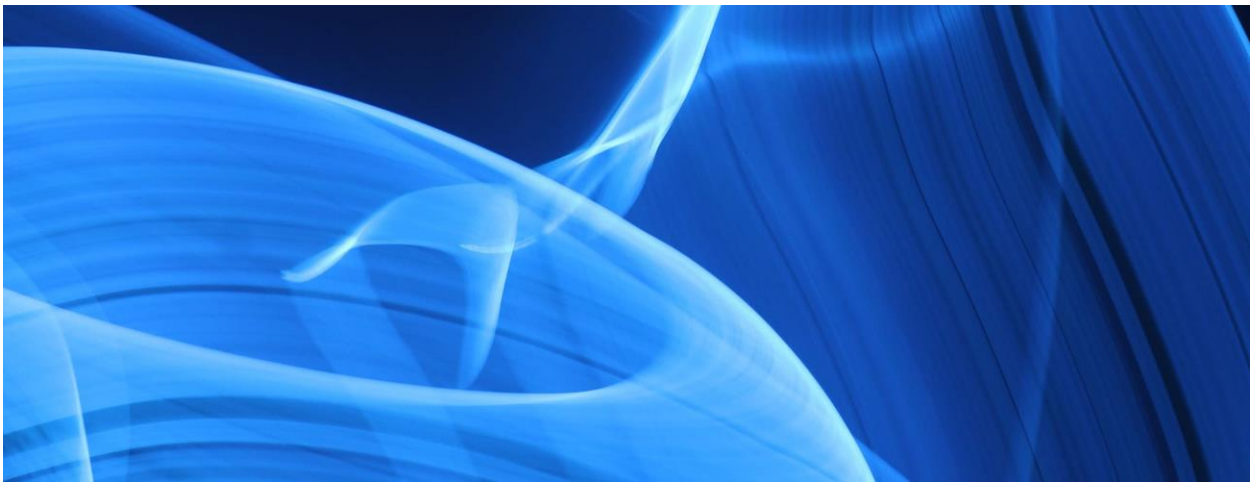


Quantum Computing Could Offer a Step Change in Fraud Prevention

JUNE 7, 2024

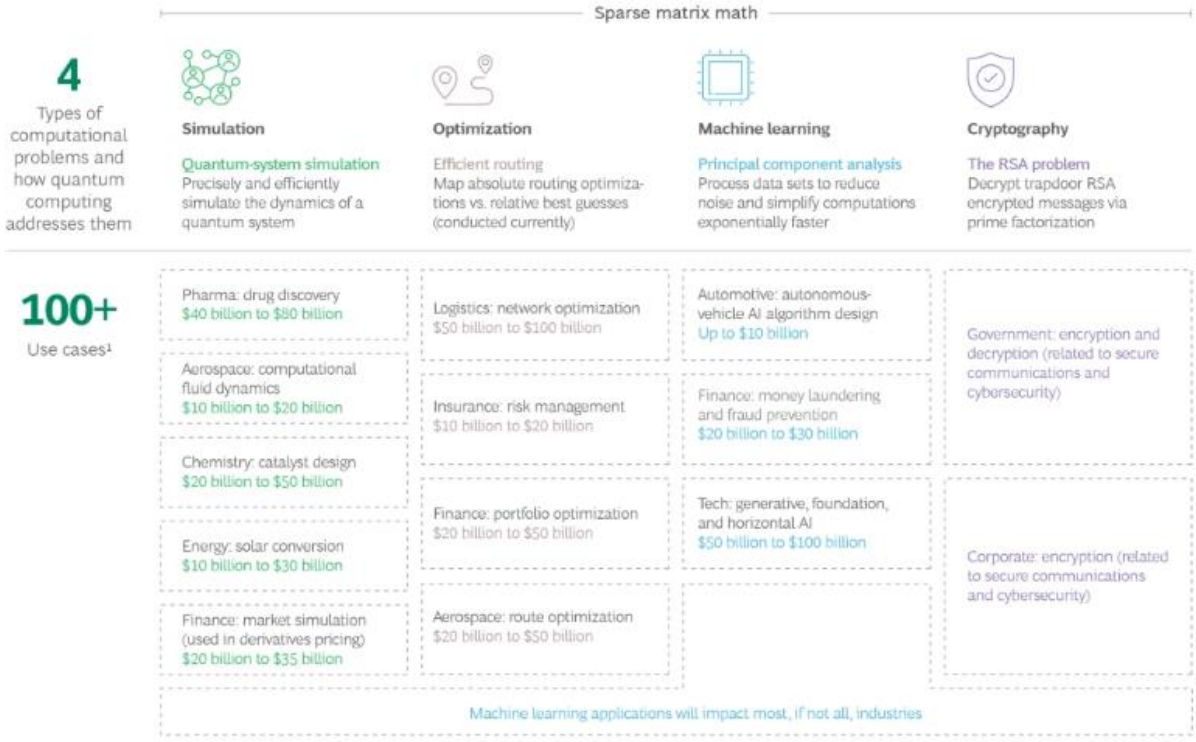
By Brad Henderson, CEO, P33
Matt Langione, Managing Director and Partner, Boston Consulting Group
Rob Gillis, Vice President, Discover Financial Services
Imed Othmani, Industry Partner, Quantum Industry & Technical Services, IBM Quantum

