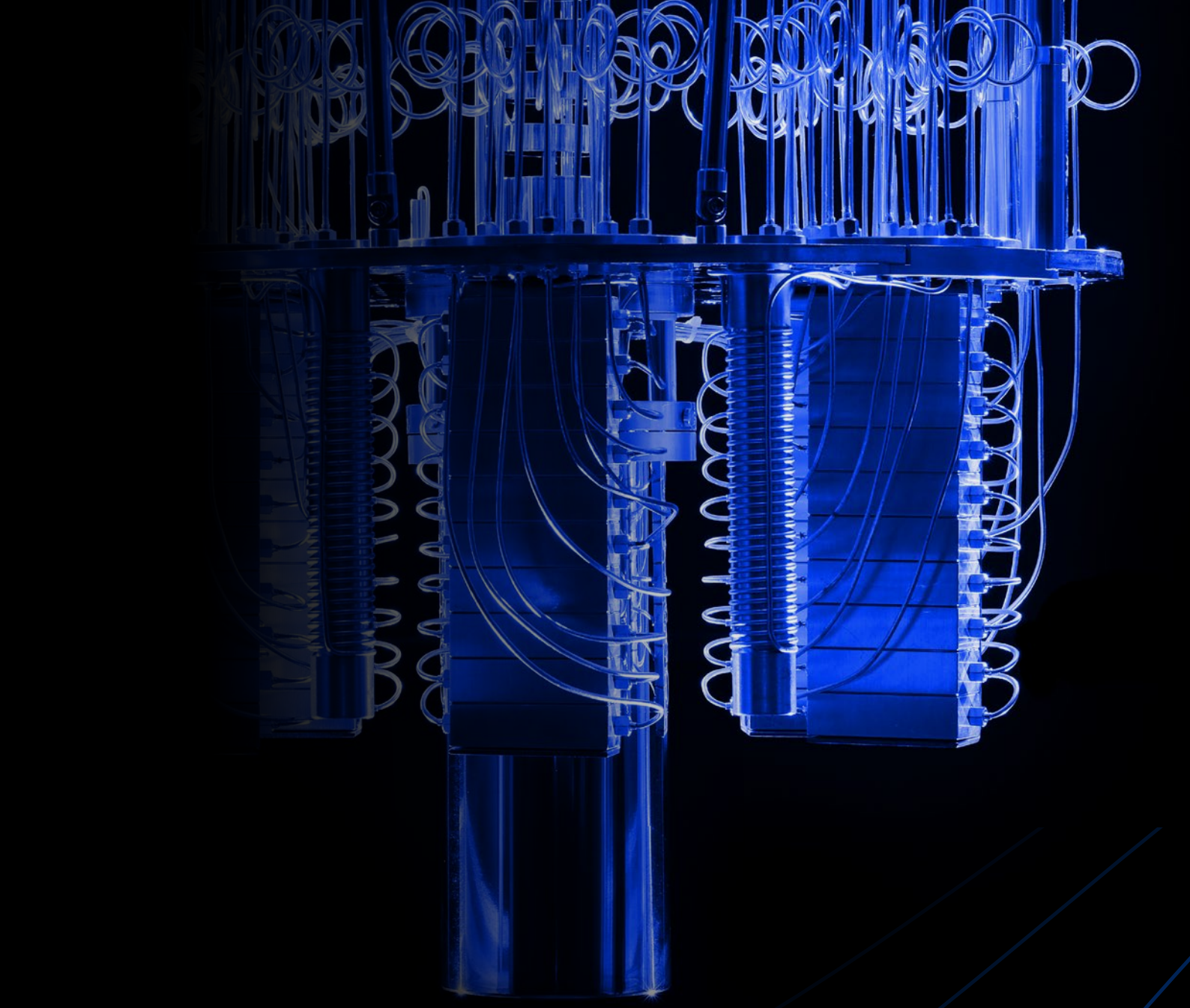


RAPORT QUANTUM
COMPUTING '22

POLSKA
IBM Quantum Innovation Center

POLSKI WĘZEŁ OBLICZEŃ KWANTOWYCH

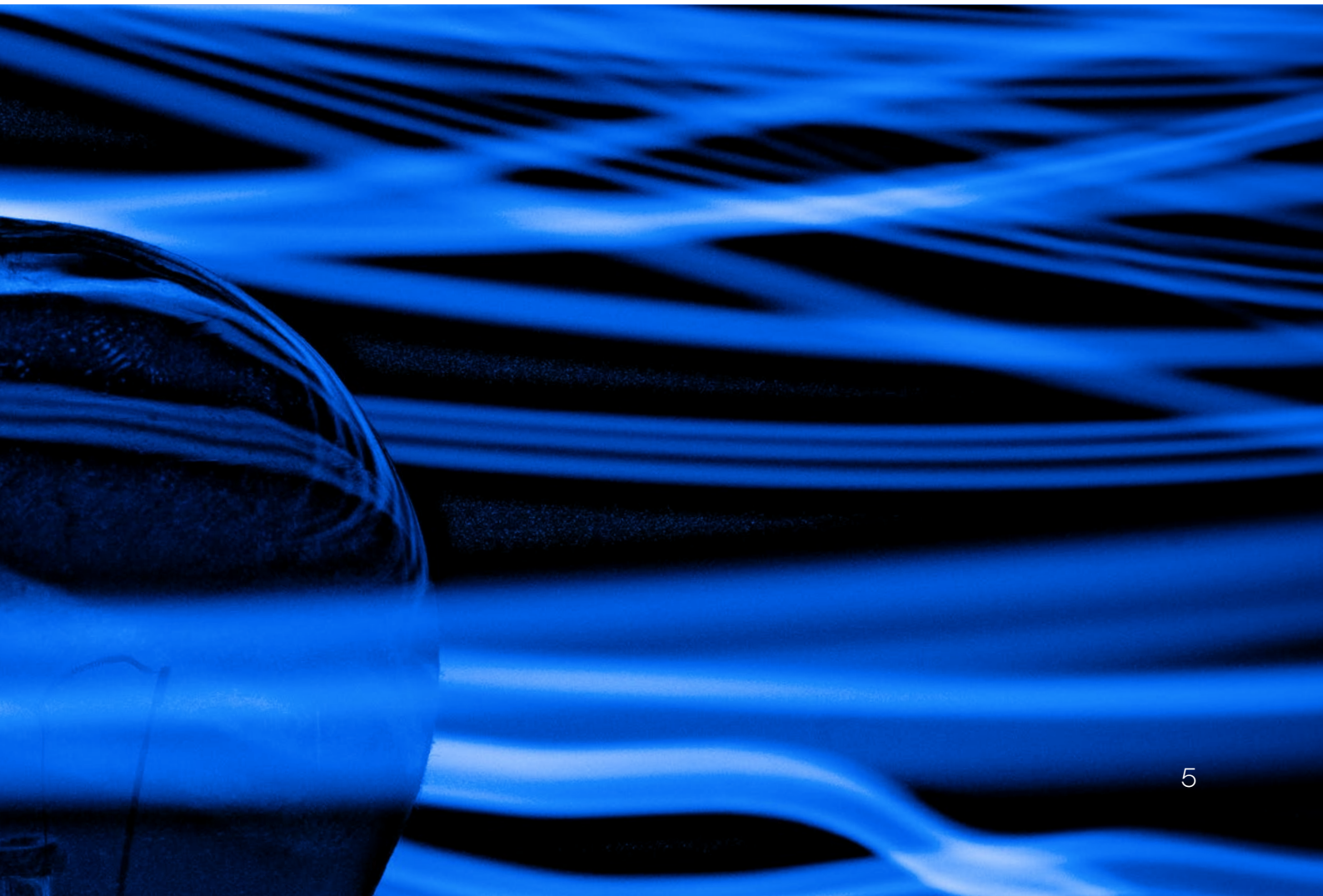
Spis treści

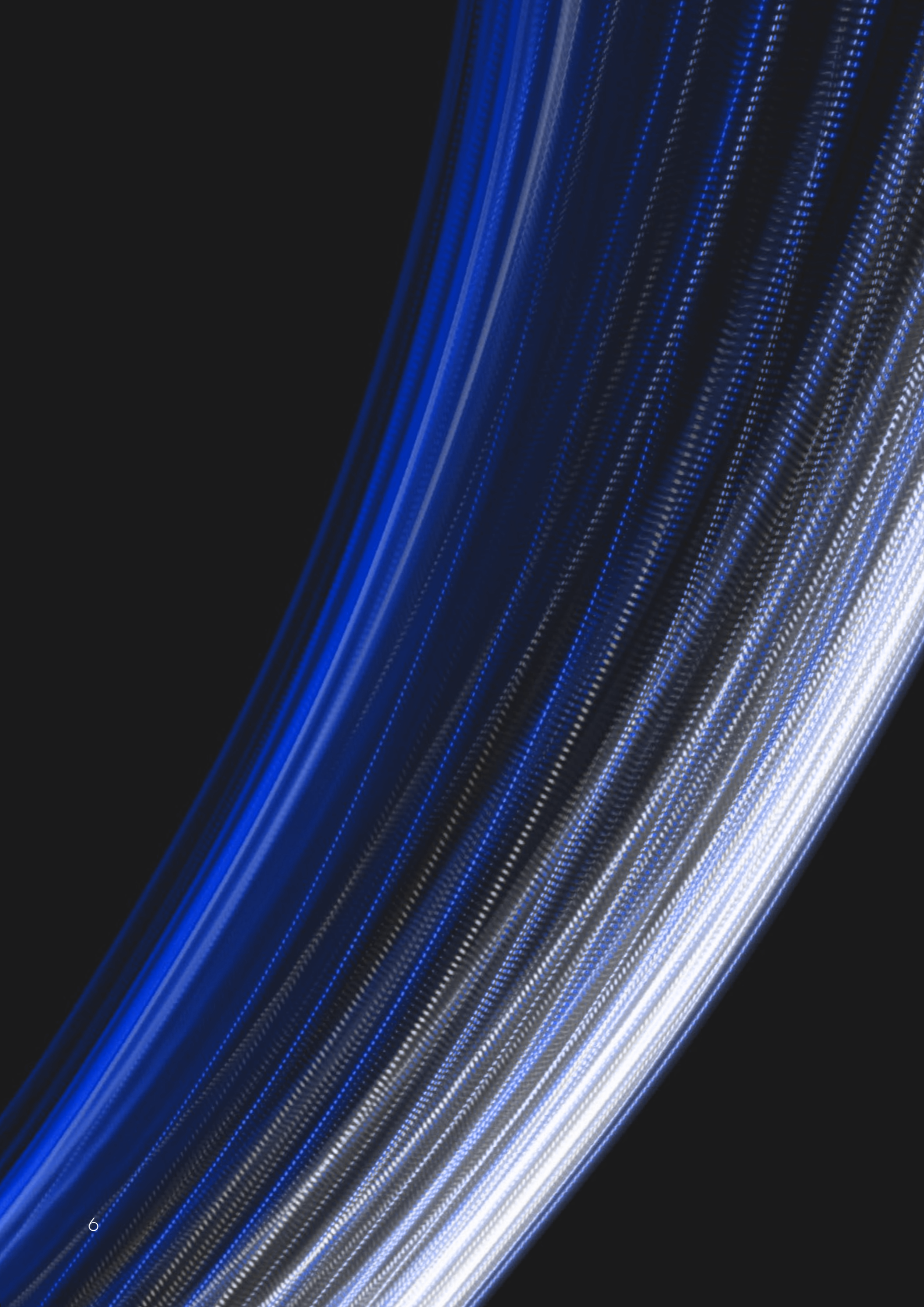
Przedmowa

Wraz z tym raportem czytelnik otrzymuje możliwość zapoznania się z efektami działalności Polskiego Węzła Obliczeń Kwantowych – IBM Quantum w ramach pierwszego etapu działalności w 2022 roku. Dokument jest wynikiem współpracy wielu zespołów naukowo-badawczych w kraju i powstał na bazie wykonanych zadań analitycznych, programistycznych i eksperymentalnych z wykorzystaniem dostępu do infrastruktury zasobów komputerów kwantowych IBM Quantum. Na podstawie zebranych doświadczeń raport przybliża również czytelnikowi aktualny stan rozwoju programowalnych bramkowych komputerów kwantowych IBM Quantum na tle wielu wyzwań, a jednocześnie możliwych zastosowań technologii kwantowych w symulacjach i obliczeniach. Należy zaznaczyć, iż raport jest formą podsumowania i nie wyczerpuje tematyki oraz wszystkich zagadnień podejmowanych przez krajowych użytkowników naukowych, lecz

stara się przybliżyć i wskazać liczne zagadnienia badawczo-rozwojowe szczegółowo podejmowane przez krajowe zespoły eksperckie. Przyjęto założenie, iż podsumowanie pierwszego etapu realizacji zadań powinno w naturalny sposób wprowadzać również czytelnika w świat technologii kwantowych wyjaśniając fizyczne podstawy funkcjonowania komputerów kwantowych. Dołożono starań, aby raport porządkował chronologicznie i tematycznie najważniejsze zagadnienia na pograniczu informatyki i fizyki, aby tym samym trafić do szerszego grona czytelników. W efekcie, raport został podzielony na trzy komplementarne Rozdziały.

Celem raportu jest wprowadzenie czytelnika w obszar zaawansowanych technologii kwantowych, możliwości ich wykorzystania w symulacjach i obliczeniach komputerowych wraz z podsumowaniem realizacji pierwszego okresu działalności Polskiego Węzła Obliczeń Kwantowych.





Rozdział 01

Rozdział 1 przedstawia szereg podstawowych zagadnień wraz z przykładami oraz licznymi ilustracjami przybliżając czytelnikowi założenia, których poznanie ułatwia zrozumienie istoty funkcjonowania komputerów kwantowych, niedoskonałości i wyzwań, a zarazem ogromnego potencjału wdrożeniowego. Wprowadzenie ułatwia czytelnikowi zrozumienie opisów i licznych odniesień zaprezentowanych w dalszych rozdziałach. Rozdział ten jest też próbą przedstawienia wielu ograniczeń i wyzwań związanych z klasycznymi podejściami do obliczeń dużej mocy.

Rozdział 02

Rozdział 2 podsumowuje realizacje głównych zadań w ramach Polskiego Węzła Obliczeń Kwantowych oraz wyjaśnia zagadnienia od strony technologicznej dla bardziej zaawansowanych czytelników zainteresowanych informatyką kwantową oraz testowym dostępem do eksperymentalnej infrastruktury komputerów kwantowych IBM Quantum. W rozdziale tym znajduje się również przegląd rozwiązań technologicznych wraz z oceną stopnia zaawansowania i planowanego rozwoju udostępnianych komputerów kwantowych IBM Quantum w perspektywie najbliższych lat.

Rozdział 03

Rozdział 3 jest podsumowaniem zebranych wyników eksperymentów krajowych użytkowników naukowych, które wykorzystywały zasoby komputerów kwantowych IBM Quantum w okresie od lutego do listopada 2022 przy wsparciu Polskiego Węzła Obliczeń Kwantowych. W tym rozdziale czytelnik znajdzie również zidentyfikowane potencjalne obszary zastosowań obliczeń i symulacji kwantowych na bazie krajowego potencjału naukowo-badawczego oraz możliwości ich wykorzystania w nauce i gospodarce.

Wstęp

Wynalezienie tranzystora – kluczowego komponentu, na którym opiera się cała współczesna elektronika.

Rozwój technologii kwantowych obejmuje również rozwój komputerów kwantowych.

Od kilku lat obserwujemy wręcz niewyobrażalny wyścig w rozwoju technologii kwantowych, za którym stoją najsilniejsze światowe gospodarki. Wiele czołowych firm technologicznych zajmujących się rozwojem komputerów kwantowych przewiduje, że kulminacja rozwoju technologii kwantowych nastąpi do roku 2030. Jest więc wciąż trochę czasu na przygotowanie się na nadchodzącą **drugą rewolucję kwantową**.

Aktualnie istnieje już wiele przykładowych oraz praktycznych rozwiązań wykorzystujących technologie kwantowe, często jednak nie są to jeszcze w pełni gotowe i powszechnie dostępne na rynku rozwiązania. Podobnie wygląda obecnie sytuacja z urządzeniami kwantowymi (nazywanymi w dalszej części komputerami kwantowymi), których aktualny stan zaawansowania wymaga jeszcze ogromnego wysiłku w ich dalszym rozwoju na poziomie zarówno sprzętowym, jak i programowym. Dopóki nie powstanie pierwszy komputer kwantowy, którego moc obliczeniowa znacząco przewyższy moc najsilniejszych superkomputerów w rozwiązaniu złożonego problemu, dopóty trudno jest realnie ocenić wpływ jaki on wywrze na różne sektory gospodarki i społeczeństwo w przyszłości. Historia uczy jednak nas, że w zdecydowanej większości przypadków nie doceniamy długoterminowego potencjału nowych, niezbadanych jeszcze technologii przełomowych, a do takich bez wątpienia należą technologie kwantowe. Komputery kwantowe nie są szybszymi komputerami lub nowymi generacjami bardziej wydajnych klasycznych superkomputerów. Fundamentalne założenia leżące u podstaw budowy współczesnych maszyn liczących, od najmniejszych układów scalonych, mikroprocesorów, aż po wydajne procesory w komputerach osobistych czy najsilniejsze superkomputery, znacząco różnią się od tego, jak funkcjonuje komputer kwantowy, gdzie jego działaniem rządzi nie klasyczna, a kwantowa mechanika.

W raporcie przyglądamy się bliżej temu na jakim etapie rozwoju są komputery kwantowe oraz jak możemy je już dziś eksperymentalnie wykorzystać. Podczas gdy inżynierowie pracują nad udoskonaleniem kolejnych generacji komputerów kwantowych, na przecięciu się informatyki, matematyki, fizyki i wielu innych dziedzin naukowych, opracowywane są nowe metody i algorytmy kwantowe. To właśnie dzięki współpracy praktyków i teoretyków poszerza się potencjalny obszar zastosowań obliczeń kwantowych, a jednocześnie wskazywane są coraz to nowsze wymagania, które nowe generacje komputerów kwantowych muszą spełnić, aby znalazły one zastosowania w praktyce.

Cofnijmy się jednak do początku lat 80, kiedy rozwój komputerów klasycznych nabierał dopiero rozpędu. Jednym z kluczowych momentów, a jednocześnie silnym impulsem do teoretycznych prac związanych z zastosowaniami obliczeń kwantowych były rozważania Richarda Feynmana. Wykorzystując klasyczne komputery do modelowania i symulacji zjawisk fizycznych na poziomie atomów i molekuł Feynman wykazał, że złożoność tych problemów jest bardzo duża, a czas potrzebny na klasyczne obliczenia musi być liczony w miliardach lat i jest dla nas najzwyczajniej nie do zaakceptowania. Aby zmierzyć się z nietrywialnym problemem Feynman zaproponował ideę budowy symulatora kwantowego oraz wykorzystania jego kwantowej natury do symulacji kwantowych zamiast klasycznych obliczeń. Tym samym pojawiły się nowe obszary zastosowań komputerów kwantowych oraz przełomów jakie możemy spodziewać się w inżynierii materiałowej, biochemii czy nanotechnologii.

W obliczu wspomnianej już wcześniej tegorocznej nagrody Nobla z fizyki, aby nieco przybliżyć podstawowe etapy rozwoju mechaniki kwantowej, należy jednak cofnąć się w czasie do lat 60 ubiegłego stulecia i słynnego twierdzenia Bella. John Bell odpowiedział na fundamentalne pytania i naukowe spory, które od lat 30 toczyli najwybitniejsi fizycy świata z Albertem Einsteinem na czele. Teoretyczne założenia zostały potwierdzone eksperymentalnie, a to już mały krok do etapu wdrożenia.

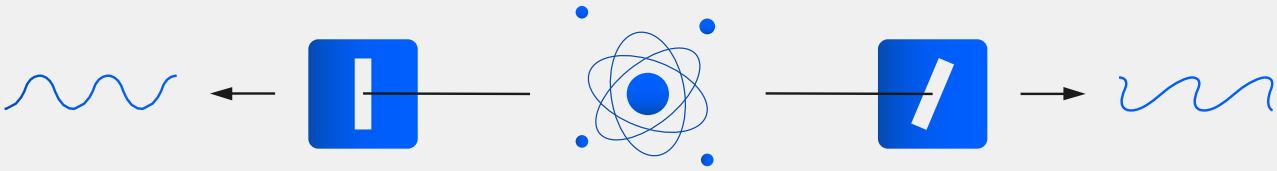
Technologie kwantowe obejmują szerokie spektrum możliwych zastosowań wykraczających znacznie poza obszar komputerów i obliczeń kwantowych, w tym obejmują technologie kwantowej komunikacji i kryptografii oraz nowe generacje sensorów stosowanych w metrologii i technikach pomiarowo-obrazowych. Dalszy postęp technologiczny w każdym z tych obszarów może w najbliższych latach przynieść zupełnie nowe i trudne do przewidzenia konsekwencje dla społeczeństwa, nauki oraz gospodarki.

Splątanie kwantowe na miarę Nobla

4 października 2022 Szwedzka Akademia Nauk ogłosiła przyznanie tegorocznej nagrody Nobla z fizyki dla trzech naukowców — Alain Aspect, John F. Clauser oraz Anton Zeilinger — "**za eksperymenty ze splątanymi fotonami, ustalające naruszenie nierówności Bella i pionierską informatykę kwantową**". Prowadzenie tych badań naukowych było kluczowe w zrozumieniu podstaw mechaniki kwantowej jako fundamentalnej nauki rządzącej prawami naszego świata, a także przetarło szlak dla technologii kwantowych, w tym komputerów kwantowych.

Tegorocznych noblistów można traktować jako ojców drugiej rewolucji kwantowej, gdzie bardzo ważnymi i szeroko wykorzystywanymi elementami są stany splątane oraz tzw. nierówności Bella. Każdy z Noblistów przeprowadził przełomowe eksperymenty wykorzystujące splątane stany kwantowe. Powyższe zagadnienia są kluczowe nie tylko dla komputerów i obliczeń kwantowych, ale również dla komunikacji kwantowej. Nobliści pokazali w swoich pracach eksperymentalnych wykorzystujących splątane fotony, że na poziomie mikroświata nierówności Bella nie są zachowane. Aby zrozumieć wagę konsekwencji tego faktu, zastanówmy się nad samym **splątaniem kwantowym**. W pierwszej kolejności trzeba uświadomić sobie, że świat kwantowy nie jest deterministyczny i wiele „równoległych" stanów może współistnieć ze sobą z różnymi prawdopodobieństwami, a dopiero akt pomiaru niejako materializuje jeden z nich.

Wyobraźmy sobie, że wyemitowane zostaną dwa fotony w przeciwnych kierunkach, a pomiar stanu jednego z fotonów określa to, co zmierzymy, obserwując drugi foton. Mówimy wtedy o splątaniu kwantowym tych fotonów. Jednak trzeba pamiętać, że każdy z tych fotonów jest **superpozycją** (takim niepodglądanym współistnieniem) różnych stanów i dopiero przy pomiarze manifestuje się konkretna wartość badanego parametru, jednocześnie określając pomiar tego parametru u drugiego fotonu. Jest to o tyle szokujące z punktu widzenia naszej intuicji, że to wpływanie na pomiar drugiego fotonu nie zależy od tego, jak daleko się on znalazł. To, co się wydarzy w kontekście jednej cząstki w splątanej parze, automatycznie określa, co się stanie z drugą cząstką, nawet jeśli znajdują się w odległych miejscach (np. w przeciwnych kątach pokoju lub skrajnych brzegach galaktyki). Jednocześnie



już od długiego czasu dyskutowano, czy ta korelacja w splątanej parze wynika z tego, że cząstki posiadają tzw. ukryte zmienne i instrukcje określające jaki, powinien być wynik eksperymentu. W tym miejscu musimy przejść do twierdzenia Bella i jego nierówności. W dużym uproszczeniu twierdzenie określa, że jeśli istnieją ukryte zmienne, to korelacja pomiędzy wynikami większej liczby pomiarów nigdy nie przekroczy pewnego progu. Jednocześnie mechanika kwantowa przewiduje, że pewien typ eksperymentów łamie nierówność Bella i w rezultacie daje mocniejszą korelację, niż ta klasycznie możliwa.

John Stuart Bell opisał w 1964r. twierdzenie, które dotyczy mechaniki kwantowej i pokazuje, w jaki sposób różni się ona od mechaniki klasycznej. Twierdzenie Bella, zwane również **nierównością Bella**, powstało bazując na podstawowym i wspomnianym powyżej założeniu mechaniki kwantowej, czyli, że stan splątany dwóch cząstek kwantowych (np. fotonów) nie może być sprowadzony do opisu stanów jego poszczególnych elementów. Pojedyncza cząstka w danej splątanej parze nie posiada określonego stanu. Twierdzenie mówi, iż powiązania pomiędzy rezultatami pomiarów właściwości takich cząsteczek mogą być silniejsze niż w sytuacji, gdy ich stan byłby zdefiniowany. Główne założenie twierdzenia Bella, czyli, że „żadna lokalna teoria zmiennych ukrytych nie może opisać wszystkich zjawisk mechaniki kwantowej" odpowiada na tzw. **paradoks EPR** [1]. Paradoks EPR jest wcześniejszym wynikiem pracy Alberta Einsteina, Borysa Podolskiego i Nathana Rosena, która opiera się na założeniach, że parametry cząstek kwantowych posiadają wartości niezależne od aktów obserwacji, a oddziaływania fizyczne zachodzą ze skończoną prędkością. Bell w swojej pracy udowodnił, że powyższa teoria tzw. realizmu lokalnego wymusza statystyczne korelacje wyników pomiarów, które nie są spełnione przez mechanikę kwantową i tym samym pokazał, że jest ona sprzeczna z tym założeniem [2].

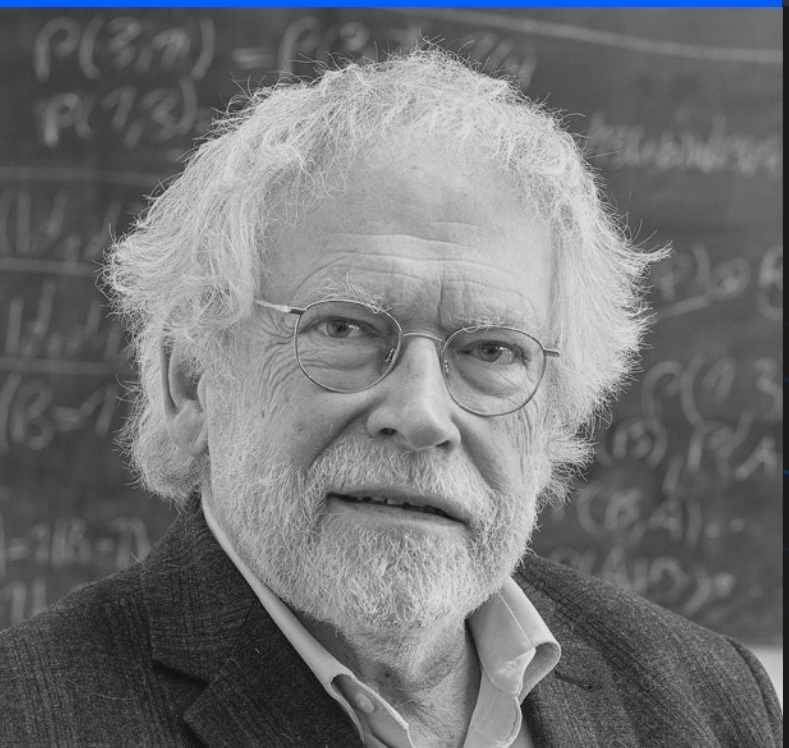
Nierówność Bella można dość prosto zobrazować - albo rzeczywistość nie odpowiada założeniom realizmu lokalnego, albo istnieje błąd w samej mechanice kwantowej. Rozstrzygnięcie tej kwestii można osiągnąć tylko w drodze eksperymentu, nad czym pracowali tegoroczni nobliści. Używając dość luźnej analogii można powiedzieć, że to trochę tak, jakbyśmy obserwowali pary rozbiegających się w dwie strony bliźniaków i obserwowali różne szczegóły ich wyglądu. W świecie dużych wielkości, gdzie rządzi mechanika Newtonowska, wszelkie obserwowane korelacje dotyczyłyby cech obiektywnych, jednoznacznych i immanentnych. Gdyby te pary braci były kwantowe, zauważylibyśmy, że patrzenie na jednego z braci, określa to, co widzimy u drugiego. Natomiast nierówności Bella utwierdzają nas w tym, że ci bliźniacy nie umawiają się w chwili rozbiegnięcia się, jak będą wyglądać szczegóły ich wyglądu, jak ich ktoś w końcu zobaczy.

John F. Clauser

J.F. Clauser & Assoc., Walnut Creek, CA, Stany Zjednoczone

Alain Aspect

Université Paris-Saclay oraz École Polytechnique, Palaiseau, Francja



Anton Zeilinger

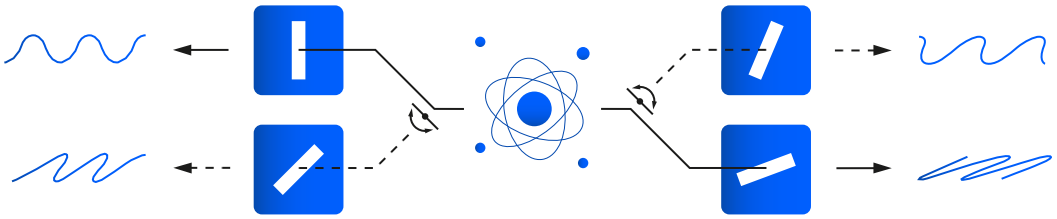
University of Vienna, Austria

John Clauser

John Clauser zaprojektował układ eksperymentalny, którego wyniki obaliły tzw. nierówności Bella, udowadniając tym samym, że mechanika kwantowa wyklucza realizm lokalny. Użył on atomów wapnia, które po oświetleniu specjalnym światłem emitowały splątane fotony. Po obu stronach atomu ustawił filtry do pomiaru polaryzacji cząstek. Seria pomiarów wykluczyła możliwość istnienia lokalnych zmiennych ukrytych.

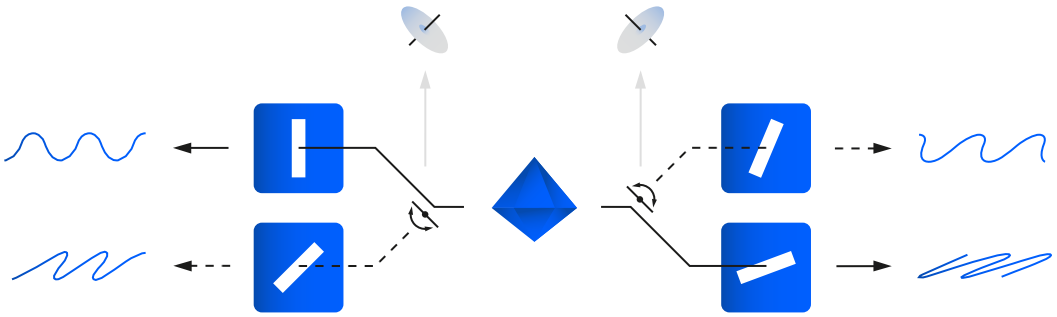
Alain Aspect

Alain Aspect powtórzył i udoskonalił eksperymenty Clausera, a także jako pierwszy udowodnił eksperymentalnie dualizm korpuskularno-falowy pojedynczych fotonów. Wprowadził on modyfikację pozwalającą na zmianę ustawienia filtrów po tym jak foton został wyemitowany z atomu. Pozwoliło to potwierdzić, że na wyniki nie wpłynęło początkowe ustawienie aparatury badawczej.



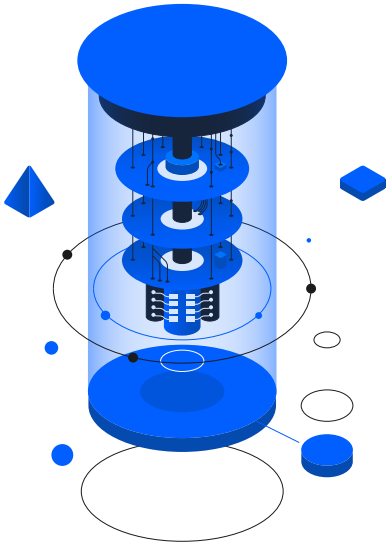
Anton Zeilinger

Anton Zeilinger wykonał kolejne testy nierówności Bella, tym razem korzystając ze specjalnego kryształu jako źródła fotonów, a także losowości do ustawiania konfiguracji filtrów. W jednym z eksperymentów, do ustawienia aparatury wykorzystano sygnały z odległych galaktyk, co pozwoliło wykluczyć możliwość ich wzajemnego oddziaływania. Zeilinger prowadził także badania nad kwantową teleportacją cząstek oraz badał splątanie kwantowe fotonów wysyłanych na duże odległości, co pozwoliło mu osiągnąć już w 2004 r. kanał komunikacji kwantowej o długości 144 km.



Zdjęcia autorstwa (od góry) **[Peter Lyons, Royal Society uploader, Jaqueline Godany], licencja CC.**

Kiedy klasyczne komputery przestają sobie radzić



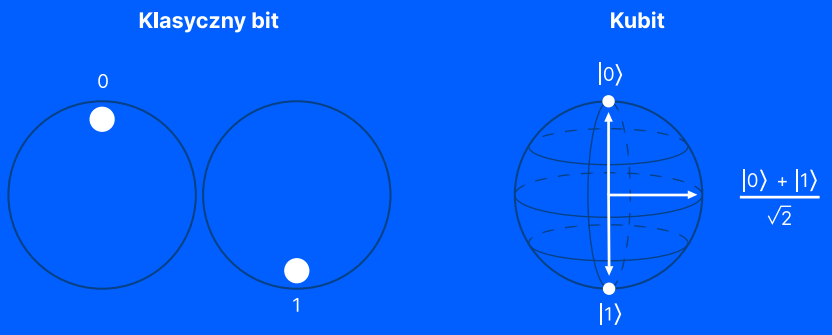
W dzisiejszych czasach trudno wyobrazić sobie świat bez wszechobecnych klasycznych komputerów. Stanowią one filar funkcjonowania instytucji i przedsiębiorstw, a także znajdują szerokie zastosowania codziennego użytku w wielu gospodarstwach domowych. Rozpoczynając od pracy biurowej z dokumentami, arkuszami kalkulacyjnymi czy innymi zaawansowanymi programami, przez wykorzystanie dedykowanych maszyn do pracy na liniach przemysłowych i produkcyjnych, aż do multimedialnej rozrywki, którą są w stanie dostarczyć w formie filmów, muzyki, gier czy interaktywnych symulacji.

Tak jak zaznaczyliśmy już na wstępie, za wszystkimi zastosowaniami klasycznych komputerów stoją prawa fizyki i elektroniki, a każda operacja na komputerze klasycznym opiera się o zakodowane i sterowane przepływy energii elektrycznej zakodowanych w ciągi binarne zer i jedynek. Zasadniczo więc, warto myśleć o informatyce jako o nauce obliczeniowej wywodzącej się z matematyki i fizyki, a więc i podlegającej jej prawom.

