

Nieuws

- + Organisatie
- + Producten
- + Vakgebied
- + Bankensector
- + Thema

Profiel

- + Nederlandse Verenigin...

Meer nieuws over

- Informatie Technologie

Quantum computer: waarom zo anders dan de klassieke computer?

15 januari 2021 | Banken.nl

General awareness quantum computing'. Zo heet de maandelijkse workshop georganiseerd door banken, bedrijfsleven en wetenschap. Quantumcomputing gaat in de (nabije?) toekomst immers ook de bankensector raken. Quantumdeskundige Marten Teitsma (HvA) geeft - samen met QuSoft - de workshopdeelnemers inzicht in de grondbeginselen van de quantumtechnologie. En laat zijn licht schijnen over de kansen en bedreigingen.

Marten Teitsma is bijzonder lector Applied Quantum Computing aan de Hogeschool van Amsterdam (HvA). Teitsma is gespecialiseerd in quantumtechnologie. Op de HvA legt hij het verband tussen de fundamentele quantumwetenschap enerzijds, en praktisch onderzoek en onderwijs anderzijds.

Teitsma: "Quantumtechnologie bestaat uit drie onderdelen: quantum computing, quantum communication en quantum sensing. Quantum computing gaat over rekenen volgens de principes van de quantumwetenschap. Quantum communication over het communiceren via netwerken volgens dezelfde principes. Quantum sensing gaat over het 'voelen' van de omgeving, over magnetisme en tijd bijvoorbeeld. Voor banken is vooral quantum computing van belang."



Qubit

"Bijzonder aan quantum computing is dat je gebruik kunt maken van drie quantummechanische effecten: superpositie, interferentie en entanglement (verstrengeling)", vervolgt Teitsma: "Bij superpositie gaat het niet om de 'klassieke' databit die of een 0 of een 1 is. Maar om een qubit (quantumbit), die zowel een 0 als een 1 kan zijn. Belangrijk daarbij is dat je bij meting wel altijd een 0 of een 1 ziet; de eigenlijke superpositie valt dus nooit te meten. Interferentie stelt ons in staat om de superpositie van een of meer qubit(s) te doen veranderen.

De ontwikkelaar van een algoritme zorgt daarvoor; hij of zij laat de qubits op elkaar reageren. Sommige posities worden dan versterkt, terwijl andere worden verzwakt. Quantum-deeltjes worden vaak omschreven als golven en ondervinden vergelijkbare effecten. Vergelijk het met twee stenen die je tegelijkertijd in het water gooit; als de kringen elkaar raken, zie je dat de golven elkaar soms versterken, soms verzwakken. Dat is interferentie. Maak je daar op een slimme manier gebruik van, dan kun je middels interferentie een bepaalde oplossing die je zoekt, versterken en meetbaar maken."

"Bij entanglement zijn de qubits met elkaar verstrengeld. Als ze verstrengeld zijn, dan is het resultaat van een meting op één qubit onlosmakelijk verbonden met de andere qubit – ongeacht de afstand tussen de qubits. Die afstand kan een centimeter of kilometer zijn, maar ook de andere kant van het universum. Dus doe je een meting, dan weet je ook het resultaat van de andere meting. Er is geen communicatie tussen die twee qubits – dat laatste is in 2015 ook aangetoond door de TU Delft, een heel mooi Nederlands resultaat. Die drie quantummechanische effecten zijn het fundament van quantum computing, waardoor we met een quantumcomputer andere dingen kunnen doen dan met een klassieke computer."

Geleidelijke ontwikkeling

Hoe ver is de ontwikkeling van de quantumcomputer nu? Nog niet zo heel ver, aldus Teitsma: "Er zijn een paar kleine quantumcomputers, en die zijn ook nog eens noisy. Wat betekent dat ze niet perfect zijn, ze vertonen fouten. De TU Delft bouwt er nu een, en onder andere IBM heeft een aantal kleine. Het is nu nog niet zeker wanneer er wel een grote (full-scale fault-tolerant) quantumcomputer komt. De verwachtingen lopen zeer uiteen – van 5 tot 35 jaar. Sommigen zeggen zelfs: die komt er nooit.

Waarschijnlijk wordt het een geleidelijke ontwikkeling. Rome is immers ook niet in een dag gebouwd. Op dit moment wordt hard gewerkt aan de foutcorrectie. Voor het realiseren van 1 foutloze qubit zijn nu nog, afhankelijk van de hardware en software, van enkele tot soms wel duizenden andere qubits nodig. Of en hoe dat minder kan - daar is veel onderzoek naar en daarin worden ook stappen gezet."

