Uitgave van de Koninklijke Vereniging van Archivarissen in Nederland

archievenblad

sinds 1892 jaargang 121 2017

10

Blockchains en archivering

Geert-Jan van Bussel ■

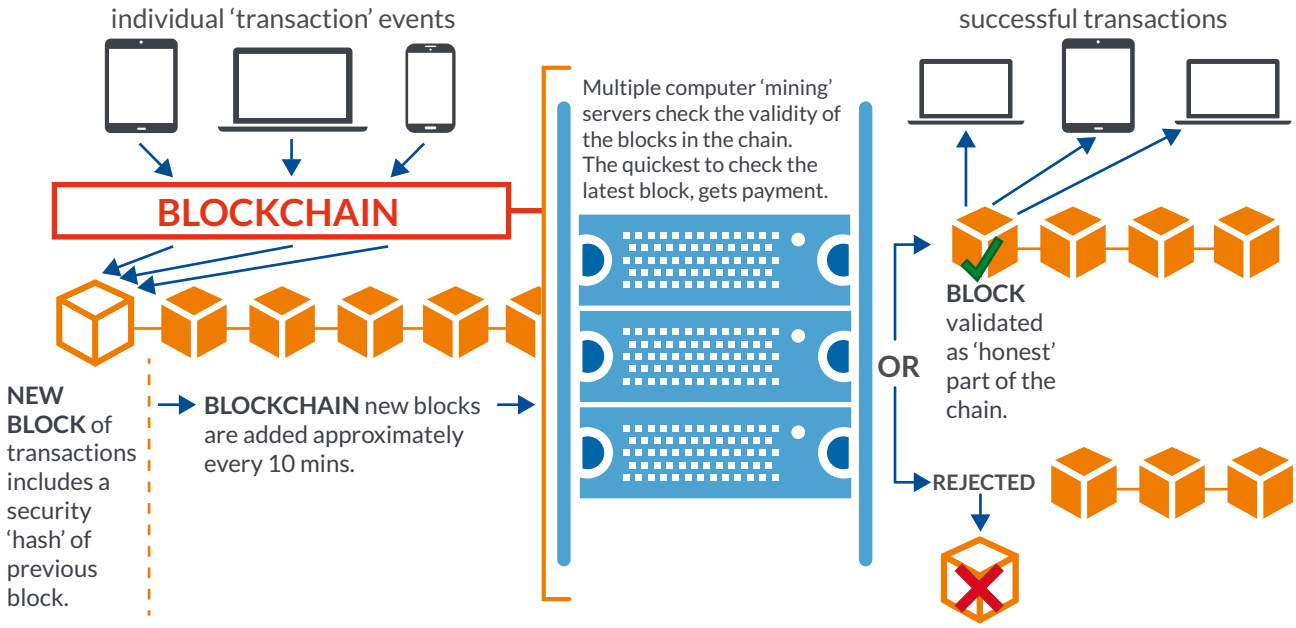
Rond 2008 werd de blockchain bedacht als een van de antwoorden op het wegvallen van het vertrouwen in de banken als bemiddelaars in financiële transacties. Het is bedacht om betalingen te verrichten met bitcoins, een alternatieve munt die zonder tussenkomst van banken wordt gebruikt. In hoeverre kan de blockchain gebruikt worden in archivering?

Foto: Sjoerd Knibbeler.

