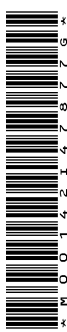


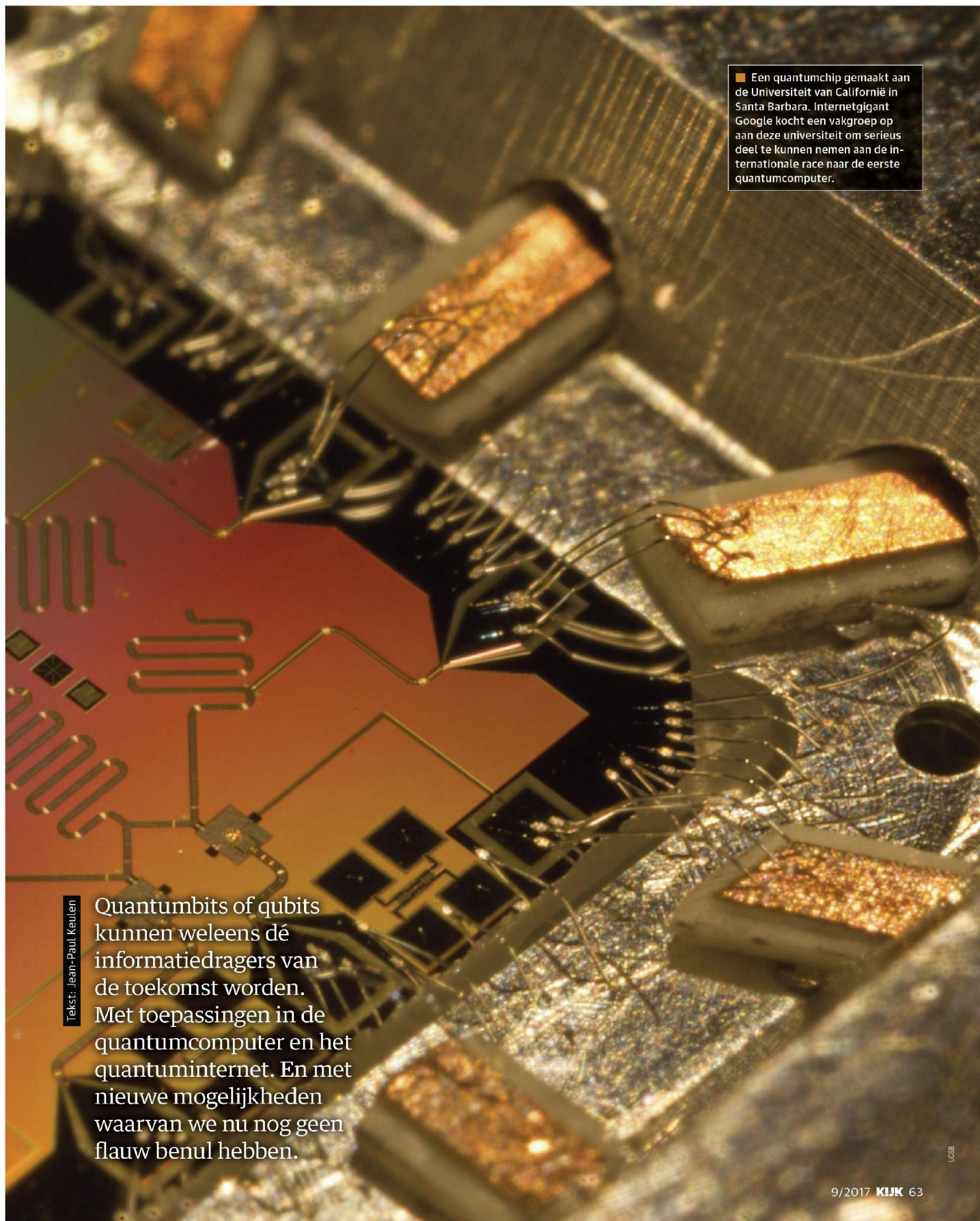


WAT HET MANIPULEREN VAN DE WERELD VAN
HET ALLERKLEINSTE ONS GAAT OPLEVEREN

DAAR KOMEN DE QUBITS!

62 Kijk 9/2017





■ Een quantumchip gemaakt aan de Universiteit van Californië in Santa Barbara. Internetgigant Google kocht een vakgroep op aan deze universiteit om serieus deel te kunnen nemen aan de internationale race naar de eerste quantumcomputer.

Tekst: Jean-Paul Keulen

Quantumbits of qubits kunnen weleens de informatiedragers van de toekomst worden. Met toepassingen in de quantumcomputer en het quantuminternet. En met nieuwe mogelijkheden waarvan we nu nog geen flauw benul hebben.

LCS

9/2017 **KIJK** 63

Quantum- MIJLPALEN

1900 Max Planck stelt dat energie alleen in pakketjes met een bepaalde grootte kan worden geabsorbeerd en uitgezonden: de zogenaamde quanta.

