Directed Acyclic Graph (DAG)

Acyclishe gerichte graaf

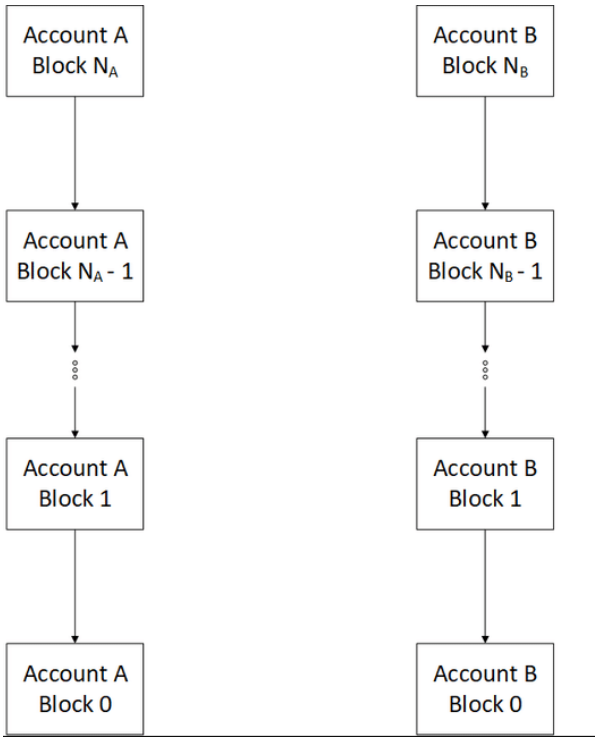
Gebruikt in

IOTA, Nano, Obyte, Hashgraph

- IOTA
- Nano
- Obyte
- Hashgraph

Hoe werkt het?

Een DAG is geen blockchain in de standaard zin van het woord. Het is een gerichte, niet-cyclische graaf, denk hier bij aan de nodes en takken uit git versiebeheer. Iedere gebruiker heeft zijn eigen bloackchain, genaamd block-lettice, waar alleen zij naar kunnen schrijven. De andere gebruikers hebben hier een kopie van. Het voordeel hiervan is dat het asynchroom te werk kan gaan wat hoge transactie snelheden mogelijk maakt.

