LES NOVES TECNOLOGIES APLICABLES A LA GESTIÓ DE DOCUMENTS: la cadena de blocs

Hrvoje Stančić, doctor, professor associat
Departament de Ciències de la Informació i la Comunicació
Facultat d'Humanitats i Ciències Socials
Universitat de Zagreb
Ivana Lucica, 3, Zagreb, Croàcia
hstancic@ffzg.hr

INTRODUCCIÓ

Actualment els documents digitals es poden crear de dues maneres: es poden digitalitzar a partir de documents en paper existents o es poden generar digitalment. La digitalització, en el sentit més ampli, és la transformació d'un senyal analògic en un senyal digital equivalent. En un sentit més estricte, representa la transformació de diferents materials en el format digital, convertint-los en un codi binari desat en un fitxer informàtic.[1] La digitalització divideix el concepte de preservació en dues parts: la preservació del contingut o la informació registrats en un document i la preservació de l'objecte físic, és a dir, el suport que conté la informació. El contingut informatiu es digitalitza i es desa separat de l'objecte físic (Stančić, 2000). És important assenyalar que qualsevol document preservat digitalment ha de mantenir intactes les seves característiques d'autenticitat, fia-

bilitat, integritat i usabilitat (ISO 15489-1:2016 Informació i documentació: Gestió documental. Part 1, Conceptes i principis, 2016). La confiabilitat d'un document fa referència a l'exactitud, la fiabilitat i l'autenticitat d'aquest document (Base de dades terminològiques d'InterPARES Trust). L'arxiu i la preservació representen un repte singular, perquè es tracta d'activitats a llarg termini. El problema de la preservació i el manteniment a llarg termini de la informació digital es pot interpretar com la preservació de documents perquè la tecnologia en què es basen no esdevingui obsoleta. Els objectes digitals requereixen un manteniment constant i continu i depenen d'un ecosistema complex de maquinari, programari, normes i reglaments que canvia constantment, s'esmena o se substitueix. En comparació amb els documents analògics, els documents digitals s'exposen a un risc més elevat de deteriorar-se, sobretot pel ritme accelerat a què es desenvolupen les tecnologies de la informació. La preservació dels documents digitals va molt més enllà de la preservació d'un fitxer informàtic: l'objectiu és permetre l'accés als continguts i, alhora, garantir que se'n mantenen les característiques importants.

1.1. SIGNATURES I SEGELLS DIGITALS

La conseqüència del comerç electrònic i les comunicacions digitals és la creació d'un nombre creixent de documents digitals que també poden contenir signatures o segells digitals. Per això, cal analitzar els reptes de la preservació a llarg termini d'aquest tipus de documents.

Malgrat que tècnicament són el mateix, la diferència entre les signatures digitals [2] i els segells digitals és que la signatura digital només es pot associar amb una persona física i la clau de signatura només pot estar controlada per la persona signatària, mentre que un segell digital pot només es pot associar a una persona jurídica i la clau de signatura només pot estar controlada pel procés que assigna un segell per tal de garantir la integritat i l'origen. (What is an electronic seal? [Què és un segell electrònic]) (eIDAS, 2014).

Per preservar-los a llarg termini, els documents amb signatura digital també han de tenir les característiques bàsiques d'autenticitat, fiabilitat, integritat i usabilitat, cosa que exigeix un mètode més complex de preservació en comparació amb els documents digitals sense signatures ni segells digitals. De la mateixa manera que hi ha diferències entre la preservació de documents digitals a curt i llarg termini, també hi ha diferències entre la preservació dels documents digitals

que contenen signatures o segells digitals i els que no. Els documents signats o segellats digitalment presenten un nivell més de complexitat en forma de signatura o segell digital, per la qual cosa la seva preservació és més complicada.

Malgrat que els documents amb signatura digital es poden preservar durant un període més prolongat, poden perdre la seva validesa jurídica si no es poden validar o si perden la propietat de no repudi. Si es produeix un error en el procés de validació de la signatura digital, la confiabilitat del document digital queda desestimada. Aquest problema sorgeix perquè una signatura digital i, més en concret, el certificat en què es basa, tenen una durada limitada i la validació d'aquesta signatura requereix una connexió amb l'autoritat de certificació (AC) que depèn de la infraestructura de claus públiques (PKI, per les sigles en anglès). Si algun dels elements d'aquest sistema falla, la validació de la signatura digital no funcionarà. Això és especialment important a l'hora de preservar documents que contenen signatures digitals avançades (Herceg, Brzica, & Stančić, 2015).

