AUDIT
MAGAZINE

RUBRIEKEN | 1 JULI 2020

EEN ANDERE KIJK OP BLOCKCHAIN

Auteur: Jelte Coenraads MSc EMA RAAustin Distel
Beeld: Hitesh Choudhary
Leestijd: 2 min

Een unieke en tevens belangrijk eigenschap van blockchain is dat alles wat op de blockchain wordt opgeslagen onveranderlijk is. Of beter gezegd: eens opgeslagen is voor altijd opgeslagen.

Maar is dat ook zo? En waar moeten auditors dan op letten? Om die vragen te kunnen beantwoorden is het belangrijk om meer te begrijpen van het consensus algoritme van een blockchain. Dat is de manier waarop het computernetwerk overeenstemming bereikt over welke transacties of datamutaties geldig zijn en welke ongeldig zijn.

Zonder meteen in de technische details te duiken, is het goed om te weten dat er veel verschillende manieren zijn om consensus te bereiken. Denk aan een democratie. Nederland, Engeland en Amerika zijn democratische landen, maar de manier waarop zij een leider kiezen verschilt in elk van deze landen. Een blockchain kun je vergelijken met een digitale democratie en iedere blockchain heeft zijn eigen ‘spelregels’. Voor een auditor is het van belang te begrijpen met welke vorm van blockchain je te maken hebt.

Het bitcoinnetwerk maakt bijvoorbeeld gebruik van het zogenaamde ‘proof-of-work’-consensusalgoritme (PoW). Dit is gebaseerd op de totale hoeveelheid rekenkracht die in het netwerk beschikbaar is. Kort gezegd houdt dit in dat 51% van de computerrekenkracht een mutatie in de blockchain moet goedkeuren en accepteren voordat deze mutatie aan de blockchain wordt toegevoegd. Hoe meer hardware en rekenkracht je bezit, hoe meer stemrecht of macht je dus hebt.

Een ander populair consensusalgoritme is ‘proof-of-stake’ (PoS). Daarbij gaat het om de waarde van jouw aandeel (stake) in het totale netwerk. In zo’n geval zijn er blockchain tokens in omloop die te koop en verhandelbaar zijn. Dus hoe meer tokens en geld je bezit, hoe meer stemrecht en macht je hebt of kunt verkrijgen in het blockchainnetwerk.

Er zijn nog tientallen varianten en andere algoritmes om consensus te bereiken, waarbij het er altijd om gaat dat een meerderheid van het netwerk akkoord moet gaan met een mutatie in de betreffende blockchain. Een persoon of entiteit kan dus een belang van 51% of meer verkrijgen om de block-chain te manipuleren, dat wordt een 51%-aanval genoemd.

Om terug te komen op de vraag of alles op de blockchain onveranderlijk is? Nee, het is wel degelijk mogelijk om historische data op de blockchain te wijzigen, mits de meerderheid van het netwerk daar mee instemt. Staat uw organisatie op het punt om een blockchaintoepassing te implementeren, dan is het als auditor verstandig om de spelregels van het betreffende consensusalgoritme te onderzoeken en te achterhalen hoe de macht van de verschillende stakeholders in het netwerk verdeeld is. Wanneer een organisatie een private blockchain of een consortium blockchain opzet, kan de organisatie zelf de spelregels bepalen. Er zijn ook websites die voor verschillende publieke blockchains bijhouden hoeveel het kost om een 51%-aanval uit te voeren. Voor bitcoin kost het momenteel zo’n 10 miljoen euro aan stroomverbruik voor één dag. Dat is nog los van de miljarden aan investeringen in de hardware die daarvoor nodig is. Nu begrijpt u waarschijnlijk ook waarom men zegt dat transacties op de bitcoin blockchain niet te manipuleren zijn.

Dit artikel is de tweede in een reeks van vier, waarin *Audit Magazine* een andere kijk op blockchain onderzoekt. Een bijdrage van Jelte Coenraads, internal auditor bij ABN-AMRO.

Tags: AM onderzoekt, Blockchain

Bron url: https://auditmagazine.nl/rubrieken/een-andere-kijk-op-blockchain-3/