국제금융센터

글로벌 은행권의 양자 컴퓨팅 활용 및 전망

이상원 | 글로벌은행부장(3705-6216)
황원정 | 책임연구원(3705-6156)

■ **[이슈] 올해 양자역학 탄생 100주년을 맞아 양자 컴퓨팅Quantum Computing 기술에 대한 관심과 기대가 커지고 있는 상황에서 은행 등 금융권의 활용 가능성을 점검**

■ **[잠재 활용 분야] 해외 주요 은행들은 ▲투자전략 및 포트폴리오 관리 ▲금융자산 거래(Pricing & Trading) ▲고객 신용평가 ▲사기 및 사이버 위협 탐지 등의 업무에 양자 솔루션의 잠재력을 실험**

○ (포트폴리오 관리) 양자 알고리즘은 다양한 매개변수와 다변량 모델의 동시 평가 능력을 갖추고 있어 은행은 이를 활용해 최적의 투자전략을 결정하고, 다양한 금융자산의 최적 조합을 찾아내 포트폴리오 리스크를 최소화하고 이익을 극대화

○ (금융자산 거래) 양자 컴퓨팅을 통한 복잡하고 다양한 데이터의 실시간 계산 및 처리 능력 향상은 금융자산의 가격책정Pricing과 매매Trading 효율성 개선으로 이어져 은행이 자본시장 부문에서 경쟁력을 높이는 기회를 제공

○ (고객 신용평가) 은행은 고객 채무불이행 가능성 예측 및 대손충당금 계산, 대출 승인 등의 과정에서 여러 변수를 다루고, 신속한 판단 및 낮은 오류가 요구되는 바 양자 컴퓨팅 기법이 신용평가 개선에 기여

○ (사기 탐지) 사기 수법과 사이버 공격이 고도화되는 상황에서 은행은 양자 기술을 활용해 비정상적 거래, 부정 행위 징후 등 계속 진화하는 사기 패턴은 물론 지능형 사이버 위협을 정확하고 신속하게 식별함으로써 피해를 최소화

■ **[평가 및 전망] 금융산업에서 혁신 잠재력이 큰 양자 컴퓨팅의 도입은 일부 대형은행들을 주축으로 개념증명Proof of Concept 등 초기 실험단계로 평가. 향후 양자 기술의 성숙화로 상용화 가능성이 열려 있는 만큼 기회와 리스크에 대한 선제적인 대비가 요구**

○ AI와 양자 기술의 융합(AQ)에 따른 시너지 효과로 인하여 물리적 세계뿐 아니라 디지털 세계에서 다양한 혁신적 활용 사례 창출이 기대

○ 그러나 현재 사용되는 암호화 기술이 양자 기반 해킹 등의 위협에 노출될 수 있으므로 양자방어 암호Quantum-Defense Cryptography 시스템 구축 등 대비 전략을 수립할 필요

□ **[이슈] 올해 양자역학 탄생 100주년[1]을 맞아 양자 컴퓨팅Quantum Computing 기술에 대한 관심과 기대가 커지고 있는 상황에서 은행 등 금융권의 활용 가능성을 점검**

[참고 1] 양자 기술Quantum Technology이란?

□ **(개념) 양자역학Quantum Mechanics의 기본 원리를 활용하여 정보의 생성, 전달, 저장 및 계산 방식을 혁신함으로써 기존의 고전적 기술로는 불가능한 복잡한 문제를 해결하려는 첨단 융합기술**

○ 모든 물리적 독립체의 최소 단위인 양자의 상태를 제어함으로써 기존 기술이 접근하기 어려운 수준의 계산 속도, 보안성 및 정밀도 달성

□ **(4대 양자 원리) ①중첩Superposition ②얽힘Entanglement ③간섭Interference ④측정Measurement**

○ ①중첩: 한 입자가 동시에 여러 상태에 존재할 수 있다는 성질. 기존 방식(정보를 0 또는 1이라는 불연속적 상태의 Bit 단위 처리)과 달리 Qubit는 정보를 0, 1 또는 0과 1의 중첩 처리

○ ②얽힘: 두 개 이상의 입자가 서로 강하게 연결되어 한 입자의 상태가 바뀌면 다른 입자도 즉시 영향을 받는 현상으로 이는 Qubit 크기의 기하급수적 확장을 가능

○ ③간섭: 서로 다른 양자 상태가 중첩되어 결과를 강화하거나 상쇄시키는 현상으로 계산 효율성 결정

○ ④측정: 양자 상태를 관측하는 순간 여러 가능한 상태 중 하나로 확정되는 성질

□ **(3대 응용 분야) ①양자 컴퓨팅 ②양자 통신 ③양자 센싱**

○ ①양자 컴퓨팅: 양자비트를 이용한 대량의 병렬 연산 수행. 가장 큰 성장 잠재력을 보유

○ ②양자 통신: 빛의 양자 현상을 이용한 통신 기술. 정보 해킹 원리적 차단 등 보안상 장점

○ ③양자 센싱: 양자 시스템을 이용해 대상의 물리적 성질을 분석 및 감지하고 계측. 초정밀 측정이 가능

자료: 외신종합

○ 작년 인공지능AI 기술이 산업 및 일상 전반에 본격적으로 통합·확산되기 시작했다면 금년 들어 양자역학이 '차세대 혁신 기술Next Breakthrough Technologies'로 부각

- 양자 컴퓨팅 상용화 기대 속에 `25년 노벨 물리학상이 양자기술 개발 기회를 제공한 미국 존 클라크 교수, 미셸 드보레 교수 및 존 마티니스 교수에 수여