1.2. SEGELLS DE TEMPS DIGITALS

En el context de les signatures digitals, el segell de temps digital té un paper important. Representa un certificat signat digitalment d'un emissor de segells de temps que confirma l'existència de les dades o els documents a què fa referència el segell de temps en el moment que s'indica en aquest segell. El segell de temps digital ofereix una prova fiable que el document o les dades s'han creat abans o just abans de la data i l'hora que s'indiquen en el segell de temps digital. No es permet modificar les dades, els documents o el segell de temps i aquests canvis són fàcils de detectar. Per tant, el segell de temps digital garanteix: 1) que el document o les dades existien en aquesta forma en el moment que s'indica en el segell de temps, 2) que el document o les dades no s'han modificat després del moment que s'indica en el segell de temps, 3) que la verificació de la signatura digital es pot realitzar amb fiabilitat fins i tot després de la revocació o el venciment del certificat (en aquest cas, es pot comprovar que el document o les dades no s'han modificat, però no es pot comprovar la validesa del certificat de la signatura), i 4) que el document o les dades s'han enviat o rebut en el moment que s'indica en el segell de temps. L'autoritat de segellat de temps (TSA) signa digitalment el valor *hash* de les dades o els documents juntament amb la data i hora (provinent d'una font fiable, per exemple, es pot vincular al temps universal coordinat) i d'aquesta manera s'emet un segell de temps digital que, més enda-

vant, es combina amb les dades o els documents i la clau privada de la persona signatària per crear la signatura digital en què s'indica l'hora de la signatura.

1.3. PRESERVACIÓ A LLARG TERMINI DE DOCUMENTS AMB SIGNATURA DIGITAL

La preservació a llarg termini dels documents digitals que contenen signatures digitals o segells digitals és un repte per als arxivers. Aquests documents digitals no són fàcils de preservar, no només pels constants avenços tecnològics, sinó també perquè els certificats en què es basen tenen una durada limitada. Per exemple, l'Organisme Financer (FINA), una autoritat de certificació (AC) de Croàcia, emet certificats amb dos anys de validesa, mentre que els certificats de l'Organisme per a les Activitats Comercials (en croat, Agencija za komercijalnu djelatnost, AKD) tenen una validesa de cinc anys (utilitzats en els documents d'identitat electrònics). En general, els certificats arrel de l'emissor tenen un període de validesa més llarg, per exemple, de deu anys. Quan el certificat venci, ja no es podrà comprovar la validesa de la signatura digital, però encara es podrà comprovar la integritat del document en si. Actualment existeixen diversos mètodes de preservació a llarg termini dels documents digitals que contenen signatures digitals o inclouen segells digitals.

Segons el PREMIS (Diccionari de dades per a les metadades de preservació: PREMIS versió 3.0, 2015), els repositoris de preservació utilitzen les signatures digitals de tres maneres:

1. *Per a l'enviament al repositori*, un agent (autor o presentador) signa un objecte per afirmar que n'és realment l'autor o presentador;

2. *Per a la difusió des del repositori*, el repositori signa un objecte per afirmar que realment és l'origen de la difusió;

3. *Per a l'emmagatzematge arxivístic*, és possibles que un repositori vulgu arxivar objectes signats perquè es pugui confirmar l'origen i la integritat de les dades.

Només en el tercer cas, en què el repositori utilitza les signatures digitals com un instrument per confirmar-ne l'autenticitat al llarg del temps, s'han de preservar tant la signatura com la informació necessària per validar la signatura.

Segons Blanchette (Blanchette, 2006), des de la perspectiva dels arxius hi ha tres opcions possibles:

1. *Preservar les signatures digitals:* aquesta solució requereix l'ús d'uns mitjans considerables per preservar els mecanismes necessaris per a la validació de les signatures i no aborda la necessitat de preservar també la intel·ligibilitat dels documents;

2. *Eliminar les signatures:* aquesta opció és la que requereix menys adaptació per part de les institucions d'arxiu, però empobreix la descripció del document, atès que elimina la signatura com un element tècnic que serveix per garantir l'autenticitat dels documents;

3. *Registrar el rastre de les signatures en forma de metadades:* aquesta solució requereix pocs mitjans tècnics i registra tant l'existència de la signatura com el resultat de la seva verificació. Això no obstant, les signatures digitals perden el seu caràcter especial d'element principal de prova de l'autenticitat del document. A més, aquest mètode requereix l'existència d'un tercer fiable per preservar i autenticar les metadades.

Alguns autors sostenen que l'única opció és la primera, és a dir, desenvolupar un servei d'arxivística fiable (TAS, per les sigles en anglès) que pugui garantir que la signatura d'un document es podrà continuar validant passats uns anys (Dumortier & Van den Eynde).

Tanmateix, els resultats dels projectes InterPARES anteriors recomanen la tercera opció, és a dir, organitzar un arxiu digital per comprovar la validesa de les signatures digitals en la fase d'ingesta, afegir la informació sobre la validesa a les metadades dels documents i preservar els documents sense tornar a abordar la validesa de la signatura digital. Així, la qüestió de la confiança passa del document (signat digitalment) a l'arxiu que preserva els documents digitals i les metadades (sobre la validesa) associades. Aquesta opció segueix el model més tradicional de la preservació arxivística, que contrasta amb la premissa subjacent de les tecnologies de la cadena de blocs i de registres distribuïts, que no depenen d'un tercer fiable ni d'un intermediari de preservació (Nakamoto, 2008).