Nieuwe materialen en medicijnen

Waar liggen de maatschappelijke kansen van quantum computing? Teitsma: "Kansen? Dat vind ik lastig te beantwoorden. Nieuwe technologie wordt vaak gehyped en gepresenteerd als oplossing voor talloze problemen. Maar veel problemen hebben geen technologische oorsprong. Ze behoeven dus ook geen technologische oplossing. Bovendien: de eerste quantumrevolutie in de jaren twintig leidde tot kernenergie en kernwapens. Is dat vooruitgang? Wel kun je in het algemeen zeggen dat de kansen van de quantumcomputer liggen in de snelle berekening van sommige problemen."

"Met simulatie van materialen op quantumniveau verkrijgen we beter inzicht in het gedrag van een molecuul. Die kennis zou inzetbaar zijn voor de ontwikkeling van bijvoorbeeld nieuwe materialen en medicijnen. Of inzetbaar voor de energietransitie. Ook zijn er uitdagingen binnen de logistiek, risico-analyse en klimatologie die een klassieke computer eenvoudigweg jaren en jaren zou kosten om te berekenen. Een full-scale fault-tolerant quantumcomputer kan die uitdagingen wel aan.

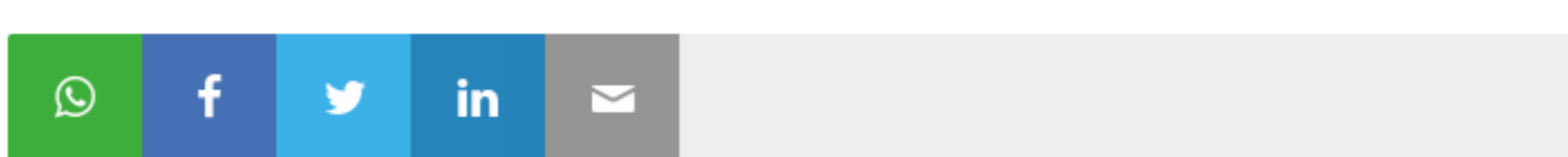
Voor banken zou zo'n quantumcomputer kunnen helpen bij de optimalisatie van het portfolio; hij kan beter de risico's en rendementen op de verschillende assets berekenen. Ook bij de machine learning die wordt ingezet bij fraude-detectie, kan de quantumcomputer veel betekenen. De verwachting is dat quantumcomputers samen met klassieke computers een hybride systeem gaan vormen, waarbij de quantumcomputer specifieke taken uitvoert."

Code kraken

Bedreigingen zijn er zeker ook, aldus Teitsma: "De quantum computer kan een bedreiging vormen voor de huidige beveiliging op de communicatie middels het RSA-protocol; een encryptiealgoritme dat veel gebruikt wordt voor elektronische handel, waaronder de beveiliging van transacties. Met een klassieke computer kost het kraken van dat protocol vele duizenden jaren. Een quantumcomputer zou dat protocol binnen een dag kunnen 'kraken'. Een quantumcomputer is niet zozeer sneller, maar lost problemen op een heel andere manier op – mits goed geprogrammeerd.

Maar zo ver is het nog lang niet, wil ik benadrukken. Er is nog geen full-scale fault-tolerant quantumcomputer waarmee dat zou kunnen. Wat ik aan banken wil meegeven? Dat is iets wat wij en de banken in de NVB-werkgroep ook constateerden: het start bij bewustzijn. Binnen elke sector en elke bank krijgen heel veel mensen direct of indirect te maken met de quantumcomputer; het gaat iedereen raken. Daarom is onze eerste stap een workshop awareness voor een brede doelgroep, over de kansen en bedreigingen van de quantumcomputer. Stap twee wordt meer specifieke workshops voor ontwikkelaars en voor security."

