

# 하버드비즈니스리뷰

# Harvard Business Review

HBRKOREA.COM

## IT MANAGEMENT

### 비즈니스 리더를 위한 양자 컴퓨팅 안내서

### How Companies Can Address Their Historical Transgressions

조너선 루앤, 앤드루 맥아피, 윌리엄 D. 올리버

#### 저작권 공지

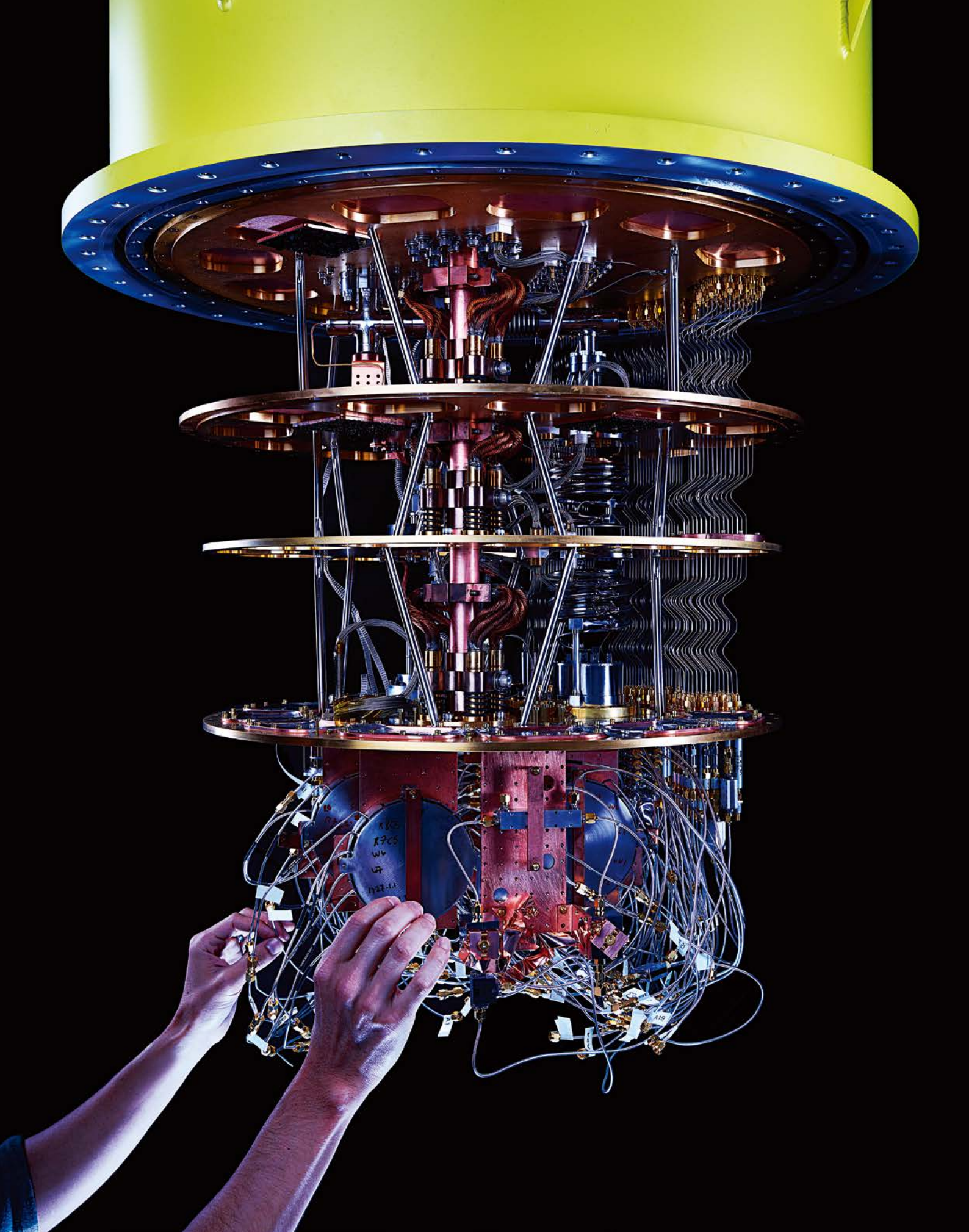
본 PDF 문서에 실린 글, 그림, 사진 등 저작권자가 표시되어 있지 않은 모든 자료는 Harvard Business School Publishing Corporation(HBSP)에 있습니다. Harvard Business Review Korea 콘텐츠는 HBSP 공식 라이선스 계약을 맺고있는 ㈜동아일보사의 사전 동의 없이는 어떠한 경우도 사용할 수 없습니다.

#### PDF 복사 및 배포 안내

기업, 학교 등에서 단체 열람용으로 구매 배포가 필요할 경우 별도 저작권료를 지불하셔야 합니다. (문의: 02-6718-7803 / help@hbrkorea.com)  
저작권료 지불 없이 무단 복제, 전송, 공중송신, 배포 기타 저작권법에 위반되는 방법으로 사용할 경우 저작권법 제 136조에 따라 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해질 수 있습니다.

#### 하버드비즈니스리뷰 코리아, 이렇게 신청하세요.

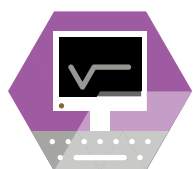
- 발행정보 | 격월 1회 발행, 연 6회 발행
- 가격 | 날권 25,000원
- 1년 정기구독료 | 150,000원
- 1년 매거진 + 디지털 패키지 | 210,000원
- 인터넷구독 신청 | [www.hbrkorea.com](http://www.hbrkorea.com)
- 구독 문의 | 02-2020-0580, 02-6718-7803 / [help@hbrkorea.com](mailto:help@hbrkorea.com)





# 비즈니스 리더를 위한 양자 컴퓨팅 안내서

말 많은  
양자 컴퓨터,  
정말 그대로  
이뤄질까?



IT MANAGEMENT



AUTHORS

조너선 루엔

MIT

슬론경영대학원 강사

앤드루 맥아피

MIT

디지털경제이니셔티브  
설립자

윌리엄 D.

