International Journal of Management, Economics and Commerce
International, Peer Reviewed journal
E-ISSN: **2584-2609**

THE FUTURE OF FINANCIAL DATA SECURITY: CHALLENGES AND OPPORTUNITIES OF QUANTUM COMPUTING

Dr. Pragnesh B. Dalwadi

Assistant Professor,
Shree Bhaikaka Government Arts & Commerce College, Sojitra
Sardar Patel University, Vallabh Vidyanagar, Anand
ORCID-ID: https://orcid.org/0000-0001-7483-3724
E-Mail ID: pragnesh1606@gmail.com

Abstract

Quantum computing is set to transform various industries. Among them, the financial sector is especially vulnerable due to its reliance on encryption for securing transactions, customer data and proprietary financial models. Quantum computing threatens financial institutions by breaking current cryptographic methods, making them more vulnerable than other industries. This paper examines the potential impact of quantum computing on financial data security and focuses on the challenges and opportunities it presents. Quantum computers can solve complex mathematical problems more efficiently than classical computers. They pose a significant threat to current cryptographic systems that safeguard financial data. To mitigate this risk, financial institutions must adopt quantum-resistant encryption to maintain data integrity and privacy. On the other hand, quantum computing offers opportunities for enhancing financial security through advanced algorithms and improved risk assessment models. The paper also explores ethical and regulatory considerations, emphasizing the need for proactive measures to align technological advancements with societal values and legal frameworks. Addressing these challenges while leveraging opportunities will enable the financial industry to navigate the quantum era securely.

Keywords: *Quantum computing, financial data security, cryptography, risk assessment, regulatory frameworks*

1. INTRODUCTION

1.1 Background

Quantum computing is an emerging field that applies quantum mechanics to perform complex computations beyond the reach of classical computers. Unlike classical computers that process data in binary (0s and 1s), quantum computers utilize quantum bits, or 'qubits,' which can exist in multiple states at once due to a phenomenon called superposition. This capability allows quantum computers to process a vast number of possibilities at once, potentially solving computational problems much faster than classical computers.

1.2 Relevance to Financial Data Security

The financial sector relies heavily on data security to protect sensitive information such as personal client details, transaction records and proprietary financial strategies. Presently, this security is maintained through complex encryption methods that are computationally infeasible for classical computers to break. Nevertheless, the rise of quantum computing presents a major challenge to existing encryption standards. Quantum computers could potentially solve the mathematical problems underlying current cryptographic systems much more proficiently, rendering existing encryption methods vulnerable.

1.3 Purpose and Scope

This paper evaluates the impact of quantum computing on financial data security, highlighting the risks and exploring potential solutions. It provides an overview of quantum computing principles, assesses current financial security practices, examines quantum threats, and presents mitigation strategies. Additionally, it discusses regulatory and ethical considerations to ensure a secure transition into the quantum era.

2. OVERVIEW OF QUANTUM COMPUTING

2.1 Fundamental Principles

Quantum computing is based on the core principles of superposition and entanglement in quantum mechanics.

- **Superposition**: This principle allows qubits to exist in multiple states simultaneously. In classical computing, a bit is either a 0 or a 1. In contrast, a qubit can be both 0 and 1 at the same time, enabling quantum computers to process a vast number of possibilities concurrently.

- **Entanglement**: This phenomenon occurs when qubits become interconnected such that the state of one qubit directly influences the state of another, regardless of the distance separating them. Entanglement allows quantum computers to perform complex calculations more efficiently than classical computers.

2.2 Current State of Development

Quantum computing is still in the experimental phase, with advancements from IBM, Google, and other tech firms. IBM aims to develop the first fault-tolerant quantum computer by 2028, while Google has announced plans to introduce commercial quantum applications within the next five years. As large-scale quantum computers become a reality, financial institutions must prepare for their impact on data security.

3. FINANCIAL DATA SECURITY: CURRENT PRACTICES

In the financial sector, safeguarding sensitive information is paramount. Financial institutions employ a range of cryptographic methods to ensure the confidentiality, integrity and authenticity of data. These methods can be broadly categorized into symmetric encryption, asymmetric encryption, and hybrid approaches.

