Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment in Mission-Critical Environments

Farzam Toudeh-Fallah[1], Marco Pistoia[1], Yasushi Kawakura[2], Navid Moazzami[3], David H. Kramer[1], Robert I. Woodward[4], Greg Sysak[3], Benny John[1], Omar Amer[1], Antigoni O. Polychroniadou[1], Jeffrey Lyon[1], Suresh Shetty[1], Tulasi D. Movva[1], Sudhir Upadhyay[1], Monik R. Behera[1], Joseph A. Dolphin[4], Paul A. Haigh[4], James F. Dynes[4], Andrew J. Shields[4]

[1]JPMorgan Chase Bank, N.A. [2]Toshiba America, Inc [3]Ciena, Inc [4]Toshiba Europe Ltd

***Abstract*—This article describes experimental research studies conducted towards understanding the implementation aspects of high-capacity quantum-secured optical channels in mission-critical metro-scale operational environments based on Quantum Key Distribution (QKD) technology. The test bed for this research study was carefully designed to mimic such environments.**

To the best of our knowledge, this is the first time that an 800 Gbps quantum-secured optical channel—along with several other Dense Wavelength Division Multiplexed (DWDM) channels on the C-band and multiplexed with the QKD channel on the O-band—was established at distances up to 100 km, with secure-key rates relevant for practical industry use cases. In addition, during the course of these trials, transporting a blockchain application over this established channel was utilized as a demonstration of securing a financial transaction in transit over a quantum-secured optical channel.

In a real-world operational environment, deployment of such high-capacity quantum-secured optical channels multiplexed with the quantum channel will inevitably introduce challenges due to their strict requirements, such as high launch powers and polarization fluctuations. Therefore, in the course of this research, experimental studies were conducted on the impact on the system performance—and specifically on the quantum channel—of several degradation factors present in real-world operational environments, including inter-channel interference (due to Raman scattering and nonlinear effects), attenuation, polarization fluctuations and distance dependency. The findings of this research pave the way towards the deployment of QKD-secured optical channels in high-capacity, metro-scale, mission-critical operational environments, such as Inter-Data Center Interconnects.

I. Introduction

Quantum Key Distribution (QKD) is a well-known symmetric-key distribution method that does not rely on computational assumptions. Rather, it leverages principles of quantum mechanics to provide communication channels with unconditional security, mathematically proven by multiple studies [1]–[3]. This article mainly concerns itself with the implementation, deployment and integration of QKD technologies into real-world network infrastructures. For a detailed discussion of the theory behind QKD, as well as its security and challenges, and a survey of state-of-the-art real-world tests, see [4]–[6].

A. Novel Contributions of This Work

This paper describes in detail a joint experimental research study conducted by JPMorgan Chase, Toshiba and Ciena at JPMorgan Chase's Optical Transport Lab in Columbus, Ohio aimed at understanding the implementation and deployment aspects of an 800 Gbps QKD-secured optical channel in mission-critical metro-scale operational environments. The test bed for this research study was carefully designed to mimic such environments.

To the best of our knowledge, this research study is the first one to demonstrate an 800 Gbps QKD-secured optical channel along with several other Dense Wavelength Division Multiplexed (DWDM) channels on the C-band, multiplexed with the QKD quantum channel on the O-band, at distances up to 100 km. At a 70 km distance over a Corning SMF-28 optical fiber, this system achieved a secure-key rate (SKR) of 66.16 kbps, capable of supporting 258 QKD-secured DWDM data channels using Advanced Encryption Standard Galois/Counter Mode encryption with a key size of 256 bits (AES-256-GCM) and a key refresh rate of 1/sec. In addition, during the course of these trials, transporting a blockchain application over this established channel was utilized as a demonstration of securing a financial transaction in transit over a quantum-secured optical channel.

In real-world operational environments, requiring a third site just for the purpose of QKD to work is impractical, since the deployment of any new technology must be done within the facilities and sites already in place—for example between two metro-area data centers. The experimental research described in this article was conducted purely based on real-world operational equipment, with no employment of any kind of simulation or emulation, and without the need for the deployment of additional sites dedicated to QKD. Therefore, the solution presented here is directly applicable to metro-scale operational environments.

Fiber-optic links deployed in the field are very expensive commodities; dedicating a fiber just to the quantum channel would be considered unacceptable in a real-world operational environment. Consequently, when considering a QKD solution suitable for production, the optical and quantum channels must be multiplexed on the same fiber. Even though this requirement is of utmost importance, the deployment of high-capacity QKD-Secured optical channels multiplexed with the quantum channel introduces challenges—such as polarization fluctuations as well as nonlinear effects associated with high launch powers—which have been shown to have negative

impact on the performance of the quantum channel.

