

De onveranderlijke blockchain

Blockchain. Dat woord hebben de meesten van ons wel eens op het nieuws voorbij horen komen. Waarschijnlijk samen met de term bitcoin. Maar de blockchain is niet bitcoin. Bitcoin is wel een blockchain. Maar hoe zit dat dan eigenlijk? Aan het einde van deze les weten leerlingen waar een blockchain voor gebruikt kan worden en hoe een blockchain werkt. Specifieker kijken we naar het mechanisme waardoor het onmogelijk is om iets dat in de blockchain staat weer te veranderen. Ongeveer. Want dat is best ingewikkeld. De les heeft zowel doe- als praatopdrachten en is daardoor afwisselend en interactief. Totale duur: 45 min.

VERBINDING MET BEROEPEN EN DE ARBEIDSMARKT:

Hoewel de blockchain op het moment voornamelijk in verband gebracht wordt om digitaal geld te ontwikkelen (en daarmee “echt” geld te verdienen) bespreken we in deze les aantal andere zaken waar blockchain technieken voor gebruikt kunnen worden. En soms ook al echt gebruikt worden. Denk aan auto's die hun eigen parkeergeld betalen of koffiebonen waarvan je zeker weet dat ze echt uit het land komen wat op de verpakking staat. Dus van programmeur tot bankier en van automonteur

tot eigenaar van een koffiewinkel; we gaan steeds meer met blockchain te maken krijgen.

- Introductie : Kennismaking: Wat is blockchain nou eigenlijk? (5 min)
- Verdieping: We kijken naar de techniek achter blockchain (15 min)
- Doen: In groepjes zelf een blockchain maken (20 min)
- Afronding: Wat kunnen we met een blockchain doen? (10 min)

DOEL VAN DE LES

- Leerlingen leren wat een blockchain is
- Leerlingen leren waarom je gegevens in een blockchain niet aan kan passen
- Leerlingen denken na over toepassingen van blockchaintechniek

VOORBEREIDING

Van tevoren kun je een aantal dingen doen:

- Lees de handleiding en lesbrief
- Klik door de slides voor op het scherm
- Zorg dat de zes blokken uit de lesbrief losgeknipt of gesneden zijn zodat ze los neergelegd kunnen worden.

BENODIGDHEDEN:

- Scherm met internetverbinding
- Genoeg vellen papier waarop de leerlingen

DOEL VAN DE LES

Domein curriculum 2021	Leerdoelen Digitale vaardigheden	Leerdoel (kern)vak: Wiskunde	21st century skills
Data & informatie	Computational thinking: De leerling kan informatie weergeven in relevante grafieken, tabellen, woorden en plaatjes (gegevens visualiseren)	14.1.1. Je verzamelt, ordent, interpreteert en vergelijkt data en je maakt een grafische representaties van data, ook met behulp van technologie.	1. Creatief denken
Digitale economie	Computational thinking: De leerling heeft inzicht in de manier waarop (een onderdeel) van een computerprogramma kan ondersteunen bij een terugkerende taak of handeling (automatisering)	12.1.1. Je herkent en beschrijft regelmaat in (meetkundige) patronen en tabellen herkennen, en je zet deze voort.	2. Samenwerken

INTRODUCTIE

Slide 1, Luisteren

Leg uit: Blockchain. Dat woord hebben de meesten van ons wel eens op het nieuws voorbij horen komen. Waarschijnlijk samen met de term bitcoin. Maar de blockchain is niet bitcoin. Bitcoin is wel een blockchain. Dus hoe zit dat dan eigenlijk? Aan het einde van deze les weet je waar een blockchain voor gebruikt kan worden en hoe een blockchain in werkt. Ongeveer. Want het is best ingewikkeld ;)



Slide 2, Luisteren

Leg uit: Om te beginnen is het belangrijk om te weten dat er niet één blockchain is. Er zijn er duizenden. Daarover later meer. Een blockchain is eigenlijk niet anders dan een groot logboek op internet waarin gegevens staan. Geen hele verhalen maar simpele stukjes informatie. Net zoals in dit logboek. Of, als we een beetje in onze eigen tijd blijven: een soort twitter berichtjes. In tegenstelling tot het scheepsjournaal wat jullie hier zien kan niet alleen de kapitein er in schrijven maar mag iedereen dat doen. En natuurlijk ook lezen. Maar stel nou dat er iets in staat dat je wil aanpassen? In zo'n boek kan je er een beetje typex pakken en eroverheen schrijven. En dat is een groot verschil met een blockchain. Daar kan je niet zomaar wat aanpassen. En het is niet dat het niet mag. Het *kán* gewoon echt niet. Het is onmogelijk. Ook niet stiekem. Met andere woorden: als het in de blockchain staat weet je zeker dat het klopt.