올리버

MIT 교수

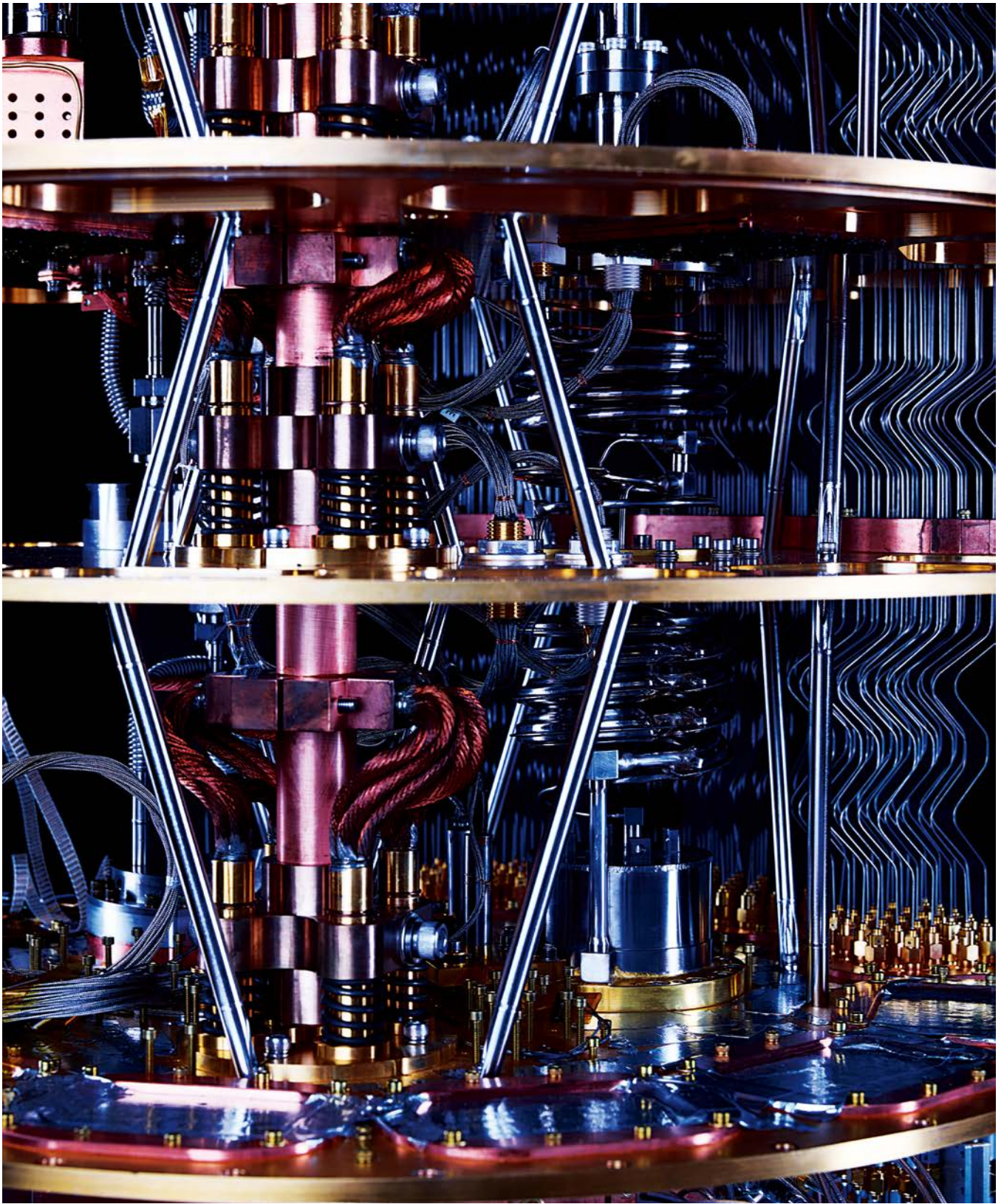


PHOTOGRAPHER SPENCER LOWELL

Harvard Business Review  
January-February 2022

117

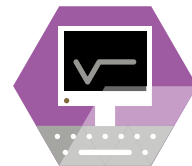




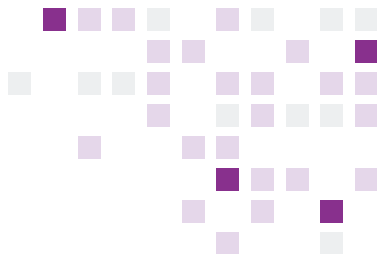


#### 사진에 대해

2017년 사진작가 스펜서 로웰이 촬영한 구글의 초전도 양자 컴퓨터.  
당시 기준 세계에서 가장 발달한 범용 양자 컴퓨터다.



IT MANAGEMENT



# 1994년

**미국 응용수학자 피터 쇼어**<sup>Peter Shor</sup>가 양자 컴퓨팅 알고리즘을 발표했다. 이론상 이 알고리즘을 이용하면 기존 트랜지스터 기반 컴퓨터로는 수십억 년이 걸리는 아주 큰 수의 소인수분해를 단 며칠로 줄일 수 있다. 오늘날 암호화와 정보 보안 인프라 상당수가 소인수분해에 기반을 두고 있다는 점에서 이는 놀라운 혁신이었다. 그로부터 7년 뒤인 2001년, IBM 과학자들은 비록 소형 양자 머신이었지만 최초로 이를 통해 쇼어의 알고리즘을 실증해내는 데 성공해 양자 컴퓨터를 현실에 구현할 수 있고 쇼어의 알고리즘도 적용이 가능하다는 것을 보여줬다.

양자 컴퓨터를 이용하면 많은 문제를 푸는 속도가 기하급수적으로 빨라지는 데다 고전 컴퓨터나 이진법 컴퓨터로 계산할 때보다 에너지

소비량도 적다. 왜 그럴까? 2차원의 미로를 떠올려 보라. 기성 컴퓨터로 미로를 빠져나갈 길을 찾으려면 하나하나 차례로 검증해봐야 한다. 총 256개의 경로로 구성된 미로라면 기존 컴퓨터로는 약 128회(올바른 길을 찾으려면 평균적으로 미로 길의 절반을 시도해야 한다)를 연속으로 돌려봐야 한다. 하지만 양자 컴퓨터는 256개의 길을 동시에 시험할 수 있다. 다르게 설명하자면 기존 8비트 이진법 컴퓨터는 0~255 사이 하나의 숫자만 나타낼 수 있지만 8큐비트<sup>Qubit</sup> 양자 컴퓨터는 0에서 255까지 모든 숫자를 ‘동시에’ 나타낼 수 있다. 어떻게 이런 일이 가능할까? 답은 양자 역학의 기본 법칙에 있다. 기존 이진법(비트) 컴퓨팅에서는 0과 1 중 하나의 값만 가질 수 있지만, 양자 컴퓨터의 연산 기본 단위인 큐비트에서는 0 또는 1이 공존(양자 중첩 현상)한다.