Thus, in the course of this experimental research project, studies were conducted towards understanding and quantifying the impact of several degradation factors present in real-world operational environments. Specifically, we investigated the degradation of the quantum channel associated with a high-capacity QKD-secured optical channel. Factors inducing this type of degradation include inter-channel interference (due, for example, to Raman scattering and nonlinear effects), attenuation, polarization fluctuations and distance dependency.

The findings of this research pave the way towards the deployment of future QKD-secured optical channels in high-capacity, metro-scale, mission-critical operational environments, such as Inter-Data Center Interconnects.

B. Paper Organization

This article is organized as follows: Section II describes the establishment of a QKD-secured 800 Gbps optical channel. Section III presents an inter-channel interference experimental study. Section IV focuses on the distance-dependency test results. Sections V and VI provide the results of experiments concerning two major degradation factors—attenuation and polarization fluctuations, respectively—on the performance of the quantum channel. Section VIII discusses prior art in the field of actual deployments of QKD-secured channels, making a comparison with the work described in this paper. Finally, Section IX concludes this article and illustrates opportunities for future research directions.

II. Establishing an 800 Gbps QKD-Secured Optical Channel

Figure 1 depicts the abstract test-bed configuration used in the trial. As seen from this figure, the optical data channel and the quantum channel are multiplexed on a Corning SMF-28 optical fiber, while the communications between the optical and QKD devices are established using Application Programming Interfaces (APIs) on both sides.

Figure 2 shows the actual test-bed configuration. Ciena Waveserver 5 systems (referred to as *the Waveserver systems* throughout this article) were utilized to establish an 800 Gbps optical wave on the C-band as the Channel Under Test (CUT), which carries pseudo-random traffic. The Waveserver systems are able to generate and receive two 800 Gbps waves per sled and up to 4 sleds per system. However, during the course of these experimental trials, only two ports (1/1 and 1/2) were used to generate the 800 Gpbs waves as needed. For establishing the quantum channel, the Toshiba Multiplexed QKD system (referred to as *the QKD system* throughout this article) were utilized. This system consists of two devices which contain transmitters, receivers and post-processing units on both sides (*Alice* and *Bob*), capable of establishing a quantum channel in order to generate keys based on the Decoy-State Phase-Encoded Bennett-Brassard 1984 (BB84) QKD protocol [7]–[9]. These devices can also multiplex incoming optical channels on the C-band with their quantum channel generated on the O-band, and launch both on the same optical fiber.

The 800 Gbps signal generated by the Waveserver system on the C-band on port 1/1 (the CUT) was inserted into the QKD system. The CUT was then multiplexed with the quantum channel on the O-band by the QKD system and both were transmitted over an optical fiber. On the receiver side, the reverse operation took place. Also, as shown in Figure 2, communications between the Waveserver systems and the QKD systems were conducted via an API link between the Waveserver and the QKD Control Server device. This communication was used by the Waveserver systems to retrieve the QKD-generated keys from a key management system on the QKD Control Server. The API link characteristics were based on the specifications of the European Telecommunications Standards Institute; ETSI GS QKD 014 [10]. The two endpoints of the QKD system were connected via a 70 km Corning SMF-28 optical-fiber spool (ITU-T Recommendation G.652.D compliant).

The following list details the relevant specifications for this configuration:

- P_{CUT} = 0 dBm
- λ_{CUT} = 1531.51 nm
- λ_{S1} = 1529.55 nm
- λ_{S2} = 1530.33 nm
- λ_{S3} = 1528.77 nm
- λ_{QC} = 1312.73 nm
- SMF-28: α_{1550} = 0.18 dB/km
- SMF-28: α_{1310} = 0.32 dB/km

Here, λ_{CUT} and P_{CUT} represent the CUT's wavelength and launch power respectively, λ_{QC} indicates the wavelength of the quantum channel, λ_{S1}, λ_{S2}, λ_{S3} represent the three QKD system service channels over the C-band and α is the attenuation coefficient.

It should be mentioned that λ_{CUT} was placed as close as possible to the lower edge of the C-band in order to take into account any potential interference from the QKD-secured optical channel on the quantum channel. Due to the presence of some of the required service channels on the C-band, 1531.51 nm was the closest channel we could select for this purpose.

Upon deploying this configuration, the quantum-secured optical channel at 800 Gbps was established, at which point the QKD systems, Alice and Bob, generated the keys. Those keys were then accessed by the Waveserver systems to secure the optical link (CUT) using AES-256-GCM encryption over the Optical Transport Network (OTN) standard protocol. Therefore, in this configuration, the keys were generated by the QKD systems, while the actual encryption of the 800-Gbps optical channel was performed by the Waveserver systems using the AES-256-GCM encryption method utilizing the QKD-generated keys.