3.1 Symmetric Encryption

Symmetric encryption utilizes a single secret key for both encryption and decryption processes. The Advanced Encryption Standard (AES) is a widely adopted symmetric encryption algorithm in the financial industry. AES operates on fixed block sizes and supports key lengths of 128, 192, or 256 bits, providing a robust defence against brute-force attacks. Its efficiency and security make it suitable for encrypting large volumes of data, such as transaction records and customer information.

3.2 Asymmetric Encryption

Asymmetric encryption, also known as public-key cryptography, involves a pair of keys: a public key for encryption and a private key for decryption. The RSA (Rivest–Shamir–Adleman) algorithm is a prominent example used in securing financial communications. RSA facilitates secure data transmission over unsecured networks by enabling secure key exchange and digital signatures, ensuring data authenticity and integrity.

3.3 Hybrid Encryption

Hybrid encryption combines the strengths of both symmetric and asymmetric encryption. In this approach, asymmetric encryption is used to securely exchange symmetric keys, which are then employed for encrypting the actual data. This method leverages the security of asymmetric encryption for key distribution and the efficiency of symmetric encryption for data processing. For instance, the integration of M-IDEA with a 512-bit key size and DS-RSA methodology has been proposed to enhance data security in the financial sector.

3.4 Data-in-Transit and Data-at-Rest Encryption

Financial institutions must protect data both during transmission (data-in-transit) and when stored (data-at-rest).

- **Data-in-Transit**: Transport Layer Security (TLS) protocols are employed to encrypt data transmitted over networks, safeguarding against interception and man-in-the-middle attacks. This is crucial for online banking services and financial APIs.
- **Data-at-Rest**: Sensitive information stored in databases, cloud servers, or mobile devices is encrypted using methods like AES to prevent unauthorized access and data breaches. Implementing strong encryption for data-at-rest ensures that even if storage media are compromised, the data remains protected.

3.5 End-to-End Encryption (E2EE)

E2EE ensures that data is encrypted on the sender's side and only decrypted by the intended recipient, preventing intermediaries from accessing the information. This approach is vital for securing sensitive financial activities, such as mobile banking and digital payments, by maintaining data privacy throughout the communication process.

These cryptographic practices form the foundation of financial data security, enabling institutions to protect sensitive information against unauthorized access and cyber threats. However, the emergence of quantum computing presents new challenges to these established methods.

4. IMPACT OF QUANTUM COMPUTING ON CRYPTOGRAPHY

Quantum computing introduces computational capabilities that could potentially undermine current cryptographic systems. Understanding these impacts is crucial for developing strategies to protect financial data in the quantum era.

4.1 Threats to Current Encryption

Quantum algorithms, particularly Shor's algorithm, pose significant risks to existing cryptographic methods.

- **Shor's Algorithm**: This algorithm can efficiently factor in large prime numbers, a foundational aspect of RSA encryption. The ability to factorize these numbers rapidly would render RSA and similar encryption schemes insecure against quantum attacks.
- **Grover's Algorithm**: While symmetric encryption algorithms like AES are more resistant to quantum attacks, Grover's algorithm can still reduce their security by effectively halving the key length. For instance, a 256-bit key would offer the security equivalent of a 128-bit key against quantum attacks, necessitating the use of longer keys to maintain security.

4.2 Timeline for Quantum Threats

Experts predict that practical quantum computers capable of breaking current encryption algorithms could emerge within the next decade. A report by the Quantum-Safe Financial Forum, led by Europol, advises the financial sector to prepare for these risks now, as quantum computers are expected to be operational within 10 to 15 years, potentially sooner.

4.3 Harvest-Now, Decrypt-Later Attacks

A significant concern is the "harvest-now, decrypt-later" strategy, where adversaries collect and store encrypted data today, anticipating the ability to decrypt it once quantum computers become available. This approach threatens the long-term confidentiality of sensitive financial information, as data considered secure now may become vulnerable in the future.

4.4 Implications for Financial Institutions

The potential for quantum computers to break current encryption standards poses several risks for financial institutions:

- **Data Breaches**: Confidential customer information and proprietary financial data could be exposed if encrypted data is decrypted by quantum means.
- **Loss of Trust**: The compromise of secure communications and transactions could erode client trust and damage institutional reputations.
- **Regulatory Challenges**: Institutions may face compliance issues if they fail to protect data adequately against emerging threats, leading to legal and financial repercussions.

