Nyzo mesh: Tijd en diversiteit als valuta

Wat is Nyzo?

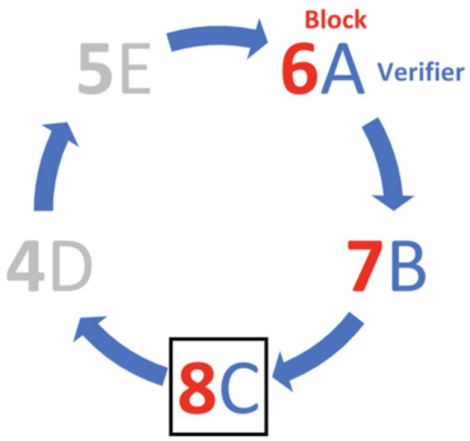
Nyzo is een open-source initiatief. Het netwerk is gedecentraliseerd, democratisch en zeer efficiënt. De block-time is slechts 7 seconden en het systeem past zich perfect aan aan hoge transactievolumes. Dit is niet weer een andere copy-paste fork: Dit is géén afgeleide van een ander project en het zijn **niet** slechts een paar nieuwe functies of een kleine ontwerpwijziging ten opzichte van andere projecten. Dit is een geheel nieuwe code-base, helemaal opnieuw opgebouwd om de meest efficiënte, meest democratische, gemakkelijkst te gebruiken cryptocurrency ter wereld te zijn.

Tijd als valuta

Bewijs van diversiteit vereist actieve participatie in de vorm van tijd- en verificatieprocessen in de blockchain om een bepaalde invloed op het systeem als geheel uit te oefenen. De 'proof-of-diversity' blockchain gebruikt verificatiecycli om de autoriteitsvorm van de blockchain vast te stellen.
Dit is geen 'proof-of-work' en het is geen 'proof-of-stake'. Het is een volledig nieuw consensusmechanisme dat voor zijn kracht afhankelijk is van **diversiteit van participatie**. Hoewel proof-of-diversity zijn eigen zorgpunten heeft die moeten worden aangepakt om de integriteit van de blockchain te waarborgen, **is het immuun voor de aanvallen en problemen inherent aan proof-of-work en proof-of-stake systemen** en tegelijkertijd zeer efficiënt.

Het basisconcept van proof-of-diversity is eenvoudig: De verifiers produceren om de beurt blocks in een circulaire volgorde, waardoor een cyclus ontstaat. Sommige eenvoudige consensusregels zorgen ervoor dat verifiers niet te snel worden toegevoegd of uit de cyclus worden verwijderd. (Om de bijzonderheden te lezen, raden we aan het Nyzo whitepaper en daaropvolgende release-opmerkingen te lezen)

- Verificatie cyclus (mesh van 5, block hoogte 8):

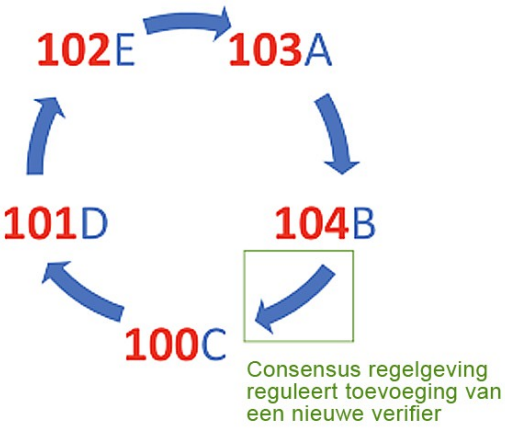


Verifier D genereert block	4
E	5
A	6
B	7
C	8

Hoe blokken worden geproduceerd (hierboven) - Hoe nieuwe nodes aan de cyclus worden toegevoegd (hieronder)

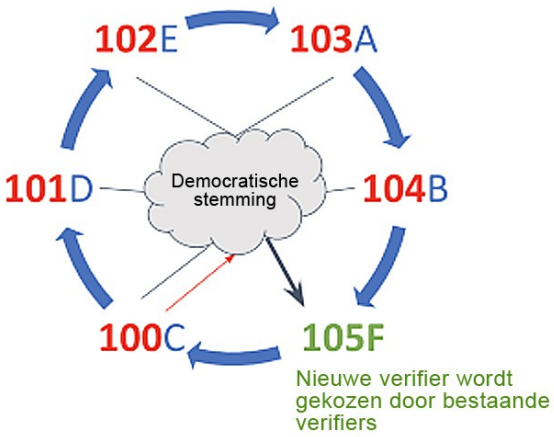
Nodes in de queue, wachtend om aan de cyclus deel te nemen