III. Inter-Channel Interference

After successfully establishing an 800 Gbps quantum-secured optical channel at 70 km distance, in which the CUT and quantum channel were multiplexed on the same fiber, the

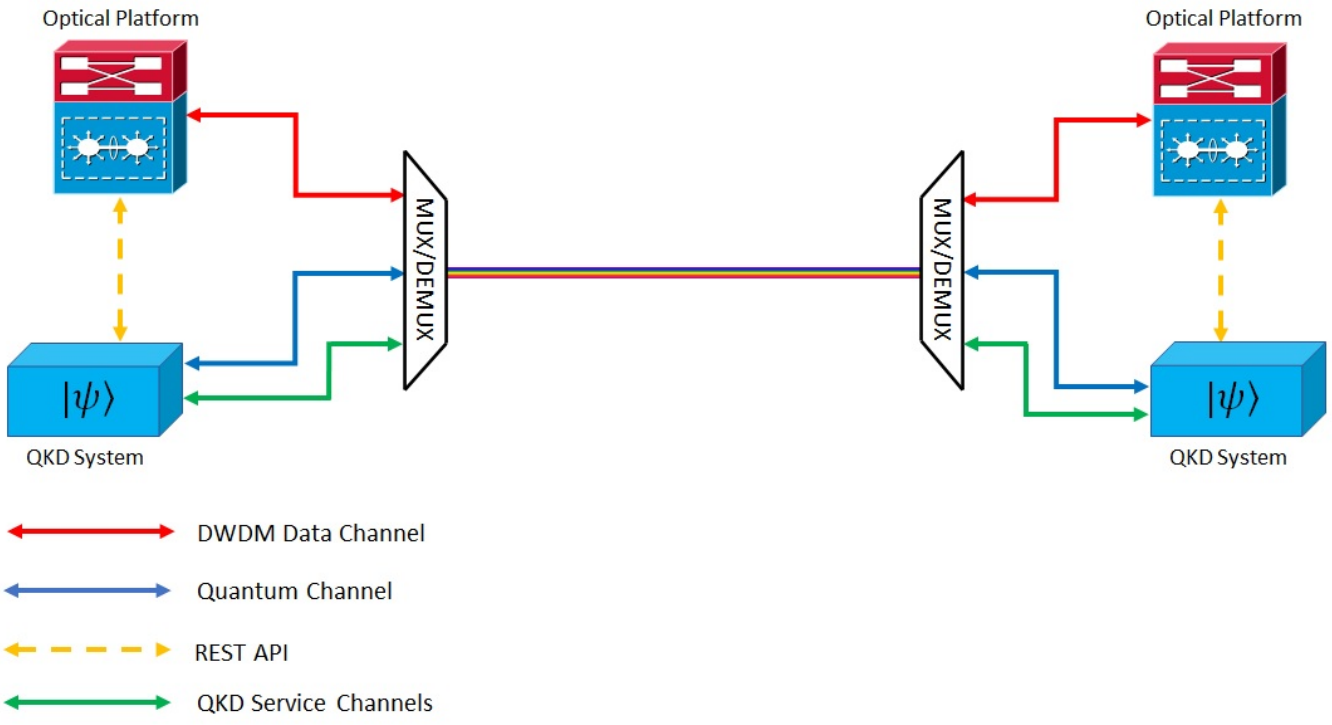

Fig. 1. Abstract Test-Bed Configuration

next step was to add additional optical channels. This served two purposes:

1) This configuration creates a more realistic and efficient operational environment in which several optical channels are multiplexed on the C-band via DWDM.
2) Multiplexing other optical channels results into launching higher powers into the fiber, which in turn induces degradation impacts—such as Raman scattering and nonlinear effects—on the quantum channel.

As pointed out before, the Waveserver systems were able to support generation of two 800 Gbps waves per sled. In order to multiplex additional optical channels, the Ciena 6500 Photonic Line System (referred to as *the photonic line system* throughout this article) and the Ciena 6500 Transponders (referred to as *the transponders* hereafter) were added to the test bed. The transponders that were available in the lab were able to establish 100 Gbps waves on the International Telecommunication Union - Telecommunication (ITU-T) C-band grid. By using the photonic line system, we were able to multiplex multiple optical channels using DWDM, providing required amplification and preparing the signals for launching into the fiber.