1905 Albert Einstein gebruikt het idee van Planck om uit te leggen hoe het kan dat bepaalde materialen elektronen uitzenden als je er licht op schijnt.



Het quantumlab van IBM. Deze computergigant wil "commercieel beschikbare, universele quantumcomputersystemen voor de zakenwereld en de wetenschap" ontwikkelen.

Als je de inhoud van je pc-kast nu al ingewikkeld vindt, kun je het apparaat over een paar decennia maar beter helemaal niet meer opschrijven. Mogelijk tref je dan naast de gebruikelijke hardware een extra processor aan die op zo'n 270 graden onder nul wordt gehouden. Met daarin een aantal bits die op een totaal andere manier werken dan de bits die we kennen. Bits die via een geheel eigen internet een superveilige verbinding kunnen leggen met andere computers - én met een grote computer ergens ver weg, die dingen kan waar de supercomputers van nu eeuwen mee bezig zouden zijn.

Dit zou allemaal werkelijkheid moeten worden dankzij de quantummechanica. Een tak van de wetenschap waarvan zelfs de grootste wetenschappers toegeven dat ze er uiteindelijk weinig van begrijpen. En die ook nog eens behoorlijk ver van ons bed is. Want in de quantummechanica draait het om het gedrag van de allerkleinste deeltjes. Niet echt iets wat een grote rol speelt in ons dagelijks leven dus.

Of toch wel? De quantumrevolutie (zoals de inzichten wel worden genoemd

die de quantummechanica ons in de eerste helft van de twintigste eeuw bracht) leverde onder meer cd-, dvd- en Blu-ray-spelers, computers en smartphones op. Ons bestaan is dus stiekem al decennialang doordrenkt van technologieën die we aan de quantummechanica danken.

Maar in de tussentijd heeft de wetenschap niet stilgezeten. We leren steeds beter hoe we de wereld van het allerkleinste écht kunnen manipuleren; een ontwikkeling die wel de tweede quantumrevolutie wordt genoemd. En die brengt een hele reeks nieuwe toepassingen in beeld, met de quantumcomputer en het quantuminternet als belangrijkste speerpunten.

Het telraam voorbij

Allereerst de quantumcomputer. Daarvan is het nut wel duidelijk, zou je zeggen; een nog snellere computer dan we nu hebben, is altijd meegenomen. Maar zo moet je een quantumcomputer niet zien. Hij werkt op een compleet nieuwe manier, zegt informaticus Stacey Jeffery, die zich aan het onderzoekscentrum QuSoft van het Amsterdamse Centrum voor Wiskunde en Informatica bezig-

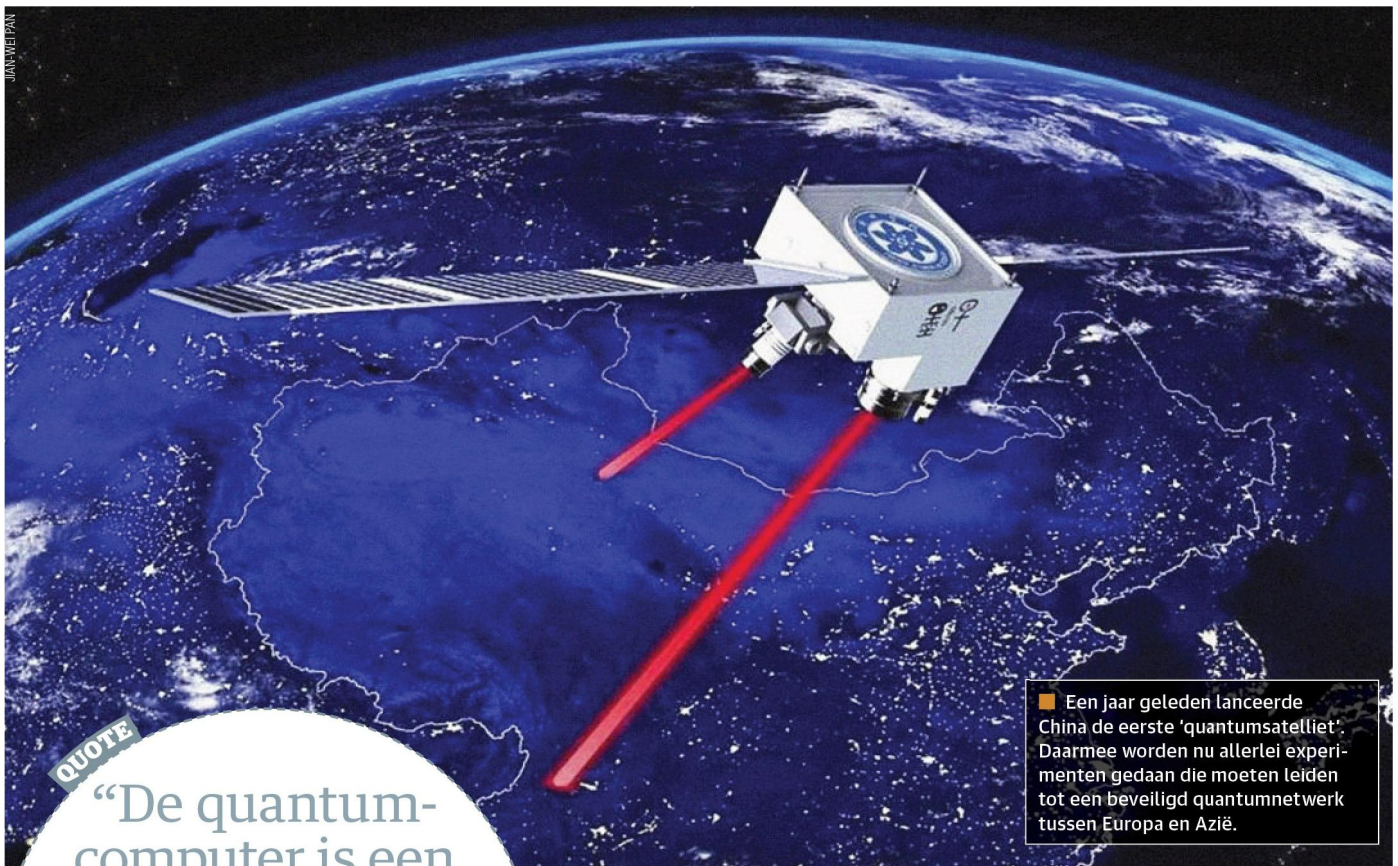
houdt met software voor quantumcomputers. "Van het telraam tot de supercomputer: allemaal werken ze in zekere zin met bits die naar een soort geheugen worden weggeschreven en gemanipuleerd. Maar voor de quantumcomputer geldt dat niet meer. Voor het eerst in de geschiedenis gaan we daarmee het telraam echt voorbij."

