Gedistribueerde systemen: van efficiëntie tot vertrouwen

Intreerede

uitgesproken door

prof.dr.ir. D.H.J. Epema

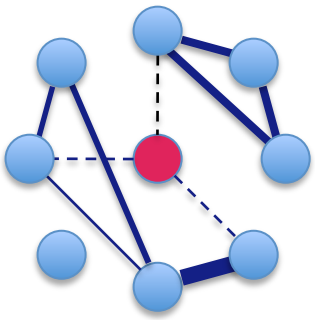
op 27 mei 2016

bij de aanvaarding van het ambt van hoogleraar in de

Gedistribueerde Systemen

aan de

Technische Universiteit Delft



Mijnheer de rector magnificus,
Leden van het college van bestuur,
Collegae hoogleraren en andere leden van de universitaire gemeenschap,
Zeer gewaardeerde toehoorders,
Dames en heren,

1. Inleiding

Slide 1: Gedistribueerde systemen: van efficiëntie tot vertrouwen
Hoe vaak heeft U vandaag Uw smart phone of tablet gebruikt? En als U dat deed, wat deed U er dan mee? Heeft U de route naar de aula van de TU Delft opgezocht? Of heeft U snel even een bedrag overgemaakt via Uw bank? Heeft U wellicht nog iets gegoogled vandaag? En heeft U misschien zelfs, ik durf het bijna niet te vragen, opgezocht wat gedistribueerde systemen zijn? Veiligheidshalve ga daar maar niet vanuit.

Wat ik vanmiddag dan ook eerst zal doen is U uitleggen wat de kenmerken van gedistribueerde systemen zijn aan de hand van een klein beetje geschiedenis en een paar voorbeelden. Het zal U dan hopelijk duidelijk worden dat dergelijke systemen de gewoonste zaak van de wereld zijn. Daarna zal ik U iets vertellen over het onderzoek in gedistribueerde systemen dat ik met mijn groep doe.

Slide 2: Wat is een gedistribueerd systeem?
Het begin van het vakgebied Gedistribueerde Systemen is vrij nauwkeurig te bepalen. Tot 1980 waren computers bakbeesten die in grote speciale kamers in hun eentje hun werk stonden te doen. Omstreeks 1980 kwam daar verandering in. Computers werden veel kleiner en goedkoper—de PC kwam er aan—maar nog veel belangrijker is dat veel van de netwerktechnologie die we nu nog gebruiken, uit die tijd stamt. Daardoor waren computers die geografisch gespreid, oftewel gedistribueerd, opgesteld stonden in staat met elkaar te communiceren en met elkaar samen te werken. Zo konden ze nu gemakkelijk bestanden bij elkaar ophalen en email versturen. Communicatie en samenwerking, dat zijn de kenmerkende eigenschappen van een gedistribueerd systeem.

Slide 3: 2005-2015: Twee trends
Als we nu een grote sprong in de tijd maken, dan zien we dat in de laatste tien jaar twee trends de ontwikkeling van computersystemen in de wereld hebben gedomineerd. Ten eerste zijn dat datacenters, grote fabriekshallen met eentonige rijen kasten zoals U hier ziet, die vol geschoven zijn met een soort grote grijze pizzadozen. Dat zijn de computers. Aan de achterkant van die

kasten is het een grote warboel van draden die al die computers met elkaar verbinden. Als U ergens een beetje afgelegen in het landschap een wat sinister gebouw ziet staan met een hoog hek erom heen zonder duidelijk opschrift, dan kan dat zomaar een datacenter zijn. De bovenste foto voldoet aardig aan deze beschrijving. Het is een datacenter op slechts een paar kilometer hier vandaan. Als je als datacenters alleen de speciaal voor dat doel bestemde gebouwen telt, staan er in Nederland op dit moment 171. De afmeting van datacenters kan oplopen tot meer dan 30.000 vierkante meter. Overigens zal ik vandaag ook zo nu en dan het woord “cluster” gebruiken. Dat is apparatuur van dezelfde soort als in datacenters, maar van bescheidener omvang.

De tweede trend zijn tablets en smart phones, waarvan er onderhand miljarden zijn. Via deze apparaten doet U erg weinig dat geen communicatie vereist met datacenters.