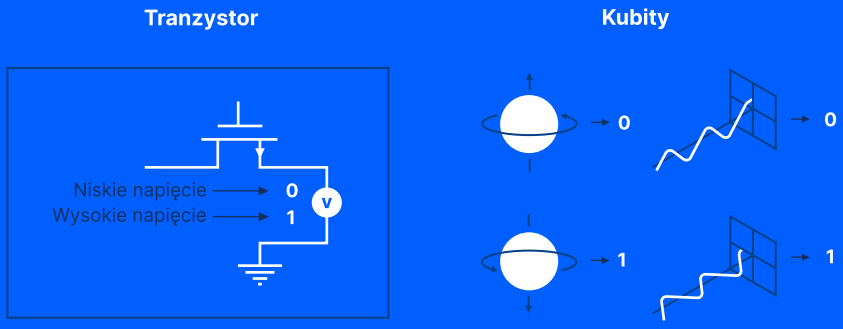
Podstawową jednostką służącą do przetwarzania informacji w klasycznych komputerach jest **bit**. Jednym bitem jest w tym przypadku stan wspomnianego już tranzystora działającego jak prosty przełącznik. Najogólniej mówiąc, logicznej „jedynce” odpowiada wysokie napięcie, a logicznemu „zeru” napięcie niskie. Choć napięcie przyjmuje dowolne wartości z pewnego przedziału, na potrzeby kodowania informacji rozróżniane są tylko **dwa możliwe stany**. Odpowiednikiem klasycznego bitu jako podstawowej klasycznej jednostki informacji jest dowolny kwantowy układ dwustanowy - **kubit**.

Kubit jako dwustanowy układ i podstawowa kwantowa jednostka informacji może w rzeczywistości bazować na różnych cząstkach kwantowych, takich jak na przykład:

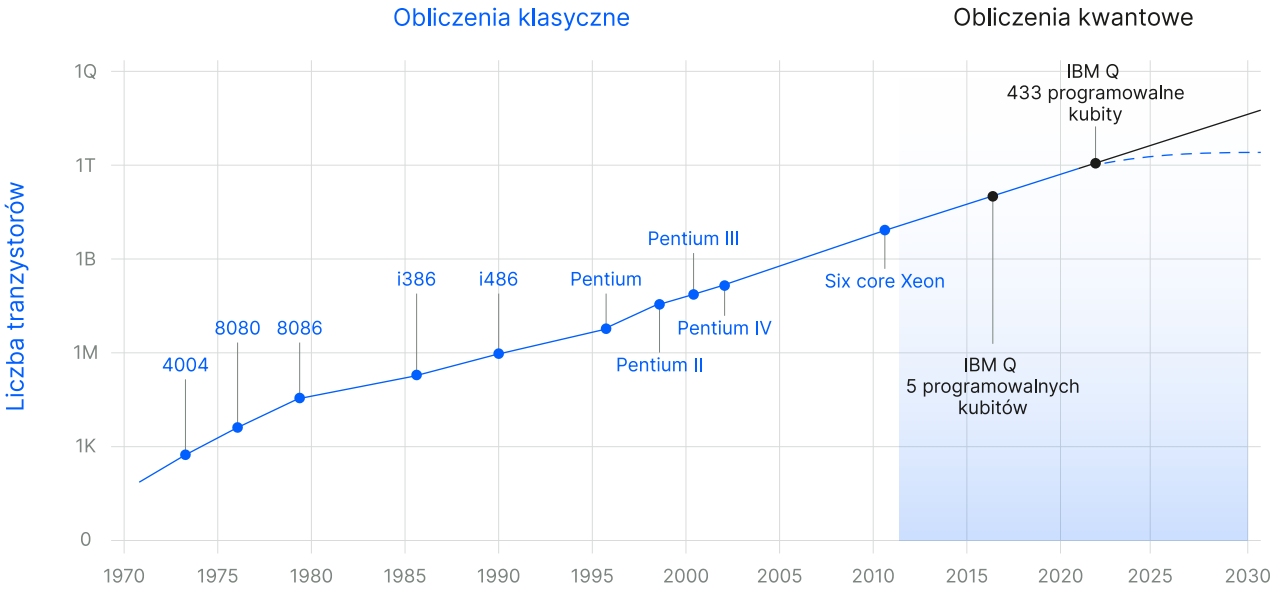
- dwa spiny elektronu
- dwa poziomy energetyczne atomu
- foton o dwóch wzajemnie ortogonalnych stanach polaryzacji.



To właśnie w tym miejscu warto upatrywać analogii pomiędzy klasycznym, a kwantowym komputerem wynikającej z dwustanowości podstawowej jednostki informacji. Nie zmienia to jednak faktu, że sposób zapisu i przetwarzania informacji w przypadku komputerów kwantowych jest znacząco różny. Warto również zaznaczyć, iż wymienione powyżej różne cząstki kwantowe są obecnie budulcem wykorzystywanym do eksperymentalnych konstrukcji **różnych typów komputerów kwantowych.** W odróżnieniu od bitu, kubit wykazuje naturę kwantową, gdyż może znajdować się w **superpozycji** dwóch stanów bazowych. Obrazowo rzecz ujmując, kubit może więc być w obu stanach jednocześnie, np. być jednocześnie trochę bardziej jedynką i trochę mniej zerem. W przypadku klasycznego bitu jest to oczywiście niemożliwe. Superpozycja to jedna z fundamentalnych własności obiektów kwantowych wykorzystywanych w komputerach kwantowych.



Choć na pierwszy rzut oka wszystkie operacje wykonywane w klasycznym komputerze dzieją się w sposób natychmiastowy, to w rzeczywistości każda z nich zajmuje pewien bardzo krótki odcinek czasu. Pomimo że, dla dzisiejszych maszyn cyfrowych nie jest wyzwaniem wykonanie tysięcy czy nawet milionów takich operacji, to wiele zadań stawianych zarówno przez współczesną gospodarkę jak i zwykłych użytkowników jest na tyle złożona, że wciąż stanowi wyzwanie nawet dla najpotężniejszych superkomputerów.

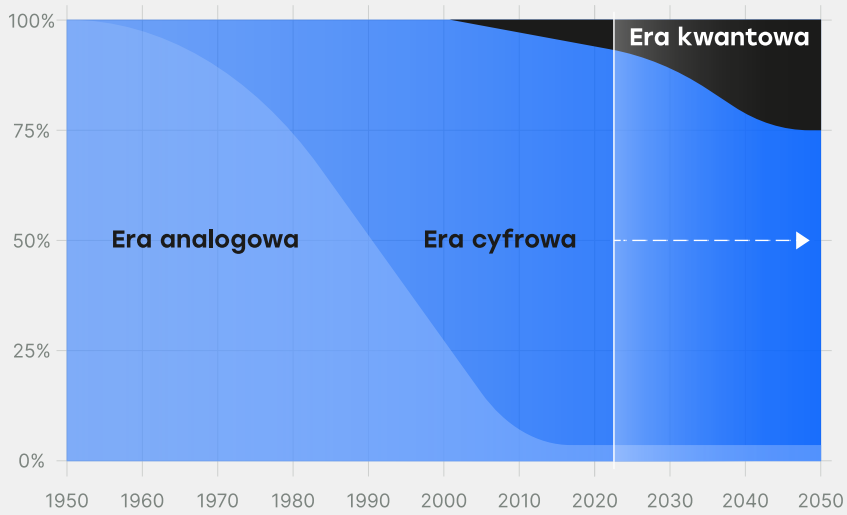


Okazuje się, że komputery klasyczne, oparte o krzemową technologię tranzystorów, mają wiele ograniczeń. O ile klasyczne komputery dobrze sprawdzają się w przypadku wielu zadań, np. wyświetlanie stron internetowych, czy obsługa programów użytkowych edytujących tekst, dźwięk czy materiały wideo, o tyle często można usłyszeć o nowych wyzwaniach i problemach z przetwarzaniem i analizą większej ilości danych. Przykładem może być tutaj produkcja map elektronicznych. Użytkownicy zazwyczaj nie mają problemu z ich wyświetlaniem, jednak samo ich stworzenie wymaga wykorzystania ogromnej mocy obliczeniowej klasycznych superkomputerów. Edycja jednego fragmentu geometrii drogi często wiąże się z przeliczeniem przyległych do niej dróg czy też sprawdzeniem dopuszczalności samej zmiany. Uogólniając, często takie obliczenia właśnie ze względu na ich złożoność obliczeniową są wykonywane w przybliżony sposób, a i tak mogą zajmować sekundy, minuty, godziny czy dni, co dla użytkownika końcowego już jest zauważalnym narzutem czasowym.

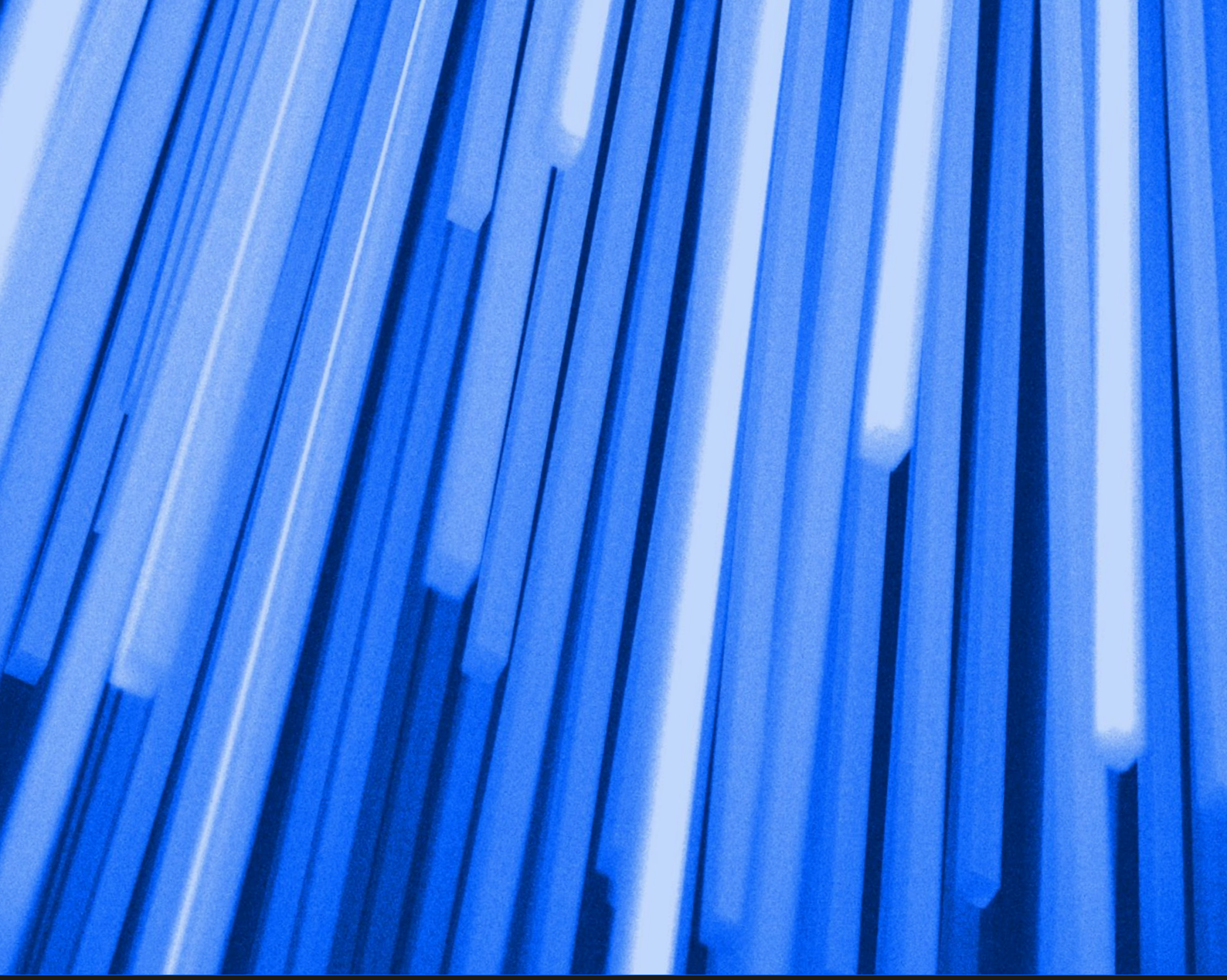
W ostatnich latach rozwój klasycznych komputerów ma dynamikę wzrostu mniejszą niż wskazuje wspomniane na wstępie **prawo Moore'a**. Wielu wskazuje, że jesteśmy świadkami końca ery prawa Moore'a określającej dynamiczny postęp rozwoju klasycznych komputerów w ostatnich dekadach. Tak jak wyjaśniliśmy na wstępie raportu, jest to spowodowane dojściem do fizycznej bariery rozmiarów tranzystorów, których rozmiar zbliża się do rozmiaru pojedynczych atomów. W tak małej skali niepomijalną rolę odgrywają właśnie zjawiska kwantowe, które w przypadku klasycznych układów dwustanowych stanowią dużą przeszkodę dla dalszej miniaturyzacji. W związku z tym coraz większą uwagę poświęca się nowym rozwiązaniom,

które pozwolą utrzymać tempo rozwoju i sprostać wciąż rosnącemu zapotrzebowaniu współczesnego świata na moc obliczeniową. Propozycją rozwiązania tego problemu jest wykorzystanie zjawisk mechaniki kwantowej za pomocą **programowalnego komputera kwantowego**. Dotychczasowe postępy technologii kwantowych obserwowane na przestrzeni ostatnich kilkunastu lat pozwalają przypuszczać, że tempo wzrostu mocy obliczeniowej kolejnych generacji procesorów kwantowych będzie znaczące.

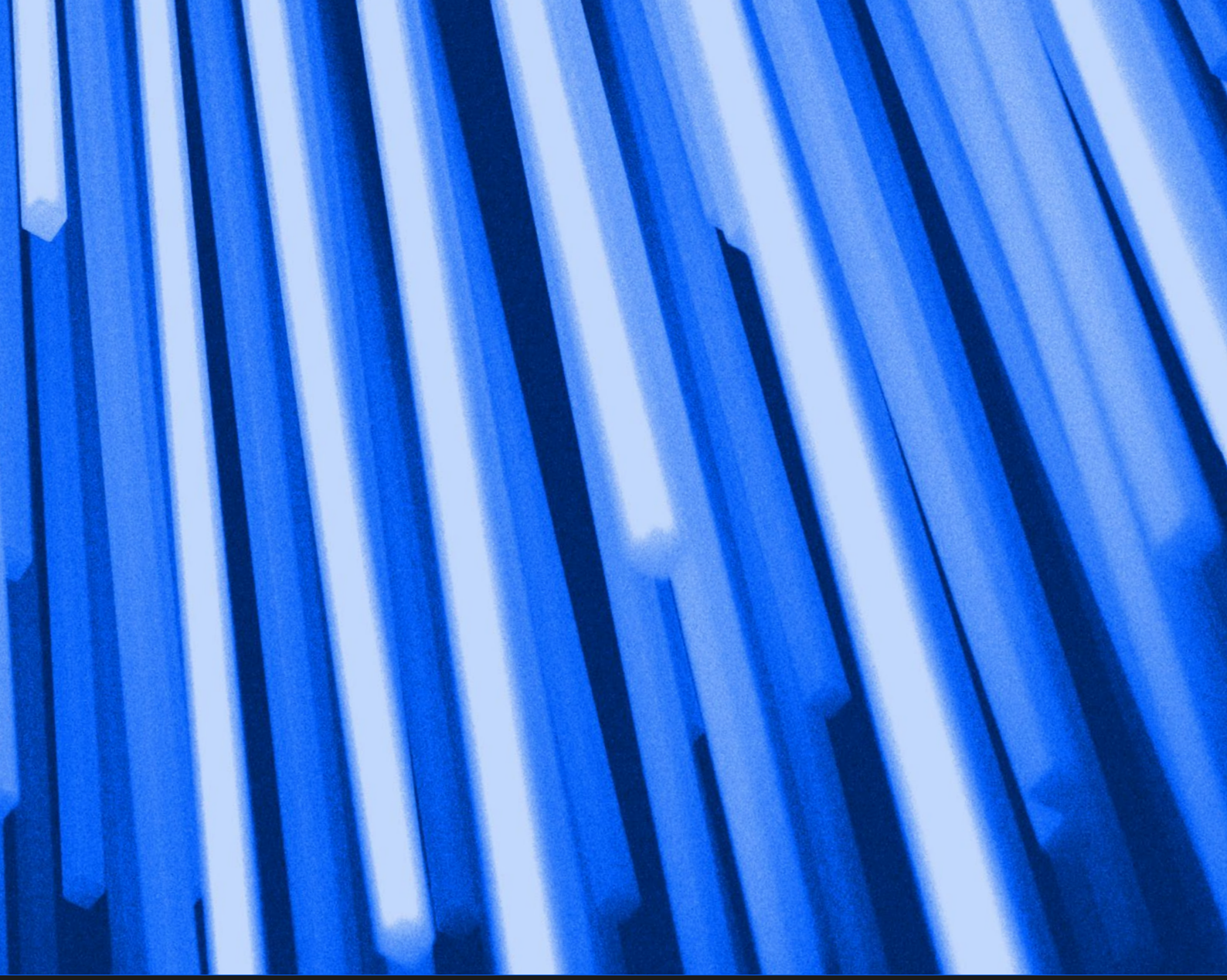
Warto podkreślić, że w najbliższej przyszłości nie należy spodziewać się, że komputery kwantowe całkowicie zastąpią klasyczne komputery. Do zdecydowanej większości codziennych zastosowań klasyczne urządzenia cyfrowe nadają się po prostu znacznie lepiej. Jedynie w przypadku wybranych i wymagających zadań, komputer kwantowy ma dużą szansę, aby uzyskać przewagę nad jego klasycznym odpowiednikiem. Niestety, do dziś w praktyce i oficjalnie **przewaga kwantowa nie została jeszcze wykazana**. Trwają intensywne prace, aby dokonać tego kolejnego przełomu technologicznego. Niemniej jednak, w raporcie postaramy się pokazać wybrane obszary zadań i zagadnień ważnych dla przemysłu, nauki i społeczeństwa w Polsce, które w pierwszej kolejności mogą z takiej przewagi kwantowej skorzystać.



Rozwój technologiczny możliwości przechowywania, przesyłania i przetwarzania informacji z wykorzystaniem analogowych, cyfrowych i kwantowych technologii.



Świat komputerów kwantowych



ROZDZIAŁ

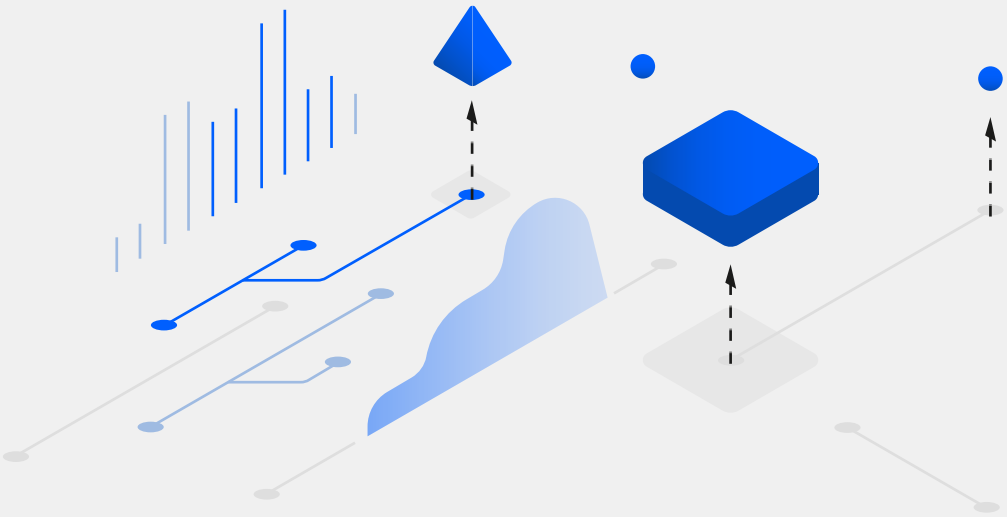
01

Wprowadzenie

Zapoczątkowana w połowie XX wieku rewolucja cyfrowa, zwana także trzecią rewolucją przemysłową, przyniosła ze sobą narzędzia i wynalazki, które na zawsze odmieniły gospodarkę i przemysł, a także doprowadziły do powstania tzw. społeczeństwa informacyjnego. Zamiast pracy i kapitału, strategicznym zasobem stały się dane, informacja i wiedza.

Zanim omówimy podstawowe zasady działania komputerów kwantowych warto tytułem wprowadzenia przypomnieć zasady działania klasycznych komputerów. Wydarzeniem, które znacznie przyspieszyło te zmiany, było wynalezienie tranzystora pod koniec lat czterdziestych XX wieku — kluczowego komponentu, na którym opiera się klasyczny komputer. Tranzystor jest elementem półprzewodnikowym, co oznacza, że w pewnych warunkach przewodzi prąd, a w pewnych nie. Działanie tranzystora opiera się na sterowaniu przepływem prądu elektrycznego z wykorzystaniem fizycznych własności półprzewodników. Tranzystory to najmniejsze elementy klasycznego komputera, które przełączają się pomiędzy dwoma stanami napięciowymi, czyli stanami binarnymi 0 i 1. Z tranzystorów natomiast zbudowane się bramki logiczne realizujące podstawowe funkcje logiczne algebry Boole'a oraz różne typy pamięci klasycznego komputera. Wraz z rozwojem techniki liczba dostępnych tranzystorów i budowanych z nich bramek logicznych wzrastała w niewiarygodnym tempie. Współczesne komputery wykorzystują już **miliony bramek logicznych** do przetwarzania informacji, czyli danych zapisanych w postaci binarnej.

Bramki logiczne to pewien ściśle określony, ale jednak abstrakcyjny model, który pozwala przejść z fizycznego spojrzenia na klasyczne komputery na poziom logiczny. Jest to o tyle istotne, że właśnie tutaj można dopatrywać się subtelnej granicy pomiędzy czysto fizycznym a matematycznym ujęciem istoty działania klasycznego komputera. Zakładając odpowiedni poziom niezawodności działania bramek logicznych, od pewnego momentu nie musieliśmy już skupiać się tylko na technicznych aspektach, fizycznych właściwościach czy kontroli przepływu elektronów w tranzystorach.



W efekcie postępu technologicznego mogliśmy naturalnie przejść na nieco wyższy, logiczny poziom oraz skupić się na istocie działania bramek logicznych, czyli operacjach na dwóch stanach binarnych 0 i 1. **Binarny sposób zapisu informacji oraz jej przetwarzanie z wykorzystaniem wielu bramek logicznych to zasada działania każdego klasycznego komputera**. Samo przetwarzanie informacji w komputerze odbywa się zgodnie ze skończonym i precyzyjnie zdefiniowanym ciągiem instrukcji realizującym określony algorytm, który umożliwia wykonanie zadania i rozwiązanie problemu. Jedną z kluczowych właściwości klasycznego komputera jest możliwość zapisu i wgrywania ciągu instrukcji w postaci programów komputerowych zapisanych w różnych językach programowania. Dzięki temu, że liczba dostępnych bramek logicznych umożliwiała coraz bardziej zaawansowane przetwarzanie danych, jednocześnie wzrastała moc obliczeniowa komputerów. Pojawiały się równocześnie języki programowania wysokiego poziomu, czyli kolejne warstwy abstrakcji ułatwiające programowanie klasycznych komputerów. Przetwarzaniem informacji, w tym tworzeniem programów komputerowych, opisem procesów algorytmicznych, rozwiązywaniem problemów z wykorzystaniem komputerów, obliczeniami i ich złożonością zajmuje się informatyka. Tym samym, w dużym skrócie i uproszczeniu, na tle działania klasycznych komputerów, pokazując kolejne warstwy abstrakcji, przeszliśmy w krótkim opisie od fizyki i matematyki do informatyki.

Przez ostatnie dekady przyzwyczailiśmy się przechowywać i przetwarzać informacje w oparciu o binarny zapis danych, bramki logiczne i układy scalone, z których zbudowane są główne elementy, czyli procesory klasycznych komputerów. Wielu z nas traktuje klasyczne komputery jako osobiste i podręczne narzędzia tak powszechne w użytkowaniu, że nie zastanawiamy się nad ich fizyczną naturą. Rozwój trwa w najlepsze i wszystko wskazuje na to, że komputery klasyczne jeszcze przez długi czas z nami pozostaną. Nie wszyscy jednak zdajemy sobie sprawę, iż w dużym uproszczeniu, liczba tranzystorów i bramek logicznych wchodzących w skład układu scalonego od lat pięćdziesiątych ubiegłego stulecia regularnie rosła w równych okresach czasu. W efekcie co dwa lata podwajała się nam również dostępna moc obliczeniowa klasycznych komputerów zgodnie ze znanym **Prawem Moore'a**.

Problem w tym, iż od kilkunastu lat inżynierowie, naukowcy i technicy poważnie zmagają się z dalszą miniaturyzacją tranzystorów, bramek logicznych i układów scalonych. Na rynku pojawiają się oczywiście reklamowane mocno nowe generacje procesorów, ale w ogólności składają się one jednak z coraz większej liczby rdzeni. Nie są to niestety szybsze procesory

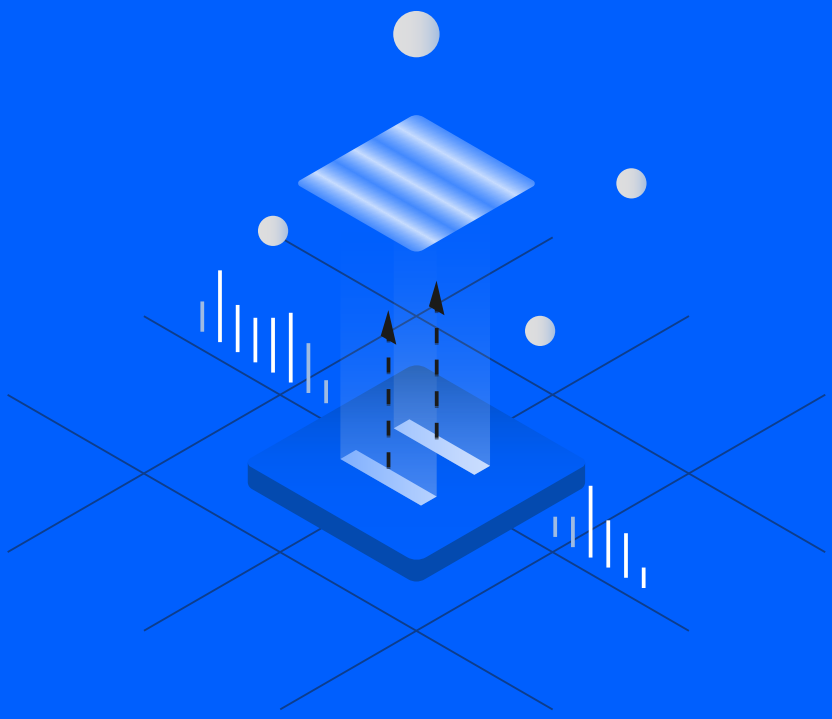
ogólnego przeznaczenia wytworzone w procesach technologicznych dalszej miniaturyzacji, a raczej coraz silniej wyspecjalizowane układy scalone i procesory dedykowane do realizacji określonych funkcji. Ich efektywne i współbieżne wykorzystanie wymaga zaawansowanych umiejętności programistycznych i doświadczenia. Innymi słowy, coraz trudniej jest nam od strony aplikacyjnej wydobyć potencjalną moc obliczeniową drzemiącą w już nie setkach, tysiącach, a setkach milionów układów przetwarzania najsilniejszych klasycznych superkomputerów na świecie. Dodatkowo, dochodzi szereg praktycznych wyzwań oraz kosztów związanych z wysokim zużyciem energii superkomputerów i chłodzeniem zapewniającym im odpowiednie warunki pracy. Mówiąc krótko, dalsze zmniejszanie skali układu scalonego powoduje pojawienie się efektów kwantowych, które utrudniają lub wręcz uniemożliwiają produkcję szybszych klasycznych procesorów. Skala wytwarzanych układów scalonych osiągnęła obecnie rozmiary kilku nanometrów, a to już swojego rodzaju **bariera miniaturyzacji pomiędzy dobrze znanym nam klasycznym, a jeszcze nieodkrytym kwantowym światem**. To właśnie niepożądane efekty mechaniki kwantowej stoją za tą barierą dalszego rozwoju klasycznych komputerów. Dzięki ogromnemu wysiłkowi nauki i techniki, efekty kwantowe, które przeszkadzały w ostatnich latach w dalszej miniaturyzacji tranzystorów okazują się nowym i przełomowym budulcem urządzeń kwantowych (nazywanych dalej w raporcie komputerami kwantowymi). Tym samym, komputery kwantowe mogą teoretycznie nie tylko udostępnić nam niewyobrażalną moc obliczeniową, ale potencjalnie znacząco poprawić wydajność energetyczną przetwarzania informacji, znajdując wiele nowych, praktycznych oraz przełomowych zastosowań.

”

Polska pierwszym hubem kwantowym w Europie Środkowo-Wschodniej

Janusz Cieszyński Sekretarz Stanu,
Pełnomocnik Rządu do Spraw
Cyberbezpieczeństwa w KPRM
4.02.2022 r.

1.1



Jak to właściwie działa?

Aby zobrazować działanie komputera kwantowego, wyobraźmy sobie, że szukany konkretnego, interesującego nas rękopisu. Dostaliśmy informację, że poszukiwane przez nas pismo znajduje się w pewnym starym księgozbiorze, w którym na skutek wielu lat braku odpowiedniej opieki zaniedbane zostało alfabetyczne ułożenie wolumenów. Mając zaufanie do otrzymanej informacji o obecności rękopisu na półkach naszego księgozbioru, zabieramy się do poszukiwań. Zaczynając od pierwszego regału, przeglądamy kolejne pozycje, sprawdzając, czy któraś z nich jest tą, której szukamy. Szybko jednak orientujemy się, że na poszukiwaniach spędzimy więcej czasu, niż zakładaliśmy — księgozbiór jest duży, a półki na każdym z kilkudziesięciu regałów wręcz uginają się pod ciężarem wszelakiej maści ksiąg i pism, nie wspominając o wypełnionych skrzyniach pozostawionych między regałami.

Nie jesteśmy w stanie określić czy będziemy mieli szczęście i szukaną księgę znajdziemy od razu, po kilku pierwszych próbach, czy może zrealizuje się najgorszy możliwy przypadek i znajdziemy ją dopiero pod koniec naszych poszukiwań. Jeśli wielokrotnie przeszukiwalibyśmy rozważany księgozbiór, to statystycznie znajdowalibyśmy szukaną księgę w połowie maksymalnego czasu poszukiwań. Rozsądek jednak nakazuje nam zaplanowanie tyle czasu, ile zajmuje przeszukanie całej biblioteki.

Rozważmy teraz ponownie ten sam księgozbiór. Załóżmy, że zarówno księgozbiór jak i pisma w nim przechowywane mają szereg pewnych specyficznych, wręcz zadziwiających właściwości. Mając dokładną wiedzę o tym, jakiej konkretnie pozycji szukamy, możemy wykorzystać ją do tego, aby lekkim potrząsaniem regałów wprawić je w drgania w taki sposób, aby szukany przez nas rękopis wypadł na podłogę, **samemu się ujawniając**. Oczywiście potrząsanie regałem jest znacznie szybsze niż przeglądanie wszystkich książek, które się na nim znajdują, więc dzięki wspomnianym właściwościom zaoszczędziliśmy sporo czasu. Ważne jest tutaj podkreślenie, że możemy to zrobić z **dowolną** książką znajdującą się na regale — o ile jesteśmy w stanie jednoznacznie zdecydować, czy jest to książka, której szukamy, czy też nie.

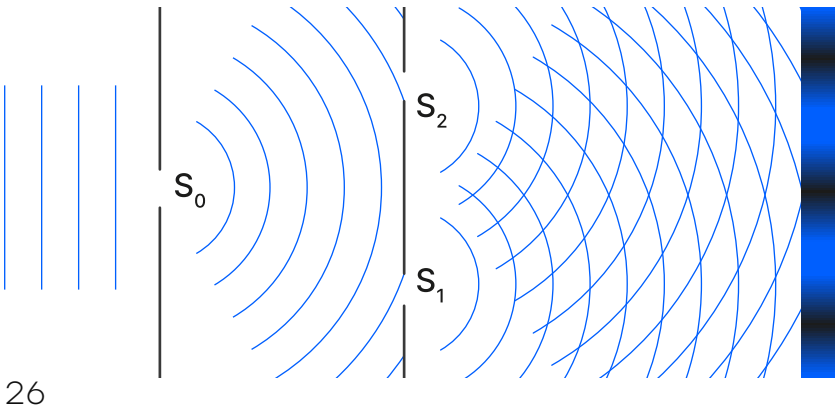
Wyobrażenie to wydaje się być nieprawdopodobne w otaczającym nas, makroskopowym świecie, jednak jest to bardzo dobra analogia do tego, co możemy faktycznie zaobserwować na poziomie kwantowym.

Eksperyment z dwoma szczelinami

Komputery kwantowe nie wykorzystują zjawisk klasycznej fizyki, lecz odpowiednio wykorzystują efekty znane z mechaniki kwantowej. Jednym z najbardziej znanych przykładów obrazujących niezwykłe właściwości kwantowe cząstek jest słynne doświadczenie z dwoma szczelinami. Po raz pierwszy doświadczenie zostało zaprojektowane i wykonane przez angielskiego fizyka Thomasa Younga na początku XIX wieku, które wielu z nas może pamiętać jeszcze z lekcji fizyki.

W samym doświadczeniu wykorzystane zostało światło płomienia świecy. Choć nie było to idealne źródło fotonów, to już wtedy udało się zaobserwować wzór interferencyjny na ekranie, świadczący o **falowej naturze światła**. Dopiero około 100 lat później eksperyment ten wstrząsnął jednak światem naukowym, kiedy udało się uzyskać spójne źródło światła, pozwalające na generację pojedynczych fotonów. Okazało się, że seria pojedynczych fotonów przepuszczonych przez identyczny układ szczelin również wytwarza **prążki interferencyjne** na ekranie. Aby jednak obraz interferencyjny w ogóle powstał, wymagana jest obecność fotonu w obu szczelinach. Choć było to trudne do przyjęcia oraz burzyło wszelką dotychczasową intuicję na temat praw natury i klasycznej fizyki, jedynym wytłumaczeniem musiało być to, że ten sam pojedyńczy **foton znajdował się w obu szczelinach jednocześnie**! Dziś, po wielu latach eksperymentów i teoretycznych rozważań, w tym z udziałem tegorocznych noblistów z fizyki, wiemy, że takie zjawisko faktycznie występuje i dotyczy ono nie tylko fotonów, ale też innych cząstek elementarnych występujących w mikroświecie. Nazywamy je właśnie superpozycją i objawia się ono tym, że do momentu pomiaru cząstka zachowuje się tak, jakby była w każdym możliwym stanie jednocześnie.

