Architektura komputerów

Wykład 14
Komputery kwantowe

Wojciech Kordecki

Collegium Witelona
Wydział Nauk Technicznych i Ekonomicznych
Zakład Informatyki

Semestr letni 2023/24

Fizyka kwantowa – źródła wiedzy

Przy przygotowywaniu tego wykładu intensywnie korzystałem z materiałów opracowanych przez prof .Ryszarda Tanasia z Zakładu Optyki Nieliniowej Instytutu Fizyki UAM w Poznaniu:

http://zon8.physd.amu.edu.pl/~tanas/lecture.html
http://zon8.physd.amu.edu.pl/~tanas/QC.html

Kubit

W informatyce klasycznej podstawową jednostką jest bit: 0 albo 1. Bit nie może być jednocześnie w stanie 0 i 1.

Kubit (qubit) – dowolny stan kwantowy układu dwupoziomowego o stanach własnych $|0\rangle$ i $|1\rangle$, który może być superpozycją stanów własnych

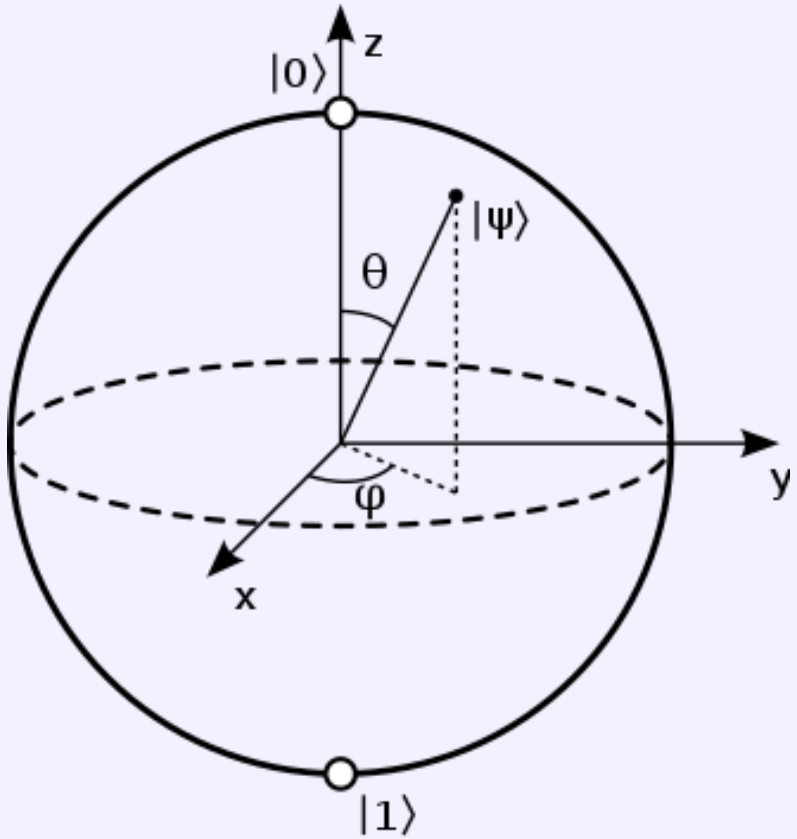
$$|\Psi\rangle = a|0\rangle + b|1\rangle$$
$$|a|^2 + |b|^2 = 1,$$

gdzie $a, b \in \mathbb{C}$.
Sfera Blocha – trójwymiarowa sfera zespolona o promieniu jednostkowym. Daje możliwość wizualizacji pojedynczego bitu kwantowego (kubitu) w stanie $|\Psi\rangle$.

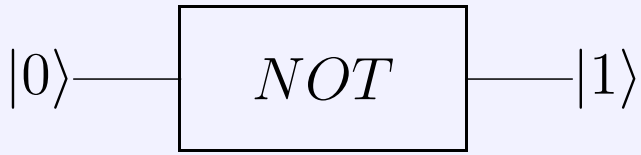
Sfera Blocha

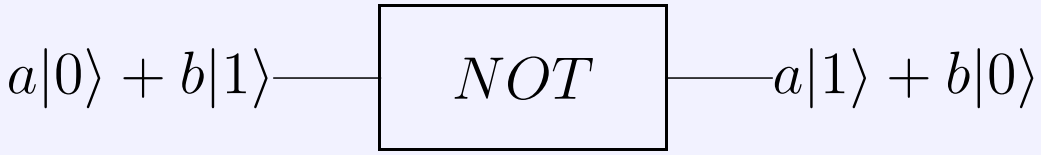
$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