Els resultats de la recerca del projecte InterPARES Trust actual demostren que hi ha una quarta opció basada en els principis de les tecnologies de la cadena de

blocs i de registres distribuïts, és a dir, registrar la validesa de la signatura digital en la cadena de blocs. Explicarem aquest mètode a continuació.

2. CADENA DE BLOCS

Per tal de comprendre com les tecnologies de la cadena de blocs i de registres distribuïts es poden utilitzar en el marc de la gestió de documents, s'explicaran els principis subjacents.

Una cadena de blocs és una base de dades distribuïda de documents (de transacció) que emmagatzema els valors *hash* de les dades, la informació, les transaccions o els documents i està associada al concepte *tecnologia de registres distribuïts* (DLT, per les sigles en anglès). El nom es compon de dos termes: «cadena», que fa referència a la interconnexió dels blocs, i «bloc», referència al conjunt complet de continguts. Aquesta cadena creix linealment i l'encriptació d'un bloc nou, en el context de les criptomonedes, es denomina *mineria*. La cadena de blocs s'executa a través d'una xarxa d'igual a igual en què cada equip connectat (node) emmagatzema dades sobre totes les transaccions (una cadena de blocs no emmagatzema dades, només desa els seus valors *hash*).

Per entendre millor les tecnologies de la cadena de blocs i de registres distribuïts, cal entendre les tecnologies i els conceptes subjacents. Per això, tot seguit explicarem què són els algorismes *hash*, l'arbre de Merkle, el consens distribuït i, en darrer lloc, la cadena de blocs.

2.1. ALGORISMES HASH

La funció *hash*, o resum de missatge, és una funció *unidireccional* que calcula ràpidament una cadena de caràcters de longitud fixa a partir d'una dada, una informació o un document de qualsevol mida. Que sigui unidireccional significa que no és possible recrear el document original encara que se'n sàpiga la funció *hash* i el seu valor. És extremadament difícil i gairebé impossible crear «col·lisions», és a dir, tenir dos o més documents amb sentit amb el mateix valor *hash*. Per això el valor *hash* resultant també s'anomena *empremta digital*. En la figura 1 es mostra un exemple d'un generador de valors *hash* en línia que utilitza les funcions *hash* MD5 i SHA. Si algú rep el fitxer .docx amb el resum d'aquest article i el valor *hash* corresponent, pot generar el *hash* del fitxer rebut i comparar-lo amb

el valor *hash* rebut. Si els dos valors coincideixen, el fitxer no s'ha modificat, és a dir, no s'ha posat en perill la seva integritat.

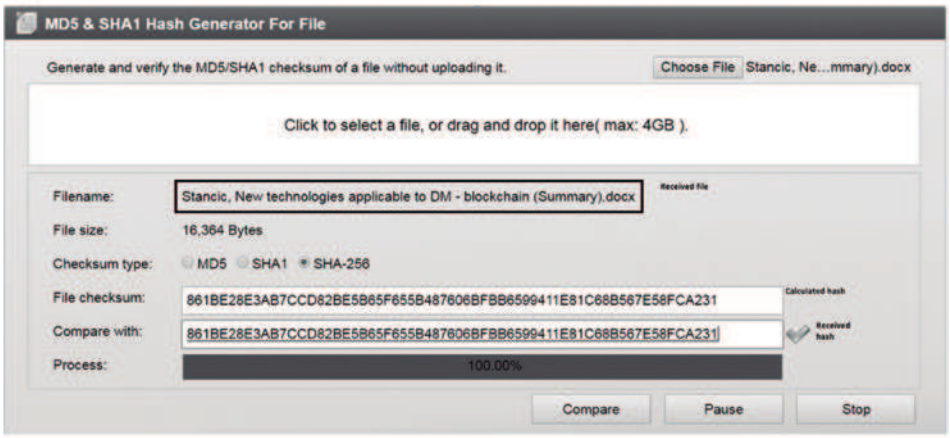

Figura 1. Comparació dels valors *hash* amb el generador de valors *hash* Online MD5, http://onlinemd5.com/

2.2. ARBRE DE MERKLE

Els valors *hash* es poden agrupar per formar un sol *hash*, acció que s'il·lustra en l'exemple següent (figura 2). Una empresa crea una sèrie de documents cada hora. Es calcula un valor *hash* per a cada document. Cada hora tots els valors *hash* de tots els documents s'agrupen i es genera un *hash* «per hora». Al final de la jornada de vuit hores del dilluns, per exemple, els vuit valors *hash* «per hora» s'agrupen i es genera un valor *hash* per al dilluns. Aquest *hash* s'anomena *hash* arrel o *hash* superior. Aquest mètode el va introduir per primera vegada Ralph C. Merkle (Merkle, 1980) l'any 1980. Com que l'estructura sembla un arbre (de cap per avall), es va anomenar arbre de Merkle.