Zaskakującym rezultatem tego eksperymentu była obserwacja probabilistycznej natury mechaniki kwantowej. Gdy do jednej ze szczelin zostanie przyłożony detektor fotonów, obraz interferencyjny nie pojawia się, a detektor wykrywa cząstkę mniej więcej w 50% przypadków. Wszystko wskazywało na to, że akt pomiaru w nieodwracalny sposób wpływa na stan kwantowy układu. Ponadto, sam akt pomiaru sprawia, że stan kwantowy zapada się z pewnym prawdopodobieństwem. Taki stan rzeczy pociąga za sobą daleko idące i fundamentalne pytania o prawa rządzące naturą.



Paradoks EPR

Z interpretacją rzeczywistości, jaką mechanika kwantowa zaoferowała na początku XX wieku, nie zgadzało się wielu wybitnych fizyków, w tym sam Albert Einstein, który splątanie nazywał „upiornym działaniem na odległość". Wraz z Podolskym i Rosenem zaproponował on w 1935 r. eksperyment myślowy znany jako paradoks EPR [2].

Wyobraźmy sobie eksperyment, w którym dwie cząstki, np. fotony, zostają odpowiednio przygotowane, a następnie rozdzielone na dowolnie dużą odległość. Jeżeli wpłyniemy w jakiś sposób na stan jednej z cząstek, stan splątanego partnera wydaje się natychmiastowo również ulegać zmianie. Efekt ten sprawia wrażenie, że informacja o zmianie stanu została przekazana z prędkością większą od prędkości światła, co w jawny sposób stoi to w sprzeczności z powszechnie uznawaną **zasadą lokalności**. Odpowiedzią na powstały paradoks, według trzech wspomnianych uczonych było istnienie pewnych ukrytych, potencjalnie niemożliwych do zmierzenia zmiennych, które od samego początku eksperymentu zawierały informacje o tym, jak ma zachować się para splątanych cząstek.

Twierdzenie Bella

W celu zilustrowania twierdzenia Bella posłużymy się prostą analogią. Wyobraźmy sobie urządzenie z trzema przyciskami oraz żarówką. Wciśnięcie jednego z przycisków powoduje zapalenie się żarówki na jeden z dwóch kolorów. Drugie identyczne urządzenie zostaje odpowiednio przygotowane, a następnie oddzielone od pierwszego, w sposób, który uniemożliwia jakąkolwiek niekontrolowaną komunikację między nimi.

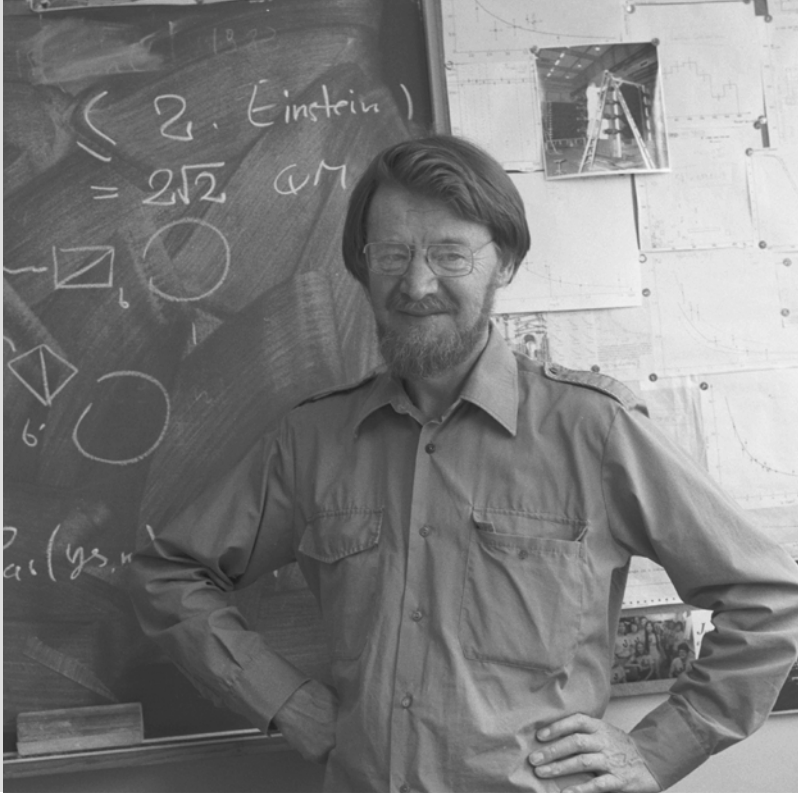
Jeżeli na obu urządzeniach zostanie wciśnięty ten sam przycisk, obie żarówki zawsze zapalają się na ten sam kolor. Ponowne naciskanie tego samego przycisku sprawia, że żarówka dalej świeci tym samym kolorem. Jest to sytuacja analogiczna do **dwóch splątanych cząstek.**

Co jednak stanie się, jeśli na obu urządzeniach wciśniemy różne przyciski? Wówczas na pierwszy rzut oka nie widać żadnej reguły — czasami kolor żarówek jest taki sam, a innym razem różny. Istnieją dwie możliwości wyjaśnienia takiego zachowania — albo rezultat wciśnięcia danego przycisku został już wcześniej zaprogramowany w obu urządzeniach, albo jest on zupełnie losowy, zależny za każdym razem od rzutu monetą.

John Stewart Bell

postać której dokonania przybliżyły ludzkość do zrozumienia jak wszechświat działa w mikroskali. W 1964 r. wykazał on matematycznie, że korelacji w splątanej parze cząstek nie można wytłumaczyć żadną lokalną teorią zmiennych ukrytych [2].

Źródło: Zdjęcie autorstwa CERN PhotoLab



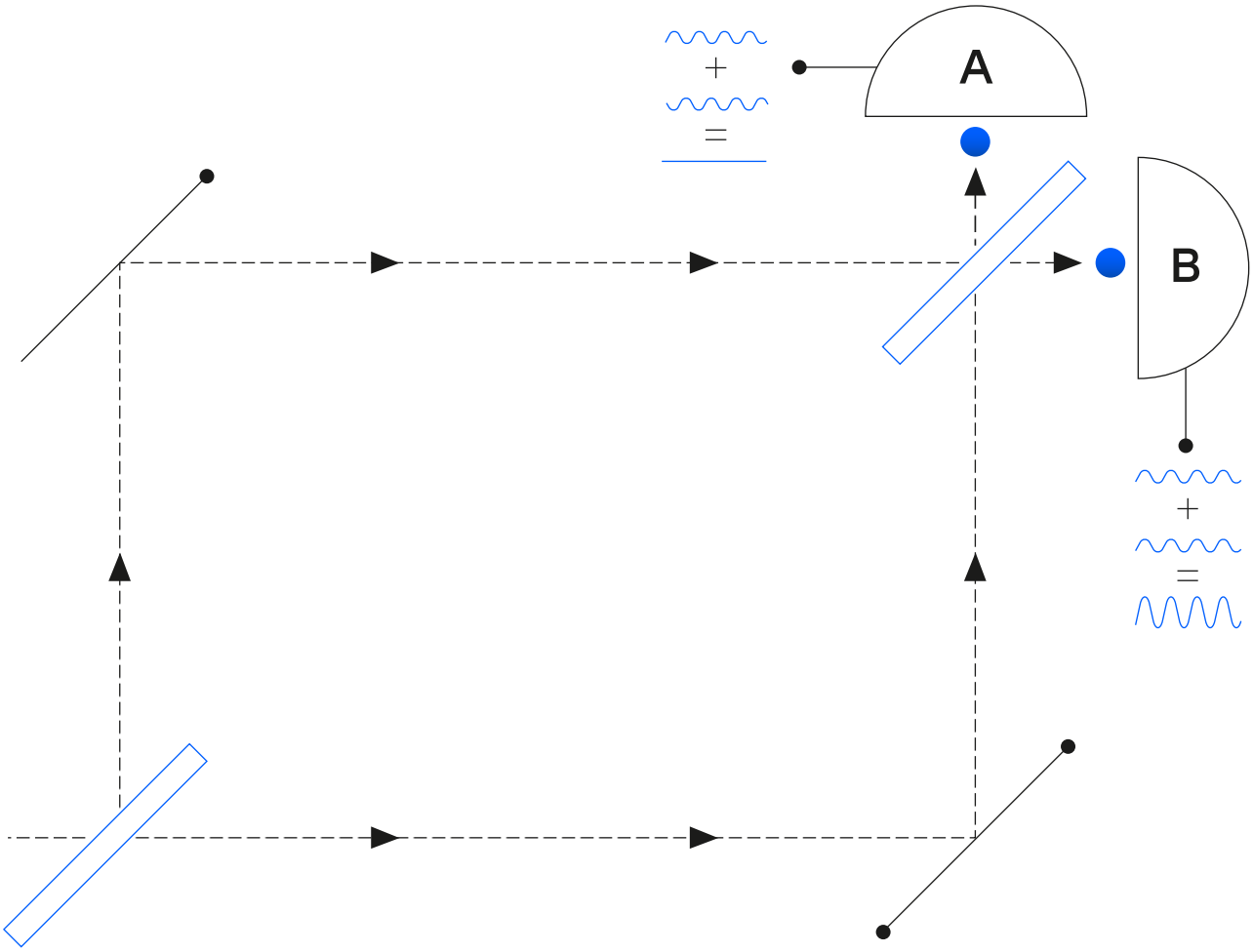
W celu ustalenia, która wersja jest prawdziwa, wykonujemy prosty test, wciskając po kolei na obu urządzeniach wszystkie możliwe kombinacje przycisków. Dla przykładu załóżmy, że ukryty mechanizm determinujący zachowanie obu urządzeń działa w następujący sposób: przycisk 1 zapala żarówkę na szaro, przycisk 2 na niebiesko, a przycisk 3 na szaro. Wyniki eksperymentu możemy przedstawić w tabeli:

UKRYTY MECHANIZM	**PRZYCISKI**							
1 ○ 2 ● 3 ○	1 - 1	1 - 2	1- 3	2 - 2	2 - 3	3 - 1	3 - 2	3 - 3
Ten sam kolor?	Tak	Nie	Tak	Nie	Tak	Nie	Tak	Nie

Jak można zauważyć, żarówka zapaliła się na ten sam kolor w 5 na 9 możliwych przypadków, co odpowiada szansie równej ok. 55%. Ponieważ zakładamy istnienie ukrytego mechanizmu, bez względu na to, ile razy powtórzymy doświadczenie, zawsze otrzymamy te same wyniki. Podobne rozumowanie można przeprowadzić dla każdej innej kombinacji kolorów określonych w tym mechanizmie i w każdym przypadku rezultat będzie identyczny — zgodność w 5 na 9 przypadków. Jeżeli natomiast urządzenia działałyby w sposób losowy, czyli zgodny z założeniami mechaniki kwantowej, szansa na to, że kolory będą takie same, wynosi dokładnie 50%.

Zgodnie z twierdzeniem Bella, w doświadczeniach fizycznych z rzeczywistymi cząstkami kwantowymi obserwujemy właśnie tę drugą ewentualność, a więc nie mógł istnieć żaden ukryty mechanizm zawczasu determinujący wynik analogicznego eksperymentu. Nagroda Nobla z fizyki w 2022 roku powędrowała do grona trzech naukowców, którzy eksperymentalnie udowodnili naruszenie nierówności Bella.

Rozbrajamy bombę



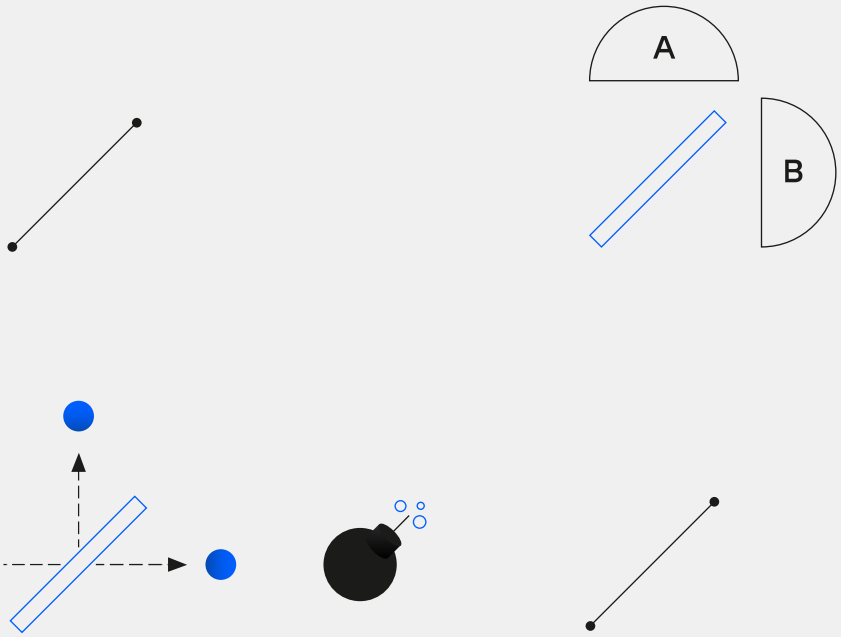
Na prostym przykładzie pokażemy, jak można wykorzystać **superpozycję** i **splątanie**, w celu uzyskania lepszego niż jest to możliwe klasycznie detektora bomb. Do tego celu potrzebne będzie skonstruowanie obwodu optycznego składającego się ze źródła fotonów, dwóch płytek półprzepuszczalnych, dwóch zwierciadeł oraz dwóch detektorów. Pojedynczy foton po przejściu przez pierwszą płytkę półprzepuszczalną znajduje się w stanie superpozycji, co oznacza, że znajduje się jednocześnie w górnej i dolnej ścieżce. Następnie interferuje sam ze sobą, przez co następuje wygaszenie na drodze do detektora A i wzmocnienie na drodze do detektora B. Ponieważ na ścieżce do detektora A występuje interferencja destruktywna, to

prawdopodobieństwo odczytu fotonu w detektorze B wynosi 100%. Jest to pewnego rodzaju transformacja opisanego wcześniej eksperymentu z dwoma szczelinami, w którym również cząstka interferowała sama ze sobą, dzięki czemu możliwe było utworzenie wzoru interferencyjnego na ekranie.

Do układu na jednej ze ścieżek fotonu dodamy teraz bombę, która wybucha przy kontakcie z fotonem. Ponieważ wybuch bomby stanowi klasyczny akt pomiaru, istnieje 50-procentowe prawdopodobieństwo, że bomba wybuchnie. Jeżeli jednak foton przeleciał górną częścią obwodu, to znów z prawdopodobieństwem 50% rozdzieli się na wiązkę górną i dolną, a zatem z równym prawdopodobieństwem aktywuje detektory A i B.

Brak interferencji jest związany z aktem pomiaru wykonanym przez bombę. Od tego momentu foton nie znajduje się on już w stanie superpozycji, a przyjmuje konkretną pozycję w układzie. W przeciwieństwie do poprzedniego przypadku, mamy teraz jakąkolwiek szansę na aktywację detektora A. Z prawdopodobieństwem 25% możemy wykryć bombę bez konieczności jej detonacji.

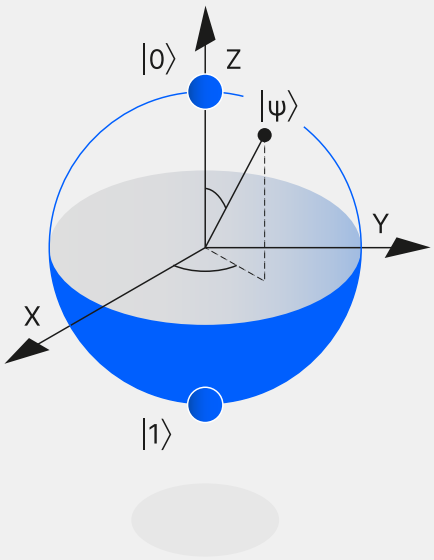
Prawdopodobieństwo 25% nie wydaje się duże, zwłaszcza jeśli zależy od niego detonacja bomby. Jednak nadal jest to więcej niż bylibyśmy w stanie zrobić, wykorzystując zasady mechaniki klasycznej, gdzie niemożliwe byłoby wykrycie bomby bez jej detonacji. Poza tym, stosując innego rodzaju płytki półprzepuszczalne ze współczynnikami transmisji i odbicia innymi niż 50%, możliwe jest zbliżenie się do prawdopodobieństwa równego 100%.

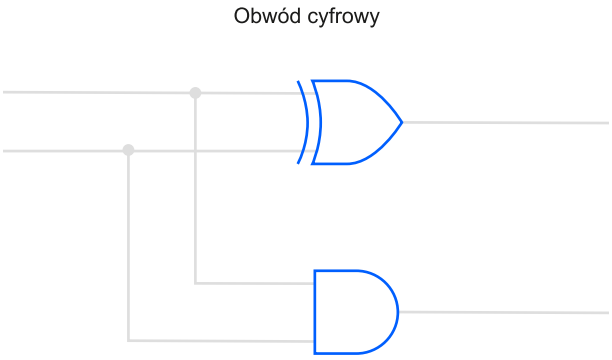


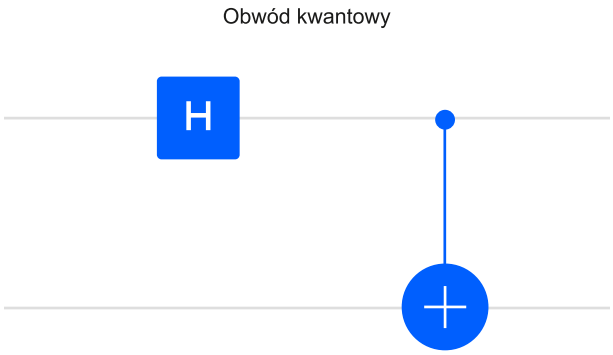
Jak osiągnąć przewagę w obliczeniach?

W praktyce można zaprojektować wiele eksperymentów, które będą przedstawiać intrygujące zjawiska kwantowe. Przykładem zastosowania takich procesów fizycznych mogą być bardzo dokładne kwantowe sensory. Jednak do przeprowadzenia obliczeń kwantowych, potrzebujemy uzyskać zmienne, które będzie można wykorzystać w algorytmach kwantowych. Dlatego analogicznie do klasycznego bitu — zmiennej przyjmującej jedną z dwóch wartości binarnych — 0 lub 1, posłużymy się teraz naszym kubitem — kwantową zmienną binarną. Kubit, wprowadzony w stan superpozycji znajduje się w obu stanach jednocześnie i dopiero jego odczyt powoduje otrzymanie konkretnej wartości. Możemy wykorzystać tę własność, wykonując równolegle wiele obliczeń przy użyciu tej samej cząstki, by następnie szybko odczytać właściwy wynik. Osiągnięcie takiego przyspieszenia nie byłoby możliwe przy użyciu klasycznego komputera.

Graficzną reprezentację kubitu przedstawia **sfera Blocha**, czyli zespolona sfera o promieniu 1, w której przy pomocy dwóch kątów można zakodować punkt reprezentujący kubit. Wówczas operacje na kubitach można przedstawić jako rotacje lub transformacje wokół osi X, Y, Z, gdzie X i Z są osiami rzeczywistymi związanymi z różnymi bazami pomiarowymi kubitu, natomiast oś Y jest związana z zespolonym czynnikiem fazowym kubitu. Prawdopodobieństwo odczytu danego stanu zależy od położenia wektora względem biegunów sfery.

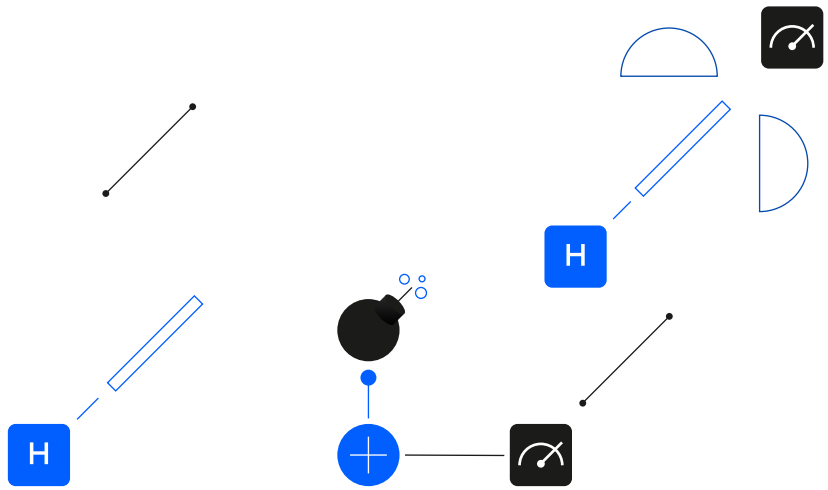




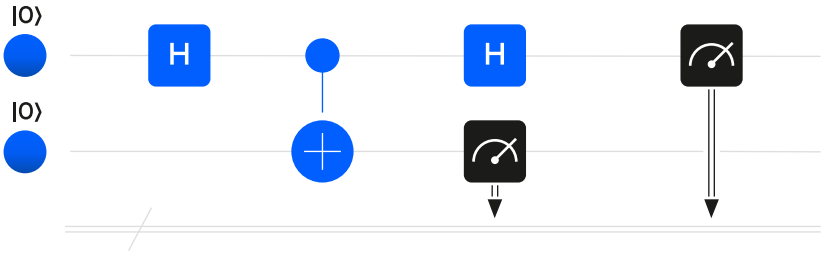


Każdy algorytm kwantowy można zapisać przy pomocy transformacji kubitów. Poprzez analogię do układów logicznych (cyfrowych), do zapisu algorytmów kwantowych stosuje się obwody kwantowe składające się z bramek. Do najpopularniejszych **bramek** należą **X**, **Y** oraz **Z**, służące do rotacji kubitu wokół odpowiadających osi na sferze Blocha, a **także bramka Hadamarda (bramka H) służąca do tworzenia superpozycji** oraz dwukubitowa bramka **CNOT tworząca splątanie pomiędzy kubitami**. Opisany powyżej układ z bombą można przedstawić za pomocą takiego właśnie **obwodu kwantowego** , wykorzystując bramki wytwarzające superpozycję i splątanie.

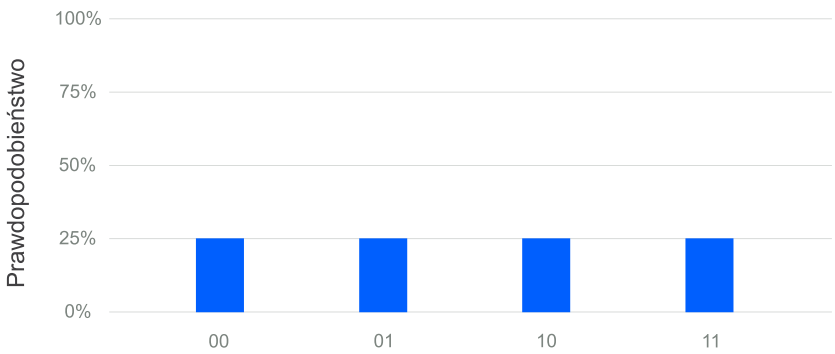
Wyniki uruchomienia takiego obwodu kwantowego są probabilistyczne, jednak wykonując pewną liczbę prób, można zauważyć rozkład zbliżony do teoretycznego. Obrazuje to histogram, na którym możliwe są 4 możliwości. Wartość 1 pierwszego kubitu oznacza detonację bomby. Jeśli bomba nie została zdetonowana i wartość kubitu pierwszego wynosi 0, mamy dwie możliwości dla kubitu drugiego - 0 i 1. Ich prawdopodobieństwa są równe i wynoszą odpowiednio 25%.

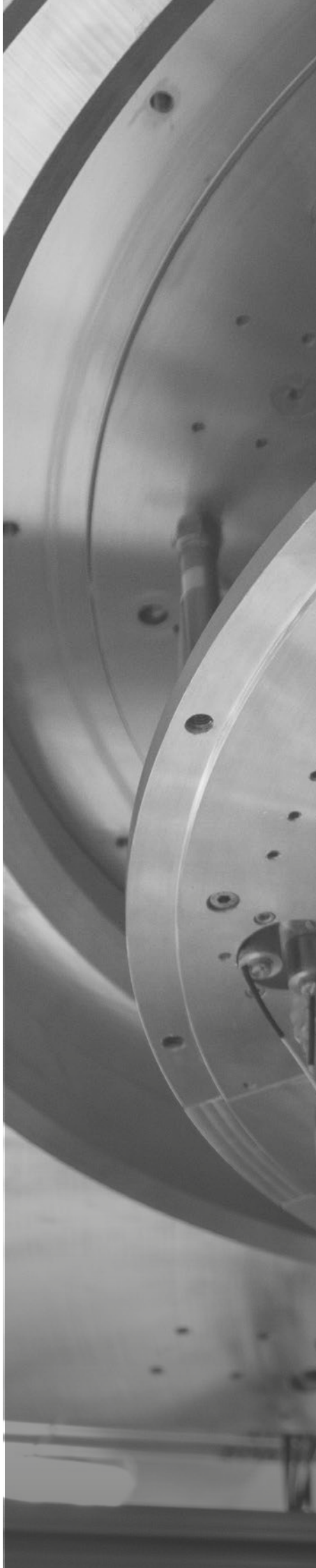


Programowanie komputerów kwantowych sprowadza się do projektowania i budowy obwodów kwantowych składających się z wielu bramek kwantowych. Ponieważ pomiar i otrzymanie wyniku w komputerze kwantowym zawsze związane jest z jakimś prawdopodobieństwem, należy wielokrotnie wykonać odczyt.



Kluczowym zadaniem w programowaniu komputera kwantowego jest stworzenie układu kwantowego w taki sposób, aby **prawdopodobieństwo odczytania najlepszego wyniku dla rozwiązywanego problemu było jak największe.**

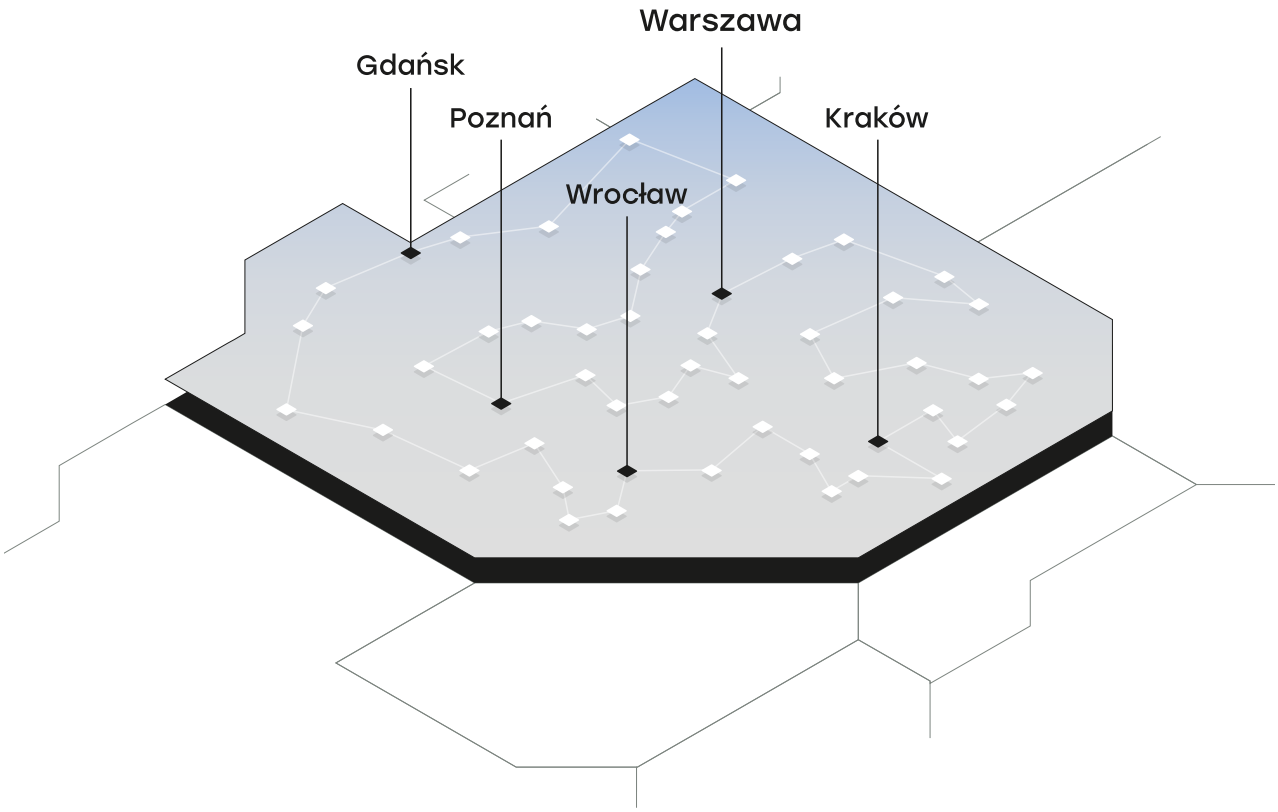




Źródło: IBM Quantum Computer Interior

1.2

Do czego można to wykorzystać?



Wcielmy się w rolę sprzedawcy

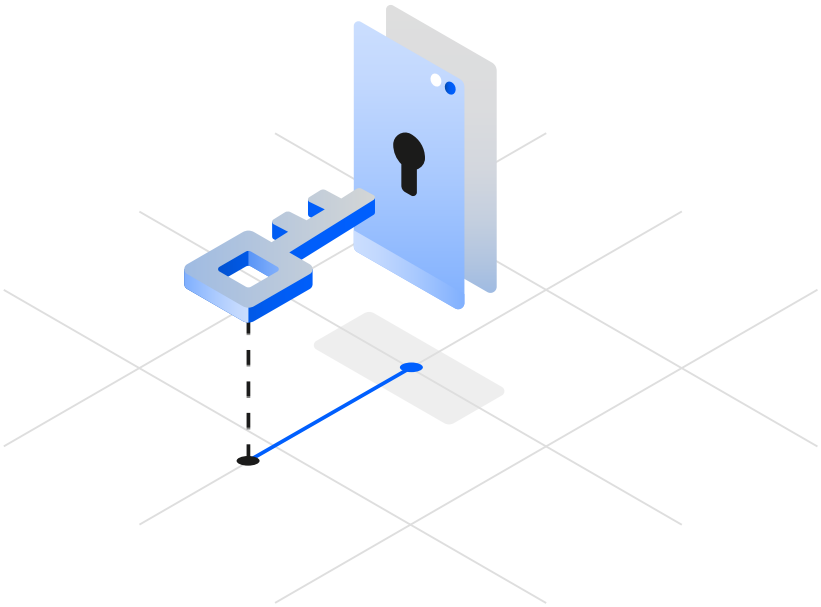
Przykładem zadania zbyt złożonego nawet dla superkomputerów, które po odpowiednim przekształceniu można rozwiązać na komputerze kwantowym może być optymalne ułożenie trasy dla przedstawiciela handlowego w taki sposób, aby ten mógł w jak najkrótszym czasie rozwieźć wszystkie przesyłki. O ile dla niewielkiej liczby punktów do odwiedzenia, zwykły komputer jest w stanie obliczyć optymalną trasę w krótkim czasie, o tyle dla większej liczby takich miejsc (większej niż kilkanaście) złożoność obliczeniowa rośnie do niewyobrażalnie dużych rozmiarów*. Dzieje się tak, ponieważ liczba wszystkich możliwych tras, zwana również permutacją, rośnie bardzo szybko wraz ze wzrostem punktów docelowych. Przykładowo, jeśli kierowca chciałby ustalić najszybszą trasę między szesnastoma miastami wojewódzkimi w Polsce, najszybszy superkomputer rozwiązałby taki problem w jedną setną sekundy. Wydaje się to rozsądnym

* Obecnie prędkość najszybszych superkomputerów jest na poziomie jednego exaFLOPS-a, czyli około 10^{18} operacji zmiennoprzecinkowych na sekundę, co daje około 10^{21} operacji na godzinę, a więc około 10^{25} operacji rocznie. Wszystkich tras, którymi kurier może odwiedzić miasta jest n!, a więc dla 25 paczek mamy około 10^{25} możliwości. Przyjmujemy dla uproszczenia, że jedną możliwą drogę wystarczy wykonać tylko jedną operacje, chociaż w rzeczywistości ta liczba byłaby jeszcze kilkanaście razy większa.

i akceptowalnym czasem. Co by się jednak stało, gdyby zaszła potrzeba odwiedzenia kolejnych dziewięciu miast? Okazuje się, że dla 25 miast, obliczenie najkrótszej trasy przez najszybszy na świecie superkomputer zajęłoby już cały rok!* Jeśli dalej byśmy zwiększali liczbę miast, będzie jeszcze trudniej. Dla wybranych 37 miast w Polsce o liczbie mieszkańców większej niż 100 tysięcy, czas obliczeń wyniósłby trylion lat (dla porównania: szacowany wiek wszechświata to 13 miliardów lat), a dla wszystkich miast powiatowych w Polsce, takie obliczenia zajęłyby 10^{609} lat. Taki okres czasu obliczeń jest tak duży, że trudno nawet wskazać jakąś rozsądną i ciekawą analogie.

Korzystając z komputerów kwantowych możemy **„zrównoleglić" obliczenia.** Można sobie to porównać do sytuacji, w której komputer kwantowy korzystając ze zjawiska superpozycji i splątania wielu kubitów, niejako jednocześnie sprawdza wszystkie potencjalne trasy kuriera i wybiera z nich tę najlepszą.

Uwaga na bezpieczeństwo Internetu



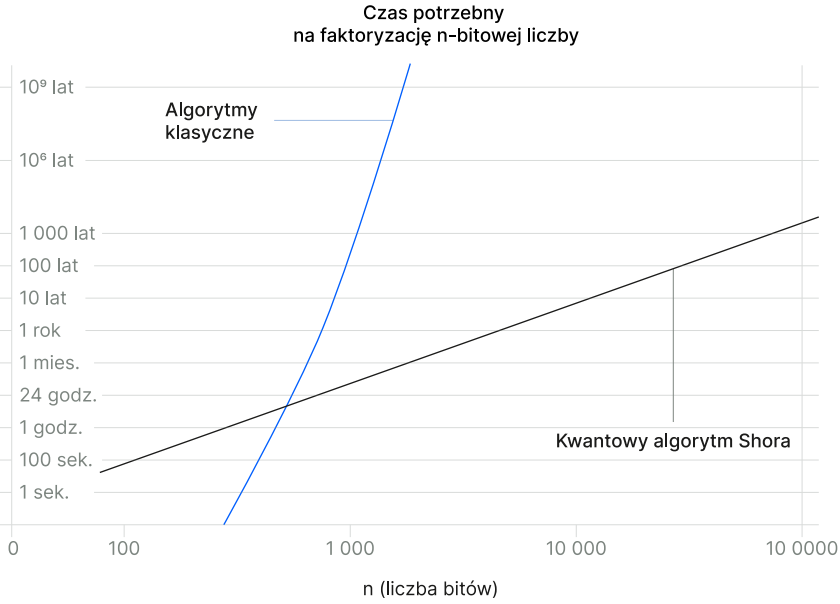
Algorytm Shora

Jednym z najpopularniejszych zastosowań, do których możliwe będzie zastosowanie komputerów kwantowych, jest **kryptografia kwantowa**. Obecnie jednym z najczęściej używanych algorytmów do szyfrowania haseł na stronach internetowych, czy też zabezpieczania transakcji bankowych jest algorytm RSA oparty o parę asymetrycznych kluczy. Swoją popularność zawdzięcza temu, iż mimo swej prostoty złamanie zabezpieczeń, czyli odkrycie klucza prywatnego, jest niesamowicie czasochłonne dla klasycznych superkomputerów. Wynika to z pewnych matematycznych właściwości, o które oparty jest algorytm RSA. Jednym z kroków do wygenerowania pary kluczy (publicznego — do szyfrowania wiadomości, oraz prywatnego — do odszyfrowywania wiadomości) jest pomnożenie przez siebie dwóch, bardzo dużych liczb pierwszych.