Slide 3, Luisteren

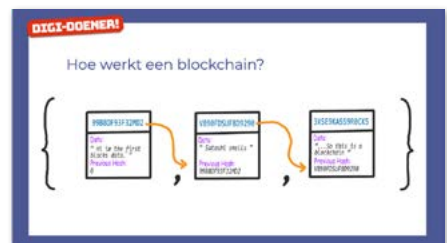
Leg uit: Deze afbeelding geeft schematisch weer waaruit een blockchain is opgebouwd.

Je ziet hier drie blokken die aan elkaar geketend zijn: een ketting van blokken. Nu weet je ook waar de Engelse naam 'blockchain' vandaan komt. Een blok bestaat uit een aantal onderdelen:

- Een ID of hash: dat is het unieke nummer van dit blok (in deze afbeelding is dat de blauwe cijferreeks)
- Het bericht dat je wil versturen
- Het ID van het vorige bericht

In het voorbeeld wat we hier gebruiken wordt het ID door de computer berekend door het een ingewikkelde rekensom op los te laten. De rekensom maakt gebruik van alle gegevens van het blok. En doordat die uitkomst weer in het volgende blok staat kun je de gegevens niet zomaar aanpassen, want dan klopt het volgende blok niet meer!

Laten we dit eens zelf uitproberen!



Verdiepende informatie

De informatie van het nieuwe blok wordt het internet op gestuurd en mag door iedereen berekend worden. Op het moment dat iemand de juiste oplossing heeft gevonden mag het blok erbij en komt het bij iedereen precies hetzelfde in de chain. Degene die de rekensom het eerst heeft uitgerekend krijgt vaak een beloning!

VERDIEPING EN DOEN

Slide 4, Doen

Leg uit: We gaan nu zelf een blockchain maken. Op het scherm zien jullie een leeg blok en daarnaast een alfabet spiekbrieftje. Het blok wordt het eerste blokje van onze blockchain. We gaan de blockchain gebruiken om berichtjes te sturen en daarvoor gaan we ons eigen sommetje gebruiken.

Controleer allemaal of je zes blokken hebt en het alfabet spiekbrieftje op je lesbrief. Voor de eerste opdracht pak je een leeg blok en schrijf je er een bericht in. Het makkelijkst is een bericht van één (kort) woord.

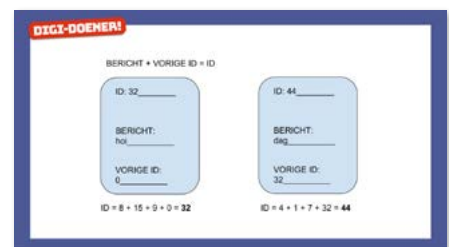


Slide 5, Doen

Leg uit: We gaan nu het ID uitrekenen. De rekensom die we daarvoor gaan gebruiken is
 “VORIGE ID + TEKST = NIEUW ID”

Omdat dit het eerste blok is, hebben we nog geen vorige ID. Daarom vullen we hier een 0 in.

Nu gaan we de letters van de tekst optellen, daarvoor moeten we de letters omzetten naar getallen. Daarvoor gebruiken we gewoon de positie van de letter in het alfabet. Je kan daarvoor het spiekbrieftje gebruiken dat je hebt gekregen. Als ons bericht “hoi” is krijgen we dus de volgende som:
 $0 + 8 + 15 + 9 = 32$



Ons ID is dus 32. We hebben nu een compleet blok. Bij het volgende blok kunnen we nu 32 invullen bij “VORIGE ID”

Doen: Opdracht 1 t/m 3

Slide 6, Doen

De leerlingen hebben nu allemaal een blockchain van vier blokken. We gaan nu proberen de blockchain te vervalsen. We gaan kijken wat er gebeurt als we blok twee vervangen met een blok met een ander bericht.

Doen: Opdracht 4

Antwoord: Wat er gebeurt is dat het ID veranderd. En daardoor klopt het volgende blok niet meer.
 Let op! Met deze rekensom is het mogelijk dat je toevallig



uitkomt op hetzelfde ID. Mocht dat het geval zijn, leg dan uit dat dat natuurlijk met de echt rekensom van b.v. bitcoin niet mogelijk is.

VERDIEPING HAVO/VWO

Maar wat gebeurt er nou als je niet alleen blok 2, maar ook blok drie en vier vervangt?