  • `22년 노벨 물리학상 수상자인 프랑스 양자 전문가 알랭 아스페 교수 등이 설립한 스타트업 Pasqal은 200 Qubit 양자 컴퓨팅을 최초로 개발. `24년에는 1,000 Qubit 시연에 성공[2]

[1] 1925 년은 독일 물리학자 베르너 하이젠베르크가 미시 세계의 입자 운동을 설명하는 행렬역학을 발표해 양자역학의 수학적 기초를 세우고, 오스트리아 물리학자 에르빈 슈뢰딩거가 파동함수의 시간적 변화를 설명하는 슈뢰딩거 방정식을 발표하며 양자역학을 이해하는 핵심 기틀을 마련하는 등 양자역학이 새로운 물리학 체계로 태동한 시기. UN 은 양자역학 법칙 수립 100 주년을 기념해 2025 년을 세계 양자과학기술의 해 International Year of Quantum Science and Technology 로 지정

[2] 2024 년 12 월 Google Quantum AI 가 발표한 실험용 양자 컴퓨터 칩 Willow(105 Qubit)는 현 시점 가장 성능이 우수한 슈퍼 컴퓨터가 10.7 조년 걸리는 계산을 5 분만에 처리 가능

- 또한 양자 컴퓨팅 상용화에 신중하던 Nvidia의 CEO 젠슨 황도 지난 여름 동 기술이 '변곡점infection point'에 도달했다고 평가하며 우호적인 입장으로 선회

  • BofA는 양자 컴퓨팅이 영향력 면에서 AI를 능가한다고 평가하면서 이의 발전은 불의 발견이나 인터넷 발명과 같은 기술적 혁명에 비견. 향후 10년 가장 혁신적 기술 중 하나로 지목

○ 특히 은행 등 금융업의 경우 복잡성 증가, 데이터 집약적, 높은 최적화 수요 등의 특성 감안 시 향후 양자 컴퓨팅 도입의 이점이 큰 부문의 하나로 관심이 점증

- Forbes紙가 2025년에 주목해야 할 10대 은행/금융 기술 트렌드들 중 하나로 '양자금융Quantum Finance'을 지목

  • 금융서비스의 양자 컴퓨팅 도입에 따른 미래의 경제적 가치를 최대 $7,000억(`35년 McKinsey)~$8,000억(`40년 BCG)으로 추정(VS 화학 $3,240억/생명과학 $1,830억/자동차 $630억, McKinsey)

- 글로벌 50개 주요 은행들의 약 80%가 양자 기술 실험 및 전략적 투자 형태로 참여 중이며, 은행권의 양자 기술 전문인력 수도 `24.8월 이후 10% 증가(Evident)

  • Deloitte에 따르면 `32년까지 금융서비스 회사들의 양자 컴퓨팅에 대한 투자 규모가 $190억에 달할 것으로 예측

<표 1> 양자 컴퓨팅 발전의 3단계

1단계	이론적 연구 (1980년대~)	1980년대부터 양자 컴퓨팅의 이론적 연구가 시작되었고 이 시기에 양자 컴퓨팅의 기본 원리와 알고리즘이 연구
2단계	실험적 연구 (1990년대~)	1990년대부터 양자 컴퓨팅의 실험적 연구가 시작되고 양자 컴퓨팅의 원리를 활용하여 간단한 계산을 수행하는 실험적인 양자 컴퓨터가 개발
3단계	상용화 연구 (2000년대~)	2000년대부터 양자 컴퓨팅의 상용화 연구가 시작되어 다양한 기업들이 양자 컴퓨팅의 연구와 개발을 시작

자료: 삼성SDS

□ **[잠재 활용 분야] 해외 주요 은행들은 ▲투자전략 및 포트폴리오 관리 ▲금융자산 거래(Pricing & Trading) ▲고객 신용평가 ▲사기 및 사이버 위협 탐지 등의 업무에 양자 솔루션의 잠재력을 실험**

◎ 투자전략 및 포트폴리오 관리

양자 알고리즘은 다양한 매개변수와 다변량 모델을 동시에 평가할 수 있는 능력을 갖추고 있어 은행은 이를 활용해 최적의 투자전략을 결정하고, 다양한 금융자산의 최적 조합을 찾아내 포트폴리오 리스크를 최소화하고 이익을 극대화할 수 있음

○ **투자전략 정확도 향상**: 양자 컴퓨팅은 기존 전통 컴퓨팅 방식보다 복잡한 시장 역학 분석 등을 더욱 효율적으로 수행함으로써 정확한 통찰력을 제공할 수 있음. 이는 은행의 보다 효과적인 투자전략 수립으로 연결

- 은행은 양자 컴퓨팅을 도입하여 불확실한 상황에서 결과 예측에 사용되는 수학적 기법인 몬테카를로Monte Carlo 시뮬레이션을 초고속으로 실행할 수 있으며, 이는 금융 예측의 정확성 및 시기적절성(실시간 시장 예측) 향상에 기여

  • 몬테카를로 시뮬레이션은 방대한 변수를 다루기 때문에 많은 시간과 자원이 필요한데 양자 컴퓨터는 기존 슈퍼 컴퓨터로 처리하기 어려운 대규모 데이터 세트와 고도화된 모델을 다루는데 강점을 보유

○ **포트폴리오 최적화Optimization**: 자산 수가 많아질수록 조합 가능성이 급증하는 등 투자 포트폴리오 구성이 조합 최적화Combinatorial Optimization의 형태를 보이는 경우가 많아 은행은 경쟁력 강화 차원에서 양자 컴퓨팅 기술의 활용에 특히 주목