기업은 양자 컴퓨팅으로 투자 전략, 암호 기능, 신제품 개발 등에서 더욱 최적화된 결과를 끌어낼 수 있다. 양자 연구에 천문학적인 투자가 쏟아지고 민간 부문의 경쟁이 치열하며 수학 및 과학계 인재들이 연구에 전념하고 있다. 글로벌 시장조사기관 CB인사이트에 따르면 양자 분야에 투입된 벤처캐피탈 자금은 2015~2020년 동안 500% 증가했다. 2016년에 설립된 양자 컴퓨팅 스타트업 사이퀀텀<sup>PsiQuantum</sup>은 글로벌 자산운용사 블랙록<sup>BlackRock</sup>과 마이크로소프트 등으로부터 6억6500만 달러 이상의 자금을 조달했다. R&D 선도기업인 허니웰, IBM, 인텔도 차세대 양자 기술을 개발하기 위해 한창 경쟁하고 있다. 컨설팅 업계는 클라이언트를 지원하기 위해 인재풀을 확장하고 있다. 액센추어는 전 세계에 걸쳐 쿼텀 전문팀 15개 이상과 100명 이상의 전문가를 보유하고 있

## 내용 요약

### 문제

양자 컴퓨터는 고전 컴퓨터보다 기하급수적으로 더 빠르게 문제를 푼다. 양자 컴퓨터로 크게 두 가지가 달라진다. 첫째는 공공 네트워크의 현행 사이버 보안 인프라의 무력화이고, 둘째는 알고리즘의 비약적 발전으로 새로운 세상이 도래할 것이라는 점이다.

### 원인

과학자들이 상업용 양자 컴퓨터를 개발하기 위해 애쓰지만 무수한 한계의 벽에 부딪치고 있다. 일단 상업화에 성공하면 과거 Y2K를 앞두고 일었던 혼란(문제 해결에 미국과 미 기업이 1000억 달러 이상을 투입함)이 가벼운 소동으로 보일 정도의 대격변이 나타날 것이다.

### 해결책

이 아티클은 양자 컴퓨터가 어떻게 기존 사이버보안의 패러다임을 뒤집을 뿐 아니라 투자와 혁신을 촉진하고 여러 업계를 재편할지를 다루고 있다.



다.(참고: 아티클의 필자 중 두 명이 MIT 디지털경제 이니셔티브 소속으로 액센추어는 해당 센터에 재정적으로 지원하고 있다.) 2021년 5월 구글은 2029년까지 실제 작동하는 양자 컴퓨터를 만들기 위해 수십억 달러를 투자하기로 약속했고, 이에 따라 캘리포니아 샌타바버라에 양자 AI 캠퍼스를 마련해 자사의 양자 전문가 수백 명을 수용하고 양자 데이터센터, 연구소, 양자 프로세서 칩 제조 시설을 구축할 것으로 전망된다.

과거에 비해 볼 때 혁신 기술들은 이 같은 환경에서 등장한다. 그리고 장담컨대 양자 컴퓨팅은 비교도 안 되게 엄청난 혁신을 가져올 것이다. 양자 컴퓨터 혁신으로 오늘날 비즈니스 업계에 가공할 만한 갑작스러운 변화 두 가지가 동시에 닥칠 것이다. 첫째, 공공 네트워크를 통해 디지털 공간의 개인정보 보호와 보안을 보장하기 위해 구축한 현재의 인프라가 무력해진다. 인프라를 개선하지 않는 기업은 치명적인 공격에 속수무책으로 당할 것이다. 둘째는 첫째보다 긍정적인 변화다. 알고리즘이 대폭 발전하면서 오늘날 불가능한 많은 일을 컴퓨터로 처리할 수 있고 나아가 새로운 세상이 도래할 것으로 보인다.

그렇다면 언제쯤 상업용 양자 컴퓨터가 등장할까? 쇼어의 알고리즘에 대한 개념 증명이 나온 지 20년 가까이 지났는데도 과학자들은 아직 대형 양자 컴퓨터를 개발하는 데 무수히 많은 벽에 부딪히고 있다. 양자 컴퓨터가 실제 상용화되리라 여기고 흥분하거나(보는 태도에 따라 격정하거나) 하는 것은 시기상조라는 회의론도 나온다. 1947년 트랜지스터가 처음 발명된 이래 4비트 프로세서의 개발까지 25년이 걸렸고 인텔이 트랜지스터 수백만 개를 탑재한 펜티엄 프로 칩이 소개될 때까지 25년이 추가로 필요했다는 사실을 환기하는 것도 도움이 된다. 하드웨어는 물리적 시간이 필요하다. 양자도 예외가 아니다.

하지만 분명 양자의 시대가 오고 있다. 기업 매니저라면 양자로 인해 어떻게 디지털 분야 투자가 늘고 업계가 재편되며 혁신이 촉발될지 미리 생각해도 절대 이르지 않다. 양자 때문에 당장 새로운 비즈니스가 창출되거나 몰락할 일은 없겠지만 오늘날 양자를 응용한 기술을 확실히 이해해두면 알맞은 포지셔닝을 할 수 있어 향후 10년 동안 이익을 거두고 재앙을 피할 수 있다.