Quantum computing has the potential to produce breakthroughs in a number of industries, such as aerospace, chemicals, pharmaceuticals, financial services and energy, creating $450-850B annually for businesses and offering a wide range of benefits for consumers and governments. One increasingly urgent potential application is fraud prevention. Today fraud carries staggering costs for consumers, governments and financial institutions with $2T in money laundered every year, more than $40B lost in

identity scams and nearly $30B lost in credit card fraud alone [1].These numbers are expected to rise in the future with the growth of GenAI and e-commerce.

Quantum computers might one day arm financial institutions and regulators with the tools they need to fight this growing threat. Advances in quantum computing hardware and software, including IBM research published in Nature, suggests quantum computers could have real-world applications before the emergence of fault tolerance. IBM has also demonstrated a clear path to error corrected quantum computer before the end of decade. Together, this brings into focus a range of industrial use cases[2] [3].

Exhibit 1 – Quantum Computing Enables Hundreds of Use Cases[4]



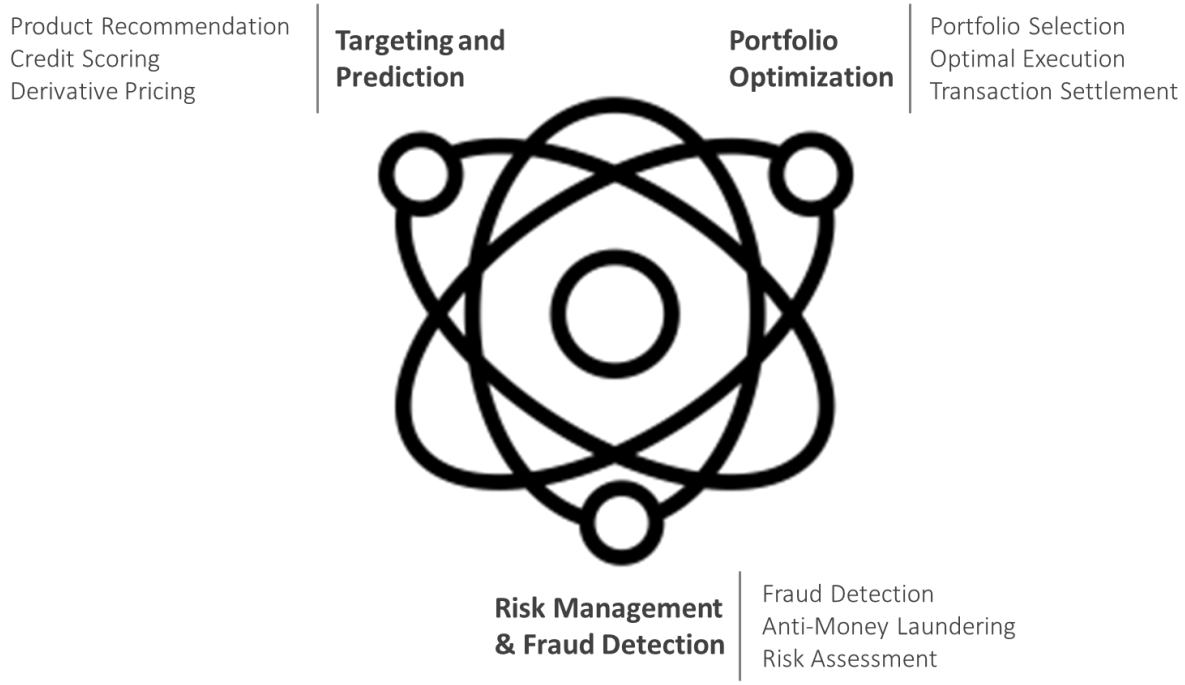
Financial Services, Fraud Detection, and Quantum Computing

[1] Nilson Report; Javelin 2021 Identity Fraud Study
[2] Youngseok, K. et all. Evidence for the utility of quantum computing before fault tolerance. Nature (2023)
[3] Bravyi, S., Cross, A., Gambetta, J., et al. High-threshold and low-overhead fault-tolerant quantum memory. Nature (2024)
[4] Bobier, J., Langione, M., Tao, E., Gourevitch, A., "What Happens When 'If' Turns to 'When' in Quantum Computing," *BCG*, July 2021

The financial services industry has been an early leader in exploring emerging quantum computing applications, with several use cases at the proof-of-concept stage. Key quantum computing use cases for financial services include portfolio optimization, risk management, and fraud detection[5].