- 기존 알고리즘의 경우 자산배분 조합 변수가 많거나 제약조건이 복잡해질수록 효율성이 떨어지는 반면, 양자 컴퓨팅은 복잡한 포트폴리오 최적화 문제를 효율적으로 해결할 수 있는 강점을 보유

  • 양자 컴퓨팅의 경우 여러 경로를 동시에 탐색할 수 있는 능력을 구비하고 있기 때문에 조합 가능한 시나리오가 매우 많아 기존의 전통적 계산으로는 탐색 비용이 급증하는 문제와 비교해 우위

해외 주요 은행 사례 Ⅰ

☐ **(JPMorgan)** 2017년부터 몬테카를로 시뮬레이션 등 포트폴리오 최적화를 가속화하고자 IBM과 양자 컴퓨팅 소프트웨어 테스트

○ `23.3월 양자 컴퓨팅 업체 QC Ware와 함께 발표한 논문에서 시장 마찰Market frictions 및 트레이딩 제약요인Trading constraints을 고려한 포트폴리오 리스크 완화 전략을 양자 컴퓨팅 기법으로 연구

- 기존의 딥 헤징Deep hedging 프레임워크에 양자 딥러닝Quantum deep learning을 적용해 학습 효율이 향상되는지 점검하고, 양자강화 학습Quantum reinforcement learning 기반의 새 프레임워크를 제안

○ `24.10월 양자 하드웨어(Trapped-ion 양자 컴퓨터) 상에서 소규모 포트폴리오 최적화 문제를 실행했다고 게재

☐ **(Ally Financial)** 양자 솔루션 업체 Multiverse Computing과 컨설팅사 Protiviti와 협력 하에 양자 컴퓨팅을 활용해 금융지수 추적Index tracking을 강화하는 새로운 알고리즘을 개발하는 등 투자 포트폴리오 구축에 관심

○ 적은 주식(나스닥 100 펀드의 종목 수는 기존 포트폴리오 대비 4배 하회, S&P 500 펀드의 종목 수는 10배 하회)을 사용해 기존 포트폴리오와 동일한 수익률로 투자 포트폴리오를 자동으로 최적화하는 방안을 도출. 포트폴리오 최적화 시간도 기존 최대 30시간에서 즉시 실행으로 크게 단축

☐ **(NatWest)** Fujitsu가 조합 최적화 문제 해결을 위해 개발한 양자 솔루션 Digital Annealer(1 Qubit 소프트웨어 구동)를 활용해 은행 관리자가 고품질 유동자산 포트폴리오에 적합한 구성을 결정할 수 있도록 실험

○ 기존 컴퓨터보다 300배 빠른 속도와 높은 정확도로 포트폴리오 배분을 완료

☐ **(Barclays)** 포트폴리오에서 자산 수 120,000개 이상, 제약조건 20개 수준의 문제까지 양자 컴퓨팅이 적용 가능하다며 응용 가능성 언급

☐ **(BMO)** IBM Quantum Network*에 캐나다 은행 중 최초로 가입하고, `25년말까지 양자 컴퓨팅 기술을 활용해 새로운 양자 기반 솔루션을 개발하는 목표를 제시. 초기 중점 추진 분야는 복잡한 투자 포트폴리오 전략을 최적화하는 새로운 접근법을 개발하는데 있음

* 은행권에서는 JPMorgan, Wells Fargo, Goldman Sachs, Truist, Barclays, BMO, MUFG, Mizuho 등이 참여

◎ 금융자산 거래(Pricing & Trading)

양자 컴퓨팅을 통한 복잡하고 다양한 데이터의 실시간 계산 및 처리 능력 향상은 금융자산의 가격책정$_{Pricing}$과 매매$_{Trading}$ 효율성 개선으로 이어져 은행이 자본시장 부문에서 경쟁력을 높이는 기회를 제공

○ **Pricing 경쟁력 제고**: 자산의 Pricing 과정에서 확률 모델링, 수치 해법, 몬테카를로 시뮬레이션 등이 통상 사용되는데, 양자 컴퓨팅이 전통 방식보다 이를 훨씬 빠르고 정확하게 실행할 수 있어 유리

- 특히, 옵션 등 복잡한 파생상품의 Pricing 과정에서 양자 몬테카를로 방식을 적용한 표본수$_{sample}$ 축소 또는 계산 속도 향상이 기대

  • 다만 현재 양자 컴퓨팅 도입은 규모, 오류 등의 한계로 인하여 단순 옵션이나 자산 수가 제한적인 것부터 시작하는 것이 현실적

○ **Trading 전략 향상**: 여러 시장 변수와 거래조건을 고려할 때 양자 기술의 대표적 특성(중첩$_{Superposition}$ + 얽힘$_{Entanglement}$ → 병렬$_{Parallel}$ 연산)이 기존 컴퓨팅 방식보다 잠재적으로 시장 탐색을 더 빠르고 효과적으로 실행시킬 수 있어 자산의 Trading 전략에 적합

- 특히, 복잡한 데이터 세트를 즉시 처리할 수 있는 양자 컴퓨팅의 능력은 알고리즘$_{Algorithmic}$ 및 고빈도$_{High-Frequency}$ Trading 분야에서 유망

해외 주요 은행 사례 II

☐ **(Goldman Sachs)** 영국 스타트업 Quantum Motion과 다양한 시장동향, 변동성 및 시간 민감성에 따라 결정되는 옵션의 Pricing 모델을 개선하는 효율적 양자 알고리즘을 개발