Aby odszyfrować klucz publiczny, niezbędne jest odwrócenie tego procesu, czyli tak zwana faktoryzacja, która dla klasycznych komputerów jest niezwykle trudnym zadaniem. Przykładowo, do złamania 2048-bitowego klucza, zwykły klasyczny komputer potrzebowałby trylionów lat.

```python
from qiskit.algorithms import Shor

shor = Shor()

result = shor.factor(15)
```

Okazuje się jednak, że przy pomocy pewnych matematycznych twierdzeń dotyczących mnożenia wywodzących się z teorii liczb, jesteśmy w stanie tak zmodyfikować problem faktoryzacji, aby wprowadzić do niego cykliczność. Zauważył to amerykański naukowiec Peter Shor w 1994 roku [3]. Shor opracował algorytm wykorzystujący kwantową transformatę Fouriera i zawartą w niej negatywną interferencję fal do znalezienia częstotliwości wspomnianej cykliczności, co w konsekwencji prowadzi do rozwiązania problemu. O ile na ten moment nie stwarza to niebezpieczeństwa dla obecnie używanych systemów zabezpieczających ze względu na niewielką moc dostępnych komputerów kwantowych, o tyle już dzisiaj niezbędne jest podejmowanie działań przygotowujących świat cyfrowy na moment, w którym komputery kwantowe będą na tyle zaawansowane, aby być w stanie łamać zabezpieczenia internetowe.



POTENCJALNE RYZYKA

- Kradzież tożsamości
- Deszyfrowanie poufnych danych
- Odkodowanie kluczy prywatnych
- Złamanie szyfrowania RSA

Krytycznym przypadkiem użycia pozostaje zdolność komputerów kwantowych do złamania szyfrowania RSA. W dniu 4 maja 2022 r. Kancelaria Prezydenta Stanów Zjednoczonych opublikowało memorandum NSM-10 wymagające przejścia wrażliwych krajowych systemów na kryptografię odporną na kwantowe obliczenia [17]. Stany Zjednoczone to pierwszy kraj, który podjął systemowe działania zabezpieczające przed potencjalnym zagrożeniem związanym z niepożądanym wykorzystaniem komputerów kwantowych.

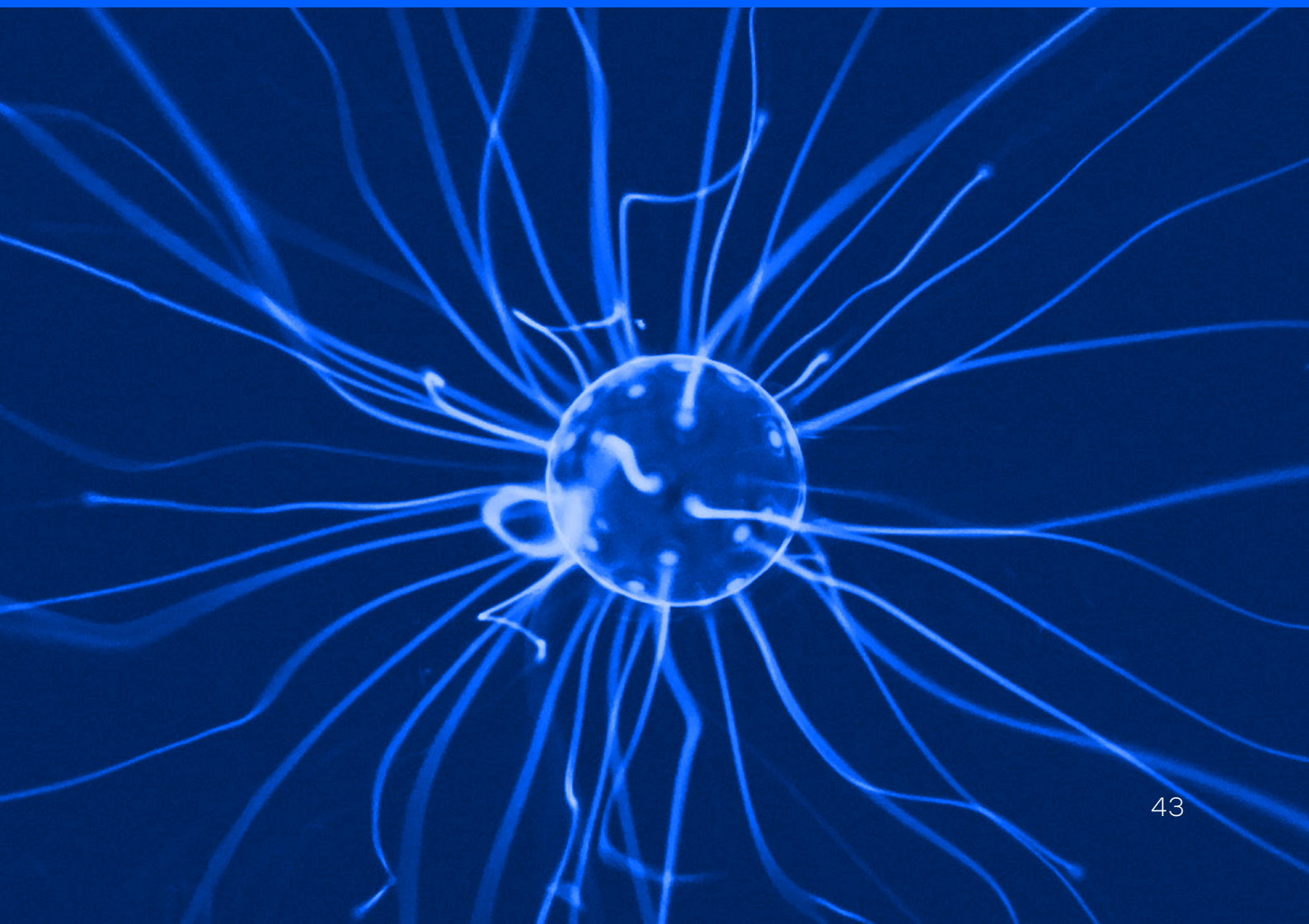
Kwantowa komunikacja

Jednym z największych zagrożeń dla naszego cyfrowego świata jest podatność komunikacji elektronicznej na zagrożenia i luki bezpieczeństwa. Hakerzy wymyślają sposoby na kradzież naszych tożsamości, środków finansowych i prywatnych danych. **Kryptografia** to gałąź wiedzy zajmująca się zabezpieczaniem informacji przed niepowołanym dostępem. Kryptografia pozwala nam na wymianę informacji na duże odległości, ale pozostaje nadal tajna przed niezamierzonymi podsłuchiwaczami. Większość nowoczesnych metod kryptograficznych opiera się na dobrze znanych problemach matematycznych takich jak **faktoryzacja**, które są trudne do rozwiązania przez klasyczne superkomputery. Możliwość pojawienia się w przyszłości komputerów kwantowych odpornych na błędy i szumy wymaga od nas ponownego przeanalizowania sposobu, w jaki zabezpieczamy nasze systemy informatyczne.

W ogólnym ujęciu komunikacja kwantowa polega na kodowaniu i przesyłaniu wiadomości wykorzystując różne konfiguracje cząstek subatomowych i ich parametry fizyczne. W pełnej konfiguracji komunikacji kwantowej przesyłamy kubity zamiast klasycznych bitów. Aktualnie w metodach komunikacji tego typu wykorzystuje się transmisję fotonów i ich zakodowanych stanów kwantowych. Takie podejście i sama koncepcja komunikacji kwantowej umożliwiają zupełnie nowe podejście do idei komunikacji oraz jest to sposób na przesyłanie kubitów pomiędzy infrastrukturą obliczeń kwantowych co umożliwia skalowanie takiej infrastruktury obliczeń. Realizacja koncepcji komunikacji kwantowej wymaga opracowania między innymi kluczowych metod efektywnego generowania par splątanych fotonów, ich dystrybucji na większe odległości co wymaga opracowania tzw. regeneratorów kwantowych. Kluczowym elementem takiego regeneratora jest tzw. pamięć kwantowa. Komunikacja kwantowa oferuje potencjalnie wiele nowych aplikacji, ale jednym z głównych i pierwszych proponowanych takich zastosowań jest wspomniana bezpieczna transmisja danych gdzie wykorzystując zasady badane przez mechanikę kwantową oferujemy integralność przesyłanego sygnału, danych i usług. Jedną z proponowanych takich metod jest tzw. kwantowa dystrybucja klucza.

Technologia QKD wykorzystywana jest do zabezpieczania informacji przesyłanej łączami sieci komputerowych na coraz większych odległościach. W ramach sieci naukowej PIONIER udało się zestawić i zabezpieczyć połączenie QKD na odcinku ponad 300 km pomiędzy Poznaniem i Warszawą w maju 2022 roku.

Kwantowa dystrybucja klucza QKD (ang. Quantum Key Distribution) jest nową formą kryptografii opartej na zasadach mechaniki kwantowej i utrzymuje nasze informacje całkowicie bezpieczne, nawet przed atakiem komputera kwantowego. Głównym zadaniem QKD jest stworzenie współdzielonego tajnego klucza pomiędzy dwoma stronami, który jest doskonale zabezpieczony. W najprostszej wersji jedna strona wysyła kubity w określonych stanach kwantowych do drugiej strony, która je obserwuje lub mierzy. Osoba próbująca podsłuchać musi również dokonać pomiary tych kubitów, co jak wiemy pozostawia wykrywalny ślad. Wynika to z zasad mechaniki kwantowej, która mówi, że nie można dokonać pomiaru stanu kwantowego bez jego zakłócenia. Jeśli kubity zostały zaburzone, obie strony wiedzą, że należy zrezygnować z wymiany i usunąć klucz. W przeciwnym razie strony mogą użyć klucza do wymiany bezpiecznej komunikacji. Warto zaznaczyć, iż już dziś rozwija się również dziedzina nauki zajmująca się algorytmami kryptograficznymi, które mają być odporne na złamanie za pomocą komputerów kwantowych – kryptografia postkwantowa. **Kryptografia postkwantowa** jest podejściem komplementarnym do QKD i skupia się na rozwijaniu nowych klasycznych metod kryptograficznych opartych na problemach matematycznych, które uważa się za trudne do rozwiązania nawet dla komputerów kwantowych. Na szczęście równolegle do rozwoju kwantowych komputerów, pojawiają się też kwantowe szyfry (np. szyfr Vernama) oraz protokoły kryptograficzne (np. BB-84), których odporność na różnego rodzaju ataki jest zagwarantowana przez kwantowe własności cząstek.



Recepta na masywne wolumeny danych

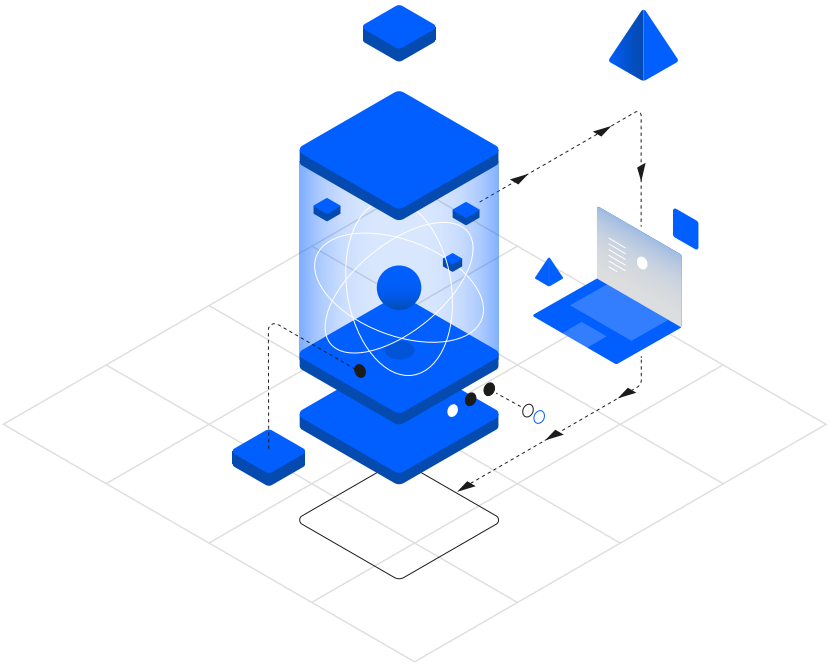
Algorytm Grovera

Omówiona na wstępie raportu analogia przeszukiwania księgozbioru jest przykładem wykorzystania jednego z najbardziej znanych algorytmów kwantowych, czyli algorytmu Grovera wymyślonego w 1996 przez Lova Grovera. Oryginalnie, algorytm Grovera został przedstawiony jako algorytm kwantowy znajdujący konkretny element z nieuporządkowanej bazy danych w czasie kwadratowo szybszym niż inne klasyczne algorytmy. Bazą danych może być dowolny zbiór elementów, np. wcześniej wspomniany księgozbiór, a jej nieuporządkowanie mówi nam tyle, że przykładowo, nie jest ona w żaden sposób posortowana, a więc nie możemy użyć żadnej strategii, która pozwalałaby nam na szybsze znalezienie elementu. Znalezienie konkretnego elementu oznacza, że potrafimy ten element rozpoznać i — jeśli go zobaczymy — jednoznacznie potwierdzić, że właśnie o ten element nam chodziło. Kwadratowe przyspieszenie oznacza tutaj, że przykładowo na rozwiązanie, zamiast 100 sekund będziemy czekać zaledwie 10 sekund, ale już dla większych zbiorów danych np. zamiast 1 000 000 sekund, już tylko 1000 sekund, itd.

Algorytm Grovera znajduje zastosowanie nie tylko w problemie przeszukiwania nieuporządkowanej bazy danych, ale również w każdym innym problemie, w którym potrafimy na podstawie każdego elementu stwierdzić, czy jest on elementem przez nas szukanym. Z tego powodu, do przykładów wykorzystania algorytmu Grovera możemy zaliczyć również wyszukiwanie średniej, mediany czy też wartości maksymalnej ze zbioru liczb. Algorytm ten może być też wykorzystany do szybszego znajdowania rozwiązania wielu obliczeniowo trudnych problemów takich jak np. znalezienie dopuszczalnego rozwiązania przyporządkowania poszczególnych składów pociągów do zaplanowanych połączeń kolejowych.

```
from qiskit.algorithms import Grover

grover = Grover()

result = grover.amplify(problem)
```

Symulacje kwantowe

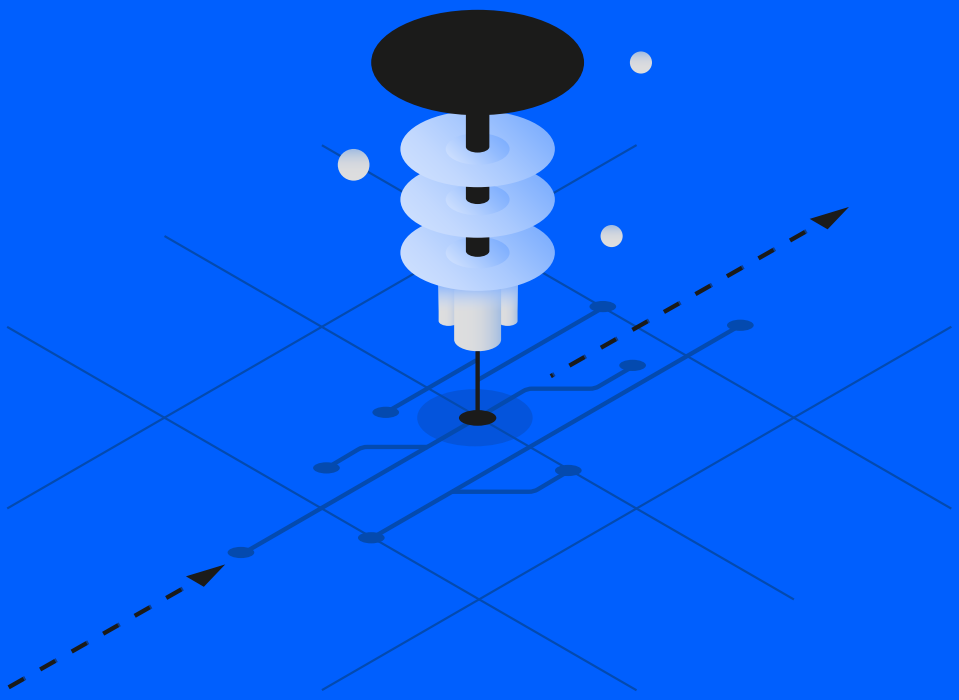


Modelowanie złożonych zjawisk i procesów znanych w chemii, biologii, farmacji czy biomedycynie, gdzie przy pewnej skali czasowo-przestrzennej należy uwzględniać już wpływ mechaniki kwantowej stanowi ogromne wyzwanie dla klasycznych superkomputerów. Przez wiele ostatnich dekad próbowano modelować różne zjawiska kwantowe z wykorzystaniem klasycznych superkomputerów i bardzo kosztowych obliczeniowo symulacji komputerowych. Już wspomniany Richard Feynman wykazał, że w praktyce musimy w klasycznych obliczeniach stosować szereg przybliżeń, uproszczeń oraz ograniczeń, które z kolei ograniczają nam dokładność obliczeń z jaką dany model odpowiada rzeczywistości.

Naturalnym rozwiązaniem tego problemu wydaje się być wykorzystanie kontrolowanego układu kwantowego, który po odpowiednim przygotowaniu jest w stanie odtworzyć wszystkie zjawiska występujące w rzeczywistym badanym układzie bez użycia przybliżeń. Idea ta od początków informatyki kwantowej stanowi najbardziej obiecujący obszar, w którym nowy paradygmat obliczeń może zyskać przewagę nad klasycznym i wnieść przy tym nieoceniony wkład do nauki i przemysłu. Wyniki uzyskane w laboratorium mogą być weryfikowane i uzupełniane przy użyciu symulacji komputerowych, które dostarczają z kolei informacji prowadzących do kolejnych odkryć.

Zasadniczym ograniczeniem powszechnie stosowanych klasycznych modeli jest konieczność stosowania pewnych przybliżeń i uproszczeń, które pozwalają utrzymać się w granicach klasycznej mocy obliczeniowej superkomputera. W przypadku komputerów kwantowych, przynajmniej w teorii, są one w stanie modelować rzeczywiste zjawiska kwantowe bez korzystania z jakichkolwiek przybliżeń i uproszczeń.

1.3

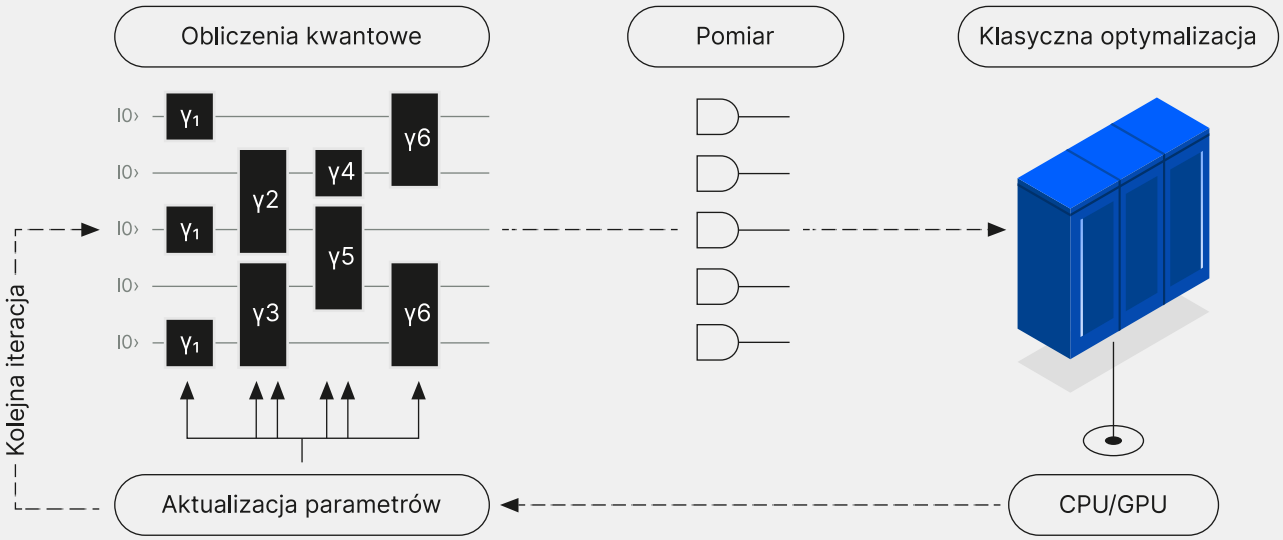


Czy to jest realne?

Pierwsze komputery kwantowe

Jesteśmy na początku drogi rozwoju komputerów kwantowych i ich zastosowań. Pierwsze teoretyczne modele komputera kwantowego zaczęły powstawać dopiero w latach osiemdziesiątych ubiegłego stulecia.

Na bazie tych prac powstały znane algorytmy kwantowe, takie jak algorytm Shora czy algorytm Grovera, które musiały jednak jeszcze wiele lat poczekać na swoją fizyczną realizację. Dopiero w 1998 roku udało się skonstruować pierwszy 2-kubitowy komputer kwantowy, który potrafił utrzymać swój stan na zaledwie kilka nanosekund [4]. Komputer ten oparty był o technologię magnetycznego rezonansu jądrowego, a jego zakres dostępnych operacji był mocno ograniczony. Rok później ukazały się pierwsze projekty komputerów wykorzystujących kwantowe wyżarzanie. Dopiero w 2003 roku po raz pierwszy udało się zaprezentować rzeczywiste działanie bramki CNOT, która jest kluczową operacją potrzebną do splątania kubitów. W 2007 roku świat obiegła informacja o zbudowaniu komputera 28-kubitowego w architekturze kwantowego wyżarzania, a w 2009 roku naukowcom udało się stworzyć pierwszy uniwersalny 2-kubitowy komputer kwantowy. Uniwersalność komputera kwantowego polega na tym, że — tak samo jak komputer klasyczny — jest on w stanie wykonać dowolne obliczenia. Każda operacja na tym komputerze miała średnio 10% szansy na to, że się nie powiedzie. W 2011 roku firma D-Wave jako pierwsza udostępniła komercyjny dostęp do komputera kwantowego specjalizującego się w rozwiązywaniu problemów kombinatorycznych, a w 2016 roku firma IBM udostępniła zdalny dostęp do 5-kubitowej maszyny kwantowej.

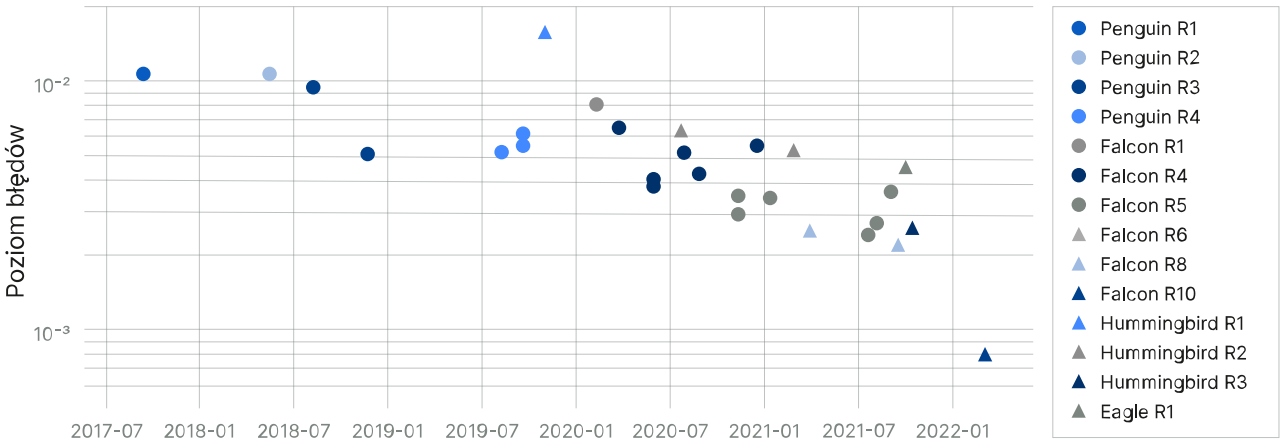


Obecnie jesteśmy świadkami ery **NISQ** (ang. **Noisy Intermediate-Scale Quantum**), czyli ery komputerów kwantowych o stosunkowo **małej liczbie kubitów**, które ze względu na swoje niedoskonałości nie są w stanie z dużą dokładnością przetwarzać skomplikowanych obwodów. Pierwszą niedoskonałością są wszelkiego rodzaju **błędy i szumy**, np. wynikające z niedokładności operacji na kubitach, niedokładności podczas ich pomiarów i odczytów, niechcianej interakcji między kubitami oraz **krótkim czasem utrzymania koherencji stanu kwantowego**. Dodatkowo, w praktyce występują rzadkie połączenie kubitów między sobą, co sprawia, że splątanie między dwoma kubitami często bywa problematyczne, zwłaszcza jeśli są one fizycznie daleko od siebie. Trzeba wtedy wykonywać skomplikowaną operację zamiany kubitów tak, aby znalazły się blisko siebie — dopiero wtedy możliwe jest ich splątanie i wykorzystanie do kwantowych obliczeń.

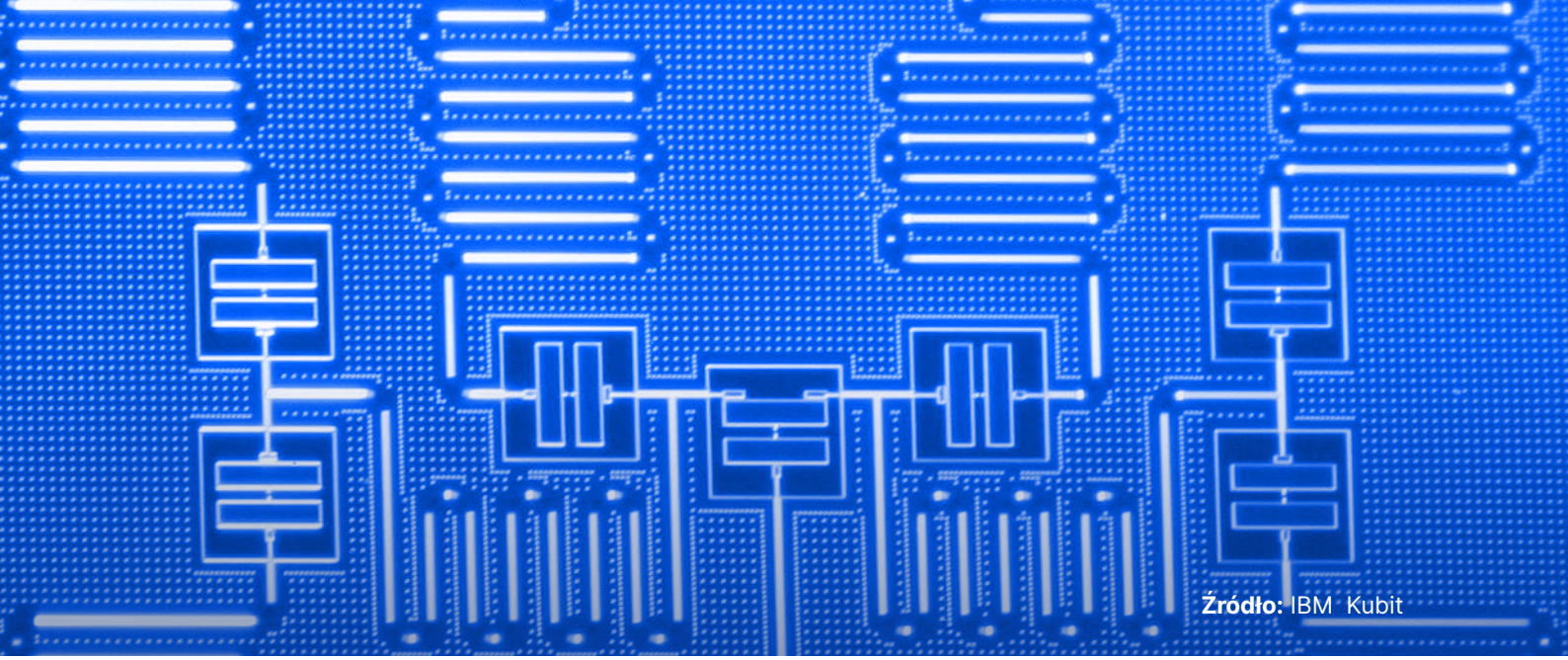
To wszystko sprawie, że obecnie konieczne jest projektowanie i korzystanie z **algorytmów hybrydowych**. W algorytmach kwantowych część obliczeń jest wykonywana przez komputer kwantowy, podczas gdy pozostałe obliczenia przeprowadza komputer klasyczny. Wśród algorytmów hybrydowych często mamy do czynienia z przetwarzaniem opartym o pętlę zwrotną, w której wynik części kwantowej zależy od specjalnych parametrów dostosowywanych i optymalizowanych przez komputer klasyczny. Optymalizowanie tych parametrów często jest same w sobie trudnym problemem, więc preferowane jest wykorzystywanie w tym celu superkomputerów i technologii HPC (ang. High Performance Computing).

Wspomniane ograniczenia związane z niedoskonałościami powodują, że dostępne komputery kwantowe nie nadają się jeszcze do powszechnego rozwiązywania problemów dużej skali. Istnieje jednak silna potrzeba użytkowa oraz potrzeba eksperymentowania z dostępnymi obecnie komputerami kwantowymi. Porównując jakość komputerów kwantowych na przestrzeni ostatnich 5 lat, możemy zauważyć znaczący postęp i rozwój. Przykładowo, między latami 2017 i 2022 firmie IBM udało się trzydziestokrotnie polepszyć jakość splątania kubitów. W 2017 roku jedna na 100 operacji splątania kończyła się niepowodzeniem, a obecnie jest to zaledwie jedna na 3000.

Najlepsza stopa błędu splątania bramki kwantowej w IBM Q



Źródło: https://quantum-enablement.org/hardware/historical.html



Źródło: IBM Kubit

Błędy w obliczeniach kwantowych

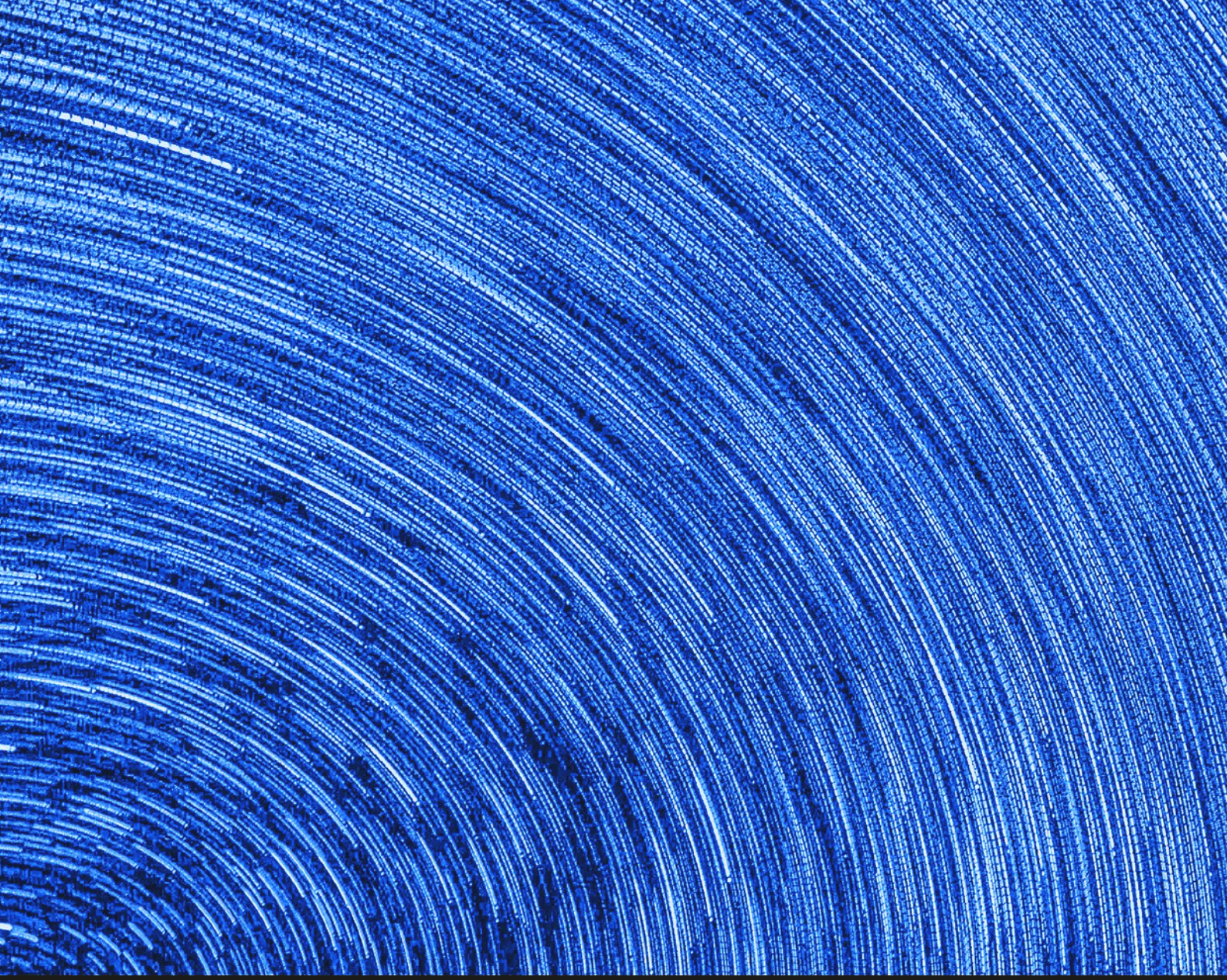
Ze względu, że kubity przyjmują dowolną wartość pomiędzy 0 a 1, wykorzystanie ich do obliczeń przywodzi na myśl ideę komputerów analogowych, które nie znalazły szerszego zastosowania właśnie z powodu dużej wrażliwości na błędy. Warto jednak zwrócić uwagę na zasadniczą różnicę między tymi podejściami. Dowiedziono, że obliczenia kwantowe mogą zostać uodpornione na działanie błędów i niedokładności, jeżeli współczynnik błędów nie przekracza pewnego stałego progu. Oznacza to, że wówczas możliwe jest w teorii poprawianie błędów szybciej, niż się one pojawiają. Idea ta jest kluczowa z perspektywy dalszego i długofalowego rozwoju komputerów kwantowych.