Dit artikel is eerder verschenen in Bank | Wereld Online, het online magazine van de Nederlandse Vereniging van Banken (NVB)



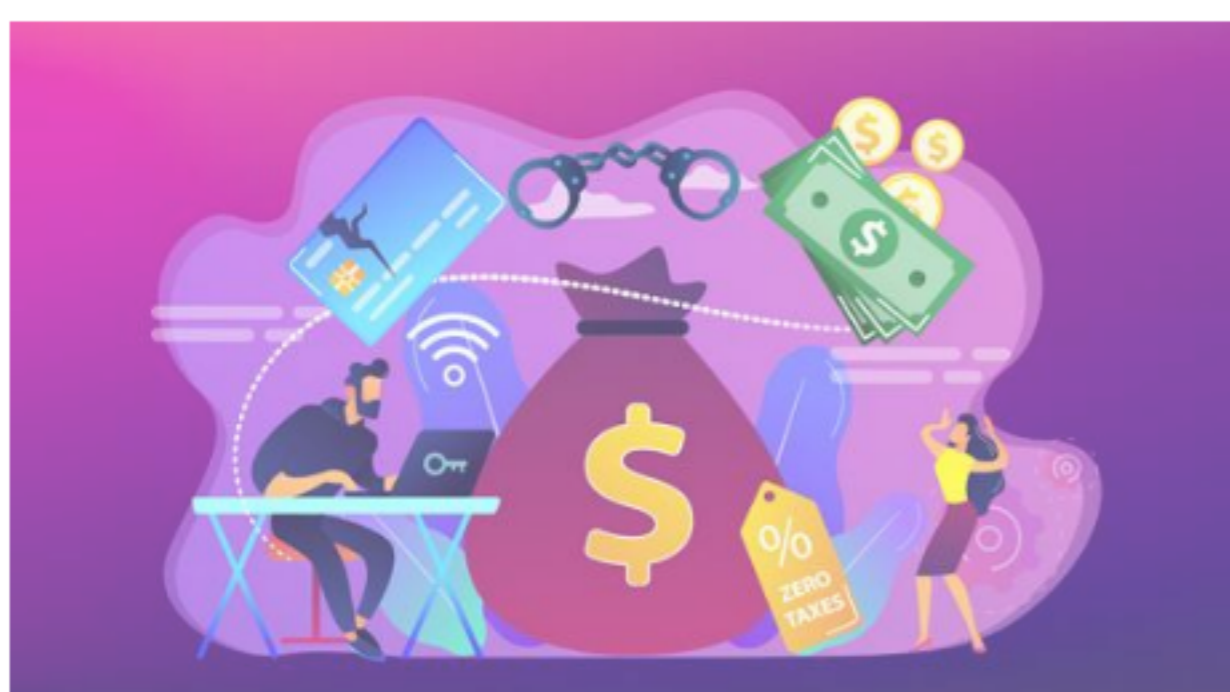
Gerelateerd nieuws



15 januari 2021
Quantum computer: waarom zo anders dan de klassieke computer?



11 januari 2021
Varrlyn voltooit Murex-projecten voor partijen in de financiële sector



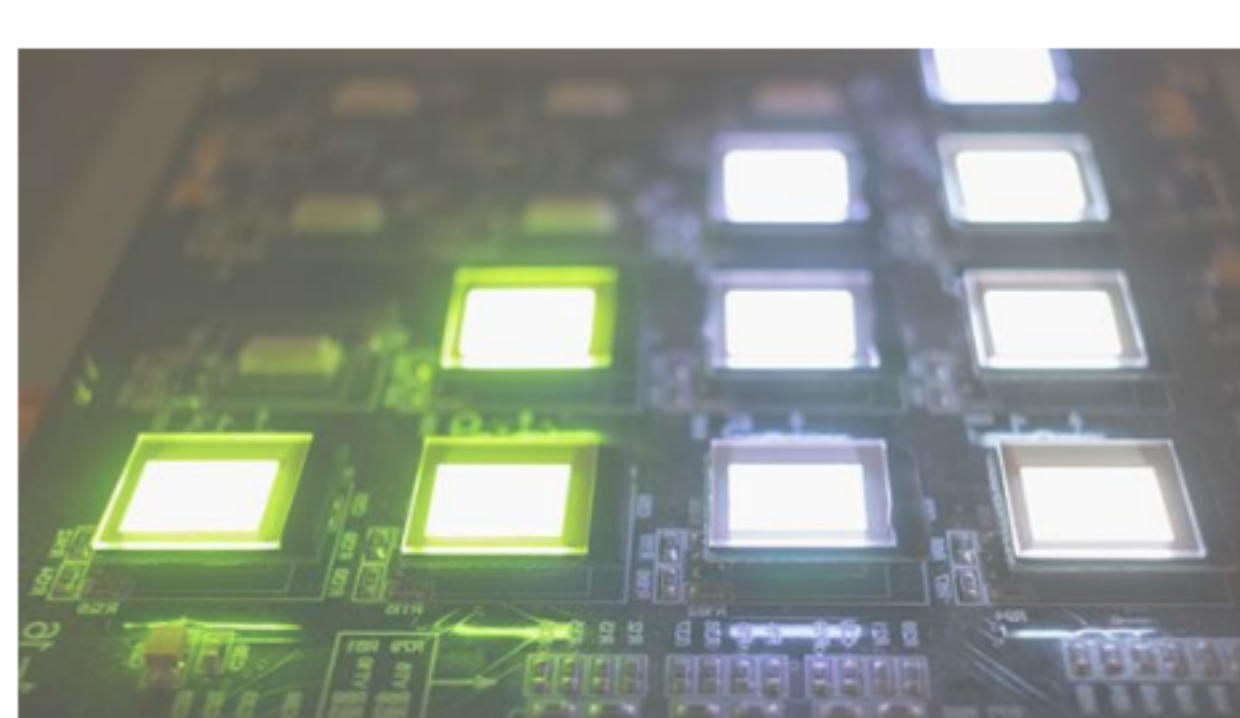
23 december 2020
Preventie van financiële criminaliteit: van silo's naar tandems