## 양자 컴퓨터란 무엇인가?

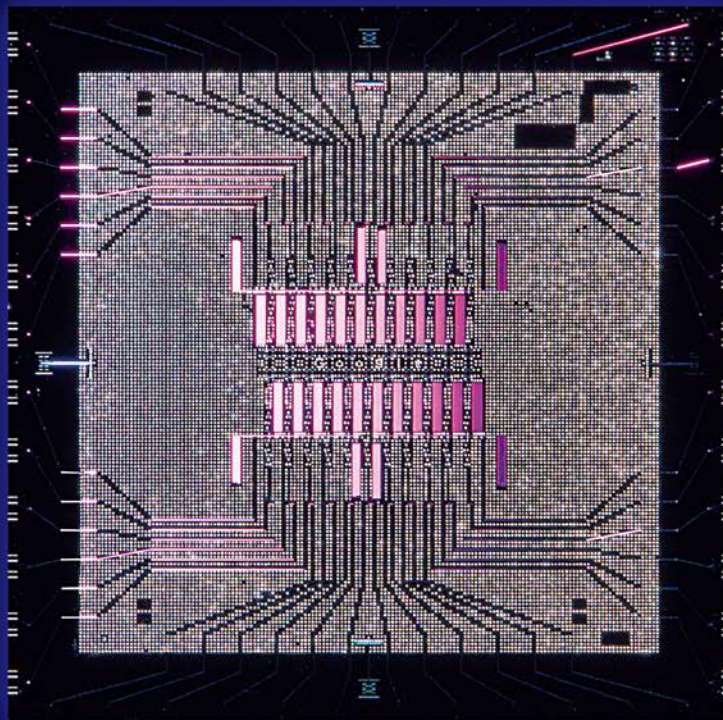
양자 역학의 법칙이란 물질과 빛이 원자<sup>atomic</sup>와 그보다 작은 아원자<sup>subatomic</sup> 입자 수준에서 어떻게 움직이는지를 연구하는 과학의 한 학문으로 MRI, 레이저, 원자시계, 나노 현미경 등등 혁신 기술의 핵심 원리다. 양자 역학을 바탕으로 컴퓨터를 개발하기 위해서는 완전히 새로운 기술을 습득해야 한다. 바로 양자 세계의 움직임을 정밀하게 제어하는 동시에 양자 특유의 ‘괴상한’ 본질을 유지하는 기술이다. 이는 성공하기 매우 어려운데, 광자와 전자 등의 양자는 극도로 섬세하고 불안정하며 움직이는 모습이 우리가 기존에 알던 물리 세계가 돌아가는 방식과 완전히 다르기 때문이다. 하지만 정확하게 통제할 수만 있다면 이런 반직관적인 양자의 행동은 버그가 아니라 기능으로 이전에 할 수 없던 일을 가능하게 해준다.

양자 컴퓨터 상용화의 가장 큰 암초는 큐비트의 중첩 상태를 오래 유지하지 못하는 데 있다. 진동, 온도 등 외부 환경이 조금만 바뀌어도 양자 역학의 중첩 현상은 금세 사라져 오류가 발생한다. 현재 큐비트를 이용하면 오류 발생률이 높아서 알고리즘의 실행 시간도 제한적이다. 이에 과학자들은 다수의 불완전한 물리적 큐비트를 연결해 오류를 보정하는 ‘논리적 큐비트<sup>Logical Qubit</sup>’를 구축하기 위해 노력하고 있다. 이렇게 하면 상업용 양자 어플리케이션을 사용하는 데 필요한 시간만큼 큐비트를 유지할 수 있다. 한 개의 논리적 큐비트를 만들려면 대개 약 1000개의 물리적 큐비트가 필요하다. 오늘날 가장 앞서나간다는 양자 컴퓨터에는 50~100개의 물리적 큐비트가 존재한다.

최근 몇 년 사이 기업들이 보다 적극적으로 양자 컴퓨터 개발에 힘쓰고 있다. 테크기업인 IBM과 구글은 양자 컴퓨터 분야를 낙관적으로 전망해 향후 2년 안에 논리적 큐비트를 실증할 수 있다고 보고 있다. 트랜지스터 기반의 컴퓨터도 단숨에 상업화에 성공하지 못했듯이 양자 컴퓨터도 논리적 큐비트가 증가하고 오류 발생이 감소하면서 차츰차츰 상업화가 가능해질 것이다.

## 기업은 어떻게 양자 컴퓨터를 활용할 수 있을까?

가까운 시일 안에 양자 컴퓨터를 개발하거나 소유할 회사는 거의 없다고 봐야 한다. 그 대신 비교적 적은 수의 전문 기업이 등장해 양자 기계를 호스팅하고 일선 회사들은 비용을 지불하고 필요할 때마다 클라우





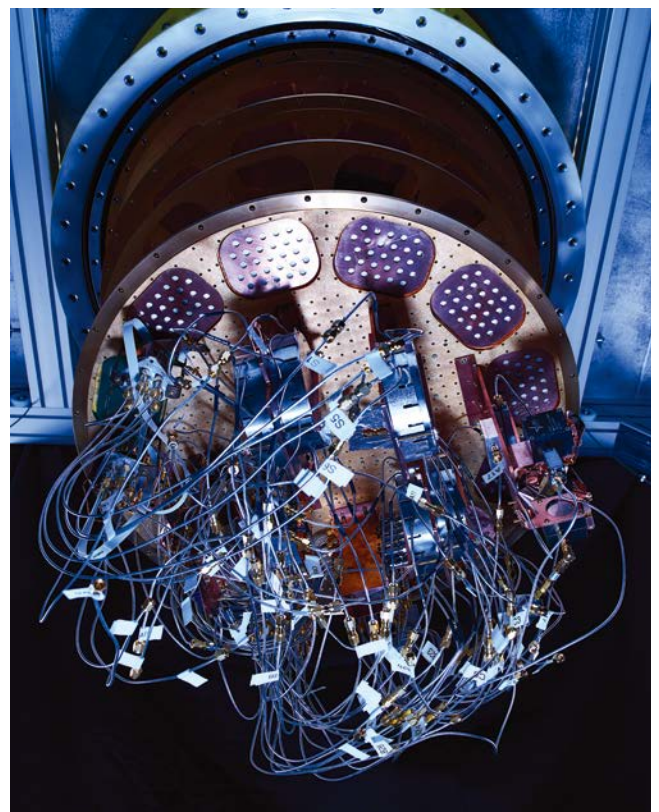
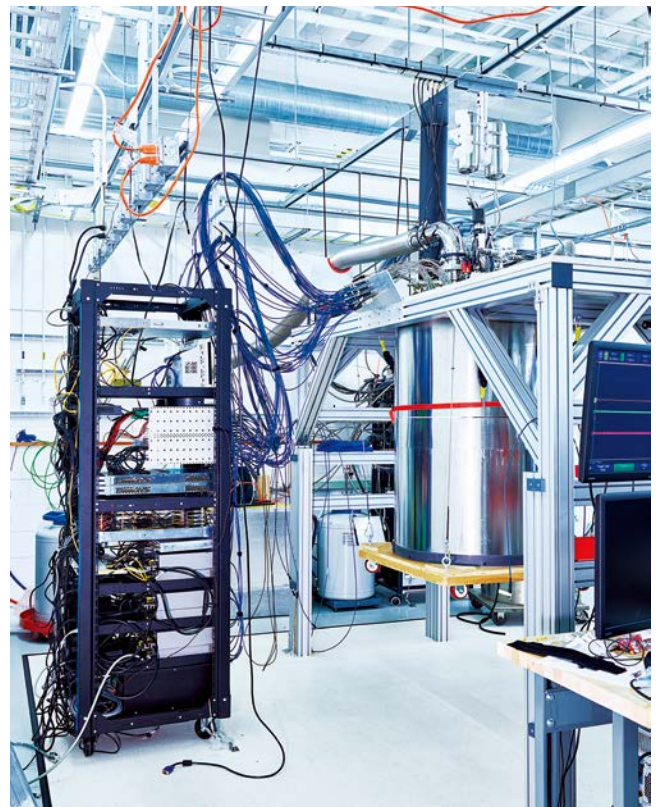


