



Een verkenning van blockchaintechnologie in het onderwijs



Inhoudsopgave

- › Een verkenning van blockchaintechnologie in het onderwijs _____ 3
- › Wat is blockchain? _____ 3
- › Welk probleem kun je oplossen met blockchain? _____ 6
- › Is blockchaintechnologie de oplossing voor jouw probleem? _____ 7
- › Conclusie: nog weinig zinvolle onderwijstoepassingen _____ 13
- › Colofon _____ 14





Een verkenning van blockchain-technologie in het onderwijs

Blockchaintechnologie krijgt de laatste jaren veel aandacht in de media. Sommige experts zien het als de meest disruptieve technologie sinds het internet. Alleen al een verwijzing naar blockchain in de naam van een bedrijf kan leiden tot een stijging in beurswaarde, zo constateerde economisch persbureau Bloomberg eind 2017. Verwachtingen in relatie tot het oplossen van vertrouwensproblemen zoals fraude zijn hooggespannen. Ook binnen het onderwijs wordt met belangstelling naar deze relatief nieuwe technologie gekeken. Buiten cryptocurrencies – digitale munteenheden – zoals Bitcoin is het echter nog onduidelijk waar kansrijke toepassingen van blockchaintechnologie liggen. Zeker in sectoren buiten de financiële wereld is meerwaarde nog moeilijk aan te tonen. De vraag is of er zinvolle blockchaintoepassingen in het onderwijs zijn.

Wat lees je in deze verkenning?

Zijn er specifieke problemen of uitdagingen in het onderwijs waarvoor blockchaintechnologie de beste oplossing zou kunnen zijn? Die vraag proberen we hier te beantwoorden. We beginnen met een korte uitleg van blockchain en welk soort problemen we daarmee kunnen oplossen. Vervolgens introduceren we op basis van de specifieke blockchainkenmerken een checklist waarmee je zelf kunt inschatten of blockchaintechnologie een optie zou kunnen zijn voor jouw specifieke uitdaging.

Wat is blockchain?

Een uitleg over blockchaintechnologie kan bijna niet anders dan starten met Bitcoin, de digitale munteenheid die Satoshi Nakamoto in 2008 introduceerde. Het bijzondere aan deze munteenheid is dat transacties die je daarmee doet, gebeuren zonder tussenkomst van een bank. De bank is normaal gesproken nodig om te controleren of financiële transacties eerlijk en veilig plaatsvinden. Omdat wij banken vertrouwen om dit voor ons te regelen, werkt ons financiële systeem. Maar wat als dat vertrouwen er niet meer is? Of als we breder kijken dan alleen Bitcoin en de financiële wereld: wat als er geen enkele partij is in een systeem die we voldoende vertrouwen om bepaalde transacties uit te voeren en te valideren? Precies dit probleem, kan worden opgelost met blockchaintechnologie. Partijen die elkaar niet van nature vertrouwen of elkaar niet kennen, kunnen het toch met elkaar eens worden over de status van gegevens, zoals of een bepaalde transactie of wijziging heeft plaatsgevonden. Zonder dat hiervoor een derde, controlerende partij nodig is.

Blockchain: een onveranderbaar digitaal register

Een blockchain is het beste te vergelijken met een digitaal register of een database met lijsten waarin transacties of gegevens in chronologische volgorde worden bijgehouden. Iedereen die meedoet aan de blockchain heeft een exacte kopie van het register en kan zien wat erin staat. Elke deelnemer kan ook transacties toevoegen aan het register. Deze transacties worden dan overgenomen op alle andere





kopieën nadat deze geverifieerd zijn. Daarom kijkt iedereen altijd naar dezelfde informatie.

Soortgelijke oplossingen bestaan al. Denk aan een gedeeld document in Google Drive waarbij je de mogelijkheid hebt om documenten samen aan te passen. Iedere deelnemer ziet elke toevoeging die wordt gedaan op hetzelfde moment. Er is echter één kenmerk die blockchains uniek maakt. Een blockchain voegt alleen nieuwe regels met transacties toe aan de onderkant van een lijst, in chronologische volgorde. In feite is het enige wat een blockchain doet het toevoegen van nieuwe rijen en die weer automatisch met alle deelnemers delen. Het is niet mogelijk om iets aan te passen in een regel die eerder is toegevoegd. Dat betekent dus ook dat je nooit meer iets kunt verwijderen uit het register. Nieuwe regels worden gebundeld in een 'blok' en deze blokken vormen samen een keten – de blockchain.