Classical computers are not always well-suited to solve fraud problems effectively and efficiently. For one thing, fraud events are rare and represent a weak statistical signal in a mass of financial transaction data. For another, patterns of fraud are complex and change over time with new and often sophisticated fraudulent behaviors. Most approaches to preventing fraud with classical computers lead to errors, including high rates of "false positives" that are costly in themselves.

Exhibit 2 – Quantum Computing Use Cases in Financial Services



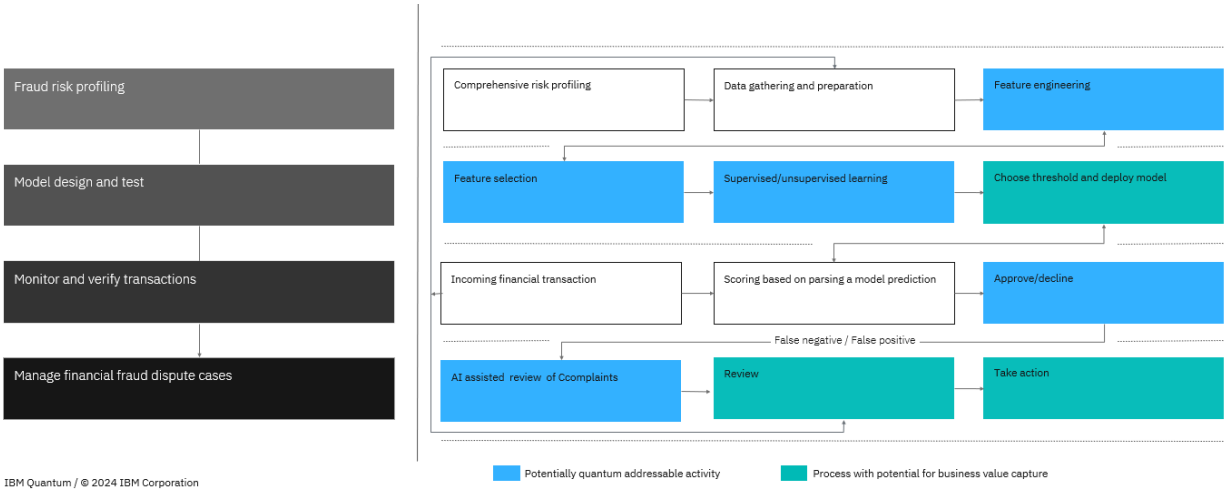
Approaches that leverage quantum computers, by contrast, have the potential to identify hidden fraud patterns with fewer false positives. Early research by IBM with hybrid quantum-classical algorithms, for example, has already demonstrated promising results benchmarked against classical machine learning methods[6]. There is ongoing research into how quantum computers could be used alongside classical computers in a

[5] Citi Global Perspectives and Solutions – *Quantum Computing*, June 2023

[6] Grossi, M., Ibrahim, N., Radescu, V., Loredo, R., Voigts, K., Von Altrock, C., Rudnik, A., Mixed Quantum-Classical Method for Fraud Detection with Quantum Feature Selection. IEEE Transactions on Quantum Engineering (2022)

fraud detection workflow—for example in feature engineering, feature selection, supervised/unsupervised learning, approve/decline decision-making, and AI-assisted complaint review.

Exhibit 3 – Fraud prevention workflow with quantum computing opportunities



Acceleration of Fraud Threats

Fraud threats are expected to accelerate dramatically with advances in AI, in particular generative AI, and their malicious use by sophisticated adversarial state- and criminal-actors. Generative AI, for example, can enable hyper-realistic impersonations and provide a platform to dramatically enhance the creation, refinement, scaling, and distribution of fraud attacks. Generative AI also poses the risk of democratizing fraud—providing anyone with access to large language models the capacity to construct highly convincing fraud attacks. Since the launch of ChatGPT at the end of 2022, ransomware attacks have increased 76%[7]. Phishing attacks have also surged—by a staggering 1,265%—since the launch of ChatGPT[8].

Current fraud detection solutions risk being overwhelmed by the availability, sophistication, scale, and reach of AI-specific fraud threats. Malicious large language models are creating content to facilitate cyberattacks and can be purchased for as little as $200 a month on the dark web[9]. This new and evolving threat requires industry and

[7] Accenture Cyber Threat Intelligence Research
[8] SlashNext State of Cyber Phishing Report 2023
[9] Accenture Cyber Threat Intelligence Research

government collaboration to develop new and robust fraud defenses using emerging technologies, including quantum computing.