W ogólności metody kwantowej korekcji błędów opierają się na kodowaniu stanu jednego logicznego kubitu za pomocą splątanego stanu wielu fizycznych kubitów. Pozwala to w efekcie na wykonanie pomiarów umożliwiających wykrycie rodzaju błędu, bez wpływania na stan logicznego kubitu. Najlepsze znane metody wymagają jednak bardzo dużej liczby nadmiarowych kubitów, co uniemożliwia ich praktyczne wykorzystanie w dostępnych aktualnie komputerach kwantowych składających się z relatywnie małej liczby kubitów. Nie oznacza to jednak, że poziom błędów nie może zostać znacząco ograniczony w inny sposób. Zwiększenie dokładności obliczeń na maszynach kwantowych obarczonych różnymi błędami jest bardzo ciekawym zagadnieniem mitygacji błędów. Zarówno od strony badawczej, jak i wdrożeniowej, wiele zespołów badawczych na całym świecie, w tym w Polsce, opracowuje nowe rozwiązania, które mogą znaleźć praktyczne zastosowania. Aktualnie dostępne metody **mitygacji błędów**, w połączeniu z dalszym postępem w zakresie jakości bramek kwantowych, mogą w niedalekiej przyszłości doprowadzić do stopniowego poprawiania się możliwych do uzyskania wyników, bez konieczności czekania na wdrożenie kosztownej **korekcji błędów**.

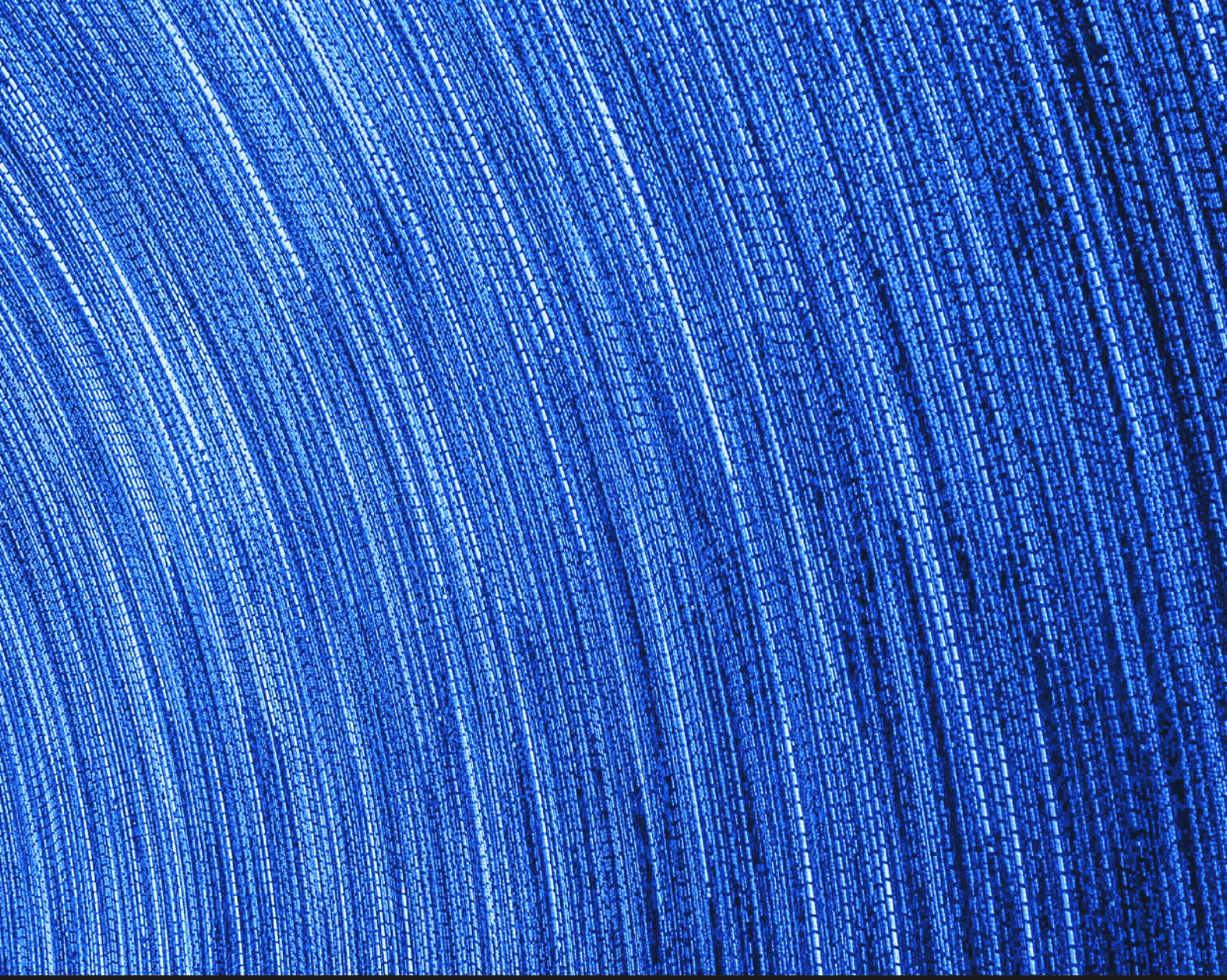
Obecne możliwości i architektury

TECHNOLOGIA	PRODUCENT	ZALETY	WADY
NADPRZEWODZĄCE KUBITY	IBM, Rigetti, Google, IQM	**Uniwersalny model obliczeń, duża stabilność większej liczby kubitów, sprawdzone komponenty**	Praca w ekstremalnie niskiej temperaturze, Ograniczone możliwości połączeń
PUŁAPKI JONOWE	Quantinuum, AQT, IonQ	**Uniwersalny model obliczeń, praca w temperaturze pokojowej, możliwość gęstego połączenia kubitów**	Mała stabilność większej liczby kubitów
NEUTRALNE ATOMY	Pasqal, QuEra, Atom Computing, ColdQuanta	**Uniwersalny model obliczeń, praca w temperaturze pokojowej**	Mała stabilność większej liczby kubitów
KWANTOWE WYŻARZANIE	D-Wave, NEC	**Duża liczba kubitów, możliwość gęstego połączenia kubitów**	Praca w ekstremalnie niskiej temperaturze, Brak uniwersalności
FOTONICZNE KUBITY	Xanadu, Quandella, Quix, ORCA, Computing	**Praca w temperaturze pokojowej, łatwość w skalowaniu architektury dla dużej liczby modów**	Mała liczba kubitów, Brak uniwersalności

Tab. 1. Zestawienie wybranych architektur komputerów kwantowych

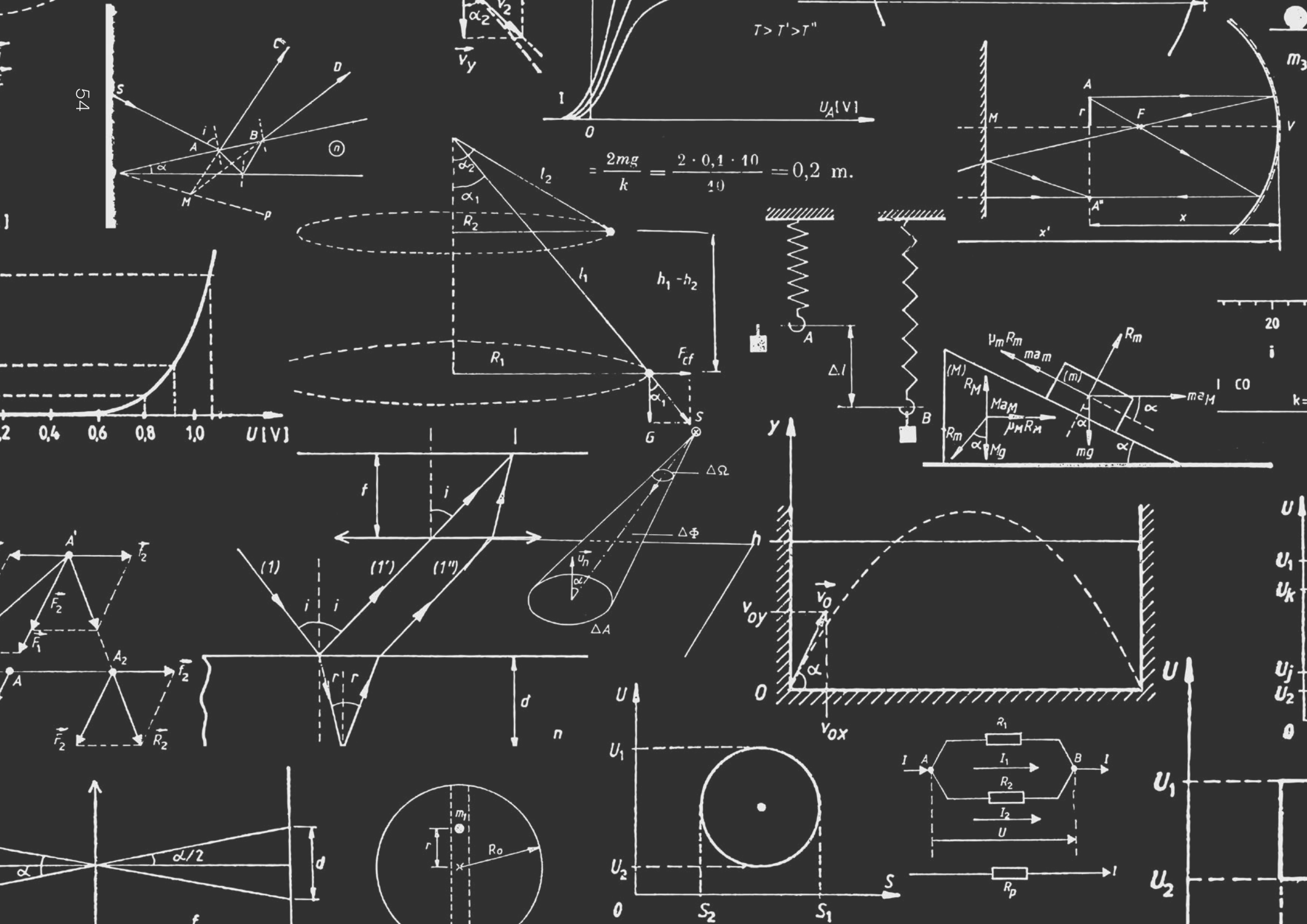


Polski węzeł obliczeń kwantowych



ROZDZIAŁ

02

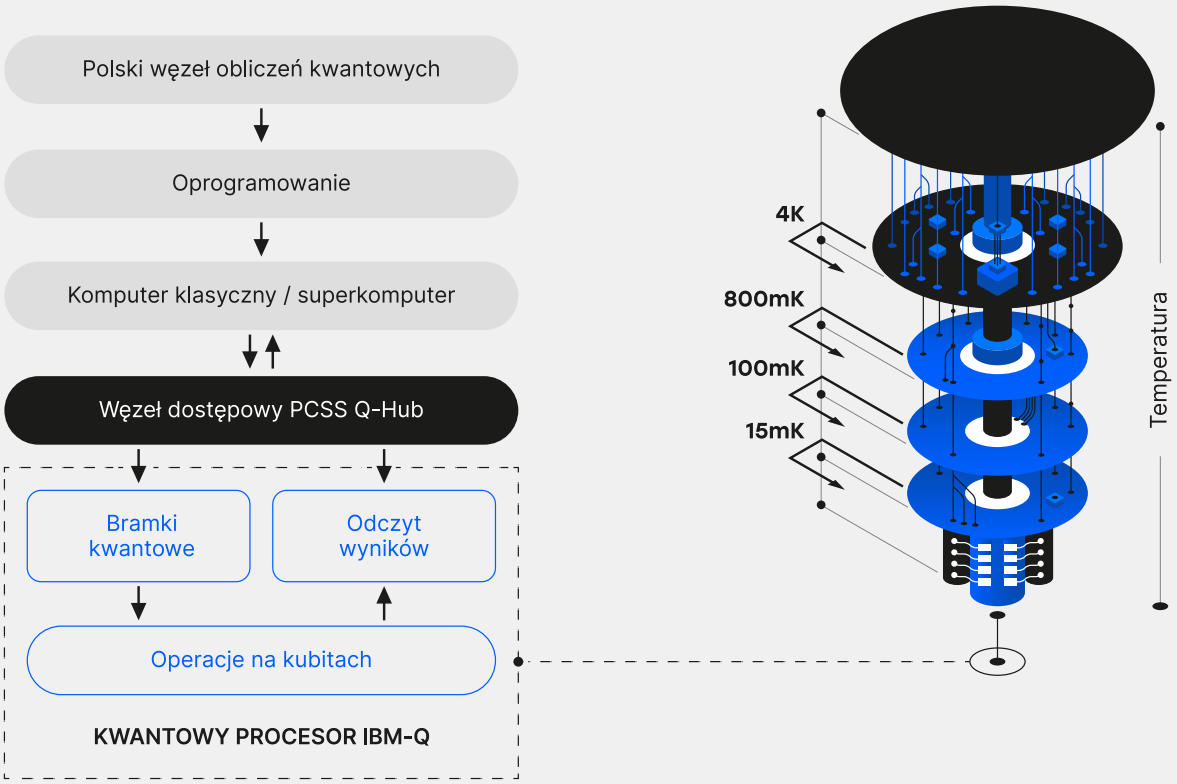

$T > T' > T''$
$U_A[V]$
$\frac{2mg}{k} = \frac{2 \cdot 0{,}1 \cdot 10}{10} = 0{,}2$ m.
$h_1 - h_2$
F_{cf}
Δl
$\mu_m R_m$
ma_m
R_m
ma_M
$\mu_M R_M$
Mg
mg
$\Delta\Omega$
$\Delta\Phi$
ΔA
v_{oy}
v_{ox}
v_o
U_1
U_2
R_p
S_1
S_2
m_1
R_o
$\alpha/2$
0,2 0,4 0,6 0,8 1,0 U[V]

Sieć IBM Quantum Network

Sieć IBM Quantum Network ma na celu optymalne wykorzystanie potencjału komputerów kwantowych i zastosowania ich do rozwiązania eksperymentalnych problemów. Krajowe instytucje zrzeszone w ramach tej sieci mają dostęp do najbardziej zaawansowanych i najnowocześniejszych systemów kwantowych IBM Q. Ekosystem ten jest systematycznie rozwijany przez firmę IBM od wielu lat. Użytkownicy z Polski mają dostęp do 127-kubitowego komputera kwantowego IBM Eagle. W listopadzie 2022 roku zaprezentowany został komputer kwantowy IBM Q z procesorem klasy Osprey, w którym dostępne będzie 433 kubitów. To kolejny etap w drodze do stworzenia ponad 1000-kubitowego programowalnego komputera kwantowego.

W ramach inicjatywy polskiego węzła obliczeń kwantowych uruchomiony został dostęp do sieci fizycznych komputerów kwantowych IBM Q

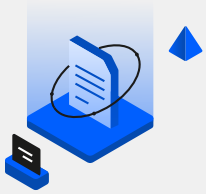
https://quantum.psnc.pl



Kroki milowe w roku 2022

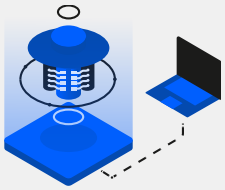
2021.12.01

Rozpoczęcie prac przygotowawczych.



2022.02.04

Podpisanie umowy IBM Q System Hub Access and Software/Technology License Agreement.



2022.02.28

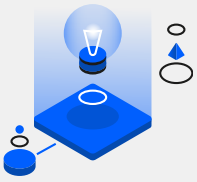
Kwantowa platforma i kwantowy węzeł (QuantumHub PL) ze zdalnym, współdzielonym dostępem do zasobów komputera kwantowego IBM.

2022.04.30

Wyniki pierwszych eksperymentów użytkowników.

2022.06.30

Rozbudowa bibliotek programistycznych i narzędzi cyfrowych dla obliczeń kwantowych.



2022.11.30

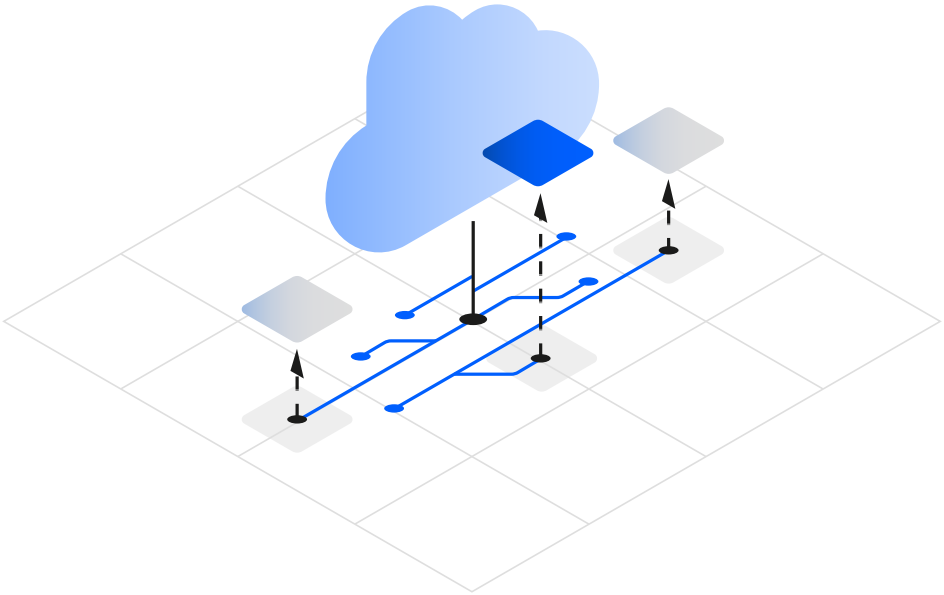
Raport roczny oraz podsumowanie pierwszej fazy działalności polskiego węzła obliczeń kwantowych.

Kwantowe centrum innowacji IBM Quantum w Polsce

Minister Cyfryzacji na podstawie Decyzji Nr DRI.ZPI.7220.10.2021 z dnia 30 grudnia 2021 Prezesa Rady Ministrów powierzył Instytutowi Chemii Bioorganicznej PAN Poznańskiemu Centrum Superkomputerowo-Sieciowemu realizację projektu "Wsparcie podmiotów realizujących zadania publiczne w sferze innowacji cyfrowych na rzecz nauki i społeczeństwa informacyjnego, poprzez zapewnienie dostępu do e-infrastruktury wykorzystującej obliczenia kwantowe, w tym dostęp do węzła IBM Q-HUB". W efekcie realizacji powierzonego zadania powołano w Poznańskim Centrum Superkomputerowo-Sieciowym pierwszy w Europie Centralnej – Polski Węzeł Obliczeń Kwantowych w ramach globalnej sieci IBM Quantum Network.

Kwantowe centra innowacji i węzły obliczeń kwantowych działające w ramach IBM Quantum Network na całym świecie to wysokiej klasy społeczność globalna, skupiająca firmy z listy Fortune 500, start-upy, instytucje akademickie i laboratoria badawcze, które pracują nad rozwojem obliczeń kwantowych i badają ich praktyczne obszary zastosowań. Członkowie sieci IBM Quantum Network wraz z zespołami IBM Quantum wspólnie badają, testują i analizują, w jaki sposób obliczenia kwantowe mogą wpłynąć na rozwój społeczeństwa informacyjnego, nauki i gospodarki.

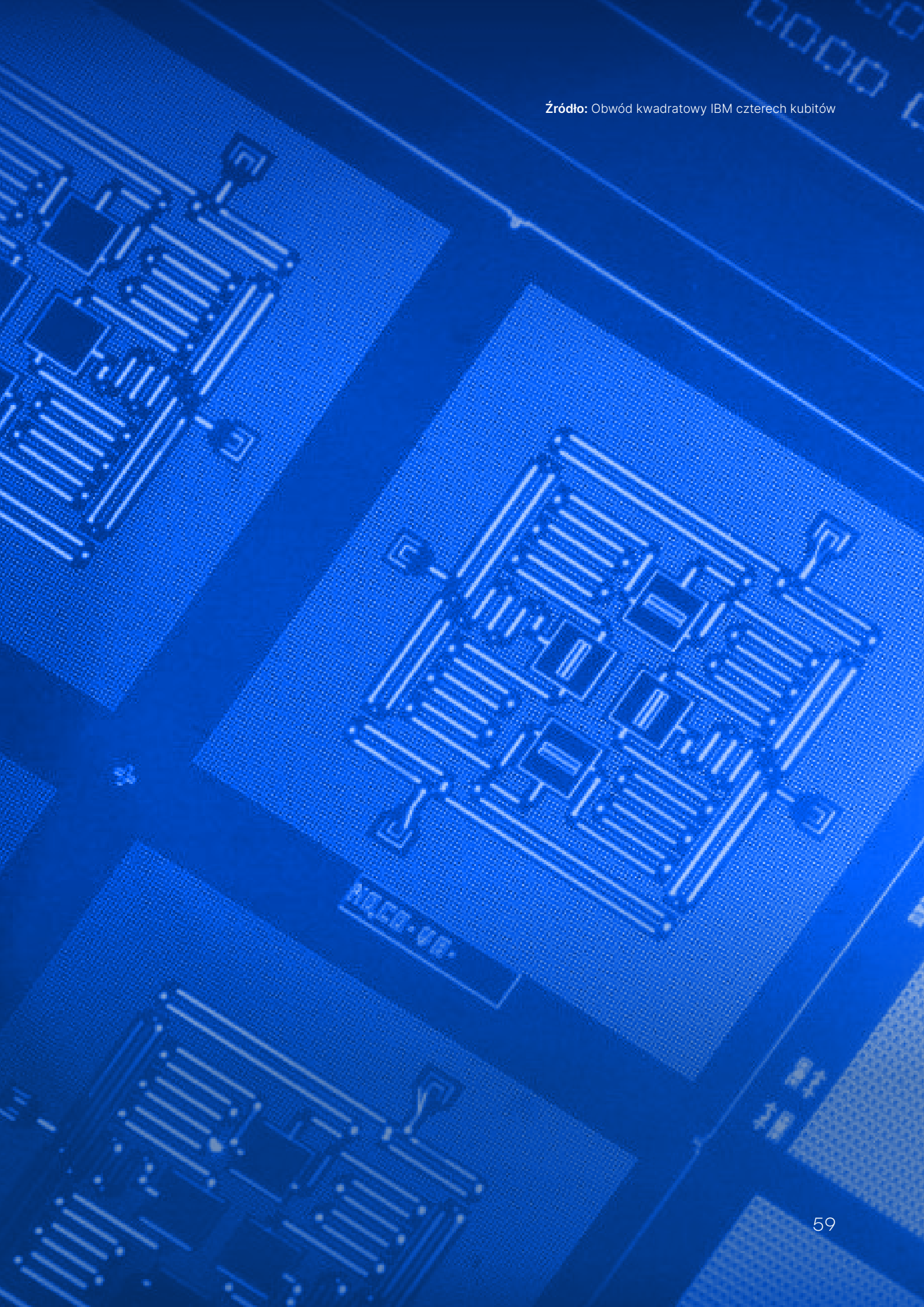
Polski Węzeł Obliczeń Kwantowych zapewnia wsparcie i zdalny dostęp dla krajowych użytkowników naukowych do różnych architektur komputerów kwantowych IBM Quantum. Podsumowanie eksperymentalnych obliczeń kwantowych użytkowników szczegółowo zostało omówione w Rozdziale 3.



Dzięki rozbudowanym zasobom superkomputerowym ośrodek udostępnia również klasyczne zasoby superkomputerowe, które umożliwiają użytkownikom uruchomienie symulacji działania komputerów kwantowych, ale dla relatywnie małej i ograniczonej liczby kubitów. Koordynator Polskiego Węzła Obliczeń Kwantowych, Poznańskie Centrum Superkomputerowo-Sieciowe ICHB PAN dysponuje odpowiednio wykwalifikowaną kadrą ekspercką z wieloletnim doświadczeniem w zakresie rozwoju, budowy i wdrażania rozwiązań infrastrukturalno-usługowych dla wysokowydajnych obliczeń na rzecz nauki i społeczeństwa informacyjnego. Realizując od ponad dwóch dekad projekty B+R z obszaru technologii informacyjno-komunikacyjnych, w tym nauk obliczeniowych o wysokiej wydajności (technologie HPC) z wykorzystaniem potencjału superkomputerów, ośrodek posiada również odpowiednie zaplecze organizacyjno-techniczne do wsparcia rozwoju nowej generacji hybrydowych algorytmów kwantowych wykorzystujących jednocześnie potencjał oraz moc obliczeniową klasycznych i kwantowych komputerów.

Misją Polskiego Węzła Obliczeń Kwantowych jest również rozwijanie i rozpowszechnianie wiedzy na temat aktualnego stanu zaawansowania komputerów kwantowych wśród partnerów, do których należą ośrodki badawcze, uniwersytety oraz w najbliższej przyszłości przedsiębiorstwa zainteresowane wykorzystaniem technologii kwantowych w różnych przełomowych zastosowaniach. Podnoszenie umiejętności użytkowników zainteresowanych technologiami kwantowymi, w tym prowadzenie warsztatów, konferencji, szkoleń i kursów, to kolejny istotny obszar działalności Polskiego Węzła Obliczeń Kwantowych.

Zapewnienie dostępu oraz stosownego wsparcia wielu zespołom eksperckim i użytkownikom w Polsce w ramach Polskiego Węzła Obliczeń Kwantowych już na obecnym etapie pozwala rozpocząć projektowanie i testy różnych algorytmów kwantowych oraz rozpocząć już dziś rozwój oprogramowania wykorzystującego nowy paradygmat obliczeń kwantowych.



Źródło: Obwód kwadratowy IBM czterech kubitów

Dostępne bramkowe komputery kwantowe

W ramach Polskiego Węzła Obliczeń Kwantowych użytkownicy mają dostęp do różnych programowalnych bramkowych komputerów kwantowych firmy IBM. Od momentu uruchomienia inicjatywy, w okresie kilku miesięcy dostępnych jest dziewięć różnych komputerów kwantowych, w tym **127-kubitowy procesor IBM Eagle** w systemie IBM Washington oraz systemy 27-kubitowe w architekturze Falcon, w tym 3 systemy o najwyższym wskaźniku Quantum Volume równym 128: IBM Kolkata, IBM Montreal oraz IBM Mumbai. W ramach Polskiego Węzła Obliczeń Kwantowych planowany jest dla użytkowników w najbliższych tygodniach dostęp do największego **433-kubitowego procesora IBM Osprey**, którego szczegóły sprzętowo-programowe opublikowano na początku listopada 2022 roku [5].

ibm_washington	Exploratory
System status	Online
Processor type	Eagle r1
Qubits	127
QV	64
CLOPS	850

ibmq_kolkata	
System status	Online
Processor type	Falcon r5.11
Qubits	27
QV	128
CLOPS	2K

ibmq_montreal	
System status	Online
Processor type	Falcon r4
Qubits	27
QV	128
CLOPS	2K

ibmq_mumbai	
System status	Online
Processor type	Falcon r5.10
Qubits	27
QV	128
CLOPS	1.8K

ibm_cairo	
System status	Online
Processor type	Falcon r5.11
Qubits	27
QV	64
CLOPS	2.4K

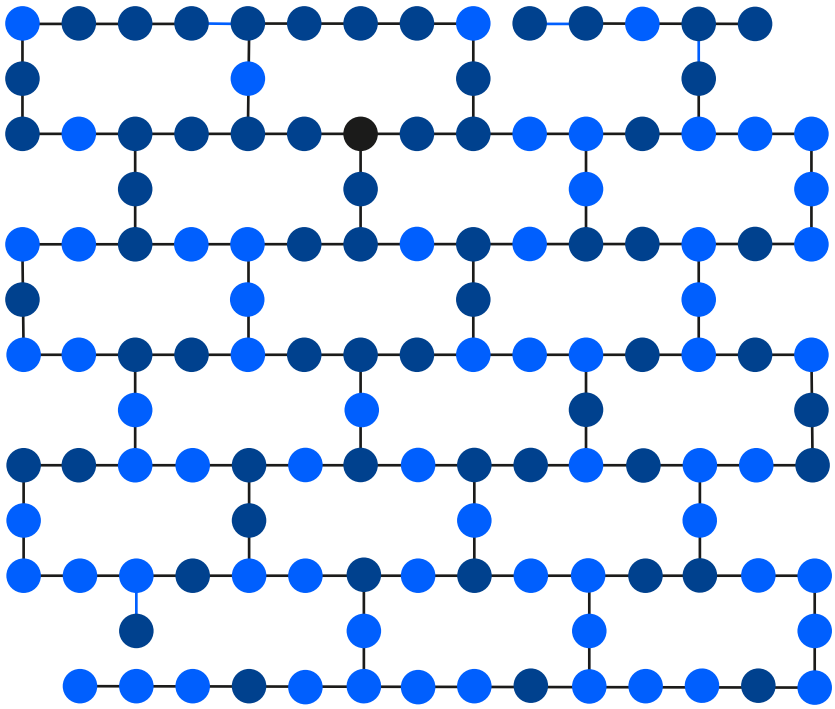
ibm_auckland	Exploratory
System status	Online
Processor type	Falcon r5.11
Qubits	27
QV	64
CLOPS	2.4K

ibm_hanoi	
System status	Online - Queue paused maintenance
Processor type	Falcon r5.11
Qubits	27
QV	64
CLOPS	2.3K

ibm_geneva	Exploratory
System status	Online - Queue paused maintenance
Processor type	Falcon r8
Qubits	27
QV	32
CLOPS	1.9K

ibmq_toronto	
System status	Online
Processor type	Falcon r4
Qubits	27
QV	32
CLOPS	1.8K

```
from qiskit import IBMQ

IBMQ.load_account()

provider = IBMQ.get_provider('ibm-q-psnc','internal','default')

backend = provider.get_backend('ibm_washington')
```



Rys. 1 Topologia połączeń pomiędzy kubitami 127-kubitowego procesora IBM Eagle w komputerze kwantowym IBM Q

Topologia połączeń kubitów w architekturach procesorów Eagle oraz Falcon opiera się na heksagonalnej strukturze heavy-hex, w której nie wszystkie kubity są ze sobą połączone. Taka metoda połączeń wymaga transpilacji logicznej obwodów, jednak znacznie redukuje szumy na bramkach kwantowych i umożliwia uzyskanie dokładniejszych odczytów.

Pełne wsparcie dla użytkowników

Od momentu powołania Polskiego Węzła Obliczeń Kwantowych oferowane jest użytkownikom wsparcie techniczne oraz merytoryczne w zakresie przeprowadzanych eksperymentów na zdalnej infrastrukturze komputerów kwantowych IBM Quantum. Powołany krajowy zespół wsparcia wraz z zespołami firmy IBM tworzącymi pakiety **otwartego oprogramowania narzędziowego Qiskit** jest w stanie w skuteczny sposób pomóc użytkownikom w zarówno projektowaniu, implementacji i testowym uruchomieniu algorytmów kwantowych. Pełne wsparcie dla użytkowników oferowane jest również na etapie eksperymentów obliczeniowych na różnych komputerach kwantowych IBM Quantum wraz z niezbędną pomocą na etapie weryfikacji i analizy uzyskanych wyników.

W pierwszych kilku miesiącach funkcjonowania Polskiego Węzła Obliczeń Kwantowych wykonano ponad 1,6 miliarda obwodów kwantowych na różnych komputerach kwantowych IBM Quantum.

W ramach Polskiego Węzła Obliczeń Kwantowych dostępnych jest też szereg narzędzi administracyjnych pozwalających na monitorowanie stanu wykorzystania przez użytkowników zasobów komputerów kwantowych, w tym monitorowana jest liczba uruchomień obwodów na komputerach kwantowych IBM Quantum, średni czas oczekiwania zadań obliczeniowych i czas wykorzystania komputerów kwantowych IBM Quantum.

W ramach Polskiego Węzła Obliczeń Kwantowych użytkownicy mają również możliwość rezerwacji na wyłączność komputerów kwantowych: IBM Kolkata oraz IBM Toronto. Taka rezerwacja zasobów umożliwia użytkownikom przeprowadzenie znacznie bardziej zaawansowanych i bardziej obciążających eksperymentów obliczeń kwantowych, bez konieczności oczekiwania zadań obliczeniowych w kolejce komputera kwantowego. Ponadto, użytkownicy mają również zapewniony stały dostęp do symulatorów komputerów kwantowych uruchomionych na klasycznej architekturze superkomputera, dzięki czemu możliwa jest weryfikacja wyników ich eksperymentów zarówno przy użyciu idealnych, jak i zaszumionych symulacji obliczeń kwantowych.