Given these potential impacts, it is imperative for financial institutions to proactively develop and implement quantum-resistant cryptographic solutions to safeguard data security in the approaching quantum era.

5. OPPORTUNITIES PRESENTED BY QUANTUM COMPUTING IN FINANCIAL DATA SECURITY

While quantum computing poses significant challenges to current cryptographic systems, it also offers promising opportunities to enhance financial data security. By leveraging quantum principles, financial institutions can develop more robust security measures to protect sensitive information.

5.1 Quantum Key Distribution (QKD)

Quantum Key Distribution is a method that uses the principles of quantum mechanics to securely distribute cryptographic keys between parties. The most well-known QKD protocol, BB84, allows two parties to detect any eavesdropping during the key exchange process. If an eavesdropper attempts to intercept the key, the quantum states of the particles used in the transmission will be altered, revealing the intrusion. This ensures that only the intended recipients have access to the cryptographic keys, significantly enhancing the security of data transmission.

5.2 Post-Quantum Cryptography (PQC)

Post-quantum cryptography involves developing cryptographic algorithms that are resistant to attacks from quantum computers. These algorithms are based on mathematical problems that are currently believed to be hard for quantum computers to solve, such as lattice-based, code-based, and multivariate polynomial problems. Implementing PQC can help financial institutions protect their data against future quantum attacks while maintaining compatibility with existing communication protocols.

5.3 Quantum Random Number Generation (QRNG)

Random numbers are essential in cryptographic applications for generating keys, initialization vectors and nonces. Traditional random number generators rely on deterministic algorithms or physical processes that may be predictable or biased. QRNGs, on the other hand, exploit inherent quantum uncertainties to produce truly random numbers. This results in higher entropy and unpredictability, strengthening cryptographic systems against attacks.

5.4 Enhanced Fraud Detection and Risk Management

Quantum computing's ability to process and analyze vast amounts of data at unprecedented speeds can improve fraud detection and risk management in the financial sector. By applying quantum algorithms to identify patterns and anomalies in large datasets, institutions can detect fraudulent activities more quickly and accurately. This proactive approach enhances the overall security of financial systems.

5.5 Secure Multi-Party Computation (SMPC)

SMPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. Quantum computing can enhance SMPC protocols by providing more efficient and secure ways to perform these computations. This is particularly useful in scenarios where financial institutions need to collaborate without revealing sensitive information to each other.

By exploring and implementing these quantum-based solutions, financial institutions can not only mitigate the risks posed by quantum computing but also enhance their data security frameworks, ensuring resilience against future technological advancements.

6. STRATEGIES FOR MITIGATING QUANTUM THREATS

As quantum computing continues to advance, financial institutions must proactively develop and implement strategies to mitigate potential threats to data security. This involves a comprehensive approach that includes assessment, planning, and the adoption of quantum-resistant technologies.

6.1 Conducting Risk Assessments

Financial institutions should begin by assessing their current cryptographic systems to identify vulnerabilities to quantum attacks. This involves:

- **Inventory of Cryptographic Assets**: Cataloguing all cryptographic algorithms, protocols and keys in use to determine which are susceptible to quantum threats.
- **Data Sensitivity Analysis**: Evaluating the sensitivity and confidentiality of data to prioritize protection efforts.
- **Threat Modelling**: Identifying potential attack vectors and assessing the likelihood and impact of quantum-based attacks.

These assessments provide a foundation for developing targeted mitigation strategies.

6.2 Developing a Quantum-Safe Roadmap

Based on the risk assessment, institutions should create a comprehensive plan to transition to quantum-resistant security measures. This roadmap should include:

- **Timeline for Implementation**: Establishing clear timelines for deploying quantum-resistant technologies, considering the institution's risk profile and the projected advancement of quantum computing.
- **Resource Allocation**: Allocating necessary resources, including budget, personnel and technology, to support the transition.
- **Stakeholder Engagement**: Involving key stakeholders, such as IT departments, security teams, and executive leadership, to ensure alignment and support.