Wat maakt een blockchain zo betrouwbaar?

Hoe zorgt blockchaintechnologie ervoor dat je niet kunt frauderen door bijvoorbeeld eerder toegevoegde regels te veranderen? Via cryptografische software gecombineerd met het 'meer ogen principe' van alle deelnemers in het netwerk. De informatie in het register wordt niet gecontroleerd door één partij, maar door iedereen die meedoet in de blockchain. Zou het je al lukken een eerder toegevoegde regel aan te passen in één kopie van het register? Dan verandert deze regel op hetzelfde moment niet in de kopieën van alle andere deelnemers, wijzigingen zijn immers niet mogelijk. Alleen geverifieerde toevoegingen worden overgenomen in kopieën. Een wijziging in een blockchain is per definitie fraude.

Alleen deelnemers kunnen een nieuwe regel toevoegen. Elke toevoeging wordt op zo'n manier versleuteld – onder andere met de

digitale handtekening van een deelnemer – dat iedereen kan controleren en valideren welke deelnemer daarvoor verantwoordelijk is. Een blok bestaat weer uit een afgesproken aantal nieuwe toevoegingen. Een blok bevat een verwijzing – een unieke code die gegenereerd is op basis van de inhoud van het blok – naar het blok ervoor, zodat alle blokken als een keten met elkaar zijn verbonden. De unieke code van dit vorige blok wordt ook gebruikt om de unieke code te genereren van dit nieuwe blok met transacties. Door blokken zo aan elkaar te verbinden worden aanpassingen achteraf nog lastiger en daarmee fraude nog onwaarschijnlijker. Als je bijvoorbeeld een oud blok zou wijzigen in één kopie van het register verandert de unieke code. En omdat die unieke code gebruikt is bij het daaropvolgende blok, kloppen die codes niet meer en wordt de keten – de blockchain – gebroken. Ook valt de wijziging op, omdat alle andere kopieën die wijziging niet bevatten en je daardoor door het netwerk kunt laten vaststellen wat de echte, gedeelde waarheid is.

Hoe worden blokken toegevoegd aan de blockchain?

Transacties moeten uiteindelijk aan de blockchain worden toegevoegd: bijgeschreven in het publiek inzichtelijke register. De bekendste manier om dat te doen noemen we het zogenaamde proof-of-work. Dat werkt zo: nieuwe transacties moeten worden verwerkt in een blok. Om deelnemers aan te moedigen dit te doen kunnen ze voor het maken van een blok een beloning krijgen. Voor het maken van een blok moet een complexe wiskundige puzzel worden opgelost. Degene die als eerste deze puzzel oplost en daarmee in staat is om een nieuw, versleuteld blok met transacties toe te voegen aan het register krijgt hiervoor een bepaalde hoeveelheid geld, zoals bijvoorbeeld bitcoin. Het maken van een nieuw blok door het oplossen van de puzzel noemen we ook wel mining. Mensen die met hun computers dit werk doen noemen we miners.





Hoe werkt zo'n versleutelde transactie in de praktijk?

In het geval van cryptocurrencies is een nieuwe regel een transactie van de ene naar de andere rekening. Het doen van de transactie werkt als volgt.

Om geld te kunnen versturen en ontvangen heb je net zoals bij een bank een rekening nodig. In het geval van cryptocurrency bestaat een rekening uit twee lange codes, die sleutels worden genoemd. De eerste sleutel is te vergelijken met een rekeningnummer. Door deze bekend te maken aan anderen, kunnen ze geld naar jou overmaken. De andere sleutel lijkt op een (pin)code of wachtwoord en kan gebruikt worden om geld dat op de rekening staat uit te geven, net zoals je bij een traditionele bank ook wachtwoorden en andere codes krijgt om overboekingen te maken.