Przykładowe statystyki wykorzystania zasobów IBM Quantum przez krajowych użytkowników w okresie luty - listopad 2022

Name
ibm-q-psnc

Poznan Supercomputer and Networking Center

Total executions
2,149,386,591

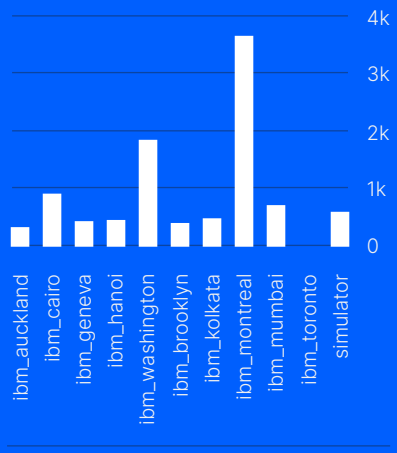
Łączna liczba uruchomień obwodów na komputerach kwantowych IBM Quantum przez użytkowników

System time
8d 14h 24m 43.3s

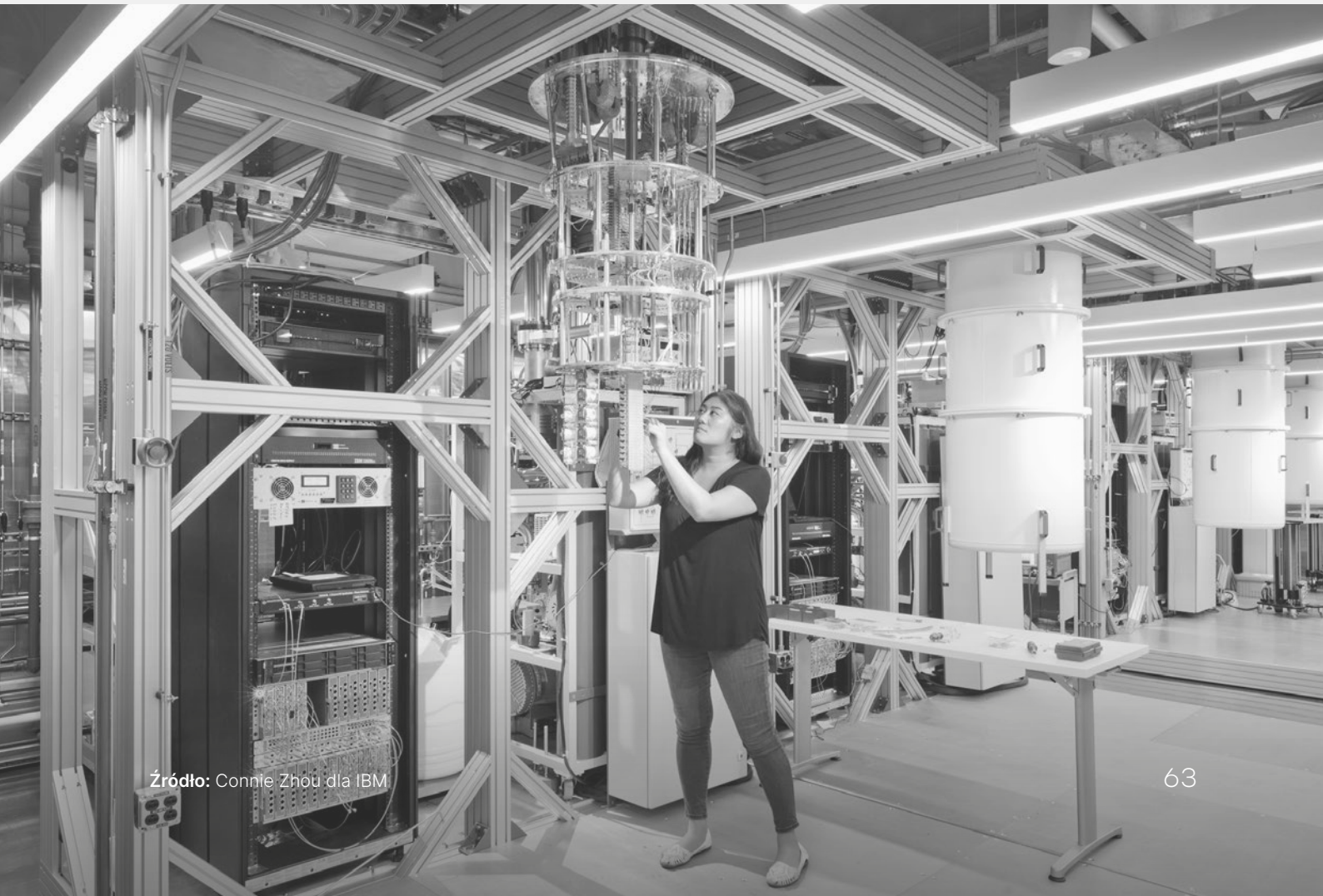
Total completed jobs
17,087

Average queue wait
4h 7m 54s

Łączny czas wykorzystywania zasobów komputerów kwantowych IBM Quantum, liczba zakończonych zadań i średni czas oczekiwania

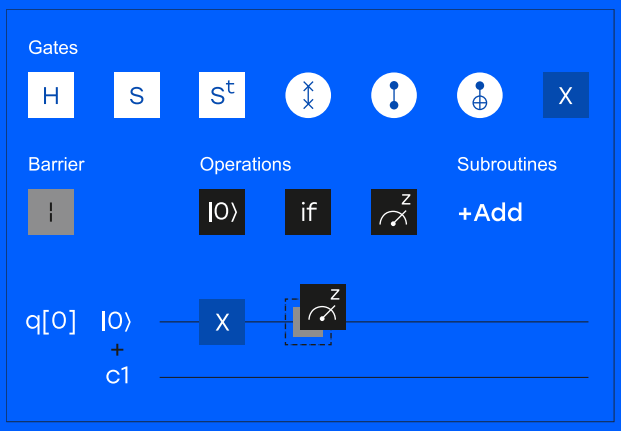


Rozkład wykorzystywania różnych generacji komputerów kwantowych IBM Quantum



Źródło: Connie Zhou dla IBM

Programowanie
„przeciągnij i upuść”



Programowanie wysokopoziomowe
w języku Python i Jupyter Notebook

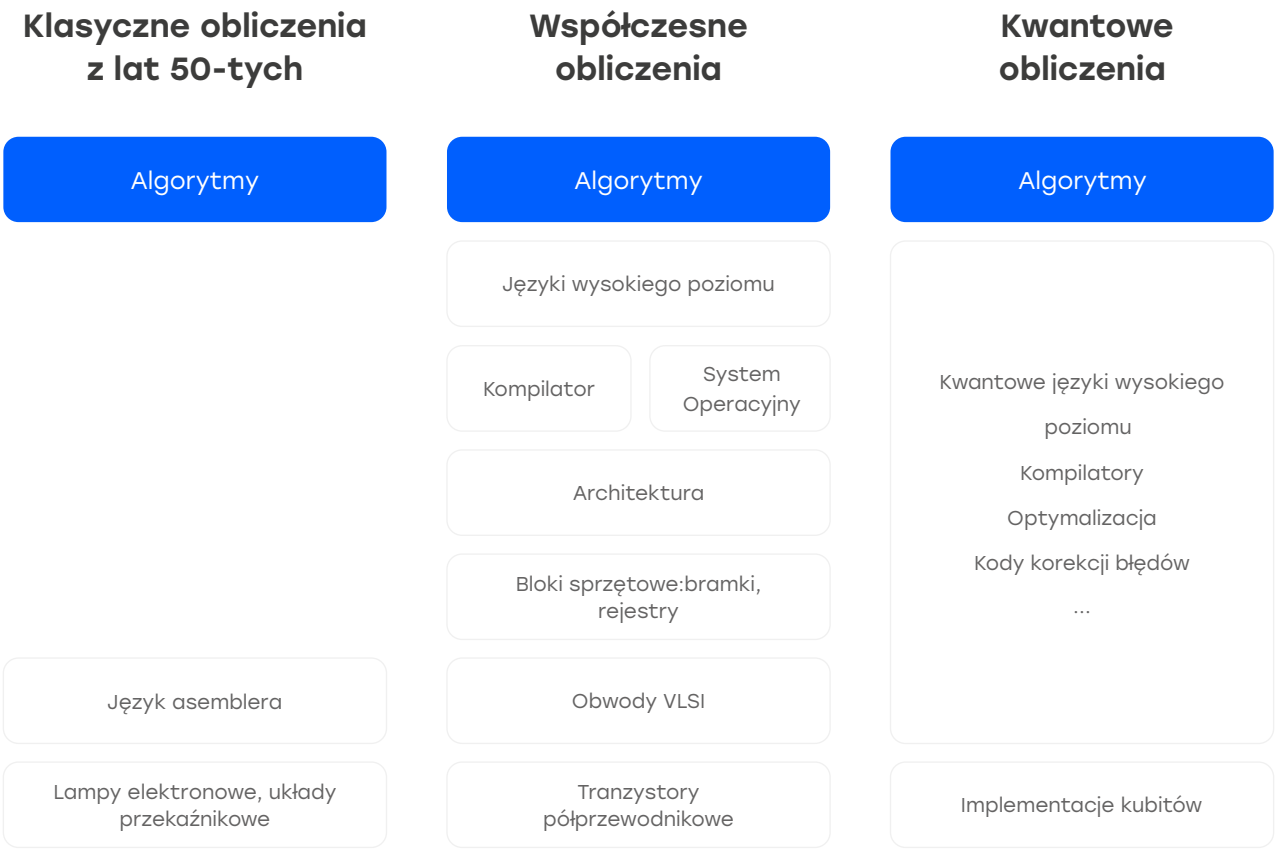
```
qc = QuantumCircuit( 2, 2)

gc.h(0)
qc.cx(0, 1)
qc.measure([ 0, 1], [0, 1])

backend = Aer.get_backend(' qasm_simulator ')
job_sim = execute(qc, backend)
sim_result = job_sim.result()

sim_result.get_counts(qc)
```

Programowanie komputerów kwantowych

Od strony technicznej i procesu wytwarzania oprogramowania, użytkownik zainteresowany obliczeniami kwantowymi musi w pierwszej kolejności skupić się na odpowiednim zaprojektowaniu obwodów za pomocą podstawowych bramek kwantowych. Przypomina to dobrze znany proces z programowania elektroniki, w którym układy projektuje się łącząc ze sobą bramki logiczne w coraz to bardziej zaawansowane funkcjonalnie układy cyfrowe. Aktualnie istnieje wiele różnych narzędzi i bibliotek programistycznych wspierających użytkownika w rozwoju oprogramowania. Najbardziej zaawansowanym, a jednocześnie bardzo intuicyjnym i przyjaznym narzędziem jest graficzny interfejs użytkownika udostępniany w powiązaniu z bezpośrednim dostępem do różnych zasobów komputerów kwantowych IBM Quantum. Graficzny interfejs użytkownika wspiera również tryb “przeciągnij i upuść”, pozwalając w szczególności mało doświadczonym użytkownikom nie tylko szybko skonstruować dowolny obwód kwantowy, ale także sprawdzić jak poszczególne bramki kwantowe wpływają na cały proces zmieniania stanów kubitów podczas przeprowadzanych obliczeń kwantowych.

W ogólności kod algorytmu kwantowego może być zapisany przez użytkownika w wysokopoziomowym języku programowania Python, który w formie skryptu lub popularnego interaktywnego środowiska Jupyter Notebook może być uruchamiany z poziomu dowolnej przeglądarki internetowej użytkownika.

Dostępne narzędzia pozwalają na korzystanie z wysokopoziomowego języka do programowania komputerów kwantowych, jednak wciąż konieczna jest ścisła kontrola nad wykonywanymi obwodami kwantowymi. Wynika to przede wszystkim z szumów i błędów z jakimi mierzymy się w przypadku dostępnych komputerów kwantowych w erze NISQ. W celu uzyskania lepszych wyników obliczeń kwantowych, przed uruchomieniem każdego obwodu użytkownik nadal powinien sprawdzić szczegółowe charakterystyki kubitów dostępnych w danym komputerze kwantowym, w szczególności uwzględnić parametry techniczne kubitów oraz sposób połączenia pomiędzy kubitami. Aktualnie opracowywane są rozwiązania sprzętowo-programowe, które mają ułatwić użytkownikom komputerów kwantowych odpowiedni dobór konkretnego komputera kwantowego oraz sposobu przeniesienia zadanego problemu na topologię urządzenia kwantowego. Jest to przykład kolejnej programowalnej warstwy abstrakcyjnej w stosie oprogramowania komputera kwantowego, która pozwoli użytkownikom i programistom skupić się na samym projektowaniu algorytmów kwantowych i badaniu ich zastosowań.



Perspektywy w ramach kwantowego hubu

01.

Zwiększanie wydajności obliczeń kwantowych oraz pozyskiwanie nowych użytkowników i instytucji

02.

Praktyczne wsparcie rozwoju kompetencji i edukacja

03.

Eksperymenty obliczeniowe złożonych algorytmów kwantowych w różnych zastosowaniach

Pierwszy rok działalności Polskiego Węzła Obliczeń Kwantowych był dedykowany na opracowanie eksperymentów testowych oraz wsparcie pierwszych użytkowników. W tym celu uruchomiono portal dostępowy do kwantowej platformy i kwantowego węzła ze zdalnym, współdzielonym dostępem do różnych zasobów komputera kwantowego IBM Quantum wspierający procesy projektowania, uruchamiania i monitorowania obliczeń kwantowych. Dodatkowo, opracowano i wdrożono wirtualne środowisko badawczo-eksperymentalne i edukacyjne dla użytkowników zainteresowanych rozwojem swoich kompetencji w zakresie technologii kwantowych z wykorzystaniem klasycznych zasobów superkomputerowych ułatwiające testy i rozwój podstawowych algorytmów kwantowych. We współpracy z użytkownikami powstały również dodatkowe narzędzia pozwalające na wykonywanie zaawansowanych obliczeń kwantowych z wykorzystaniem metod QAOA [13] i VQE [16], czyli specjalistycznych algorytmów przeznaczonych do rozwiązywania problemów kombinatorycznych i symulowania układów fizycznych.

Ważną aktywnością Polskiego Węzła Obliczeń Kwantowych było opracowanie materiałów edukacyjnych oraz szkolenia dla pracowników naukowych, studentów i użytkowników Centrów Komputerów Dużej Mocy. Zorganizowano wsparcie w ramach międzynarodowego w ramach międzynarodowych warsztatów Workshop on Quantum Computing and Communication w ramach konferencji PPAM 2022 14th International Conference on Parallel Processing and Applied Mathematics. Przeprowadzono również cykl seminariów oraz spotkań z użytkownikami poświęconych zagadnieniom obliczeń kwantowych oraz ograniczeń i możliwości wykorzystania aktualnie dostępnych komputerów kwantowych.

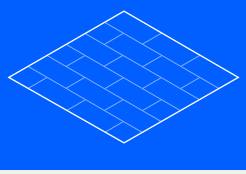
Droga do kwantowego rozwoju

Etap, na którym znajdujemy się obecnie, jest dopiero początkiem rozwoju informatyki kwantowej. Dynamiczne tempo rozwoju komputerów kwantowych pozwala wierzyć, że ich praktyczne zastosowanie będzie możliwe w najbliższych latach. Plan rozwoju technologii kwantowych przedstawiona przez firmę IBM zakłada sukcesywne zwiększanie jakości i liczby kubitów, wytwarzanych w technologii nadprzewodzących kubitów, do kilku tysięcy już w roku 2025. Następnie zakłada się udostępnianie komputerów kwantowych z coraz mniejszym poziomem błędów i szumów, składających się z tysięcy, a nawet milionów kubitów. Plany rozwoju komputerów kwantowych w kolejnych latach w oparciu również o inne technologie kwantowe, w tym pułapki jonowe, fotoniczne kubity czy neutralne atomy są również obiecujące. Zdefiniowana przez IBM metryka wydajności komputerów kwantowych - Quantum Volume, uwzględniająca liczbę kubitów w procesorach kwantowych, a także ich jakość i dokładność pozwala na zdefiniowanie nowej zależności na wzrost możliwości komputerów kwan-

W celu dalszej poprawy wydajności i utrzymania tempa skalowania komputerów kwantowych wszystko wskazuje na to, że w już w roku 2023 konieczne będzie łączenie procesorów kwantowych w większe procesory przy pomocy łączy komunikacji kwantowej. Umożliwi to wykorzystanie znacznie większej liczby kubitów, ale wymagać będzie zrównoleglania obliczeń kwantowych.

2021

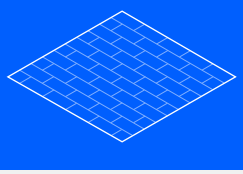
Eagle
127 kubitów



100x szybsze uruchamianie programów przy użyciu usługi Qiskit Runtime

2022

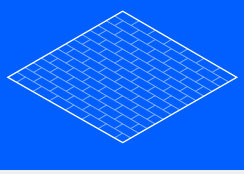
Osprey
433 kubity



Większe możliwości obliczeń przy wykorzystaniu dynamicznych obwodów kwantowych

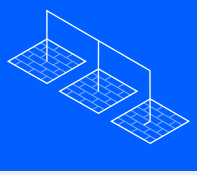
2023

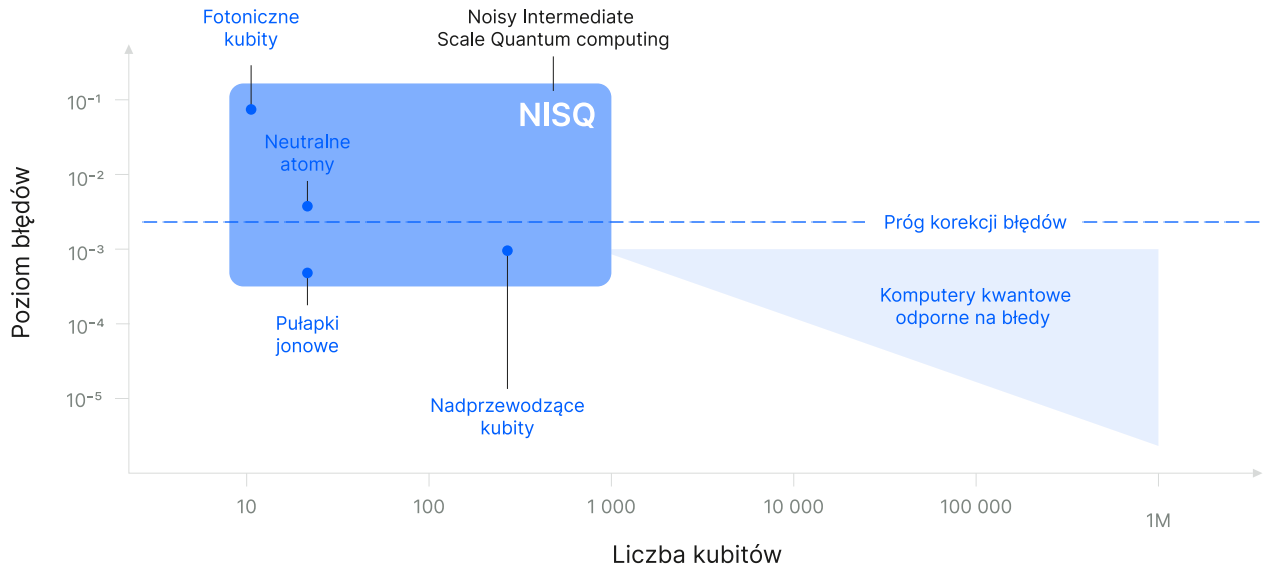
Condor
1,121 kubitów



Poszerzenie możliwości aplikacji o elastyczne obliczenia i zrównoleglenie usługi Qiskit Runtime

Heron
133 kubity x p





towych w czasie [6]. Warto podkreślić, iż wydajność komputerów kwantowych mierzona parametrem Quantum Volume przyrasta dwukrotnie w okresie niecałego 1 roku. Tym samym, koniec ery gdzie dominowało prawo Moore'a, jest swojego rodzaju początkiem ery NISQ i kolejnych etapów rozwoju technologii klasyczno-kwantowych wykorzystywanych do obliczeń i symulacji. Na przełomie kilku miesięcy działalności Polskiego Węzła Obliczeń Kwantowych udało się znacząco poprawić jakość i zwiększyć możliwości obsługi większej liczby użytkowników. Dzięki wprowadzeniu nowych abstrakcyjnych obiektów Qiskit Primitives możliwe jest bardziej wydajne wykonywanie algorytmów kwantowych. W roku 2022 udało się znacząco poprawić jakość i zwiększyć możliwości obsługi większej liczby krajowych użytkowników.

2024		2025	Po roku 2026
Crossbill 408 kubitów	**Flamingo** 1,386+ kubitów	**Kookaburra** 4,158+ kubitów	**Skalowanie w granicach 10k-100K kubitów za pomocą klasycznej i kwantowej komunikacji**
Zwiększenie dokładności Qiskit Runtime za pomocą skalowanej mitygacji błędów		Skalowanie aplikacji dzięki narzędziu przeplatającemu obwody kwantowe	Zwiększenie dokładności oraz prędkości obliczeń kwantowych za sprawą wdrożenia korekcji błędów

Kluczowe kompetencje i zagadnienia

Ważne jest wsparcie środowiska akademickiego na różnych poziomach edukacji i badań w nauce oraz gospodarce. W tym celu opracowano dodatkowe narzędzia wsparcia oraz treści edukacyjne dla krajowych użytkowników zgodne z opracowywaną ramą kwalifikacji "Programowanie komputerów kwantowych" w Zintegrowanym Systemie Kwalifikacji i obejmujące zagadnienia:

- **PODSTAWY ALGEBRY LINIOWEJ**
  - Wykonuje podstawowe obliczenia na wektorach i macierzach
  - Wykonuje obliczenia na liczbach zespolonych
  - Wykonuje obliczenia stosując notację Diraca
- **PODSTAWY TEORETYCZNE DZIAŁANIA KOMPUTERÓW KWANTOWYCH**
  - Posługuje się podstawową wiedzą z zakresu mechaniki kwantowej
  - Omawia pojęcia z zakresu informatyki kwantowej
- **WYKORZYSTANIE RZECZYWISTYCH KOMPUTERÓW KWANTOWYCH I SYMULATORÓW**
  - Korzysta z graficznego interfejsu służącego do konstruowania algorytmów kwantowych
  - Wykorzystuje komputery kwantowe przy użyciu oprogramowania narzędziowego Qiskit
  - Stosuje wybrane typy symulatorów
  - Omawia parametry komputerów kwantowych i minimalizuje wpływ błędów na obliczenia
  - Optymalizuje programy kwantowe, uwzględniając architekturę rzeczywistych procesorów kwantowych
  - Optymalizuje programy kwantowe, uwzględniając architekturę rzeczywistych procesorów kwantowych
- **WYKORZYSTANIE ISTNIEJĄCYCH ALGORYTMÓW Z UWZGLĘDNIENIEM ICH ZŁOŻONOŚCI OBLICZENIOWEJ**
  - Charakteryzuje elementy teorii złożoności obliczeniowej
  - Wykorzystuje algorytmy kwantowe
  - Ograniczenia i możliwości QPU, szumy, zakłócenia, błędy i korekcja błędów
  - Integracja hybrydowych systemów superkomputerowych i akceleratorów kwantowych

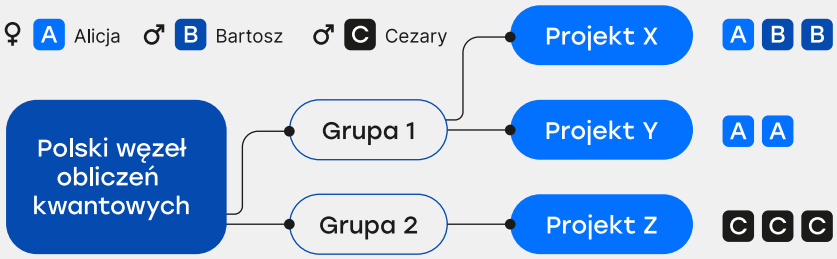
Źródło: Naukowiec Antonio Córcoles z IBM Quantum Composer

Administracja i zarządzanie obliczeniami kwantowymi

Rdzeniem dynamicznej struktury administracji i zarządzania obliczeniami kwantowymi jest Poznańskie Centrum Superkomputerowo-Sieciowe ICHB PAN, które oddelegowuje stosowne uprawnienia dla polskich instytucji naukowych i ich użytkowników dostępu do komputera kwantowego.

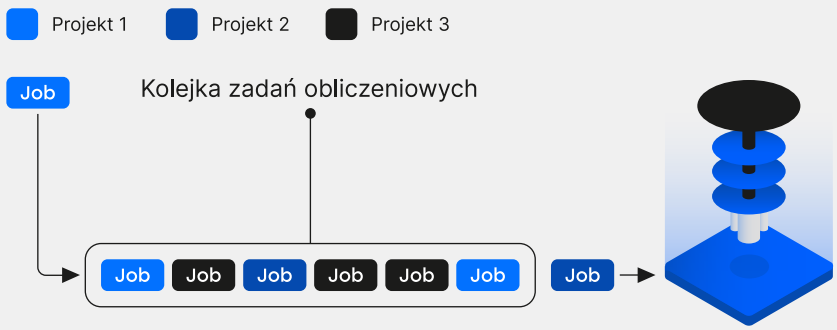
Kwantowe zadania obliczeniowe

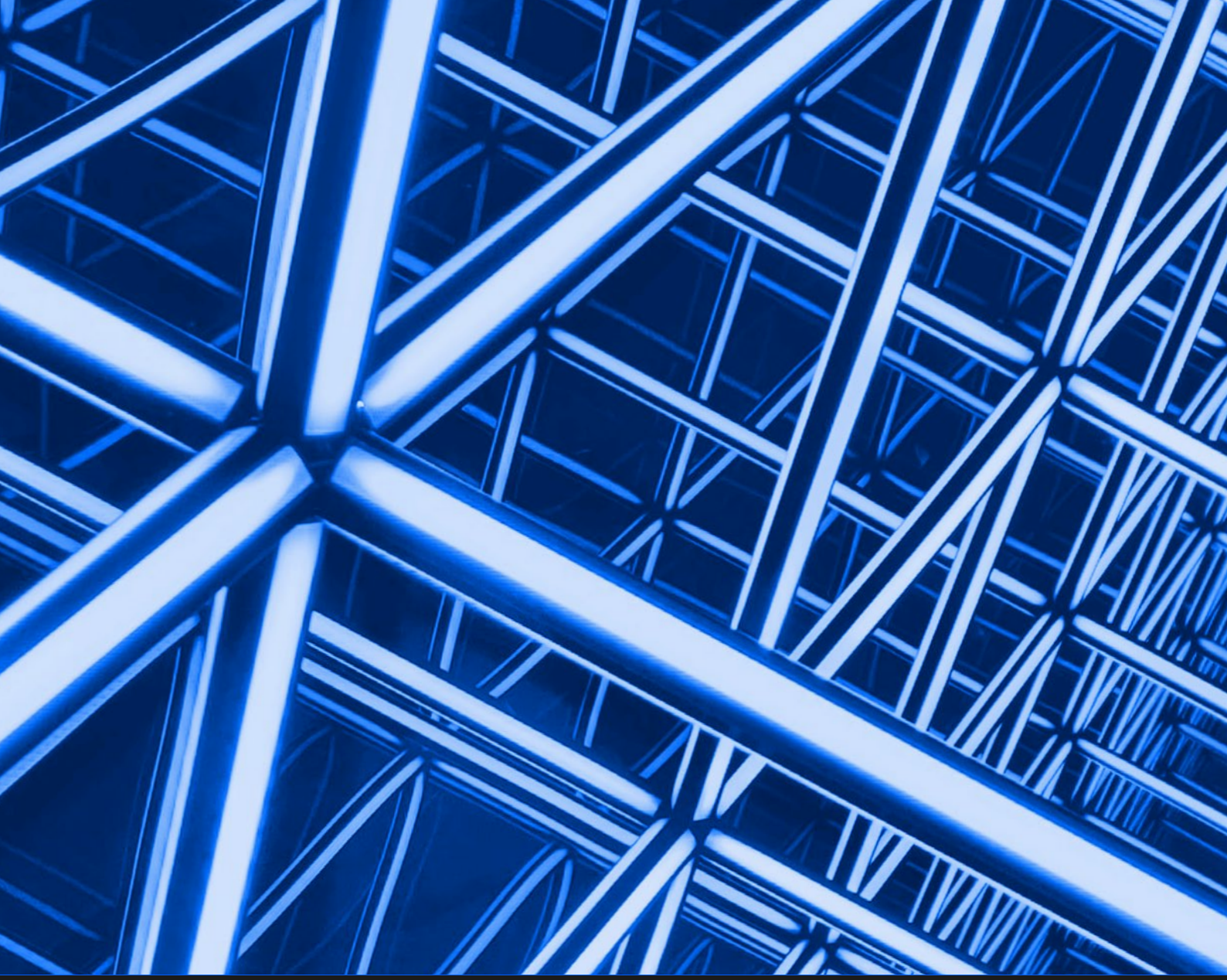
Do polskiego węzła obliczeń kwantowych przypisywane są grupy oraz projekty. Użytkownicy pracujący w ramach projektu mogą zlecać zadania obliczeniowe korzystając z alokacji przydzielonej konkretnej kombinacji grupy i projektu.



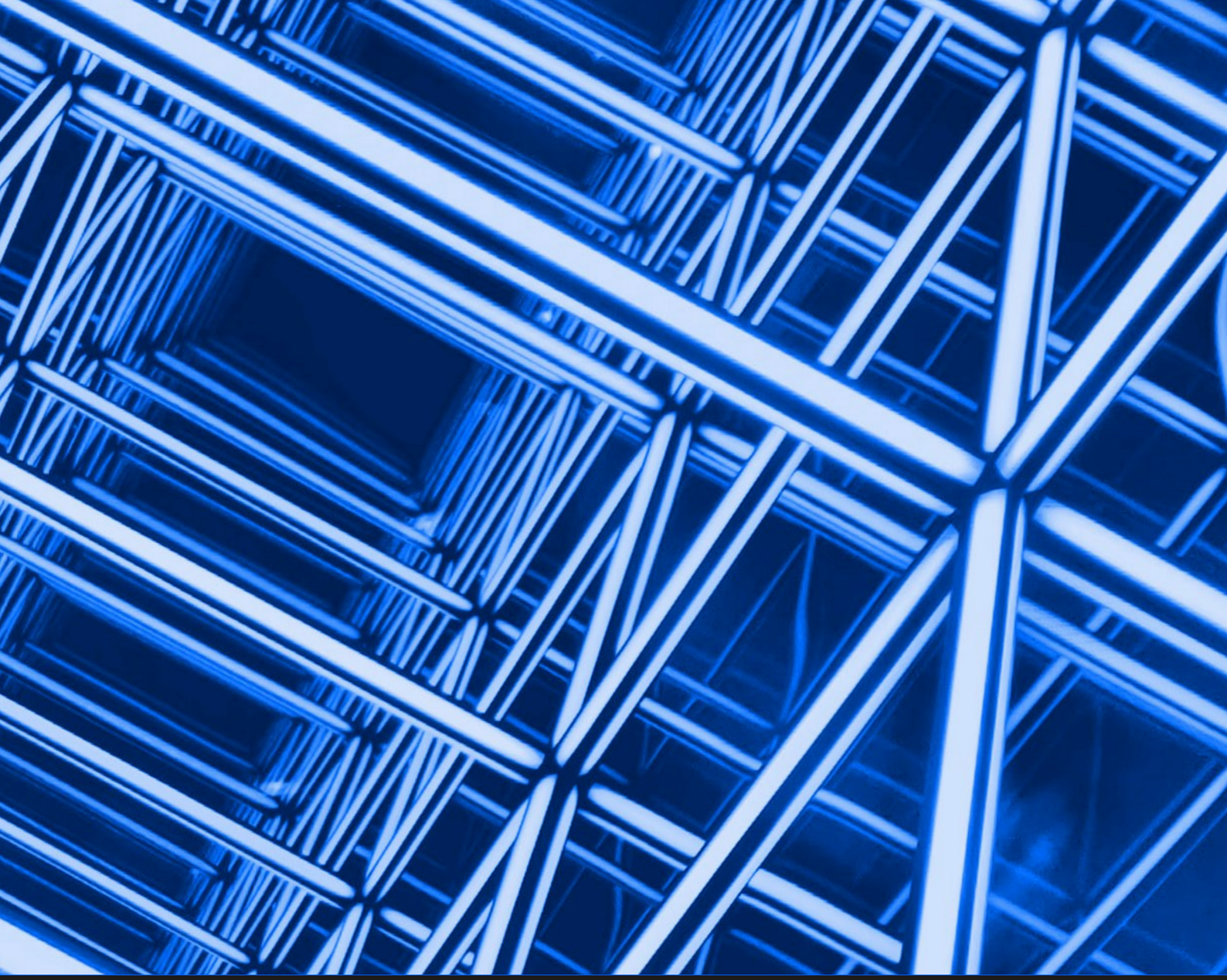
System kolejkowy

Obsługa i szeregowanie zadań do wykonania na komputerze kwantowym opiera się na dynamicznym systemie kolejkowym zapewniającym sprawiedliwy podział zasobów między różne grupy, projekty i ich użytkowników.



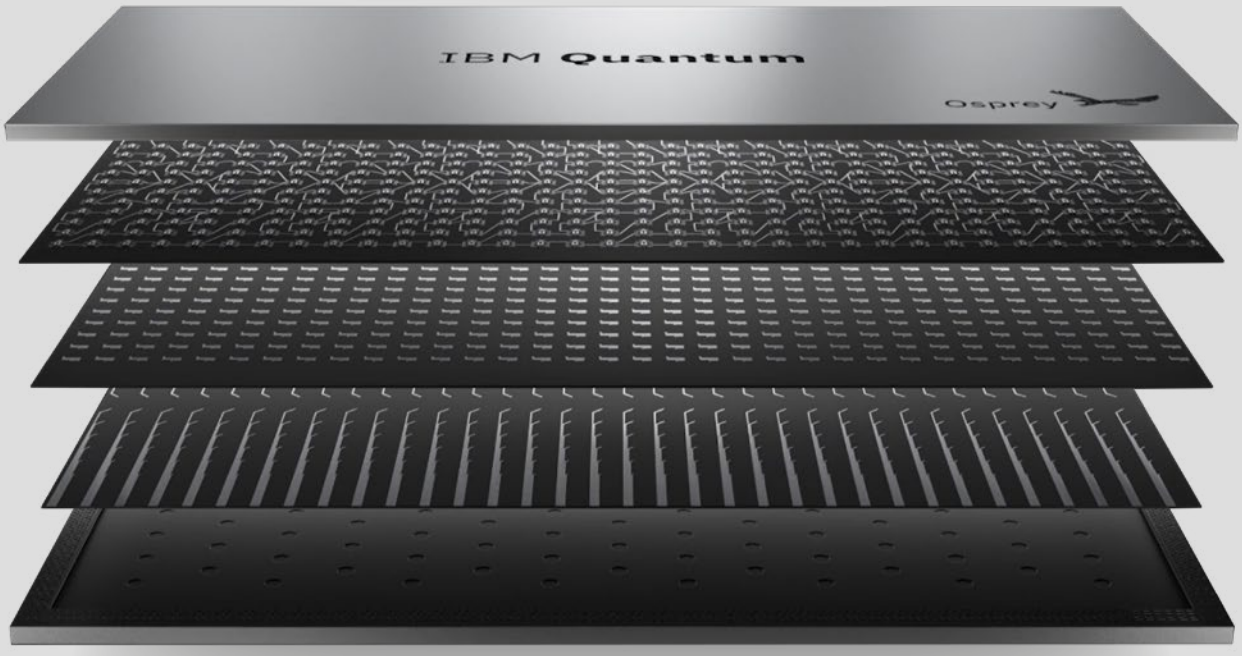


Zastosowania

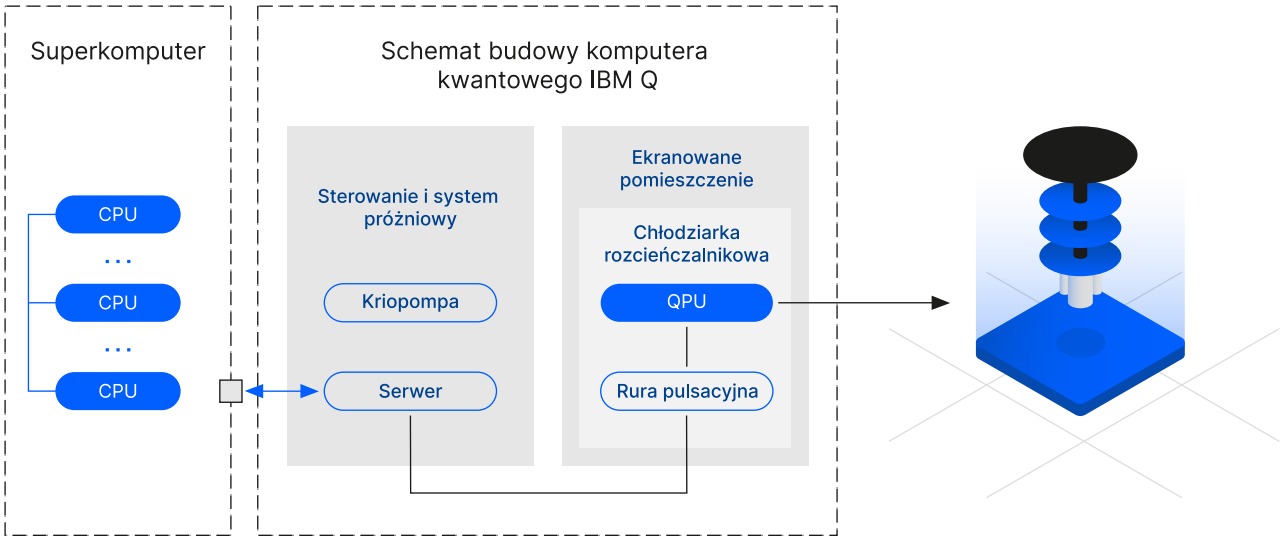


ROZDZIAŁ

03



Źródło: IBM Quantum Osprey Processor



Polski Węzeł Obliczeń Kwantowych nie tylko pośredniczy w dostępie do komputerów kwantowych IBM Quantum, ale także aktywnie nawiązuje współpracę z ekspertami oraz naukowcami z wielu ośrodków i przedsiębiorstw. Głównym zadaniem jest wsparcie różnych aktywności nad wykorzystaniem obliczeń kwantowych do rozwiązywania trudnych problemów z wielu różnych dziedzin nauki i przemysłu. Kwantowe metody obliczeniowe badane są zarówno pod kątem teoretycznym, jak i w kontekście możliwości uruchomienia ich na dostępnych zasobach. Dużo uwagi poświęcane jest również metodom mającym rozwiązać problemy samych komputerów kwantowych, a co za tym idzie przybliżyć moment, w którym osiągnięcie kwantowej przewagi stanie się możliwe. W kolejnych sekcjach podsumowane zostaną obszary zastosowań, które analizowane były w pierwszym okresie działalności Polskiego Węzła Obliczeń Kwantowych we współpracy z licznymi partnerami i eksperymentalnymi użytkownikami.