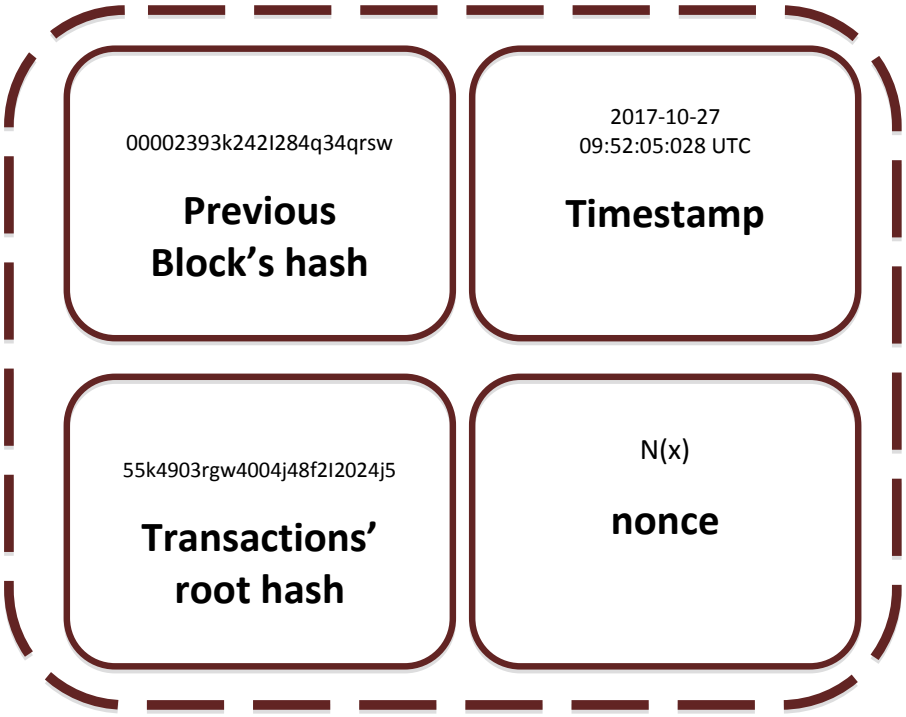
De bitcoin is, net als de achterliggende blockchaintechnologie, een uitvinding van een zekere Satoshi Nakamoto, vastgelegd in een paper in 2008.[1] Het is niet duidelijk wie (of welke groep) dat is. Nakamoto bracht in januari 2009 de eerste bitcoin-software uit en vanaf dat moment is de bitcoin een echte munt. Er zijn diverse pogingen in het werk gesteld om Nakamoto's identiteit te achterhalen, maar zonder succes.[2] Het daadwerkelijke succes van bitcoin kan worden betwijfeld, maar dat kan niet worden gezegd van de blockchaintechnologie die de bitcoin mogelijk maakte.

Wat is een blockchain?

Simpel gezegd is de blockchain een database (een register, 'ledger') waarin meerdere, wereldwijd verspreide computers samenwerken om versleutelde blokken data ('blocks') op te slaan. Elk nieuw blok bevat via versleutelde coderingen ('hashes') ook de codering van het blok ervoor. Zo ontstaat een keten ('chain') met (idealiter) volledige en onmuteerbare data. Bij de bitcoin is deze database publiek toegankelijk. De essentie van de technologie is dat data decentraal wordt bewaard,



Figuur 1. Blockchain (The Open University, graphic design by Harriet Cornish, http://blockchain.open.ac.uk/).



Figuur 2. De opbouw van een Blok.

authentiek en integer is en niet kan worden gemuteerd. Blockchain is niets anders dan een mechanisme dat de authenticiteit en integriteit van transacties geautomatiseerd waarborgt. Figuur 1 geeft het blockchainproces grafisch weer.

Een korte uitleg van het proces zoals opgenomen in figuur 1. Individuele gebruikers leggen data vast over een transactie, een betaling, een levering of een contract. Alle gegevens die noodzakelijk zijn voor die transactie (de betrokken partijen, het subject, eventuele links naar voor de transactie noodzakelijke documenten) worden vastgelegd. Dit 'databaserecord' (want in essentie is het niet anders!) wordt voorzien van een cryptografische sleutel die de ingegeven inhoud authentiseert en onmuteerbaar maakt (de transactie-hash). De transactie wordt door alle partijen in de keten automatisch gecontroleerd, waardoor vertrouwde tussenpersonen die transacties bewaken, niet langer nodig zijn. Indien goedgekeurd wordt het 'databaserecord' uiteindelijk, samen met andere goedgekeurde transacties, verzameld in een Blok. In zo'n Blok worden de transacties van de afgelopen tien minuten gecombineerd. Het Blok wordt voorzien van een 'timestamp', waardoor de exacte tijd van vastlegging wordt gedocumenteerd, en een daaraan gekoppelde 'nonce', een unieke, gecodeerde en versleutelde waarde (de Blok-hash, een soort digitale handtekening). Om de plek van het Blok in de keten van blokken te verankeren, wordt ook de Blok-hash van het voorgaande Blok opgenomen. Figuur 2 laat zien hoe zo'n Blok eruitziet.

