



# To qubit or not to qubit – is that the question?

**A point of view on the world of  
quantum cryptography and life  
in a post quantum world**

**May 2021**

-

**home.kpmg/in**

**Click here to  
access**



# Introduction (1/2)



## What is quantum?



### Shakespeare's cat

To be  
or  
not to be...

The Schrodinger's cat has been a source of memes and speculation over the years with multiple people such as Everett, Copenhagen and others trying to interpret what Schrodinger meant to say.

The cat continues to be one of the most utopian themes in modern physics and has laid down the bedrock for quantum physics.

According to physics, Quantum, also known as **plural quanta** is the least or the most minute quantification of physical property. This can also be referred to as indivisible.

For example: -

- A photon of light.
- A water molecule

The concept of superposition, which basically means that one particle can exist in 2 spin states while in motion, is one of the formative concepts in quantum computing.

To understand quantum computing, we would need to understand the key concepts below –

- **Photon**
- **Qubit**
  - Superposition
  - Entanglement
- **Polarization**

We will attempt to unravel the concepts behind this as we go further.

### Schrodinger's cat



Both

- Photon: is the **smallest unit of light** that can travel at the speed of light. It follows the Heisenberg's Uncertainty Principle, that the wave function of a particle (position and momentum) cannot be measured simultaneously.
- Qubit: Is the equivalent data unit for quantum computing systems. It exists in both states (0 and 1) at any point in time allowing simultaneous computations.

The concept of existence of a particle in two states at the same time as immortalized by Schrodinger's cat is known as **superposition**.

## Introduction

### Relevance of quantum physics in business

### Quantum computing and quantum cryptography

### How do we secure today from the future?

### Where to from here?

### In conclusion

### Acknowledgements

# Introduction (2/2)



Another important concept in quantum computing is **Quantum Entanglement**. Photon particles that have interacted at some point with each other tend to retain a characteristic and can be entangled with each other in pairs, in a process known as correlation (**similar to a pair of magnets interacting with each other**).

Knowing the spin state of one entangled photon particle – ‘up’ or ‘down’ - allows us to know the spin state of the other particle.

Therefore, quantum entanglement allows qubits that are separated by incredible distances to interact with each other instantaneously (not limited to the speed of light).

Taken together, quantum superposition and entanglement create enhanced computing power.

A 2-bit register in an ordinary computer can store only one of four binary configurations (00, 01, 10, or 11) at any given time, a 2-qubit register in a quantum computer can store all four numbers simultaneously because each qubit represents two values. If more qubits are added, the increased capacity is expanded exponentially.

Therefore, quantum computers can solve problems faster than a normal computer. This also makes it possible to store and manipulate vast amounts of information in relatively smaller number of storage units.

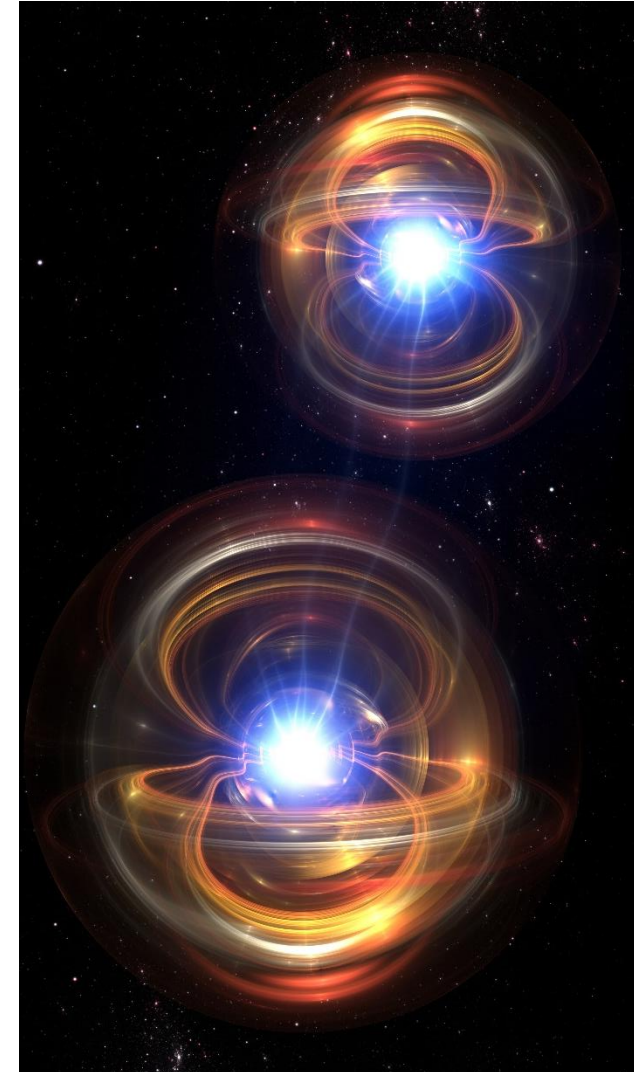
- iii. Polarization: Polarization is a concept where it is possible to **block out certain parts of the light waves** based on their geometrical orientation.

Polarization of photons and light is an important component of quantum key distribution and will be explained further.

Quantum computing is therefore a gamechanger in terms of processing speeds and storage.

Quantum computing has the potential to solve a complete problem faster to get better solutions and optimize business.

The relevance of quantum computing to business and services will be explained in subsequent sections.



