Publicatie : NRC
Datum : 09 okt 2021 Regio : Nederland Pagina : 94 Bereik : -1
cm2 : 1089 Frequentie : 6x per week AVE : € 33362,00 Oplage : 139.492

WISKUNDE

Authenticatie zonder identiteit

Hoe kun je bewijzen dat je iets weet, zonder kennis daarover te delen?

Door onze medewerker **Alex van den Brandhof**

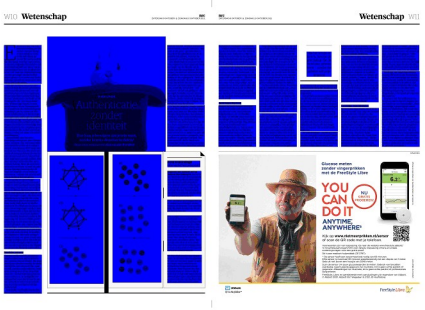
Een quizvraag: wat hebben een betaling, het bestellen van een biertje en het opladen van je Tesla met elkaar gemeen? Het antwoord: bij alle drie kan je een deel van je privacy moeten opgeven. Bij een niet-contante betaling blijft een spoor van je pinbetaling achter. Een student kan in het café naar zijn identiteitsbewijs worden gevraagd om zijn leeftijd prijs te geven. En waarom een Tesla-eigenaar zijn privacy soms moet inleveren, dat komt straks.

Alle drie hebben een potentiële toekomst met anonieme gebruikers, zonder noodzaak van een centrale autoriteit, maar wel met nagenoeg 100 procent betrouwbaarheid. Hoe dat kan? Dankzij een methode uit de cryptografie die 'zero knowledge' heet. Wiskundige Ronald Cramer vertelt erover in een Zoomgesprek. Hij is hoofd van de onderzoeksgroep cryptologie van het Centrum Wiskunde & Informatica in Amsterdam en hoogleraar cryptologie in Leiden.

„Zero knowledge wordt gebruikt om te voorkomen dat partijen zich misdragen. Dankzij zero knowledge kunnen deelnemers aan complexe systemen bewijzen dat ze zich correct gedragen, zonder ook maar iets extra's te verklappen."

Aanvankelijk was het zero-knowledgeconcept een puur theoretische exercitie. Het werd rond 1985 ontwikkeld door drie wiskundigen van het Amerikaanse MIT en de universiteit van Toronto. Het werkt een beetje als een goochelaar die een konijn uit een hoed tovert. Vooraf laat hij de lege hoed aan zijn publiek zien. Geen verstopt achterdeurtje, geen dubbele bodem. Maar als even later het konijn zichtbaar is, heeft de goochelaar daarmee bewezen dat de hoed wel degelijk een of ander geheim bevat - zonder dat geheim zelf prijs te hebben hoeven geven.

Centraal bij zeroknowledge-bewijzen is een protocol, een soort vraag-en-antwoordspel tussen twee personen, een *prover* en een *verifier*. Om te verifiëren dat de *prover* echt een of ander geheim kent, stelt de *verifier* een reeks vragen. Als de *prover* het geheim kent, kan hij elke vraag met zekerheid juist beantwoorden. Maar als hij bluft, heeft hij bij elke ronde een fiftyfiftykans op succes. De kans om twintig vragen op rij correct te beantwoorden, is dan minder dan één op miljoen. Deze kans daalt exponentieel; bij honderd rondes is die nagenoeg nul. Een oneerlijke *prover* is daardoor niet in staat om met succes te bedriegen - een eigenschap die wiskundigen 'soundness' noemen.



Publicatie : NRC
Datum : 09 okt 2021 Regio : Nederland Pagina : 94 Bereik : -1
cm2 : 1089 Frequentie : 6x per week AVE : € 33362,00 Oplage : 139.492

In 1991 landde deze techniek écht in de wiskunde, dankzij de Israëliër Avi Wigderson. Met twee collega's toonde hij voor een grote klasse wiskundige problemen aan dat er áltijd een zeroknowledgebewijs bestaat - een van zijn wapenfeiten die Wigderson dit jaar de Abelprijs opleverden.