In tegenstelling tot een traditionele bankrekening zijn deze twee sleutels bij een blockchain niet te veranderen, terwijl je bijvoorbeeld wel een wachtwoord of pincode kunt veranderen. Ze zijn met cryptografie onlosmakelijk met elkaar verbonden als een (sleutel)paar. Ondanks dat de sleutels met elkaar zijn verbonden, kan een buitenstaander met de publieke sleutel (je 'rekeningnummer') jouw geheime sleutel (je 'pincode') niet raden of herleiden. Zonder de geheime sleutel kan je niets doen met het geld dat op jouw rekening staat.

Degene die geld naar jou wil overmaken stuurt een betaalopdracht onder vermelding van de waarde die hij wil overmaken, zijn eigen rekeningnummer (de publieke sleutel) zodat je weet van wie het afkomstig is, en jouw rekeningnummer (jouw publieke sleutel) als beoogd ontvanger. Degene die het geld overmaakt, ondertekent de gehele transactie met zijn geheime sleutel. Hij bewijst daarmee dat hij eigenaar is van de rekening vanaf waar het geld wordt verzonden.

De transactie wordt gedaan en deze wordt, bij het bereiken van een vooraf afgesproken aantal transacties of verstreken tijd, in een blok samen met andere transacties toegevoegd aan het publiek inzichtelijke register (de blockchain). Nadat transacties zijn verwerkt in een blok is het geld pas echt overgemaakt. In de transactie zijn alleen de publieke sleutels zichtbaar en niet de geheime sleutel. Om toegang te krijgen tot het geld heb je dus jouw geheime sleutel nodig. Hiermee heb alleen jij toegang tot jouw geld.

Door deze manier van transacties uitvoeren is een derde partij zoals een bank niet nodig voor verificatie. Iedereen kan de volledige historie van de transacties inzien (men weet dus het 'saldo' van elke deelnemer). De volgorde van alle transacties ligt nauwkeurig vast en alle transacties zijn onveranderbaar met elkaar verbonden.





Het berekenen van het proof-of-work kost veel rekenkracht. In het geval van Bitcoin gaat het bijvoorbeeld in totaal om ongeveer 36 terawattuur per jaar. Dit is vergelijkbaar met het energieverbruik van een middelgroot land. Dit komt omdat heel veel mensen proberen om de eerste te zijn die de puzzel oplossen en daarmee strijden om de beloning en daarvoor veel computercapaciteit inzetten. Maar er zijn ook andere manieren in ontwikkeling om transacties te verifiëren die niet uitlopen op een wedloop en daardoor veel minder energie verbruiken. Een voorbeeld daarvan is proof-of-stake, waarbij verificatie wordt verdeeld onder partijen ('stake'holders), op basis van een verdeelsleutel.

Welk probleem kun je oplossen met blockchain?

Een leerlingvolgsysteem, het bijhouden van een diplomaregister, contractmanagement voor beroepspraktijkvorming of de opzet van een lerarenregister. Allemaal voorbeelden die vaak worden geopperd als het gaat over mogelijke toepassing van blockchain in het onderwijs. De vraag is echter of je aan alle voorwaarden van blockchain kunt, wilt of hoeft te voldoen. Is er een vertrouwensprobleem? Wil je dat meerdere partijen informatie kunnen toevoegen aan de blockchain en alle partijen deze informatie kunnen verifiëren? Is het oké als je niets kunt verwijderen uit de blockchain en als alle deelnemers alle transacties kunnen inzien?

Ter illustratie: een blockchaintoepassing voor een diplomaregister of om resultaten in op te slaan is niet handig als achteraf blijkt dat iemand fraude heeft gepleegd. Je kunt een diploma bijvoorbeeld nooit meer uit de blockchain verwijderen. Maar stel dat je niet het diploma op zou slaan maar alleen een unieke code waarmee je kan checken of het diploma geldig is. Dan kun je het diploma later ook ongeldig verklaren

en dat vastleggen. Deze oplossing adresseert slechts gedeeltelijk de problematiek rondom diploma fraude. Als het proces voorafgaand aan het uitgeven van diploma niet vertrouwd wordt, dan kan een blockchain daar niets aan oplossen.