## Introduction

### Relevance of quantum physics in business

### Quantum computing and quantum cryptography

### How do we secure today from the future?

### Where to from here?

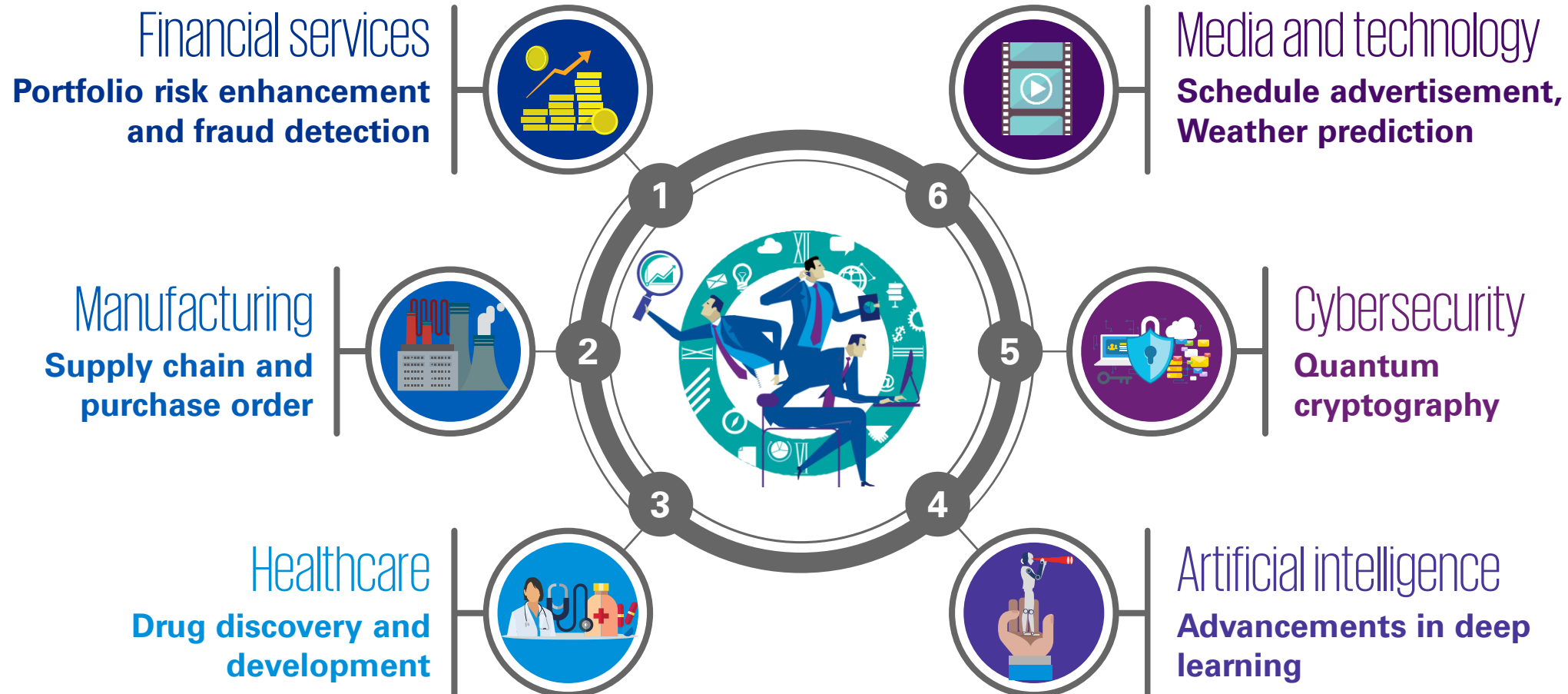
### In conclusion

### Acknowledgements

# Relevance of quantum physics in business



Quantum physics is good at solving problems where we have a small input and output having a vast array of possibilities. This is true in the case of different applications of quantum physics to computing business cases to solve problems in the future using technology such as quantum computing and quantum cryptography. The business use cases mentioned below for quantum computing are illustrative in nature and not exhaustive.



Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements



# Quantum computing and quantum cryptography (1/2)



## What is quantum computing

Quantum power is the ability to perform an operation faster than a classical computer. Quantum computing will be useful wherever there is a large, uncertain and complicated system that needs to be simulated. Using 53 bit quantum computer Google demonstrated that it was possible to perform a specific operation that would take 10,000 years in a classical computer in just 200 seconds.

This could be used for modeling complex computations such as gene modeling / mapping for biotechnology firms. It is also predicted to be used in R&D for drug discovery and design in order to ensure higher success rates in clinical trials.

In recent times, the time taken for vaccine development and its research can be immensely reduced by using quantum computing platforms.<sup>1</sup>

There could also be applications in predicting financial markets and creating complex models for prediction. Further, it can also be used to improve weather forecasts.

## Quantum computing as a service on cloud:

Quantum computing on cloud as a service is more accessible now than ever before. IBM, Google, Microsoft and Amazon are working towards achieving quantum supremacy.

Below are a few cloud based quantum services -

- IBM Quantum Experience
- Amazon Braket
- Azure Quantum

How does it work:

The commands from a classical computer will be sent to a quantum computer hosted on the cloud.

On the quantum computing cloud, these commands are translated into microwave pulses, with frequencies that control qubits and change their quantum states for high speed computation.

Once the data is processed by the quantum computers on the cloud, it is then sent back to the users in the classical form of binary data (0's and 1's) received by their computers.

## Quantum cryptography

Quantum Cryptography is the mechanism of utilizing the characteristics of photons such as superposition and entanglement to allow two users to communicate more securely than those allowed by traditional cryptography.

