Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie 2024; 43(1):158
South African Journal for Science and Technology 2024; 43(1):158
https://doi.org/10.36303/SATNT.2024.43.1.1429

SATNT / SAJST
ISSN: 2222-4173 EISSN: 0254-3486

REFERAATOPSOMMING

Blokskakel fluitjieblaserstelsel

R Krause, W Nel, RC Fouché

Departement Rekenaarwetenskap en Informatika, Universiteit van die Vrystaat, Suid-Afrika
Korresponderende outeur: *Ricus Krause* ***E-pos:*** *ricuskrause@gmail.com*

Blockchain whistleblower system: The project can be divided into two main components: Firstly, the blockchain itself as a foundation of immutability, non-repudiation and accessibility. Secondly, a whistleblower program built on blockchain technology enables users to anonymously report an incident and contact investigators while keeping their identities hidden.

Fluitjieblasers ontbloot vertoulike inligting oor misdaad en wangedrag in 'n organisasie. Fluitjieblasers neem egter 'n groot risiko deurdat hulle identiteite dikwels bekend gemaak word voordat dit veilig is om so te doen (Kleinig, 2022). 'n Fluitjieblaser kan sy/haar onderhandelingsmag verloor wanneer bewyse van die misdaad verlore raak en hulle self ook as teikens beskou magword (Ngema, 2018). Die fluitjieblaserstelsels wat tans in Suid-Afrika in plek is beskerm nie die informant nadat sy/haar identiteit bekend gemaak is nie, en sodoende kan sy/haar lewe in gevaar gestel word (Nortje, 2023). Om die ooglopende tekortkominge van huidige stelsels op te los, is dit nodig om 'n rekenaarstelsel te ontwikkel waarin die anonimiteit van 'n fluitjieblaser die eerste prioriteit is.

Blokskakeltegnologie is gebou op die fondasie van onveranderbaarheid, nie-ontkenning en toeganklikheid, wat dit in staat stel om 'n onkwesbare struktuur te vorm, wat veilig vir fluitjieblasers is. Blokskakeltegnologie maak gebruik van 'n drievoudige benadering tot sekuriteit, naamlik, die beskerming van data-eienaarskap, data-integriteit en oortolligheid (Tasca & Tessone, 2019). Nuwe transaksies word in 'n blok gestoor, waarna die nuwe blok aan die einde van die blokskakel gevoeg word. Elke blok word aan die vorige blok gekoppel deur te verwys na daardie blok se kriptografiese hutsbeeld.

Indien daar 'n verandering in 'n vorige blok se inhoud gemaak word, sal al die volgende blokke se hutsbeelde ook verander. Wanneer hierdie weergawe van die blokskakel vergelyk word met die ander weergawes in die eweknienetwerk ("P2P"), sal dit as foutief beskou en nie aanvaar word deur die ander kriptoverwerkers wat deel van die stelsel vorm nie. Die kriptoverwerkers kom ooreen om die langste geldige weergawe van die blokskakel te aanvaar, wat dit byna onmoontlik maak vir een kwaadwillige entiteit om 'n verstelling van feite in die blokskakel te bewerkstellig (Nakamoto, 2008).

Die blokskakel fluitjieblaserstelsel maak dit moontlik vir informante om kennis te gee van die bewyse van misdaad in hul besit. 'n Vaste lengte hutsbeeld word geskep deur die bewysstukke (dokumente) in 'n hutsbeeldalgoritme te verwerk. 'n Beskrywing van die bewyse word deur informante voorsien, sonder om hulle identiteit te openbaar. Hierdie beskrywing word saam met die bewysstukhutsbeeld as 'n transaksie op die blokskakel gestoor. Wanneer die bewyse oorhandig word, kan ondersoekers die bewyse deur die hutsbeeldalgoritme verwerk om die integriteit van die bewyse te bevestig. Die bewyse is geldig indien die hutsbeeld identies is aan die bewysstukhutsbeeld wat deur die informant op die blokskakel geplaas was.

Fluitjieblasers moet in staat wees om met die nodige partye te kommunikeer sonder om hulle identiteit te openbaar. Die blokskakel fluitjieblaserstelsel pas kriptografiese metodes toe om kommunikasie tussen informante en ondersoekers te beveilig. Simmetriese enkripsie deur middel van 'n geheime sleutel word gebruik om boodskappe teen ongemagtigde toegang te beskerm. Asimmetriese enkripsie word dan gebruik om die geheime sleutel te teken met albei partye se publieke sleutels (wat deel van hul blokskakeladres vorm). Die boodskap kan sodoende net ontbloot word deur die korrekte privaat sleutels van die betrokke partye te gebruik, wat slegs op hul plaaslike stelsels gevind kan word.

Verwysings

Kleinig, J., 2022, Whistleblower | Definition, Laws, Protection, & Facts | Britannica. Beskikbaar by: https://www.britannica.com/topic/whistleblower. Toegang: 17 Julie 2023.
Nakamoto, S., 2008, Bitcoin: A peer-to-peer electronic cash system. Beskikbaar by: https://www.bitcoin.org. Toegang: 17 Julie 2023.
Ngema, T., 2018, Police dockets go missing. Beskikbaar by: https://www.iol.co.za/dailynews/news/police-dockets-go-missing-16065489. Toegang: 17 Julie 2023.
Nortje, J.G.J., 2023, The protection of whistleblowers in South African criminal cases, *Journal of Financial Crime* 30(6), 1444-1457. https://doi.org/10.1108/JFC-09-2022-0234.
Tasca, P., Tessone, C.J., 2019., A taxonomy of blockchain technologies: Principles of identification and classification, *Ledger* 4. https://doi.org/10.5195/ledger.2019.140.

Nota: 'n Seleksie van referaatopsommings: Studentesimposium in die Natuurwetenskappe, 23-24 Oktober 2023, Universiteit van Pretoria. Reëlingskomitee: Prof Rudi Pretorius (Departement Geografie, Universiteit van Suid-Afrika); Dr Hertzog Bisset (Suid-Afrikaanse Kernenergie-korporasie); Dr Jean van Laar (Sentrum vir Navorsing en Voortgesette Ingenieursontwikkeling, Noordwes-Universiteit); Prof Marilé Landman, Dr Danie Pienaar en Dr Frikkie Malan (Departement Chemie, Universiteit van Pretoria); Mnr JW Hurter (Departement Plant- en Grondwetenskappe, Universiteit van Pretoria).