How the South African financial sector can embrace quantum

Working paper series

WP/2025/01

The Centre of Excellence in Financial Services is a non-profit organization focusing on collaborative research, bringing together local and international thought leaders, industry experts and academics to interrogate the role financial services can play in achieving national and international objectives. This working paper is available in electronic format on www.coefs.org.za.

Table of contents

Preface

The symbiotic relationship between humans and machines has only been exaggerated through Hollywood depictions, with very little experiential learning for the individual. However, with ChatGPT, innocuous terms like large language models, open API, chatbots and artificial intelligence have suddenly emerged as a reality. For the individual, your personal digital footprint has become a cause for concern with cyber-attacks growing and an uncomfortable uncertainty as to where it all ends.

We can see how the financial sector is focused on these issues, as national regulators, financial regulators, and policy makers, begin setting standards for compliance. However, there is an existential threat to the banking industry, the potential for mathematical encryption techniques used to safeguard the sharing of data to be breached with the use of quantum computers. With quantum computers being made available to the public, we wanted to get a sense of how quantum was being used by the financial sector, and if there was an appreciation for the compression of predicted timelines for the breach, from decades to just years.

This research is applicable to the broader financial sector but is based on interviews conducted with the banking industry to serve as a proxy, combined with engagements with international experts in the field.

The United Nations Educational, Scientific and Cultural Organization (UNESCO) has declared 2025 as the International Year of Quantum Science and Technology, and we hope that this paper will contribute to the awareness of quantum computing and other quantum technologies relevant to the financial sector. More specifically, to catalyse thinking around the imminent and inevitable impact this will have on the financial sector and society more broadly.

Mark Brits
Executive Director

Members of the working group

in alphabetical order

Mark Brits

Committee chair
Executive Director
Centre of Excellence in Financial Services

Professor Andrew Forbes

Distinguished Professor, University of the Witwatersrand
Director, South African Quantum Technology Initiative

Asande Mahlaba

Research Administrator
Centre of Excellence in Financial Services

Executive summary

Quantum computing is fundamentally different to its classical computing counterpart we use today. When fully realised, they will perform exponentially more computations than a classical computer for the same resource, exploiting "qubits" that can be both 0 **and** 1 at the same time, rather than "bits" that must be 0 **or** 1. In many problems this removes time as a limitation, solving complex tasks in near real time that might overwise take years. In the financial sector, mathematical models such as a Monte Carlo simulation, which is used to predict possible outcomes, should benefit from quantum computing.

Quantum computing also introduces the threat that traditional security protocols could be compromised, particularly those based on public key cryptography, e.g., RSA. Thus, quantum computing may provide both the threat and a potential solution. How far are we from a working quantum computer? They already exist today as noisy devices, making them suitable as testing grounds but not yet fully fulfilling their promise. Estimates within the industry suggest 2035 as a likely date for a large-scale quantum computer that is cryptographically relevant, i.e., it can be used to attack existing security protocols. This has driven the international financial sectors to immediately introduce risk assessments and countermeasures, with published outcomes already available, e.g., Project Leap (Bank of France and Deutsche Bundesbank), Bank of Canada, Bank of Japan, World Economic Forum and UK Finance to name but a few. Two strategies that have surfaced are to: (i) move away from the mathematics central to public key cryptography, as has been outlined by NIST (National Institute of Standards and Technology) in 2024 with their quantum safe cryptography algorithms, and (ii) embrace quantum as the solution in the form of quantum key distribution, negating all mathematical complexity in the problem and

embedding the security into the known laws of nature. This introduces a fundamentally secure method for sharing data.

The South African Quantum Technology Initiative has developed a quantum strategy which remains largely unknown to the financial sector and there exists an opportunity for a financial sector strategy to be crafted within the national strategy. With Q-Day representing the day when quantum computers can break traditional security protocols such as Shor's algorithm, and with predictions for this measured in years not decades, the need for a quantum safe financial sector becomes more critical.

South Africa is unlikely to develop its own quantum computer which introduces some concerns about third party dependency, but, as a country, we are well positioned to drive programmes in quantum validation and certification, quantum software development and quantum sensing. This will require a new workforce with specialised education and training programmes for skills development, and if the financial sector are early adopters, they could drive these requirements.

With quantum computing not yet resonating in the banking industry, it is unlikely that the financial sector is embracing a programme to become quantum safe. A financial sector engagement model that facilitated an in-depth conversation between financial sector companies, regulators and policy makers to develop a clear financial sector strategy would be welcomed. Developing an enabling quantum readiness roadmap would also provide the foundation for an appropriate risk-based legislative framework that supports innovation and respects the evolution of international frameworks.

Introduction

Quantum physics is a theory that has been in existence for almost a century and has given birth to disruptive technologies such as the laser (now the basis for modern manufacturing and communication), and the transistor (the essential element of computers and electronics), touching our daily lives. Recent advances in the science and technology of quantum entanglement have given rise to a "second quantum revolution", with the promise of new disruptive technologies that cut across all disciplines - acknowledged by the awarding of the 2022 Nobel Prize in Physics[1]. The reason is that quantum science and technology has enormous potential to impact on critical societal challenges such as climate, energy, food production, healthcare, and clean water as reflected in the sustainable development goals of the UN Agenda 2030. Applications foreseen in the next decades will see transformative advances in medical imaging (health), efficient light-harvesting materials, better batteries and more efficient solar cells (clean energy), ultra-security in data (communications), exponentially faster computers that can solve complex problems such as climate and extreme weather (quantum computers), and more precise measurement systems (metrology).