There are multiple research projects in progress on the impacts of quantum computing on cryptography. Notably, the National Institute of Standards and Technology (NIST) has conducted a post quantum cryptography analysis and finalized 7 algorithms which may still be usable cryptographic algorithms after quantum computing becomes commercial.

Further, there are rumors of large intelligence agencies harvesting data to be decrypted once they have access to quantum computing giving them the ability to decrypt weaker cryptographic algorithms.

## Origin of quantum cryptography

In 1994, A mathematician called Peter Shor from Bell Labs theoretically found a way in quantum computing to break code which relied on factorization of large numbers into primes.<sup>2</sup> Using the algorithm by Peter Shor, called the Shor algorithm, a quantum computer could perform the task in a few hours. This could lead to cracking most modern cryptographic algorithms in use today..

This led to the need for quantum cryptography, which eventually led to a popular algorithm known as BB84.<sup>3</sup>



1. <https://www.expresscomputer.in/guest-blogs/how-quantum-computing-can-help-in-tackling-global-pandemics-such-as-coronavirus/55229/>
2. <https://www.historyofinformation.com/detail.php?id=3877#:~:text=In%201994%20American%20applied%20mathematician,quantum%20algorithm%20for%20integer%20factorization.>
3. [http://www.iteam.upv.es/wp-content/uploads/pdf\\_articles/41.pdf](http://www.iteam.upv.es/wp-content/uploads/pdf_articles/41.pdf)

Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements

# Quantum Computing and Quantum Cryptography (2/2)



## Normal communications (TCPIP)

In traditional TCP/IP based communications, a sender transmits packets in the form of binary bits (0s and 1s) to the receiver. An attacker intercepting the traffic, can make a copy of the traffic without interfering with the message integrity as it travels to the receiver.

Quantum cryptography makes use of photons for data communication. An attacker intercepting the traffic tends to create a disturbance (change in the angle leading to changed state of data) in the communication stream affecting the integrity of the message being transmitted .

Further, while traditional communication channels makes use of two states a quantum channel make use of 4 states (positive, negative, orthogonal and rectilinear). These are the spin states in which the photon beam is interpreted by the receiver.

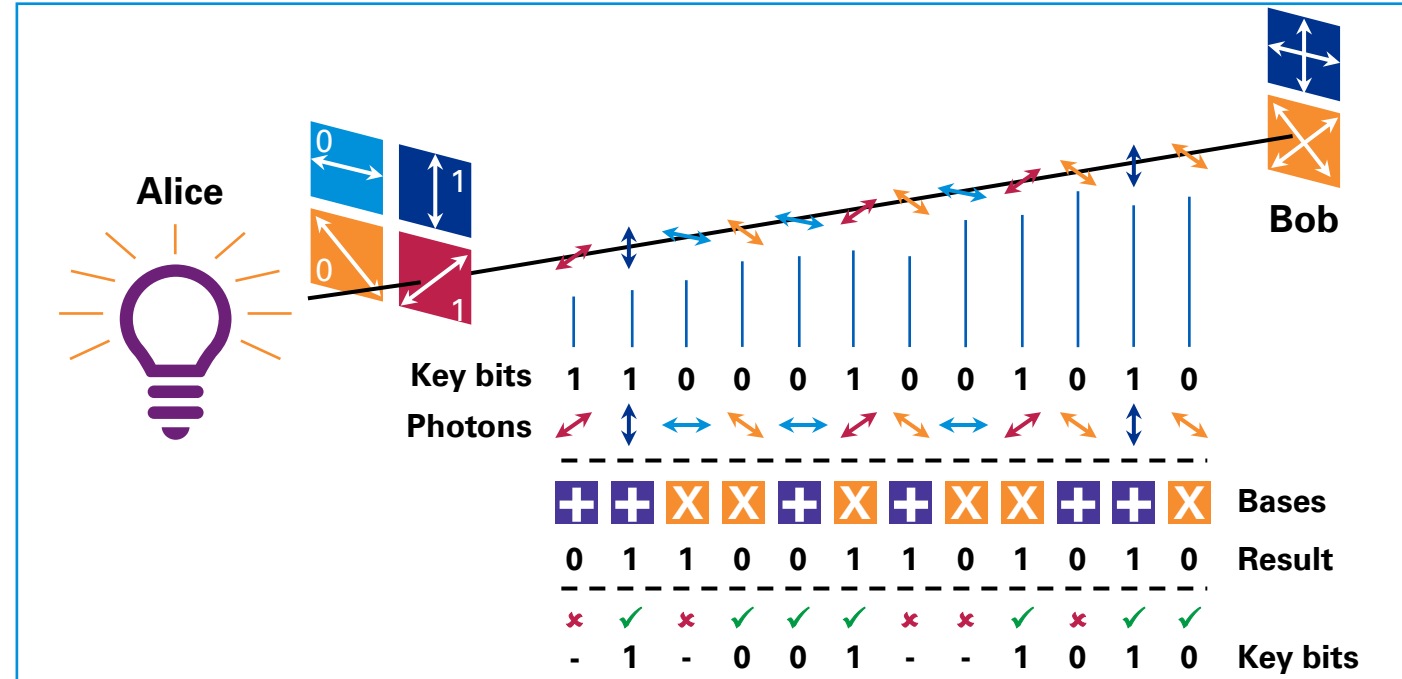
## BB84

In BB84 protocol, a sender (Alice) chooses an arbitrary basis (any one of the states mentioned earlier) for the data and sends the data over the Quantum Channel, to the receiver (Bob).

Bob measures the spin state in an randomly chosen basis. Bob then sends back information containing the data and bases chosen over the public channel to the sender and keeps the outcome of each measurement secret.

