경제 성장을 늦추지 않고 양자 컴퓨터 도입

(2023.07.26., 양자정보연구지원센터)

□ 양자 컴퓨팅 발전 가속화

○ 상용 양자 컴퓨터 개발 경쟁 시작, 생산성 역설

- 재료 시뮬레이션, 고정 최적화, 머신러닝 개선의 혁신은 현재 디지털 컴퓨터처럼 사회를 변화시킬 수 있음에도 경제적 이익 제공 경로는 불확실함
- 장기적으로 양자 컴퓨팅 채택 기업은 경쟁 우위를 점해야 하지만 단기적으로 이 기계의 도입으로 상업적 가치 정도는 불확실함
- 1970년대, 1980년대 디지털 컴퓨터의 **생산성 역설**(효율성 제공 대신 생산성의 성장이 둔화), 기업은 핵심 프로세스와 비즈니스 모델 변경 등 많은 조정이 된 후 생산성 급격하게 증가

○ 양자 컴퓨터 혁명, 더 심각하고 고비용의 학습 곡선 예측

- 높은 통합 비용과 적은 단기 보상, 비즈니스 관리자 및 엔지니어를 위한 양자 개념 번역의 어려움, 양자 컴퓨터가 제기하는 암호화에 대한 위협

○ 사회적 문제에 대한 **양자 컴퓨터의 가치 입증**

- 기업은 초기 양자 컴퓨터를 채택, 기본 비즈니스 문제 해결하고 점진적으로 개선할 수 있으나, 추가 비용과 잠재적인 실패 가능성으로 위험 회피 가능, 안정적일 때까지 양자 컴퓨터 사용 연기
- 일상적인 작업과 계산 수행을 위해 디지털 컴퓨터가 필요, 양자 컴퓨터를 사용하여 더 복잡하고 전문적인 문제 해결, 하이브리드 프로토콜 및 프로그램 개발은 1970년대보다 훨씬 어려움
- 하이브리드 시스템은 디지털 비트와 양자 큐비트 모두에 능숙하며, 기존 데이터를 양자 상태로 또는 그 반대로 인코딩 가능해야 함, 두 가지 유형의 처리 장치 간 정보 전송을 위해 디지털 및

아날로그 신호 변환기가 필요함

- 양자 컴퓨터는 일반적으로 크기가 크고 극저온 냉각이 필요하므로 많은 기업은 인터넷을 통해 클라우드에서 원격으로 서비스 구매할 것임
- 신속한 기업 참여를 위해 상업적 이점을 실제로 입증, 민간 투자 유치를 위한 정부 자금이 필요함, 기업이 양자 컴퓨팅을 산업 및 사회적 큰 과제에 적용할 수 있도록 돕는 임무로 구성
- **경제학자**: 기업 투자 장려 위해 양자 컴퓨팅의 재정적 이점 평가 위한 프레임 워크 고안
- **연구자**: 양자 컴퓨터가 사회적 거대한 과제에서 디지털 컴퓨터를 능가할 수 있는 영역 식별부터 개념 증명 사례(proof-of-concept case) 구축, 비즈니스 모델과 관행 변경, 가치 사슬 따라 협력하는 방법 포함하여 기업이 양자 기술 채택을 위해 할 일 설정

o 공통 언어에 동의하고 이해 구축

- 현재 양자 컴퓨팅과 관련하여 과학자, 엔지니어 및 비즈니스 관리자 간 공유되는 언어가 없음, 오해와 혼동으로 지연 및 추가 비용 발생
- 관리자와 엔지니어는 양자 컴퓨터에 적합한 문제 유형 선택 및 문제 해결하고 필요한 정보 유형 및 양자 지원 형식으로 데이터 준비
- 양자 컴퓨터를 위한 공통된 의미론적이고 구문론적인 언어(디지털 컴퓨터 프로그래밍에 사용되는 표준화된 통합 모델링 언어와 유사한) 개발해야 함, 비즈니스 관리자에게 프로세스를 직관적으로 만들어 소프트웨어 개발 비용을 줄임
- 고전 언어와 유사하지만, 양자 정보로 작업할 수 있는 **양자 통합 모델링 언어** 통해 과학자, 엔지니어 및 관리자는 프로토타입, 테스트베드, 로드맵, 시뮬레이션 모델 및 하이브리드 정보 기술 아키텍쳐에서 동일 페이지 유지(예, 모듈식 워크플로 등장)

- 양자 컴퓨팅에 대해 대중과 소통 전략 필요함, 인지 편향과 학습 방식이 양자 컴퓨팅 채택에 미치는 영향 이해를 위한 연구 필요

ㅇ 보안 암호화를 통한 양자 인터넷 구축

- 양자 컴퓨팅은 정보 암호화에 널리 사용되는 프로토콜을 깨뜨릴 위험이 있으며, 위험을 해결하기 위해 추가 비용이 발생함
- 기업은 데이터 및 통신 보안을 보호하기 위해 암호화를 위한 새로운 수학적 접근 방식에 투자하거나 **양자 키 분배(QKD)*** 같은 양자 기반 통신 시스템을 사용해야 함

  ※ 양자 키 분배(Quantum Key Distribution): 광섬유 케이블 또는 자유 공간을 통해 전송된 큐비트 사용, 양자역학의 확률론적 원리 사용하여 발신자와 수신자 가 키 생성을 무작위화함, 해커가 전송 중인 큐비트를 관찰하려 하면 양자 상태가 영향을 받아 발신자와 수신자는 큐비트 변조를 알아챔

- 민감한 정부 데이터 및 통신에 대한 위협은 지정학적 문제를 야기할 수 있음, 양자 인터넷 구축을 위해 조정된 네트워크에서 양자 컴퓨터와 양자 통신 기술 통합하면 보안 위협을 극복하고 인터넷 생성
- 양자 인터넷은 양자 및 고전 링크 조합을 통해 원격 양자 장치 연결하는 네트워크로, 분산형 양자 컴퓨팅 가능
- 또한 새로운 비즈니스 모델 가능, 분산형 양자 컴퓨터와 블라인드 양자 컴퓨팅 프로세스는 독점 데이터 보존, 계산 후 공유 데이터가 삭제되도록 보장하면 머신러닝 향상
- 연구자: 더 빠른 계산, 강화된 개인 정보 보호 및 기밀성으로 데이터 및 정보 공유가 고객과 기업에 어떤 이점이 있는지 판단해야 함

(원문)

1. https://www.nature.com/articles/d41586-023-02317-x