The quantum era comes with three key stages that are common to its classical counterpart: data gathering, data processing and data sharing. What sets it apart is in how it performs these tasks. Quantum sensing and metrology gathers data in a fundamentally different way, allowing sensing and measuring with resolutions and accuracies not possible with non-quantum technology. Quantum computers will allow the processing of data in a parallel fashion with resources (e.g., time) that do not scale exponentially, so that complex tasks can be solved in real-time. Quantum communication allows data to be shared and transported in a fundamentally secure manner, foregoing the need for encryption that is based on mathematical complexity.

[1] The Nobel Prize in Physics 2022 was awarded jointly to Alain Aspect, John F. Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"

Thus, quantum is universally seen as ushering in a new paradigm for information processing and communication.

South Africa already has a quantum strategy, the South African Quantum Technology Initiative (SA QuTI), that outlines the main focus areas for the country. Yet despite this, widespread adoption is lacking, particularly glaring in the financial sector where the promised benefits are tangible but as yet largely unexplored. Here quantum is a double-edged sword. Quantum computing is very fast and potentially a game changer for solving complex problems, but the same power can be used for nefarious means, e.g., decrypting large prime factorised numbers used in Shor's algorithm. Quantum brings this threat but also the solution: quantum communication is fundamentally secure and does not rely on algorithms based on mathematical complexity. When Q-Day arrives - and quantum computers can solve encryption problems in real time - we need to have quantum resistant algorithms or quantum communication systems already in place. Even long before Q-Day, data that requires long term security would have to be transmitted and stored differently to avoid "capture and process later" threats.

For these and other reasons, quantum technology as a subject is increasingly gaining attention amongst regulators and financial market participants. The allure of speed, and a new frontier in computing power, has provided opportunities for the financial sector and others to begin exploring new ways of working. The benefits of quantum, when harnessed, will provide answers to many questions, and some of them will not be in the interest of society. As the limits of quantum are being explored, this paper examines the risk concerns that will dominate the discussions amongst regulators and policymakers as they grapple with the need to protect the public from known and unknown negative impacts.

Quantum technologies

Quantum physics seems a highly esoteric topic, now a century old, yet has given birth to disruptive technologies such as the laser and the transistor. We refer to this as the first quantum revolution. Recent advances in harnessing quantum superpositions and entanglement, allowing the "engineering of quantum states", have given rise to a second quantum revolution, as shown in Figure 1, with a focus on quantum communications, quantum computing and quantum metrology. It is likely to be closely integrated to diverse technologies such as Artificial Intelligence (AI), digitisation of data, machine learning and considered a core security component of future integrated data devices.

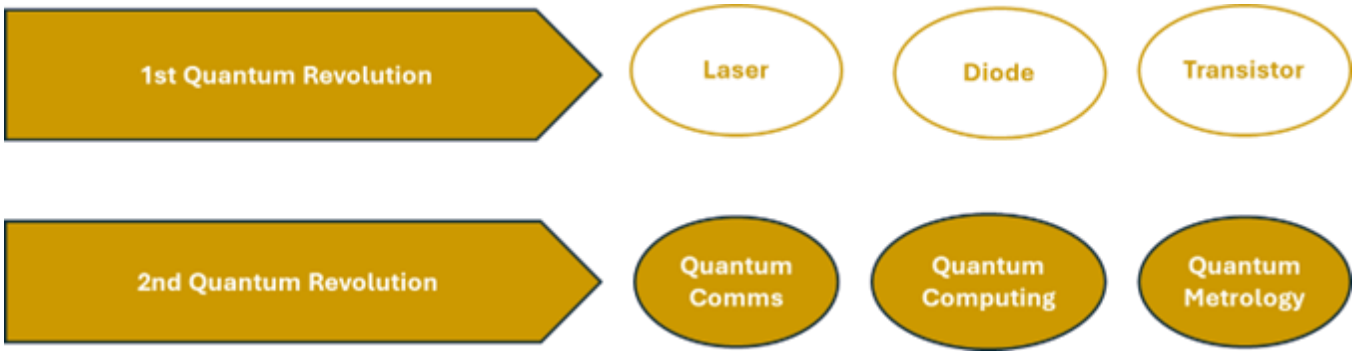

Figure 1: The 1st quantum revolution gave rise to diodes, transistors and the laser, technology used in everyday life. The 2nd quantum revolution promises to harness entanglement for new ways to communicate (quantum communication), compute (quantum computing) and measure (quantum metrology).

The promise can be framed around data, as shown in Figure 2. In the new paradigm, the existing digital approaches to data processing are enhanced with a quantum toolkit. Data is collected by "measurement" with enhanced precision and accuracy, often requiring few measurements than by traditional means. Thus, is broadly referred to as Quantum Metrology, but it encompasses quantum imaging and quantum sensing and has already given rise to new quantum devices that surpass the ability of their classical counterparts. Some of these technologies are already deployed: atomic clocks are a very mature technology, not gaining nor losing a second in 40 billion years, now commercially available as chip-scale devices. They are essential for

accurate timing in stock-market trades and are crucial to our daily navigation through GPS systems.