This configuration is depicted in Figure 3. Here, the Waveserver systems generated two 800 Gbps waves, the CUT on port 1/1 and the second one on port 1/2. These waves were then inserted into the photonic line system, which multiplexed them with eight 100 Gbps DWDM channels generated by the transponders on the C-band. After passing through an amplifier module on the photonic line system, these multiplexed DWDM channels (the two 800 Gbps and eight 100 Gbps channels) were inserted into the QKD system, which in turn multiplexed them with the quantum channel running on the O-band. As before, the two endpoints of the QKD system were connected via 70 km of Corning SMF-28 fiber. It should be noted that, in Figure 3, $N\lambda$ represents all other wavelengths that λ_{CUT} has been multiplexed with on the C-band.

As before, these optical channels were also carefully placed as close as possible to the lower edge of the C-band in order to maximize the potential of any inter-channel interference on the quantum channel. Table I provides the channel lineup for this configuration.

Channel	Wavelength (nm)
CUT	1531.51
Second 800G	1532.68
100G No. 1	1533.86
100G No. 2	1534.25
100G No. 3	1534.64
100G No. 4	1535.04
100G No. 5	1535.43
100G No. 6	1535.82
100G No. 7	1536.22
100G No. 8	1536.61

TABLE I
CHANNEL LINEUP

Figure 4 shows the Quantum Bit Error Rate (QBER) as a function of the number of optical channels as they were added one by one. This is useful to study the impact of the