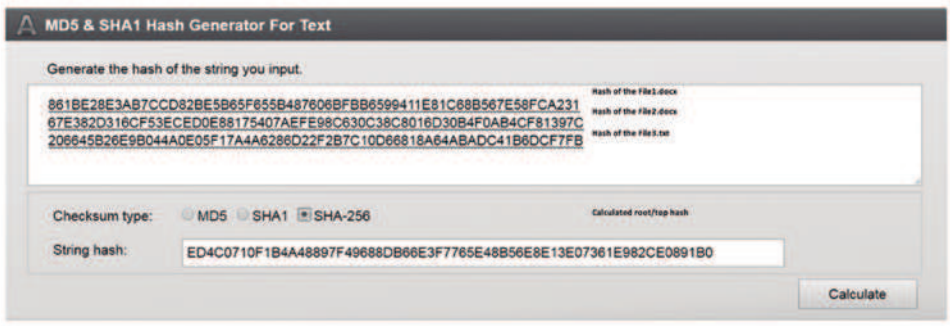

Figura 2. Creació del *hash* arrel/principal

2.3. CONSENS DISTRIBUÏT

La cadena de blocs utilitza una xarxa (d'igual a igual) distribuïda. La xarxa distribuïda no té centre, perquè tots els equips interconnectats reben el mateix tracte. Aquest tipus de xarxa no té un únic punt de control i, per tant, tampoc té un únic punt d'atac. La cadena de blocs utilitza el principi de consens distribuït, en què cada participant (node) fa constar tot el que succeeix al seu registre. El consens es fa servir per garantir que tots els registres són còpies exactes (és a dir, estan sincronitzats) i per determinar la veritat. El succés (per exemple, una transacció monetària o el registre d'un document) només es vàlid si la majoria qualificada (50% + 1 node) coincideix.

2.4. ENCADENAMENT DELS BLOCS

Satoshi Nakamoto va utilitzar el mètode de l'arbre de Merkle per crear el bitcoin, la moneda virtual o criptomoneda (Nakamoto, 2008). El ràpid creixement a escala mundial de la popularitat del bitcoin i altres criptomonedes ha disparat l'interès i l'aplicació de la tecnologia de la cadena de blocs.

La cadena de blocs crea una cadena de blocs vinculats. Ho il·lustrarem ampliant l'exemple en què s'explicava l'arbre de Merkle i que es mostra en la figura 2. L'empresa a què hem fet referència pot repetir el procés de generació de *hash* del dilluns per als documents creats cada hora el dimarts. Amb això s'obtindran dos valors *hash*: un per a cada dia. Aquests valors també es podrien agrupar per crear un únic *hash* superior que agrupi els *hash* del dilluns i el dimarts. Aquest valor *hash* únic es podria combinar amb el valor *hash* del dimecres per crear un altre *hash* superior, etc. Cada *hash* superior nou es calcula a partir del *hash* del dia i el *hash* superior anterior, de manera que els *hash* superiors es vinculen (figura 3). Cada bloc nou rep un segell de temps en el moment de la seva creació, la qual cosa garanteix que els *hash*, és a dir, les dades o els documents, existien en el moment del registre en la cadena de blocs.