Van de drie voorbeelden van gedistribueerde systemen die ik nu zal geven kent U de eerste twee allemaal, de derde zal U misschien verrassen.

Slide 4: De Google zoekmachine: efficiëntie
Allemaal voeren we dagelijks veel zoekopdrachten op het internet uit. Eén van de meest populaire systemen daarvoor is de Google zoekmachine, die we met z’n allen zo’n 4 miljard keer per dag raadplegen! Daarvoor verzamelt Google continu zoveel mogelijk pagina’s van het world wide web en bepaalt het van ieder van die pagina’s hoe belangrijk die is met een methode die *pagerank* wordt genoemd. Die methode komt erop neer dat hoe vaker er naar een webpagina verwezen wordt, hoe belangrijker deze is, wat in dit plaatje wordt geïllustreerd. De mate van belangrijkheid van pagina’s bepaalt mede hun volgorde in de antwoorden die Google stuurt.

De PCs, tablets en smart phones van de gebruikers, de computers in de Google datacenters, en de computers met webpagina’s vormen één groot gedistribueerd systeem. Gemiddeld werken per zoekopdracht 1000 computers in een datacenter gedurende tweetiende van een seconde met elkaar samen, en dat is al een gedistribueerd systeem op zich. In dit voorbeeld speelt efficiëntie een grote rol: Google wil veel zoekacties uitvoeren, en U wil snel antwoord ontvangen.

Slide 5: De Ebay markt: vertrouwen
Mijn tweede voorbeeld is Ebay, dat kopers en verkopers van tweedehands en nieuwe spullen bij elkaar brengt. Hoewel efficiëntie ook hier een rol speelt, is het veel belangrijker dat de koper en verkoper elkaar vertrouwen—de koper wil een goed artikel ontvangen, de verkoper wil zijn geld hebben. Ebay heeft hiervoor een reputatiesysteem met feedbackscores en sterren. Een verkoper krijgt of verliest een punt voor iedere positieve of negatieve feedback die hij krijgt na een transactie. Het puntentotaal bepaalt iemands reputatie, die wordt uitgedukt met een ster van een bepaalde kleur, en die je kunt gebruiken om te bepalen of je al dan niet met hem in zee wilt gaan.

Slide 6: Een groep van …
Mijn derde voorbeeld betreft eenvoudigweg een groep mensen die iets met elkaar te maken hebben, zoals collega's in een bedrijf of leden van een gezin. Veel elementen van gedistribueerde systemen vinden we hier terug. Mensen zijn tot op zekere hoogte autonoom, maar ze moeten wel met elkaar samenwerken. Daarvoor moeten ze met elkaar communiceren, maar verbindingen kunnen uitvallen en berichten kunnen verloren gaan. Als er niet snel genoeg reactie komt op een bericht, versturen ze het nog een keer. En mensen kunnen het natuurlijk met elkaar oneens zijn, maar moeten dan toch tot overeenstemming zien te komen.

In plaats van personen als leden van een groep had ik net zo goed de afdelingen van een bedrijf, de faculteiten van een universiteit, of de ministeries in Den Haag kunnen nemen. De moraal van dit verhaal is dat veel problemen in gedistribueerde systemen lijken op problemen in systemen die allang bestonden voor er computers waren. Van oplossingen die in die systemen zijn bedacht kunnen we leren voor gedistribueerde systemen.

In de rest van deze rede zal ik iets meer vertellen over de twee onderzoeksrichtingen van mijn groep. Eén heeft te maken met efficiëntie in datacenters, de ander met vertrouwen tussen gebruikers.

2. Gedistribueerde gegevensverwerking

Slide 7: Gedistribueerde gegevensverwerking
De eerste van die richtingen is gedistribueerde gegevensverwerking. De totale hoeveelheid digitale gegevens in de hele wereld is nu zo'n 10 zettabyte. Dat zegt zelfs binnen de informatica niet veel mensen meteen iets, maar het komt neer op 300.000 digitale foto's in hoge resolutie voor iedere aardbewoner. Al deze gegevens moeten worden bewerkt door gedistribueerde systemen. Hier ziet U de stappen die daarvoor nodig zijn:

1. Allereerst is er de toepassing, met een beschrijving van de gegevens en de vraag die over die gegevens moet worden beantwoord—denkt U bij voorbeeld aan het bepalen van de belangrijkheid van webpagina's.