After the sender gets the receiver's info, the receiver can compare it to their own chosen bases and select the coincidences. The sender sends the information on the coinciding bases back to receiver and the

## Introduction to Quantum Key Distribution<sup>4</sup>



Quantum Key Distribution (QKD) QKD provides a way of distributing and sharing secret keys that are necessary for cryptographic protocols. The concept is similar to that of symmetric key cryptography except the fact that the key is shared over quantum channel and the data is shared over public channel.

One of the challenges for QKD is the distance over which the photons can travel, which is typically around 100 kms.

A number of organizations globally have been able to circumvent this restriction and share keys up to 500 kms using newer protocols such as Sending-or-not-Sending Twin Field (SNS-TF).

4. Courtesy QNu Labs

Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements

# How do we secure today from the future? (1/3)



**Quantum computing and supremacy may still be a race, but quantum cryptography is a reality and is here to stay**



## Quantum random number generator –

Random number generation is a key security element in cryptography today. It has applications in multiple areas across generation of seed keys, random passwords, OTPs, session keys and other trusted forms of communication.

The strength of the key, lies in the strength of the entropy source used for generating the cryptographic keys.

Random key generators with widely used libraries have today been identified as insecure and vulnerable to prediction or bias.

Quantum random generators provide a truly random number with unique entropy which allows a user to generate a completely unique and random number without any practical bias.

Below, is a brief comparison between traditional number generators and quantum generators.

Classical RNG <sup>4</sup>	Quantum RNG <sup>5</sup>
Software based pseudo random generators that use algorithms are limited by the original seed numbers.	Not limited by any initial seed numbers, making it truly random.
Physical random generators limited to either high entropy or high throughput, never both.	Can achieve both high entropy and high throughput.
Classical physics on which physical random generator depend, are deterministic and predictable	Quantum physics based random generators are fundamentally and intrinsically random.
Physical random generators are prone to bias and has to be corrected with post-processing algorithms	The bias, if any, are negligible.
Vulnerable to quantum computers.	Impregnable to quantum computers.

5. Courtesy : QNU Labs

Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements

# How do we secure today from the future? (2/3)



## Entropy as a Service (EaaS)

The increase in IoT devices today and in critical infrastructure has resulted in organizations wanting to use secure cryptography without possibly having to configure or replace their infrastructure.

Key as a service without having the pains of managing the infrastructure is already a known concept with Cloud Service Providers (CSP) such as AWS and Azure, which provide key management services. There are traditional banking infrastructure such as HSM(Hardware Security Modules) which are responsible for encrypting traffic across all possible banking channels such as ATM and SWIFT.

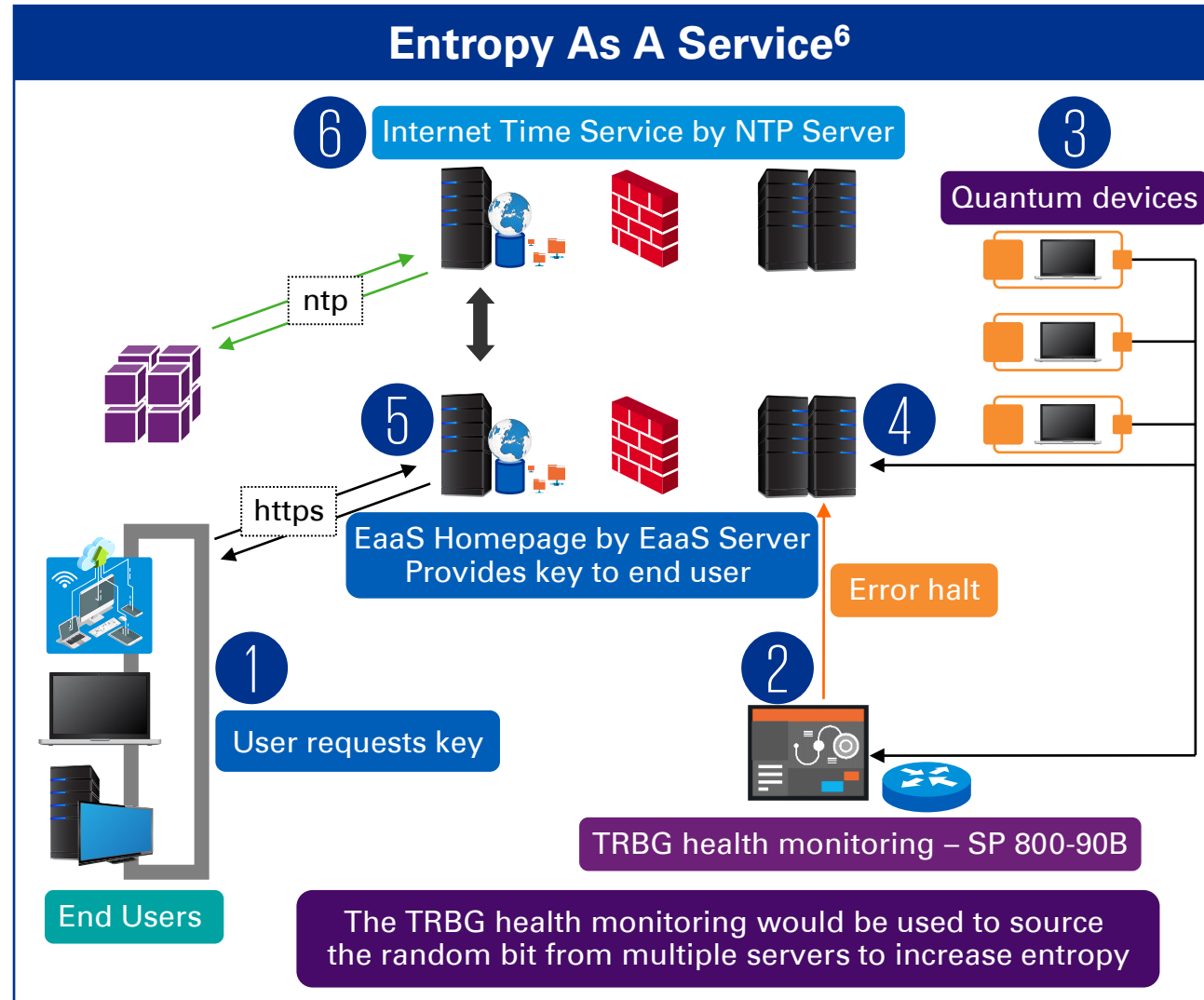
EaaS generates a seed which is provided to the local server or Public Key Infrastructure (PKI) setup to increase the randomness of the locally generated key. The EaaS server itself never saves the keys or gains knowledge of the ultimate key.