☐ **(HSBC)** IBM과 공동으로 진행한 양자 컴퓨팅 시범 사업에서 유럽 장외 회사채 시장에 Heron 양자 프로세서를 적용한 결과 훨씬 더 정확한 호가로 주문이 체결될 가능성이 기존 방법 대비 최대 약 34 % 개선된 것으로 판명

○ 양자 컴퓨팅 알고리즘을 사용하여 경쟁 입찰 과정에서 실시간 시장 상황과 리스크 추정치를 고려해 고객 문의에 대한 가격을 신속하고 자동으로 책정. 매매 예측력 향상은 궁극적으로 마진 증가와 유동성 증대를 의미

☐ **(BBVA)** 스위스 양자 컴퓨팅 업체 Terra Quantum과 공동으로 양자 컴퓨팅을 활용한 변종$_{Exotic}$ 파생상품의 Pricing 속도와 정확도를 향상시킬 수 있는 시범 테스트를 성료

○ 0.001초(ms) 수준의 Pricing과 표준 CPU 하드웨어 대비 약 260배 더 빠른 추론$_{Inference}$이 가능해짐에 따라 계산 및 비용 효율성이 향상

☐ **(Intesa Sanpaolo)** 파생상품의 Pricing에 양자 응용 프로그램을 적용하는 방안을 연구

☐ **(MUFG)** 일본 스타트업 Groovenauts(발행 주식의 약 18% 지분 인수)의 양자 컴퓨팅 기술인 Quantum Annealing을 활용해 다양한 변수의 조합을 분석하고 최적의 해법을 찾아 파생상품의 Trading 효율성을 개선할 계획

◎ 고객 신용평가

은행은 고객의 채무불이행 가능성 예측 및 대손충당금 계산, 대출 승인, 금리 산정 등의 과정에서 여러 변수(재무·비재무 정보, 거시경제 및 시장 지표 등)를 다루고, 신속한 판단 및 낮은 오류가 요구되는 바 양자 컴퓨팅 기법이 신용평가 개선에 기여할 것으로 기대

○ 양자 알고리즘은 비전통적 데이터와 복잡한 행동 지표를 분석하여 신용이 낮거나 서비스가 부족한 대출자에 대한 모델링을 개선하고, 은행이 새로운 고객층에 대한 책임 있는 대출을 확대하는 데 도움이 될 것임

- 특히, 기업금융 분야에서 담보 최적화, 채무불이행 확률 추정, 유동성 관리 개선 등을 위해 양자컴퓨팅 기술을 시험

  • 일례로 중소기업 대출 등 데이터가 충분치 못한(few-shot) 제약조건 하에서도 양자 강화 모델 및 양자 머신러닝$_{QML}$이 새로운 가능성을 탐색

해외 주요 은행 사례 Ⅲ

☐ **(Barclays)** IBM과 파트너십을 맺고 신용 리스크 분석 및 담보 관리 분야에 중점을 두고 양자 컴퓨팅을 활용하는 방안을 모색

☐ **(Crédit Agricole)** 양자 기술 기업 Pasqal과 전략적 협력관계를 체결하고 양자 컴퓨팅을 활용한 신용등급 하락 예측에 관한 연구 논문을 발표

○ 또한 양자 컴퓨팅 업체 Quandela와 혁신적인 Hybrid classical-quantum algorithm을 공동 개발함으로써 기존의 컴퓨팅 방식 대비 신용 리스크 모델의 예측 성능이 향상

☐ **(Intesa Sanpaolo)** 신용평가에 양자 응용 프로그램을 적용하는 방안을 연구. 양자 알고리즘이 채무불이행 예측 모델의 정확도를 향상시키고 불확실성을 정확하게 정량화할 수 있도록 지원

☐ **(Yapı Kredi)** 4,297개 중소기업 고객을 대상으로 한 재무위험 분석 모델에 양자 컴퓨팅 기술을 도입. 향후 최대 600,000개 기업고객을 대상으로 적용 범위 확장이 목표

○ 약 17,000개의 제약조건을 포함한 복잡한 기업관계 네트워크(거래, 채무관계, 공급망 등)를 대상으로 양자 컴퓨팅을 이용해 한 기업의 재무위기가 다른 기업에 어떤 영향을 미치는지 전염위험Contagion risk을 예측하는 모델을 구현하고 약 7초 만에 해당 분석을 수행

◎ 사기 및 사이버 위협 탐지

사기 수법과 사이버 공격이 고도화되는 상황에서 은행은 양자 기술을 활용해 비정상적 거래, 부정 행위 징후 등 계속 진화하는 사기 패턴은 물론 지능형 사이버 위협을 더욱 정확하고 신속하게 식별함으로써 피해를 최소화할 수 있음

○ 사기 탐지 품질 향상: 기존의 사기 탐지 방식을 양자 알고리즘 모델로 대체 및 강화함으로써 작업 속도와 정확성을 높일 수 있음. 특히 고객신원확인KYC 및 자금세탁방지AML 부분의 활용 잠재력에 주목

- 최소 3년 내 현재 최고 수준의 컴퓨팅 보다 사기탐지 능력을 15% 높이는 양자 알고리즘이 출현할 가능성(Oxford Quantum Circuits)
  - 양자 컴퓨팅은 금융사기 탐지 능력을 향상시켜 은행들이 매년 $100억~$400억에 달하는 손실을 줄이는 데 기여할 것으로 기대(AWS)
- 향후 양자 검색Quantum search 기능은 암호화된 데이터 세트에 대한 확인 속도를 높여 KYC를 강화. 이는 은행의 컴플라이언스 및 고객 경험 향상에 도움