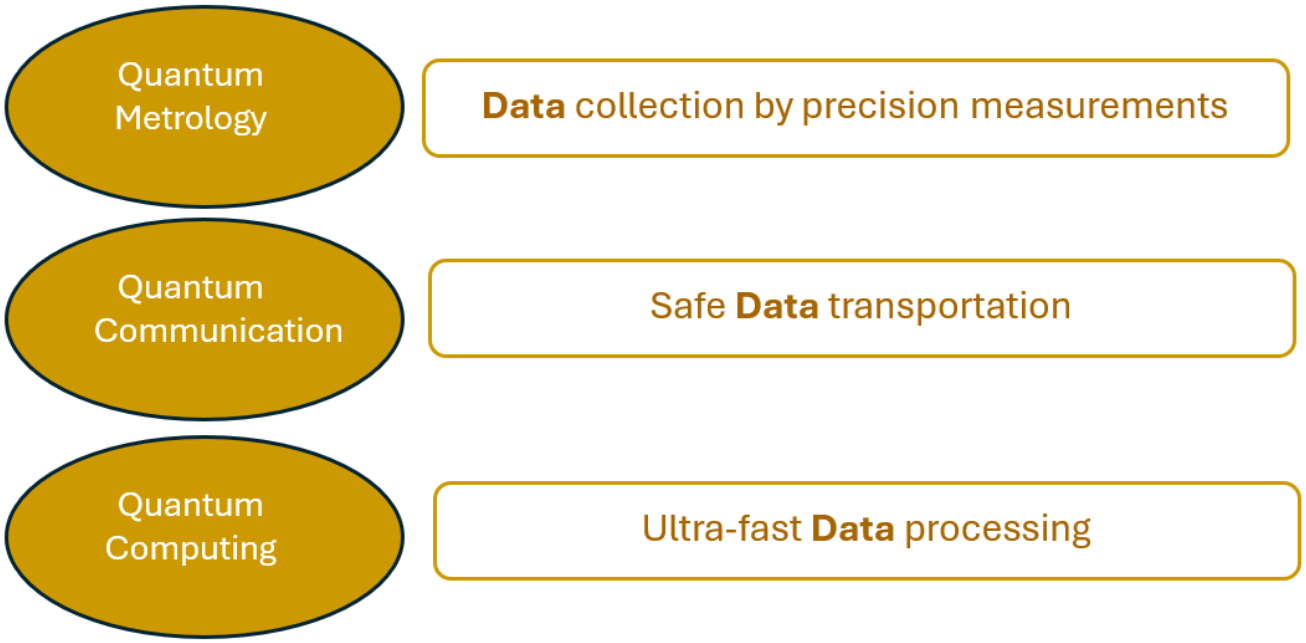

Figure 2: The 2nd quantum revolution is data centric. The traditional digital approach to data processing is enhanced with a quantum toolkit for precise data collection (Quantum Metrology) beyond what is possible with classical approaches, secure data transfer (Quantum Communication) in a manner that is not reliant on mathematical algorithms, and fast data processing (Quantum Computing) for solving problems that would otherwise require an exponential scale up in resources.

Quantum mechanics dictates that quantum states cannot be copied, quantum outcomes are completely random, and quantum states are sensitive to disturbance. Together this lays the foundation for fundamentally secure communication systems that are not based on mathematical algorithms for their security: quantum communication. This allows the transfer of data in a secure manner regardless of the technology of your adversary - i.e., it is unhackable. Today we have terrestrial satellites that facilitate a quantum network across nodes, and commercial quantum key distribution technology that has been deployed in business and municipal precincts. The final step in the data flow is to process the data. Traditional processing using electronic logical gates (our conventional computers) often require exponentially increasing resources for the desired outcome, e.g., the time to search a database might

increase unfavourably with the size of the database, or the computing hardware might increase unfavourably with the data size, and so on.

Quantum computing harnesses quantum superpositions to exponentially increase its apparent resource with limited hardware, thus "cancelling out" the exponential increase in complexity of the aforementioned examples. This allows quantum computers to speed up the data processing time, and to tackle problems that would not be possible on classical machines. Quantum computing is driven mostly by non-academic entities such as DWave, PsiQuantum, Xanadu, Amazon, Google, IBM and Microsoft to name but a few, most offering a commercially available quantum computer delivered via the cloud. Next to the established players, there is a vibrant and rapidly growing start-up scene in both hardware and software for quantum computing and technology.

The potential of the new revolution for global economies cannot be understated. The market size of quantum technologies as of 2024, is estimated to be ~$838m. Quantum sensing is the largest at $587m, with quantum computing ($127m) and quantum communication ($124m) making up the remaining numbers. The present growth projections suggest that the market will increase to ~$1.8 billion by 2029, with quantum computing at $966m, followed by quantum sensing at $617m and quantum communication at ~$249m. This makes quantum technology of economic importance, but it is also of strategic importance due to the nature of the technology: the ability to out-compute existing cryptography systems rendering them vulnerable, but with the capability to circumvent this through built in cryptography for fundamentally secure systems. This has opened a race for quantum supremacy amongst nations, and as a result, all developed nations the world over, as well as all BRICS countries, have national strategies for quantum technologies, as shown in Figure 3. The global investment exceeds $42 billion, with China having invested (and spent) by far the largest fraction at $15 billion. South Africa's investment is modest in comparison to its peers, but it has been strategically allocated for maximum impact and has been increased to ~R140m for the five-year cycle starting in April 2025.