Eksperymentalne obliczenia kwantowe krajowych użytkowników

Aby przygotować się na nadchodzącą drugą rewolucję kwantową oraz zidentyfikować potencjalne obszary zastosowań komputerów kwantowych potrzebna jest strategiczna wizja budowy ekosystemu kwantowego w Polsce poprzez ścisłe i cykliczne interakcje pomiędzy czterema podstawowymi komponentami:

- badania i rozwój w zakresie możliwości oraz ograniczeń obliczeń kwantowych wykorzystywanych do budowy algorytmów kwantowych, aplikacji i usług wykorzystujących hybrydową klasyczno-kwantową moc obliczeniową;
- ramy kwalifikacyjne i kompetencje kluczowe z obszaru technologii kwantowych na poziomie studiów wyższych, studiów doktoranckich i kursów podyplomowych;
- aktywną współpracę z przedstawicielami rożnych branż i sektorów gospodarczych, w tym innowacyjnych polskich podmiotów i start-upów;
- zagwarantowanie infrastruktury dostępu do komputerów kwantowych i obliczeń w oparciu o różne technologie kwantowe.

Polski Węzeł Obliczeń Kwantowych w roku 2022 podjął szereg działań wpisujących się w powyższe strategiczne założenia, w szczególności w pierwszej kolejności zabezpieczył i zapewnił użytkownikom dostęp do komputerów kwantowych. Bardzo ważnym zadaniem było również nawiązywanie bliższej oraz bezpośredniej współpracy z użytkownikami. Kluczowa była również wymiana doświadczeń z wieloma krajowymi ośrodkami naukowo-badawczymi. Tym samym, w pierwszej kolejności wsparte zostały działania wcześniej już podejmowane przez wiele polskich zespołów eksperckich w zakresie modelowania, charakterystyki i budowy algorytmów kwantowych w oparciu o eksperymenty wykorzystujące najbardziej zaawansowane programowalne komputery kwantowe IBM Q.

Dostępnym komputerom kwantowym jeszcze brakuje możliwości rozwiązywania wielu trudnych i złożonych problemów w praktycznych zastosowaniach. Warto podkreślić, iż nie jest to powód do tego, aby nie wspierać różnych podejmowanych działań, które weryfikują wydajność oraz stopień zaawansowania algorytmów kwantowych zarówno od strony teoretycznej [8], jak i aplikacyjnej [9].

Szukając potencjalnych pierwszych zastosowań, w okresie od lutego do listopada 2022 roku w ramach Polskiego Węzła Obliczeń Kwantowych podjęto działania niezbędne do zidentyfikowania polskich zespołów eksperckich zainteresowanych dostępem i wsparciem w rozwoju kwantowych obliczeń z wykorzystaniem rzeczywistej infrastruktury komputerów kwantowych. Na bazie tych aktywności zidentyfikowanych zostało kilka obszarów, które wraz z rozwojem komputerów kwantowych mogą znaleźć praktyczne zastosowania w różnych dziedzinach nauki i gospodarki, w tym:

Mitygacja i korekcja błędów w komputerach kwantowych
Fizyka, Centrum Fizyki Teoretycznej PAN

Algorytmy kwantowe w optymalizacji kombinatorycznej i ich zastosowania w problemach szeregowania zadań
Informatyka, Politechnika Poznańska

Algorytmy kwantowego uczenia maszynowego
Fizyka, Uniwersytet im. Adama Mickiewicza

Badanie właściwości chemicznych wodoru i helu
Chemia kwantowa, Uniwersytet im. Adama Mickiewicza

Metody badania wydajności komputerów kwantowych
Informatyka, Instytut Informatyki Teoretycznej i Stosowanej PAN

Algorytmy kwantowe w pozytonowej tomografii emisyjnej
Fizyka Jądrowa, Narodowe Centrum Badań Jądrowych

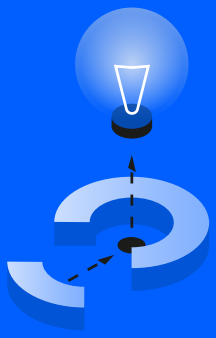
Algorytmy kwantowe w analizie bioobrazowej
Bioinformatyka i Medycyna, Instytut Chemii Bioorganicznej PAN

Algorytmy kwantowe w problemach logistyki i magazynowania
Logistyka, Sieć Badawcza Łukasiewicz – PIT

Ponadto, zidentyfikowano jednostki naukowe funkcjonujące jako Centra Komputerów Dużej Mocy zainteresowane przystąpieniem oraz wsparciem użytkowników w ramach Polskiego Węzła Obliczeń Kwantowych:

- **AKADEMIA GÓRNICZO-HUTNICZA**
  Cyfronet
- **POLITECHNIKA GDAŃSKA**
  CI TASK
- **POLITECHNIKA WROCŁAWSKA**
  WCSS
- **UNIWERSYTET WARSZAWSKI**
  ICM

W ramach dodatkowych aktywności promujących technologie kwantowe, w tym potencjał obliczeń i komputerów kwantowych, zidentyfikowano również inne jednostki naukowo-badawcze oraz przedsiębiorstwa zainteresowane bliższą współpracą z Polskim Węzłem Obliczeń Kwantowych w kolejnym roku jego działalności w następujących dziedzinach:



LOTNICTWO I TRANSPORT:

Algorytmy kwantowe w problemach zarządzania logistyką, transportem i przestrzenią powietrzną

BANKOWOŚĆ I FINANSE:

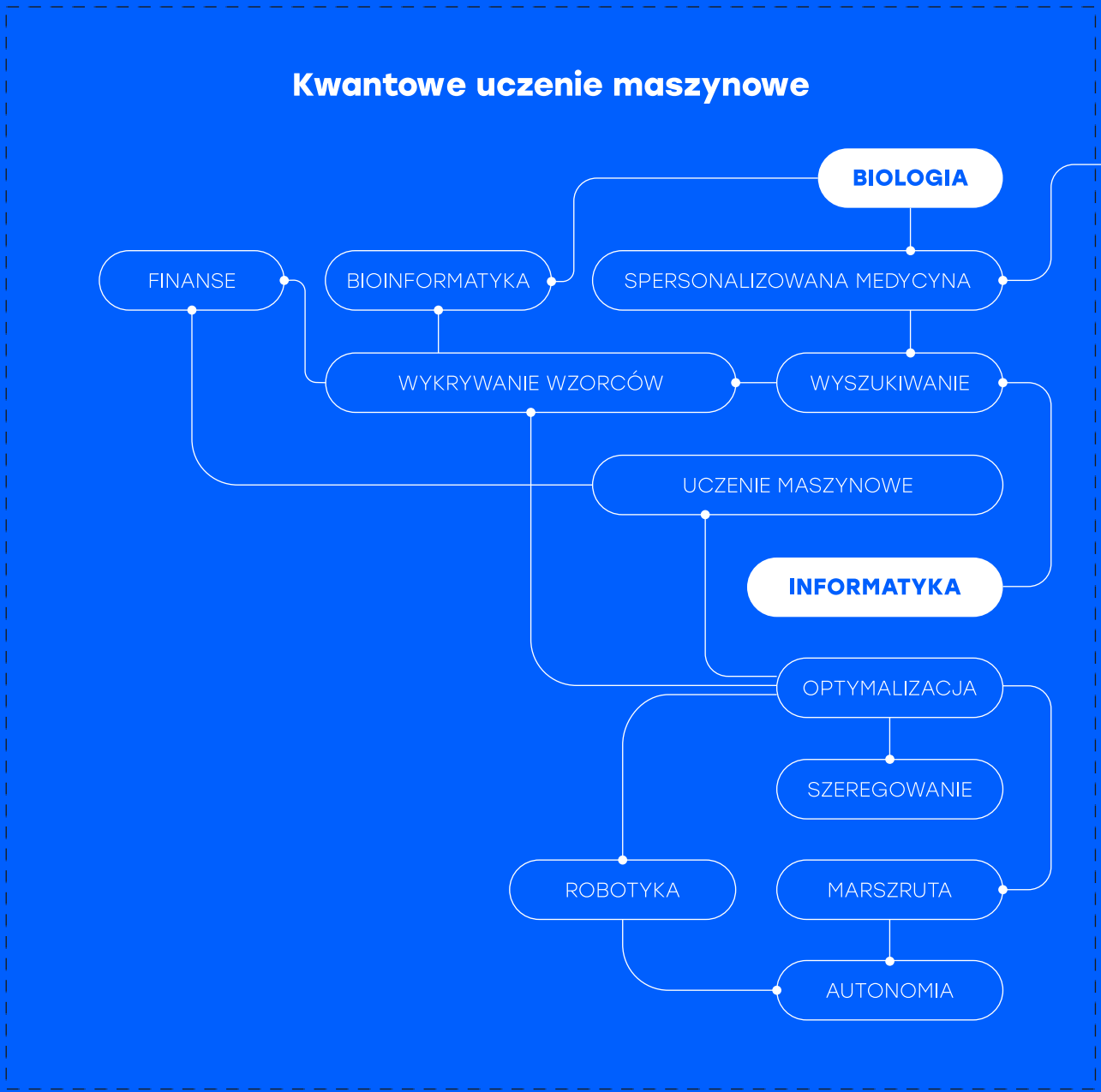
Kwantowa wycena opcji, poprawa modeli finansowych i wykorzystanie kwantowej matematyki finansowej

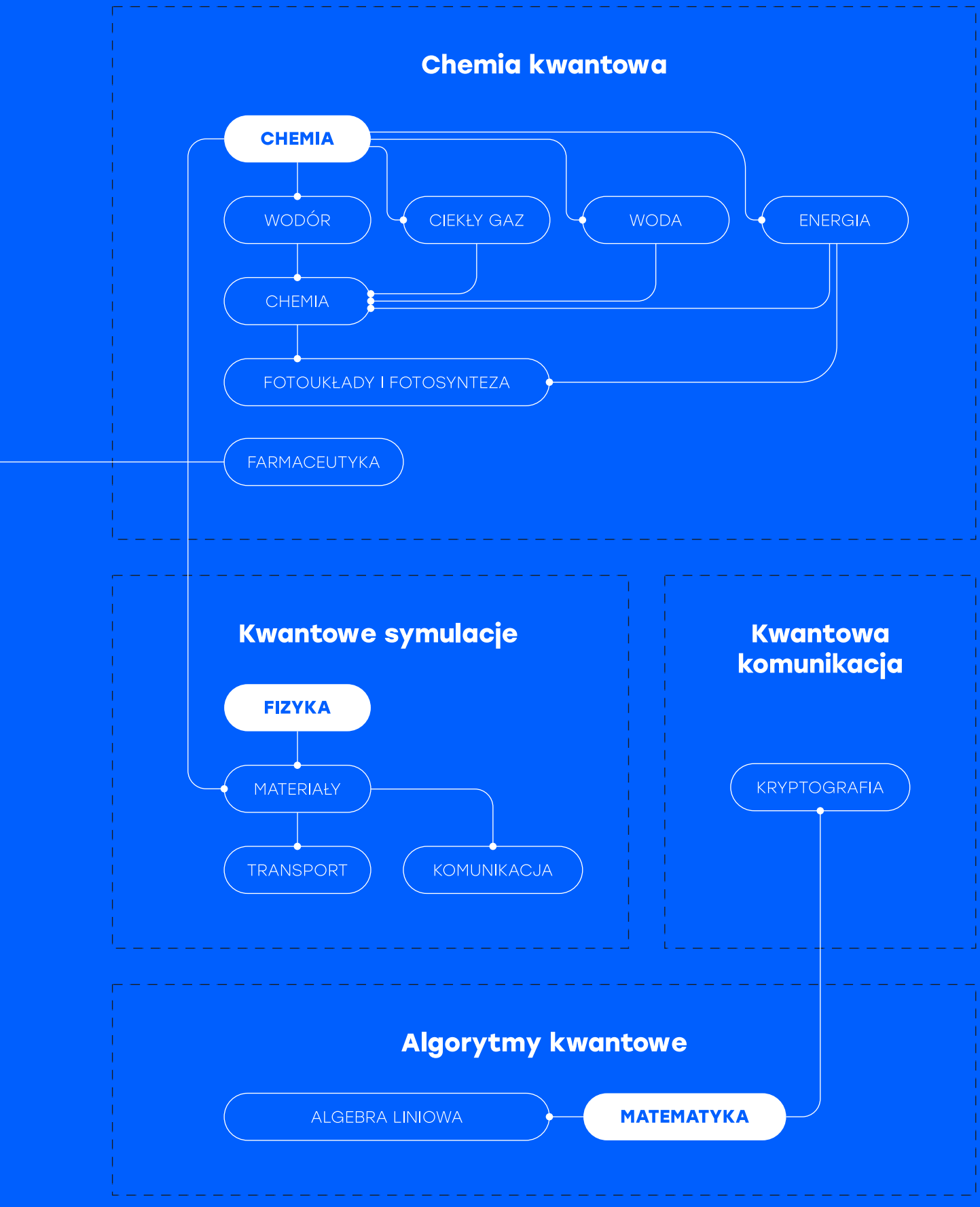
OBRONNOŚĆ I SEKTOR KOSMICZNY:

Weryfikacja dokładności i jakości algorytmów kwantowych

Źródło: IBM Quantum Lab

Zastosowanie obliczeń kwantowych



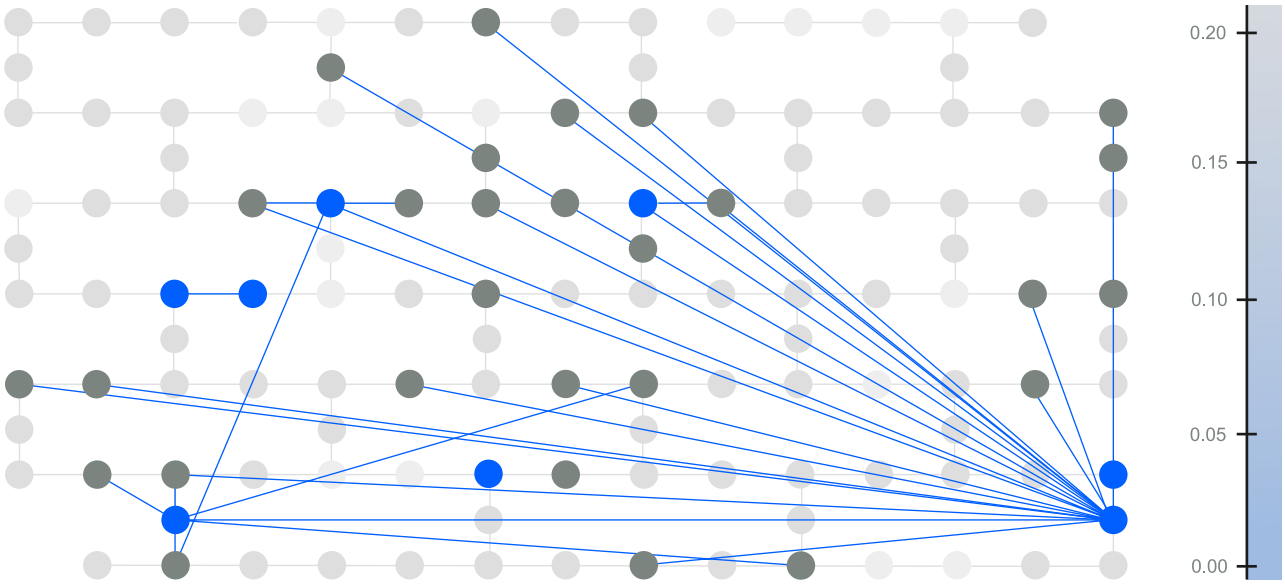

Chemia kwantowa
CHEMIA
WODÓR
CIEKŁY GAZ
WODA
ENERGIA
CHEMIA
FOTOUKŁADY I FOTOSYNTEZA
FARMACEUTYKA
Kwantowe symulacje
FIZYKA
MATERIAŁY
TRANSPORT
KOMUNIKACJA
Kwantowa komunikacja
KRYPTOGRAFIA
Algorytmy kwantowe
ALGEBRA LINIOWA
MATEMATYKA

Ograniczanie i korekcja błędów w komputerach kwantowych NISQ

Tak jak już zaznaczyliśmy w poprzednich częściach raportu, obliczenia wykonywane na dostępnych komputerach kwantowych IBM Quantum w trwającej obecnie erze NISQ są podatne na błędy. Dzieje się tak, ponieważ obecna technologia potrzebna do korekcji błędów kwantowych nie została jeszcze opracowana. Błędy w komputerach kwantowych pochodzą z kilku źródeł. Niektóre są spowodowane niedoskonałościami w implementacji bramek kwantowych, które są podstawowymi elementami składowymi układów kwantowych (tak jak w przypadku bramek logicznych w klasycznych układach cyfrowych). Kolejnym źródłem błędów jest pomiar końcowego stanu kwantowego urządzenia. Pomiary są integralną częścią przetwarzania informacji kwantowej, ponieważ każdy algorytm kwantowy kończy się pomiarem. Pomiary są także ważnym etapem pośrednim procedur korekcji błędów kwantowych.

Do tej pory większość analiz nie uwzględniała możliwości występowania skorelowanych błędów odczytu (określanych niekiedy jako cross-talk). Wykrywanie i charakteryzacja korelacji błędów pomiarowych jest trudnym zadaniem, ponieważ złożoność generycznych modeli szumu opisujących korelacje skaluje się wykładniczo z liczbą kubitów. Oznacza to, że charakterystyka skorelowanych błędów pomiarowych w obecnie dostępnych urządzeniach, takich jak np. dostępny w ramach Polskiego Węzła Obliczeń Kwantowych 127 kubitowy komputer IBM Washington, nie może być wykonana przy użyciu standardowych metod kwantowej tomografii detektorów.

Wstępne badania niektórych komputerów kwantowych NISQ wykazały, że wielkość błędów odczytu pojedynczego kubitu jest rzędu dwóch bramek kubitowych. Oznacza to, że błędy odczytu są dość znaczne i nie można ich lekceważyć. Ponadto charakterystyka błędów pomiaru może być wykorzystana w metodach mitygacji (ograniczania) błędów do poprawy jakości wyników.



Celem badań Centrum Fizyki Teoretycznej PAN było opracowanie i przetestowanie efektywnej metody charakteryzacji skorelowanych błędów odczytu. Metoda ta jest rozszerzeniem standardowej tomografii detektorów kwantowych, która pozwala uzyskiwać dane w zrównoleglony sposób. Wyniki eksperymentalne uzyskane przez wykonanie odpowiedniego zbioru obwodów kwantowych pozwalają na rekonstrukcję zredukowanych (tj. działających tylko na podzbiór kubitów) operatorów pomiaru, które są wykonywane na urządzeniu kwantowym. W ten sposób można zweryfikować wiele aspektów błędów pomiarowych. Po pierwsze, struktura zredukowanych operatorów pomiarowych pozwala ilościowo scharakteryzować siłę korelacji w błędach pomiarowych między kubitami w urządzeniu. Co ciekawe, cross-talk okazuje się występować nawet między kubitami, które są fizycznie daleko od siebie na urządzeniu. Po drugie, opracowane techniki umożliwiły charakteryzację błędów koherentnych. Wstępne wyniki pokazują, że występują one w zredukowanych operatorach pomiarowych opisujących pomiar na odpowiednio dużej liczbie kubitów. Ponadto, wiele aktualnych badań koncentruje się na tzw. stochastycznych modelach szumu błędów pomiarowych, w których relacja pomiędzy idealnymi operatorami pomiaru a operatorami realizowanymi na urządzeniu jest określona przez macierz stochastyczną. Opracowana przez Centrum Fizyki Teoretycznej PAN metoda pozwala zrekonstruować taką macierz dla klasy modeli lokalnych błędów pomiaru, w której korelacje w błędach pomiarowych ograniczone są do grup kubitów, tzw. klastrów. W ramach eksperymentów wykazano, że techniki mitygacji błędów kwantowych korzystające z charakteryzacji błędów pomiarowych dokonanych zaproponowaną metodą mogą przynieść znaczną poprawę szacowania energii Hamiltonianów wielociałowych [10]. Jest to ważne zagadnienie w algorytmach kwantowych istotnych dla zastosowań praktycznych, takich jak optymalizacja kombinatoryczna lub chemia kwantowa.

Optymalizacja kombinatoryczna

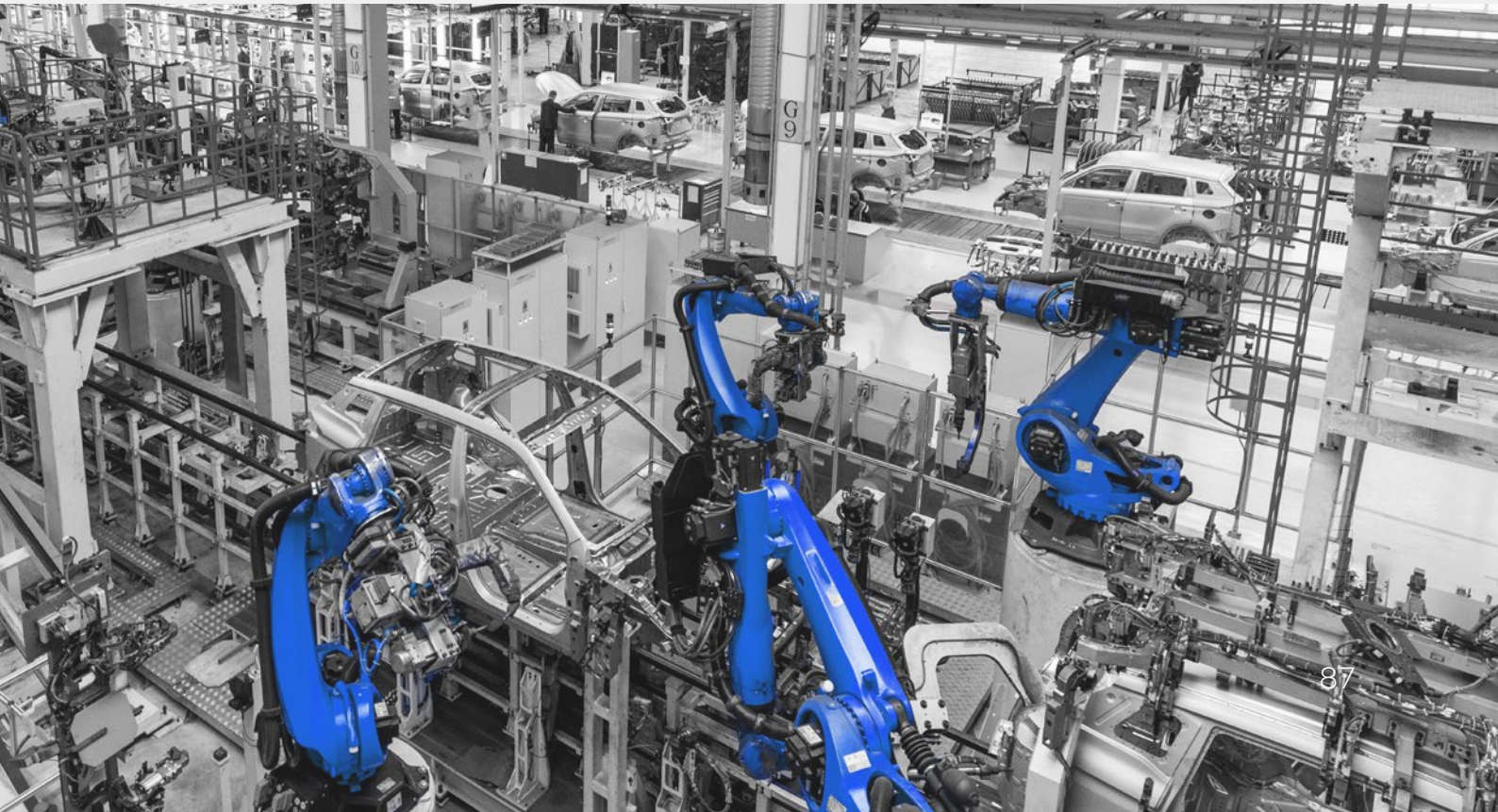
Jednym z głównych obszarów zastosowań obliczeń kwantowych są wspomniane już w przykładzie sprzedawcy trudne obliczeniowo problemy optymalizacji kombinatorycznej. Do problemów kombinatorycznych należy wiele znanych w informatyce problemów, w tym problem komiwojażera, problem plecakowy, problem kolorowania mapy czy różne odmiany szeregowania zadań w procesach produkcyjnych i systemach komputerowych. Wiele z opracowanych klasycznych algorytmów rozwiązujących problemy kombinatoryczne znajduje zastosowania do rozwiązywania odpowiednio zamodelowanych problemów oraz procesów w nauce i gospodarce. Znalezienie rozwiązania optymalnego dla wspomnianych problemów kombinatorycznych jest krótko mówiąc obliczeniowo trudne, a dla dużych instancji tych problemów wręcz niemożliwe w skończonym czasie z wykorzystaniem klasycznych komputerów. W ogólności problemy kombinatoryczne dzieli się na dwie klasy: problemy decyzyjne – rozwiązaniem jest poszukiwanie odpowiedzi „tak” lub „nie” dla wybranej instancji problemu oraz problemy przeszukiwania, w których poszukuje się optymalnego rozwiązania oceniając je zgodnie z przyjętą funkcją celu.

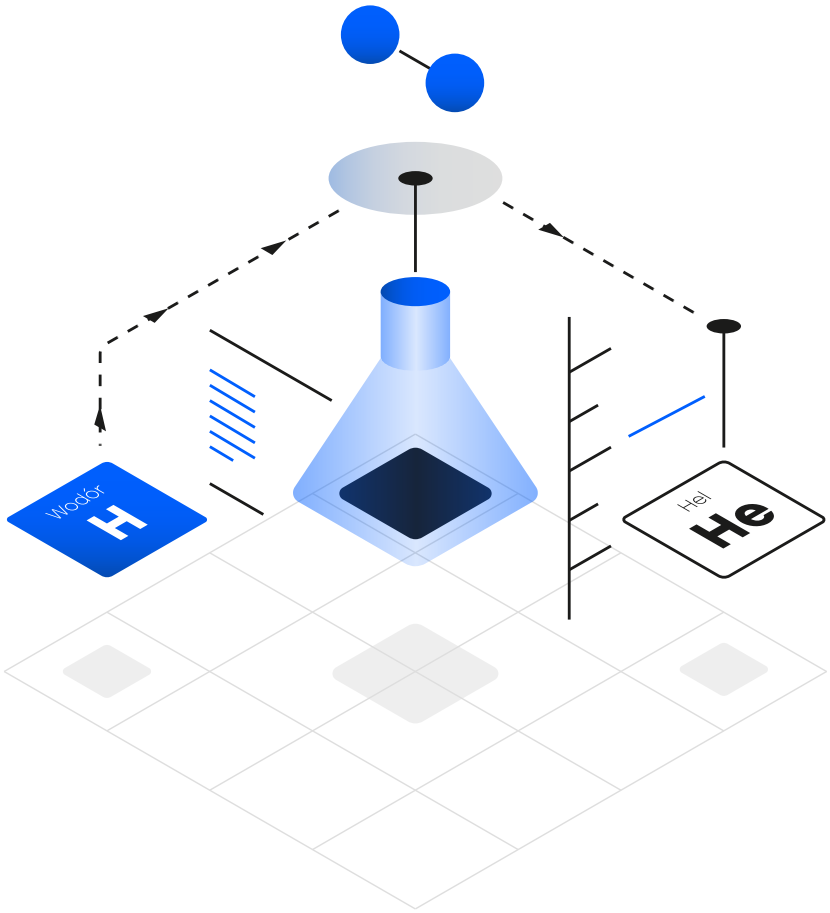
Praktycznymi problemami, które mają kluczowe znaczenie dla przedsiębiorstw wytwarzających złożone produkty przy użyciu zarówno wielofunkcyjnych, jak i wyspecjalizowanych maszyn i taśm montażowych są problemy szeregowania. Z problemami szeregowania możemy się zetknąć przy okazji praktycznie każdego procesu produkcyjnego składającego się z co najmniej kilku kroków. Przykładami zastosowań jest produkcja elektroniki precyzyjnej, produkcja części i podzespołów lub procesy technologiczne obróbki materiałów.

W praktyce, w wielu problemach optymalizacji kombinatorycznej poszukuje się rozwiązań o najlepszej wartości funkcji celu spośród wszystkich dopuszczalnych rozwiązań. Liczba dopuszczalnych rozwiązań zależy bardzo silnie od instancji danego problemu. Niestety w praktyce są to najczęściej problemy, gdzie skala wymaganych klasycznych obliczeń rośnie znacznie szybciej niż wielkość instancji problemu. Okazuje się jednak, że klasyczne problemy optymalizacji kombinatorycznej można przekształcić do postaci, w których funkcje celu odpowiadają poziomom energii Hamiltonianianów, czyli operatorów znanych nam dobrze z mechaniki kwantowej [11][12][13].

Wiele ze wspomnianych problemów optymalizacji kombinatorycznej może w naturalny i klasyczny sposób być modelowane w oparciu o teorię grafów. Teoria grafów z pozoru może wydawać się czysto teoretycznym zagadnieniem interesującym jedynie matematyków oraz informatyków teoretycznych, jednak również i tutaj możemy znaleźć szereg potencjalnych zastosowań obliczeń kwantowych. Przykładowo, problem znalezienia maksymalnej kliki w grafie, czyli takiego podgrafu, w którym wszystkie wierzchołki są ze sobą wzajemnie połączone, występuje często w ekonomii, widzeniu komputerowym, chemii czy biologii. Zarówno problem znalezienia maksymalnej kliki w grafie jak i problem znalezienia maksymalnego cięcia (czyli takiego podziału grafu na dwa podgrafy, aby po obcięciu krawędzi liczba krawędzi łączących różne podgrafy była jak największa) występuje bardzo często podczas projektowania i produkcji układów scalonych. Rozwiązanie tego typu trudnych problemów może zredukować koszty ich wytworzenia oraz poprawić ich wydajność.

W Poznańskim Centrum Superkomputerowo-Sieciowym ICHB PAN w ramach eksperymentów wydajnościowych komputerów kwantowych IBM Q badano między innymi zależności między energią a maksymalnym czasem wykonania wszystkich zadań w testowych instancjach wybranych problemów szeregowania. Ponadto, w ramach współpracy z zespołem Politechniki Poznańskiej opracowano i eksperymentalnie zweryfikowano algorytmy kwantowe w problemach optymalizacji kombinatorycznej oraz klasycznych problemach szeregowania zadań.





Chemia kwantowa

Za sprawą zaawansowanych metod obliczeniowych implementowanych na superkomputerach, możliwe stało się badanie złożonych układów chemicznych poza laboratorium, a więc w sposób najczęściej tańszy i szybszy. Dokonania i postępy w tej dziedzinie umożliwiły wykonywanie symulacji, pozwalających na przewidywanie jak prawdziwe cząsteczki chemiczne zachowają się w określonych warunkach. Chemia obliczeniowa jest powszechnie stosowana w procesie projektowania nowych lekarstw czy materiałów. Do przykładowych właściwości, które można uzyskać na podstawie klasycznego modelowania numerycznego, należą struktura cząsteczki, energie oddziaływań międzycząsteczkowych i energia całkowita cząsteczki. Symulowanie cząsteczek wykonywane jest na podstawie zasad mechaniki kwantowej. Dokładne wyniki można jednak uzyskać tylko dla najprostszych układów, gdyż modelowanie większych cząsteczek wymagałoby ogromnych, niemożliwych do uzyskania mocy obliczeniowych, o których wspominał prawie cztery dekady temu Richard Feynman [14]. W związku z tym nieuniknione jest stosowanie wielu uproszczeń prowadzących do klasycznych obliczeń łatwiejszych do wykonania, lecz nieodzownie obarczonych pewnymi niedokładnościami. W przypadkach wysoce złożonych układów poziom tych przybliżeń uniemożliwia praktyczne wykorzystanie uzyskanych wyników z klasycznych symulacji. Odpowiedzią na problem symulowania złożonych cząsteczek chemicznych mogą być komputery kwantowe. Algorytmy o największym

potencjale, podobnie jak w przypadku innych dziedzin, są jednak wciąż poza zasięgiem konstruowanych obecnie komputerów kwantowych w erze NISQ. Dlatego tak ważne jest obecnie badanie i udoskonalanie metod hybrydowych łączących potencjał klasycznych i kwantowych komputerów. Takie podejścia mogą pozwolić w praktyce na uzyskanie kwantowej przewagi wcześniej niż zbudowanie pełnoskalowego komputera kwantowego odpornego na błędy. Do czołowych przedstawicieli takiego podejścia należy szeroko analizowany przez badaczy hybrydowy algorytm VQE (ang. Variational Quantum Eigensolver).

W ramach współpracy z Uniwersytetem im. Adama Mickiewicza przeprowadzono szereg eksperymentów z wykorzystaniem komputerów kwantowych IBM Q symulując właściwości fizyczne i chemiczne cząsteczek takich jak H_2, LiH oraz atomów wodoru i helu. Obliczenia miały na celu zbadanie możliwości praktycznego wykorzystania zarówno samego algorytmu VQE jak i dostępnych komputerów kwantowych IBM Q. Sporo uwagi poświęcono kluczowej trudności, z jaką wiąże się stosowanie VQE do obliczania własności badanego układu, czyli tzw. problemowi pomiarów (ang. measurement problem). Wiąże się on z niekorzystnym skalowaniem liczby koniecznych do wykonania pomiarów względem zadanej dokładności końcowego wyniku. Zastosowane w eksperymentach techniki pozwoliły na znaczne ograniczenie wpływu tego problemu i poprawienie skalowania obliczeń kwantowych.