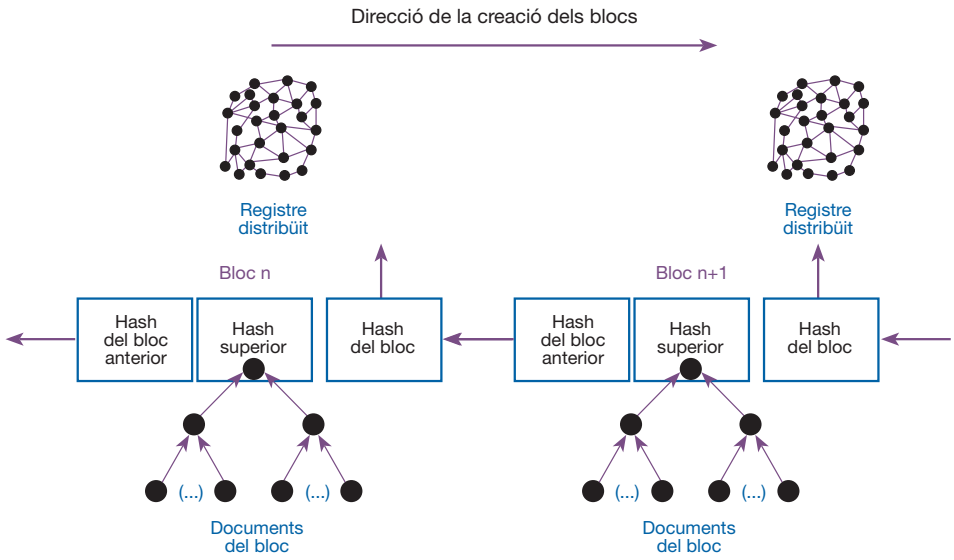

Figura 3. Creació de la cadena de blocs

El concepte de la cadena de blocs té diversos punts forts. Primer de tot, en la cadena de blocs només s'emmagatzemen (es registren) els valors *hash*. Les dades o els documents reals als quals s'assigna un hash s'emmagatzema en els sistemes institucionals de gestió de documents. En segon lloc, cada bloc addicional reforça els anteriors, perquè els blocs s'encadenen i cada bloc nou depèn dels enllaços dels blocs anteriors. I, en darrer lloc, la modificació de qualsevol bloc de la cadena invalida tots els blocs següents.

3. L'ÚS DE LA CADENA DE BLOCS EN LA GESTIÓ DE DOCUMENTS

La gestió de documents digitals millora la productivitat empresarial i l'eficàcia organitzativa. Les funcions de gestió de documents més habituals són la traçabilitat de les versions, els passos de seguiment (on/quan era/és el document) en el procés empresarial, la verificació dels canvis, l'estructura i el contingut dels documents i l'intercanvi simplificat i fiable de documents. La cadena de blocs podria ser útil en diferents aspectes dels processos de gestió de documents. Per exemple, quan es crea una versió nova d'un document, es pot registrar en la cadena de blocs. En fer-ho, com que cada bloc nou de la cadena de blocs rep un segell de temps, queda clar quina versió del document s'ha creat en cada moment i quins canvis s'han fet, es poden traçar i verificar, si cal, l'estructura i el

contingut del document. A més, en l'exercici de l'activitat, sovint els documents s'envien a altres parts. El registre en la cadena de blocs podria oferir les proves necessàries que un document no s'ha manipulat, tal com es mostrava en la figura 1.

D'altra banda, els documents contenen sovint signatures o segells digitals. Un cop esdevenen documents, ja no s'han de modificar; a més, al llarg del procés de gestió de documents i arxiu, han de mantenir intactes l'autenticitat, la integritat, la fiabilitat i la usabilitat i alguns d'ells també han de preservar les característiques de no repudi, seguretat i confidencialitat. El problema, com ja s'ha indicat, és que els certificats utilitzats en les signatures digitals vencen en un període d'entre dos i cinc anys, la qual cosa deixa els conservadors de documents i els arxivers en una situació en què la validesa de les signatures digitals ja no es pot confirmar. En el projecte InterPARES Trust[3] s'està desenvolupant la solució TRUSTER[4] VIP[5] anomenada TrustChain. S'estan investigant les possibilitats d'utilitzar el segellat de temps basat en connexions i la tecnologia de la cadena de blocs per a la preservació a llarg termini de documents signats digitalment. TrustChain és un model basat en la cadena de blocs que es pot utilitzar per registrar la informació relativa a la validesa dels certificats digitals de les signatures digitals de la cadena de blocs en el moment de l'ingrés a l'arxiu dels documents signats o segellats digitalment quan els certificats digitals encara són vàlids. Més endavant, quan el període de validesa dels certificats digitals venç, es pot:

1. Confirmar que el certificat digital era vàlid en el moment de l'ingrés,

2. Confirmar que el document no s'ha modificat (tornant a calcular el valor *hash* i comparant-lo amb el *hash* registrat i el que es troba en la signatura digital),

3. Deduir que quan els punts 1 i 2 són correctes, és com si el certificat digital encara fos vàlid.

El concepte TrustChain es va publicar en la ponència de l'INFuture2017 «A model for long-term preservation of digital signature validity: TrustChain» (Un model per a la preservació a llarg termini de la validesa de les signatures digitals: TrustChain) (Bralić, Kuleš, & Stančić, 2017). Tanmateix, el model encara es troba en una primera fase conceptual i es continuarà desenvolupant.

4. DISCUSSIÓ

Aplicar la cadena de blocs en un procés de gestió de documents no és difícil. Enigio Time[6], un dels investigadors associats del projecte InterPARES Trust que també ha participat en el desenvolupament del model TrustChain, ha desenvolupat un agregador de cadena de blocs (figura 4). El sistema de gestió de documents (DMS, per les sigles en anglès) es connecta a través d'una API[7] a l'agregador de cadena de blocs, que al seu torn registra els valors *hash* de la cadena de blocs. A més, publica els valors *hash* registrats perquè tothom pugui comprovar la integritat del document. Cal insistir que només es registren i publiquen els valors *hash* dels documents i que els documents en si es queden en el DMS. La cadena de blocs no emmagatzema els documents i per això aquest concepte es pot fer servir fins i tot en el cas de documents sensibles o classificats.