Antwoord: dan heb je de blockchain “gehackt”. In het echt werkt het ongeveer ook zo maar dan is het gelukkig een heel stuk moeilijker.

AFRONDING

Erg gaaf en slim natuurlijk, zo’n systeem dat altijd de waarheid verteld. Maar wat heb je daar nou aan? Laten we eens wat voorbeelden bekijken

Slide 7, Praten met de klas

Vraag aan de klas: Waarom zou je blockchain gebruiken om te stemmen?

Leg uit: Stemmen is altijd een gevoelige zaak. Of het nou gaat om de Tweede Kamerverkiezing, de nieuwe president van Amerika of wie de klassenvertegenwoordiger moet worden. Er wordt namelijk vaak mee gesjoemeld. Dat komt bijvoorbeeld omdat het mis gaat met tellen of mensen stemmen stiekem twee keer. Of er kan achterhaald worden wie er op wie gestemd heeft. Al deze problemen kan je oplossen met een blockchain.



Slide 8, Praten met de klas

Leg uit: Er zijn veel nep/namaak producten in de wereld. Die zijn vaak lekker goedkoop. Maar als je veel betaald voor een echte “adidas” wil je wel zeker weten dat het ook echt het product is dat je gekocht hebt. Bij het voorbeeld op het scherm is het meteen duidelijk. Maar kun jij aan een koffieboon zien dat deze wel echt uit Brazilië komt? Of kan jij aan het melkpoeder zien dat het wel de echte voor baby’s van nutricia is, en niet gewoon koffiemelkpoeder van het café op de hoek?



Vraag aan de klas: Waarom zou je hier blockchain voor gebruiken?

Uitleg: Door een blockchain te gebruiken van het begin (waar de bonen groeien) tot aan het einde (in de winkel) weet je in de winkel zeker dat de informatie over waar deze bonen vandaan komen klopt. Dat gaat ongeveer als volgt: vanaf het moment dat de bonen geplukt worden totdat ze in de winkel liggen zitten een heleboel stappen: ze gaan naar de opslag, daarna naar de haven daarna in een container daarna op een boot en daarna misschien wel op een andere boot en daarna komen ze aan in een haven en gaan ze door naar het distributiecentrum om uiteindelijk in de winkel terecht te komen. Al deze stappen worden bijgehouden. Maar zijn daardoor erg gevoelig voor fouten en fraude. Met een blockchain kan je dit proces beter automatiseren zonder dat je het

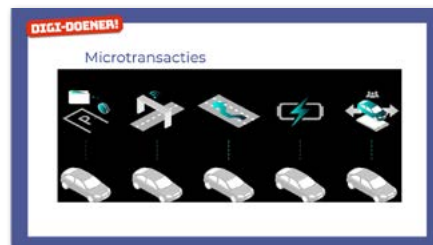
risico loopt dat er met de gegevens gerommeld wordt: dat kan namelijk niet.

<https://www.duurzaambedrijfsleven.nl/futurefood/25547/een-eerlijkere-koffieketen-met-dank-aan-blockchain>

Slide 9, Luisteren

Leg uit: Microtransacties zijn hele kleine betalingen. Van soms wel een fractie van een cent. Microtransacties kan je gebruiken om bijvoorbeeld het opladen van je auto te betalen. Of om heel precies de parkeermeter te betalen.

Omdat je het bij microtransacties hebt over heel veel kleine betalingen is het belangrijk om zeker te weten dat het echt klopt! En ohja, de transactiekosten zijn gratis want je gebruikt geen bank!



Slide 10, Luisteren

Leg uit: Persoonsgegevens zijn superbelangrijk: het is wie je bent. Deze gegevens zijn opgeslagen op allerlei plekken zoals bij de gemeente en bij de belastingdienst. Maar het staat ook je op identiteitskaart of paspoort.

Doordat het op al die verschillende plekken staat is het het aanpassen van je gegevens niet heel makkelijk. Misschien is het handig(er) om al jouw gegevens op één plek te bewaren. Een plek waar iedereen bij kan maar niet iedereen zomaar wat aan kan passen. Je raad 't het al: een blockchain is hier een goede mogelijk. En zoals we besproken hebben is een blockchain erg veilig.



Slide 11, Praten met de klas, doen

Bespreken: Vraag aan de leerlingen: Wat kun je zelf nog verzinnen?

Een aantal voorbeelden:

- Nieuws - nieuwsartikelen zijn van de journalist die het geschreven heeft
- Medische gegevens - veilig opslaan
- Beleggen - transparant en veilig
- Authenticatie (inloggen e.d.)
- Openbaar vervoer
- Wat nog meer?