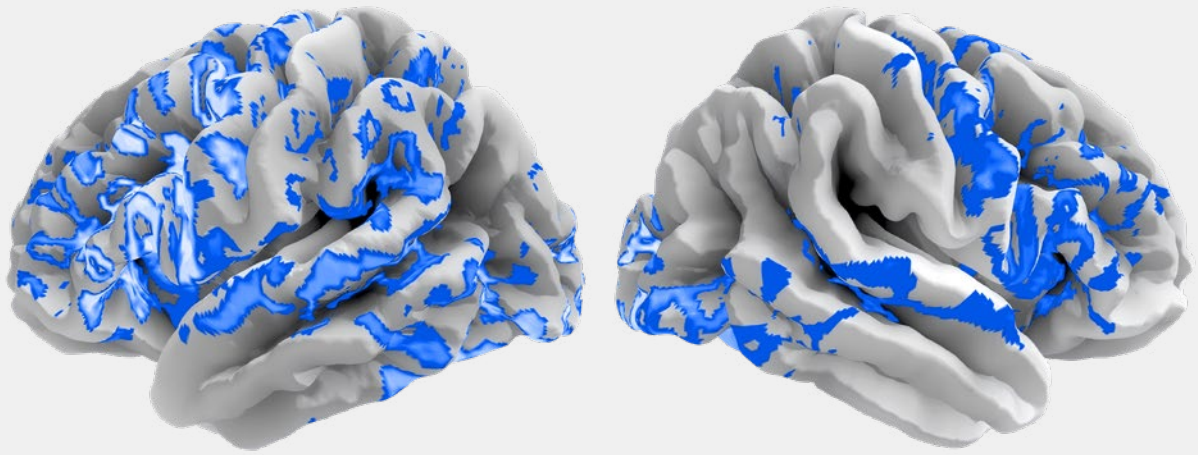
PROF. JACEK KOMASA, WYDZIAŁ CHEMII UAM

„Prowadzone obecnie prace badawcze w dziedzinie chemii kwantowej koncentrują się na znalezieniu algorytmów pozwalających skutecznie wykorzystać możliwości komputera kwantowego do odtworzenia wyników dobrze znanych z obliczeń klasycznych. Obserwując obecny trend w usuwaniu ograniczeń technicznych w komputerach kwantowych można przypuszczać, iż w niedługiej perspektywie czasowej obliczenia wykonywane przy pomocy takich komputerów przewyższą swoją efektywnością obliczenia klasyczne. Obecna sytuacja przypomina tę z lat 80, kiedy to dostępna moc obliczeniowa ówczesnych komputerów istotnie ograniczała możliwości predykcyjne teorii kwantowej.

Sztuczna inteligencja i uczenie maszynowe

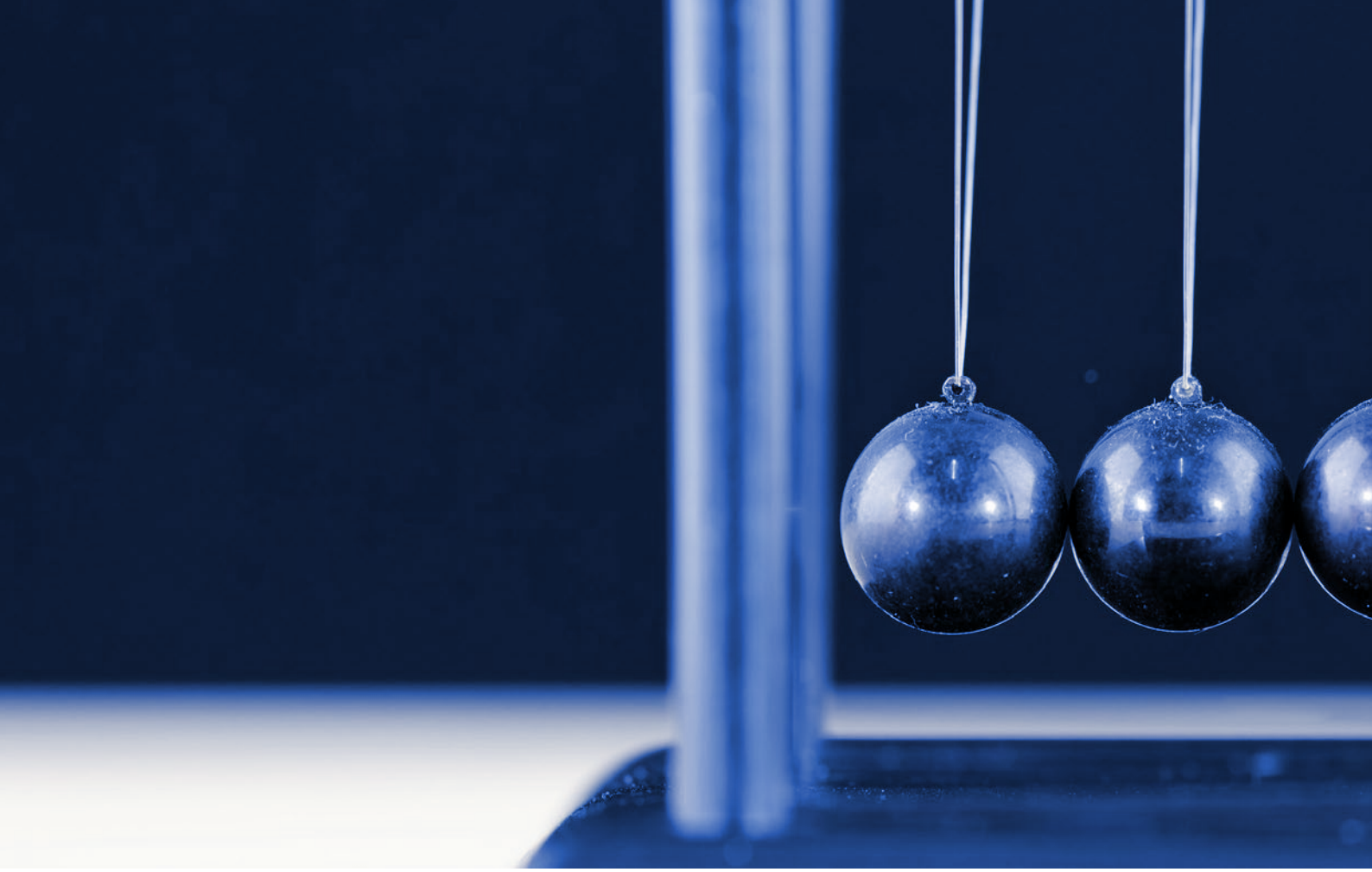
Uczenie maszynowe to gałąź informatyki i sztucznej inteligencji, obejmująca algorytmy pozwalające maszynom samodzielnie uczyć się wykonywania różnych zadań na podstawie danych. Sztandarowymi przykładami użycia uczenia maszynowego są np. sterowanie autonomicznymi samochodami, programowanie samodzielnych robotów, rozpoznawanie mowy czy klasyfikacja i generacja dźwięku oraz obrazu. Wiele klasycznych algorytmów uczenia maszynowego, takich jak np. głębokie sieci neuronowe, wykorzystują różnego rodzaju obliczenia oparte o podstawowe operacje matematyczne. Dla prostszych zastosowań liczba neuronów w modelu nie jest duża, jednak wraz ze wzrostem skomplikowania problemu liczba jednostek obliczeniowych wzrasta do ogromnych rozmiarów, a trenowanie ich wymaga coraz więcej czasu. Bardzo szybko rosną też rozmiary zbiorów danych treningowych, będących wejściem algorytmu uczącego. W związku z tym, trenowanie dużych modeli staje się coraz trudniejsze, nawet wykorzystując i masywnie zrównoleglając klasyczne obliczenia na superkomputerach oraz korzystając z zaawansowanych technologii HPC, w tym wydajnych akceleratorów graficznych GPU.

Komputery kwantowe odpowiadają na ten problem, umożliwiając transformację problemu do wielowymia-



rowej przestrzeni Hilberta poprzez zastosowanie kwantowej reprezentacji danych. Umożliwia to oszczędność jednostek obliczeniowych i daje większe możliwości w odnajdowaniu korelacji w zbiorach danych, przez co uczenie może przebiegać szybciej, a wyniki działania algorytmu mogą być dokładniejsze. Jako jeden z głównych eksperymentów dla przetestowania możliwości wykorzystania programowalnych komputerów kwantowych IBM Q wykorzystano i przetestowano kwantową wersję algorytmu maszyny wektorów wspierających QSVM (ang. Quantum-enhanced Support Vector Machine). Algorytm polega na znalezieniu korelacji między zmiennymi w zbiorze uczącym i znalezienia jego transformacji umożliwiających poprawną klasyfikację. Dzięki możliwości zastosowania kwantowej przestrzeni rozwiązań, wykorzystującej splątanie między kubitami, możliwe było znalezienie korelacji w wielowymiarowej przestrzeni Hilberta.

Pierwsze eksperymenty na komputerach kwantowych IBM Q przeprowadzono na referencyjnym zbiorze obrazów MNIST, składającym się z obrazów ręcznie pisanych cyfr o rozmiarze 28x28 pikseli. Algorytm QSVM nauczył się poprawnie wykrywać konkretne cyfry na podstawie uśrednionej jasności pikseli z kwadratowych obszarów na obrazie.



Uczenie Maszynowe

Innym fundamentalnym zastosowaniem dającym przewagę w uruchamianiu kwantowych algorytmów uczenia maszynowego jest ich zdolność do uczenia się pojęć o naturze kwantowej, co jest w praktyce nieosiągalne dla klasycznych maszyn. Z wykorzystaniem dostępu do komputerów kwantowych przez zespół z Uniwersytetu im. Adama Mickiewicza przeprowadzone zostały eksperymenty z generatywnymi modelami stanów kwantowych QGAN (ang. Quantum Generative Adversarial Network) oraz QCGN (ang. Quantum counterpart of Generative Adversarial Network).

Generatywne uczenie przeciwstawne jest jednym z najbardziej ekscytujących przełomów w uczeniu maszynowym. Znajduje ono zastosowanie w różnych wymagających zadaniach np. takich jak generowanie obrazów i filmów. Niedawno kwantowa wersja takiego uczenia została teoretycznie zaproponowana i wskazano iż ma potencjał wykazania wykładniczej przewagi nad swoim klasycznym odpowiednikiem. W badaniach zaproponowano nowe podejście do kwantowego uczenia przeciwstawnego wykorzystujące osiągnięcia teoretyczne w zakresie rozróżnialności stanów kwantowych.

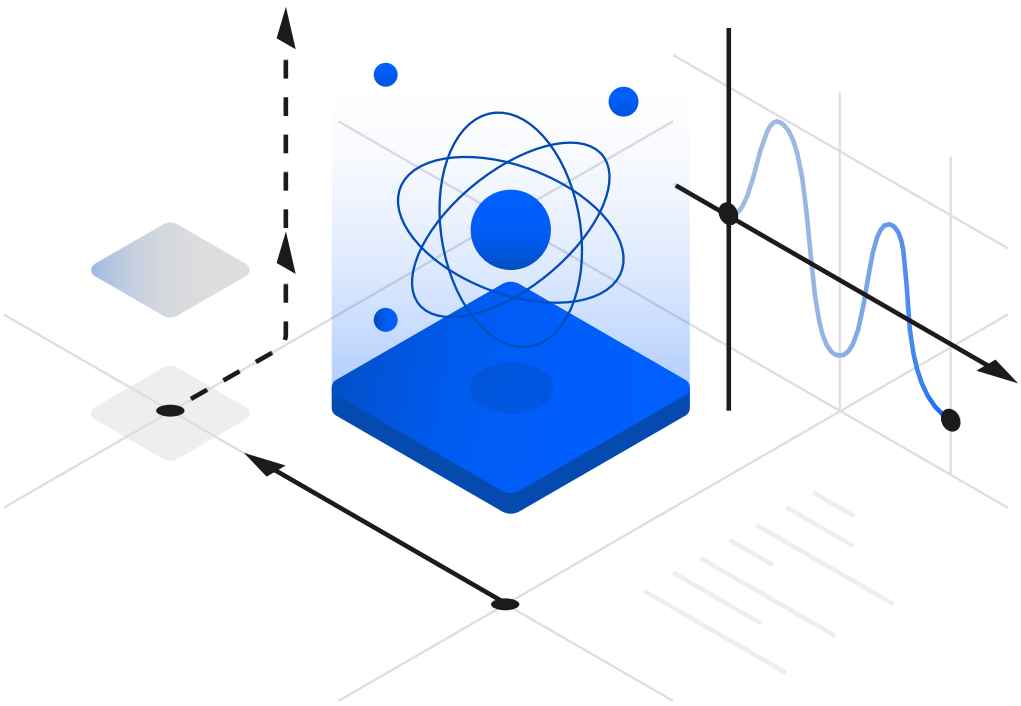
Przeprowadzono szereg eksperymentów dzięki dostępowi i użyciu rzeczywistych zaszumionych procesorów kwantowych IBM Q. Udało się zademonstrować w ten sposób poprawność działania nowego podejścia w przypadku małej liczby kubitów. Praktyczne zasto-

sowanie takiego podejścia wymaga jednak więcej prac badawczych związanych z użyciem mechanizmów ograniczania szumów.

Badania niehermitowskiej mechaniki kwantowej są obiecującym obszarem nauki z zakresu mechaniki kwantowej opisującej układy otwarte, tj. takie, gdzie pojawiają się szumy. W przypadku próby kompensacji strat w układzie może dojść do sytuacji, gdzie początkowo różne dozwolone kwantowo poziomy energetyczne staną się nierozróżnialne. Takie konfiguracje związane są z tzw. punktami wyjątkowymi. Zakłada się, że badania takich punktów pozwolą na opracowanie metod kwantowo ulepszonej detekcji procesów fizycznych oraz metod zabezpieczania przed szumem procesów kwantowych. Ma to kluczowe znaczenie dla opracowania nowych sensorów kwantowych oraz dla opracowania nowych metod walki z szumem w procesorach kwantowych. W przeprowadzonych badaniach zespół z Uniwersytetu im. Adama Mickiewicza opracował metodę wykrywania punktów wyjątkowych w układzie procesorów kwantowych IBM Q.

Zidentyfikowane zostały parametry, dla których obserwacja takich punktów jest możliwa. Opracowanie mechanizmu wykorzystującego punkty wyjątkowe w praktycznych zastosowaniach wymaga dalszych prac badawczych, w tym dostępu do nowych generacji komputerów kwantowych.

Fizyka wysokich energii i badania jądrowe



Spodziewany wzrost liczby zachorowań, połączony z kosztami ekonomicznych terapii nowotworowych powoduje, że problem ten staje się jednym z podstawowych wyzwań z którymi współczesne społeczeństwa muszą się zmierzyć. W tym kontekście niezwykle istotny jest dalszy rozwój nowych medycznych technik diagnostycznych, które pozwolą na wykrycie choroby na wczesnym etapie, co jest jednym z kluczowych czynników skutecznej terapii onkologicznej. Obecnie w diagnostyce szeroko wykorzystuje się nieinwazyjne techniki obrazowania medycznego takie jak Tomografia Komputerowa (ang. Computed Tomography CT), Rezonans Magnetyczny (ang. Magnetic Resonance Imaging MRI) oraz Pozytonowa Tomografia Emisyjna (ang. Positron Emission Tomography PET), które pozwalają na stworzenie obrazów organów lub całego ciała pacjenta. W ostatnich latach wraz z badaniami nad nową generacją skanerów PET, w szczególności obejmujących całe ciało pacjenta (ang. Total-body PET), pojawiły się propozycje opracowania technik, które dostarczyłyby dodatkowych informacji o zmianach chorobowych, rozszerzając klasyczną informację dostarczaną przez obraz pacjenta. Narodowe Centrum Badań Jądrowych (NCBJ) w ramach prac badawczych przeprowadziło testy z wykorzystaniem symulatorów i rzeczywistych komputerów kwantowych.

Dla każdego z nich przeprowadzono testy: n-kubitowego generatora liczb losowych (w celu sprawdzenia odchylenia maszyny rzeczywistej od modelu teoretycznego), algorytmu Deutscha-Jozsy, algorytmu Bernsteina-Vaziraniego, algorytmu Simona, kwantowej transformacji Fouriera, algorytmu Shora, algorytmu Grovera i kwantowego przetwarzania obrazu. Wykonano również testy komunikacji klastra superkomputera oraz symulacje splątania kwantowego dla układu dwóch fotonów z rozpadu parapositronium podczas rozproszenia Comptonowskiego z wykorzystaniem obecnych w bibliotece narzędziowej Qiskit operatorów Krausa.

NCBJ planuje dalsze prace nad symulacjami i analizami danych eksperymentalnych z detektora J-PET, działającego w oparciu o splątane kwantowo pary i trójki fotonów z anihilacji elektronowo-pozytonowej. Jest to dojrzała tematyka, uprawiana w NCBJ od dekady, w której spodziewane jest znaczne przyspieszenie rekonstrukcji obrazów przy użyciu algorytmów kwantowych. Drugim jest przewidywane zastosowanie algorytmów kwantowych do rekonstrukcji kaskad elektromagnetycznych w kalorymetrze elektromagnetycznym, służącym do detekcji cząstek o wysokich energiach w eksperymencie LHCb w CERNie. Jest to również zaawansowana tematyka, związana z silnym zaangażowaniem NCBJ w te konkretne badania doświadczalne. Trzecim obszarem są badania strukturalne na Europejskim Laserze na Swobodnych Elektronach XFEL, gdzie NCBJ wnosi istotny wkład w obszarze inżynierii IT i metodach numerycznych. Rekonstrukcje obrazów cząsteczek mogą być skutecznie przenoszone na zasoby kwantowe, a efektywne przyspieszenie ich wykonywania zależy od stopnia dekomponowalności problemu. Czwartym obszarem jest obliczeniowa dynamika płynów (CFD), ze szczegółowymi polami zastosowań w obliczeniach reaktorowych i obliczeniach środowiskowych. Zagadnieniami tymi zajmuje się specjalizowany zakład w Departamencie Badań Układów Złożonych w NCBJ.

PROF. WOJCIECH WIŚLICKI, NCBJ

W NCBJ przewiduje się rozwój kilku pól zastosowań technologii obliczeń kwantowych, od analiz danych eksperymentalnych, poprzez zaawansowane algorytmy rekonstrukcji obrazów, aż po obliczenia znajdujące zastosowania w obliczeniach reaktorowych i środowiskowych.

Sektor finansowy

Ważnym polem zastosowania różnego typu optymalizacji i obliczeń wielkoskalowych jest sektor finansowy. Optymalizacja portfela inwestycyjnego pod względem maksymalizacji zysku z inwestycji czy minimalizacji ryzyka jest istotną częścią operacji wielu instytucji na całym świecie, w tym w szczególności instytucji finansowych, banków, domów maklerskich itd. Dotychczas optymalizacja uwzględniała złożone kryteria i zmienne wejściowe była zadaniem bardzo trudnym dla klasycznych komputerów, dlatego często do rozwiązania tego problemu wykorzystuje się heurystyki, lub algorytmy uczenia maszynowego oparte na danych historycznych. Dzięki możliwości równoległego przeszukiwania przestrzeni rozwiązań przez komputer kwantowy możliwe jest znajdowanie optymalnych strategii inwestycji i prowadzenie efektywnych symulacji zachowań rynków różnego rodzaju aktywów. Wielokryterialna optymalizacja zarówno w zakresie ilości zmiennych decyzyjnych, jak i różnorodności funkcji celu jest możliwa dzięki zagregowaniu wszystkich parametrów do funkcji energii, optymalizowanej przez algorytm kwantowy. Przykładem konkretnych zastosowań komputerów kwantowych może być kwantowy model wyceny opcji, w którym wypłata zależy od średniej ceny aktywa bazowego w pewnym w pewnym okresie czasowym w przeciwieństwie do standardowych opcji (amerykańskich i europejskich), w których wypłata zależy od ceny aktywa bazowego w określonym momencie (zapadalności) [15].

W ramach współpracy z instytucjami finansowymi zbadano możliwości wykonania eksperymentów z wykorzystaniem referencyjnych i testowych danych finansowych. Zostały wykonane wstępne testy możliwości użycia komputerów kwantowych, do prostego zadania optymalizacji portfela finansowego. Rozwój infrastruktury kwantowej wkrótce może dać możliwość rozszerzenia tych przykładów o dodatkowe parametry wejściowe i kryteria optymalizacyjne, uwzględniając nowe ryzyka związane ze zmianami klimatycznymi ocenianych inwestycji, co umożliwi wykorzystanie ich w nowych zastosowaniach.

Inne zastosowania

Kolejnym ważnym obszarem potencjalnych zastosowań komputerów kwantowych IBM Q, w tym zastosowania wspomnianych kwantowych algorytmów uczenia maszynowego, były eksperymenty z analizą danych medycznych przeprowadzone przez Poznańskie Centrum Superkomputerowo-Sieciowe ICHB PAN. Zgromadzone referencyjne dane bioobrazowe pozyskiwane są najczęściej przy pomocy skanera Rezonansu Magnetycznego podczas gdy osoby badane wykonują zadania mentalne dotyczące, np. funkcji językowych mózgu czy zdolności motorycznych. Celem pozyskiwania tego typu danych jest lepsze zrozumienie skomplikowanych procesów zachodzących w korze mózgowej podczas wykonywania pozornie łatwych, wykonywanych „automatycznie", codziennych czynności. Eksperyment z analizą wyników z Funkcjonalnego Rezonansu Magnetycznego (fMRI) przy pomocy komputera kwantowego może wykazać, że modele kwantowe są lepszą reprezentacją złożonych procesów zachodzących w mózgu niż klasyczne modele statystyczne. Będzie to miało bezpośredni wpływ na dokładność modeli funkcji mózgowych i może przyczynić się, np. do lepszej diagnostyki zaburzeń działania centralnego układu nerwowego w przypadku schorzeń takich jak afazja i apraksja (zaburzenia mowy i funkcji motorycznych, występujące najczęściej w następstwie udaru), a także choroby Alzheimera, choroby Parkinsona, depresji czy schizofrenii.

Dodatkowo, Instytut Informatyki Teoretycznej i Stosowanej PAN opracował narzędzie o nazwie PyQBench służące do testowania bramkowych komputerów kwantowych, w tym udostępnionych zasobów IBM Q, na podstawie ich zdolności do rozróżniania pomiędzy dwoma pomiarami von Neumanna w różnych bazach. Opracowane narzędzie pozwala na uruchomienie benchmarków wykorzystujących rozróżnianie między pomiarem w bazie obliczeniowej a pomiarem w bazie definiowanej przez sparametryzowaną rodzinę Fouriera. Użytkownik może wybierać, czy eksperyment zostanie przeprowadzony przy pomocy postselekcji czy alternatywnej metody "sumy prostej" oraz kontrolować różne aspekty przeprowadzanego eksperymentu, takie jak liczba próbek używanych w samplowaniu, indeksy kubitów, zakresy kąta dla sparametryzowanej rodziny Fouriera. Jeżeli użytkownik chce użyć pomiaru w innej bazie, może wykorzystać PyQBench jako bibliotekę programistyczną. Ten tryb użycia wymaga większego nakładu pracy, ale pozwala na rozszerzenie parametrów eksperymentu. Warto wspomnieć, że w przypadku zasobów komputerów kwantowych udostępniających informacje o kalibracji kubitów, PyQBench wspiera mitygację błędów metodą matrix-free measurement mitigation. W ramach zagwarantowanego dostępu do zasobów IBM Q wykonano szereg eksperymentów na podstawie benchmarku rozróżniania pomiarów von Neumanna.

Eksperyment z analizą wyników z Funkcjonalnego Rezonansu Magnetycznego (fMRI) przy pomocy komputera kwantowego może wykazać, że modele kwantowe są lepszą reprezentacją złożonych procesów zachodzących w mózgu niż klasyczne modele statystyczne.

OBSZARY POTENCJALNYCH ZASTOSOWAŃ	MATERIAŁOZNAW-STWO I BIOLOGIA	ZŁOŻONE SYSTEMY I PROBLEMY	ISTNIEJĄCA TECHNOLOGIA I BADANIA
BRANŻE	Energia, żywność i rolnictwo, produkcja, chemia, medycyna.	**Finanse, transport i logistyka, branże o złożonych produktach (lotnictwo, motoryzacja itp.).**	Branże z intensywnym wykorzystaniem technologii AI, blockchain i HPC, przemysł energetyczny i materiałowy, komunikacja.
PRZYKŁADY UŻYCIA OBLICZEŃ KWANTOWYCH	Odkrywanie i projektowanie nowych cząsteczek i materiałów, wpływające na wiele dziedzin: rozwój zaawansowanych materiałów, projektowanie leków, uprawy i nawozy, zielone katalizatory wodoru, baterie, chemia.	**Zarządzanie i optymalizacja skomplikowanych systemów z dużą liczbą zmiennych lub niewiadomych, od wysoce złożonych problemów szeregowania zadań, logistyki i łańcucha dostaw, do modelowania portfeli finansowych i profili ryzyka.**	Wpływ na istniejące technologie, w tym AI i blockchain, a także nowe metody obliczeniowe dla nauki.
SPOŁECZNE I ŚRODOWISKOWE WPŁYWY	Zmniejszenie zużycia energii, wydajne materiały i procesy, bardziej wytrzymałe i przyjazne naturze gatunki roślin, przyspieszone odkrywanie reakcji, medycyna spersonalizowana.	**Zmniejszenie zużycia energii i emisji w całej globalnej sieci, obiegowe modele biznesowe.**	Możliwość łamania obecnej kryptografii, zastosowanie potencjalnie silniejszej kryptografii z większym poziomem prywatności i bezpieczeństwa. Przyspieszenie eksploracji w podstawowych badaniach naukowych.

OBSZARY POTENCJALNYCH ZASTOSOWAŃ	MATERIAŁOZNAWSTWO I BIOLOGIA	ZŁOŻONE SYSTEMY I PROBLEMY	ISTNIEJĄCA TECHNOLOGIA I BADANIA
ILUSTRACYJNE PRZYKŁADY	Molekuły z odpowiednimi atrybutami do sekwestracji węgla.	**Optymalizacja transportu i logistyki przynosząca środowiskowe i ekonomiczne korzyści.**	Możliwość przyspieszenia procesów trenowania algorytmów uczenia maszynowego.
	Bardziej naturalnie odporne ziarna, aby poprawić produkcję żywności, przy jednoczesnym unikaniu monokultur.	**Poprawa oceny kredytowej klientów w czasie rzeczywistym.**	Złamanie RSA i szyfrowanie kryptowalut. Przyczynianie się do naszego fundamentalnego zrozumienia kwantowego.
ZASADNICZE PROBLEMY KWANTOWE	Symulacja kwantowa, optymalizacja kombinatoryczna, algebra liniowa i faktoryzacja liczb pierwszych.		

Tab. 2. Źródło: World Economic Forum, Global Future Council on Quantum Computing [7].

Podsumowanie i wnioski

Wszystkie omówione w raporcie zagadnienia oraz przykładowe zastosowania pokazują, że wejście w erę technologii kwantowych jest nie tylko interesującym kierunkiem badań naukowych, ale wręcz koniecznym krokiem, aby zapewnić bezpieczeństwo w sieci i poradzić sobie z coraz trudniejszymi problemami oraz większymi wolumenami danych przetwarzanych przez klasyczne komputery. Raport jest też próbą odpowiedzi na wiele zadawanych przez użytkowników fundamentalnych pytań związanych z technologiami, komputerami i obliczeniami kwantowymi.

Raport odpowiada na pytania:

- **Czy możemy zastąpić tranzystory i wykorzystać efekty kwantowe do obliczeń i symulacji?**
- **Czy komputer kwantowy to tylko nowa, bardziej wydajna generacja superkomputerów?**
- **Czy i jakie komputery kwantowe są dostępne dla krajowych użytkowników?**
- **Jaki jest paradygmat programowania komputera kwantowego?**
- **Jakie są główne bariery technologiczne w istniejących i przyszłych komputerach kwantowych**
- **Co i w jakim stopniu może potencjalnie ograniczyć zakres praktycznych zastosowań komputerów kwantowych?**
- **Do rozwiązywania jakich problemów mogą być wykorzystane w pierwszej kolejności komputery kwantowe?**
- **Jakie umiejętności są nam potrzebne, aby rozpocząć eksperymenty z komputerami kwantowymi?**

PCSS | Poznańskie Centrum
Superkomputerowo-Sieciowe

Referencje

1. A. Einstein, B. Podolsky, and N. Rosen. (1935) Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? A Phys. Rev. 47, 777. https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777

2. J. S. Bell. (1964) On the Einstein Podolsky Rosen paradox., Physics Physique Fizika 1, 195. https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195

3. Shor, P.W. (1997) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26, 1484-1509. https://doi.org/10.1137/S0097539795293172

4. Chuang, Isaac L.; Gershenfeld, Neil; Kubinec, Mark (1998). "Experimental Implementation of Fast Quantum Searching". Physical Review Letters. 80 (15): 3408–3411. Bibcode:1998PhRvL..80.3408C. doi:10.1103/PhysRevLett.80.3408. S2CID 13891055

5. IBM Quantum-centric supercomputing: The next wave of computing. https://research.ibm.com/blog/next-wave-quantum-centric-supercomputing

6. Cross, Andrew W.; Bishop, Lev S.; Sheldon, Sarah; Nation, Paul D.; Gambetta, Jay M. (2019). "Validating quantum computers using randomized model circuits". Phys. Rev. A. 100 (3): 032328. arXiv:1811.12926

7. World Economic Forum - State of Quantum Computing: Building a Quantum Economy, https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf

8. Application-Oriented Performance Benchmarks for Quantum Computing. Lubinski, T., Johri, S., Varosy, P., Coleman, J., Zhao, L., Necaise, J., Baldwin, C.H., Mayer, K.H., & Proctor, T.J. (2021). https://arxiv.org/abs/2110.03137

9. Quantum Algorithm Zoo, https://quantumalgorithmzoo.org/

10. McNulty, D., Maciejewski, F.B., & Oszmaniec, M. (2022). Estimating Quantum Hamiltonians via Joint Measurements of Noisy Non-Commuting Observables. https://arxiv.org/abs/2206.08912

11. Kadowaki, T., & Nishimori, H. (1998) Quantum annealing in the transverse Ising model. Physical Review E, 58, 5355-5363. https://arxiv.org/abs/cond-mat/9804280

12. Lucas, Andrew. (2014) Ising formulations of many NP problems. https://arxiv.org/abs/1302.5843

13. Farhi, Edward et al. (2014) A Quantum Approximate Optimization Algorithm. arXiv: Quantum Physics https://arxiv.org/abs/1411.4028

14. Feynman, R.P. Simulating physics with computers. (1982) Int J Theor Phys 21, 467–488 https://doi.org/10.1007/BF02650179

15. Pracht, Rafał and Ryterski, Adam and Plewa, Julia and Stefaniak, Marek, FX Asian Option Pricing Using Quantum Computers (2022). http://dx.doi.org/10.2139/ssrn.4137397

16. Peruzzo, A., McClean, J., Shadbolt, P. et al. (2014) A variational eigenvalue solver on a photonic quantum processor. Nat Commun 5, 4213. https://doi.org/10.1038/ncomms5213

17. National Security Agency/Central Security Service, President Biden Signs Memo to Combat Quantum Computing Threat [Press release], 4 May 2022, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3020175/president-bidensigns-memo-to-combat-quantum--computing-threat/

Przypisy i źródła

Str. 1 Okładka IBM Quantum Dilution Refrigerator, https://flic.kr/p/23R2fqS

Str. 4 Nejc Soklič dla Unsplash, https://unsplash.com/photos/wO42Rmamef8

Str. 6 Solen Feyissa dla Unsplash https://unsplash.com/photos/QtW6mf1JMu8

Str. 11 Fot. Maciej Rutkowski (Biblioteka zdjęć PCSS)

Str. 14 Zdjęcia autorstwa (od góry) [Peter Lyons, Royal Society uploader, Jaqueline Godany], licencja CC.

Str. 20 Christopher Burns dla Unsplash, https://unsplash.com/photos/Kj2SaNHG-hg

Str. 24, 36, 46, Pawel Czerwinski dla Unsplash, https://unsplash.com/photos/WVKFthwtJwU

Str. 29 John Stewart Bell, https://pl.wikipedia.org/wiki/John_Stewart_Bell

Str. 35 Quantum Computer Interior, https://flic.kr/p/SrvZqe

Str. 39 Marten Bjork dla Unsplash, https://unsplash.com/photos/6dW3xyQvcYE

Str. 43 Karlis Reimanis dla Unsplash, https://unsplash.com/photos/Y31Z6Mf7rys

Str. 48 Fot. Maciej Rutkowski (Biblioteka zdjęć PCSS)

Str. 50 IBM Qubit Device, https://flic.kr/p/Yq44fF

Str. 52 Derek Thomson, https://unsplash.com/photos/NqJYQ3m_rVA

Str. 54 Dan Cristian Pădureț dla Unsplash, https://unsplash.com/photos/h3kuhYUCE9A

Str. 59 Obwód kwadratowy IBM czterech kubitów, https://flic.kr/p/roqFwu

Str. 63 Naukowiec IBM Quantum dr Maika Takita w Centrum Badawczym Thomasa J Watsona IBM Quantum Lab, https://flic.kr/p/2kRq6pU

Str. 67 Fot. Maciej Rutkowski (Biblioteka zdjęć PCSS)

Str. 71 IBM Quantum Composer, https://flic.kr/p/GGdJyp

Str. 72 Fot. Maciej Rutkowski (Biblioteka zdjęć PCSS)

Str. 74 H Liu, https://unsplash.com/photos/bv8xNCs2AvE

Str. 76 IBM Quantum Osprey Processor, https://flic.kr/p/2nX9Kpe

Str. 81 IBM Quantum Lab, https://flic.kr/p/2kRpFVS

Str. 87 usertrmk, Linia Do Produkcji Samochodów, https://pl.freepik.com/darmowe-zdjecie/panoramiczna-linia-do-produkcji-samochodow-do-spawania-karoserii-nowoczesna-montownia-samochodow_26149998.htm

Str. 89 Misael Moreno, https://unsplash.com/photos/fN6K30xtiKE

Str. 92 engin akyurt, https://unsplash.com/photos/KUeJcc4YUug

Str. 97 Nick Chong, https://unsplash.com/photos/N__BnvQ_w18

Str. 99 Cristiano Firmani, https://unsplash.com/photos/tmTidmplLWw

Str. 102 drmakete lab, https://unsplash.com/photos/hsg538WrP0Y

Opracowanie raportu w zespole PCSS

Kierownik projektu i redakcja:	dr hab. inż. Krzysztof Kurowski
Opisy merytoryczne:	Artur Binczewski Cezary Mazurek Tomasz Pecyna Tomasz Piontek Piotr Rydlichowski Mateusz Slysz Marek Subocz Konrad Wojciechowski
Skład i grafiki:	Diana Kruger Mateusz Barancewicz Robert Wielgocki
Podziękowania za współpracę:	Mateusz Bała Filip Maciejewski Krzysztof Matysiak Łukasz Pawela Arkadiusz Piwoński Patrycja Tulewicz Kamil Wereszyński