- 양자 컴퓨팅은 현재 금융서비스 업계에 매년 수십억 달러의 비용을 초래하는 컴플라이언스 프로세스를 획기적으로 간소화시켜 줄 것으로 기대(UK Finance)
- 양자 컴퓨팅을 활용한 KYC 기능 강화가 금융회사의 보다 타겟팅되고 개인화된 고객 마케팅 및 홍보 활동에 기여할 가능성(Guidehouse)

- 아울러 자금세탁의 경우 다중 계정 및 여러 국가에 분산되어 복잡한 네트워크를 형성하고 있어 양자 알고리즘이 이를 빠르게 분석해 은닉된 금융범죄 클러스터 등을 찾아내는데 유용

○ <u>사이버 공격 감지 강화</u>: 양자 알고리즘은 빈번해지고 지능화되는 사이버 공격의 위협에 대해 기존 컴퓨팅 기술보다 더 빠르게 사이버 보안 위협을 탐지함으로써 신속한 대응이 가능

- 양자 암호화로 인코딩된 금융 데이터는 상태를 변경하여 모양을 바꾸고 도청을 방지하기 때문에 해커 등 외부에서 접근이 힘들고, 그 결과 여타 디지털 보안 방식보다 훨씬 더 안전

해외 주요 은행 사례 Ⅳ

☐ **(HSBC)** 미국과 영국의 합작사인 Quantinuum과 양자 컴퓨팅의 사기 탐지 활용, 사이버 보안 등의 활용에 초점을 두는 다단계Multi-stage 프로젝트를 공동 추진

○ 우선 순위로 두고 있는 사기 탐지 부문에서 양자 머신러닝QML, 양자 자연어처리QNLP 등의 기술을 적용해 기존 대비 향상된 탐지 정확도 및 복잡한 데이터 패턴 인식력 확보를 모색

○ Quantinuum의 Quantum Origin 플랫폼을 사용해 기존 인프라에 양자 알고리즘을 적용하여 거래를 보호하고 KYC 프로세스를 강화하는 암호화 키를 생성할 예정

☐ **(Intesa Sanpaolo)** 사기 탐지의 정확도, 속도 및 적응성 측면에서 기존의 머신러닝 방식을 능가하는 변형 양자 컴퓨팅Variational Quantum Computing: VQC 솔루션을 성공적으로 구현함으로써 비용 절감 및 고객 경험 개선에 도움

○ VQC의 사기 탐지율(92%)이 기존 솔루션 대비 9%p 향상. 이는 연간 수백만 달러의 사기 손실 방지를 의미

○ 사기 탐지 시 1종 오류False Positive Rate*(2.3%)의 문제도 기존 방식(5.1%)대비 크게 개선. 그 결과 연간 약 280만건의 1종 오류가 감소해 사기 관련 수동 검토 비용이 약 840만 유로 절감. 또한 사기 관련 고객 서비스 문의가 14% 감소하고, 만족도 점수는 3.2p 증가

* 모델이 실제로 부정적Negative 상황인데 긍정적Positive이라고 잘못 예측한 경우

□ **[평가 및 전망] 금융산업에서 혁신 잠재력이 큰 양자 컴퓨팅의 도입은 일부 대형은행들을 주축으로 개념증명Proof of Concept 등 초기 실험단계로 평가. 향후 양자 기술의 성숙화*로 상용화 가능성이 열려 있는 만큼 새로운 기회와 함께 수반되는 리스크에 대한 선제적인 대비가 요구**

* BCG는 2035년 경 양자 컴퓨팅 시장이 성숙기에 진입할 것으로 예측

<양자 컴퓨팅의 미래>

○ 현재 양자 컴퓨팅 기술은 실질적 응용 상태에는 도달하지 못한 상황. 양자 우위Quantum Advantage 도달* 및 양자 컴퓨팅 상용화를 위해서는 △기술적 난제 극복 △지속적인 연구개발 투자<p.13 [참고 2] 주요국의 양자 컴퓨팅 투자 및 정책> 등이 관건

* 기존 컴퓨터가 현실적인 시간 내에 해결할 수 없는 문제를 양자 컴퓨터가 지속적으로 처리할 수 있는 능력을 갖추게 되는 양자 우위 도래 시점은 IBM `26년말, BofA `33년, Meta `34년 등으로 다양한 예측 존재

- 지난 2월 핀란드 중앙은행이 발표한 자국 내 영업 중인 약 30개 금융기관들을 대상으로 한 양자 기술 관련 서베이 결과, 이들의 10%가 양자 컴퓨팅 활용에 대한 실험 및 시범 운영을 진행하였고, 13%는 내년에도 이를 계획 중이라고 응답
  - 다만 이들 가운데 20%는 적어도 현재로서는 양자 기술이 자신들의 비즈니스에 어떤 이점도 가져다주지 못할 것이라며 신중한 입장
- 양자 컴퓨터가 기존 슈퍼 컴퓨터와 하이브리드 통합 등의 형태로 점진적인 도입이 예견되는 가운데, 양자 기술 전문가들의 75%가 `35년까지 완전 범용Fully fault-tolerant 양자 컴퓨터가 구현될 것으로 전망(QuEra Computing, McKinsey)
  - 실제로 금융업에서 대규모 문제들을 해결하기 위해서는 수천~수백만개의 Qubit가 필요하기 때문에(Barclays) 양자 시스템이 금융업계에 전면 채택되려면 적어도 5~10년이 필요할 것으로 예측(HSBC, Medium)