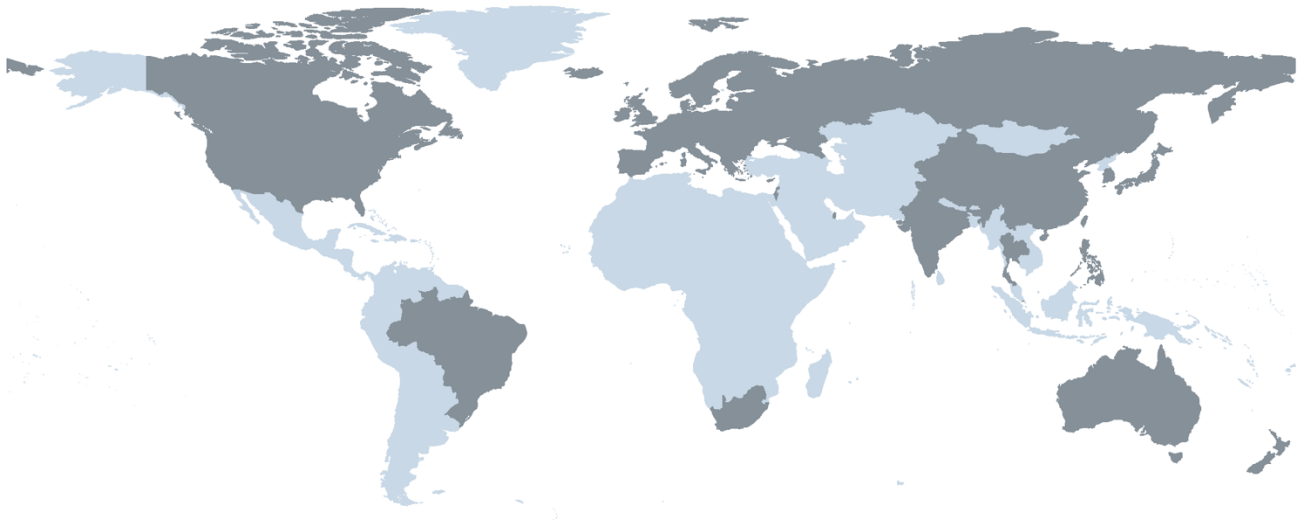

Figure 3: The estimated global investment into quantum is $4-5 billion per year, while venture capital investment is estimated to have peaked at $2.5 billion in 2022. The graphic shows countries with funded national strategies (dark grey), with some regions under-represented, e.g., only Brazil in South America, only South Africa in Africa, and only Israel and Qatar in the Middle East.

It is instructive to consider the approaches and successes of some of the pioneering nations in the quantum race. The UK was the first to publish a national quantum strategy (in 2015) and has invested heavily since, at around 1.1 billion Pounds spent, and a further 2.5 billion Pounds committed over the next 10 years. The government investment has attracted private investment of about $860m, with over 40 new quantum start-ups in operation in the UK as a result. In 2016, China embarked on their quantum future project, with specific emphasis on a national quantum communications network. Their total spend already exceeds $15 billion, far more than any other nation, and they have established a satellite quantum network that links to ground stations in China. In very broad brushstrokes, the US leads quantum computing activities, China leads quantum communication technologies, and the UK/Europe lead quantum sensing technologies.

Status of quantum computing and communication technologies in the financial sector

Quantum computing is very much at the research and development stage, with demonstration phase devices available on-line or for purchase. Presently the technology is in what is referred to as the noisy intermediate scale quantum (NISQ) computing phase – quantum computers have too few "useful" qubits (their building blocks) for them to fulfil their promise, but advances are reported at a steady rate. When the potential is fully realised, estimated to be when we have ~1000 "useful" qubits, they will not only solve problems faster than classical computers but will be able to solve problems that would not be possible on a classical system. Within the financial sector, the broad applications areas that a quantum computer could then add value to include: portfolio optimization, risk management, fraud detection, derivative pricing, market prediction, AI, security and blockchain. This will cut across corporate, investment and retail banking, risk and cybersecurity, asset and wealth management and the operational aspects of the business, with an estimated value at >$600 billion by 2035. The value lies in handling problems with multiple and complex variables, e.g., in securities lending, and doing so in real-time. When blended with AI it offers the potential for "immediate" and "intelligent" risk analysis, with the potential for faster decision making and higher margins at lower risk levels. It should be seen as a powerful tool that will give rise to blended computing, a hybrid of classical and quantum hardware running in the background, which the user will be unaware of. While it will not require quantum experts, it will be essential for users to have a quantum-literate workforce.

Finally, there is the less obvious benefit that quantum computers require far less energy to run than equivalent classical counterparts, this due to the parallel nature of their processing requiring exponentially less resources. This benefit can be orders of

magnitude lower than that required to run modern supercomputers, for what might be called a "quantum energy advantage". In an age when energy is in ever increasing demand due to AI and data centres, a long-term solution without sacrificing performance is surely to be welcomed.

The cybersecurity impact is likely to be doubled edged. Shor's algorithm has been specifically written for quantum computers, providing a recipe for breaking large prime factors in polynomial time rather than exponential time, and could be able to do so within a decade. To address this, NIST has tested and released Post-Quantum Encryption Standards, which are recommended for uptake immediately to circumvent an attack by a quantum computer. Eight years in the making, they alter the type of mathematical problem on which the complexity is based, shifting to a realm where quantum computers are not thought to add significant advantage. History though holds a different lesson: any security solution that is based on the seemingly intractable nature of a problem can be broken when paradigms are shifted, e.g., the enigma machine. The lesson is that security by "technological difficulty or complexity" is not the equivalent to "fundamentally secure". Quantum, however, offers fundamentally secure communication solutions.

