Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie
ISSN: (Online) 2222-4173, (Print) 0254-3486

Trouelose oorsprongverifikasie van elektroniese intellektuele eiendom deur middel van blokskakeltegnologie ("blockchain technology")

Authors:
Riaan Bezuidenhout,
W Nel,
AJ Burger

Affiliasie:
Departement Rekenaarwetenskap en Informatika, Universiteit van die Vrystaat
Posbus 339, Bloemfontein, 9300

Korresponderende outeur:
R Bezuidenhout
E-pos: rbez@mweb.co.za

Hoe om hierdie artikel aan te haal:
Riaan Bezuidenhout, W Nel, AJ Burger, Trouelose oorsprongverifikasie van elektroniese intellektuele eiendom deur middel van blokskakeltegnologie ("blockchain technology"), *Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie* 38(1) (2019). https://doi.org/10.36303/SATNT.2019.38.1.759

A blockchain application for the trustless provenance verification of electronic intellectual property: This study will develop a prototype blockchain application for a trustless provenance verification of electronic intellectual property. The goal is to develop a system through which the owner of intellectual property can store the proof of ownership of an electronic artefact, publicly, on a specific date.

Komplekse transaksies tussen vreemde partye vind daagliks in die moderne wêreldekonomie plaas. Aangesien die afwesigheid van vertroue 'n struikelblok vir handel is, noodsaak dit meganismes om vertroue tussen partye te bewerkstellig, wat gelei het tot die ontwikkeling van vertrouensinstansies soos banke en versekeringsmaatskappye (Warburg 2016). Wanneer vertrouensinstansies faal, kan dit tot groot ontwrigting in wêreldekonomieë lei. In reaksie hierop het Nakamoto (2008) 'n metode vir trouelose elektroniese kontant (Bitcoin) ontwikkel. Hierdie tegnologie kan ook toegepas word waar 'n derde party die integriteit van 'n stel feite waarborg (Nomura Research Institute 2016).

Blokskakelstelsels span twee kriptografiese komponente, naamlik elektroniese handtekeninge en hutsbeelde ("message digests") in, om die integriteit en geskiedenis van alle transaksies in 'n blokskakel te waarborg. Hierdie blokskakel word openbaar gemaak en kan deur enige persoon gelees word. 'n Poging om inligting in die blokskakel te verander, sal onmiddellik deur die kriptografiese veiligheidsmaatreëls ontbloot word (Buterin 2013).

Inligting word by die blokskakel in die vorm van 'n transaksie gevoeg. Hierdie transaksie word elektronies deur die eienaar onderteken (Paar & Petzl 2010) en na 'n eweknienetwerk van kriptoverwerkers ("miners") gestuur (Nakamoto 2008). Enige onafhanklike persoon kan nou die eienaar van die transaksie bevestig. Die netwerk van kriptoverwerkers voeg nuwe transaksies in blokke aan die einde van die blokskakel by (Nakamoto 2008). Elke blok transaksies word gekoppel aan die volgende een deur middel van 'n kriptografiese verwysing (hutsbeeld) (Paar & Petzl 2010). Indien enige transaksie-inhoud verander word, of 'n blok transaksies uit die blokskakel verwyder word, stort hierdie ketting van verwysings in duie, wat daarop dui dat met die inhoud van die blokskakel gepeuter is (Buterin 2013). Die netwerk van kriptoverwerkers weier om ongeldige blokskakels aan te vul en kom onderling ooreen dat die langste geldige blokskakel die enigste geldige weergawe van die feite voorstel. Die sekerheid van ouer transaksies versterk in so 'n mate dat daar 'n statisties onbeduidende kans is dat iemand daarmee kan peuter (Nakamoto 2008).

Indien 'n outeur 'n elektroniese artefak (dokument, sagteware, ensovoorts) skep, kan die vraag ontstaan: "Hoe kan die outeur sy inligting in die openbaar bekend maak en ter enige tyd bewys dat die artefak, sedert 'n sekere datum, in sy besit was?" Hierdie navorsingsprojek is daarop gerig om 'n prototipestelsel te ontwikkel waar 'n outeur die elektroniese artefak op 'n blokskakel kan laai en waarmee die oorsprong van die artefak enige tyd geverifieer kan word. Dit word gedoen deurdat die outeur 'n transaksie skep wat uit sy/haar persoonlike besonderhede, sowel as die artefak, bestaan. Deur die transaksie elektronies met sy/haar privaatsleutel te onderteken, kan bewys word dat slegs die outeur die transaksie kon saamstel asook wat die presiese inhoud van die transaksie was. Deur die transaksie in 'n pasgemaakte

Nota: 'n Seleksie van referaatopsommings: Studentesimposium in die Natuurwetenskappe, 25–26 Oktober 2018, SA Akademiegebou, Pretoria, Suid-Afrika. Gasredakteurs: Prof Rudi Pretorius (Departement Geografie, Universiteit van Suid-Afrika); Prof Chris Swanepoel (Departement Besluitkunde, Universiteit van Suid-Afrika); Me Andrea Lombard (Departement Geografie, Universiteit van Suid-Afrika)

blokskakel op te neem, kan die tydstip van byvoeging bewys word én dat dit nie sedertdien verander is nie.

Literatuurverwysings

Buterin, V., 2013, *Etherium: A next generation smart contract and decentralized application platform*. Beskikbaar by: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdfhttp://eth [Toegang op 15 November 2019].

Nakamoto, S., 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System.* Beskikbaar by: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986 [Toegang op 15 November 2019].

Nomura Research Institute, 2016, *Survey on Blockchain Technologies and Related Services FY2015 Report.* Beskikbaar by: https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf [Toegang op 15 November 2019].

Paar, C. & Petzl, J., 2010, *Understanding Cryptography,* Heidelberg: Springer.

Warburg, B., 2016, *How the blockchain will radically transform the economy*. Beskikbaar by: https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy [Toegang op 15 November 2019].