Cruciaal is het feit dat een quantumcomputer gebruikmaakt van quantumbits of qubits. Die zijn niet 0 of 1, zoals een gewone bit, maar kunnen zich in een wazige toestand van 0 en 1 tegelijk bevinden. Dat wordt dan een superpositie van 0 en 1 genoemd; een moeilijk te bevatten verschijnsel dat alleen binnen de quantummechanica mogelijk is. Die eigenschap kan de quantumcomputer slim benutten door bij een berekening meerdere mogelijkheden tegelijk te bekijken. "Stel je voor dat een computer de weg naar Amsterdam moet bepalen en bij een kruispunt komt", zegt quantumcomputerdeskundige Stephanie Wehner van het Delftse QuTech. "Een klassiek programma kan dan eerst linksaf gaan en kijken waar dat toe leidt, en vervolgens rechtsaf slaan. Een quantumcomputer kan in zekere zin

1911 Ernest Rutherford legt de basis voor een nieuw beeld van het atoom: een kleine, zware atoomkern waar elektronen banen omheen beschrijven.

1913 Niels Bohr verklaart hoe elektronen in hun baan rond de atoomkern kunnen blijven, door voort te borduren op de ideeën van Planck en Einstein.

1924 Wolfgang Pauli komt met het uitsluitingsprincipe: twee deeltjes kunnen zich niet in exact dezelfde toestand bevinden.



QUOTE

“De quantum-computer is een oplossing op zoek naar een probleem.”

Natuurkundige Carlo Beenakker vat in een mooie soundbite samen dat eigenlijk nog helemaal niet zo duidelijk is waar we een quantumcomputer straks precies voor gaan gebruiken.

■ Een jaar geleden lanceerde China de eerste 'quantumsatelliet'. Daarmee worden nu allerlei experimenten gedaan die moeten leiden tot een beveiligd quantumnetwerk tussen Europa en Azië.

tegelijkertijd linksaf en rechtsaf slaan, in de hoop zo sneller de juiste weg te vinden.” Wehner geeft toe dat dit simpeler klinkt dan het is. “Vervolgens is het heel moeilijk om het goede antwoord eruit te vissen.”

Een ander groot voordeel van een quantumcomputer is de manier waarop hij krachtiger te maken is. “Als je een supercomputer twee keer zo snel wilt laten rekenen, moet je er in feite een tweede supercomputer naast bouwen”, zegt natuurkundige Julia Cramer, eveneens van QuTech. “Bij een quantumcomputer kun je al een veel complexer probleem oplossen door maar één enkele qubit toe te voegen.” Een quantum-

computer met 1000 qubits is dus aanmerkelijk beter dan eentje met 999 qubits, en een computer met 1001 qubits nóg heel veel beter.