Als je een (onderwijs)probleem goed analyseert en naast de kenmerken of voorwaarden van blockchain legt, blijkt in veel gevallen dat het eenvoudiger en efficiënter is om andere, al bewezen functionaliteit in te zetten. Denk aan database-replicatie, versleuteling van informatie en digitale handtekeningen of certificaten.

Waarom zijn er zoveel blockchain pilots en initiatieven?

Blockchain staat in de belangstelling en experts verwachten veel van de technologie. Er is sprake van een ware hype. Daarom wagen veel organisaties zich aan pilotprojecten. Door er nu ervaring mee op te doen, verwachten ze eerder voordeel te kunnen halen en hun concurrentiepositie te verbeteren. Deze pilots dienen dus om uit te zoeken waar kansen liggen voor hun sector of bedrijf en ook welke hindernissen nog moeten worden genomen. Dit soort projecten gebruiken uiteindelijk vaak maar een deel van de mogelijkheden van blockchain. Denk aan het synchroniseren van informatie tussen verschillende deelnemers of het digitaal ondertekenen van informatie. Uitdagingen waarvoor het vaak eenvoudiger en efficiënter is om andere, al bewezen, oplossingen in te zetten. Er zijn daarom tot op heden nauwelijks succesvolle 'echte' blockchainimplementaties bekend.



Is blockchaintechnologie de oplossing voor jouw probleem?

Om te achterhalen of blockchaintechnologie een oplossing is voor een bepaald probleem hebben we een checklist gemaakt. De checklist bestaat uit tien vragen over vertrouwen, blockchain-beperkingen en soorten blockchain. Aan de hand van de antwoorden op de eerste acht vragen kun je inschatten of blockchaintechnologie zinvol is voor jouw specifieke uitdaging. Op basis van de tot nu toe bekende pilots en toepassingen van blockchaintechnologie, stellen we vast dat dit zelden het geval zal zijn. De meest voorkomende redenen zijn dat er geen vertrouwensprobleem is, of dat er in de blockchain geen gegevens gewijzigd kunnen worden. En zelfs als er wel een vertrouwensprobleem is, kan blockchaintechnologie dit probleem vaak niet oplossen. Kom je toch tot de conclusie dat blockchain een oplossing voor jouw probleem biedt? Dan kun je met de laatste twee vragen vaststellen welk soort blockchain het beste past.

We lichten de checklist op de volgende pagina's toe. Bij de toelichting betrekken we ook voorbeelden van mogelijke toepassingen die we uit gesprekken met betrokkenen in het onderwijsveld hebben gehaald.

Checklist blockchaintechnologie

- 1 Zijn er meerdere deelnemende partijen?
- 2 Bestaat er wantrouwen tussen de deelnemers?
- 3 Zijn er meerdere onafhankelijke partijen voor verificatie?
- 4 Ontbreekt een vertrouwde derde partij?
- 5 Is de hoeveelheid data die verwerkt moet worden beperkt?
- 6 Mogen wijzigingen of transacties met een lage snelheid worden verwerkt?
- 7 Mogen en moeten gegevens permanent worden opgeslagen?
- 8 Is er een koppeling nodig met fysieke objecten?

Vraag 1 t/m 8 met 'ja' beantwoord? Bepaal dan met vraag 9 en 10 het soort blockchain.

- 9 Mogen de transacties publiek inzichtelijk zijn?
- 10 Zijn de partijen die de transacties vastleggen bekend?





Vertrouwensvragen

1 Zijn er meerdere deelnemende partijen?

De transacties die gedaan worden, moeten relevant zijn voor meerdere deelnemende partijen. Het moet gaan over informatie die met meerdere partijen gedeeld moet worden. Denk bijvoorbeeld aan gegevens over vrijstellingen voor vakken van de ene universiteit bij de andere universiteit. Dit kan interessant zijn voor studenten, leraren en andere universiteiten. Blockchain biedt geen voordeel bij gebruik als intern, gesloten systeem binnen één organisatie. Er kan dan net zo goed gebruik gemaakt worden van een willekeurige database-technologie om informatie op te slaan en te verwerken.

