Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie 2025; 44(1):159
South African Journal for Science and Technology 2025; 44(1):159
https://doi.org/10.36303/SATNT.2025.44.1.4134

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

REFERAATOPSOMMING

Effektiwiteit verifikasie van nie-liniêre Bewys-van-Werk blokskakel konsensus-algoritmes

JDP (Johandré) Bothma, W Nel, RC Fouché

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

Verifying the efficiency of nonlinear probability of success Proof-of-Work blockchain consensus algorithms: This research aims to verify the energy efficiency of new nonlinear Proof-of-Work (nlPoW) algorithms compared to Bitcoin's PoW algorithm. By implementing nlPoW in an isolated test network and analysing computation data generated during the mining process, the study will assess its energy impact in relation to that of the Bitcoin PoW.

Die gebruik van blokskakelstelsels groei geweldig en daar word verwag dat wêreldwye besteding aan blokskakelstelsels byna R330 biljoen gaan bereik met blokskakelstelsels wat moontlik 10 tot 20% van die globale ekonomiese infrastruktuur teen 2030 gaan beheer (Yirrell, 2024). Hierdie navorsing het ten doel om by te dra tot die veld wat gemoeid is met die verbetering van konsensus-algoritmes in blokskakelstelsels, met die spesifieke fokus op kriptogeldeenhede waarvan Bitcoin die oudste en steeds die gewildste is met 'n markkapitalisasie van R20 triljoen (Forbes Advisor, 2024).

Die huidige Bewys-van-Werk-algoritme (BvW-algoritme) wat deur Bitcoin (Nakamato, 2009) gebruik word het die problematiese gevolg dat 'n buitensporige hoeveelheid energie deur die Bitcoin-netwerk verbruik word. Die probleem groei soos die Bitcoin-netwerk groei en meer energie aangewend word om berekeninge te doen met die hoop om 'n geldige blok te vind terwyl die kans op sukses per berekening al kleiner word. Hierdie toestand kan grootliks toegeskryf word aan die lineêre verhouding tussen 'n myner se berekeningsvermoë en hul kans om suksesvol 'n geldige blok te vind. Gebaseer op hierdie bevinding is 'n nuwe stel nie-lineêre Bewys-van-Werk-algoritmes (nlBvW-algoritmes) wat hierdie lineêre verhouding verbreek voorgestel deur Bezuidenhout, Nel en Burger (2020). Alhoewel statistiese modellering bevind het dat hierdie algoritmes meer energiedoeltreffend as die BvW-algoritme is, is hul effektiwiteit nog nie in 'n werklike blokskakelstelsel getoets nie. Hierdie studie poog om die resultate van die statistiese modellering te verifieer deur die nlBvW-algoritmes in 'n geslote toetsnetwerk te implementeer.

Die studie is in twee dele verdeel. Eerstens is die Bitcoin-toepassing aangepas om dit moontlik te maak om die konsensusalgoritme wat tydens die mynproses gebruik word te verander. Die nodige kode om die data rakende die aantal berekeninge wat uitgevoer word op te vang, is ook bygevoeg. Die twee nlBvW-algoritmevariasies wat met statistiese modellering die beste gevaar het, tesame met die oorspronklike BvW-algoritme as maatstaf word in die toetsnetwerk geïmplementeer. Aangesien 'n direkte verband bestaan tussen die hoeveelheid berekeninge ("hashes") wat gedoen word en die energie wat verbruik word, word die hoeveelheid berekeninge wat gedoen word in die netwerk vir elke algoritme vergelyk. Indien daar gevind word dat die nlBvW-algoritmes wel beter energiedoeltreffendheid bereik, sal met fase twee voortgegaan word.

Tydens die tweede fase sal die moontlike invloed van gesamentlike transaksieverwerking ("pooled mining") op die effektiwiteit van die nlBvW-algoritmes ondersoek word. Dele van die toetsnetwerk sal omskep word in groepe wat saam werk om dus hul kans op sukses te verbeter. Tydens beide fases sal die data verwerk word en beskrywende sowel as inferensiële statistiek sal gebruik word om dit te analiseer. Indien dit gevind word dat die nlBvW-algoritmes beter energiedoeltreffendheid het as die BvW-algoritme sal dit toekomstige blokskakelstelsels in staat stel om dieselfde sekuriteitreëls as die Bitcoin-stelsel te volg met beter energieverbruik en 'n laer impak op die omgewing.

Bibliografie

Bezuidenhout, R., Nel, W., Burger, A.J., 2020, Nonlinear proof of work - Improving the energy efficiency of Bitcoin mining, *Journal of Construction Project Management and Innovation* 1(1), 20-32. https://doi.org/10.36615/jcpmi.v10i1.351.

Forbes Advisor, 2024, Top 10 Cryptocurrencies of September 24, 2024. Available from: https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/ Accessed 3 January 2026.

Nakamoto, S., 2009, Bitcoin: A Peer-to-Peer Electronic Cash System. Available from: https://bitcoin.org/en/bitcoin-paper Accessed 3 January 2026.

Yirrell, S., 2024, Blockchain Statistics: Top Stats, Facts and Trends for 2024. Available from: https://connect.comptia.org/blog/blockchain-statistics Accessed 30 September 2024.

Nota: 'n Seleksie van referaatopsommings: Studentesimposium in die Natuurwetenskappe, 30-31 Oktober 2024, Universiteit van die Vrystaat. Reëlingskomitee: Prof Rudi Pretorius (Departement Geografie, Universiteit van Suid-Afrika); Dr Hertzog Bisset (Suid-Afrikaanse Kernenergie-korporasie; Dr Ernie Langner (Departement Chemie, Universiteit van die Vrystaat); Dr Wynand Nel (Departement Rekenaarwetenskap en Informatika, Universiteit van die Vrystaat) en Prof Liesl van As (Departement Dierkunde en Entomologie, Universiteit van die Vrystaat).