Klein beginnen

Nu het slechte nieuws: het maken en laten samenwerken van qubits is zo lastig dat quantumcomputers op dit moment nog maar een handjevol qubits hebben. “Tijdens mijn promotieonderzoek ben ik van één naar vier qubits gegaan”, vertelt Cramer. “De publicaties die nu verschijnen, hebben het over vijf tot negen qubits op een chip.”

En bij dat soort aantallen biedt een quantumcomputer nog geen voordelen, zegt Jeffery. “Tien qubits kun je op een klassieke computer nog prima simuleren. Zelfs een smartphone kan daarmee uit de voeten.” Maar dat zal snel veranderen, vervolgt ze. “Zowel Google als IBM heeft aangekondigd in de nabije toekomst een quantumcomputer met vijftig qubits te willen realiseren. Misschien lukt dat zelfs al voor het eind van dit jaar. Dat aantal is niet meer te simuleren met een klassieke computer.” Toch zijn we ook met vijftig qubits nog ver verwijderd van de machine waar

wetenschappers van dromen. Deze zogenoemde universele quantumcomputer heeft in principe zoveel qubits als je maar wilt, werkt perfect en kan een breed scala aan rekenproblemen oplossen. Daar zullen we echter nog wel een paar decennia op moeten wachten. Waar Jeffery en collega's zich nu mee bezighouden, is ervoor zorgen dat we straks ook met zo'n beperkte quantumcomputer al aan de slag kunnen. Daarvoor moeten de voor een volwaardige computer bedachte programma's worden aangepast, zodat ze ook al iets doen op een machine met, zeg, tweehonderd qubits.

Maar zelfs de perfecte quantumcomputer van de verre toekomst kan niet zomaar elke denkbare berekening uitvoeren. Slechts voor een beperkt rijtje toepassingen overtreft een quantumcomputer op dit moment een klassieke computer. Voor heel veel ander rekenwerk blijven we aangewezen op de opvolgers van onze vertrouwde pc's. Met wat voor problemen kan een quantumcomputer dan wél uit de voeten? Allereerst het simuleren van de quantumwereld zelf. “Alles wat volgens de wetten van de quantum-



1925 Werner Heisenberg geeft de quantummechanica zijn eerste complete wiskundige formulering. Hiermee is de theorie volwassen geworden.

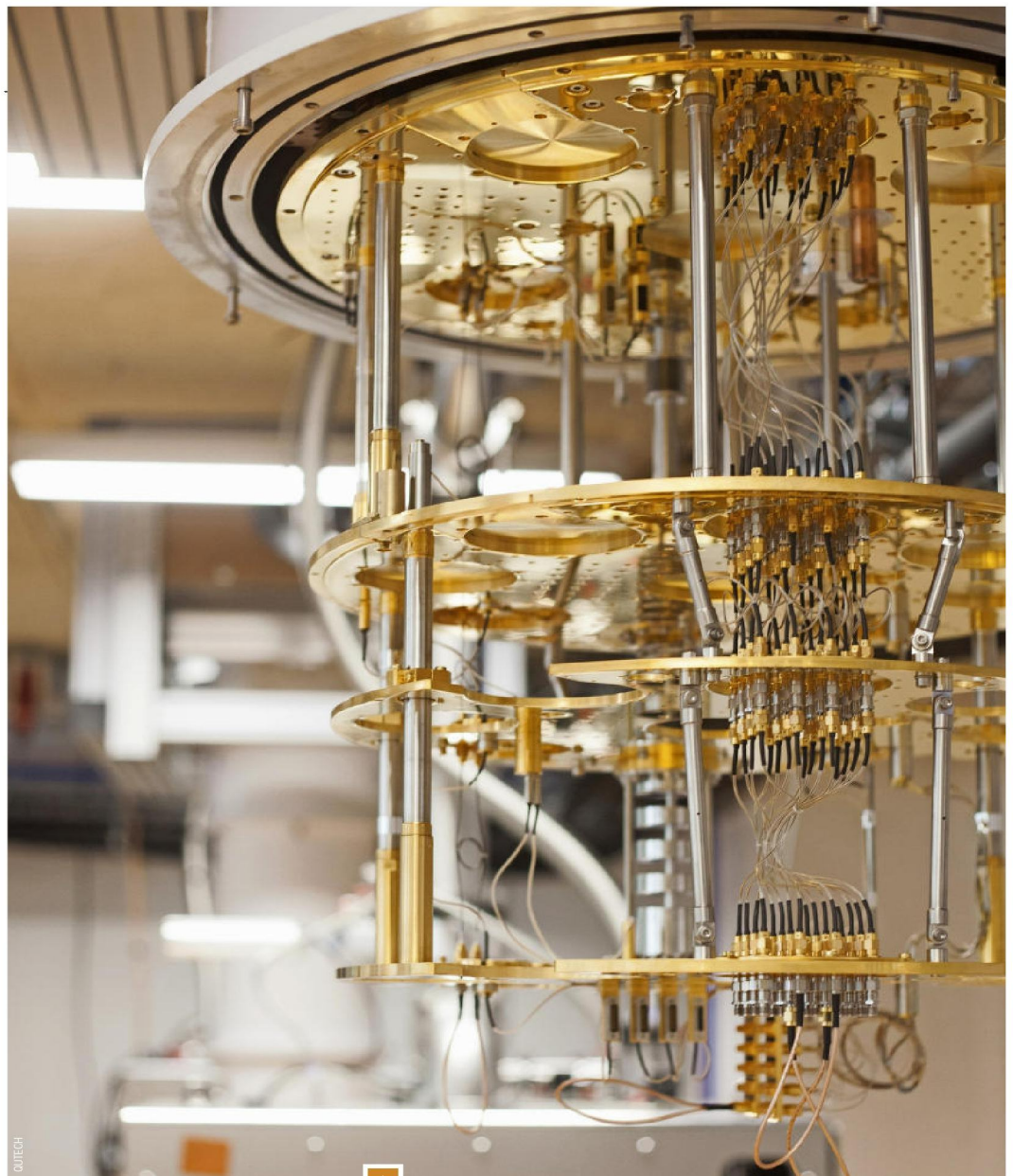
» mechanica werkt, kun je efficiënt doorrekenen op een quantumcomputer, terwijl dat vrij moeilijk is op een klassieke computer”, zegt Cramer. Jeffery voegt daaraan toe: “Bij een klein aantal deeltjes lukt het nog wel, maar bij grotere hoeveelheden heb je al gauw zoveel geheugen en rekentijd nodig dat het praktisch gezien onmogelijk wordt. Niemand gaat een supercomputer honderd jaar laten draaien voor één berekening.”

