TruStage™

Quantum computing

risk overview

While widespread quantum computing is on the horizon, many financial institutions are actively exploring its potential. Some industry organizations are in early stages of investing, researching, and preparing algorithm developments that will be ready to leverage this technology once it matures. Just as many disruptive technologies, quantum computing could bring beneficial improvements along with potential challenges and risks.

In very simple terms, Quantum computing uses the principles of quantum mechanics to process information. Quantum computers process data using quantum bits or “qubits” using principles of superposition and entanglement to perform many calculations simultaneously, at unprecedented speeds.

With its immense processing power, quantum technology can analyze vast and complex transaction datasets almost instantly – even spotting hidden patterns that classical computers might miss in certain tasks or functions.

In the financial services industry, it is predicted that quantum computing could be used in:

- Corporate banking
- Enterprise risk management
- Cybersecurity
- Retail banking
- Payments
- Asset/Wealth management
- Investment banking
- Operations & finance
- Lending and loan processing

Though early versions of quantum computing may not be perfect, the advancing technology has the potential to significantly accelerate the speed at which complex problems are assessed and solved.

Where to start?

To begin to learn about quantum computing in the financial industry space, you should consider working with current and potential vendors and partners to develop a plan to implement when it finally comes to fruition.

Many suggest that quantum computing will have the ability to improve efficiency and speed that may enable better real time analysis, simulations, and decision making. Others suggest that enhanced financial modeling with quantum computing processing large data sets and complex financial models will help build better risk management, asset valuation, and portfolio management.

Advanced fraud detection is also commonly discussed where it is predicted that it will help detect transaction patterns and enhance overall fraud monitoring. Another risk management benefit could be stronger cybersecurity through encryption methods and securing communications.

Quantum computing holds the potential to revolutionize the financial industry in the lending area - particularly in mortgage lending where it will significantly improve risk assessments, loan processing and loan fraud detection.

However, not all is good news as quantum computing will likely pose threats to secure web traffic, digital contracts, digital signatures, email authentication, phishing protection, cryptocurrencies, and more.

Impact of quantum computing

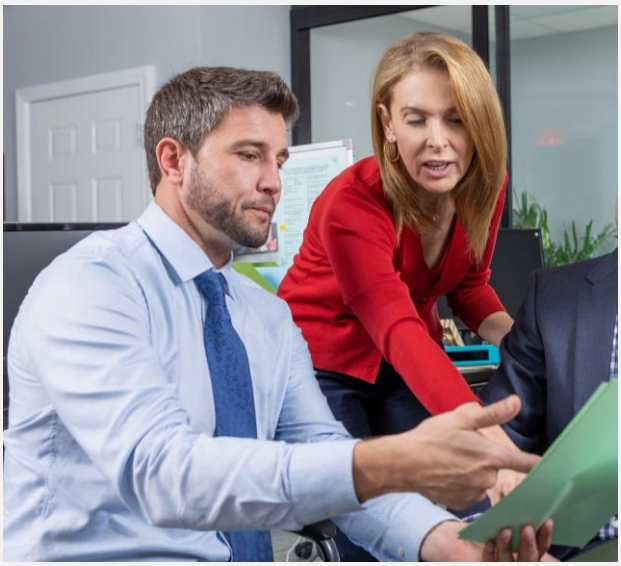
Lending practices

With quantum computing's ability to process vast amounts of data, possible beneficial impacts for lending programs may include:

- Enhanced risk assessment
  - Faster risk assessment and scenario analysis
  - More accurate credit scoring
  - Improved loan-level pricing
  - Optimized portfolio management
  - Improved and more timely decisions-making simulations for complex financial models
- Streamlined loan processing
  - Faster loan origination
  - Reduced processing costs
  - Improved efficiency
- Enhanced fraud detection
- Personalized loan products
- Improved market analysis
- Potential to use hybrid models for improvement. For example, using a hybrid technology such as AI/ML to help accelerate workflows, offerings, and selection processes

Some potential challenges by combining quantum computing and lending may include:

- Reliable developments of quantum algorithms with speed and accuracy
- Hardware limitations
- Integration with existing systems and compatibility or incorporation challenges
- Data privacy and security vulnerabilities



Enterprise risk management (ERM)

Risk is one of the most complex business units within the credit union when you consider identification, mitigation, and reporting across all business functions. Quantum computing may be able to allow risk departments and decision makers to consider a broader set of variables and assets when simulating risks, reducing the cost of risk and facilitating larger deals with even higher margins.

Fraud management

Quantum computing has been discussed as possessing the abilities to enhance pattern recognition that can help enable organizations to quickly detect emerging financial crimes with greater confidence. Quantum machine learning algorithms could potentially handle larger datasets with far fewer trained parameters and create complex models more efficiently than their classical counterparts. This could enhance the predictive capabilities of financial models, leading to more accurate risk assessment and decision-making.