Moeilijke puzzels

Tegenwoordig vormen zeroknowledgebewijzen een spil bij initiatieven rondom decentralisatie. Het gaat daarbij om situaties waarbij de macht niet bij één centrale partij ligt, maar waarbij partijen samenwerken. Denk in de analoge wereld aan bepaalde taken die van het Rijk naar gemeenten verschuiven. In de digitale wereld gaat het erom dat de macht om een netwerk te beheren verschuift naar meerdere partijen of eindgebruikers zelf.

Een ander voorbeeld: transacties met cryptomunten. Bij cryptovaluta, zoals de bitcoin, worden transacties niet door één centrale instantie - een bank in dit geval - gecontroleerd, maar door de gebruikers van de zogeheten blockchain, waarop die transacties worden geregistreerd.

Een blockchain is een soort keten van computers. Elke computer bevat een kopie van de data die op de blockchain zijn opgeslagen. Het toevoegen van nieuwe informatie daaraan gebeurt met geavanceerde technieken uit de cryptografie. Denk aan moeilijke puzzels, die de computers op de blockchain moeten oplossen. Pas nadat dat elke computer is gelukt, wordt die informatie - een transactie als het om geld gaat - toegevoegd. In plaats van één centrale bank ligt de controle dus bij alle gebruikers. Omdat niemand op eigen houtje informatie kan wijzigen, is de veiligheid ongekend hoog.

De bitcoin mag dan zonder centrale bank functioneren, wat bitcoin gemeen heeft met een klassieke pinbetaling is dat gebruikers hun privacy inleveren. Alle transacties blijven altijd zichtbaar op de blockchain.

Dat het ook anders kan, bewijst de firo. Deze cryptomunt is in veel opzichten vergelijkbaar met de bitcoin. Allebei worden ze gerund op decentrale netwerken en maken ze gebruik van geavanceerde cryptografie, met openbare en geheime sleutels. Het grote verschil: de firo heeft zero knowledge in zijn protocol verwerkt. Elke gebruiker kan daardoor volledig anoniem én veilig geld overmaken.

De blockchains van cryptomunten zijn het bekendst, maar blockchains kunnen meer. Estland was bijvoorbeeld het eerste land in Europa dat de overheidsadministratie en patiëntendossiers opslaat op een blockchain. Het is efficiënt en kostenbesparend.

En is het ook veilig? In Estland beweert men van wel. Voor veel andere landen, waaronder Nederland, is de technologie niet rijp genoeg om in de zorgsector te gebruiken. „Blockchain kán een toegevoegde waarde hebben, maar wees zorgvuldig", was de conclusie van twee onderzoeken die Zorginstituut Nederland in 2019 liet uitvoeren. Is het privacyvraagstuk een knelpunt? Niet als zero knowledge op de juiste manier geïmplementeerd wordt.

Strijd tegen Big Tech

Binnen de blockchaintechnologie wordt veel onderzoek gedaan naar een nieuwe vorm van zeroknowledgebewijzen, de 'zk-SNARKs'. De term 'zk-SNARK' staat voor *zero-knowledge Succinct Non-Interactive Argument of Knowledge*. Nóg abstracter dan de traditionele zero-knowledgebewijzen - laat op deze plek genoeg zijn dat het bij deze nieuwe variant niet nodig is dat er communicatie nodig is tussen de *prover* en *verifier*. Handig, omdat het in de praktijk van grote gedecentraliseerde netwerken onrealistisch is dat gebruikers permanent online zijn.

Mogelijke toepassingen zijn er volop. Google Scholar vindt vanaf begin 2020 al zo'n drieduizend resultaten. Zo werken onderzoekers van de TU Delft mee aan de ontwikkeling van eIDAS, een EU-brede aanvulling op het bekende DigiD. En in maart van dit jaar deden de Delftenaren een proef met studenten. De horeca was gesloten, maar de wetenschap ging door in coronatijd , dus mocht biercafé Doerak in Delft zijn deuren even openen voor een experiment. Hoe bewijs je dat je alcohol mag drinken zonder je geboortedatum kenbaar te maken?