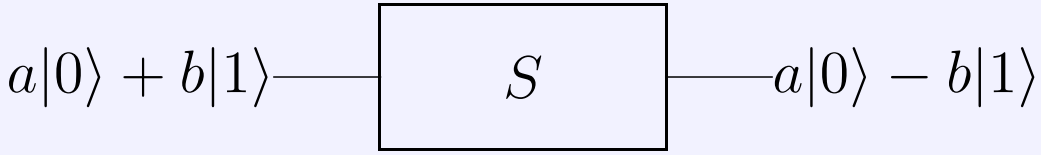
Źródło: Wikipedia



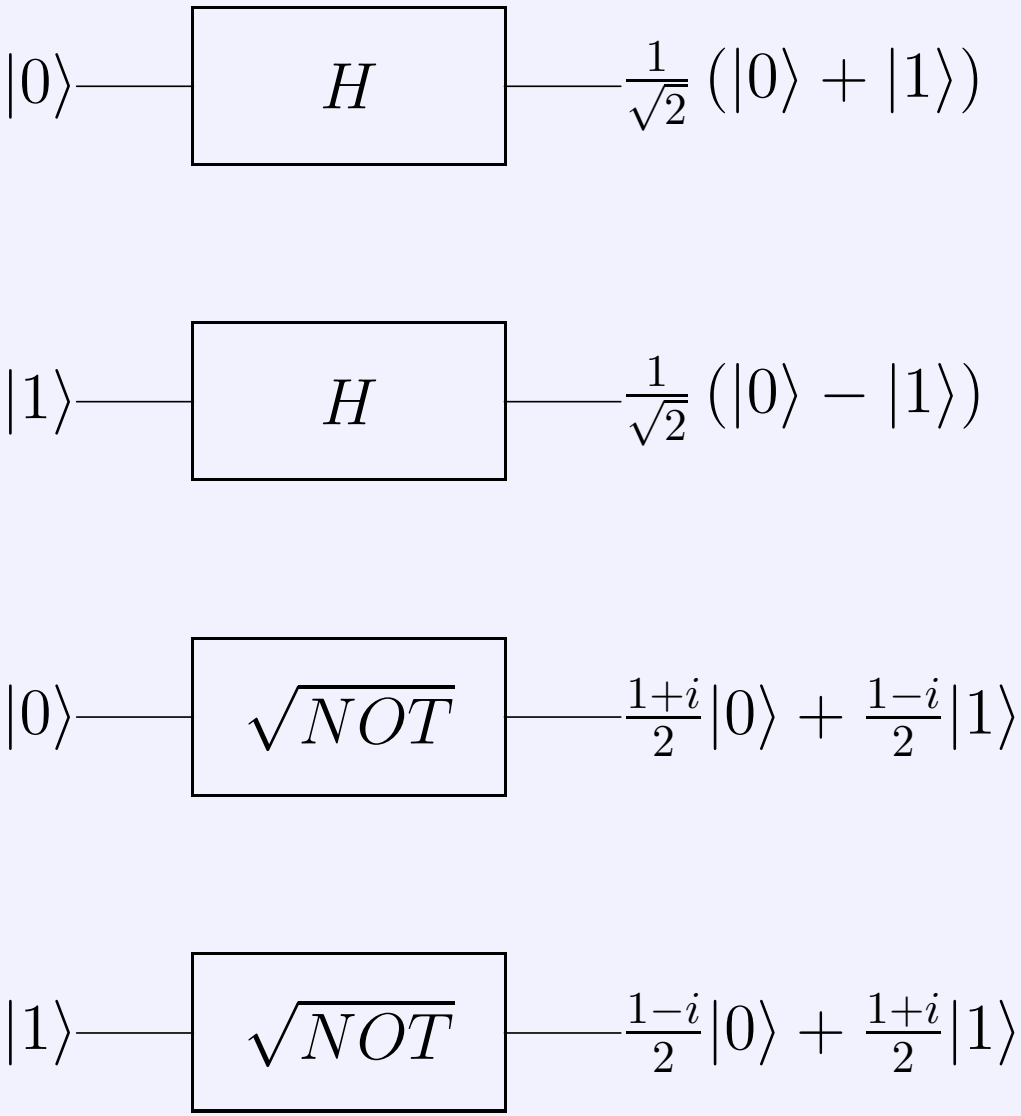
Bramki kwantowe (1)







Bramki kwantowe (2)



Stany bazowe i bramki

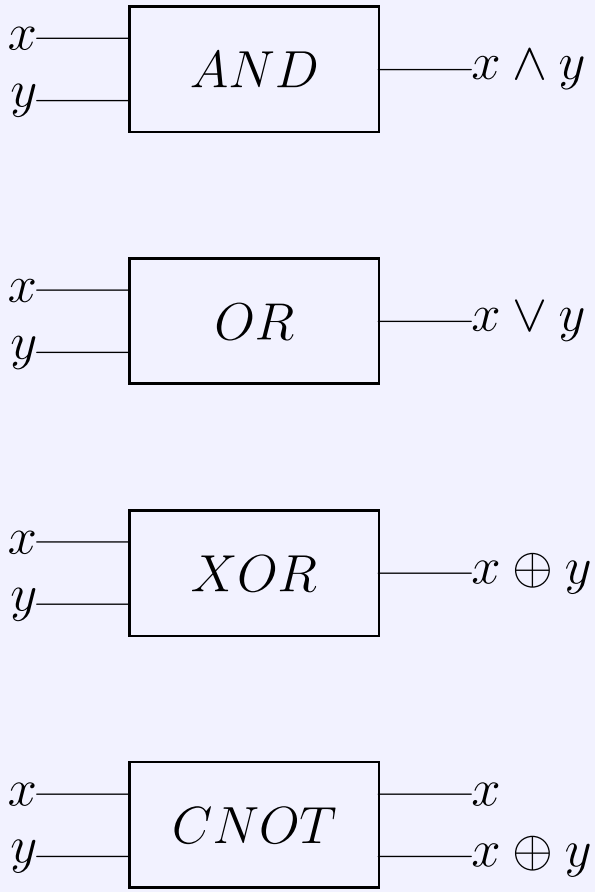
Stany bazowe:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

Bramka jednokubitowa:

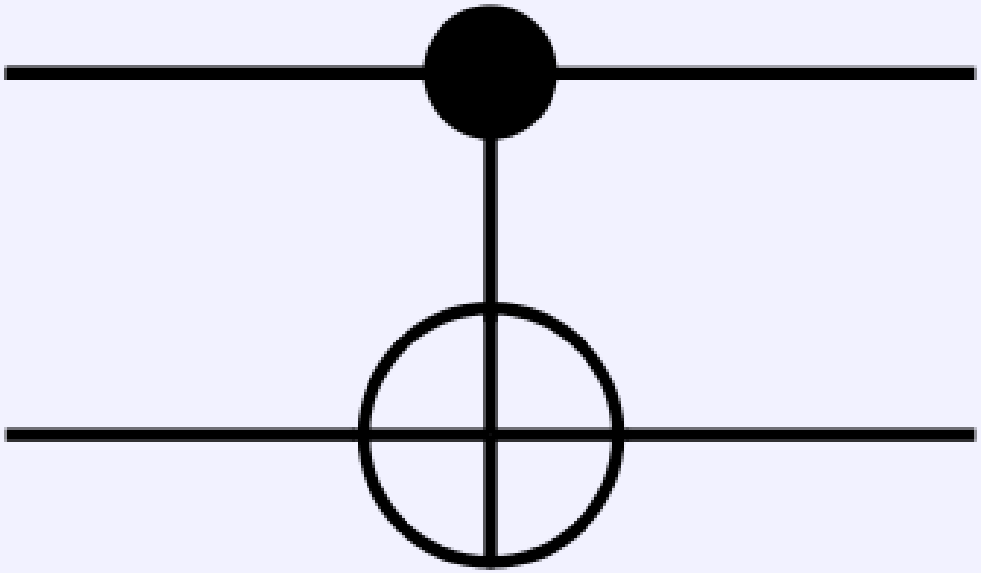
$$NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}, \quad \sqrt{NOT} = \begin{bmatrix} \frac{1+i}{\sqrt{2}} & \frac{1-i}{\sqrt{2}} \\ \frac{1-i}{\sqrt{2}} & \frac{1+i}{\sqrt{2}} \end{bmatrix}.$$

Bramki klasyczne dwubitowe

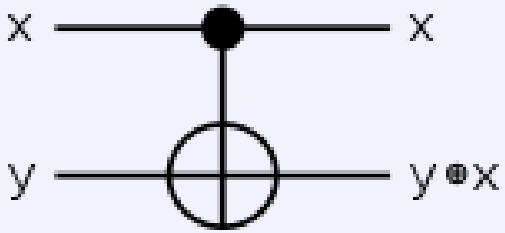


$x \oplus y \equiv x + y \mod 2.$

Bramka kwantowa CNOT



Bramka kwantowa i klasyczna CNOT



input		output	
x	y	x	y+x
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

input		output	
x	**y**	**x**	**y+x**
0	**0**	**0**	**0**
0	**1**	**0**	**1**
1	**0**	**1**	**1**
1	**1**	**1**	**0**

Działanie bramki

$$NOT|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle,$$

$$H|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right),$$

$$\sqrt{NOT}|0\rangle = \begin{bmatrix} \frac{1+i}{\sqrt{2}} & \frac{1-i}{\sqrt{2}} \\ \frac{1-i}{\sqrt{2}} & \frac{1+i}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1+i}{\sqrt{2}} \\ \frac{1-i}{\sqrt{2}} \end{bmatrix} = \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle.$$

Działanie bramki CNOT

$$|00\rangle \rightarrow |00\rangle,$$
$$|01\rangle \rightarrow |01\rangle,$$
$$|10\rangle \rightarrow |11\rangle,$$
$$|11\rangle \rightarrow |10\rangle,$$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

CNOT – komentarz

Jeżeli kubit pierwszego podukładu jest w stanie 1 , CNOT dokonuje operacji NOT na drugim podukładzie, a jeżeli pierwszy podukład znajduje się w stanie 0 , CNOT pozostawia drugi podukład w niezmienionym stanie. Zatem stan drugiego kubitu (ang. target qubit) jest kontrolowany przez stan pierwszego qubitu (ang. controlled qubit).

Bramka CNOT może wpływać także na stan kubitu kontrolnego – jest to jedna z cech odróżniających ją od bramek klasycznych. Pozwala ona na wprowadzenie nowych efektów do obwodów kwantowych.

Źródło: S. Bugajski, J. A. Miszczak, Z. Motyka. Symulacje optyczne obliczeń kwantowych

Splątanie – przykład

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \quad |\Psi_1\rangle.$$

$$CNOT|\Psi_0\Psi_1\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).$$

Stan, niedający się przedstawić jako iloczyn dwóch stanów – stan splątany.

Para EPR

$$\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

jest znaną parą EPR

Jeśli pomiar jednego kubitu da 1, co zdarzy się z prawdopodobieństwem 1/2, to drugiego musi dać 1 i na odwrót.

Paradoks EPR

Mechanika kwantowa zakłada, że przed pomiarem wielkości kwantowej mierzona zmienna nie ma ustalonej wartości, dopiero pomiar ją ustala, a wcześniej można mówić tylko o rozkładach prawdopodobieństwa.
Istnieją jednak pewne tzw. stany splątane par cząstek, (. . .) które mają taką właściwość, że gdy dokonujemy pomiaru wartości jakiejkolwiek składowej spinu każdej z cząstek, ale dla obu cząstek względem tego samego kierunku przestrzennego, otrzymujemy zawsze przeciwne wyniki (pełna anty-korelacja).
Jeśli takie cząstki oddalimy od siebie, a potem zmierzymy pewną składową spinu jednej z nich, to pomiar da nam nie tylko jej wartość, ale jednocześnie wartość identycznej składowej spinu tej drugiej (gdyby ktoś chciał dokonać pomiaru w tym samym kierunku). (. . .).
Źródło: Wikipedia
https://pl.wikipedia.org/wiki/Paradoks_EPR

Para EPR intuicje

Intuicje naiwne, ale przekonywujące, choć niekoniecznie prawdziwe.

Dwie karty: czerwona i niebieska.
Odwracamy, tasujemy, losujemy jedną, a drugą ekspediujemy na księżyc.
Kartę wylosowaną odwracamy.
Jeśli wylosowana jest czerwona, to ta druga na księżycu musi być niebieska.

Zasada działania

Komputer kwantowy – układ fizyczny, do opisu którego wymagana jest mechanika kwantowa, zaprojektowany tak, aby wynik ewolucji tego układu reprezentował rozwiązanie określonego problemu obliczeniowego.
Dane w komputerach kwantowych są reprezentowane przez aktualny stan kwantowy układu stanowiącego komputer. Jego ewolucja odpowiada procesowi obliczeniowemu. Odpowiednie zaplanowanie ewolucji układu kwantowego, czyli stworzenie odpowiedniego algorytmu kwantowego pozwala teoretycznie na osiągnięcie wyników w znacznie efektywniejszy sposób, niż za pomocą tradycyjnych komputerów.