The generation of the seed via quantum cryptography requires expensive equipment. Therefore, EaaS helps organizations utilize the advantages of quantum cryptography without setting up costs.

This is a subscription-based model in general and helps organizations integrate secure keys over their traditional communication channels.

This can be used to provide entropy bits, time stamp and server's digital signature over the Internet to the requesting client organization. This can then be used for a variety of systems such as vehicle management, IoT devices (especially wearable devices transmitting sensitive patient health data).

6. Courtesy : QNU Labs



Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements

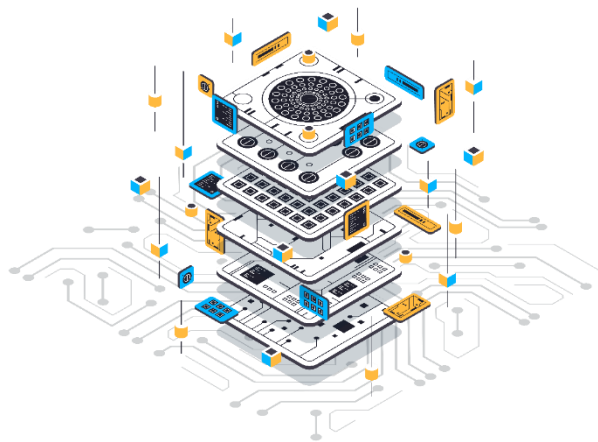


# How do we secure today from the future? (3/3)

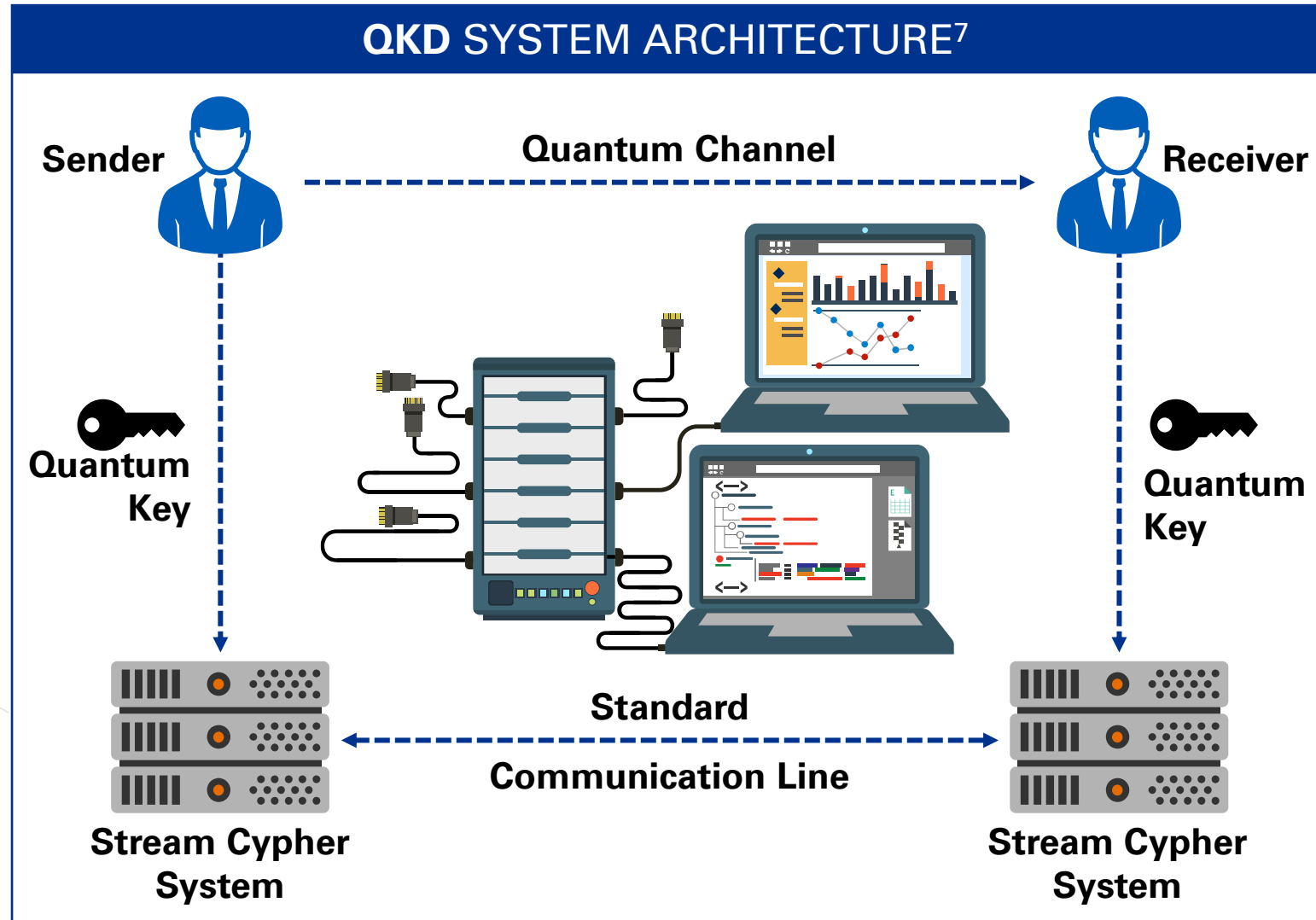
## Quantum Key Distribution (QKD) and key management –