Onderzoeksleider Johan Pouwelse van het Delft Blockchain Lab: „Onze veldtest toont aan dat je met je mobiel en een veilige QR-code met behulp van een zeroknowledgebewijs kunt aantonen dat je 18+ bent." Voor identiteitsverificatie zijn daar bovenop nog wel biometrische persoonsgegevens nodig. Anders kan een 17-jarige makkelijk de smartphone van een oudere broer of zus lenen.

Een toepassing uit een heel andere hoek: geconnecteerde voertuigen, auto's die verbonden zijn met je smartphone, met de garage, oplaadstations en dergelijke. Het opladen van een elektrische auto kost tijd, waardoor planning vooraf nodig is. Bij de serviceproviders zijn de locaties en het oplaadpatroon van de auto dan bekend. Onderzoekers van de Florida International University publiceerden vorig jaar een artikel waarin zij een zeroknowledgebewijs presenteren dat privacybehoudende authenticatie mogelijk maakt en de noodzaak van een centrale autoriteit wegneemt.

Een ambitieus nieuw project komt van Dfinity, een non-profitorganisatie die in mei het startschot gaf voor het creëren van een 'nieuw internet', gebaseerd op blockchaintechnologie. Dfinity werd in 2015 opgericht in Californië en heeft tegenwoordig nog een tweede onderzoekscentrum in het Zwitserse Zug. Het ideaal van Dfinity is een vrij en open internet, waarbij techreuzen als Amazon, Alphabet en Microsoft niet langer heer en meester zijn over iemands gegevens.

De ontwikkelaars van Dfinity werken aan een gedecentraliseerd blockchainnetwerk dat zo'n vrij internet mogelijk moet maken. Het doel is dat het netwerk uitgroeit tot duizenden onafhankelijke datacenters, verspreid over de hele wereld. IT-systemen kunnen daar dan rechtstreeks op draaien en zijn niet meer afhankelijk van centrale platforms.

Dfinity kreeg rijke investeerders zo ver om hun revolutionaire plannen met miljoenen dollars te ondersteunen. Aan het feit dat allerlei relevante gegevens gevoelig zijn om over miljoenen computers wereldwijd te distribueren, hebben de tweehonderd techspecialisten van Dfinity uiteraard gedacht. Cramer: „Onder de motorkap van Dfinity speelt zero knowledge een sleutelrol om ervoor te zorgen dat partijen aan de rest van het netwerk kunnen aantonen dat ze zich gedragen, zonder dat ze geheime informatie prijsgeven die een kwaadwillende deelnemer in staat zou stellen de functionaliteit van de machine te ondermijnen."

Van mega- naar kilobytes

Bij dat tover-ingrediënt, dat er in de digitale wereld voor zorgt dat iemand de controle over zijn privacy behoudt, vraag je je tegelijkertijd af of er niet ook bezwaren zijn. Kun je een zeroknowledgebewijs faken? Is de technologie ecologisch verantwoord? Het zijn twee voor de hand liggende vragen. Nee, is het antwoord op de eerste vraag. Zeroknowledgebewijzen zijn *safe* en dat komt door de 'soundness-eigenschap'. Wat betreft de tweede vraag: zero knowledge heeft juist de laatste jaren een enorme ontwikkeling in de efficiëntie doorgemaakt. Cramer: „De data die je bij een zeroknowledgebewijs moet communiceren is van mega- of giga- naar kilobytes gegaan." Drie jaar geleden was er voor een firo-transactie op een moderne laptop meer dan een halve minuut rekentijd nodig. Na een upgrade met diverse cryptografische innovaties werd dit teruggebracht naar twee seconden.