Illinois Quantum Ecosystem and The Bloch Tech Hub

Governor JB Pritzker has executed on a bold vision to ensure Illinois is a nexus of cutting-edge quantum research to address opportunities and challenges. Illinois hosts unique quantum-specific assets including the Chicago Quantum Exchange (CQE), an intellectual hub that is one of the largest collaborative teams working on quantum science in the world; Duality, the nation's first quantum startup accelerator; and The Bloch Quantum Tech Hub, the nation's only quantum innovation team rallying entire industry sectors around society's most urgent challenges, one of two quantum Economic Development Administration (EDA)-designated Tech Hubs.

The broader Chicagoland quantum ecosystem is also home to the seven world-leading institutions that anchor the CQE: the University of Chicago (UChicago), the US Department of Energy's Argonne National Laboratory (Argonne) and Fermi National Accelerator Laboratory (Fermilab), the University of Illinois Urbana-Champaign (UIUC), the University of Wisconsin-Madison, Northwestern University, and Purdue University. The region is one of the country's largest quantum-ready talent pipelines, awarding almost 60,000 degrees and certificates annually in quantum-relevant skills, and is the largest producer of quantum-related PhDs in the nation.

Furthermore, Illinois is also the site of four of the ten National Quantum Initiative (NQI) Act Centers—U.S. Department of Energy QIS Research Centers and National Science Foundation Quantum Leap Challenge Institutes:

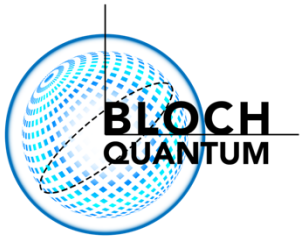
- Q-NEXT | Next Generation Quantum Science and Engineering (DOE/Argonne / UChicago)
- SQMS | Superconducting Quantum Materials and Systems Center (DOE/Fermilab / UChicago)
- HQAN | Hybrid Quantum Architectures and Networks (NSF / UIUC)
- QuBBE | Quantum Sensing for Biophysics and Bioengineering (NSF / UChicago)

This technical expertise, combined with a diverse industry base - with a strong presence across key quantum sectors, such as finance, energy, biotech, and manufacturing – make the region an ideal testbed for commercial quantum applications.

Quantum Shield and The Bloch Tech Hub

The Chicago region was recently recognized for its leadership in quantum technology and designated an EDA Tech Hub for quantum technologies—*The Bloch Tech Hub*—by the Biden-Harris administration. The Bloch Tech Hub, as part of the Chicago Quantum Exchange, is one of only 31 Tech Hub designees from nearly 400 applications across the country, and one of two quantum Tech Hubs.

Exhibit 4 – The Bloch Quantum Tech Hub



The nation's only quantum innovation team rallying entire sectors around society's most urgent challenges—to combat financial fraud, secure the energy grid, and accelerate the development of life-saving drugs—by bringing critical industries and quantum technologists together to build large-scale solutions to global problems.

Leading Members:

IBM	Microsoft
qBraid	Infleqtion
mHub	UIUC
University of Chicago	City Colleges of Chicago

A key project within The Bloch Tech Hub is Quantum Shield, designed to develop pre-competitive quantum computing solutions to prevent and detect financial fraud—with all parties benefiting except for bad actors. Banks and payments networks regularly interact and coordinate with bank regulators and federal law enforcement—Federal Reserve, Federal Bureau of Investigation, and U.S. Department of the Treasury—to identify and combat new and evolving fraud threats. A consortium model is also an ideal pre-competitive structure to research, develop, and test quantum fraud detection solutions.

Quantum Shield stakeholders comprise technology, banking, payments, government, consulting, and community organizations that bring diverse assets, expertise, and perspectives to shape quantum fraud solutions. This includes technology leadership

from IBM and NORC at the University of Chicago (NORC); industry leadership from Discover Financial Services and other financial services participants; policy leadership from the federal and state agencies; thought leadership from Boston Consulting Group, P33, and Innovate Illinois; and community leadership from Financial Health Network and NORC.

Quantum Shield continues to engage other public and private organizations to participate in the consortium and collaborate on quantum computing solutions to defend against the growing threat of financial fraud to U.S. economic and national security. The time is now to work together to build collective defenses against the rising threat from AI-specific fraud. We invite members of the financial services industry to contact Meera Raja, VP of Deep Tech at P33 (meera.raja@p33chicago.com), to join Quantum Shield's efforts.