2. Daarna moet er een algoritme worden gekozen of gemaakt dat de vraag beantwoordt, bijvoorbeeld pagerank.

3. Dan moet een programma worden geschreven dat het algoritme uitvoert. Zo'n programma kan bestaan uit meer dan honderduizend aparte taken die met elkaar communiceren. Dat is hier geïllustreerd met de ovalen als de taken en de rechthoeken als de gegevens die ze aan elkaar sturen.

4. En tenslotte, en dat doen we in de Groep Gedistribueerde Systemen, is er de gedistribueerde gegevensverwerking, het bepalen van de verdeling van de programma's en de gegevens over de beschikbare computers en de optimalisatie van de verwerking.

Slide 8: Ketens van gegevensverwerking
Gedistribueerde gegevensverwerking omvat veel meer dan alleen het uitvoeren van programma's in datacenters. Er is meestal een hele keten van het verzamelen, het filteren, het verdelen, het verwerken, het analyseren en het opslaan van gegevens. Het voorbeeld dat ik hier laat zien is dat van de deeltjesversneller bij CERN in Genève, die per jaar 30.000 Terabyte aan meetgegevens over botsingen van elementaire deeltjes verzamelt. Deze gegevens worden verdeeld over 170 datacenters in 42 landen, en de resultaten moeten aan het eind worden verzameld, geanalyseerd en opgeslagen.

Slide 9: Uitdagingen en oplossingen
Gedistribueerde gegevensverwerking is zeker geen revolutionair onderwerp, maar het is een wel onderwerp waarin aldoor nieuwe uitdagingen ontstaan. Eén daarvan is de aldoor toenemende schaal, die zich uit in de hoeveelheid gegevens en de afmeting van de programma's en de datacenters. Dat een grotere schaal vraagt om nieuwe oplossingen zien we al bij heel simpele problemen. Een afspraak maken met een man of vijf lukt nog wel gewoon per email, maar bij meer personen moeten we onze toevlucht nemen tot datumprikkers en doodles.

Een andere uitdaging komt voort uit aldoor nieuwe typen toepassingen. In het door Alexandru Iosup van onze groep geleide project Graphalytics ontwerpen en beoordelen we gedistribueerde systemen voor *graph processing*. Dat is het analyseren van netwerken, zoals dat van LinkedIn met zijn connecties tussen honderden miljoenen leden.

Slide 10: Hoe verdeel je de capaciteit van datacenters?
Wat ik tot nu toe verteld heb ging over de efficiënte verwerking van een enkele job. Echter, datacenters moeten een continue stroom van jobs verwerken, van korte zoekopdrachten tot jobs die uren bezig zijn met pagerank. De vraag is dan hoe de beschikbare rekencapaciteit over al die jobs moet worden verdeeld. De werkelijkheid is nog veel complexer. Zo kunnen allerlei bedrijven een deel van de capaciteit van een datacenter huren zoals in de cloud, met ieder hun eigen jobs. En wellicht kan de totale belasting over meerdere datacenters worden gespreid.

Ik zal U nu aan de hand van een concreet voorbeeld een idee geven van ons onderzoek op dit gebied.

Slide 11: Probleem: “slowdown” door grote klanten
Veel problemen om capaciteit te verdelen in gedistribueerde systemen laten zich aan de hand van alledaagse situaties uitleggen. In dit geval is dat een supermarkt. Als iemand met maar een paar artikelen de pech heeft bij de kassa achter iemand met een volle kar te staan, zal zijn wachttijd aanzienlijk oplopen. De maat die wij gebruiken voor dit verschijnsel is de zogenaamde “slowdown”. Die wordt berekend door de tijd die een job in totaal kwijt is te delen door de tijd die nodig is voor zijn bediening. In dit voorbeeld is de tweede klant in totaal 20 plus 180 seconden bij de kassa kwijt, en is zijn slowdown dus 10. De kleintjes lijden onder de grote.

