Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie 2022; 41(1):115
South African Journal for Science and Technology 2022; 41(1):115
https://doi.org/10.36303/SATNT.2022.41.1.939
Open Access article distributed under the terms of the
Creative Commons License [CC BY-NC 3.0]
http://creativecommons.org/licenses/by-nc/3.0

SATNT / SAJST
ISSN: 2222-4173 EISSN: 0254-3486
© 2022 The Author(s)
REFERAATOPSOMMING

'n Ondersteunende stelsel vir die toets van konsensus-algoritmes

JDP Bothma, W Nel, RC Fouché

Departement Rekenaarwetenskap en Informatika, Universiteit van die Vrystaat, Suid-Afrika
***Korresponderende outeur:** J Bothma **E-pos**: johandrebothma@gmail.com*

A support system for the test of consensus algorithms: The project is twofold: The first part consists of an analyser for identifying and extracting sections of the Bitcoin blockchain suitable for testing new algorithms. The second part is a pseudo-random number generator utilising data within the Bitcoin blockchain for use by a newly developed nonlinear proof-of-work algorithm.

Bitcoin is 'n populêre digitale geldeenheid met 'n markaandeel van ongeveer 40% en 'n markkapitalisasie van R5.4 biljoen gemeet in November 2022 (CoinMarketCap, 2022). Bitcoin rus op drie pilare: die blokskakeldatastruktuur, 'n eweknienetwerk ('P2P') en die Bewys-van-Werk- (BvW) konsensusalgoritme. Hierdie konsensusalgoritme het egter aansienlike tekortkominge waarvan hoë energieverbruik slegs een is. Die wye reeks moontlike toepassings van die onderliggende tegnologie van Bitcoin dryf konstante navorsing en ontwikkeling van nuwe, beter algoritmes (Ferdous et al. 2020). In die ontwikkeling van nuwe konsensusalgoritmes moet die hipotese dat 'n nuwe algoritme meer effektief as 'n bestaande een is, getoets word. Die Bitcoin-blokskakel met die BvW-algoritme is geskik as maatstaf as gevolg van sy populariteit en bestaande gebruik as maatstaf vir ander algoritmes.

Om die effektiwiteit van verskeie algoritmes te vergelyk, moet die invloed van ander faktore, soos berekeningsvermoë en mynpoele, verminder word. Die BvW-algoritme pas die moeilikheidsgraad vir die oplossing van 'n blok aan na gelang van die berekeningsvermoë van die netwerk. Hierdie eienskap verseker dat, gemiddeld, een blok elke tien minute opgelos word (Drescher 2017; Nakamoto 2009). Geen toetsnetwerk kan egter ooit dieselfde berekeningsvermoë besit as die huidige Bitcoin-netwerk nie. Sonder dieselfde berekeningsvermoë sal dit 'n geïsoleerde toetsnetwerk buitensporig lank neem om algoritmes te toets aangesien die moeilikheidsgraad gemik is op 'n veel hoër berekeningsvermoë. Historiese tydperke waar die berekeningsvermoë van die Bitcoin-netwerk soortgelyk was aan dié van 'n toetsnetwerk bestaan egter. Die blokskakel, wat in daardie periode gebruik is, kan dus gebruik word tydens eksperimentele toetsing van nuwe algoritmes.

Hierdie projek vergemaklik die toets van nuwe algoritmes deur hierdie probleem as die primêre doel te hanteer. Die berekeningsvermoë van die toetsnetwerk word bereken en ingevoer, waarna die program afdelings ('epochs') in die Bitcoin-blokketting met 'n geskikte moeilikheidsgraad vir toetsdoeleindes gaan soek. Data uit die geïdentifiseerde afdelings kan dan onttrek word vir gebruik deur die toetsnetwerk. Tweedens dra die projek ook by tot die ontwikkeling van die nie-linière BvW-algoritme. Hierdie nie-linière algoritme wyk af van die BvW-algoritme deur 'n dinamiese teiken aan elke myner toe te ken in plaas van 'n uniforme teiken oor die netwerk heen (Bezuidenhout et al. 2020). Om te verhoed dat kriptoverwerkers hul dinamiese teikenwaarde manipuleer, kyk hierdie projek na verskeie pseudo-ewekansige nommergenerasiemetodes met data vanuit die bestaande Bitcoin-blokskakel. Die doel is om hierdie gegenereerde nommers tydens teikenbepaling te gebruik om moontlike manipulasie te verhinder.

Verwysings

Bezuidenhout, R., Nel, W., Burger, A., 2020, Nonlinear proof-of-work: improving the energy efficiency of bitcoin mining. *Journal of Construction Project Management and Innovation* 10(1), 20-32. https://doi.org/10.36615/jcpmi.v10i1.351.
CoinMarketCap., 2022, Global cryptocurrency charts. Beskikbaar van: https://coinmarketcap.com/charts/. Geraadpleeg 16 November 2022.
Drescher, D., 2017, Blockchain basics: A non-technical introduction in 25 steps. Apress Media LLC. https://doi.org/10.1007/978-1-4842-2604-9.
Ferdous, M.S., Chowdhury, MJ.M., Hoque, M.A., et al., 2020., Blockchain consensus algorithms: A survey. http://arxiv.org/abs/2001.07091
Nakamoto, S., 2009, Bitcoin: A peer-to-peer electronic cash system. Beskikbaar van: https://bitcoin.org/bitcoin.pdf. Geraadpleeg 16 November 2022.

Nota: 'n Seleksie van referaatopsommings: Studentesimposium in die Natuurwetenskappe, 28–29 Oktober 2021, Noordwes-Universiteit. Reëlingskomitee: Prof Rudi Pretorius (Departement Geografie, Universiteit van Suid-Afrika); Dr Hertzog Bisset (Suid-Afrikaanse Kernenergie-korporasie); Prof Cornie van Sittert (Navorsingsfokusarea: Chemiese Hulpbronveredeling, Noordwes-Universiteit).