드 서비스에 접근하는 클라우드 컴퓨팅 스타일의 사업 모델이 등장할 것으로 예상된다. 아마존웹서비스<sup>AWS</sup>와 구글 클라우드<sup>Google Cloud</sup>, 마이크로소프트 애저<sup>Microsoft Azure</sup>의 클라우드 컴퓨팅을 기업에서 구축하는 현재의 방식과 유사할 것이다.(참고: 필자 중 윌리엄 올리버는 위 3개사와 함께 아티클에 등장하는 다른 회사들의 지원을 받아 연구하고 있다.) 양자 컴퓨터만 단독으로 사용하지 않고 업무별로 양자 컴퓨터든 고전 컴퓨터든 그때그때 가장 적합한 컴퓨터를 이용하는 하이브리드 방식이 등장할 것이다. 양자 컴퓨팅 클라우드 인프라 덕분에 리소스를 공유할 수 있게 되면서 규모의 경제를 통한 비용 감축과 접근성 제고가 가능해질 것이다. 이는 수요를 촉진하고 발전을 가속할 것으로 기대된다.

양자 하드웨어와 소프트웨어(알고리즘)가 같이 발전하면서 알고리즘 설계 전문가에게 자기 아이디어와 가정을 실험하고 반복할 기회가 생긴다. 또한 상업용 머신을 개발한 다음 테스트까지 몇 년을 기다릴 필요 없이 기존의 알고리즘을 개선해 새로운 알고리즘을 만들 수 있을 것이다.

양자 알고리즘은 기존 컴퓨터에서 사용하는 알고리즘과 매우 다르다. 비즈니스 프로세스에 적용할 가능성이 큰 알고리즘은 크게 다섯 개로 나뉜다. 어떤 알고리즘은 잘 활용하면 일상적인 업무를 더욱더 빠르게 처리할 수 있게 하고, 어떤 알고리즘은 우리에게 새로운 지평을 열어줄 것이다.

**I** **시물레이션.** 리처드 파인만<sup>Richard Feynman</sup>과 폴 베니호프<sup>Paul Benioff</sup> 같은 양자 분야의 선구자들이 양자 컴퓨터를 최초로 구상하던 때 그들은 이를 통해 자연의 법칙에 얹힌 비밀을 밝혀낼 수 있으리라 믿었다. 그 비전이 현실로 되는 순간을 지금 우리는 목격하고 있다. 이를테면 대기 중 존재하는 질소를 흡수해 암모니아 같은 질소화합물을 만드는 식물의 질소 고정<sup>nitrogen fixation</sup> 과정처럼 강한 상관관계가 있는 전자 100개의 화학 반응을 모델링하는 것은 아무리 성능이 뛰어나도 고전 컴퓨터로는 불가능하다. 하지만 2017년 스위스 취리히연방공과대<sup>ETH Zurich</sup> 이론화학 교수 마르쿠스 라이허<sup>Markus Reiher</sup>가 이끄는 연구팀이 주어진 과제를 처리하는 데 필요한 양자 시스템의 규모를 계산해 실제로 적용이 가능한 방법을 소개했다. 연구팀에 따르면 각각 약 100개의 논리적 큐비트로 구성된 최신 컴퓨터를 이용하면 주어진 목표를 달성할 수





## 양자 시뮬레이션으로 효율이 좋은 배터리 화합물을 발견하는 등 신소재 화학 분야의 문제들을 해결할 수 있다면 지구 온난화 문제를 더 효과적으로 대응할 수 있다.

있다. 자연의 과정을 모방해 획기적인 혁신에 성공한 경우는 수도룩하다. 아래 대표적인 사례를 3개 소개한다.

→ **화학**. 1900년대 초 프리츠 하버(Fritz Haber)와 카를 보슈(Carl Bosch)는 대기 중 질소와 산소를 이용해 직접 암모니아를 합성하는 질소 고정 공정을 개발했다. 이 합성법은 지금도 농작물 비료를 제조하는 데 사용하고 있으며 덕분에 수십억 명이 먹을 식량을 생산하고 있다. 한 세기도 전에 나왔다는 게 신기할 정도지만, 이제는 우리에게 막대한 부담을 부여하고 있다. 현재 하버-보슈 공정은 전 세계 에너지 소비량의 1~2%, 이산화탄소 배출량의 1.4%를 차지한다. 이런 문제를 바로 잡을 수 있다. 양자 컴퓨터가 도움이 될 것이다.

가령 자연에서 얻은 효소를 활용하면 훨씬 적은 에너지를 사용해도 하버-보슈 공정을 이용했을 때와 같은 결과를 얻을 수 있다. 안타깝게도 고전 컴퓨터로는 효소를 형성하는 화학 반응을 정확히 모델링하기는 무리다. 양자 컴퓨터로는 언젠가 가능한 일로, 이는 화학 기업에 비료와 기타 화학제품을 더욱 에너지 효율적인 방식으로 제조할 새로운 기회를 선사한다.