Slide 12: Oplossing: snelkassa’s
Een oplossing die supermarkten vooral in de VS hiervoor hebben is aparte kassa’s voor klanten met weinig artikelen.

Slide 13: Rijen in datacenters
Hoe kunnen we dit idee nu in datacenters gebruiken? Wel, we kunnen de computers in partities verdelen, net zoals de kassa’s in een supermarkt, ieder met zijn eigen rij van jobs. Als we aannemen dat we de verwerkingstijd van jobs goed kunnen schatten, gebruiken we de timers behorend bij de rijen om te bepalen bij welke rij een job moet aansluiten.

In de praktijk kunnen we zulke schattingen vaak niet doen. In dat geval laten we alle jobs bij rij 1 aankomen en geeft de timer van iedere rij de maximale hoeveelheid bediening aan die ze daarin krijgen. Overschrijdt een job die hoeveelheid, dan moet hij bij de volgende rij aansluiten om daar verder bediend te worden. In een supermarkt zou zulke terugkoppeling natuurlijk een bende worden.

We kunnen de partitionering ook gewoon achterwege laten. Wat we dan wel doen is de rijen een prioriteit geven: iedere processor die vrij komt zoekt eerst naar werk in rij 1, als die leeg is in rij 2, etc.

Slide 14: Hoe groot is de verbetering?
Ik zal U nu het voornaamste resultaat van dit onderzoek laten zien. Deze grafiek laat de slowdowns van de jobs zien met de normale manier om de capaciteit te verdelen. Voor iedere job die is uitgevoerd is er een klein rondje zichtbaar. Op de horizontale as staat het totale aantal seconden dat alle taken van een job bij elkaar nodig hebben gehad, met een logaritmische schaal. De grootste jobs zijn 10.000 keer zo groot als de kleinste. Op de verticale as staat de slowdown van de jobs. Twee dingen vallen op: de slowdown bereikt waarden van maar liefst 60, en de grootste slowdowns treden op links in de grafiek, bij de kleintjes.

In de tweede grafiek ziet U het resultaat van wat de beste manier van capaciteitsverdeling blijkt te zijn, zonder partitionering, maar met terugkoppeling. Wat direct opvalt is dat de slowdowns veel kleiner zijn, en dat

ze veel gelijkmatiger zijn over de afmetingen van jobs. Dit onderzoek is gedaan door Bogdan Ghiţ, een van mijn huidige promovendi.

Voor dit soort onderzoek doen we veel experimenten, iets waar ik nu in een intermezzo in het algemeen iets over wil vertellen.

3. Experimentele informatica

Slide 15: Experimenten in de informatica

Meer dan alleen theorie, is informatica ook een experimentele wetenschap. Zo kun je, als je bij voorbeeld nieuwe ideeën voor snellere zoekmachines of voor betere methoden voor capaciteitsverdeling hebt, die programmeren, installeren op een computersysteem dat je ter beschikking hebt, en hun gedrag in dat systeem analyseren. Als je daarvoor geen geschikt systeem hebt, kun je simulaties doen. Dan programmeer je een computermodel van wat je ook maar wilt onderzoeken en voert dat vervolgens uit op een meestal veel kleinere computer.

Slide 16: De Distributed ASCI Supercomputer

Bij het doen van experimentele informatica zijn er drie problemen. Allereerst is er voldoende geld nodig voor apparatuur. Nu zijn we in Nederland zo gelukkig dat we een gedistribueerd systeem hebben dat alleen bestemd is voor experimenteel informatica-onderzoek, de zogenaamde Distributed ASCI Supercomputer, de DAS. Dit systeem, met *clusters* bij de universiteiten in Amsterdam, Leiden en Delft, en bij ASTRON, het Nederlands Instituut voor Radio-Astronomie in Drente, is voor een groot deel door NWO gesubsidieerd. Het is nu al in zijn vijfde generatie, en heeft veel onderzoek in de informatica in Nederland mogelijk gemaakt. Tevens heeft de DAS geholpen om NWO ervan te overtuigen dat informatica ook een experimentele discipline is, die geld voor apparatuur nodig heeft.