Źródło: Wikipedia

Rejestry kwantowe

Rejestr kwantowy (ang. quantum registers) – układ wielu kubitów, który, zgodnie z jednym z podstawowych postulatów mechaniki kwantowej, może być rozpatrywany jako układ izolowany złożony z wielu układów składowych (poszczególnych kubitów należących do rejestru).

Jedną ze szczególnych własności informatyki kwantowej jest fakt, iż wraz z liniowym wzrostem liczby kubitów w rejestrze kwantowym, rośnie w tempie wykładniczym wymiar przestrzeni stanów takiego rejestru.

Zalety komputerów kwantowych (1)

Komputer kwantowy, mimo że wykorzystywałby inne właściwości fizyczne niż klasyczne komputery, nie umożliwiałby rozwiązywania nowej klasy problemów. Każdy problem rozwiązywalny przez komputer kwantowy może zostać rozwiązany przez komputer klasyczny. Jednak dzięki specyficznym własnościom komputerów kwantowych pewne problemy można byłoby rozwiązać znacznie szybciej, co w praktyce znacznie poszerzyłoby zakres problemów do jakich mogą być użyte komputery.

Zalety komputerów kwantowych (2)

Klasycznym przykładem jest tutaj algorytm faktoryzacji Shora, służący do rozkładu liczb na czynniki pierwsze. Wykonanie podobnego algorytmu dla kilkudziesięciocyfrowych liczb na współczesnych komputerach przekroczyłoby średnią długość życia człowieka, a dla liczb jeszcze większych – czas istnienia wszechświata.
Na komputerach kwantowych możliwe byłoby wykonanie tych operacji w bardziej realnym okresie.

Źródło: Wikipedia

Algorytmy

Jeśli rejestr kwantowy zawiera superpozycję bardzo wielu uzyskanych równolegle wyników, to aby wyłuskać z niego potrzebne nam dane, potrzebujemy algorytmów kwantowych. Algorytmy wykonywane przez komputer kwantowy są algorytmami probabilistycznymi. Oznacza to, że uruchamiając ten sam program na komputerze kwantowym dwukrotnie, można by było otrzymać zupełnie różne wyniki ze względu na losowość procesu kwantowego pomiaru.

Znane m.in.:

- algorytm Shora (faktoryzacji, czyli rozkładu liczb na czynniki pierwsze) 1994,
- algorytm Grovera (przeszukiwania bazy danych) 1995,

Algorytm Shora (1)

Źródło: Wikipedia.

Kwantowy algorytm Shora – algorytm kwantowy umożliwiający rozkład na czynniki pierwsze liczby naturalnej N w czasie $O\left((\log N)^3\right)$ i wykorzystując pamięć $O(\log N)$ przy wykorzystaniu komputera kwantowego. Algorytm ten stanowi teoretyczne zagrożenie dla powszechnie używanego w internecie kryptosystemu RSA.
Klucz publiczny w RSA jest iloczynem dwóch dużych liczb pierwszych. Możliwość efektywnego odtworzenia tych liczb na podstawie klucza publicznego pozwalałaby poznać klucz prywatny i tym samym złamać cały szyfr.

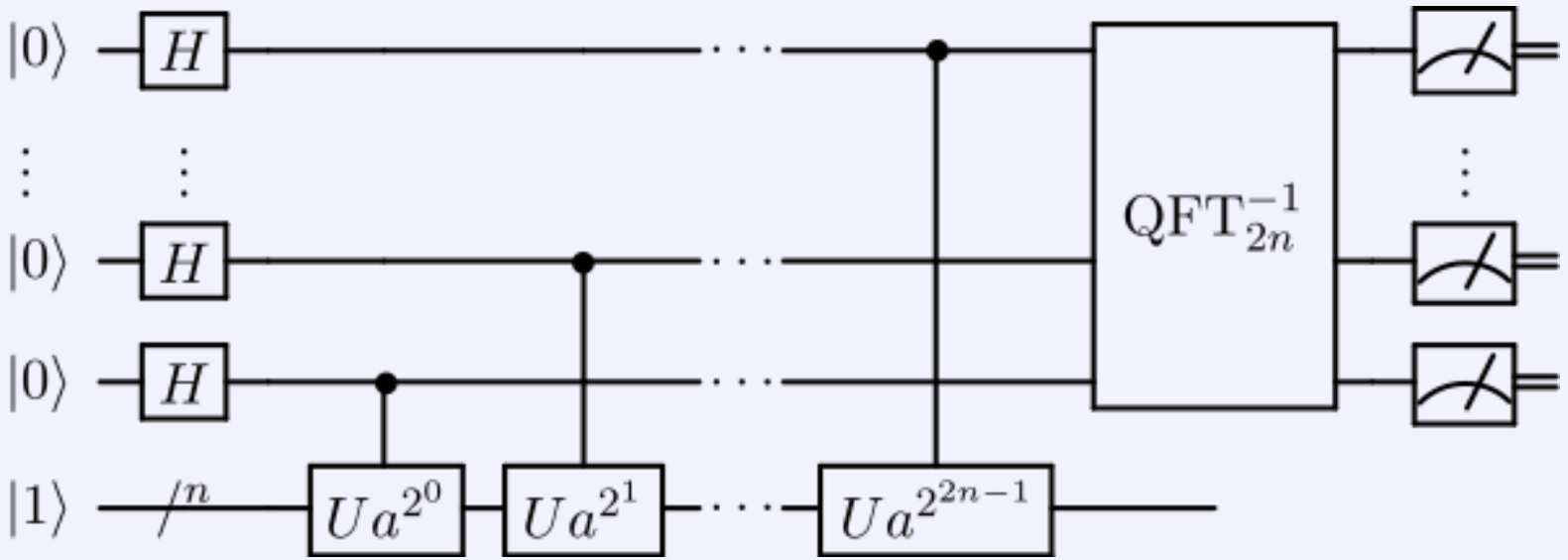
Algorytm Shora (2)

Jak większość algorytmów kwantowych, algorytm Shora jest algorytmem probabilistycznym: zwraca poprawną odpowiedź jedynie z pewnym prawdopodobieństwem. Ponieważ jednak odpowiedź może być szybko sprawdzona, powtarzanie algorytmu umożliwia uzyskanie poprawnej odpowiedzi w sposób efektywny z dowolnie dużym prawdopodobieństwem.