→ **에너지**. 관성 가둠 핵융합(Inertial Confinement Fusion, ICF)은 중수소와 삼중수소로 이뤄진 연료 펠릿에 고출력 레이저를 압축시켜 적절한 조건에서 고온의 열을 생성하도록 하는 방식이다. 이론적으로 관성 가둠 방식에서 방출되는 에너지량은 레이저의 에너지 사용량보다 에너지원으로 사용하기 좋다. 이를 현실에 구현하기 위해서는 관성 가둠 과정에서 발생할 수 있는 수많은 변수를 극도로 정교하고 정확하게 배치해야 하는데, 고전 컴퓨터로는 성공한 경우가 매우 적다. 구글 엔지니어링 디렉터 하르무트 네벤(Hartmut Neven)은 양자 컴퓨터로 더 나은 원자로를 설계할 수 있어 풍부하고 깨끗한 에너지를 손에 넣을 수 있을 것이라 주장한다.

→ **생명과학**. 2018년 하버드대 화학자 3명은 신약 개발 과정에 양자 컴퓨터를 활용할 수 있다는 내용의 논문을 발표했다. 논문에는 양자 컴퓨터 기술이 어떻게 더 빠르고 더 정확하게 분자 구조를 규명해 상당한 발전을 이뤄낼 수 있는지에 대한 설명이 담겨 있다. 같은 해 이들은 양자 애플리케이션 스타트업 자파타(Zapata) 컴퓨팅을 공동 설립해 벤처캐피털리스트로부터 지금까지 6500만 달러 이상을 조달했다.

실험실의 실험관이 아니라 컴퓨터로 새로운 분자를 얻고 싶어 하는 주체가 스타트업만은 아니다. 제약부문에서는 애브비(AbbVie), 바이엘(Bayer),

글락소스미스클라인(GSK), 다케다, 화이자 등등 17개의 제약업체가 큐팜(QuiPharm)이라는 컨소시엄을 만들어 양자 컴퓨팅 하드웨어와 소프트웨어의 발전에 박차를 가하기 위해 전문지식을 최대한 활용하고 있다. 2019년에는 바이오젠(Biogen)과 캐나다 양자 컴퓨팅 전문업체 1Q비트(1QBit)가 손잡고 양자를 이용한 분자 비교 기술을 개발했다. 이는 신약 개발 초기 단계에서 분자구조를 그래프 등으로 변환해 가상으로 비교해서 약 후보물질의 치료 효과를 예측하는 중요한 파트다.

양자 컴퓨팅으로 광합성 같은 화학 반응에도 새로운 인사이트를 얻을 수 있을지 연구하는 전문가들도 있다. 또한 양자 시뮬레이션으로 보다 효율 좋은 배터리 화합물이나 태양광 전지를 발명하거나 보다 에너지 효율적인 송전선의 개발 등 신소재 화학의 골치거리를 해결할 수 있다면 지구 온난화 문제에도 더 효과적으로 대응할 수 있다.

## 2

**선행방정식**. 현재 우리가 쓰는 컴퓨터 상당수가 공학, 금융, 화학, 경제, 컴퓨터과학 분야에서 선행방정식을 핵심으로 한다. 양자 컴퓨터를 활용하면 선행방정식의 해의 추출에서 비약적인 발전을 이룰 수 있다.(우리 MIT 동료 과학자들이 공동 개발한 HHL 알고리즘이 대표적이다.) 양자 컴퓨터로 선행방정식을 응용한 기술 중 많은 기대를 한몸에 받는 분야가 머신러닝의 강화학습이다. 신경망은 인간 두뇌의 작동 방식을 참고해 컴퓨터 프로그램이 특정 작업을 수행하도록 학습시키는 방법으로 최근 이런 신경망을 채택해 다양한 어플리케이션을 가동하는 경우가 급증했다. 컴퓨터 모델의 강화학습 수요가 증대한 것도 영향을 줬다.

추천 알고리즘을 예로 들어보자. 넷플릭스는 아카이브에 있는 모든 영화에 대한 모든 구독자의 기호 데이터를 대형 행렬로 모델링한다. 아직 시청하지 않은 영화를 회원에게 추천하기 위해서다. 양자 알고리즘을 이용하면 기존 컴퓨터보다 더 빠르고 더 정확하게 입맛에 맞는 콘텐츠 추천이 가능해진다. 특히 행렬의 크기가 클 때 유용하다.

또 다른 연립방정식 어플리케이션의 경우 인공지능 성능을 강화해 사진과 영상에서 유용한 정보를 끌어낼 수 있다. 이를테면 업계 대표 양자 기업들의 연구팀들이 최근 양자 컴퓨터와 기존 컴퓨터를 어떻게 함께 활용하면 원본 이미지와 영상을 만들어낼 수 있는지 설명하는 논문을 발표했다. 입증한 내용을 보면 이 어플리케이션은 생성적 적대 신경



망(generative adversarial networks, GAN)이라 불리는 머신러닝 기술을 활용해 손으로 쓴 숫자의 고해상도 이미지를 생성한 것을 알 수 있다. 당장은 초보적인 수준에 불과하지만, 언젠가 미 컴퓨터 애니메이션 스튜디오 픽사에서 그래픽 디자이너가 아니라 양자 컴퓨터로 만든 캐릭터와 배경이 등장하는 영화를 상영한다고 상상해보자. 그 밖에 양자 GAN 어플리케이션으로 건축에서는 3D 물체 제작, 게놈 연구에서는 합성 DNA 데이터 구축을 통한 항암제용 새로운 분자 생산 등이 있다.

선형방정식 알고리즘은 물론 다른 알고리즘에서도 나타난 문제로 데이터 로딩이 있다. 고전 컴퓨터에 있던 대량의 데이터를 어떻게 양자 컴퓨터로 전송할 것인가가 문제다. 이 문제를 해결하면 양자 컴퓨터의 상업화가 가속될 것이다.

### 3

**최적화.** 최적화 알고리즘은 주어진 시나리오에서 어떤 결정을 내려야 원하는 결과를 얻을 가능성이 큰지 밝혀낸다. 예를 들어 투자운용 매니저가 기대수익률과 리스크 사이 균형을 찾아서 클라이언트에 가장 적절한 은퇴 전략을 고르는 상황을 떠올려 보자. 양자 최적화 알고리즘을 이용하면 더 좋은 은퇴 전략들을 짤 수 있고 가장 알맞은 전략을 고르기 위해 계산하는 시간도 대폭 빨라진다.