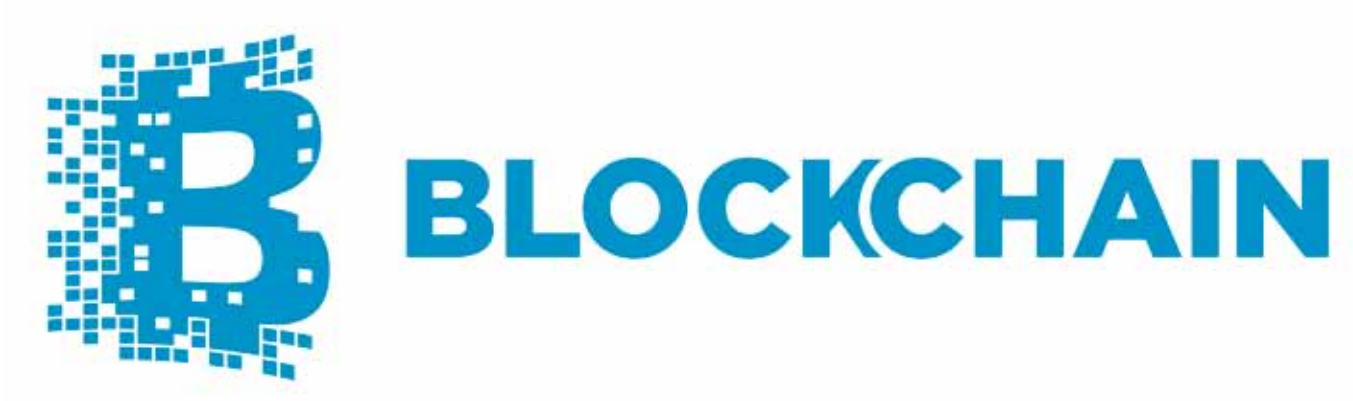
Als het Blok is aangemaakt, wordt de validiteit ervan door gedistribueerde 'mining servers' gecontroleerd. Wanneer de validiteit vaststaat, wordt het Blok definitief aan de Blockchain toegevoegd. De 'databaserecords' zijn dan toegevoegd aan de 'ledger', het register, waardoor de transacties altijd toegankelijk en vindbaar zijn.[3]

Voordelen

Blockchaintechnologie is bedoeld om transacties te faciliteren tussen mensen en organisaties die elkaar *niet kennen* en *niet (hoeven te) vertrouwen* zonder een betrouwbare intermediair. Dat is ook het cruciale kenmerk van de blockchain: technologie gebruiken als intermediair en waarborg voor betrouwbaarheid. In de meeste publicaties, onderzoeks- en adviesrapporten, worden vele andere voordelen benadrukt, zoals het feit dat:

- het vele malen moeilijker wordt voor hackers om het hele systeem te manipuleren en 'plat te leggen';
- het wegvallen van een of meerdere computers niet betekent dat de gedistribueerde keten faalt;
- alle transacties volledig transparant, controleerbaar, betrouwbaar en raadpleegbaar zijn;
- het publieke register ervoor zorgt dat de historiciteit van de data is gewaarborgd;
- en de kosten voor transacties door het wegvallen van de intermediairs lager worden.