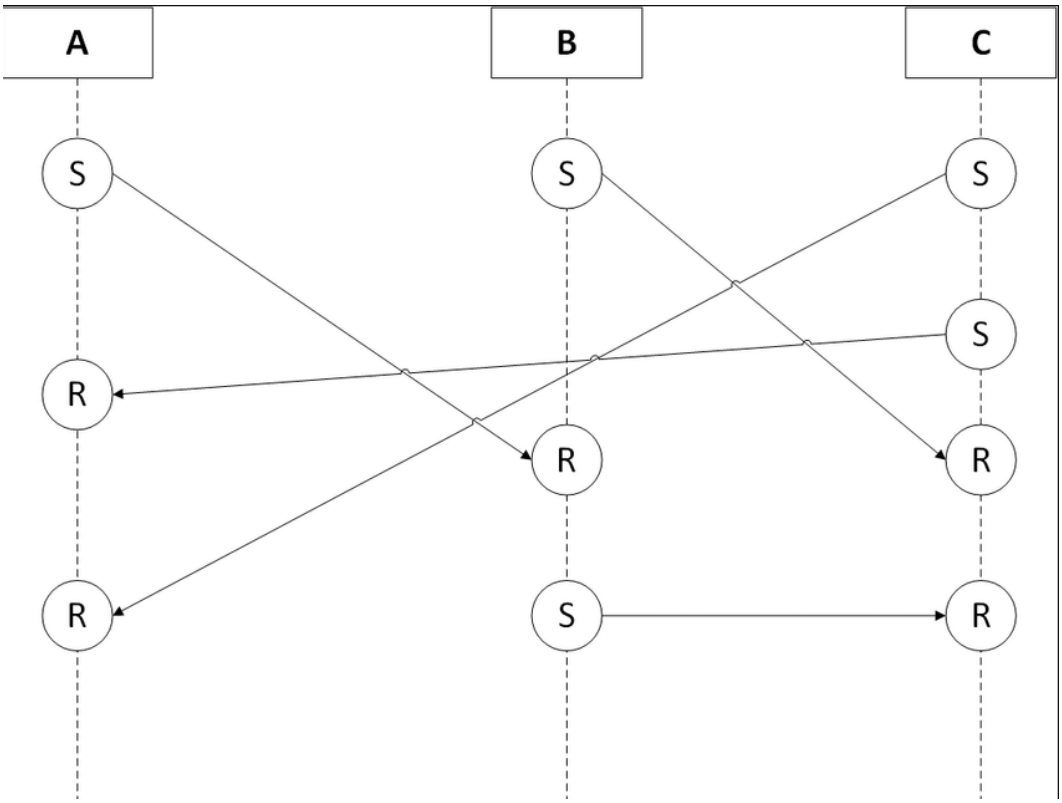


Structuur van de block-lettice

Transacties

Er zijn verschillende manieren om transacties te valideren. Nano gebruikt een methode waar er een send transactie en een receive transactie wordt aangemaakt. Met het aanmaken van de send transactie worden fondsen van het account van de verstuurder afgehaald die in afwachting blijven totdat de bijbehorende receive transactie wordt aangemaakt.

Bij het aanmaken van transacties wordt vaak een Proof of Work operatie uitgevoerd om te voorkomen dat gebruikers zeer veel transacties aanmaken wat kal leiden tot DoS.



Overzicht transaction handling

Voordat een transactie wordt toegevoegd, moet deze op voorgaande nodes worden worden doorgebouwd. Omdat het een graaf is zit je met meerdere takken, daarom wordt er door middel van een algoritme een gewicht aan iedere tak gegeven. Dit gewicht is gebaseerd op het aantal bevestigde transacties. Het bevestigen van een transactie gebeurt wanneer een nieuwe transactie deze refereerd.

Double-spending

Wanneer een node oudere transactie bevestigd, wordt er een pad naar de aller eerste transactie gemaakt. Hierbij wordt gekeken of er voldoende balans is. Dit bad kan meerdere routes hebben, maar slechts één hoeft er bevestigd te worden.

Wanneer gebruikers aan een ongeldig pad blijven bouwen, lopen ze het risico dat hun transacties genegeerd worden. Hoewel het kan zijn dat hun transactie legitiem is, zolang de transactie daarvoor dat niet is, kan de hele tak worden genegeerd. Het is dus van eigen belang om double-spending te voorkomen door alle transacties te controleren en door te blijven bouwen aan een legitiem pad.

Consensus algoritme

Nano gebruikt een Open Representative Voting (ORV) consensus algoritme. Met ORV kiest een gebruiker een representatieve node die voor hun stemt als een voting proxy. Deze node houdt zich bezig met het verifieren van digitale handtekeningen en handelt conflicten tussen transacties af, waarbij het stemt op de volgens de node geldige transactie.

De stemmen zijn balans gewogen. Dit betekend dat een stem evenveel waard is als de hoeveelheid munten die de node vertegenwoordigd.

Om een 51% aanval uit te voeren moet een node dus 51% van alle bestaande munten vertegenwoordigen.

Hashgraph gebruikt een "gossip"protocol. Waarbij steeds een transactie met enkele willekeurige nodes wordt gedeeld, die dit vervolgens ook weer met enkele willekeurige nodes delen todat het hele netwerk van deze transactie afweet.

IOTA gebruikt het Tangle consensus algoritme. Hierbij moet je voordat je een transactie verstuurd eerst twee eerder ontvangen transacties valideren. Het "two-for-one, pay it forward" consensus versterkt de validiteit van de transacties hoe meer transacties er worden toegevoegd.

Om niet geldige transacties als geldig te verklaren, moet je over 1/3 van alle transacties genereren. Zolang er weinig transacties zijn, heeft IOTA hierom een gecentralizeerde

node, de "coordinator" toegevoegd die alle transacties dubbel checkt. Wanneer er een voldoende volume transacties is zal deze worden weggehaald.