sense particulars dificultats.

2

Més en concret, l'article 41.1 de la LRJSP defineix l'actuació administrativa automatitzada com "qualsevol acte o actuació efectuada íntegrament a través de mitjans electrònics per una Administració pública en el marc d'un procediment administratiu i en la qual no hagi intervingut de manera directa cap empleat públic", com succeiria en el cas de l'ús d'un contracte intel·ligent per prendre una decisió administrativa, especialment en procediments molt reglats.

Exemples d'aquesta actuació administrativa automatitzada poden ser l'expedició de rebuts de registre electrònic d'entrada de documents, la producció de còpies electròniques autèntiques, l'expedició de certificacions de dades inscrites a registres administratius, o la producció de notificacions i comunicacions electròniques, entre d'altres (Alamillo i Urios, 2011).

Resulta especialment rellevant indicar que, conforme a l'epígraf 2 del mateix article 41 de la LRJSP, *"s'ha d'establir prèviament l'òrgan o òrgans competents, segons els casos, per a la definició de les especificacions, programació, manteniment, supervisió i control de qualitat i, si s'escau, auditoria del sistema d'informació i del seu codi font*", i *"indicar l'òrgan que s'ha de considerar responsable als efectes d'impugnació",* el que es podrà fer a la disposició de caràcter general que reguli aquesta actuació.

3

3. Cap a la implementació de la *blockchain* per part de les entitats locals

En definitiva, ens trobem davant d'unes tecnologies que ofereixen unes aplicacions d'extraordinària importància pel procediment administratiu i l'actuació de les administracions públiques, que, de ben segur, poden contribuir a l'increment de les garanties i a la lluita contra les irregularitats procedimentals i que poden ser perfectament emprades ja sense necessitat de procedir a cap modificació substancial del marc legal vigent.

Tot i el que s'acaba de dir, resulta convenient considerar una sèrie de qüestions a l'hora de procedir a la implementació d'aquestes les tecnologies de registre distribuït per part d'una entitat local:

1. En primer lloc, cal identificar els possibles casos d'ús d'aquesta tecnologia per part de l'entitat local, entenent que hi ha situacions més idònies que altres per entrar en aquest espai.

   A tall d'exemple, es pot esmentar l'experiència de Govern d'Aragó, respecte a la creació d'un registre basat en blockchain per a la presentació d'ofertes de contractació.

2. En segon lloc, cal valorar la modalitat contractual a emprar per a l'execució del projecte, en especial atenent al model de finançament de l'operativa de la xarxa. Habitualment ens trobarem davant d'un contracte de serveis, que inclourà tasques de programació i el consum del servei de cadena de blocs.

3. En tercer lloc, és important regular mitjançant una disposició de caràcter general l'ús que es farà del sistema de cadena de blocs per part de l'entitat local.

Referències

ALAMILLO DOMINGO, I. i URIOS APARISI, F.X. (2011). *L'actuació administrativa automatitzada en l'àmbit de les administracions públiques. Anàlisi jurídica i metodològica per a la construcció i l'explotació de tràmits automàtics*. Escola d'Administració Pública de Catalunya, Generalitat de Catalunya. Recuperat de http://eapc.gencat.cat/ca/publicacions/colleccions/estudis_de_recerca_digitals/3_actuacio_administrativa_automatitzada/

CONSORCIO ALASTRIA. (Octubre de 2017). *Alastria Identitat Digital.* Obtingut de https://alastria.io/assets/resources/Alastria-Identitat.pdf

ALLEN, C. (2016, 04 27). *The path to self-sovereign identities.* Recuperat de Coindesk: https://www.coindesk.com/path-self-sovereign-identity/

ISO TC 307/WG 1 N0318. Blockchain and distributed ledger technologies — Terminology.

SZABO, N. (1994). *Smart contracts*. Recuperat de http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

SWAN, M. (2016). Blockchain Temporality: Smart Contract Time Specifiability with Blocktime. En J. Alferes, L. Bertossi, G. Governatori, P. Fodor, & D. Roman (Ed.), *Rule Technologies. Research, Tools, and Applications. RuleML 2016. Lecture Notes in Computer Science, vol 9718* (págs. 184-196). Cham: Springer. doi:10.1007/978-3-319-42019-6_12

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM (2018). *Blockchain for Government and Public Services*. Recuperat de https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf?width=1024&height=800&iframe=true

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM (2018). *Blockchain and the GDPR. Recuperat de* https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf?width=1024&height=800&iframe=true

Impulsem la societat del coneixement
al servei de tots els municipis

LOCALRET