Algorytm ten opublikował Peter Shor w 1994 roku. W 2001 roku grupa informatyków z firmy IBM i Uniwersytetu Stanford zademonstrowała jego działanie na 7-kubitowym komputerze kwantowym opartym o jądrowy rezonans magnetyczny. Dokonano wtedy rozkładu liczby $15 = 3 \cdot 5$.

Faktoryzacji liczby 21 dokonano w 2011 roku.

Algorytm Shora (3)



Algorytm Shora (4)

Ciekawe artykuły:

https://futurenow.com.ua/pl/co-to-jest-algorytm-shora-jakie-sa-jego-mozliwosci-i-zagro#google_vignette

https://ibm.quantum.psnc.pl/algorytm-shora/

https://www.deltami.edu.pl/2017/12/algorytm-faktoryzacji-shora/

Komputery D-Wave Systems (1)

13 lutego 2007 firma D-Wave Systems zaprezentowała 128-kubitowy układ, nazywany pierwszym na świecie komputerem z rejestrem kwantowym. Nie ma jednak pewności, czy można go tak nazwać: zaprezentowano bowiem jedynie jego działanie, pomijając budowę. W 2009 roku D-Wave Systems stworzyło dla Google komputer kwantowy wyszukujący grafiki.W maju 2011 firma Lockheed Martin zakupiła wyprodukowany przez D-Wave Systems komputer za 10 milionów dolarów, podpisując jednocześnie kilkuletni kontrakt na jego obsługę i opracowanie odpowiednich algorytmów. W 2012 roku na komputerze kwantowym zaprezentowano znajdowanie najniższej energii zwiniętego białka.

Źródło: Wikipedia

Komputery D-Wave Systems (2)

W styczniu 2012 roku badacze z D-Wave Systems 84-kubitowym komputerem kwantowym obliczyli kilka liczb Ramseya. Było to największe dotychczas przeprowadzone obliczenie kwantowe.
3 miesiące później przy pomocy 2 kubitów udowodniono, że algorytm Grovera jest poprawny w 95% przypadków. W kwietniu D-Wave Systems poinformowało o Vesuvius – 512-kubitowym czipie, który może dokonywać więcej niż 10^{38} obliczeń naraz, co zajęłoby przeciętnemu PC miliony lat. W sierpniu przy pomocy 5 nadprzewodzących rezonatorów i 4 kubitów fazowych (nadprzewodzące urządzenie bazujące na tunelowaniu Josephsona) pokazano, że algorytm Shora jest poprawny w 50% przypadków, co zgadza się z teorią.

Źródło: Wikipedia

Dygresja – liczby Ramseya

Liczbą Ramseya $R(q_1, q_2, q_3, \ldots, q_k)$ dla $k, q_1, q_2, \ldots, q_k \in N$ i $k \geq 2$ nazywamy najmniejszą liczbę n, taką że dla dowolnego k-pokolorowania krawędziowego n-wierzchołkowego grafu pełnego K_n istnieje i, $1 \leq i \leq k$, takie, że w pokolorowanym grafie jest klika rozmiaru q_i, której wszystkie krawędzie są w kolorze i.

$R(3, 3) = 6$ – w zbiorze 6 osób zawsze znajdziemy 3 osoby znające się wzajemnie lub 3 osoby, które się nie znają.

Wyznaczenie wartości liczb Ramseya jest bardzo trudnym obliczeniowo zadaniem. Często mamy do dyspozycji bardzo dokładne ich oszacowania, a nie jesteśmy w stanie określić ich wartości, mimo że nie są to wielkie liczby.

https://pl.wikipedia.org/wiki/Twierdzenie_Ramseya#Liczby_Ramseya

Dygresja – liczby Ramseya $R(r,s)$

Liczba	Wartość	Odkrywca i rok
R(3,3)	6	Greenwood i Gleason, 1955
R(3,4)	9	Greenwood i Gleason, 1955
R(3,5)	14	Greenwood i Gleason, 1955
R(4,4)	18	Greenwood i Gleason, 1955
R(3,6)	18	Kery, 1964
R(3,7)	23	Kalbfleich, 1966
R(3,8)	28	Graver i Yachel, 1968
R(3,9)	36	McKay i Zhang Ke Min, 1992
R(4,5)	25	McKay i Radziszowski, 1995

Dygresja – oszacowania $R(r,s)$

$$36 \leq R(4,6) \leq 40$$
$$43 \leq R(5,5) \leq 48$$
$$102 \leq R(6,6) \leq 121$$
$$205 \leq R(7,7) \leq 497$$
$$282 \leq R(8,8) \leq 1532$$
$$565 \leq R(9,9) \leq 5366$$
$$798 \leq R(10,10) \leq 17730$$

Źródła:
https://en.wikipedia.org/wiki/Ramsey%27s_theorem

Aktualizowany przegląd w THE ELECTRONIC JOURNAL OF COMBINATORICS (2021): Small Ramsey Numbers

Algorytm kwantowy

W roku 2011 zaproponowany został kwantowy algorytm obliczania dwukolorowych liczb Ramseya $R(m, n)$.
Algorytm został następnie użyty eksperymentalnie do wyliczenia liczb $R(2, 4)$, $R(2, 5)$, $R(2, 6)$, $R(2, 7)$, $R(2, 8)$, $R(3, 3)$, używając komputera kwantowego o 84 kubitach.
Minimalna liczba kubitów niezbędna do wyliczenia dwukolorowej liczby Ramseya wynosi $N(N-1)/2$ gdzie N jest wartością wyliczanej liczby.
Zaproponowany algorytm kwantowy sprawdza, czy dla danej liczby wierzchołków wszystkie grafy mają własność podaną w definicji.
Dla znalezienia liczby Ramseya algorytm uruchamiany jest kolejno dla coraz większych N szukaną wartością $R(m, n)$ jest najniższe N dla którego zwróci on odpowiedź pozytywną.