Die voordelen hebben ervoor gezorgd dat de technologie een enorme ontwikkeling heeft doorgemaakt en de belangstelling aanzienlijk is toegenomen. De Nederlandse overheid en semioverheid participeert (of initieert) bijvoorbeeld al in ongeveer 25 pilots, waaronder pilots bij de Kamer van Koophandel, het Kadaster, de Raad voor de Rechtsbijstand, De Nederlandse Bank, de ministeries van Buitenlandse Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Financiën en Veiligheid en Justitie, de Algemene Rekenkamer, de Belastingdienst, de Inspectie Leefomgeving en Transport, het Zorginstituut Nederland en de Dienst voor Registers. Daarnaast zijn diverse provinciale en gemeentelijke organen blockchaintechnologie aan het testen in het kader van onder andere de Omgevingswet. Ook hebben vele financiële instellingen pilots en implementaties van blockchaintechnologie ondernomen. >>



Haarlemmerolie

Het is opvallend dat vele van deze pilot- en implementatie-projecten uitgevoerd worden door partijen die als intermediair kunnen worden aangemerkt. Het doel waarvoor de blockchain-technologie primair bedoeld was, het uitschakelen van de intermediair, komt hierdoor op de achtergrond. Het zijn de andere genoemde voordelen die het doen lijken alsof de technologie Haarlemmerolie is voor een groot aantal heden-daagse problemen die te maken hebben met beveiliging, authenticatie, cybercrime en de authenticiteit en integriteit van data. In de meeste pilots kennen de ketenpartners elkaar en weten ze dat ze elkaar over het algemeen kunnen vertrouwen, waardoor de toepassing van de technologie een totaal ander karakter krijgt dan oorspronkelijk bedoeld. Het tweede cruciale kenmerk van de blockchain, transacties faciliteren tussen partijen die elkaar niet kennen en niet vertrouwen, verdwijnt daardoor naar de achtergrond.

Blockchain en archivering

Eind 2016 publiceerde Victoria Lemieux, associate professor aan de University of British Columbia in Vancouver, een artikel over 'trusted records' en de rol van blockchaintechnologie.[4] Lemieux plaatst een aantal kanttekeningen bij de genoemde voordelen van de blockchain vanuit het gezichtspunt van betrouwbaar recordsmanagement. Op basis van een case inzake de registratie van kadastrale gegevens in Honduras ging ze in op de kwets-baarheden van de publieke blockchaintechnologie. Zo is het mogelijk dat hackers de keten manipuleren en muteren, kunnen timestamps worden gemanipuleerd door de kloktijd te vertragen of versnellen, kan malware de controle over de keten over-nemen en kunnen er problemen ontstaan in het managen van de nonces. Deze problemen kunnen worden beperkt wanneer de technologie niet met een publiek register werkt, maar met een meer beperkte, afgesloten en 'private' variant. Dat schuift echter een derde cruciaal kenmerk van de blockchaintechnologie terzijde. Veel van de Nederlandse pilots werken met een dergelijke 'private' blockchain.

In relatie tot recordsmanagement zijn er een aantal andere belangrijke overwegingen te maken. Een blockchain is gericht op transacties die in data te vervatten zijn. Het zijn net, zoals eerder aangegeven, records in een database. Het is niet bedoeld voor het opnemen van objecten, zoals pdf's, tiff's en andersoortige veel voorkomende bestandsformaten. Het zou wel kunnen om Binary Large Objects (BLOB's) op te nemen, maar er is geen enkele blockchaintoepassing die dat ook daadwerkelijk doet. Kostenoverwegingen zijn daarvoor bepalend. Oplossingen als Storj (https://storj.io/) en Filecoin (https://filecoin.io/) zijn Dropbox-, Box- of Hubic-alternatieven gebaseerd op de blockchain, maar ook zij slaan de objecten niet op in de keten zelf. Ze maken gebruik van opslagruimte ter beschikking gesteld door gebruikers of datacenters. In de blockchain worden enkel hashes van de (wel of niet versleutelde) objecten opgenomen. Deze kunnen de integriteit van de op andere plekken opgeslagen documenten verifiëren, maar ze kunnen niet garanderen dat de objecten altijd beschikbaar blijven. Als deze objecten onderdeel uitmaken van de transactie (wat tot nu toe bijna altijd het geval is), dan kan een dergelijke opslag van bestanden niet als een 'trusted digital repository' worden aangemerkt.