A well-defined roadmap facilitates a structured and efficient transition to quantum-safe security.

6.3 Implementing Post-Quantum Cryptography

Adopting quantum-resistant cryptographic algorithms is crucial for safeguarding data against future quantum attacks. Steps include:

- **Algorithm Selection**: Choosing appropriate post-quantum algorithms based on factors such as security, performance, and interoperability.
- **System Integration**: Integrating new algorithms into existing systems and applications, ensuring compatibility and minimal disruption.
- **Testing and Validation**: Conducting thorough testing to validate the security and performance of the new algorithms under various scenarios.

Early adoption of post-quantum cryptography ensures long-term data security.

6.4 Enhancing Key Management Practices

Effective key management is vital in a quantum-threat landscape. Institutions should:

- **Increase Key Sizes**: Utilize larger key sizes for symmetric encryption to counteract potential quantum attacks.
- **Regular Key Rotation**: Implement policies for frequent key rotation to minimize the risk of key compromise.
- **Secure Key Storage**: Ensure cryptographic keys are stored securely, using hardware security modules (HSMs) or other secure methods.

7. CASE STUDIES ON QUANTUM COMPUTING IN FINANCIAL DATA SECURITY

7.1 JPMorgan Chase and IBM Collaboration

JPMorgan Chase has partnered with IBM to explore quantum computing applications in cyber security. This collaboration aims to understand how quantum technologies can address complex security challenges in the financial sector. By leveraging IBM's quantum computing expertise, JPMorgan Chase seeks to develop advanced cryptographic solutions to protect sensitive financial data.

7.2 Thales and Quantinuum Partnership

Thales, a leader in cyber security solutions, has collaborated with Quantinuum to enhance data protection for financial services. By integrating Thales's Luna Hardware Security Modules (HSMs) with Quantinuum's quantum computing capabilities, the partnership aims to develop quantum-resistant encryption methods. This approach ensures that financial institutions can safeguard their data against emerging quantum threats.

7.3 Quantum Economic Development Consortium (QED-C) Report

The QED-C released a report titled "Quantum Technology for Securing Financial Messaging," which explores the potential impact of quantum computing on the financial sector. The report assesses quantum-resistant technologies and guides strategies for achieving security across the sector. It emphasizes the importance of adopting quantum-safe encryption methods to protect financial messaging systems.

7.4 Europol's Quantum Safe Financial Forum

The Quantum-Safe Financial Forum, led by Europol, has advised Europe's financial sector to start preparing for the risks posed by quantum computers. The forum emphasizes the need for financial institutions to identify vulnerable cryptographic standards, secure alternatives, and plan for operational changes accordingly. This proactive approach aims to mitigate potential threats to customer confidentiality and communication authentication.

7.5 Signal and Apple's Adoption of Post-Quantum Encryption

In response to the looming threat of quantum computing, companies like Signal and Apple have begun adopting post-quantum encryption methods. These initiatives aim to protect user data against future quantum attacks by implementing quantum-resistant algorithms. This proactive stance highlights the importance of early adoption of quantum-safe technologies in the tech industry.

These case studies demonstrate the financial sector's recognition of quantum computing's dual role as both a potential threat and a tool for enhancing data security. By proactively engaging with quantum technologies, these institutions aim to stay ahead of emerging risks and leverage new opportunities for safeguarding financial data.

8. FUTURE DIRECTIONS AND RECOMMENDATIONS

As quantum computing continues to evolve, financial institutions must adopt forward-looking strategies to address both the challenges and opportunities it presents. This chapter outlines key recommendations for preparing the financial sector for a quantum future.

8.1 Investment in Quantum Research and Development

Financial institutions should invest in quantum computing research to stay abreast of technological advancements. By collaborating with academic institutions, technology firms, and industry consortia, they can:

- **Stay Informed**: Keep up-to-date with the latest developments in quantum technologies and their potential applications in finance.
- **Develop Expertise**: Build in-house expertise to understand and implement quantum-resistant security measures.
- **Innovate**: Explore new financial products and services enabled by quantum computing capabilities.

Such investments will position institutions to leverage quantum advancements effectively.