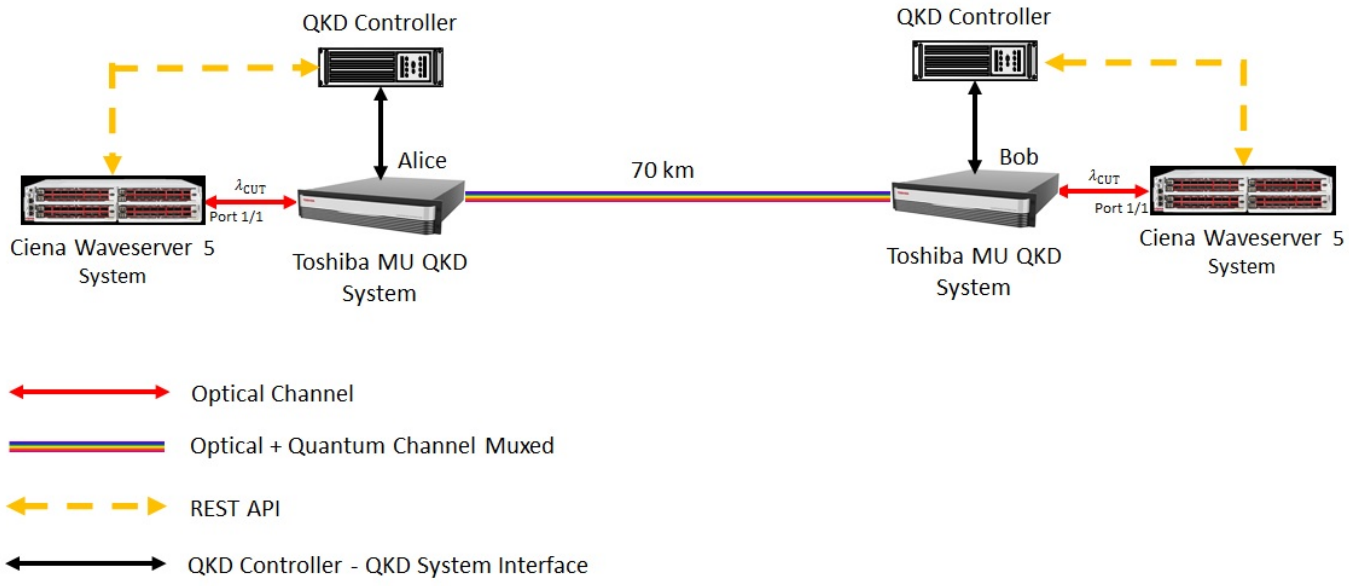

Fig. 2. Actual Test-Bed Configuration

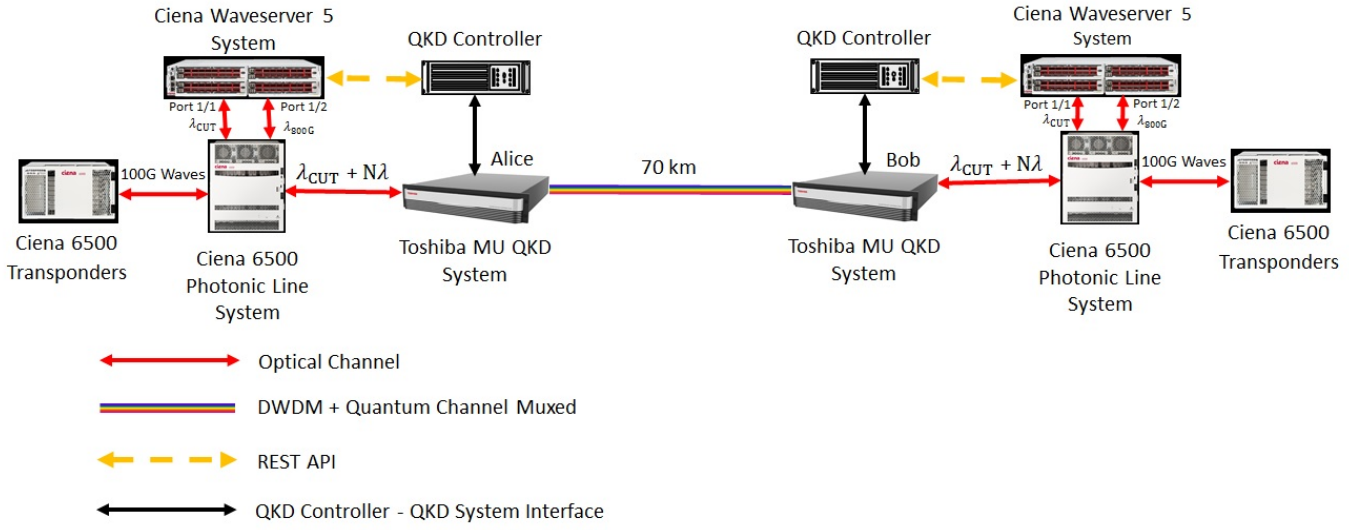

Fig. 3. Test-Bed Configuration with All the DWDM Channels Added

inter-channel interference imposed by the optical channels onto the quantum channel. As seen in the figure, QBER increased slightly as a function of the number of added optical channels (3.94% to 4.14%), due to the Raman scattering of the DWDM optical channels causing interference with the quantum channel. However, this increase was very well tolerated by the system and did not have any impact on the overall operational functionality.

Since this test-bed configuration is the closest to the actual operational environments in the field, the rest of the experiments were conducted over this configuration.

IV. Distance Study

The focus of this part of the research study was the performance of the system as a function of the distance. For this purpose, different fiber spools were used to analyze the impact of increasing the distance on the system performance. All fibers were of type Corning SMF-28 G.652.D. It should also be mentioned that for 80 km to 100 km distances, the launch power on the Waveserver systems were increased to 2 dBm in order to keep the 800 Gbps optical signals within the acceptable power levels at the receivers.

Figure 5 shows the results of this study. Here, an SKR of 66.16 kbps was achieved at a 70 km distance while securing an 800 Gbps optical channel multiplexed with another 800