Because quantum states cannot be copied, it is not possible to intercept a message, make a copy for yourself, and pass the original on. Further, when this is attempted with a quantum state, the state is immediately altered, and if entangled, its entangled partner is likewise affected. This enables fundamentally secure connections from peer to peer, and the transferring of information in a fundamentally different manner. Quantum communication also leverages on another fundamental property of quantum systems: perfect randomness. It is not possible to predict or guess the quantum state that you will receive. Together these properties foster security based on the laws of nature itself.

In the financial sector, quantum communication has the ability to replace blockchain technology with its quantum counterpart, eliminating money laundering and offering truly non-falsifiable payments. Such "quantum money" could revolutionise security for intra- and interbank trades. The inherent randomness of has

been harnessed for perfect quantum random number generators, ideal for boosting the accuracy and speed of classical Monte Carlo simulations, while quantum versions would offer additional speed-up. Then there is the immediate benefit of creating secure keys (quantum key distribution), sharing keys across network nodes (quantum secret sharing), and teleporting information from one place to another without ever physically sending the data. Of these technologies, quantum key distribution systems are now commercially available and deployed across municipal and satellite links.

The importance of quantum communications to circumvent a quantum attack is clear: such an attack would undermine cybersecurity, eroding the foundation of trust and stability upon which the financial sector operates. Further, this threat cannot be seen as "in the future"; the present risk is "capture now and decrypt later", compromising data that must be secure over long time periods. Although other risks are more immediate, and the legacy digital environments in the sector may make the transition to a quantum-secure system seem long and expensive, it nevertheless has to be factored into future plans. In a globally connected financial system, quantum-safe means all parties are quantum enabled. Here the UK has noted several risks that are both internal and external, for instance, inadequacies due to legacy systems (internal), insufficient quantum talent (internal) and market instability caused by unequal access or distribution of the technology (external), stating categorically in late 2023 that "UK financial sector firms, the third parties that supply them, and regulators that oversee them need to develop comprehensive plans to become Quantum Safe".

The South African quantum technology initiative

The South African Quantum Technology Initiative was formally presented and approved by the Department of Science and Innovation (DSI) Executive Committee in March 2021, supported by R8 million in seed funding for 2021/22, and a R54 million for a 3-year programme from 2023-2025. More recently, it has been allocated R142 million for a 5-year period from 2025-2030. SA QuTI seeks to create the conditions in South Africa for a globally competitive research environment in quantum technology, and to grow a local quantum technology industry for South Africa. SA QuTI plans to implement programmes to address several key recommendations made in the strategy, which have been paraphrased from the strategy document below:

1. Education and training programmes, to build skills
2. Advocacy, to create awareness and disseminate information on quantum technologies to key stakeholders, including the public, government and private sector.
3. Create critical mass, through strengthening established quantum centres and supporting senior and emerging research chairs.
4. Governance and coordination, for national coordination, particularly of synergetic activities, and to drive legislative, standardisation and certification activities. The aim is to

   SUPPORT the development of local quantum technological capabilities in general,

   COORDINATE quantum technology projects to the benefit of South Africa,

   NURTURE public-private partnerships between research communities to deliver intellectual property that can be commercialized.

5. Establish flagship programmes, in the focus areas of communication, computing and sensing, to drive science through to technology, and allow for faster uptake by commercial partners.
6. Establish new emerging centres, with the aim of diversity in demographics, geographics, and in quantum theme.
7. Accelerate a quantum industry through strategic and financial support for technology development and deployment
8. Facilitate quantum technology legislation and validation, by providing a national context for a quantum enabled future through government interventions in the form of local economic clusters, legislation with respect to the transition to and adoption of quantum technology and formalise the need for validation.

The plan moots the notion that "more of" the present will not move South Africa into a quantum future. The hope is that the co-ordinated approach will see the rapid growth of a quantum community in South Africa, addressing critical mass and succession planning. Awareness and outreach are crucial, not only to the public but also to government and private sector stakeholders. For example, in addition to the usual public outreach programmes and initiatives, the strategy also speaks to lobbying government for legislative changes, working closely with standards institutes to drive quantum validation and certification. The strategy is to convert "trained students" into a "quantum-literate workforce", and to this end SA QuTI seeks to have government ministries on board to create an environment for the deployment of quantum technologies, e.g., that encryption should become quantum by some agreed date based on detailed discussion and that an economic zone is created for quantum technologies to encourage local production. Key to the initiative is where to fund quantum, and this is largely dictated by the flagship projects. South African will not build a quantum computer but rather use commercially available quantum computers and focus on quantum software development. In a quantum communications flagship, the idea is to focus on technology integration from partner institutes across South Africa, comprising

sources, detectors, protocols and networks, to establish local quantum secure links between universities, key government sites, and strategic industry locations in the financial sector. In quantum sensing there is a strong health focus, to apply quantum technologies to locally relevant issues.

Progress over the past three years of SA QuTI has been significant, now reaching nearly half of the universities in South Africa through direct investment, and nearly all of them through workshops and training events. SA QuTI support has been extended to students and programmes at potential new quantum centres, encompassing institutions such as the University of Pretoria, the University of Cape Town, Sol Plaatje University, the University of the Western Cape, and the Durban University of Technology. This strategic investment aims to foster the growth of quantum research and education across diverse academic landscapes within South Africa.