In de Groep Gedistribueerde Systemen hebben we een traditie van echte experimenten, uiteraard op de DAS. Soms kost het echter teveel tijd om die te doen, omdat we teveel gevallen willen bestuderen. Ik heb het er net niet bij gezegd, maar het onderzoek naar capaciteitsverdeling dat ik U liet zien is nu juist met simulaties gedaan. Wel hebben we daarbij een paar experimenten op de DAS uitgevoerd om die simulaties te valideren. Het bleek dat de afwijking kleiner was dan 1%, wat verbluffend nauwkeurig is.

Slide 17: Wat zijn goede experimenten?

Het tweede probleem bij experimenten in de informatica is dat we in het toepassen van goede methoden daarbij achterlopen bij de “echte” beta-wetenschappen, zoals de natuurkunde. Om het beter te doen zou er meer aandacht moeten worden besteed aan drie aspecten:

Ten eerste de precieze beschrijving van experimenten zodat anderen in staat zijn ze te reproduceren, of althans volledig te begrijpen;

Ten tweede de vergelijkbaarheid van experimenten, waarmee ik bedoel dat onderzoekers hun experimenten zo inrichten dat hun werk met dat van anderen kan worden vergeleken;

En ten derde de duidelijke en volledige weergave, analyse en verklaring van de resultaten.

Helaas is het met deze aspecten in veel artikelen niet best gesteld.

Slide 18: Wat zijn informatica-experimenten waard?
Het derde probleem is de vraag wat de waarde is van experimenten in de informatica. Wat we namelijk aan het doen zijn is kunstmatige systemen maken die we daarna observeren om conclusies te trekken over hun gedrag, dat we nota bene zelf geprogrammeerd hebben. Dat is iets heel anders dan het observeren en bestuderen van de natuur om ons heen.

Hoe algemeen geldig zijn de resultaten van onze experimenten? Resultaten verkregen in het ene systeem hoeven niet overeen te komen met die in een ander systeem, dat misschien wel veel groter of nieuwer is. Ieder systeem is uniek in zijn specifieke structuur, en in feite creëren we onze eigen wereld als we een systeem of een simulatiemodel bouwen. Maar als we niet dezelfde conclusies kunnen trekken uit waarnemingen in verschillende systemen, bedrijven we dan wel wetenschap? Zijn er wellicht in de informatica verschillende werkelijkheden, in tegenstelling tot in de natuurwetenschappen?

Ik denk dat experimenten in gedistribueerde systemen en hun resultaten heel lang waardevol kunnen blijven als het onderzochte probleem abstract genoeg is en niet specifiek van bepaalde hardware afhangt, en als je verschillende oplossingen met elkaar vergelijkt. De onderlinge verschillen tussen de resultaten van die oplossingen doen er toe, niet de precieze waarden die ze opleveren. Het voorbeeld dat ik U gaf van de capaciteitsverdeling in datacenters voldoet aan deze twee criteria.

4. Cooperatieve systemen

Slide 19: Cooperatieve systemen
Ik kom nu tot onze tweede onderzoeksrichting, Cooperatieve Systemen. Dat is de naam die wij gebruiken voor systemen waarin de gebruikers vrijwillig via het internet transacties met elkaar aangaan. Die transacties kunnen van alles zijn: het uitwisselen van video's, het handelen in goederen via Ebay, of het huren van accommodatie via Airbnb. Voordat gebruikers bereid zijn een transactie met iemand aan te gaan, willen ze liefst zijn reputatie kennen en vertrouwen in hem hebben.

In de afgelopen vijftien jaar hebben we in onze groep veel onderzoek gedaan naar zogenaamde peer-to-peersystemen. Dat is een vorm van cooperatieve systemen waarin de deelnemers direct met elkaar communiceren, en niet via websites zoals die van Ebay. Eén zo'n systeem is het Tribler peer-to-peersysteem voor video-distributie, dat onder leiding van Johan Pouwelse van onze groep met een groot team is ontworpen. Tribler heeft een reputatiesysteem dat een hoge reputatie toekent aan peers die veel data naar anderen sturen, direct of indirect. Dat is hier links weergegeven met de zwarte pijlen. Hierdoor zijn peers bereid data naar hen terug te sturen als ze daarom vragen, hier weergegeven door de rode pijlen.