In fraud detection, for instance, quantum machine learning could help identify anomalies that might be missed by traditional algorithms which then can help financial institutions stay ahead of evolving fraud threats.

Impact of quantum computing

Cybersecurity

Whether you foresee the use of quantum computing to bolster cybersecurity defenses or take its super abilities to break safeguards used to protect your private information, this is trending discussion topic.

As stewards of data security, credit unions are constantly in the search for ways to enhance current securities to protect against incidents that threatens the integrity, availability, and confidentiality of highly sensitive information.

Of course, significant concerns related to data breaches - exposing sensitive member information and corporate intellectual property - exist. Breaches result in significant financial losses, reputational damage, and legal liabilities for organizations.

Harvest now, decrypt later threat

A primary concern is quantum computing's ability to decrypt currently available cryptographic protocols for harvest now decrypt later purposes. This allows bad actors to collect encrypted data now and store it for later decryption when quantum computers become powerful enough, posing a longer-term threat to data with lasting value.

Sensitive historical data, presumed secure, could become vulnerable.

Quantum computing's potential to break current encryption poses significant cyber risks to industries relying on secure transactions and data storage, particularly in finance and healthcare. The ability to decrypt sensitive information, like banking details, could lead to widespread identity theft and financial fraud.

Quantum computing could reshape malware strategies. Cybercriminals might exploit vulnerabilities in legacy cryptographic systems, releasing malware signed with compromised keys.

Brute force attacks in which bad actors use all possible combinations to decrypt encryption keys and algorithms in an attempt to access data is also a significant cyber concern.

NIST response

The National Institute of Standards and Technology (NIST) released three new standards in efforts to mitigate the risk of quantum technology. These standards were developed to select quantum-resistant algorithms that would augment the public-key cryptographic algorithms

These standards emphasize the importance for financial services providers to be especially cognizant of this potential threat, given the vast amounts of sensitive consumer data they work with.

The NIST standards are built for the future and include:

- Encryption algorithms' computer code
- Instructions for implementation
- Intended uses

NIST encourages computer system administrators to begin transitioning to the new standards as soon as possible.

Action steps to take now

- Identify critical systems reliant on encryption, including digital signatures, encrypted cloud data, VPNs, and key exchanges.
- Incorporate quantum readiness into your vendor vetting – similar to approaches taken for the use of artificial intelligence.
- Re-encrypt long-term confidential and sensitive data with quantum-resistant algorithms.
- Integrate quantum-resistant algorithms alongside current encryption methods to ensure a smooth transition.
- Stay up-to-date with NIST's standards and recommendations.
- Collaborate with peer organizations, technology providers and partners to build knowledge and identify solutions.

Impact of quantum computing

Vendor & supply chain management

Where your organization relies on external third-party providers, you will need to evaluate their guidance for managing and controlling quantum computing.

Special attention should be given to data used or stored in a third-party environment. It is critical that you understand the vendor's readiness for managing the use and risks of quantum computing.

Vendors will also need their own set of unique operation requirements in addition to specialize hardware and stable system environments.

Critical vendor questions

Being open in vendor discussions is essential for long-term trust and compliance. Their responses can help you ensure that solutions and processes remain transparent, even as the use of quantum technology grows more sophisticated.

Some key questions to ask include:

- What is your governance over the safe and ethical use of quantum computing?
- How do you ensure the security and privacy of data as impacted by quantum computing?
- How are you managing updates and maintenance for data protection to ensure systems, products and services remain effective and secure over time?
- Can you provide an explanation how your organization is using or plans to use quantum computing for decisions or outputs?

Other considerations

Blockchain and Cryptocurrency

Vulnerabilities in the security of blockchains, cryptocurrency and cryptocurrency wallets could potentially allow theft by reversing keys. The anticipated threats by quantum is its potential to break a variety of encryption like cryptography, which is used to verify and secure sensitive data in transactions.

There are concerns over the potential security dangers to cryptocurrency wallets posed by quantum computing. A cryptocurrency wallet is a device or program that stores your cryptocurrency keys and allows you to access your coins. These wallets contain the necessary private keys and address needed to sign cryptocurrency transactions. Anyone who knows the private key can control the coins associated with that address.

Talent and skills

These developing quantum technologies revolve around combining a fundamentally new technology into organizations and their existing systems. The jump into quantum computing is a significant step.

Quantum computing requires a proficiency in quantum information science — a subject area with a substantial skills shortage.

Undoubtably, many organizations will likely struggle to find the right skilled talent in a timely manner. And with cybersecurity skills and talent gaps already at high levels, this will certainly add to the talent management and recruiting challenges.

Looking for additional insights? Contact a TruStage™ risk consultant by contacting us at **riskconsultant@trustage.com** or at **800.637.2676**.

TruStage™