F, G, H, I, J, K
L, M, N, O, P



Het laatste toegevoegde 50-block block hash wordt gebruikt om deterministisch willekeurig de nieuwe verifier te selecteren

Block 100
(hash: cd01d9Sc7747775S-1b11Saf567cd331d-634850103faf9d01-8fe810cd1bc01cc1)



Voor een gedetailleerd overzicht, lees de Nyzo ontwerpmethodiek door @jimtalksdata

Hoewel het consensusmechanisme 'Proof of diversity' wordt genoemd, het resultaat van een juiste diversificatie van verifiers komt daarentegenvoort uit de consensusregels die actief worden ingevoerd in en goedgekeurd door het netwerk.

Een belangrijk gegeven in het geval van Nyzo is dat het een bepaalde hoeveelheid tijd kost voor een node in de queue kan deel nemen aan de cyclus. Zoals eerder vermeld, geeft de open **'attack vector', die is embedded in het klassieke consensus systeem voor proof-of-work niets om de factor Tijd**, het vindt alleen berekeningen, die worden opgelost, belangrijk, een beslissende actie met onmiddellijke gratificatie voor de deelnemende miner. Dit is waar de altcoins in-wording, waarbij besloten is om het proof-of-work systeem te gebruiken, het risico lopen dat het onmiddellijk

bevredigende karakter van de invloed van één entiteit op een netwerk een reële en onvoorziene bedreiging vormt voor de gesteldheid van het netwerk en de integriteit van de blockchain.

Dit staat in schril contrast met de modus operandi van Nyzo en het proof-of-diversity in het algemeen. In het geval dat een slechte speler de controle probeert te krijgen over de cyclus om een reorganisatie van de blockchain uit te voeren, moet hij eerst toegang krijgen tot 50% van de 'private keys' van de verifiers in de cyclus aanwezig **of** zich herhaaldelijk aan de cyclus toevoegen totdat hij 50% van de totale verifiers in de cyclus heeft verzameld.

Elke verifier in de cyclus kan voorstellen om een nieuwe queue node in aanmerking te laten komen voor deelname aan de cyclus, gelijk als in een democratie. Zodra de blockchain-regels bepalen dat een nieuwe verifier mag deelnemen aan de cyclus, krijgt de top-voted verifier, degene die meer dan 50% van de cyclus-verifiers stemmen achter zich heeft, toestemming om de cyclus te betreden. Standaard stemt de verifier automatisch deterministisch willekeurig voor een verifier in de wachtrij op basis van de laatste (50-block hoogte) block hash, wat resulteert in een **geautomatiseerde, uniforme en tegelijkertijd individueel gegenereerde stemming**.

In het geval van een slechte speler, die controle probeert te krijgen over de cyclus door nieuwe nodes aan de queue toe te voegen, zijn er verschillende voordelen die voortvloeien uit het consensusmechanisme als geheel, laten we een hypothetisch scenario bekijken.