The programme has established five nodes around South Africa at the University of the Witwatersrand (Wits), the University of KwaZulu-Natal (UKZN), Stellenbosch University (SU), Cape Peninsula University of Technology (CPUT), and the University of Zululand (UNIZULU). A 2024 snapshot reveals ~90 students and postdocs supported at the various nodes, and ~20 full-time academics. The nodes' activities include outreach, education, human capital development and research, with disciplines covering quantum physics, quantum engineering, quantum communication, quantum computing, quantum simulation, quantum machine learning, quantum chemistry, quantum devices, quantum biology, quantum materials and commercialisation and prototyping of quantum technology. The nodes have used SA QuTI funding to leverage investment and grow activities across each host institution, for example, new initiatives such as WitsQ (Wits), the Centre for Quantum Computing and Technology (UKZN) and the Centre for Quantum Science and Technology (SU). These initiatives and centres aim to foster interdisciplinary collaboration, industry engagement, and have established various dedicated positions ranging from postgraduate students to professors. The CPUT node is currently the only engineering faculty in the country that is engaged in quantum technology and driving technology development, while the

UNIZULU node, predominately in chemistry, is investigating topological materials and superconductors for potential technological applications.

The main national nodes have been significantly supported and have now well-established quantum programmes. Significant co-investment has been attracted, notably through industry, university, and external investors. The focus on technology development is moving steadily with image teleportation, AI enhanced quantum imaging and quantum measurement devices at Wits. There are also early prototypes for nitrogen-vacancy single photon source, nanowire-based quantum random number generators and quantum plasmonic biosensors. The first spinouts, Button Optics (Wits), QUSTEL (SU) and GWP Q Labs (CPUT) have been launched with the aim to commercialise technology and devices, with Button Optics already receiving venture capital funding. Science continues at a good pace with >120 journal papers since 2022, several making international news, for instance, the first high-dimensional teleportation (nature communications) and the first quantum topologies (nature photonics). Advocacy is ongoing and includes a healthy online presence (website and social media), regular (almost weekly) talks to public, academic and commercial entities, with further information and videos available on their website.

SA QuTI and the financial sector

SA QuTI's strategy and implementation is potentially well aligned with the financial sector. In particular,

SA QuTI provide opportunities for training and awareness, from a high-level overview to in-depth on particular quantum technologies, to promote quantum literacy,

SA QuTI provides access to quantum computing facilities, as well as training and expertise to make use of a quantum computer, reducing the entry barrier for financial sector technical staff,

SA QuTI nodes have extensive experience and know-how on quantum computing, as well as young student talent. This can be leveraged by the financial sector to "play" on a quantum computer at low risk and low investment,

SA QuTI seeks to deploy quantum technologies in the financial sector, by empowering local crypto service providers and by partnering with financial sector players to develop test beds for quantum cryptography,

AS SA QuTI centres are at universities, access to quantum talent for uptake as interns allows for a low cost entry into quantum,

SA QuTI could assist with strategic input on becoming quantum ready for a quantum future.

The financial sector could help move South Africa into this quantum future by become active participants in the use of quantum technologies, e.g., quantum computers for solving financial problems by testing the hacking potential of quantum computers. They could be strategic in their quantum intent, budget for a quantum exploration programme, and absorb young talent to explore the potential of quantum to impact on their business.

Quantum readiness of the financial sector

Focusing on the experiences of the banking industry, we were surprised to find no projects being funded in quantum research, nor a formal quantum strategy within any of the banks. Many of the senior bankers interviewed were aware of quantum security and in some cases had personally researched the subject, but there was no engagement with SA QuTI and limited awareness of a national quantum strategy. Some banks have held discussions at leadership levels about quantum computing, but there are no clear strategies emerging. Security risk mitigation in communication and fraud reduction would be the focal point of conversations, while potential efficiency opportunities to be harnessed through quantum computing have not been considered.

The substantial cost and technical complexity of building a quantum computer makes it impractical for South Africa to build a local option. However, quantum software development tailored for financial applications, research into quantum security and encryption technologies through strategic partnerships, would be achievable. Third party dependency remains a concern among regulators and quantum computing will add to this dialogue.

South Africa has the potential to become a trusted jurisdiction for quantum security validation and certification globally but will need to manage the current geopolitical tensions well to do so.

The highly regulated nature of banking combined with their compliance culture, and the ever-present security concerns, provided a natural backdrop to the suggestion that quantum should be regulated. However, regulation should be considered, within the need for some flexibility to ensure innovation is not inadvertently stifled, and a risk-based approach rather than technology-based approach was proposed as an appropriately balanced interim measure. With international standards more likely to govern best practices in quantum computing, this recommended regulatory flexibility

should embrace the rapid evolution of quantum globally and allow for immediate transformation of the regulatory framework.

Aligning quantum regulation with existing data protection laws and industry security standards would be needed to provide an enforceable legal framework. Self-regulation is not practical, and with the highly interconnected nature of finance, could leave the system unintentionally exposed through a single point of failure. The main concern is the misuse of quantum computers and the most prevalent threat, that of the potential to break existing encryption standards.