Opslag en vernietiging

Een blockchain is onmuteerbaar. Dat impliceert ook dat de in een blockchain opgenomen data niet vernietigd kunnen worden, waardoor de wettelijke verplichting tot vernietiging niet kan worden uitgevoerd. Ook al zouden de verbonden objecten wel kunnen worden verwijderd, de contextuele data van de transactie in de blockchain blijven bestaan. Er wordt onderzoek gedaan naar de mogelijkheden om een redigeerbare blockchain te creëren, maar of dergelijke grootschalige vernietigingsoperaties kunnen worden uitgevoerd is nog maar zeer de vraag.[5] Vernietiging van de data breekt de blockchain, net zoals het verwijderen van de objecten van de opslagmedia waarop ze zijn opgeslagen. In beide gevallen is dan een vergelijking van de hashes van de 'originelen' en de blockchain niet langer mogelijk.

De wijze van opslag van objecten die gekoppeld zijn aan de blockchain (en dat kunnen er heel veel zijn!) dient op een verantwoorde en gecontroleerde wijze plaats te vinden. Ze dienen namelijk om volledig inzicht te krijgen in de transacties en de objecten (of dossiers) die daar onderdeel van zijn. Die objecten zijn immers (net als de data over de transactie vast-gelegd in de blockchain) 'records', archiefstukken. Ze zijn ook nodig om de hashes in de blockchain te laten controleren of de objecten 'zijn gebleven zoals ze zijn vastgelegd'. Dat vereist de aanwezigheid van digitale archieven, bewaarstrategieën en de inrichting van een technische infrastructuur die de blijvende toegankelijkheid van die objecten regelt. De opslag van die objecten vindt in die omgeving contextueel plaats. Iets wat een blockchain ook niet of nauwelijks doet.

Nut

Dat alles doet de vraag rijzen wat het nut van die blockchain is. Met de technologie zelf is weinig mis. Voor recordsmanagement is een 'private blockchain' nodig, maar in de meeste toepassingen is dat al standaard. Er is dan beperkte toegang tot de block-chain, bijvoorbeeld door de partners in een ketenorganisatie. De

blockchain dient als een contextueel (meta)datasysteem, een absoluut betrouwbaar register van handelingen en transacties. Als er wordt gewerkt met zaken, dossiers of andere opslagmethodieken voor objecten, dan moeten er voorzieningen zijn voor het behoud daarvan. Denk bijvoorbeeld aan een koppeling met een zaaksysteem of applicaties voor recordsmanagement of een e-depot. Bij de meeste experimenten met blockchaintechnologie is hiervan op dit moment geen sprake.[6] Vooral het feit dat objecten duurzaam moeten worden bewaard, zal (in eerste instantie) niet leiden tot kostenvermindering.

Doel?

De vraag wat het doel van de blockchain is, wordt te weinig gesteld. Zeker omdat de drie cruciale kenmerken van de blockchaintechnologie (publiek, geen intermediair, onbekende en niet vertrouwde partners) in de meeste pilots niet worden ingevuld, is dat een belangrijke vraag. Traditionele databasetechnologie is namelijk over het algemeen sneller, heeft een betere performance en is meer schaalbaar. De vraag waarom de technologie wordt gebruikt dient dan ook meer te worden gesteld, zeker omdat privacy in een blockchain niet kan worden gewaarborgd (verwijdering van persoonsgegevens bijvoorbeeld). De Algemene verordening persoonsgegevens dient dan ook de leidraad te zijn bij het gebruik van de technologie.