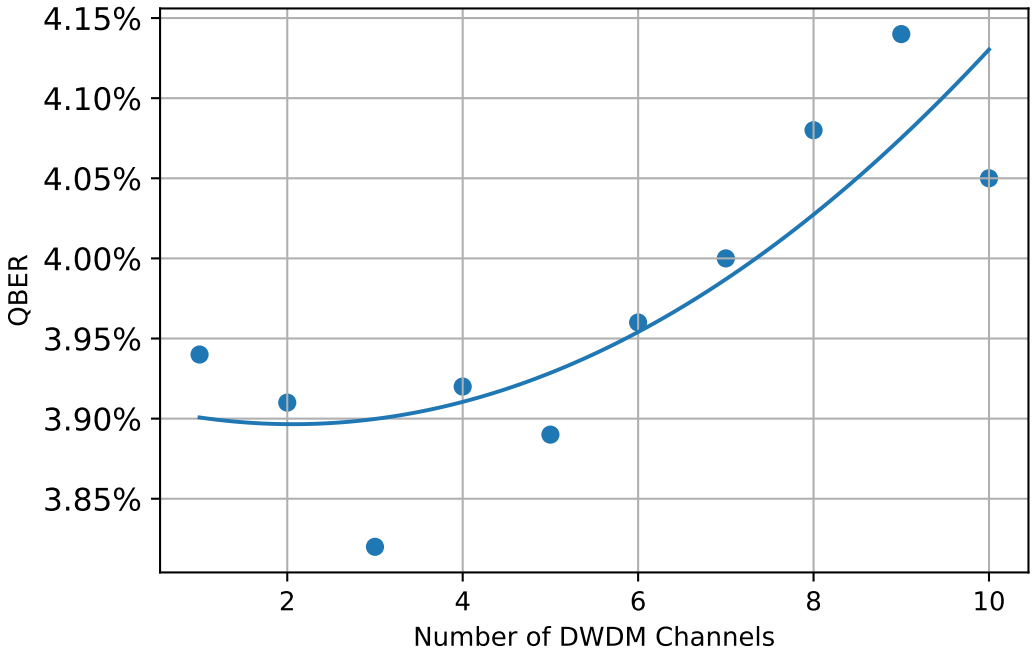

Fig. 4. QBER vs Added DWDM Channels

Gbps and eight 100 Gbps channels on the C-band. Although in this experiment there were ten optical channels present, at this rate the system has the potential to quantum-secure up to 258 optical channels using AES-256-GCM encryption while refreshing the key at a rate of 1/sec. Table II illustrates the achieved SKR as a function of the distance. Notably, an SKR of 2 kbps was achieved at a distance of 100 km.

Distance (km)	SKR (bps)
70	66163
80	30500
90	12000
100	2000

TABLE II
ACHIEVED SKR VS DISTANCE

V. Impact of Attenuation

Understanding the impact of increased attenuation on the QKD system in a fixed-length fiber scenario is important in order to understand the behavior of the system in a mission-critical environment. Whether the increased attenuation is as a result of a physical line issue or the presence of an eavesdropper, the network operator requires enough time to proactively investigate and avert an outage. In order to conduct this study, the fiber distance was set to the baseline value of 70 km and a Variable Optical Attenuator (VOA) was inserted into the quantum channel. As shown in Figure 6, the insertion point was right between the termination point of the 70 km fiber and the receiver port on Bob's QKD system. The VOA had an insertion loss of 0.737 dB and the target wavelength was set to 1310 nm in order to directly impact the quantum channel. The VOA attenuation value was increased at 1 dB increments on an hourly basis and measurements were taken.

Figure 7 provides the results of this study. The baseline with the VOA insertion shows a bit lower performance compared to the baseline without, i.e. a QBER of 3.61% vs 3.56% and an SKR of 50 kbps vs 66.16 kbps. This might be attributed to a combination of the VOA insertion loss and additional signal degradation at the interfaces introduced when connecting the signal in and out of the VOA itself.

Figure 7 also shows that the maximum attenuation tolerated on top of a 70 km fiber in this configuration was 9 db, after which the key generation process stopped.This is explained by the decreasing number of photons in the quantum channel arriving at the receiver due to increasing channel loss. Once the received quantum channel photons approach the noise level of the detectors, the signal-to-noise ratio becomes insufficient to distill QKD keys. This response to the induced attenuation in the form of gradual adjustment to the key generation rate—as opposed to an abrupt disruption in the process—is beneficial in mission-critical operational environment. The reason for this is that in those environments, it is vital to be aware of any degradation in the communication channel before the actual outage takes place. In that way, upon observing any degradation, the operator can proactively run a diagnosis on the system, identify the root cause (physical line issues or presence of an eavesdropper), and take necessary action before the system shuts down.

VI. Polarization Fluctuations

State of Polarization (SOP) fluctuation plays a major role as a degradation factor in fiber-optic networks. This effect, mostly