Artykuł: arXiv, 2015

Komputery D-Wave Systems (3)

Na początku 2014 roku John Smolin i Graeme Smith przedstawili pracę, w której argumentują, że maszyna posiadana przez D-Wave Systems nie jest komputerem kwantowym. Natomiast w marcu 2014 roku w „Nature Physics" przedstawiono wyniki eksperymentów dowodzących, że D-Wave One jest jednak komputerem kwantowym. Znów test z czerwca 2014 nie wykazał różnicy pomiędzy klasycznym komputerem a maszyną D-Wave Systems, lecz firma odpowiedziała, że różnica jest zauważalna dopiero dla bardziej zaawansowanych problemów niż te rozwiązywane w teście.

Źródło: Wikipedia

Komputery D-Wave Systems – artykuł w Spiders's Web

Rok 2014: Google – wielkie rozczarowanie.

http://www.spidersweb.pl/2014/06/komputer-kwantowy-d-wave-two.html

Komputery kwantowe 2017

Najnowsze wynalazki IBM to 50-kubitowy komputer kwantowy oraz 20-kubitowy kwantowy system obliczeniowy, który można udostępnić innym użytkownikom w chmurze obliczeniowej.
IBM zdołał utrzymać stan kwantowy dla obu systemów przez 90 mikrosekund. Choć brzmi niewiele, amerykańskie przedsiębiorstwo osiągnęło w rzeczywistości wielki sukces w utrzymaniu kubitów.

http://zmianynaziemi.pl/wiadomosc/naukowcy-stworzyli-najwydajniejszy-komputer-kwantowy

Bitcoin i komputery kwantowe

Chip, Jacek Tomczyk, 10 listopada 2017.
https://www.chip.pl/2017/11/komputery-kwantowe-zagrozeniem-dla-bitcoina-systemow-banko

Business Insider, Norbert Biedrzycki, 24 kwietnia 2017.
https://businessinsider.com.pl/technologie/nowe-technologie/komputery-kwantowe-i-moce-obliczeniowe-maszyn/5q9xv4m

Historia

Od 1968 do 2023.

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication

(. . .)

4 December – IBM presents its 1121-qubit 'Condor' quantum processor, the successor to its Osprey and Eagle systems. The Condor system was the culmination of IBM's multi-year 'Roadmap to Quantum Advantage' seeking to break the 1 000 qubit threshold.

6 December – A group led by Misha Lukin at Harvard University realises a programmable quantum processor based on logical qubits using reconfigurable neutral atom arrays

IBM Q System One (1)

IBM, 8 stycznia 2019 roku – pierwszy na świecie komercyjny komputer kwantowy.

IBM Quantum System One is the first circuit-based commercial quantum computer, introduced by IBM in January 2019.

This integrated quantum computing system is housed in an airtight borosilicate glass cube that maintains a controlled physical environment. Each face of the cube is 9 feet (2.7 m) wide and tall. A cylindrical protrusion from the center of the ceiling is a dilution refrigerator, containing a 20-qubit transmon quantum processor. It was tested for the first time in the summer of 2018, for two weeks, in Milan, Italy.

https://en.wikipedia.org/wiki/IBM_Q_System_One

IBM Q System One (2)

Sercem komputera jest 20-to kubitowy procesor zdolny obsługiwać nawet najbardziej wymagające aplikacje, takie jak dogłębne analizowanie danych finansowych, obliczenia naukowe czy optymalizowanie różnego rodzaju operacji logistycznych.

Źródło:
https://www.computerworld.pl/news/IBM-Q-System-One-Big-Blue-chce-podbic-rynek-komputerow-kwa411808.html

IBM Q System One (3)

Urządzenie wyprodukowane przez IBM ma wielkość samochodu i znajduje się w centrum obliczeniowym IBM w Poughkeepsie, w stanie New York. 20-kubitowy komputer kwantowy można wynająć za pośrednictwem chmury. (...) Przed nami zatem jeszcze długa droga zanim komputery kwantowe rozwiną się na tyle, aby powszechnie zacząć je stosować w firmach. Jednak już teraz można wykorzystać ich moc w chmurze obliczeniowej IBM.

Źródło: Chip 2019

IBM Q System One (4)

Pomysł IBM polega na umożliwianiu klientom dostępu do maszyny, która w ich imieniu będzie rozwiązywać problemy. Czy w przyszłości uda się stworzyć taki komputer, który będzie można bezpiecznie transportować i składać w biurach lub domach? Nic nie jest wykluczone, a Arvind Krisha, dyrektor IBM Research oraz Hybrid Cloud przekonuje, że prognozy są obiecujące.

W tym roku ma zostać otwarte także pierwsze centrum IBM Q Quantum Computation Center przeznaczone dla klientów zainteresowanych korzystaniem z tego systemu. Będzie się mieścić w Poughkeepsie, w stanie Nowy Jork.