Een veelgehoord voorstel is het op de blockchain opslaan van gegevens over vakken of resultaten, die een leerling of student succesvol heeft behaald bij een onderwijsinstelling, zodat hij hier op een andere instelling niet meer aan hoeft te werken. Blockchain is echter geen oplossing voor het gehele probleem. Er is een andere randvoorwaarde noodzakelijk buiten blockchain, namelijk een gemeenschappelijke taal. Zodat een instelling kan beoordelen of de inhoud en vaardigheden die een leerling opgedaan heeft op een andere instelling overeenkomt met hoe zij dat doen.

2 Bestaat er wantrouwen tussen de deelnemers?

Blockchaintechnologie biedt uitkomst als partijen elkaar niet vertrouwen. Als deelnemende partijen elkaar wel vertrouwen, of gemakkelijk overeenstemming kunnen bereiken, zijn er

technisch eenvoudigere oplossingen om ketensamenwerking te administreren dan blockchain, zoals gegevensuitwisseling of een gezamenlijke database. Bovendien zijn blockchains niet geschikt om alle soorten wantrouwen tussen partijen weg te nemen. Vertrouwensproblemen over identiteit (wie heeft een bepaalde transactie gedaan) en autoriteit (heeft een identiteit de accreditatie om een bepaalde transactie te doen) worden met blockchain niet opgelost.

Een voorbeeld is de accreditatie van stagebedrijven. Accreditaties zou je in een blockchain op kunnen slaan zodat er altijd zekerheid is dat een organisatie een accreditatie heeft. Die gegevens worden immers onveranderlijk opgeslagen. Maar de blockchain kan de rol van partijen die de accreditaties geven niet overnemen, omdat alleen de uitkomst wordt opgeslagen. Als men geen vertrouwen heeft dat de accrediterende partij goed beoordeelt of een organisatie aan de voorwaarden voldoet, lost een blockchain dat niet op.

3 Zijn er meerdere onafhankelijke partijen voor verificatie?

Een belangrijke voorwaarde is dat er binnen de blockchain objectief kan worden vastgesteld of een transactie geldig is en dat dit door meerdere onafhankelijke partijen wordt gecontroleerd. Het feit dat er verificatie gedaan kan worden door meerdere partijen zorgt ervoor dat het vertrouwensprobleem opgelost kan worden. Is er maar één partij die de verificatie doet, dan verliest blockchain zijn echte voordelen. Er blijft dan slechts een mechanisme over om





gegevens op te slaan, dat gedeeld wordt met lezers. Zij hebben nog steeds vertrouwen nodig in die ene verifiërende partij. De resultaten van een student zijn bijvoorbeeld niet onafhankelijk vast te stellen, een stagebegeleider moet een cijfer geven. Andere, externe partijen kunnen niet checken of dit cijfer terecht is.

Het is dus niet evident duidelijk wat er zou moeten gebeuren als een transactie in het onderwijs als ongeldig bestempeld zou worden en wat er nu specifiek te verifiëren valt. Als een onderwijsinstelling bijvoorbeeld een diploma of een deelcertificaat zou uitdelen hebben de andere instellingen geen reden om die informatie of het bewijs te verwerpen.

Er zijn ook andere, eenvoudigere oplossingen naast blockchain zoals digitaal ondertekende documenten waarmee de echtheid van bijvoorbeeld een diploma kan worden vastgesteld.

4 **Ontbreekt een vertrouwde derde partij?**

Blockchain is alleen een oplossing als partijen geen derde, onafhankelijke partij in de arm kunnen of willen nemen om hun vertrouwensprobleem op te lossen. In het onderwijs is deze derde partij vaak juist wel aanwezig in de vorm van een examencommissie of partijen als OCW, DUO, Sectorraden, SURFnet en Kennisnet. In het geval er wel problemen zijn rondom beveiliging en vertrouwen, zijn deze vaak met eenvoudigere technologie te verhelpen. Denk aan geavanceerde encryptie of een gedistribueerde database.