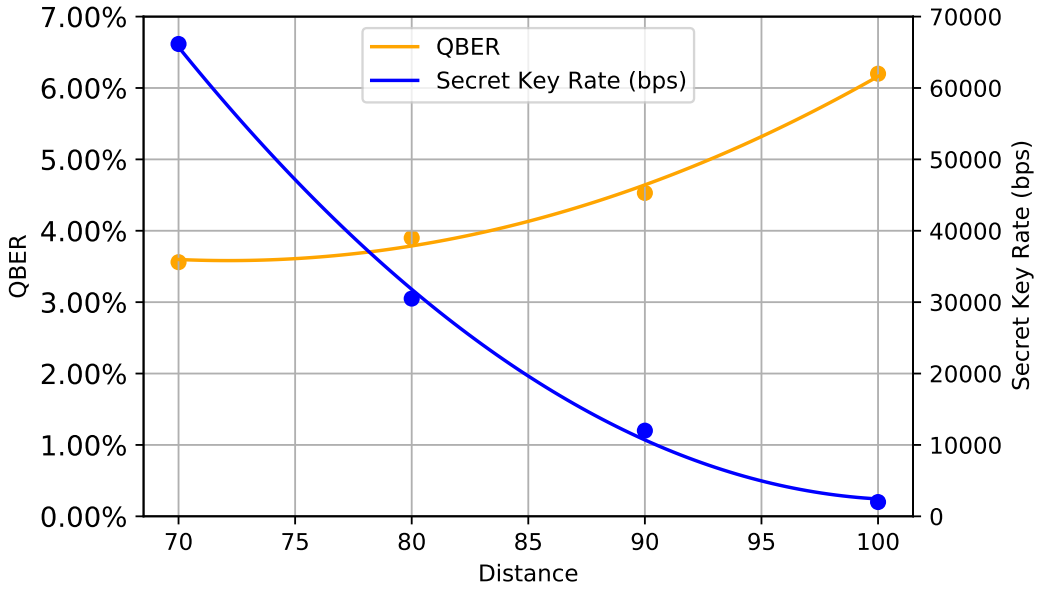

Fig. 5. Distance Study Results

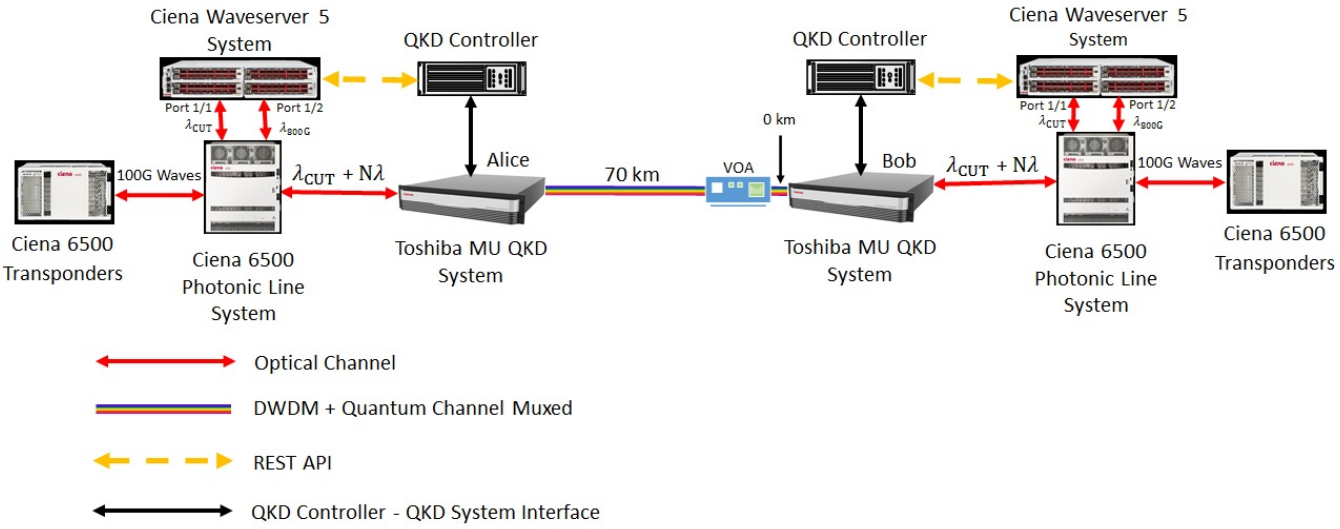

Fig. 6. Attenuation Testing Configuration

known as SOP Transients, is present in most operational networks as a result of vibrations in the environment such as underground fibers installed next to the railroad tracks, lightning strikes and other factors. As an example, research conducted on Optical Ground Wires (OPGW) has revealed SOP Transients on the order of 5.1 Mrad/sec as a result of lightning strikes [11]. OPGW is an aerial cable technology specifically designed for high voltage power line installations. These cables consist of a nucleus containing optical fibers and an armor, generally composed of one or more layers of aluminum wire, steel wire or aluminum-coated steel wire [12]. Therefore, any system to be deployed in operational fiber-optic networks should be able to tolerate such SOP fluctuations in order to prevent any service interruptions.

Figure 8 depicts the test-bed configuration for the SOP fluctuation study. Here, an SOP Controller was placed between the termination point of the 70 km fiber and the receiver port on Bob's QKD system.

During the course of this study, it was observed that setting the SOP Controller in scrambling mode at a Stokes angular velocity of 50 rad/sec in a sustained mode caused the key generation process to stop. Although lightning strikes are usually sub-millisecond events, their impact on the quantum channel established on aerial OPGW fibers should be studied. As such, based on the findings of this trial, future research into quantifying the exact impact of extreme SOP transients