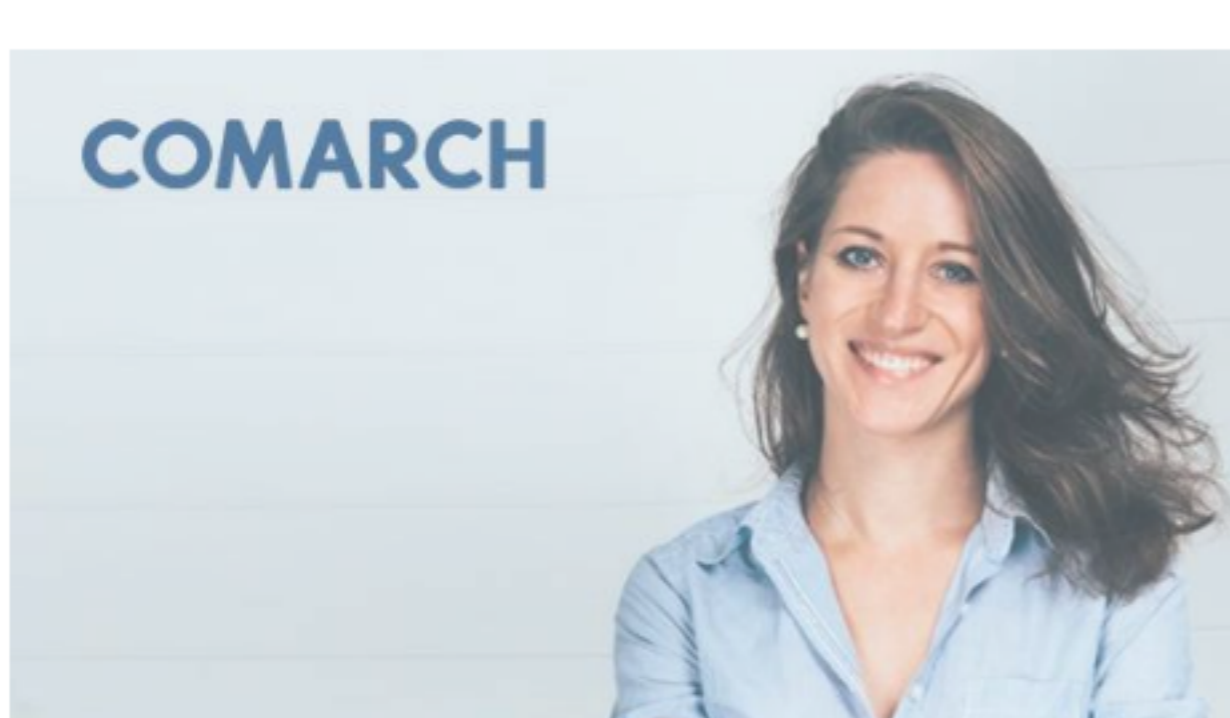
07 december 2020
Softwarebedrijf Backbase helpt banken bij digitale transformatie



07 december 2020
Vertrouwen met snuffje controle: Early Warning Systems bij factoring



25 november 2020
Het nieuwe financiële paradigma vraagt meer flexibiliteit van banken



23 november 2020
Portfoliomanagement voor particuliere beleggers op een keerpunt



19 november 2020
Europees cloud-project Gaia-X lijkt vroege dood te sterven

Meer nieuws laden



Meld je aan voor de nieuwsbrief