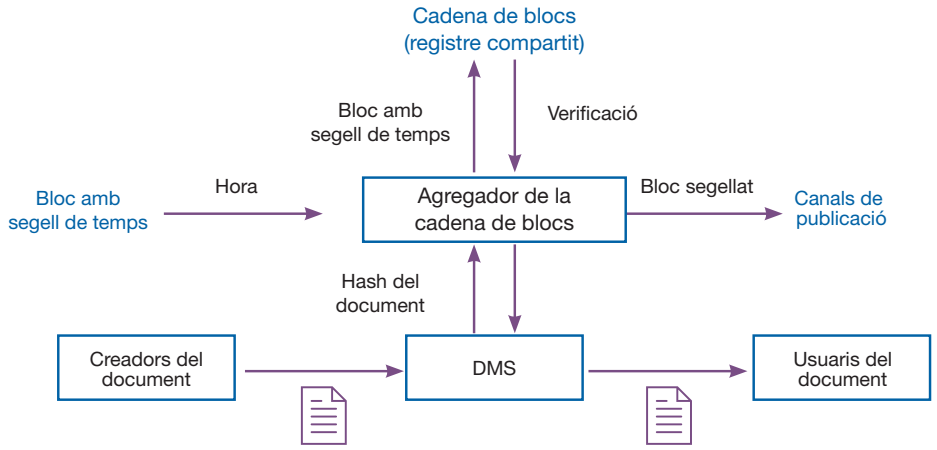

Figura 4. Connexió del DMS a la cadena de blocs amb l'agregador de la cadena de blocs

5. CONCLUSIÓ

«La tecnologia de la cadena de blocs ha captat l'atenció com a base de criptomonedes com el bitcoin, però les seves possibilitats van molt més enllà, ja que permet que les aplicacions tecnològiques existents puguin millorar infinitament i que s'utilitzin aplicacions noves que abans no eren pràctiques. S'espera que la cadena de blocs, també anomenada *tecnologia de registres distribuïts*, revolucioni la indústria i el comerç i fomenti un canvi econòmic a escala mundial perquè és immutable i transparent i redefineix la confiança, ja que fa possibles solucions segures, ràpides, fiables i transparents que poden ser públiques o priva-

des. Podria donar poder a les persones de països en vies de desenvolupament amb identitat reconeguda, propietat d'actius i inclusió financera» (Underwood, 2016). Hi ha moltes aplicacions de la cadena de blocs que podrien transformar la societat. Algunes d'aquestes aplicacions són serveis financers basats en la cadena de blocs, aplicacions de propietat intel·ligent (per exemple, registre de la titularitat dels actius), contractes intel·ligents, aplicacions dels sectors sanitari o musical, certificació notarial, traçabilitat de la procedència, així com aplicacions d'administració en línia (*e-government*) com ara votacions, gestió d'identitats, etc. A més, la cadena de blocs es podria utilitzar per establir la transparència dels governs i la seva comunicació amb els ciutadans.

En el marc de la gestió de documents i tenint en compte totes les característiques de la cadena de blocs així com les tecnologies i els conceptes subjacents, es podria concloure que la cadena de blocs es pot utilitzar per:

- Confirmar la integritat d'un document,

- Confirmar que un document existia o es va crear en un moment determinat (és a dir, no després que se li donés un segell de temps i es registrés en la cadena de blocs),

- Confirmar una seqüència de documents,

- Confirmar/millorar el no repudi d'un document, i

- Millorar les possibilitats de validació dels documents signats digitalment durant la preservació a llarg termini.

6. TREBALL EN EL FUTUR

La cadena de blocs es troba en un procés de normalització accelerada (que va començar l'abril del 2017) per part de l'Organització Internacional de Normalització (ISO/CT 307)[8] amb l'objectiu de fomentar la interoperabilitat i l'intercanvi de dades entre usuaris, aplicacions i sistemes. A més, el CEN i el CENELEC han creat un grup de debat sobre les tecnologies de la cadena de blocs i registres distribuïts per identificar les necessitats específiques de normalització a Europa, per fer encaixar aquestes necessitats (inclosa la governança de la cadena de blocs i la tecnologia de registres distribuïts en el marc del Reglament general de protecció de dades) en els camps d'estudi actuals de l'ISO/CT 307 i fomentar

una major participació europea en aquest comitè tècnic de l'ISO.[9] L'autor ha estat nomenat president del comitè tècnic croat de l'ISO/CT 307 Mirror Technical Committee amb l'Institut Croat de Normalització i treballarà en la normalització de la terminologia de la cadena de blocs com a membre del grup de treball de terminologia de l'ISO/CT 307.

Pel que fa al model TrustChain, en el futur el treball se centrarà en el desenvolupament complet del model i en la creació d'un prototipus que funcioni.

7. RECONEIXEMENTS

La recerca que es presenta en aquest article forma part d'un estudi de recerca més ampli, «Model per a la preservació de la confiabilitat dels documents digitals amb signatura, segell de temps i/o segell digitals (model de preservació TRUSTER)», que forma part del projecte internacional de recerca multidisciplinària InterPARES Trust, http://www.interparestrust.org.