Blockchain kenmerken

5 **Is de hoeveelheid data die verwerkt moet worden beperkt?**

Blockchain is op dit moment nog niet geschikt voor het verwerken van transacties waarin grote hoeveelheden gegevens zitten. De hoeveelheid data die met een transactie kan worden opgeslagen is namelijk beperkt en transacties kosten veel energie (afhankelijk van de manier waarop transacties worden verwerkt). Transacties die veel data bevatten, zoals afbeeldingen of video, zijn niet geschikt.

Video's opslaan als geverifieerd resultaat in je digitale portfolio is dus geen geschikte toepassing van blockchain. Omdat iedereen een kopie moet hebben van deze gegevens is het geen efficiënte manier om grote hoeveelheden gegevens op te slaan. Dit wil je zo compact mogelijk houden vanwege de opslagcapaciteit en verwerkingskracht die nodig is. Alle transacties moeten namelijk gevalideerd en permanent opgeslagen worden door alle deelnemers.

Gegevens met betrekking tot de voortgang van leerlingen of behaalde competenties en vakken zijn betrekkelijk compact qua omvang. De werking van blockchain zou op dit specifieke aspect niet per se een belemmering zijn.





6 Mogen wijzigingen of transacties met een lage snelheid worden verwerkt?

Blockchain is niet geschikt om grote hoeveelheden transacties snel te verwerken. Het verificatieproces is ingewikkeld en zorgt er daarmee voor dat transacties maar met een beperkte snelheid kunnen worden vastgelegd in nieuwe blokken. Bestaande blockchains doen er gemiddeld minimaal 10 seconden over om een nieuwe transactie vast te leggen in een blok. Wanneer het dus om milliseconden gaat, zoals bijvoorbeeld bij het aan- en verkopen van aandelen, is blockchaintechnologie niet geschikt.

In het onderwijs vormt snelheid in de regel geen obstakel, onafhankelijk van de manier van verwerking. De registratie van bijvoorbeeld nieuwe cijfers hoeft niet binnen milliseconden te gebeuren.

7 Mogen en moeten gegevens permanent worden opgeslagen?

Dan is blockchain een goede oplossing. Als je gegevens wilt kunnen verwijderen of later nog wilt kunnen wijzigen, is blockchain niet geschikt. Persoonsgegevens die niet te verwijderen zijn, leveren een conflict op met het recht om vergeten te worden. Iets wat verplicht is volgens de Algemene Verordening Gegevensbescherming (AVG), Europese regelgeving die recent is ingevoerd. Daarom is blockchain geen geschikte oplossing als het gaat om transacties die te maken hebben met persoonlijke gegevens over bijvoorbeeld leerlingen, die je op enig moment weer uit je administratie moet kunnen verwijderen.

Een ander voorbeeld zijn weer de accreditaties van leerbedrijven. Accreditaties van leerbedrijven moeten in de loop van een al geaccrediteerde periode kunnen worden ingetrokken. Dat is in het geval van blockchain onhandig. Ditzelfde zou kunnen gebeuren met diploma's of andere resultaten die achteraf ongeldig kunnen worden verklaard.

Voortgangsgegevens over de stage zijn ook ongeschikt voor blockchain. De gegevens over de student die een bepaalde stage volgt moeten uiteindelijk ook weer kunnen worden verwijderd en mogen dus niet permanent worden opgeslagen in een blockchain. Het gaat hier namelijk om persoonsgegevens.

8 Is er een koppeling nodig met fysieke objecten?

Blockchain werkt alleen als de gegevens puur digitaal zijn. Je kunt niet met blockchain verifiëren of iets in de echte wereld verandert. Het is bijvoorbeeld niet handig om blockchain in te zetten voor het wereldwijd registreren van het eigendom van diamanten. Een blockchain kan immers nooit checken of een diamant ook echt fysiek is overhandigd aan een nieuwe eigenaar. Het verwerken van geld en de transacties ervan is wel mogelijk, want dit gebeurt tegenwoordig volledig digitaal.

*Vraag 1 t/m 8 met 'ja' beantwoord?
Bepaal dan met vraag 9 en 10 het soort blockchain.*





Meer over soorten blockchain vind je op pagina 12 onder 'Wie mag wat op de blockchain'.