    ※ 참고로 IBM은 2033년까지 10만 Qubit의 기술을 갖춘 양자 컴퓨터 개발을 목표로 제시
- 양자 컴퓨터의 주요 기술적 과제로 △Qubit의 부정확성 문제 △초저온/초전도 운영 환경 △양자 전문 인력 부족 등이 상존<표 2>. 이의 극복을 위해서는 오류 정정Error-corrected 논리적 Qubit의 개발 등이 중요(Citi)
  - BofA는 `24년 기준 $3억으로 추산되는 양자 컴퓨팅 시장이 `30년초 $40억으로 고성장할 전망이며, 기술적 장벽 극복 시 예측치가 이를 크게 상회할 가능성도 제기. Fortune紙의 `32년 글로벌 양자 컴퓨팅 시장($126.2억)에 대한 낙관적 예측에 주목

<표 2> 양자 컴퓨팅의 주요 기술적 과제

과제	내용
양자 상태의 본질적인 불안정성	* 양자 얽힘Entanglement을 유지하는 기술적 어려움으로 인하여 Qubit가 점점 더 많아질수록 비일관성, 즉 "잡음"이 발생 - Qubit는 유용한 계산을 수행할 때 양자 입자간 연결 상태를 단 몇 분의 1초의 매우 짧은 시간만 유지 * 외부 환경의 "간섭"으로 양자 상태가 파괴될 시 양자 시스템이 양자 속성을 잃고 기존의 컴퓨팅 시스템처럼 동작하는 'Decoherence' 문제 발생 - Qubit의 상태가 변하면 입력이 손실되거나 변경될 수 있으며, 이는 결과의 정확도 저하로 연결 **⇒ 양자 컴퓨팅 시스템의 계산 오류율 등 부정확성 문제 발생** **- 효과적인 오류 정정 기술을 개발하는 것이 양자 컴퓨터의 지속적인 발전에 필수적(UBS)**
초저온/초전도/고진공 운영 환경 필요	* 양자 컴퓨팅의 구동을 위해서 영하 273°C 유지 위한 냉각 시스템과 전기저항 0이 되는 초전도 상태 등이 필수로 시스템 제어 비용 부담 상당 **⇒ 양자 컴퓨터 시설 구축 및 전력 공급 등 유지·관리비 부담으로 소규모 조직의 기술 접근성 제한, 단기 투자수익률ROI 저하 등이 불가피**
양자 기술 전문가 부족	* 양자 컴퓨팅에 대한 기업의 수요와 이를 충족할 수 있는 양자 전문가 수 사이에는 큰 격차가 존재하는 등 숙련된 전문가가 전세계적으로 부족 - McKinsey에 따르면 양자 관련 일자리 3개당 자격을 갖춘 양자 관련 지원자는 단 1명에 그친 것으로 조사. 양자 관련 인재 풀이나 일자리 창출 예측 속도에 큰 변화가 없다면 `25년 양자 일자리의 절반 미만만이 채워질 가능성 - 은행권 양자 전문가 채용 공고의 약 2/3를 차지하는 JPMorgan의 경우 양자 기술 숙련 인력으로 구성된 팀을 조직하는 데 어려움 호소 **⇒ 조직 내 물리·수리모델링·컴퓨터사이언스 관련 전공 인력의 외부 파트너와 협업 등을 통해 인재를 확보함으로써 양자 역량을 키울 필요**

자료: 국제금융센터

<기회: AI + 양자 기술의 시너지>

○ 특히, AI 기술 발전 및 수요 가속화*로 경제·산업 전반의 영향력이 커지고 있는 가운데 AI와 양자 기술의 융합(AQ)에 따른 시너지 효과로 인하여 물리적 세계 뿐만이 아니라 디지털 세계에서 다양한 혁신적 활용 사례 창출이 기대

* 전세계 AI 시장 규모는 `23년 $1,890억에서 `33년 $4.8조로 25배 급증해 전체 첨단기술Frontier tech 시장에서 점유율(23년 7%→`33년 29%)이 4배 넘게 증가할 전망(UNCTAD)

- AI 모델 학습에 막대한 컴퓨팅 리소스가 필요한 데 다중 계산이 가능한 양자 컴퓨팅을 활용해 학습을 가속화함으로써 AI 알고리즘의 속도와 추론 능력 향상이 가능

  • 또한 양자 컴퓨팅은 기존의 GPU와 메모리에 대한 의존성을 줄일 수 있는 잠재력을 가지고 있어 거대언어모델LLM의 학습 및 운영 관련 비용 효율화에도 도움이 될 것임

  • 양자 기술은 일반 AI에 기존의 한계를 뛰어넘는 추진력을 불어넣는 '로켓 연료'가 될 수 있을 것으로 기대(BofA)

- 양자 컴퓨팅이 AI와 통합될 경우 더 많은 경제적 가치*와 새로운 비즈니스 기회가 창출될 것으로 보이나, 비용-편익 분석 등 사전 검증 절차의 필요성도 중요

* BofA에 따르면 현재 전세계적으로 생성되는 데이터(`22년 120ZB→`25년 183ZB 예상)의 24%에 양자 컴퓨팅 기능을 적용할 경우 글로벌 GDP가 2배 확장될 것으로 추산