Publicatie : NRC
Datum : 09 okt 2021 Regio : Nederland Pagina : 94 Bereik : -1
cm2 : 1089 Frequentie : 6x per week AVE : € 33362,00 Oplage : 139.492

En drugs- en wapenhandelaars, kunnen die hun zwarte firomunten dankzij zero knowledge niet makkelijk witwassen omdat de transacties voor het publiek onzichtbaar zijn? Cryptomuntontwikkelaar Riccardo Spagni zei eens in een interview: „Als het goed genoeg is voor een drugsdealer, is het goed genoeg voor alle anderen."

Cramer vindt het volkomen verkeerd om een verband te leggen tussen fraude en zero knowledge: „Zero knowledge ís geen digitale munt, noch een blockchain. Het is een methode uit de cryptografie om van een gecodeerde boodschap een gewenste eigenschap te bewijzen, zonder die boodschap zelf prijs te geven." Cramer vergelijkt het met een raket waar de aandrijving verkeerd is ingehangen. „Dat kun je de aandrijving natuurlijk niet aanrekenen." En zo is het met op zero knowledge gebaseerde cryptomunten ook. „Zero knowledge is een algemeen principe. Firo is een 'macroscopische toepassing' die daar, al dan niet op correcte wijze, gebruik van maakt."

Als het konijn te zien is, bewijst de goochelaar dat de hoed een geheim bevat - zonder dat geheim zelf prijs te geven

Zero knowledge

Hoe werkt het protocol?

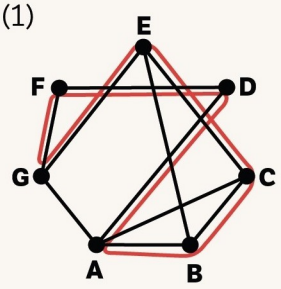
Gegeven: een netwerk dat bij Prem en Vera bekend is. In rood is een hamiltoncircuit (1) aangegeven: een wandeling waarbij elk knooppunt één keer wordt aangedaan. Prem beweert dat het netwerk zo'n circuit bevat. Vera wil weten of hij niet bluft. Hoe kan Prem bewijzen dat hij zo'n circuit kent, zónder de lijnen daarvan prijs te geven?

Prem hernoemt de knooppunten (2) en noteert van elk lijnstuk de hernoemde eindpunten (3) op een bierviltje. Hij draait de viltjes om (4), zodat Vera ze niet ziet.

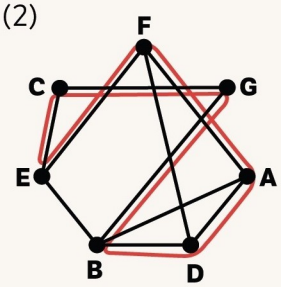
Vera vraagt Prem het complete netwerk (5) óf het circuit (6) te laten zien. Bij (5) zegt hij hoe hij de punten had hernoemd en draait alle viltjes om. Vera kan dan het netwerk construeren en vaststellen dat dit overeenkomt met het origineel, maar over het circuit weet ze niets. Bij (6) draait Prem alleen de viltjes om waarop de circuitlijnen staan. Vera kan dan zien dát er zo'n circuit bestaat, maar omdat de knooppunten hernoemd zijn, weet ze niet waar het zich in het netwerk bevindt.

Als Prem bluft, kan hij twee dingen doen: hij hernoemt de knooppunten óf hij verzint een even groot netwerk met daarin een hamiltoncircuit. Hij heeft dus 50 procent kans op overleven. Maar Prem en Vera herhalen dit vraag-en-antwoordspel heel vaak. De kans dat Vera's checks allemaal goed gaan, daalt dan exponentieel snel naar nul. Als Prem niet bluft, gaan al Vera's checks goed.

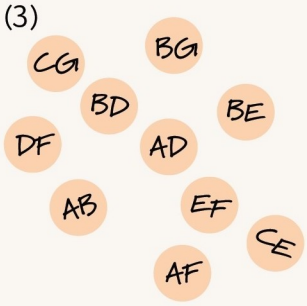
(1)



(2)



(3)



Publicatie : NRC
Datum : 09 okt 2021 Regio : Nederland Pagina : 94 Bereik : -1
cm2 : 1089 Frequentie : 6x per week AVE : € 33362,00 Oplage : 139.492