Źródło:
https://www.focus.pl/artykul/pierwszy-komercyjny-komputer-kwantowy-wchodzi-na-rynek

IonQ (1)

IonQ is a quantum computing hardware and software company based in College Park, Maryland. They are developing a general-purpose trapped ion quantum computer and software to generate, optimize, and execute quantum circuits.

IonQ was co-founded by Christopher Monroe and Jungsang Kim, professors at The University of Maryland. and Duke University in 2015, with the help of Harry Weller, a partner at venture firm New Enterprise Associates.

IonQ's hardware is based on a trapped ion architecture, from technology that Monroe developed at the University of Maryland, and that Kim developed at Duke.

Źródło:
https://en.wikipedia.org/wiki/IonQ

IonQ (2)

Inżynierowie zaprezentowali (...) najbardziej zaawansowany komputer kwantowy na świecie. Jest on zdolny do wykonania rekordowej liczby operacji jednocześnie na 79 kubitach. Co najważniejsze, jest to urządzenie nieco inne od podobnych tego typu, ponieważ jako pierwsze bazujące na iterbie. Tymczasem konkurencja w postaci Google i IBM-a wciąż wykorzystuje krzem. Iterb jest wydajniejszy, ale bardzo ciężko dostępny, gdyż w każdej jednej tonie ziemi możemy znaleźć jego tylko 3 gramy.
IonQ informuje, że każdy kwant reprezentowany jest w komputerze przyszłości przez jeden atom iterbu, który został zamknięty w pułapce jonowej. Urządzenie dysponuje w tej chwili pamięcią, w której można zapisać 160 kubitów danych.

Źródło:
http://www.geekweek.pl/news/2018-12-19/firma-ionq-pokazala-najbardziej-obecnie-wydajny-na-swiecie

IonQ (2) c.d.

Na razie naukowcy wykonali kilka testów, a wśród nich znalazł się standardowy z użyciem algorytmu Bernsteina-Vaziraniego. W trakcie jednego z eksperymentów, zadaniem maszyny było odgadnięcie liczby z przedziału od 0 do 1023. Zwykłe komputery potrzebują aż 11 prób dla 10-bitowej liczby, tymczasem komputery kwantowe potrzebują zaledwie dwóch podejść. IonQ już w pierwszym podejściu zgadywał 73 procent z zadanych liczb. W przypadku tradycyjnego komputera osiągnięcie podobnego wyniku w pierwszym podejściu jest niemożliwe.

Źródło:
http://www.geekweek.pl/news/2018-12-19/firma-ionq-pokazala-najbardziej-obecnie-wydajny-na-swiecie

IonQ (3)

Inżynierowie amerykańskiej firmy IonQ użyli iterbu do zbudowania najwydajniejszego na świecie komputera kwantowego. To pierwsza tego typu maszyna, która jeden atom wykorzystuje do zakodowania jednego kubitu danych.

Według IonQ, to obecnie najbardziej wydajny komputer kwantowy. Każdy kwant jest reprezentowany przez jeden atom iterbu zamkniętego w pułapce jonowej. Komputer ma pamięć, w której można zapisać 160 kubitów danych. Może też wykonywać rekordową liczbę operacji jednocześnie na 79 kubitach. Dzięki temu posłuży do wykonywania większej liczby skomplikowanych obliczeń. W przyszłym roku urządzenie zostanie udostępnione naukowcom rozwiązującym problemy z dziedzin takich jak medycyna, chemia, logistyka i energetyka.

Źródło:
https://www.chip.pl/2018/12/79-kubitowy-komputer-kwantowy-ionq-operuje-na-pojedynczych

Symulacja komputera kwantowego (1)

Programistom z australijskiego University of Melbourne udało się stworzyć największą jak do tej pory symulację komputera kwantowego.

Superkomputer Magnus, który został użyty do symulacji, ma 60 wirtualnych kubitów. Aidan Dang, Charles D. Hill i Lloyd C. L. Hollenberg wykorzystali 14 terabajtów pamięci RAM, czyli milion razy mniej, niż wcześniej wymagała podobna symulacja. Dokonali tego przez optymalizację algorytmu Shora. Duże znaczenie w modelowaniu miała nowa jednostka stosowana w komputerach kwantowych, czyli kudit (...). Kudity są wielowymiarowymi stanami kwantowymi, dwuwymiarowy kudit to nic innego jak kubit.

Źródło:
https://www.chip.pl/2018/07/60-wirtualnych-kubitow-i-14-terabajtow-pamieci-ram-symuluj

Symulacja komputera kwantowego (2)

Zadaniem 60-kubitowego modelu było rozłożenie liczby 961307 na czynniki pierwsze. Programiści wykorzystali w tym celu kwantowy algorytm Shora, który od lat pomaga w testowaniu komputerów kwantowych. Służy do faktoryzacji (rozkładu) liczby całkowitej, co może być użyte do łamania zabezpieczeń algorytmów takich jak np. kryptografia klucza publicznego.

Symulacje tego typu służą sprawdzaniu algorytmów dla budowanych komputerów kwantowych. Microsoft stworzył język programowania Q# przeznaczony właśnie do modelowania algorytmów kwantowych. Technologia jeszcze jest w stosunkowo wczesnej fazie rozwoju, a konstrukcje takie jak 50-kubitowy IBM czy 49-kubitowy procesor Intela mają przed sobą jeszcze długą drogę w zwiększaniu mocy obliczeniowej. Niemniej w przyszłości komputery kwantowe będą w stanie rozwiązywać problemy, które dla superkomputerów są nieosiągalne.

Bitcoin i komputery kwantowe

Potencjalny atak na kryptowaluty przeprowadzony z wykorzystaniem procesorów kwantowych może odbyć się również poprzez ingerencję w samą transakcję, modyfikując jej odbiorcę. Gdy transakcja jest publikowana w sieci, jej podpis zawiera klucz prywatny nadawcy, uwierzytelniający jej autentyczność. Komputer kwantowy mógłby potencjalnie odszyfrować klucz prywatny i zmodyfikować nadawcę transakcji, tworząc fałszywy podpis cyfrowy.