- 양자 컴퓨팅 기술이 AI와 공생한다면 궁극적으로 인간과 같거나 인간을 뛰어넘은 지능을 갖춘 범용인공지능Artificial General Intelligence 도달에 일조할 것으로 기대(McKinsey)
- 한편 양자 기술 도입 시 기존 AI 모델 대비 어느 정도 개선되는지를 미리 파악하기 위해서 비용 및 운영 리스크 대비 개선 효과에 대한 구체적 수치 등의 검증이 필요

<위협: 현재 암호화 체계의 무력화>

○ 아울러 양자 컴퓨팅 성능의 발전으로 인하여 현재 사용되는 암호화 기술이 양자 기반 해킹 등의 위협에 노출될 수 있으므로 양자방어 암호Quantum-Defense Cryptography 시스템 구축 등 대비 전략을 수립할 필요

- 사이버 범죄자들이 양자 컴퓨팅 기술을 악용해 현재 수학적 알고리즘(소인수 분해)에 기반한 공개키 암호화(RSA) 방식을 해독하며 보안 시스템이 무력화될 우려가 제기
  - 양자 컴퓨터는 Shor's algorithm을 통해 소인수 분해를 빠르게 수행할 수 있으며<그림 2> 이는 공개키 암호화 기술의 보안상 취약성 증대를 초래
  - 특히, 타원곡선 암호화(ECC)* 방식을 채택하고 있는 디지털 자산 등 블록체인 기술도 양자 컴퓨터의 성능 발전으로 인해 해킹에 취약할 소지

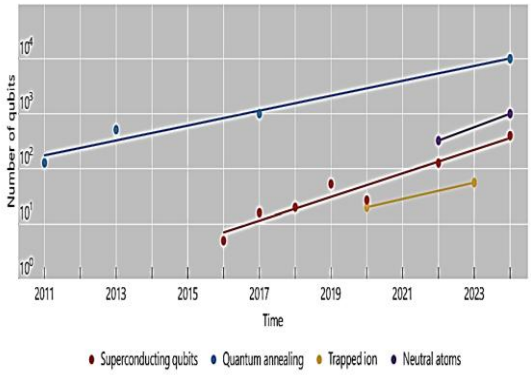
    * 타원곡선의 수학적 구조를 활용해 RSA 등 기존 보다 짧은 키로 높은 보안성을 제공하는 공개키 암호화 방식으로 블록체인 분야의 디지털 서명 등에 주로 활용
- 금융업계, 보안전문가 등은 양자 컴퓨터가 기존의 일반적 암호화 체계를 완전히 깨트리는 시점인 'Q-Day'가 실질적으로 5년 정도 밖에 남지 않았다며 우려
  - IBM 연구소는 현재의 암호화 보안 체계가 완전히 해제될 수 있는 시기를 2020년대 내로, Citi는 2027년으로, HSBC의 경우 최소 2030년으로 각각 예상
  - 반면 미국(National Institute of Standards and Technology)과 유럽(Quantum Safe Financial Forum)의 관계 당국은 `35~`40년 경 기존 암호화 체계가 무력화될 것으로 진단
- 이에 서구 대형은행들을 중심으로 양자암호 기술(양자내성 암호Post-Quantum Cryptography;PQC* 및 양자암호키 분배Quantum Key Distribution;QKD**) 투자 등에 대한 필요성을 인지하고 선제적으로 대응

  * PQC는 양자 컴퓨터 공격에 저항력을 구축하도록 현재 암호 기술에 기반해 더 복잡한 수학적 알고리즘으로 설계된 알고리즘. 민감한 금융 데이터 보호를 위해 양자 컴퓨팅의 해독 시간을 늘리는데 초점

  ** QKD는 이론적으로 해독 불가능한 암호화를 구현하는 방법. 양자난수발생기Quantum Random Number Generator;QRNG를 사용해 실제로 예측할 수 없는 난수를 생성하여 양자 컴퓨팅으로도 해독 불가능한 암호를 구현
  - 미국 5대 은행들은 QKD, QRNG 등 양자보안 기술 탐색 및 검증 목적으로 Quantum Computing과 $33.2만 규모의 양자 통신 시스템 구매 계약 체결(`25.7월)

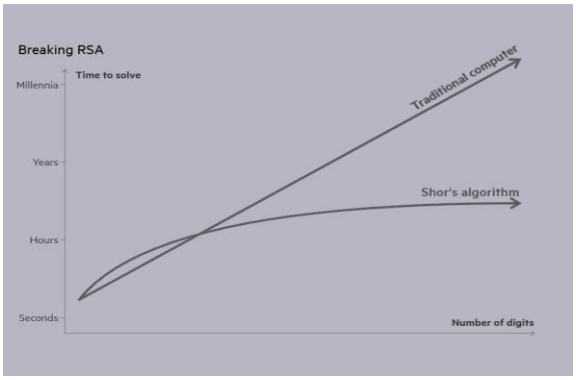
- JPMorgan의 CIO는 준비 태세 강화 차원에서 양자보안에 투자하고 있다고 강조하면서, PQC와 QKD를 통합하는 이중 대응전략을 준비 중이라고 부언
- Barclays, BNP Paribas, Santander, CaixaBank, Intesa Sanpaolo 등은 Europol 산하 Quantum Safe Financial Forum에 참여해 양자내성 전환 등을 논의
- HSBC의 경우 `23년 QKD를 활용해 외환 거래(€3천만)를 성공적으로 수행하였고, `24년 PQC VPN 터널과 QRNG를 토큰화된 금$_{\text{HSBC Gold Token}}$의 매매에 적용
- 스페인 Banco Sabadell은 암호화 프로토콜 현대화를 목표로 암호화 전환 민첩성에 중점을 두고 PQC 도입을 모색하기 위한 프로젝트를 진행
- 파라과이 Ueno Bank는 SignQuantum과 QANplatform의 양자방어 디지털 서명 및 블록체인 기술을 도입에 나서는 등 양자암호 사이버 보안 솔루션 구축에 착수