8.2 Adoption of Quantum-Resistant Cryptography

Transitioning to quantum-resistant cryptographic algorithms is essential for long-term data security. Institutions should:

- **Evaluate Current Systems**: Identify cryptographic algorithms vulnerable to quantum attacks.
- **Implement Quantum-Safe Algorithms**: Adopt algorithms recommended by standardization bodies like the National Institute of Standards and Technology (NIST).
- **Test and Validate**: Ensure new cryptographic implementations maintain system performance and security.

Proactive adoption of quantum-resistant cryptography will mitigate future risks.

8.3 Development of Quantum Risk Management Frameworks

Institutions should integrate quantum risks into their existing risk management frameworks by:

- **Assessing Quantum Threats**: Regularly evaluate the potential impact of quantum computing on various aspects of operations.
- **Scenario Planning**: Develop scenarios to understand potential quantum-related disruptions and responses.
- **Policy Formulation**: Establish policies to guide decision-making related to quantum technologies.

A structured approach to quantum risk management will enhance organizational resilience.

8.4 Collaboration with Industry and Regulatory Bodies

Engaging with industry peers and regulators is crucial for a coordinated response to quantum challenges. Institutions should:

- **Participate in Industry Consortia**: Join groups like the Quantum Economic Development Consortium (QED-C) to share knowledge and best practices.
- **Engage with Regulators**: Work with regulatory bodies to develop guidelines and standards for quantum security.
- **Collaborate on Standards**: Contribute to the development of international standards for quantum-resistant technologies.

The collaboration will ensure a unified and effective approach to quantum readiness.

8.5 Continuous Monitoring and Adaptation

Given the rapid pace of quantum advancements, institutions must:

- **Monitor Technological Developments**: Keep track of breakthroughs in quantum computing and cryptography.
- **Update Security Protocols**: Regularly revise security measures to incorporate new quantum-resistant techniques.
- **Train Personnel**: Provide ongoing education and training to staff on quantum-related topics.

9. ETHICAL AND REGULATORY CONSIDERATIONS IN QUANTUM COMPUTING FOR FINANCIAL DATA SECURITY

As quantum computing advances, it introduces not only technological challenges and opportunities but also significant ethical and regulatory considerations for financial data security. This chapter delves into these aspects, emphasizing the importance of proactive engagement to ensure the responsible integration of quantum technologies in the financial sector.

9.1 Ethical Considerations

The deployment of quantum computing in finance necessitates careful ethical deliberation to uphold public trust and ensure equitable outcomes. Key ethical considerations include:

- **Data Privacy**: Quantum computing's potential to break current encryption standards poses a threat to individual and corporate data privacy. Financial institutions must prioritize the development and adoption of quantum-resistant encryption methods to protect sensitive information.
- **Equity and Access**: The high cost and complexity of quantum technologies may lead to unequal access, where only large institutions can afford implementation, potentially exacerbating existing disparities in the financial sector.
- **Transparency and Accountability**: As financial institutions adopt quantum algorithms for decision-making, ensuring transparency in these processes becomes crucial. Stakeholders must be able to understand and challenge decisions that significantly impact them.

9.2 Regulatory Considerations

Regulatory bodies play a pivotal role in guiding the safe and ethical integration of quantum computing into financial services. Key regulatory considerations include:

- **Standardization of Quantum-Resistant Protocols**: Regulators should collaborate with industry experts to establish and promote standards for quantum-resistant cryptographic protocols, ensuring a unified approach to data security.
- **Compliance and Enforcement**: Existing data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, may need to be updated to address the unique challenges posed by quantum computing. Regulators must ensure that financial institutions comply with these evolving standards.
- **Risk Assessment and Management**: Regulatory frameworks should mandate that financial institutions conduct regular risk assessments related to quantum threats and implement appropriate mitigation strategies.
- **Global Collaboration**: Given the borderless nature of financial transactions, international regulatory cooperation is essential to develop cohesive strategies for quantum security.