The QKD mechanism takes the quantum key service a notch higher by allowing organizations to generate and manage their own quantum keys. In their base model this allows an organization to implement an architecture to communicate and transmit secure keys over traditional channels.

This enables organizations to secure the keys in use while still leveraging the standard communication channels. In this way even if the standard channel is compromised the keys are still secure.



7. Courtesy QNU Labs



Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements

# Where to from here? (1/3)



Implementations of quantum cryptography at certain levels equates to science fiction that we see on television screens. However, 20 years ago who would have thought every Indian would have access to mobile phones, internet and digital shopping would be a way of life for us? .

However, futuristic technology often begs the question that while theoretically possible, is it practically feasible for large scale commercial use apart from defense departments or government funded research projects.

The advent of Quantum Key Distribution (QKD) does show that many of these use cases have left the siloed and secretive corridors of defense departments and research, and have now moved to commercial use cases.

## Post quantum cryptography

NIST has been conducting post quantum cryptography research on various algorithms which they think will not survive once a quantum computing engine is commercialized with larger groups of people having easier access to these systems.

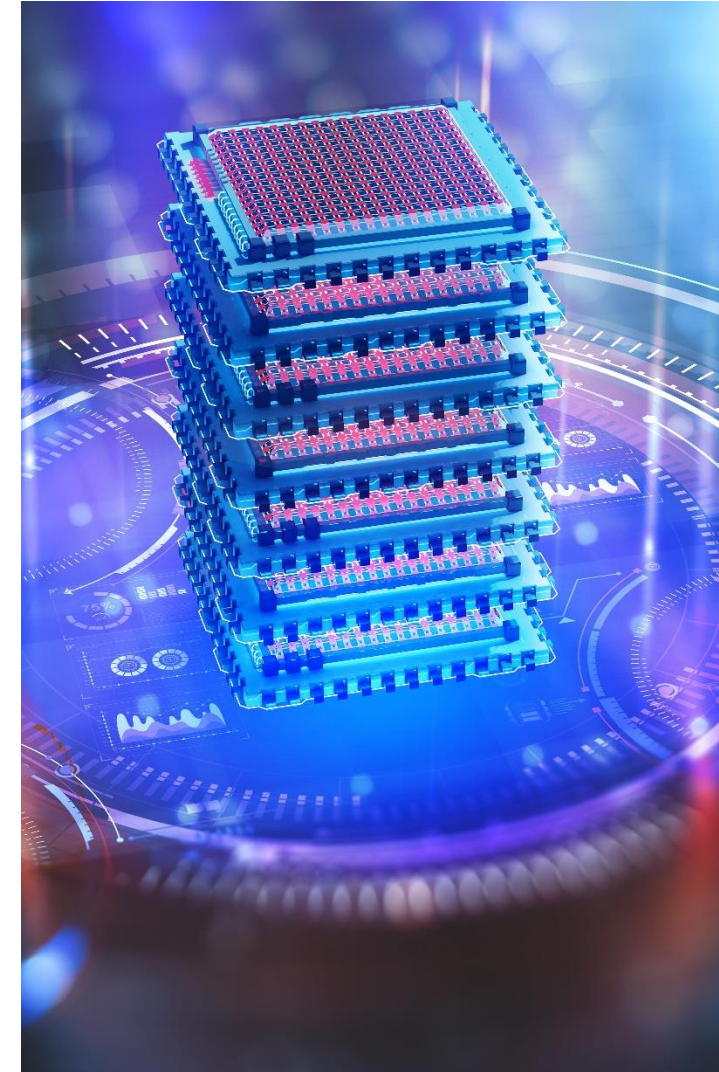
The post quantum reality is something that the world needs to brace for and there are different mechanisms using which organizations are securing their communication channels. This is particularly relevant to high risk organizations whose data is valid or relevant even after few years such as financial organizations, government agencies.

QKD is a possible solution in the long term for these organizations to implement, to secure them in the Post quantum era.

## Offsite data replication between main site and near site and near site and DR site

The recent pandemic has proved that the mechanism of shipping tapes offsite over courier channels can be abruptly brought to a stop. Cyber attacks however, specially ransomware has not stopped during this period.

Therefore, a mechanism of using quantum key distribution to encrypt data over regular channels for site to site encryption would make it far more difficult for attackers to override and provide a secure means of storing data at off-site locations without transmitting tapes physically.



Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements

# Where to from here? (2/3)



## Say goodbye to vulnerable version of TLS

A large part of server administration in today's time specially in industries with high user confidentiality such as Banking and Financial Services (BFS) are reliant on securing data-in-transit. Therefore, it requires in depth considerations from a security perspective for generating secure keys using hardware devices such as HSMs or internal root servers.