Eén van de doelen in deze onderzoeksrichting is om een universeel reputatiesysteem te ontwerpen waarin deelnemers hun reputatie van de ene omgeving naar de andere kunnen meenemen. Dat systeem moet bestand zijn tegen kwaadaardige lieden die reputaties kunstmatig willen schaden of juist opkrikken.

Slide 20: Bitcoin en de blockchain

Een onderwerp waarbij vertrouwen een wel heel grote rol speelt, is geld. In het verleden is vaak geprobeerd een virtuele valuta te ontwerpen waarbij geld elektronisch tussen computers wordt verstuurd zonder, en dat is essentieel, tussenkomst van banken. Het grootste probleem daarbij is om te voorkomen dat hetzelfde geld meerdere keren wordt uitgegeven. In het verleden is dit nooit gelukt, maar nu is er een virtuele valuta die daadwerkelijk wordt gebruikt, en die inwisselbaar is tegen echt geld, namelijk Bitcoin.

Bitcoin berust op een elegant gedistribueerd systeem dat de blockchain wordt genoemd. Kort gezegd, in de taal van bankrekeningen is de blockchain een door alle rekeninghouders gezamenlijk bijgehouden afschriftenboekje. Iedere 10 minuten komt er een nieuw afschrift, een block, dat alle overboekingen bevat die wereldwijd in Bitcoin zijn gedaan, en dat wordt gekoppeld aan het vorige block. Ik zal zo meteen vertellen doe die afschriften tot stand komen.

Bitcoin en de blockchain staan sinds kort erg in de belangstelling, in de wetenschappelijke wereld, bij financiële instellingen, en bij veel andere bedrijven. Geprobeerd wordt om de blockchain te gebruiken voor andere doelen dan alleen geld waarbij het onomstotelijk vastleggen van digitale gegevens vereist is, zoals aandelen, notariële aktes, en reserveringen van gemeenschappelijke auto's. Ook de overheid heeft begrepen dat Bitcoins echt wat waard zijn. Mocht U het idee opvatten om belasting te vermijden door vlak voor de jaarwisseling Uw vermogen in Bitcoins om te zetten en vlak erna weer terug, dan moet U eerst maar eens goed de toelichting bij de elektronische aangifte lezen.

De blockchain staat op onze onderzoeksagenda, om te kijken hoe die kan worden aangepast voor andere toepassingen dan virtuele valuta's, en om fundamentele problemen ervan aan te pakken. Ik zal U aan de hand van de

drie basisideeën van Bitcoin en de blockchain een paar van die problemen laten zien.

Slide 21: Hoe wordt dubbel uitgeven voorkomen?
Anders dan bij bankrekeningen worden in Bitcoin niet de saldi van de klanten bijgehouden, maar alleen alle overboekingen, hier transacties genoemd, die ooit zijn uitgevoerd. Daaruit kan het saldo van iedereen natuurlijk worden afgeleid. Een transactie moet de eerdere transacties aangeven die de bronnen zijn van het over te boeken bedrag. Transacties kunnen meerdere begunstigden hebben, wat kan worden gebruikt om eventueel wisselgeld naar jezelf terug te sturen. In andere toepassingen van de blockchain zal de inhoud van transacties natuurlijk heel anders zijn.

Bitcoin gebruikt versluieringstechnieken om transacties alleen leesbaar te maken voor degenen voor wie ze bedoeld zijn. Bitcoin-gebruikers hebben een sleutel, opgeslagen in een klein bestand, om na te gaan of zij de begunstigde van een transactie zijn. Zo'n sleutel moet je geheim houden en goed bewaren. Als iemand anders 'm in handen krijgt kan hij je Bitcoins uitgeven, en als je 'm kwijtraakt ben je ook je Bitcoins voor altijd kwijt. In Bitcoin worden alle transacties verspreid naar alle deelnemers via een peer-to-peersysteem. Het dubbel uitgeven van geld wordt dus voorkomen door alle transacties openbaar te maken!

Slide 22: Hoe worden transacties bevestigd?
Het verspreiden van transacties is niet genoeg, ze moeten ook worden gecontroleerd op dubbel uitgeven en ze moeten worden bevestigd. Dat gebeurt met blokken, de afschriften, die een verwijzing naar het vorige blok en nog niet bevestigde transacties bevatten. Ook de blokken worden via het peer-to-peer-systeem naar iedereen verspreid.