Soorten blockchain

9 Mogen de transacties publiek inzichtelijk zijn?

Publiek betekent dat iedereen een wijziging of transactie kan inzien. Dat is bijvoorbeeld niet gewenst bij het vastleggen van behaalde resultaten of notities over het gedrag van een leerling. Als het om dit soort vertrouwelijke informatie gaat, moet je kiezen voor privaat: een beperkt aantal van tevoren aangewezen partijen die deze informatie wel mogen bekijken en verifiëren. Bij andere zaken is het juist weer handig om voor publiek te kiezen. In het onderwijs zijn er weinig soorten informatie te bedenken die publiek inzichtelijk moeten zijn. In het publieke domein zou je wel kunnen denken aan kadastrale informatie, waarbij juist de historie van eigenaarschap van gebouwen relevant is en publiek beschikbaar moet zijn.

10 Zijn de partijen die de transacties vastleggen bekend?

In het onderwijs is dit vaak het geval. Als schoolbesturen bijvoorbeeld alleen onderling gegevens willen uitwisselen, overdragen en verifiëren – bijvoorbeeld omdat ze andere partijen zoals het ministerie van OCW niet direct vertrouwen – kunnen ze gebruikmaken van een permissioned blockchain waarbij alleen zij deelnemers zijn.





Wie mag wat op de blockchain?

De blockchain die wordt gebruikt voor Bitcoin-transacties is volledig openbaar en iedereen kan transacties toevoegen. Maar er zijn ook andere varianten van blockchains mogelijk. We leggen hieronder de verschillen uit.

Publiek versus privaat

Vooraf wordt afgesproken hoe toegankelijk de gegevens zijn die worden opgeslagen in de blockchain. Ofwel alles is publiek, ofwel alles wordt alleen in beperkte kring gedeeld (privaat).

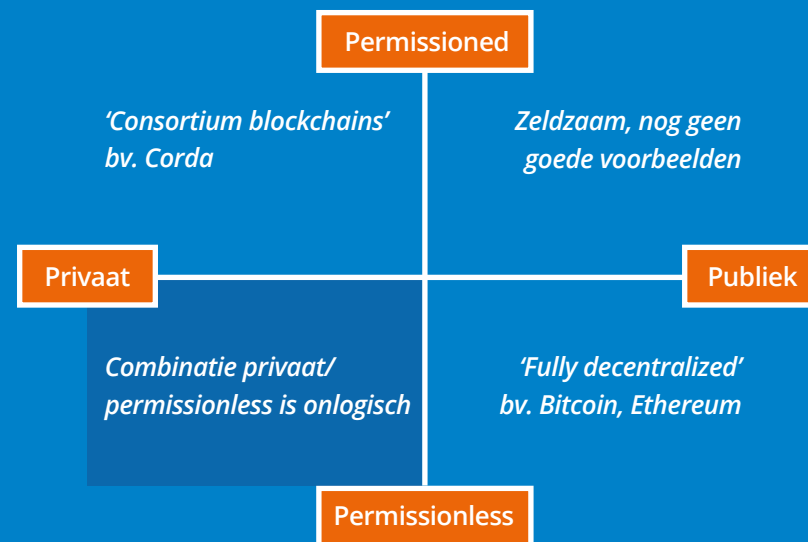
Permissionless versus permissioned

Bitcoin is een voorbeeld van een permissionless blockchain: iedereen mag deelnemen en nieuwe transacties toevoegen en blokken verifiëren. In een permissioned blockchain is vastgelegd wie of welke partijen dit mogen doen. Dit type blockchain is over het algemeen efficiënter omdat het aantal verifiërende partijen beperkt is, bijvoorbeeld een aantal partijen die samenwerken binnen het onderwijs.

Soorten blockchain

Traditionele blockchains zoals Bitcoin zijn publiek en permissionless. Er is een beperkt aantal voorbeelden van privaat en permissioned (consortium) blockchains, zoals Corda dat transacties tussen bestaande financiële instellingen vastlegt. Deze combinatie biedt echter zelden meerwaarde boven een al bewezen functioneel vergelijkbare oplossing.