NOTES

1. *Enciclopèdia croata* (Miroslav Krleža Institute of Lexicography, 2017).
2. Els termes *signatura electrònica* i *signatura digital* se solen utilitzar indistintament per referir-se al mateix. No obstant això, en aquest article el terme *signatura electrònica* s'utilitzarà per fer referència a les signatures en què la identitat de la persona signatària no es pugui comprovar, mentre que el terme *signatura digital* s'utilitzarà per fer referència a les signatures en què l'autoritat de certificació (AC) confirmi la identitat de la persona signatària (excepte en les citacions, en què s'emprarà la terminologia original).
3. InterPARES Trust, <http://interparestrust.org>.
4. TRUSTER, model per a la preservació de la confiabilitat dels documents digitals amb signatura, segell de temps i/o segell digitals.
5. VIP, sigles en anglès de preservació de la informació sobre la validesa.
6. Enigio Time, <https://www.enigio.com/>.
7. API, interfície de programació d'aplicacions.
8. ISO/CT 307, <https://www.iso.org/committee/6266604.html>
9. Nou grup de debat del CEN i el CENELEC sobre les tecnologies de la cadena de blocs i registres distribuïts_(DLT), <https://www.cencenelec.eu/news/articles/Pages/AR-2017-012.aspx>

BIBLIOGRAFIA

1. BASE DE DADES TERMINOLÒGIQUES D'InterPARES TRUST. <http://arstweb.clayton.edu/interlex> [Consulta: 28, desembre, 2017].
2. BLANCHETTE, Jean-François. «The Digital Signature Dilemma: To Preserve or Not to Preserve». Annales des Télécommunications. Vol. 61, núm. 7-8 (2006), p. 908-923.
3. BRALIĆ, Vladimir; KULEŠ, Magdalena; STANČIĆ, Hrvoje. «A model for long-term preservation of digital signature validity: TrustChain». Dins: ATANASSOVA, Iana; ZAGHOUANI, Wajdi; KRAGIĆ, Bruno; AAS, Kuldar; STANČIĆ, Hrvoje; SELJAN, Sanja (ed.). INFuture2017: Integrating ICT in Society [en línia]. Zagreb: 2017, p. 89-113. <https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain>.
4. Diccionari de dades per a les metadades de preservació: PREMIS, versió 3.0. 2015.
5. DUMORTIER, Jos; VAN DEN EYNDE, Sofie. Electronic Signatures and Trusted Archival Services [en línia]. <http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf> [Consulta: 15, maig, 2015].
6. HERCEG, Boris; BRZICA, Hrvoje; STANČIĆ, Hrvoje. «Digitally signed records - friend or foe?». Dins: inFuture2015: e-Institutions – Openness, Accessibility and Preservation. Zagreb: Universitat de Zagreb, Facultat d'Humanitats i Ciències Socials, Departament d'Informació i Ciències de la Comunicació, 2015, p. 147. <https://doi.org/10.17234/INFUTURE.2015.18>.
7. MERKLE, Ralph C. «Protocols for public key cryptosystems». Dins: IEEE Symposium on Security and Privacy. Núm. 122 (1980), p. 122-134.
8. NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System [en línia]. (31 d'octubre de 2008). <https://bitcoin.org/bitcoin.pdf> [Consulta: 21, novembre, 2015].
9. ORGANITZACIÓ INTERNACIONAL DE NORMALITZACIÓ. ISO 15489-1:2016 Informació i documentació: Gestió documental. Part 1, Conceptes i principis [en línia]. <https://www.iso.org/standard/62542.html>.
10. PARLAMENT EUROPEU. Reglament (UE) núm. 910/2014. eIDAS [en línia]. <https://www.eid.as/home/>.
11. STANČIĆ, Hrvoje. «Digitization of documents». Dins: 2. i 3. seminar Arhivi, knjižnice, muzeji - Mogućnosti suradnje u okruženju globalne informacijske infrastrukture. Zagreb: Hrvatsko knjižničarsko društvo, 2000, p. 64-70.
12. UNDERWOOD, Sarah. «Blockchain Beyond Bitcoin». Dins: THE ASSOCIATION FOR COMPUTING MACHINERY. Communications of ACM. Núm. 59 (Nova York, EUA, novembre de 2016).
13. What is an electronic seal? [en línia]. <https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-an-electronic-seal> [Consulta: 28, desembre, 2017].