Om een blok te maken moet een Bitcoin-deelnemer zelfgekozen gegevens aan een blok toevoegen zodat een bepaalde bewerking uitgevoerd op het hele blok een extreem klein getal oplevert. Aangezien het resultaat van die bewerking volstrekt onvoorspelbaar is, komt dit neer op ontzettend vaak gokken. Dit kost erg veel rekentijd op computers, maar bewijst wel dat de maker van een blok veel werk heeft verzet.

Bitcoin-deelnemers zijn bereid om blokken te maken omdat ze er een beloning voor krijgen. Ze mogen namelijk in een blok een transactie opnemen die uit het niets een bedrag van 25 BTC naar henzelf overmaakt, wat tegen de huidige koers neerkomt op ruim 11.000 Dollar. Het systeem is zo ingesteld dat er maar één blok per 10 minuten wordt gemaakt. Dit leidt tot het fundamentele schaalbaarheidsprobleem dat er in Bitcoin wereldwijd maar ongeveer 100 transacties per minuut kunnen worden gedaan, terwijl er in Nederland alleen al 6000 PIN-transacties per minuut plaatsvinden.

Slide 23: Hoe worden transacties vastgelegd?
Uiteindelijk worden alle transacties in Bitcoin voor iedereen in het peer-to-peer-systeem zichtbaar vastgelegd in de blockchain, de keten van alle blokken. Het is echter mogelijk dat twee deelnemers ongeveer gelijktijdig een nieuw blok vinden dat volgt op hetzelfde vorige blok. Hierdoor vindt er een vertakking in de blockchain plaats. Dit is een typisch probleem in gedistribueerde systemen: bijna gelijktijdig doen verschillende computers bij gebrek aan communicatie tegenstrijdige acties en zijn ze het dus oneens. Er is een manier om het weer eens te worden waarbij één van de twee takken wordt afgestoten. Alle transacties in die tak worden dan ongeldig, en moeten opnieuw worden gedaan. En dit is het tweede fundamentele probleem van de bockchain: het duurt veel te lang voor een transactie zeker is, je moet daarvoor toch wel een uur wachten.

Ik kan moeilijk geloven dat valuta's als Bitcoin een grote vlucht zullen nemen. Het grote publiek zal ze niet begrijpen en dus niet vertrouwen, en winkeliers zijn bang voor rare koersschommelingen. Maar misschien moeten we sterker dan bij gewone valuta een onderscheid maken tussen geld als betaalmiddel en geld als bezit, en is een valuta als Bitcoin vooral geschikt voor het eerste.

De blockchain daarentegen is een veelbelovend systeem, uit praktisch en theoretisch oogpunt. Om de fundamentele problemen die ik heb genoemd op te lossen, wordt in de praktijk gedacht aan het beperken van de openbaarheid van blockchains en het bevestigen van transacties door daartoe aangewezen partijen. Het wordt er dan niet eleganter op, maar organisaties willen nu eenmaal zaken onder controle houden.

Dames en heren, ik hoop dat ik U een beetje duidelijk heb gemaakt wat gedistribueerde systemen zijn, en watvoor onderzoek wij daarin doen. Vooral hoop ik dat U mij nu een beetje gelooft als ik zeg dat de gedachtenwereld van gedistribueerde systemen toch wel een beetje lijkt op die van de werkelijke wereld.

5. Informatica-onderwijs op het VWO

Slide 24: informatica-onderwijs op het VWO
Tenslotte wil nog iets zeggen over informatica-onderwijs, maar dan niet op de universiteit maar op de middelbare school. Al lange tijd bestaat er een keuzevak informatica in de bovenbouw van het VWO. Het vak staat er niet zo best voor. De huidige opzet dateert van de jaren '90, slechts 5% van de leerlingen kiest het, het examen bestaat alleen uit een Schoolexamen en kent geen Centraal examen, en op basis van wat ik van studenten die het vak gedaan hebben hoor, ben ik niet erg onder de indruk van de inhoud. Van onze eerstejaars hebben tegenwoordig ongeveer 40% dit keuzevak op het VWO gedaan, maar hun studieresultaten zijn nauwelijks beter dan die van de rest.