Een blockchain is niet bedacht als een tool voor recordsmanagement. Het kan als zodanig worden gebruikt als er geen objecten hoeven te worden vastgelegd, als we overgaan tot het uitbannen van ongestructureerde informatieobjecten in ons werk en als we bereid zijn alleen maar te werken met gestructureerde data. Anders zullen altijd aanvullende applicaties nodig zijn voor het duurzaam beheer van objecten. Dit alles staat overigens los van de vraag of die blockchain zelf behouden kan worden.

Stof tot nadenken

Blockchaintechnologie is een disruptieve ontwikkeling die stof tot nadenken geeft en vele mogelijkheden biedt. Het is geen tool voor recordsmanagement, maar zou op dit moment in een archiveringsomgeving kunnen worden gebruikt als het wordt gecombineerd met zaaksystemen, recordsmanagementapplicaties of e-depots. De gezamenlijke Nederlandse archiefdiensten zouden een blockchain kunnen inzetten als het openbare metadatasysteem van al hun archieven, waarin alle beschrijvingen zitten van de digitale archieven in hun e-depots. Waarbij dan wel onmiddellijk de vraag moet worden gesteld of dat niet op een andere, effectievere manier te realiseren is... ■

Noten

1 ■ S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Online bron. 17 oktober 2008. Geraadpleegd op 23 oktober 2017 van https://bitcoin.org/bitcoin.pdf.

2 ■ A. Greenberg, G. Branwen, 'Bitcoin's creator Satoshi Nakamoto is probably this unknown Australian genius.' Online bron. 12 augustus 2015. Geraadpleegd op 23 oktober 2017 van https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/; A. Greenberg, 'New clues suggest Craig Wright, suspected Bitcoin creator, may be a hoaxer'. Online bron. 12 november 2015. Geraadpleegd op 23 oktober 2017 van https://www.wired.com/2015/12/new-clues-suggest-satoshi-suspect-craig-wright-may-be-a-hoaxer/

3 ■ Er zijn boeken die de blockchain op een toegankelijke wijze introduceren: D. Drescher, *Blockchain Basics. A Non-Technical Introduction in 25 Steps* (Apress, 2017); T. Laurence, Blockchain for Dummies (John Wiley & Sons, 2017); W. Mougayar, *The Business Blockchain. Promise, Practice and Application of the Next Internet Technology* (John Wiley & Sons, 2016). Ook in het Nederlands zijn er goede introducties: S. Vermeend en P. Smit, *Blockchain, de technologie die de wereld radicaal verandert,* (Vrije Uitgevers, 2017) en P. Bessems, *Blockchain organiseren. Fundamenten voor een nieuwe sociaaleconomische orde* (MijnManagementboek.nl, 2017).

4 ■ V. Lemieux, 'Trusting records: is Blockchain technology the answer?', *Records Management Journal*, Vol. 26, No. 2, pp. 110-139, https://doi.org/10.1108/RMJ-12-2015-0042.

5 ■ G. Ateniese, B. Magri, D. Venturi, en E. Andrade, 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends', *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, Parijs, April 26-28, 2017, pp. 111-126. Voor een online versie: https://eprint.iacr.org/2016/757.pdf (deze PDF betreft een uitgebreidere versie dan de gepubliceerde versie).

6 ■ Voor wat betreft het behouden van contextuele relaties wordt onderzoek gedaan. Te noemen is: V.L. Lemieux, M. Sporny, '*Preserving the Archival Bond in Distributed Ledgers: A Data Model and Syntax', Proceedings of the 26th International Conference on World Wide Web Companion*, Perth, Australia, April 3-7, 2017, pp. 1437-1443,

Geert-Jan van Bussel ■ directeur van Van Bussel Document Services te Helmond en docent-onderzoeker aan de Hogeschool en Universiteit van Amsterdam.