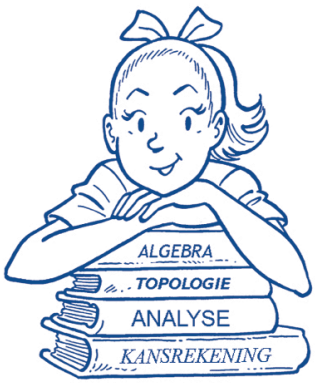
WISKUNNEND WISKE



© 2020, Standaard Uitgeverij, Antwerpen, België

DE HEBBERIGE HACKERS

OPDRACHT 1

Wiske heeft zich aangesloten bij een ethisch hackerscollectief. De 7 hackers bundelden hun krachten en maakten samen 10 miljoen aan bitcoins buit van een criminele organisatie. Ze geven de cryptomunten terug aan de rechtmatige eigenaars, en mogen als beloning 1 miljoen houden.
De hackers besluiten de bitcoins als volgt te verdelen:
de oudste hacker doet een voorstel tot verdeling en alle leden (inclusief de oudste) stemmen voor of tegen. Als minstens 50% voor stemt, dan zullen de bitcoins op die manier verdeeld worden. Anders zal de hacker die het voorstel deed uit het collectief worden gezet en zal het proces worden herhaald met de overblijvende leden. Hierbij mag je aannemen dat 1 bitcoin als geheel wordt beschouwd. Ze zullen dus niet verder opgedeeld worden, bijvoorbeeld in honderdsten.
Omdat de hackers allemaal erg hebberig zijn zullen ze hoe dan ook tegen stemmen als ze bij een voorstel hetzelfde aantal munten zouden krijgen door voor of tegen te stemmen.
Als je ervan uitgaat dat alle hackers even slim en hebberig zijn, wat zal er dan gebeuren?

WISKUNDIG WEETJE

Cryptomunten, zoals de bitcoin, zijn allemaal gebaseerd op blockchaintechnologie. Een blockchain is een logboek waarin alle transacties opgenomen worden. Dus van zodra iemand een transactie uitvoert en daarvoor betaalt of ontvangt in bitcoin, wordt deze transactie in het logboek bijgehouden. Dit bijhouden gebeurt echter op zo een manier dat een bitcoin nooit tweemaal kan uitgegeven worden. Het logboek bestaat in feite uit blokken. Een blok bevat een (of meerdere) transacties, en verwijst naar een vorig blok. Tegelijk bevat een blok ook een cryptografische hash van alle informatie uit het vorige blok. Een hash is eigenlijk een wiskundige functie die de data uit een blok omzet in een reeks getallen. Denk bijvoorbeeld aan het ISBN nummer op een boek. Twee verschillende blokken kunnen niet dezelfde hash hebben, maar het is ook niet mogelijk om uit de hash van een blok de informatie uit dat blok opnieuw te reconstrueren. Je kan ook niet de tekst van een boek reconstrueren uit zijn ISBN nummer. Omdat een blok dus telkens informatie uit alle vorige blokken bevat, kan de data in een van de blokken niet gewijzigd worden zonder alle daaropvolgende blokken te herberekenen. Aldus wordt het onmogelijk om eenzelfde bitcoin tweemaal uit te geven.
De methoden om de informatie te versleutelen, worden ook alsmaar geavanceerder. Zo wordt ook gebruik gemaakt van *elliptic curve cryptography*. Elliptische krommen zijn meetkundige interpretaties van heel specifieke algebraïsche vergelijkingen. Deze objecten werden jarenlang bestudeerd in de fundamentele wiskunde zonder a priori een toepassing in gedachten te hebben. Zoals vaak bleek jaren later eens te meer dat structuren en stellingen uit de fundamentele wiskunde heel belangrijke toepassingen hebben.
Een tweede kenmerk van cryptomunten is dat ze gedecentraliseerd zijn, omdat de blockchains niet noodzakelijk door een centrale bank moeten bijgehouden worden. Het gebruik van de blockchaintechnologie heeft echter als nadeel dat er heel veel rekenkracht nodig is om de transacties telkens bij te houden en te versleutelen in de blockchain. Hoewel het aantal transacties in bitcoin wereldwijd marginaal is in vergelijking met het aantal transacties in gewone munten, verbruikt de bitcoin momenteel al op jaarbasis meer elektriciteit dan een klein land zoals Ierland.
Ook economisch zijn er verschillen met gewone munten. Omdat een centrale bank, althans in theorie, ongelimiteerd extra geld kan uitgeven, ontstaat er inflatie. De bitcoin werd echter zo ontworpen dat er maar een eindig aantal van beschikbaar zijn. Daardoor stijgt de waarde van de bitcoin in de loop van de tijd.

VUB VRIJE UNIVERSITEIT BRUSSEL