Publieke permissioned blockchains bestaan nog nauwelijks. Een mogelijke toepassing zou kunnen zijn overheidsinstanties die blokken mogen toevoegen en verifiëren en die de informatie hierover publiek beschikbaar stellen. Een combinatie van privaat en permissionless is onlogisch. Als iedereen blokken mag verifiëren, is de informatie in deze blokken namelijk automatisch publiek toegankelijk omdat iedereen een kopie van het register kan hebben.





Conclusie: nog weinig zinvolle onderwijstoepassingen

Blockchain is een ware hype. Het is een nieuwe technologie die volgens sommigen een grote impact kan hebben op hoe vertrouwen digitaal vorm kan worden gegeven. Tegelijk is gebleken dat blockchain nog een onvolwassen technologie is met beperkingen in het publieke domein. In deze verkenning hebben we geen volwassen toepassingen gevonden die relevant zijn voor het Nederlandse onderwijs.

Er zijn tal van uitdagingen in het onderwijs waarin blockchain-achtige oplossingen op het eerste gezicht een rol zouden kunnen spelen. Binnen het onderwijs zijn veel verschillende partijen betrokken bij het verzorgen van onderwijs. De uitwisseling van informatie over bijvoorbeeld leerlingen vindt plaats tussen publieke en private partijen, zorgverleners, leerbedrijven en ouders/verzorgers. Deze partijen hebben soms uiteenlopende belangen waardoor ze elkaar niet altijd vertrouwen. Op het eerste gezicht lijkt de onderwijswereld dus een ideale plek om blockchain te implementeren. Als je die echter goed analyseert – de checklist is een nuttige eerste stap voor zo'n analyse – zie je dat er nauwelijks concrete problemen te vinden zijn waarvoor blockchain een oplossing is.

Blockchaintechnologie vaak niet de beste oplossing

Blockchain biedt vooral meerwaarde wanneer aan alle voorwaarden in de checklist wordt voldaan. Anders is een andere, al bewezen functionaliteit meestal beter en eenvoudiger. Bovendien is een dergelijke oplossing vaak veel goedkoper omdat de kosten voor het toepassen van een bestaand product niet in verhouding staan tot de kosten om een nieuwe toepassing te ontwikkelen, testen en te implementeren.

Blockchaintechnologie is nog volop in ontwikkeling, ook buiten de financiële sector. Sommige van de huidige beperkingen, zoals de benodigde rekenkracht voor het verifiëren van transacties, worden in toekomst mogelijk verholpen door andere verificatiemechanismen. Voor nu moet de conclusie zijn dat blockchaintechnologie nog niet zinvol toegepast kan worden in het onderwijs. Pilots en verkenningen kunnen zinvol zijn om de technologie beter te leren kennen, daarbij moeten de verwachtingen van concrete resultaten niet te hoog zijn. En ook dan blijven de vragen uit de checklist relevant.





Een verkenning van blockchaintechnologie in het onderwijs

Datum van uitgave
Oktober 2018

Auteurs
Els Booij, Wietse van Bruggen,
Michael van Wetering

Redactie
Voxx Content in Context

Vormgeving
Tappan Communicatie

Met dank aan
InnoValor: Willem Noort, Marlies Rikken
en Maarten Wegdam
saMBO-ICT: Joël de Bruijn
SURF: Frans Ward

Deze brochure is ontwikkeld door Kennisnet en is mede mogelijk gemaakt door inhoudelijke input van InnoValor, SURF en SAMBO-ICT. Het rapport "Blockchain voor SURFnet en aangesloten instellingen – Een technologieverkenning" (november 2017) van SURF heeft als bron en inspiratie gediend voor deze publicatie.

Sommige rechten voorbehouden
Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

Over Kennisnet
Elke leerling verdient eigentijds, veilig en persoonlijk onderwijs. Daarom ondersteunt Kennisnet scholen met ict. We zorgen voor een landelijke ict-basisinfrastructuur, adviseren de sectorraden en delen onze kennis met het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo). Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).



kennisnet.nl



Kennisnet
Paletsingel 32
2718 NT Zoetermeer

T 0800 321 22 33
E support@kennisnet.nl
I kennisnet.nl

Postbus 778
2700 AT Zoetermeer