RESUM

La cadena de blocs és una tecnologia relativament nova amb un gran potencial. Tot i que és més coneguda per ser la tecnologia subjacent a les monedes virtuals, pot tenir una gran influència sobre la gestió de documents. Els processos relacionats amb l'empresa i els organismes governamentals, com ara la signatura de contractes, els canvis en el cadastre o les votacions, poden millorar en l'entorn electrònic gràcies a l'ús de la tecnologia de la cadena de blocs. Podria augmentar la fiabilitat de l'intercanvi de documents, d'un nivell relativament insegur i poc fiable a un nivell nou, més segur i fiable. Una altra qüestió que cal tractar és la preservació a llarg termini de documents signats o segellats digitalment. Els certificats d'aquests documents solen vèncer al cap d'un període d'entre dos i cinc anys. Signar-los de nou o tornar a afegir-los un segell de temps pot resultar força complicat, però la cadena de blocs podria resoldre fàcilment aquest problema. Així doncs, l'autor investiga les qüestions identificades, informa de la recerca que s'ha dut a terme en aquestes línies en el marc del projecte internacional InterPARES Trust, explica els mecanismes que hi ha darrere els resultats que la recerca ha obtingut fins ara i suggereix accions que es poden emprendre per aplicar la tecnologia de la cadena de blocs a la gestió de documents.

Paraules clau: gestió de documents, cadena de blocs, signatures digitals, preservació a llarg termini.

RESUMEN

La cadena de bloques —o blockchain en inglés— es una tecnología relativamente nueva con un gran potencial. Aunque es más conocida por ser la tecnología subyacente a las monedas virtuales, puede tener una gran influencia en la gestión de documentos. Los procesos relacionados con las empresas y

los organismos gubernamentales, como la firma de contratos, los cambios en el catastro o las votaciones, pueden mejorar en el entorno electrónico gracias al uso de la tecnología de la cadena de bloques. Podría aumentar la fiabilidad del intercambio de documentos, de un nivel relativamente inseguro y poco fiable a un nivel nuevo, más seguro y fiable. Otra cuestión que debe tratarse es la preservación a largo plazo de documentos firmados o sellados digitalmente. Los certificados de estos documentos suelen vencer al cabo de un periodo de entre dos y cinco años. Firmarlos de nuevo o volver a añadirles un sello de tiempo puede resultar bastante complicado, pero la cadena de bloques podría resolver fácilmente este problema. Así pues, el autor investiga las cuestiones identificadas, informa sobre la investigación que se ha llevado a cabo en esta línea en el marco del proyecto internacional InterPARES Trust, explica los mecanismos que hay detrás de los resultados que la investigación ha obtenido hasta ahora y sugiere acciones que se pueden emprender para aplicar la tecnología de la cadena de bloques en la gestión de documentos.

Palabras clave: gestión de documentos, cadena de bloques, firmas digitales, preservación a largo plazo.

ABSTRACT

Blockchain is a relatively new technology with great potential. Although it is best known as the underlying technology of cryptocurrencies, it may have a profound influence on document and records management. Business and government-related processes, such as signing contracts, land registry changes, or voting, can be improved in the electronic environment by the use of blockchain technology. It could raise the reliability of exchanging documents and records from a relatively insecure and untrusted level to a new, more secure and trusted degree. Another issue to be discussed is the long-term preservation of digitally signed or digitally sealed documents. Their certificates usually expire in two to five years. Re-signing or re-timestamping them might prove to be rather complicated, while the use of blockchain could solve this problem easily. Thus, the author investigates the identified issues, reports on the

research carried out along these lines at the international project InterPARES Trust, explains the mechanisms behind the research results achieved so far, and proposes actions that may be taken to implement blockchain technology in document and records management.

Keywords: document management, records management, blockchain, digital signatures, long-term preservation.

RESUMÉ

La technologie de chaînes de blocs (blockchain) est relativement récente, mais elle présente un fort potentiel. Mieux connue comme la technologie permettant l'usage des cybermonnaies, elle pourrait influencer profondément la gestion des documents et des archives. Dans le monde numérique, les processus indispensables aux entreprises et aux administrations, comme la signature de contrats, les modifications d'enregistrement d'actes ou le vote peuvent être améliorés grâce à la technologie des chaînes de blocs. Cette dernière pourrait augmenter la fiabilité des échanges de documents et d'archives d'un contexte relativement peu sûr et peu fiable à un nouvel environnement, plus sécurisé et digne de confiance. Il convient également d'aborder la question de la conservation à long terme des documents signés ou cachetés numériquement. Leurs certificats expirent généralement au terme de deux à cinq années. Le renouvellement des signatures ou des cachets correspondants risque d'être très difficile, alors que les technologies de chaînes de blocs pourraient aisément résoudre ce problème. L'auteur étudie donc les problèmes identifiés, synthétise les recherches menées dans ce domaine par le programme international de l'InterPARES Trust, explique les mécanismes ayant conduit aux résultats obtenus et suggère des mesures qui pourraient permettre d'appliquer des technologies de chaînes de blocs à la gestion des documents et archives.

Mots clés : gestion des documents, gestion des archives, chaîne de blocs, blockchain, signatures numériques, conservation à long terme
esolution of the digitization and the final degree of enlargement.