Als voorbeeld van een quantumsimulatie die heel nuttig kan blijken, noemt Cramer supergeleiding: het verschijnsel dat bepaalde stoffen hun elektrische weerstand volledig kunnen verliezen. Meestal gebeurt dat bij extreem lage temperaturen, maar er zijn ook stoffen die bij hogere temperaturen al supergeleidend worden. Hoe dat kan, is nog een open vraag. “Dat is nu vooral een zoektocht van *trial and error*, omdat we zulke materialen niet kunnen simuleren”, zegt Cramer. “Een quantumcomputer zou dat wel goed kunnen. Zo vinden we misschien een materiaal dat bij kamertemperatuur supergeleidend is.” En dat zou dan weer ons energieprobleem kunnen helpen oplossen, of een nieuwe vorm van computergeheugen mogelijk maken”, zegt Wehner.

Getallen ontbinden

Daarnaast gloren er andere toepassingen van quantumcomputers aan de horizon. Jeffery noemt het doorzoeken van een enorme berg gegevens zonder enige structuur. Stel dat een klassieke computer daar acht uur over doet, dan zou een quantumcomputer er in een paar minuten mee klaar kunnen zijn. Dat wil zeggen: als we databases straks zo kunnen opslaan dat quantumcomputers er hun qubits op los kunnen laten, én als quantumcomputers die ‘verquantumde’ data net zo snel kunnen inlezen als een klassieke computer gewone data.

Tot slot zijn quantumcomputers goed in het ontbinden van grote getallen in priemgetallen; getallen die alleen door zichzelf en door 1 deelbaar zijn. En dat trucje heeft grotere gevolgen dan je zou denken. Bij onze huidige encryptie worden digitale gegevens namelijk vaak versleuteld met behulp van een getal dat je krijgt als je twee grote priemgetallen met elkaar vermenigvuldigt. Om zo’n boodschap vervolgens te ontcijferen, zijn de oorspronkelijke priemgetallen nodig, waar als het goed is alleen jij over beschikt. Maar dan moet natuurlijk niemand die priemgetallen kunnen af-



leiden uit het ‘versleutelgetal’; daarmee zou een onverlaat immers ook jouw boodschappen kunnen ontcijferen. Momenteel is dat geen probleem, want zowel mensen als klassieke computers zijn behoorlijk slecht in het ontbinden van zulke grote getallen. Maar quantumcomputers kunnen dat klusje straks wél klaren. Nu klinkt dat laatste misschien vooral als een reden om géén quantumcomputers te ontwikkelen. Onze onlineprivacy is immers een stuk veiliger zonder. Maar, zegt Cramer, nieuwe technologie houdt je niet tegen met ethische bezwaren. “Als wij die quantumcomputer niet bouwen, doet iemand anders het wel.” Het is daarom vooral belangrijk om een