Dit voorjaar is er een Advies examenprogramma HAVO/VWO uitgebracht door het Nationaal Expertisecentrum Leerplanontwikkeling. Het examen omvat een kernprogramma met de zes domeinen die U hier ziet, en een keuze van vier uit twaalf keuzethema's. Die laatste zijn bedoeld om het vak aantrekkelijk te maken voor leerlingen van alle profielen. Overigens blijft een Centraal Examen ontbreken, dat was een randvoorwaarde voor dit advies, maar doet de status van het vak geen goed. Punten van zorg bij het advies examenprogramma, dat slechts in de vorm van globale eindtermen is geformuleerd, lijken mij de concretisering ervan, de opleiding en beschikbaarheid van voldoende bevoegde leraren, het ontwerpen van lesmateriaal, en het bij de tijd houden van dat materiaal en het programma.

Ik was nog wel even benieuwd wat er als eindterm voor het vak wordt voorgesteld op mijn vakgebied. Onder het Keuzethema Netwerken komt als eindterm voor: "Distributie: De kandidaat kan vormen van samenwerking en verdeling van functies en gegevens in netwerken beschrijven." Helemaal zo gek nog niet, alleen dat "beschrijven" klinkt een beetje slapjes! Overigens wordt het nieuwe vak pas in 2019 ingevoerd, zodat de eerste studenten die aan deze eindterm voldoen niet voor 2022 naar de TU Delft komen.

6. Dankwoord

Slide 25: Met dank aan
Dames en heren, ik ben aan het einde van deze rede gekomen, en wil tot slot een aantal mensen bedanken. Allereerst dank ik de decaan van de Faculteit Elektrotechniek, Wiskunde, en Informatica, professor Fastenau, en het College van Bestuur van de TU Delft voor het in mij gestelde vertrouwen door mij te benoemen.

Ik bedank mijn promovendi voor hun harde werk. Hier ziet U het stapeltje van hun proefschriften in mijn kast, en om U een idee te geven waar zij zoal terechtkomen, ziet U hier ook bij welke bedrijven en instellingen zij nu werken. Ik denk dat het een aardig lijstje is. De twee ronde logo's onderaan zijn van Chinese universiteiten.

Slide 26: Met dank aan
Verder bedank ik Henk Sips, mijn voorganger, voor de jarenlange leiding van de groep en voor zijn vele leerzame inzichten in de mechanismen van het universitaire bedrijf.

Heel veel dank aan Johan Pouwelse en Alexandru Iosup, de huidige twee stafleden van de Groep Gedistribueerde Systemen, voor de intensieve en inspirerende samenwerking, die met beiden al begon in 2004—en de eerste saaie dag moet nog komen. We zijn inmiddels vele promovendi, tientallen artikelen, en honderden discussies verder. Ik waardeer het zeer—en ik kijk uit naar het vervolg!

Ik heb gezegd.

1. Inleiding 1010 (6:30)
2. Gedistribueerde Gegevensverwerking 1070 (7:45)
3. Experimentele informatica 640 (4:40)
4. Cooperatieve Systemen 1255 (9:35)
5. Onderwijs op VWO 320 (2:25)
6. Dankwoord 210 (1:25)

Totaal: 4505

Bij 145 woorden/min:
30 min: 4350
35 min: 5075

Aantal woorden in aula:

1. Inleiding 976 (6 minuten)
2. Distributed Data Processing 600 (4 minuten)
3. Scheduling in datacenters 725 (4:30 minuten)
4. Experimentele informatica 759 (5 minuten)
5. Cooperative Systems 1262 (8:15 minuten)
6. Onderwijs op VWO 399 (2:30 minuten)
7. Dankwoord 230 (1:30 minuten)

Totaal: 4974 (32 minuten, 155 w/min)
In de aula: 34:15 (145/min)

Of aula:
1. 1070
2. 1263
3. 758
4. 1360
5. 405
6. 220

Totaal: 5080 (148/min)

TU/e: 5750 (43 minuten, 133 woorden per minuut)