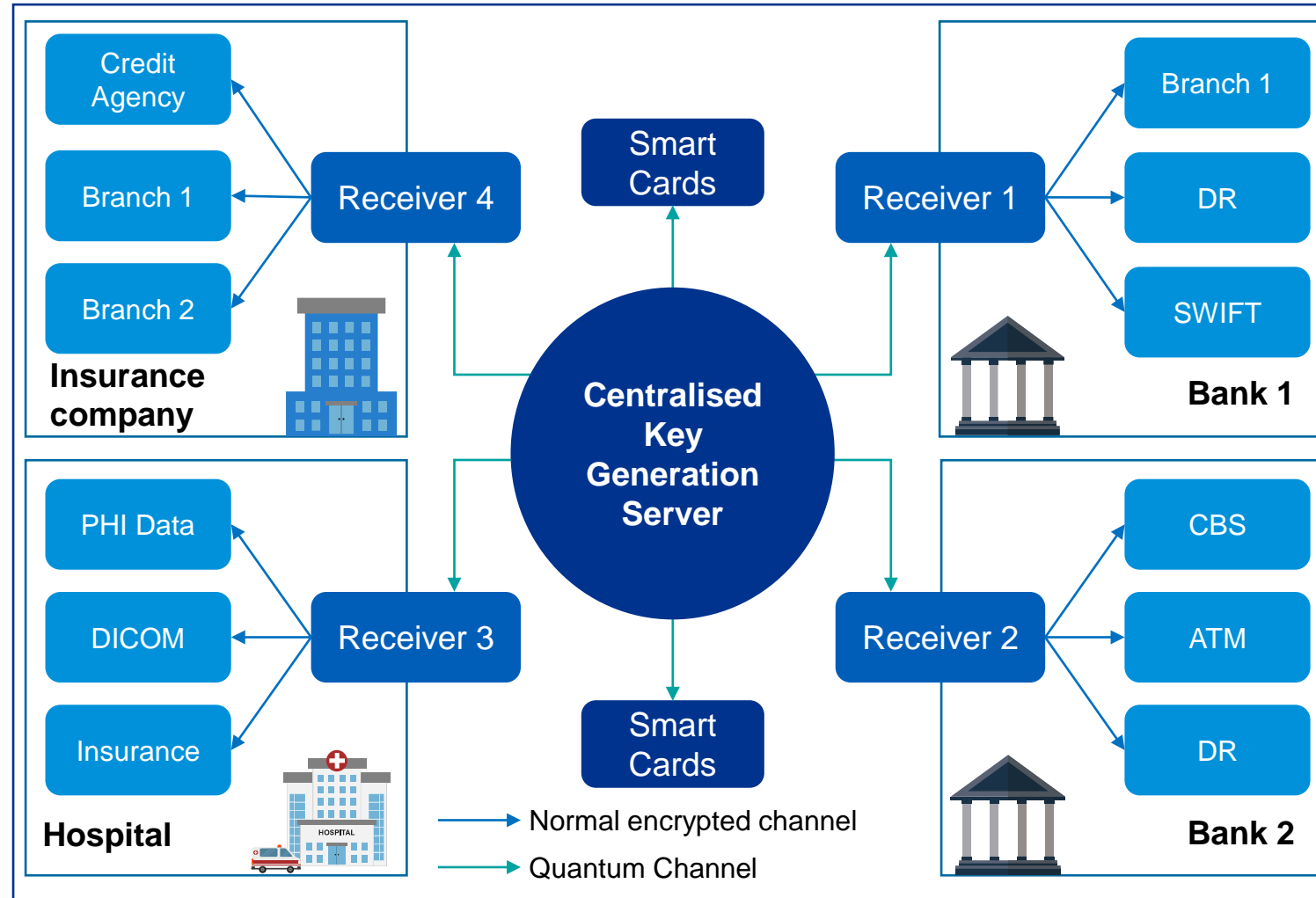
In addition, governments today, for e.g. the Indian government provides data reliance through digitally signed certificates using the Aadhaar project.

In both cases, compromise of the key in transit or use of a weak algorithm could lead to compromise of the overall data being transmitted.

In such cases, quantum key generators may prove to be a game-changer.

As shown in the illustration above, this can be used as below –

- Communications with internal business applications – the organization will leverage the keys generated by the centralized generator to encrypt communication over regular channels between external agencies such as SWIFT, limiting man in the middle attacks or internal communications to Core Banking Systems or even DR replication.



Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements



# Where to from here? (3/3)



- Smart card chips - As we move towards a new era in our digital revolution, the use of unique identification for citizens will become more and more important. These cards will contain irreplaceable identifiers for users such as biometric data which needs to be secured using the highest levels of encryption. Given a post quantum world being imminent, nation states can use quantum generated keys to encrypt the card data to ensure that they are secure.
- Hospitals – Medical institutions have a high need to transmit critical patient data across different systems, hospitals, insurance agencies and even in certain cases devices themselves. The use of quantum secured data over traditional channels would allow hospitals to transmit data without the fear of PHI data being intercepted or even worse, modified.

## Critical infrastructure and long-haul services

One of the key challenges in critical infrastructure today is the propensity of compromise of the confidentiality of critical data leading to catastrophic conditions. While security proofing of the environment is not completely possible due to legacy systems, organizations may look to move into a quantum secured network where they would

mitigate the challenges arising out of using legacy systems through highly secured traffic.