2021년 5월 자파타는 스페인 최대은행 바코빌바오비스카야아르헨타리아 BBVA와 손잡고 양자를 이용해 신용가치조정(credit valuation adjustments, CVA)을 수행하면 실제 어떤 결과가 나오는지 공동 조사한 결과를 공개했다. CVA는 금융 부분의 시스템 리스크를 최소화하기 위해 도입한 규정이다. 주로 CVA 리스크 분석 표준 기술인 몬테 카를로(Monte Carlo) 시뮬레이션을 연구했다. 몬테 카를로 시뮬레이션의 연산은 복잡하고 고전 컴퓨터로는 오랜 시간이 걸리는데, 이는 신용 부도가 일어날 수 있는 광범위한 시나리오를 전부 고려해야 하기 때문이다. 자파타와 BBVA의 공동 연구에 따르면 차세대 양자 컴퓨터의 오류 수준률이 개선되면서 고전 컴퓨터보다 속도 측면에서 우위를 점할 것이다. 대형 은행은 이미 양자 분야 투자에 들어갔다. 골드만삭스와 JP모건 체이스, BBVA 모두 금융과 재무 분야의 양자 컴퓨팅을 활용 가능성을 연구하는 데 총력을 기울이고 있다.

그 밖에도 광범위한 업종이 최적화 알고리즘의 혜택을 누릴 수 있다. 최적의 공급망 경로나 제조 설비의 생산성에 좌우되는 기업이라면 실

적 개선에서 최적화가 얼마나 중요한지 이미 잘 알고 있다. 사실 최적화 문제 대부분은 고전 컴퓨터와 알고리즘을 통해서도 충분히 해결할 수 있다. 주행거리가 30km가 넘는 출퇴근길을 위해 최적화된 경로를 찾고 있다고 가정하자. 구글맵을 이용하면 굳이 힘들게 모든 대안을 시험할 필요 없이 최적 경로 근사치를 찾을 수 있다. 이때 구글맵이 완벽한 최적 경로를 안내하든 1분도 안 되는 짧은 시간에 안내하든 우리는 그다지 큰 차이를 느끼지 못할 것이다. 하지만 이보다 수행해야 하는 작업의 규모가 크거나 약간만 좋아져도 결과가 크게 달라지는 경우라면 양자 컴퓨팅 최적화 알고리즘이 가공할 만한 지각변동을 일으킬 수 있다.

### 4

**비정형 데이터 검색.** 고전 컴퓨터로 비정형 데이터베이스에

서 원하는 정보를 정확히 찾아내려면 일치하는 항목을 찾을 때까지 하나씩 검색하는 수밖에 없다.(비정형 데이터는 데이터 구조가 없어 그 자체만으로는 내용을 찾기가 어렵다.) 더구나 각각의 컴퓨터 검색 결과에서 그 이상의 정보를 읽어낼 수는 없다. 다시 설명하자면 이번 검색 결과가 불일치하더라도 다음 검색에서 불일치 결과가 나올 가능성이 줄지 않기 때문에 도움이 되지 않는다. 이는 컴퓨터 과학의 기초적인 문제 중 하나다. 원하는 정보를 더 빨리 찾고 싶으면 고전 컴퓨터 여러 대를 한 번에 실행해 각자가 하나하나 검색하도록 해야 한다. 양자 컴퓨팅을 통하면 더 빠르게 더 광범위한 데이터를 검색할 수 있다. 데이터베이스 검색 어플리케이션에는 인터넷 검색엔진과 신용카드 거래 실시간 처리, 심지어 외계 지적 생명체 신호를 발견하기 위한 전파 신호 탐사도 포함된다.

1996년 발표한 그로버의 알고리즘은 유명한 양자 검색 이론으로 컴퓨터가 방대한 규모의 비정형 데이터베이스에서 특정 정보를 찾는 방법을 대폭 개선해 이른바 서울에서 김 서방 찾는 격이었던 이 문제를 해결했다. 미생물학 발전에 크게 일조한 게놈 기술을 예로 들어보자. 유전적으로 발현하는 심장 질환을 식별하고 전염병 현황을 실시간으로 확인하고 감시하는 데 큰 도움을 줄 수 있다. 이 기술들을 이용하려면 많은 수의 고전 컴퓨터가 필요하다. 연구원이 참조 유전체(Reference genome)에 DNA 염기서열을 참조 게놈에 매핑할 때마다 고전 컴퓨터로 방대한 데이터를 검색해야만 한다. 그로버의 알고리즘으로 훨씬 더 빨리 검색할 수 있지만, 양자 컴퓨터를 상용화해야만 활용할 수 있다.





## 매니저라면 반드시 다음을 자문해봐야 한다. 우리 회사는 머신러닝과 기타 인공지능 기술을 주로 무슨 용도로 활용하는가? 양자 컴퓨팅이 이 분야에 얼마나 많은 도움을 줄까?

비정형 데이터 알고리즘은 앞서 거론한 문제에 더해 데이터 로딩으로도 골머리를 앓고 있는데, 이는 기존 컴퓨터에 있는 방대한 규모의 데이터를 양자 컴퓨터에 얼마나 효율적으로 입력하는지가 결정적이기 때문이다.

### 5

**소인수분해와 암호화.** 앞서 이야기했듯 현재 글로벌 인터넷

보안과 개인정보 보호 인프라의 상당 부분은 소인수분해를 기반으로 한다. 은행 잔고와 비트코인, 신용카드, 소셜미디어 계정 비밀번호, 그 밖에도 사이버 범죄의 먹잇감이 될 만한 부분을 보호할 때 소인수분해 문제를 이용하는데, 이는 가능한 모든 값을 무차별적으로 대입하는 고전 컴퓨터의 방식으로는 깰 수 없다.

양자 컴퓨터로 인해 패러다임의 전환이 올 것이다. 오늘날 우리가 의존하는 암호화 시스템을 한층 더 쉽게 해제할 수 있다. 2021년 4월 사이버 보안 표준 개발을 책임지는 미 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 “쇼어의 알고리즘을 사용할 수 있는 양자 컴퓨터를 언제 적국에 넘어갈지 예상할 수 없지만, 그때가 되면 공개키 암호 알고리즘으로 보호하던 모든 비밀키와 개인키는 물론 그 키로 보호하던 모든 정보가 유출될 것”이라고 경고했다.