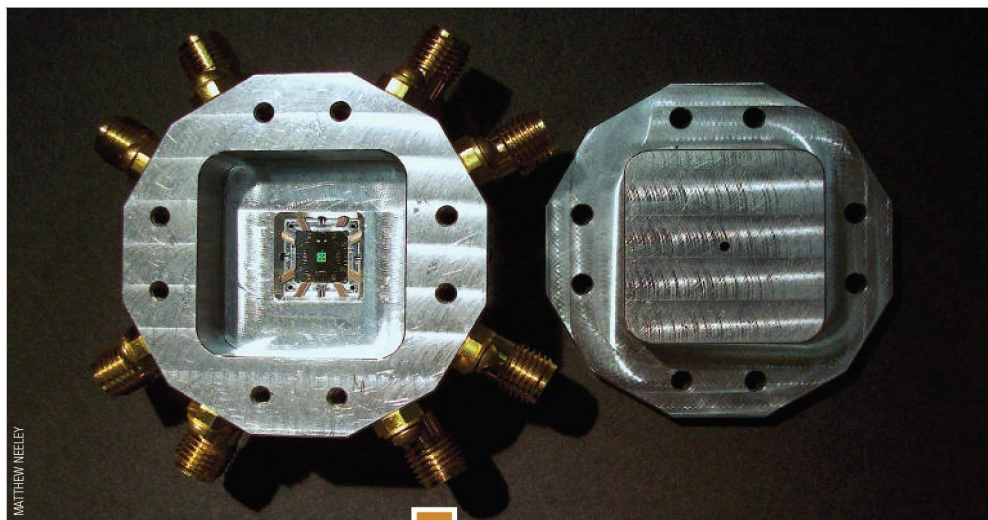
Onderaan deze ‘kroonluchter’ wordt een quantumchip bevestigd. Vervolgens hangen onderzoekers het geheel in een grote buis, die de temperatuur op enkele duizendsten graden boven het absolute nulpunt houdt – anders functioneert de chip niet.

nieuwe manier van encryptie te realiseren vóórdat de quantumcomputer er is, zegt Jeffery. Gelukkig biedt de quantummechanica ook op dat punt uitkomst. Door recente experimenten aan de TU Delft (zie het artikel ‘Ja, ze bestaan: quantumspoken’ in KIJK 2/2016) weten we nu zeker dat je deeltjes met elkaar kunt verstrengelen. Dat wil zeggen dat ze een quantummechanische band met elkaar krijgen, die op grote afstand kan blijven bestaan. Doe je vervolgens een meting aan het ene deeltje, dan heeft dat ogenblikkelijk gevolgen voor het andere deeltje – waar dat zich op dat moment ook bevindt. Dat verschijnsel is te gebruiken om een

1926 Erwin Schrödinger komt met zijn eigen versie van de quantummechanica, waar makkelijker mee te werken is dan met de Heisenberg-formulering.

1927 Heisenberg introduceert het onzekerheidsprincipe: hoe preciezer je de plaats van een deeltje weet, hoe minder nauwkeurig je de snelheid weet.

1935 Einstein en twee collega's stellen dat volgens de quantummechanica koppels van 'verstrengelde' deeltjes elkaar op grote afstand kunnen beïnvloeden.



verbinding op te zetten die niet ongemerkt kan worden afgeluisterd, vertelt Wehner. "Als twee deeltjes verstrengeld zijn, kan niets anders aan die verstrengeling deelnemen", legt ze uit. "Stel nu dat jij en ik allebei een qubit hebben, die met elkaar verstrengeld zijn. Als dan iemand ons af luistert, verdwijnt de verstrengeling. Zolang die in stand blijft, worden we gegarandeerd niet afgeluisterd en kunnen we uit onze verstrengelde deeltjes een veilige sleutel halen." En dit is geen verre toekomstmuziek. "Onder meer Toshiba verkoopt nu al systemen waarmee je over korte afstanden een 'quantumsleutel' kunt uitwisselen om veilig te communiceren."

Nederlands netwerk

De natuurkundige wereld heeft echter nog grotere ambities: toewerken naar een wereldwijd netwerk van quantummechanische verbindingen, het quantuminternet. En dat zou er sneller kunnen komen dan de eerste volwaardige quantumcomputer. Voor een quantuminternet zijn namelijk geen enorme hoeveelheden qubits nodig. Iedere gebruiker heeft genoeg aan één exemplaar. Of, vooruit, een handjevol. Binnen het quantuminternet dienen qubits namelijk niet om berekeningen uit te voeren, maar om via verstrengeling in contact te komen met andere computers.

Op de weg naar zo'n quantuminternet zou Nederland een voortrekkersrol kunnen spelen. Een samenwerking tussen QuTech, QuSoft en de universiteiten van Leiden en Amsterdam wil namelijk al in 2020 een quantumnetwerk opzetten tussen Amsterdam, Leiden, Den Haag en Delft.

Je kunt op heel wat manieren een qubit maken: een bit die niet 0 of 1 is, maar een combinatie van beide. Dit is een houder voor een chip die werkt met zogenoemde supergeleidende qubits.