9.3 Proactive Measures for Ethical and Regulatory Alignment

To align with ethical standards and regulatory expectations, financial institutions should:

- **Engage in Ethical Deliberation**: Establish ethics committees to oversee the deployment of quantum technologies, ensuring decisions align with societal values and public interest.
- **Participate in Regulatory Development**: Actively contribute to the development of regulatory frameworks by collaborating with policymakers and industry groups.
- **Invest in Compliance Infrastructure**: Develop robust compliance programs to adhere to emerging quantum-related regulations, including staff training and system upgrades.
- **Foster Public Trust**: Maintain transparency with stakeholders about the adoption and impact of quantum technologies, addressing concerns proactively to build and sustain trust.

By thoughtfully navigating the ethical and regulatory landscape, financial institutions can harness the benefits of quantum computing while safeguarding data security and maintaining public confidence.

10. CONCLUSION

Quantum computing is a transformative technology with profound implications for financial data security. While it presents significant threats to current cryptographic systems, it also offers opportunities to enhance security frameworks. The financial industry must act proactively to mitigate risks associated with quantum computing by adopting quantum-resistant encryption, implementing quantum key distribution (QKD), and investing in post-quantum cryptographic research.

Financial institutions should prioritise transitioning to post-quantum cryptographic standards as outlined by NIST, integrate quantum-safe security measures into their operations, and collaborate with regulatory bodies to ensure compliance with evolving cybersecurity policies. Additionally, investments in quantum research and development will enable organisations to leverage quantum capabilities for improved risk assessment, fraud detection, and secure multi-party computations.

Ethical and regulatory considerations must remain central to the adoption of quantum computing in finance. Transparency, accountability, and equitable access to quantum technologies will be essential to maintaining public trust and securing financial systems against emerging cyber threats.

In conclusion, while quantum computing presents formidable challenges to financial data security, it also paves the way for revolutionary advancements. A strategic, forward-thinking approach that embraces quantum resilience will allow the financial

sector to harness quantum computing's potential while safeguarding the integrity and confidentiality of sensitive financial data.

REFERENCES

[1] Boneh, D., & Lipton, R. J. (1995). Quantum cryptanalysis of hidden subgroup problems. Advances in Cryptology – CRYPTO '95, LNCS 963, 113-127. https://doi.org/10.1007/BFb0052239
[2] Capgemini. (2024). New quantum-safe cryptographic standards: Future-proofing financial security. https://www.capgemini.com/insights/expert-perspectives/new-quantum-safe-cryptographic-standards-future-proofing-financial-security-in-the-quantum-age/
[3] European Union Agency for Cybersecurity (ENISA). (2024). Quantum readiness: Preparing for the post-quantum era. https://www.enisa.europa.eu/publications/quantum-readiness
[4] Europol. (2025). Quantum Safe Financial Forum: Banks should prepare for quantum risks now. Reuters. https://www.reuters.com /technology/cybersecurity / Europol-body-banks-should-prepare- quantum-computer- risk-now-2025-02-07/
[5] EY Global. (2024). Quantum cybersecurity and the financial sector: Preparing for a secure future. https://www.ey.com/en_us/insights/strategy/financial-services-cybersecurity-for-quantum-computing
[6] Google Quantum AI. (2025). Commercial quantum computing applications are arriving within five years. Reuters. https://www.reuters.com/technology/google-says-commercial-quantum-computing-applications-arriving-within-five-years-2025-02-05/
[7] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), 212-219. https://doi.org/10.1145/237814.237866
[8] International Business Machines (IBM). (2024). Quantum-safe cryptography and the financial sector. IBM Research. https://research.ibm.com/publications/quantum-safe-cryptography
[9] KPMG. (2024). Quantum computing in financial services: Strategic considerations. https://kpmg.com/ie/en/home/insights/2024/11/quantum-computing-in-financial-services-strategy.html
[10] Moody's Analytics. (2024). Quantum computing in financial services: Trends and security risks. http:// www.moodys.com/web/en/us/insights/quantum/quantum-computing-in-the-financial-sector-2024-trends-in-review.html
[11] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723
[12] National Institute of Standards and Technology (NIST). (2023). Post-quantum cryptography standardization process. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography
[13] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484-1509. https://doi.org/10.1137/S0097539795293172
[14] World Economic Forum (WEF). (2024). Quantum security for the financial sector: Informing global regulatory approaches. https://www.weforum.org/publications/quantum-security-for-the-financial-sector