사이버 범죄자가 암호를 풀 수 없더라도 암호화 형식의 데이터 자체는 힘들이지 않고 손에 넣는 예도 있다. 이를테면 인터넷업체를 해킹해 해당 업체를 이용하면서 발생한 모든 트래픽을 복사하면 된다. 해커가 암호화한 데이터를 구해 고도로 발달한 양자 컴퓨터가 출시돼 암호를 깰 수 있을 때까지 저장해 둔다고 생각해보자. 그때가 오면 모든 데이터가 공개될 것이다. 이런 상황을 미연에 방지하기 위해서는 대형 양자 컴퓨터가 상용되기 전에 양자 컴퓨터에 대항할 수 있는 새로운 암호 기술을 선제적으로 개발해야 한다.

고전 컴퓨터로 채용할 수 있는 소위 양자내성암호(postquantum cryptography)라 하는 사이버 보안 기술 개발이 한창 진행 중이다. 2016년 NIST는 양자 컴퓨터의 공격에 저항할 수 있는 알고리즘을 만들기 위해 공모전을 열었다. 최종 승자는 2022년에 발표할 예정이지만 양자내성암호 알고리즘을 개발한다 해도 새로운 암호시스템을 설치하는 과정에서 대대적인 소프트웨어, 하드웨어, 통신 인프라의 업그레이드가 필요하다. 기존 민감 정보도 모두 다시 암호화해야 하고 새로운 암호 알고리즘에 맞게 새

로운 인프라를 구축해야 한다.

기술 개발 노력으로 발생하는 경제적 영향은 막대할 것이다. 액센추어 양자 컴퓨팅 실무 책임자 칼 두카츠(Carl Dukatz)는 앞으로 양자내성암호로 전환하면서 나타날 대격변은 과거 미 정부와 기업이 1000억 달러 이상 써가며 진정시키려 했던 Y2K(2000년) 혼란 정도는 가볍게 압도할 것이라고 본다. 양자 컴퓨터의 공격에 취약한 인프라를 대형 양자 컴퓨터가 개발되기 여러 해 전부터 미리미리 개선할 필요가 있다. 1990년대 후반 Y2K 컴플라이언스에 따라야 했던 규제당국이나 감사기관이 요구하는 ‘양자 컴플라이언스’를 잘 준수하고 있음을 보여줘야 하는 미래가 머지않았다.

다행히 양자 컴퓨터가 전적으로 위협하거나 비용만 잡아먹는 부정적인 기술인 것은 아니다. 상상도 못 했던 기술이 우리를 기다리고 있으며 양자 시대에 본격적으로 돌입하기 전 나타난 보안과 암호 분야의 변화는 그저 시시한 소동에 지나지 않을 정도로 엄청난 기회가 쏟아질 것이다.

## 지금 매니저가 해야 하는 일은 무엇인가?

상업용 양자 컴퓨터가 아직 출시된 것은 아니지만 미리 대비해도 늦지 않다. 매니저는 ‘동향 주시하기’와 ‘구상하기’ 등 이 두 가지에 집중해야 한다.

동향 주시하기는 주요 기술이 얼마나 빠르게 발전하고 있는지 수시로 확인하는 것이다. 논리적 큐비트의 최초 실증, 오류 발생률 감소, 양자 컴퓨터의 상업적 우위 증명(단순히 기술적 측면만이 아니라 다른 면에서도 고전 컴퓨터보다 상업적으로 쓸모 있는지) 등이 대표적이다. 전문가 패널 등 보유한 자원을 이용하고 경쟁 결과를 예측해 진행 경과를 점검할 수 있다. 향후 수개월 내지는 수년 뒤에 양자 컴퓨터가 생각보다 빠르게 출현해 우리가 너무 보수적으로 생각했구나 싶을 수도 있다. 반대로 좀처럼 기술이 발전될 기미가 보이지 않는다면 기존 컴퓨터가 당분간 대체를 유지할 것이라는 뜻이다.


구상하기는 양자 컴퓨터로 우리 회사는 어떤 영향을 받을지 계획과 시나리오를 세우는 것으로 동향 주시하기와 동시에 진행한다. 단기적으로는 양자 컴퓨터의 함의를 잘 이해하면서 향후 회사의 니즈와 잠재적 강점, 약점을 찾을 수 있는 직원으로 구성된 팀을 만들어야 한다.

---

매니저라면 양자 컴퓨터란 무엇이고 이것이 회사에 어떤 영향을 줄 것인지 열심히 머리를 쥐어짜기 시작해야 하는 만큼 다음 질문에 대한 답을 구할 필요가 있다. 현재 기존 컴퓨터의 한계 때문에 회사가 영향받는 영역은 어디인가? 이 영역은 양자 알고리즘의 위 다섯 개 변화에 쉽게 적응할 수 있는가? 우리 회사는 주로 어떤 목적으로 머신러닝과 기타 인공지능 기술을 활용하고, 여기에 양자 컴퓨팅이 얼마나 도움을 줄까? 마지막으로 기초 수준에서 우리가 모델로 삼을 만한 생물 또는 화학 프로세스에는 무엇이 있는가?

**양자 컴퓨터 분야의** 선구자들은 양자 컴퓨터로 제일 먼저 자연의 비밀을 밝혀낼 수 있을 거라고 생각했다. 실제로 가장 흥미진진한 문제다. 21세기 전반의 어느 시점이 되면 이 문제를 다루게 될 것이다. 다른 많은 문제와 같이 말이다. ☺

---

 **조너선 루엔**(Jonathan Ruane)은 MIT 슬론경영대학원 글로벌경제관리그룹(GEMG) 강사이자 디지털경제 이니셔티브 연구원이다. GEMG는 다양한 분야의 전문가들이 모여 글로벌 비즈니스 환경을 연구하는 곳이다.

**앤드루 맥아피**(Andrew McAfee)는 MIT 디지털경제 이니셔티브 공동 창립자이자 공동 소장이다. 슬론경영대학원 책임연구원으로 있다.

**윌리엄 D. 올리버**(William D. Oliver)는 MIT 전기공학, 컴퓨터과학, 물리학 교수 겸 동대학 링컨연구소 펠로, 양자공학센터 소장, 전자공학연구소 부소장으로 재임하고 있다. 아마존웹서비스와 구글, IBM, 마이크로소프트, 자파타 등 여러 기업의 지원으로 연구를 계속하고 있다.

번역 노이재 에디팅 최한나