For the financial sector, quantum computing poses a direct threat to widely used encryption methods including RSA (Rivest-Shamir-Adleman) and EAS 128-bit encryption. Focused engagement on digital certificates and authentication mechanisms as well as data security in motion and at rest, will provide opportunities for immediate discussion, while outdated banking encryption protocols will need to be proactively decommissioned.

The steal now, decrypt later attacks pose a significant risk to the global financial system and regulators will need to begin considering operational risk strategies to mitigate against Q-Day. Just like Y2K, when the potential for computers across the world to fail simultaneously became a global concern, strategies will need to be developed to understand the potential impact of bad actors using quantum computers to disrupt the financial sector. To keep the important functions of the financial sector available to society, until the system is quantum safe, will require a co-ordinated operational risk approach.

Implementation of quantum security solutions may require regulators to step in and mandate compliance with specific standards to overcome adoption barriers, especially in the smaller banks where budgets and expertise could be a problem. Industry alignment and industry driven research may benefit from a quantum centre of excellence.

Quantum computing provides an opportunity to explore potential use cases in fraud detection and account takeover prevention. In theory, quantum computing can

bring to the banking industry the opportunity to perform these functions in real time and if successful reduce the impact on society, but also reduce the substantial cost to banks of fraud which could cross-subsidise their investment into fraud prevention and other commercial quantum opportunities like Monte-Carlo simulations etc.

Perspectives and the way forward

South Africa's financial sector is not presently quantum safe. Barriers to mitigate this include lack of strategic intent at the decision-making levels, and lack of awareness and technical know-how at the implementation levels. The latter can be overcome through advocacy and training in collaboration with South African quantum centres, and particularly SA QuTI, who provide some "handholding" to lower the barrier to entry, training, access to quantum computers and wish to encourage internship programmes to increase quantum activity at financial institutions.

A broader financial sector stakeholder engagement model would enable knowledge transfer that creates awareness, so that the institution can begin preparing early for the broader adoption of quantum in society. Risk mitigation strategies and business opportunities require curation, and this takes time.

Regulators and policy makers should also be included in formulating a financial sector strategy, within the national strategy, that will in turn lead to a well-considered legislative framework that supports the objectives of the financial sector.

An industry-wide quantum readiness roadmap with clear business cases for financial institutions would galvanise resources, both financial and human, and with the establishment of a cross-industry or sectoral working group, would assist in the development and monitoring of progress. A quantum centre of excellence could support various industries with their adoption strategies and technology.

Software development, quantum security and compliance research should remain the focus with the potential for South Africa to offer a quantum security and compliance hub both locally, and more broadly for the African Continent, and potentially further afield.

A proactive transition to quantum-resistant encryption solutions needs to be facilitated to mitigate against earlier than anticipated quantum threats materialise. This could be achieved through a phased encryption update strategy in conjunction with the regulator.

Conclusion

Major financial players internationally have clear strategies and plans to become quantum safe, and to exploit quantum for the benefit to their business. South Africa's financial sectors are not presently quantum safe and have not yet explored the business opportunities of quantum technologies. Barriers to mitigate this include lack of strategic intent at the decision-making levels, and lack of awareness and technical know-how at the implementation levels. The latter can be overcome through advocacy and training in collaboration with South African quantum centres, and particularly SA QuTI, who provide some "handholding" to lower the barrier to entry, training, access to quantum computers and wish to encourage internship programmes to increase quantum activity at financial institutions.

For the financial sector to become quantum safe, more work needs to be done as a collective, to ensure the threats of quantum are clearly addressed, whilst the benefits are competitively explored. Regulators will need to engage on minimum standards and clear implementation guidelines to ensure the sector is quantum safe, whilst implementing strategies to address the risks of not achieving quantum safe in time.

Bibliography

Dowling, Jonathan P., and Gerard J. Milburn. "Quantum technology: the second quantum revolution." Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 361.1809 (2003): 1655-1674.

Forbes, Andrew, Francesco Petruccione, and Filippus S. Roux. "Toward a quantum future for South Africa." AVS Quantum Science 3.4 (2021).

Jung, Eliot. The Impact of Quantum Information Science and Technology on National Security. Diss. Purdue University Graduate School, 2024.

Putranto, Dedy Septono Catur, et al. "A Deep Inside Quantum Technology Industry Trends and Future Implications." IEEE Access 12 (2024): 115776.

Qureca. 2025. Quantum Initiatives Worldwide 2025. [Online] Available: https://www.qureca.com/quantum-initiatives-worldwide/#references

Thew, Rob, Thomas Jennewein, and Masahide Sasaki. "Focus on quantum science and technology initiatives around the world." Quantum Sci. Technol 5.1 (2019): 010201.

World Economic Forum. 2022. State of Quantum Computing: Building a Quantum Economy Insight Report [Online] Available: https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf

World Economic Forum. 2024. Quantum Economy Blueprint Insight report. [Online] Available: https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

Yole Group. 2024. Product report Quantum Technologies. [Online] Available: https://www.yolegroup.com/product/report/quantum-technologies-2024/

Appendix A: Interview research questions

Introductory questions:

1. Are you aware that South Africa has a Quantum strategy?
    a. If yes, are you involved in any way or have attended any events?
2. Are you aware that South Africa is not considering building a Quantum computer?
3. What do you think are the positive and negative ramifications of this decision?