Toshiba verkoopt nu al apparaten waarmee je met quantummechanica op korte afstanden een verbinding tot stand kan brengen. De eerste stap richting een quantuminternet?

Dat quantumnetwerk dient dan vooral om de technologie te demonstreren, legt Wehner uit. Er moet nog behoorlijk wat gebeuren voordat een echt quantuminternet mogelijk is. En dan is het handig als dat werk niet alleen bij universiteiten terechtkomt, maar ook allerlei bedrijven zich ermee bezig gaan houden.

Wat moeten we dan straks met zo'n quantuminternet? Allereerst kun je denken aan toepassingen die te maken hebben met quantumcomputers. Via het quantuminternet zou je die bijvoorbeeld met elkaar samen kunnen laten werken. Of je kunt een quantumcomputer (waar er in eerste instantie maar weinig van zullen zijn) op afstand bedienen met een gewone computer die is voorzien van genoeg qubits om er via het quantuminternet een verbinding mee te maken.

Maar ook zonder quantumcompu-

3 tech-giganten in de quantumwereld



1 Google kocht een onderzoeksgroep op van de Universiteit van Californië in Santa Barbara.

Deze groep streeft er nu naar om eind 2017 een quantumcomputer te hebben met vijftig qubits, die niet meer te simuleren is met een gewone computer.



2 IBM werkt ook toe naar een quantumchip met vijftig qubits, zij het met een minder strakke

deadline dan Google. Verder heeft de computerfirma een quantumchip met vijf qubits beschikbaar gesteld aan het grote publiek; wie wil, mag er gratis mee rekenen.



3 Microsoft investeert onder de naam Station Q in een aantal instituten verspreid over de

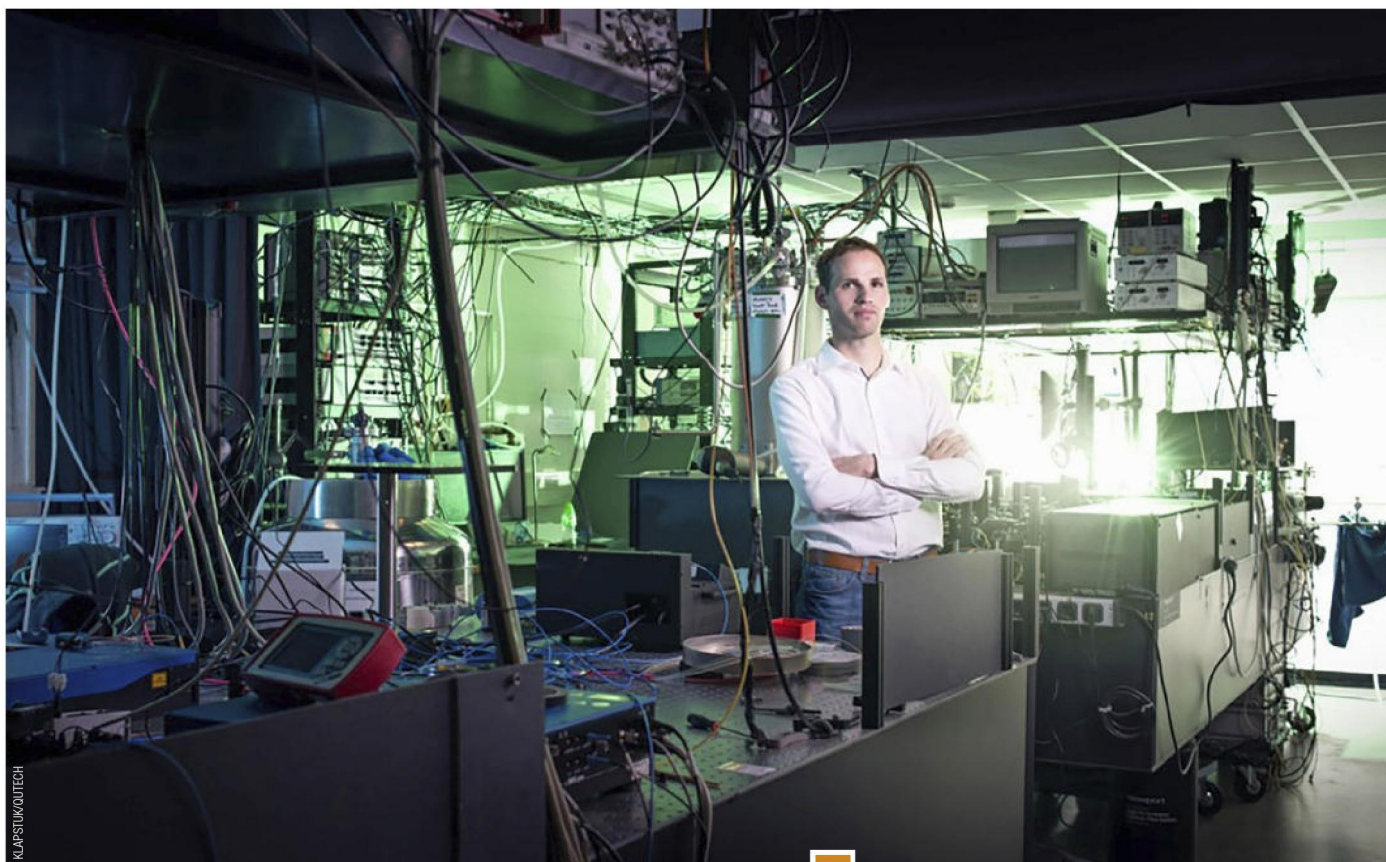
wereld, waaronder de TU Delft. De softwaregigant zet daarbij in op een ander type qubit dan Google en IBM, dat grote voordelen én grote uitdagingen kent.