<그림 1> 양자 컴퓨팅 기술의 성능 진화 속도



자료: BIS

<그림 2> Shor's algorithm의 RSA 해독 속도



자료: FT

[참고 2] 주요국의 양자 컴퓨팅 투자 및 정책

□ **'23년까지 세계 각국 정부가 발표한 양자 기술 공공투자 규모는 중국의 $150억 투자를 포함해 총 $420억. 국가적 계획은 주로 기술적 리더십, 주권 확보, 민간투자 촉진 등이 목표**

○ **(미국)** 정부는 양자 기술을 미래 국가전략의 핵심 기술로 삼고 연구 보조금 지급 외에 관련 법안 제정 등 다양한 정책 지원을 제공. 관련 특허 승인은 18,649건('00~'24년)으로 세계 1위

- 트럼프 대통령은 행정명령을 통해 '국가 양자 이니셔티브법' 재승인을 추진. 양자교육 커리큘럼 확대, 국립 양자연구소 설립 등을 포함해 산·학·연 협력구조 유지, 인재 양성과 기술 상용화를 도모
- 11.4일 에너지부$_{DOE}$는 국가 양자정보과학연구센터의 차세대 연구 프로그램에 최대 5년간 $6.25억을 지원할 계획을 발표. '25년 예산은 $1.25억이며, 이후 자금은 의회 승인에 따라 결정

○ **(EU)** EU는 지난 7월 '30년까지 유럽을 양자분야의 글로벌 리더로 만들기 위한 'EU 양자 전략' 발표. △양자 유럽 연구·혁신 이니셔티브 출범 △양자 컴퓨팅·통신·센싱 분야 인프라 개발 △양자 R&D 친화적 환경 조성 △양자 기술과 우주·안보·방위 기술 융합 △전문인력 양성 등의 내용 포함

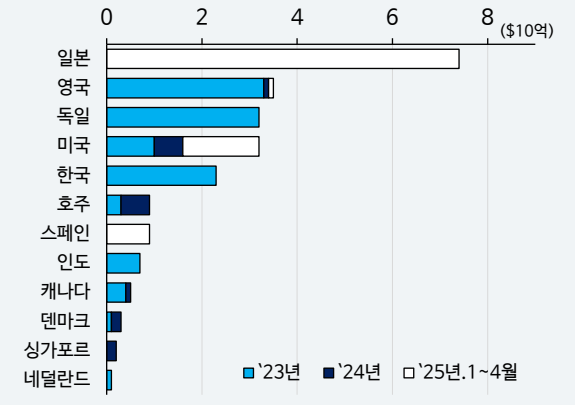
- 유럽은 EuroHPC 공동사업을 통해 1세대 하이브리드 양자-고전 컴퓨팅 시스템을 구축. 독일 정부는 '21년 항공우주센터의 양자 컴퓨팅 이니셔티브의 일환으로 4년 내 양자 컴퓨터 프로토타입을 개발하겠다고 발표

○ **(중국)** 정부는 14차 5개년 계획('21~'25년) 하에서 핵심산업 육성 계획의 한 부문으로 양자 기술(양자 컴퓨팅, 양자 암호통신, 양자 센싱)을 선정하고 $150억을 투입. 중국은 특히 암호통신 부문을 선도(논문 점유율 중국 38% vs 미국 12.5%)하는 가운데, 양자 컴퓨터의 독자 개발에도 속력

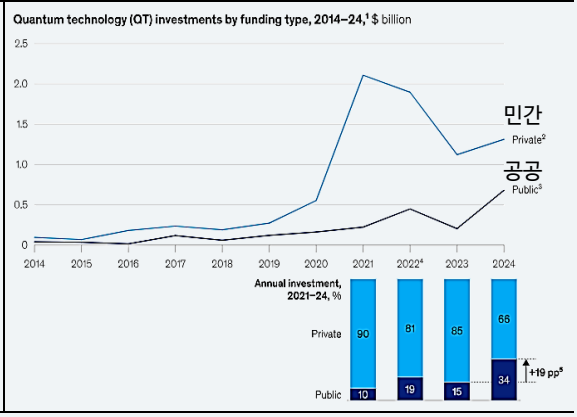
- 중국의 양자 기술 특허 신청은 '00~'24년 약 3.5만건으로 세계 1위이며, 그 중 양자 컴퓨팅 관련 특허가 약 81%를 차지. 한편, 특허 승인은 7,601건으로 미국, 일본 및 독일에 이어 4위
- 중국 내 연구기관들은 금년 중 중성원자 양자 컴퓨터(한위안 1호), 초전도 양자 컴퓨터(톈옌-504, 쭈충즈 3호) 등을 독자적으로 개발하고 상용화에 돌입

□ **양자 기술 스타트업에 대한 투자('24년 $20억) 역시 주요국 정부의 강력한 기술 투자 의지에 힘입어 전년 대비 53% 확대(공공부문의 비중 '21~23년 10~19% → '24년 34%)**

〈그림 3〉 국가별 양자 기술 공공투자 발표('23~'25.4월)



〈그림 4〉 양자 기술 스타트업 투자



자료: McKinsey ('25.6월)

자료: McKinsey, 외신종합