> *Er zijn momenteel 10.000 queue nodes die wachten om deel te nemen aan de cyclus en er zijn 1000 in-cycle verifiers, het aantal nodes dat nieuw mag deelnemen aan de cyclus is momenteel 7 per dag.*
>
> *De slechte speler moet eerst een probabilistisch voordeel in de rij krijgen om sneller deel te nemen aan de cyclus. Laten we zeggen dat de slechte speler erin slaagt om met succes 20.000 nodes te initiëren, waardoor hij een kans zou verkrijgen van 66% dat hij zich de volgende keer kan aanmelden.*
>
> *De speler moet nu 30 dagen wachten voordat al zijn nodes in aanmerking komen voor deelname aan de cyclus. Deze preventieve maatregel zorgt voor een goede bescherming tegen botnets, volmachten en creditcard fraudeurs die hun illegaal gefinancierde servers in een valuta willen verzilveren.*
>
> *De 30 dagen zijn verstreken. Gedurende deze 30 dagen heeft de Nyzo-gemeenschap de mogelijkheid gehad om een entiteit op te merken die een groot aantal nodes initieert, ze kunnen reageren voordat zelfs maar één node van deze speler het haalt. (In de verdediging van de speler, zou hij ervoor kunnen kiezen om zijn nodes druppelsgewijs actief te laten worden, gedurende de periode van een maand, resulterend in een incubatieperiode van 45 dagen.)*
>
> *We hebben nu een punt bereikt waarop de speler een aanzienlijke investering heeft gedaan om het netwerk aan te vallen en heeft daar nog niets aan verdiend.* ***De geschatte kosten op dit moment (20.000 * 4 dollar [30d]) = $ 80.000.*** *Een redelijke schatting van de kosten van servers en de werkelijke waarde van een IPv4-adres.* ***De speler heeft de interesse gewekt van mensen die bij het project betrokken zijn en die zijn in staat om op zijn acties te reageren.***
>
> ***Laten we zeggen dat de speler veel geluk heeft gehad****, dat niemand van de community actie ondernam en zijn nodes nu in aanmerking komen om deel te nemen aan de cyclus, met hetzelfde 66% voordeel dat hij eerder had. Er zijn nu 1210 (1000 + (7*30 dagen)) nodes in de cyclus. Op dit punt daalt het aantal naar 6 nieuwe toevoegingen per dag.*
>
> ***Laten we zeggen dat de speler wederom heel veel geluk heeft*** *en dat niemand van de community heeft gemerkt dat de nodes van deze speler meedoen, wat resulteert in hetzelfde voordeelratio gedurende het gehele proces vanaf hier.*
>
> *De speler krijgt elke dag +3,6/7 nodes. Na een week, +25/42 nodes.*
> *Na een maand, +100/160 nodes.*
> *Na een jaar (nog steeds met hetzelfde onvoorstelbare status quo!) +1200/1920 nodes.*

> *Op dit moment heeft de aanvaller meer dan een jaar van zijn tijd hieraan besteed, er zijn momenteel meer dan 3000 nodes in de cyclus en hij moet het 40% -getal nog zien te behalen.* ***De aanvaller heeft meer dan $ 1 miljoen en 1 jaar van zijn tijd hieraan besteed en heeft het systeem nog steeds niet succesvol kunnen aanvallen.***
>
> *De onvoorspelbaarheid van de acties die door netwerkdeelnemers worden uitgevoerd door middel van blacklisting of andere preventieve maatregelen, maakt het* ***proof-of-diversity consensus mechanisme volledig bestand tegen zo'n slechte speler****. In de tussentijd heeft de aanvaller ontdekt dat hij in feite beter Nyzo units kan verdienen, door deelname aan het netwerk, en zelfs winst kan maken door deel te nemen, in plaats van het systeem te proberen vernietigen dat hem daarentegen juist geld kan opleveren.* ***De incentive-structuur verzekert de conformiteit van alle netwerkdeelnemers - de detecteerbare aard van een reorganisatie van een blockchain, het onrealistische geluk in het voordeel van de aanvaller in dit voorbeeld, en de steeds wijzigende status-quo maken een 51% -aanval op Nyzo een onrealistisch, tijdrovend en zeer kostbare poging.***

Zoals je kunt zien, is de kracht van de tijd overweldigend en de implicaties voor klassieke proof-of-work systemen mogen ook zeker niet over het hoofd worden gezien.

Milieuvriendelijk

Als dat allemaal niet genoeg was om u te overtuigen van de implicaties van Nyzo en het bewijs van het diversiteitssysteem, hebben we nog een extra voordeel voor u in petto.

Door gebruik te maken van sterk geoptimaliseerde en goed gestructureerde code, in combinatie met historische block-consolidatie technieken, staan de technische vereisten van de node op een absoluut minimum. Een verifier kan worden uitgevoerd op een low-tier Virtual Private Server. **Dit resulteert in een verwaarloosbare CO2-uitstoot die in schril contrast staat met het huidige Bitcoin-netwerk, en een proof-of-work systeem in het algemeen.**

Een blockchain die bestand is tegen aanvallen en tegelijk milieuvriendelijk is?
Doe mee en run a node!