Komputery kwantowe nie stanowią jednak zagrożenia dla górników kopiących m.in. bitcoina za pomocą specjalnie do tego przygotowanych układów ASIC. Układy te będą zachowywać wysoką wydajność w porównaniu z komputerami kwantowymi wykorzystywanymi do miningu.

Źródło:
https://www.fxmag.pl/artykul/czy-komputery-kwantowe-zniszcza-bitcoina-i-inne-kryptowalu

Wyścig kwantowy – inwestycje

Kwantowy wyścig trwa. Chiny już inwestują w rozwój tej technologii miliardy dolarów, a sektor ten zaczęły także strategicznie postrzegać Stany Zjednoczone.
O ile w 2020 roku branża obliczeń kwantowych była warta zaledwie 500 milionów dolarów, o tyle w 2027 osiągnie 8,6 mld dol., a na inwestycje w sektor zostanie przeznaczone ponad 16 mld dol. == czytamy w artykule na stronie Voxa.
Źródło: https://forsal.pl/lifestyle/technologie/artykuly/8425495,czy-komputery-kwantowe-sa-przelomowa-tecgnologia.html

Wyścig kwantowy – wyniki dzisiaj: Zuchongzhi 2

Wydajność Zuchongzhi 2 ma być bowiem zauważalnie wyższa niż komputera Sycamore zaprojektowanego przez Google'a.

Zuchongzhi 2 to 66-kubitowy programowalny, nadprzewodzący komputer kwantowy, który zgodnie zapowiedziami jego twórców jest w stanie w ciągu 1 sek. wykonać obliczenia, które zajęłyby najpotężniejszemu superkomputerowi na świecie aż 30 bln lat. Jego twórca, Pan Jianwei, stwierdził, że ta platforma została zaktualizowana ze starszego komputera i obecnie pozwala uruchamiać zadania obliczeniowe 1 mln razy bardziej skomplikowane niż te, które mogą działać na wspomnianym już Google Sycamore.
Źródło: https://www.komputerswiat.pl/aktualnosci/nauka-i-technika/chiny-maja-najszybszy-komputer-kwantowy-na-swiecie-zuchong we3ppsg

Wyścig kwantowy – wyniki dzisiaj: Fujitsu

Firma twierdzi, że posiada najszybszy na świecie symulator kwantowy, który ma dwukrotnie wyższą wydajność od podobnych urządzeń wyprodukowanych przez dwie wiodące na tym rynku potęgi, jakimi są Intel i IBM.
Japoński gigant technologiczny informuje, że jego symulator może obsługiwać 36-kubitowe obwody kwantowe w systemie klastrowym bazującym na superkomputerze firmy PRIMEHPC FX 700, który zawiera te same procesory, które znajdują się najszybszym obecnie na świecie superkomputerze (chodzi o układ A64FX i superkomputer Fugaku).
Źródło: https://www.computerworld.pl/news/Fujitsu-mamy-najszybszy-na-swiecie-symulator-kwantowy,437337.html

Google

https://www.dobreprogramy.pl/google-stworzylo-nowy-komputer-kwantowy-przekracza-mozliwo691563302519465 6a

Podczas gdy maszyna z 2019 roku miała 53 kubity, elementy składowe komputerów kwantowych, urządzenie nowej generacji ma ich 70.
Dodanie większej liczby kubitów zwiększa wykładniczo moc komputera kwantowego, co oznacza, że nowa maszyna jest 241 milionów razy szybsza niż maszyna z 2019 roku.
Naukowcy stwierdzili, że Frontier, wiodący na świecie superkomputer, potrzebowałby 6.18 sekundy, aby wykonać jedno z obliczeń 53-kubitowego komputera Google z 2019 r. Dla porównania wykonanie obliczenia najnowszego komputera kwantowego zajęłoby mu 47.2 lat.

Unia europejska (1)

Creotech Instruments (...) Spółka wchodząca w skład międzynarodowego konsorcjum, które zbuduje dla Unii Europejskiej 100-kubitowy komputer kwantowy do 2025 roku, podpisała umowę wykonawczą z Komisją Europejską na realizację pierwszej części tego projektu.

Zakontraktowana część prac jest pierwszym etapem programu objętego umową ramową, kolejnym celem będzie uzyskanie gotowości technologicznej do budowy 1000-kubitowego rozwiązania do 2029 roku. Zgodnie z zawartą umową budżet dla konsorcjum został ustalony na ok. 20 mln EUR, z czego dla Creotech Instruments przypada ok. 2.2 mln EUR. Umowa będzie realizowana do sierpnia 2026 roku.

Unia europejska (2)

Celem pierwszego etapu budowy dużego komputera kwantowego dla Unii Europejskiej jest powstanie 100-kubitowego komputera do 2025 roku. Na bazie wypracowanych rozwiązań, do 2029 roku zakładane jest uzyskanie gotowości technologicznej do budowy dużego, 1000-kubitowego komputera kwantowego.

Polska

(. . .)

Flagowym projektem w dziedzinie technologii kwantowej w Unii Europejskiej jest Wspólne Przedsięwzięcie na rzecz Europejskich Obliczeń Wielkiej Skali (EuroHPC), które ma za zadanie stworzyć superkomputer umożliwiający walkę z rakiem, przewidywanie zmian pogody i korków w miastach.

Polska została wybrana jako jeden z sześciu już ogłoszonych ośrodków, w których znajdą się pierwsze europejskie komputery kwantowe.

Unia Europejska, 32 europejskie kraje i trzech partnerów prywatnych zadeklarowały w sumie inwestycje na poziomie ponad 100 mln EUR.

https://www.ey.com/pl_pl/digital-first/jak-komputery-kwantowe-moga-zmienicnasza-rzeczywistosc