Long haul networks are another key area where quantum cryptography could help, specially due to the possibilities of physical manipulation of the fiber in transit.



Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements



# In conclusion (1/2)



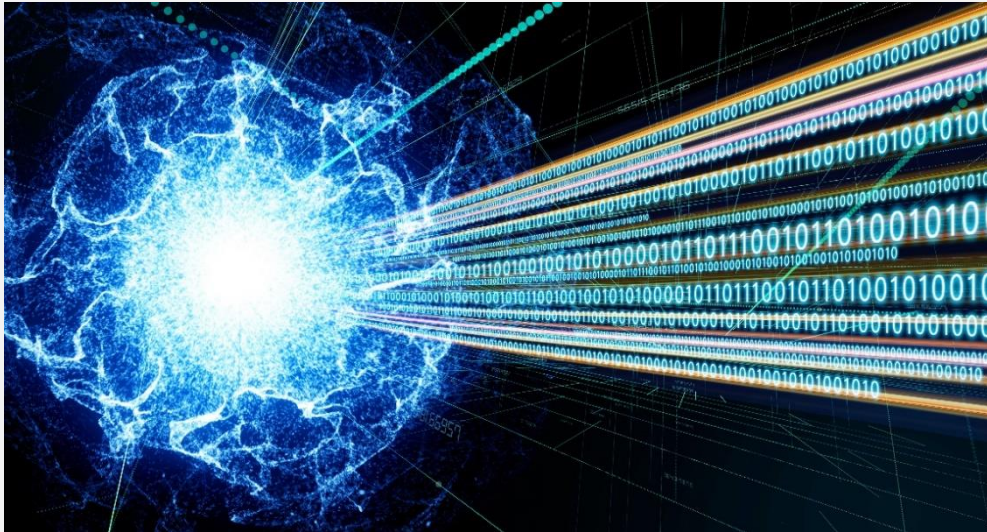
## Key challenges to quantum cryptography:

The key challenges to quantum cryptography are listed as below –

### I. Loss of qubits over long transmission

A significant challenge for quantum technology is that as the distance of the optical network increases, so does the increase in loss of photons or qubits.

This is overcome gradually with the use of new technology with organizations today showing that this is possible from the original 40 kms limitation to now up to 200 kms with negligible loss of data.<sup>8</sup>



### II. Timestamp for audit trails

The second challenge is the timing at which the photon arrived.

Photon arrival times are statistically unknown. For an organization to maintain audit logs it needs to understand the timestamp on the

photons. For organizations to do that with a certain amount of precision, there must be a quantifiable means of calculating time a photon is received accurately, which at present is not feasible.



8. <https://www.nature.com/articles/npjqi201625>

# In conclusion (2/2)



## Key challenges to quantum cryptography:

The key challenges to quantum computing are listed as below –

### III. Precision of environmental conditions

One more challenge in the path of quantum cryptography is to ensure that the environment (technology and otherwise) around which it is operating is free from disturbances generated due to vibrations, noise (white noise or channel noise) temperature and humidity variations. All these factors impact the movement of photons either due to

dispersion or due to other similar challenges impacting the photon patterns being received.

As mentioned earlier, with advances in technology, quantum cryptography has been able to work around these challenges and key distribution up to 200 Kms has been shown possible.



### IV. The usual suspect (Cybersecurity) – throwing caution to the wind

As we delve deeper into complex technologies such as QKD and others we should also keep in mind that the general concepts of application security, cryptography and other such security challenges would still need to be taken care of. Quantum cryptography is not a magic wand which promises to wish away all cyber security challenges. It is however a component of our overall

cyber security landscape and other components such as application security of the quantum key generator applications which would still need to be taken care of.

However, a large portion of data in transit challenges are expected to be reduced with the use of quantum cryptography.



Introduction

Relevance of quantum physics in business

Quantum computing and quantum cryptography

How do we secure today from the future?

Where to from here?

In conclusion

Acknowledgements

# Acknowledgements



We would like to acknowledge the active contribution of our Knowledge Partner: **QuNu Labs Pvt. Ltd.**

Special thanks to  
**Mr. Sunil Gupta,**  
Co-Founder and CEO,  
QuNu Labs Pvt. Ltd.

## Analysis and content:

Anish Mammachan  
Anish Mitra  
Apeksha Vyas  
Bhumika Verma  
Rakesh J  
Sony Anthony

## Brand and Design:

Nisha Fernandes  
Rasesh Gajjar



Introduction

Relevance of  
quantum physics  
in business

Quantum  
computing and  
quantum  
cryptography

How do we  
secure today  
from the future?

Where to from  
here?

In conclusion

Acknowledgements

# KPMG in India contacts:

**Akhilesh Tuteja****Partner and Head**

Digital Consulting in India

Co-Leader - Global Cyber security

E: [atuteja@kpmg.com](mailto:atuteja@kpmg.com)

**Atul Gupta****Partner and Head**

Digital Trust

India Cyber Security Lead

E: [atulgupta@kpmg.com](mailto:atulgupta@kpmg.com)

**Sony Anthony****Partner**

Digital Trust- Cyber Security

E: [santhony@kpmg.com](mailto:santhony@kpmg.com)

[home.kpmg/in](https://home.kpmg/in)



Follow us on:

[home.kpmg/in/socialmedia](https://home.kpmg/in/socialmedia)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG (Registered) (a partnership firm with Registration No. BA- 62445) converted into KPMG Assurance and Consulting Services LLP (a Limited Liability partnership firm) with LLP Registration No. AAT-0367 with effect from July 23, 2020.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only. (065\_THL0321\_RG)