1964 John Stewart Bell bedenkt de 'Bell-test'. Daarmee is vast te stellen of het idee van Einstein en collega's uit 1935 klopt.

1982 Alain Aspect voert de Bell-test uit: verstrengelde deeltjes lijken elkaar inderdaad op afstand te beïnvloeden. Wel is het resultaat nog niet volledig waterdicht.

2015 Het team van Ronald Hanson voert een 'waterdichte' Bell-test uit. Verstrengelde deeltjes beïnvloeden elkaar echt, hoe onwaarschijnlijk dat Einstein ook leek.



» ters kan het quantuminternet al van pas komen. Als op twee verstrengelde deeltjes dezelfde meting wordt losgelaten, rolt er namelijk twee keer hetzelfde antwoord uit, zónder dat daarvoor verder nog onderling gecommuniceerd hoeft te worden. Dat maakt het bijvoorbeeld mogelijk om klokken heel precies met elkaar te synchroniseren, zegt Wehner; zelfs als de ene klok op aarde en de andere op Mars zou staan. "Daarnaast zijn nog heel veel andere dingen bedacht", vervolgt Wehner. "Tot een manier om beter online bridge te kunnen spelen aan toe." Het doel is dan ook om het quantuminternet voor iedereen thuis beschikbaar te maken. Denk daarbij aan een pc die naast een gewone processor ook een kleine quantumprocessor heeft, en die zowel op het gewone als op het quantuminternet is aangesloten. "Maar

ik zal wel al heel oud zijn voor het zover is", zegt Wehner lachend.

Gebrekkige fantasie

Nu klinkt het rijtje toepassingen voor het quantuminternet nog niet zo indrukwekkend dat je gelijk zult zeggen: ik wil liever vandaag dan morgen beginnen met quantsurfen op het quantumweb. Hetzelfde geldt voor de quantumcomputer. Oké, quantumencryptie kan weleens gemeengoed worden, maar voor de rest lijkt het toch vooral een ding voor wetenschappelijk onderzoek.

Maar misschien komt dat vooral doordat onze fantasie ons in de steek laat. "De directeur van IBM zei in de jaren veertig dat er wereldwijd misschien een markt zou zijn voor vijf computers. En kijk nu eens om je heen", zegt Julia Cramer van QuTech. "Ik denk dat alle

Natuurkundige Ronald Hanson en enkele andere Delftse wetenschappers bewezen in 2015 dat twee deeltjes een quantummechanische band met elkaar kunnen houden, ook als ze zich een eind van elkaar vandaan bevinden. Dit verschijnsel ligt aan de basis van communicatie die niet kan worden afgeluisterd.

voorspellingen die wij nu doen over quantumtechnologie van hetzelfde kaliber zijn. We kunnen echt niet voorzien wat er allemaal mogelijk wordt. En dat is wat mij betreft juist het spannende eraan." ■

Bottomline

- 1 We leren steeds beter hoe we de werkelijkheid op kleine schaal kunnen manipuleren, wat allerlei nieuwe quantumtechnologieën mogelijk maakt.
- 2 De twee grootste toepassingen zijn het quantuminternet en de quantumcomputer, waarbij een volwaardige uitvoering van die laatste wel nog decennia op zich zal laten wachten.
- 3 Voor quantumcomputer en -internet is al een aantal toepassingen bedacht, maar de meeste ideeën komen waarschijnlijk pas als deze technologieën eenmaal echt beschikbaar zijn.



Jean-Paul Keulen is wetenschapsjournalist gespecialiseerd in natuur- en sterrenkunde. Voor dit artikel sprak hij met natuurkundige dr. ir. Julia Cramer (QuTech, Universiteit Leiden/TU Delft), informaticus dr. Stacey Jeffery (QuSoft, CWI) en hoogleraar quantuminformatie prof. dr. Stephanie Wehner (QuTech, TU Delft).

Ga voor links met meer informatie naar www.kijkmagazine.nl/artikel/quantumbits