General questions:

4. Do you think Quantum should be legislated?
5. What would a trigger point be that would convince you that Quantum computers have reach a security risk level?
6. What types of security risks do you think Quantum computers pose?
7. Once they impact on day-to-day security, what measures are you considering for mitigation?
8. Do you see Quantum as only a cost/threat or also an opportunity?
    a. If yes, what opportunities are you exploring for your organisation?
9. What Quantum technologies other than Quantum computers are you aware of?
10. Have you considered adopting and deploying Quantum technologies such as Quantum communication?
11. On a scale from 1 - 10, how would you rate your ability as an intelligent buyer of Quantum technology?
12. Would you consider it a security risk if the Quantum technologies were not home grown?

13. What sort of validation and verification processes would you like to see in place for Quantum technologies?

14. South Africa believes that it can position itself to take advantage of a Quantum economy.

    a. Do you have any measure for how big this might be?

    b. Do you think South Africa could be a neutral centre for Quantum hardware and software testing.

15. What image does "Quantum hardware" invoke? For instance, what applications will be used over what devices and for what purpose?

Industry questions:

16. How do we get widespread adoption of Quantum technology within the financial sector?

17. What could be holding us back: technology readiness, the appropriateness of the technology, or the lack of understanding?

18. What use cases do you see for banks and other financial institutions?

    a. How far off are these use cases?

19. What topics should the financial sector focus on and should we have a roadmap that is dedicated to the financial sector, building on the more general national Quantum strategy?

20. We have local players in Quantum computing, from companies to academia. Are you aware of their offering and is it relevant to you?

Organisational questions:

21. At what level have you discussed Quantum in your organisation?

    a. Has it made the agenda of your board, the agenda of a risk committee or is it still a technical discussion among interested parties?

    b. Do you intend tabling a document with your board for awareness?

22. Does your organisation have a Quantum strategy?
23. Does your organisation use or plan to use a Quantum computing?
    a. If yes, for what tasks? If no, why not?
24. What would accelerate your uptake of Quantum technologies?
25. Are you aware of any overseas peers using Quantum technology to enhance their business?
26. Do you have a budget for “Quantum” in your organisation?
    a. Is it a well-defined project or exploratory?
    b. What are the timelines involved?
27. Have you ever invested in “Quantum” either directly or indirectly?
    a. Could you share the value?

Appendix B: Draft introductory letter

To Whom It May Concern:

Quantum computing is expected to be as foundationally transformative as the onset of classical computing was in the mid-20th century, offering a new approach to computing with unparalleled power. Once a pipedream, quantum computers are now very much a reality. The pace of development is unprecedented, with quantum technologies having received investment in the order of $35b (2022). As a result, impressive demonstration devices already exist and can be accessed and utilised via the cloud, with the full promise expected to be realised within a decade.

Within the financial sector the broad applications areas that a quantum computer could then add value to include portfolio optimization, risk management, fraud detection, derivative pricing, market prediction, AI, security and blockchain. This will cut across corporate, investment and retail banking, risk and cybersecurity, asset and wealth management and the operational aspects of the business, with an estimated value at >$600 billion by 2035. The value lies in handling problems with multiple and complex variables, e.g., in securities lending, and doing so in real-time. When blended with AI it offers the potential for "immediate" and "intelligent" risk analysis, with the potential for faster decision making and higher margins at lower risk levels. It should be seen as a powerful tool that will give rise to blended computing, a hybrid of classical and quantum hardware running in the background, which the user will be unaware of. While it will not require quantum experts, it will be essential for players to have a quantum-literate workforce.

In the financial sector the impact is bi-directional, positive and negative, on existing technology areas such as AI, cybersecurity and blockchain. The primary risk is to make modern encryption redundant. While nobody knows for sure when a sufficiently powerful quantum computer will arrive, the timeline is shrinking, and transitions of this nature require time, resources and careful planning. This is not a future risk – the immediate risk is "capture now and decrypt later", compromising the security of

long-term data. Avoidance is no longer a viable strategy, with many major international financial players already planning for a quantum safe future.

In bringing this to your attention, we advocate for the following actions:

- Establishment of a Quantum Safe taskforce that cuts across all affected areas in the organisation, as well as key partners and third-party vendors.
- Assessment of the risk and opportunities that quantum technologies in general, and quantum computing in particular, bring to the organisation. To answer the question how will you be safe in a post quantum computer era, and how can you benefit from the emerging quantum economy?
- An immediate transition programme to adopt quantum safe algorithms, such as those developed and standardised by NIST.
- Development of a quantum strategy appropriately resourced for implementation.
- Engagement with South Africa's Quantum Technology Initiative (SA QuTI) to embrace quantum technologies, e.g., access to quantum computers, with the aim of exploring its risks and benefits, raising education and awareness within the organisation, staying abreast of fast changing developments, and accelerating a quantum-literate workforce.

While it may be tempting to abdicate these tasks to suppliers, particularly those offering cybersecurity, the international community strongly advises against this. According to Prof. Andrew Forbes, Director of SA QuTI, "it is vital that all parts of the financial services sector become fully aware and appropriately engaged, for only then can cross-sectorial strategies be effectively deployed. The cost of no action will be dire: imagine your organisation today but without its computing power and without its cryptographic security – what would the business look like? How will you compete in a quantum driven economy without a quantum-literate and enabled workforce?"

2025 marks the UNESCO International Year of Quantum Science and Technology, in recognition of the importance of quantum technologies in the modern world. We urge the organisation to embrace the challenge, unlock the opportunity, and implement a strategy with urgency.