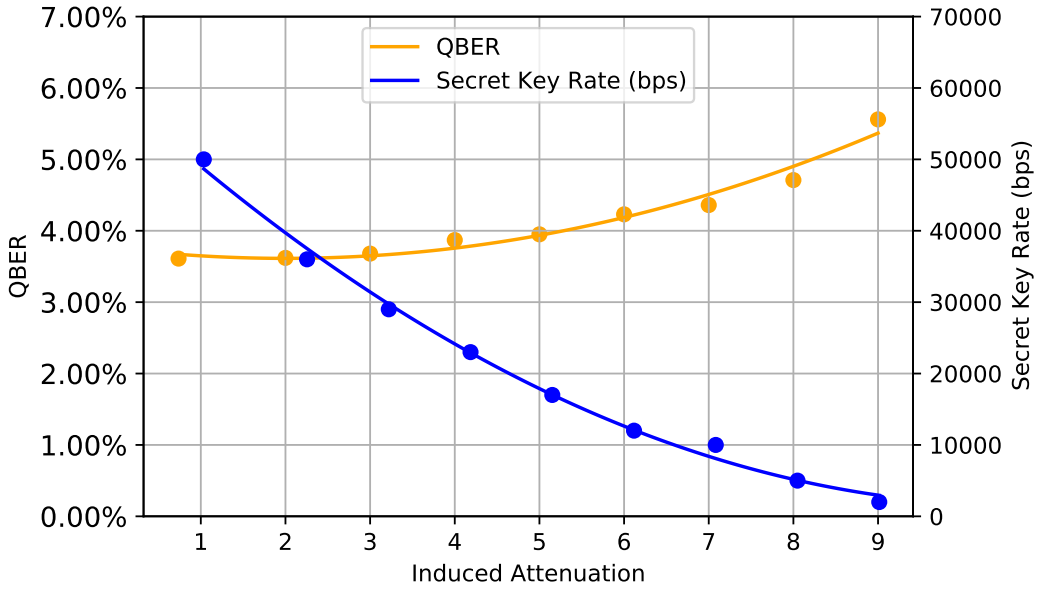

Fig. 7. Results of Study on Effect of Inducing Additional Attenuation on 70 km Fiber

on quantum channels and QKD systems are recommended.

VII. Routing a Blockchain Application over the Quantum-Secured Optical Channel

Blockchain constructions regularly make extensive use of public-key cryptography for enforcing both confidentiality and integrity through the use of encryption and digital-signature schemes, respectively. Most commonly, these cryptographic primitives are constructed based on postulates, such as the discrete-log assumption used by Diffie-Hellman and the elliptic curve cryptosystems, and the prime-factorization assumption used by RSA, both of which are now known to be false in the face of a Shor's Algorithm and a sufficiently powerful quantum computer [13]. The vulnerability of blockchain applications to the attacks conducted by quantum computers in these ways have been well studied [14]–[16].

In this section, we discuss the possibility of mitigating some of these weaknesses with the use of QKD-generated symmetric keys.

We discuss here, as an example of the confidentiality afforded to the data-in-transit of an application deployed over the quantum-secured channel, the security guarantees we achieved experimentally against a quantum-capable eavesdropper hoping to compromise the security of a blockchain application. Specifically, we installed and deployed the Liink blockchain network [17]—a permissioned blockchain based on the Quorum protocol [18] in use by JPMorgan Chase to process payments—and linked the nodes over quantum-secured channels. We start by describing briefly the Liink blockchain network to give motivation for why QKD may be applicable to it and other permissioned blockchain networks to protect their data in transit. Following that, we illustrate what additional tools may be deployed to enforce further security guarantees—this time against participants of the blockchain protocol rather than outside attackers. Specifically, we focus on possible methods that may be used to achieve blockchain consensus and enforce transaction integrity.

The Liink network, as a platform used by financial institutions, deals with large amounts of confidential information. While the information may be intended to be read by other parties in the network, confidentiality of the data while in transit must be retained against non-participants. Currently, the confidentiality of this data in transit is protected through the use of standard public-key cryptographic schemes, which will not be sufficient against a quantum-capable eavesdropper. The Liink network is an example of a permissioned blockchain network. Therefore, there is a meaningful distinction between parties that are and are not authorized participants of the network. As such, we can differentiate those two sets of actors and their distinct security profiles. Notably, we need not ensure that transaction data remains private from participants—only from non-participants. We note that here—and everywhere else we discuss confidentiality—we only refer to the confidentiality of the data-in-transit against a non-participant, not the data-at-rest.

The use of the quantum-secured channel allows us to achieve confidentiality against even quantum-equipped non-participants. In the experimental trial, as shown in the lab testbed depicted in Figure 9, the Liink application and transaction data were transmitted between two virtual machines (VMs) across the 800 Gbps quantum-secured optical channel (the CUT). The VMs were connected to switches that were in turn connected to the Waveserver systems via 100 Gbps Ethernet links, the output of which, carrying the traffic, was then sent over the CUT. A lightweight version of the Liink application was setup for this experiment. All communications

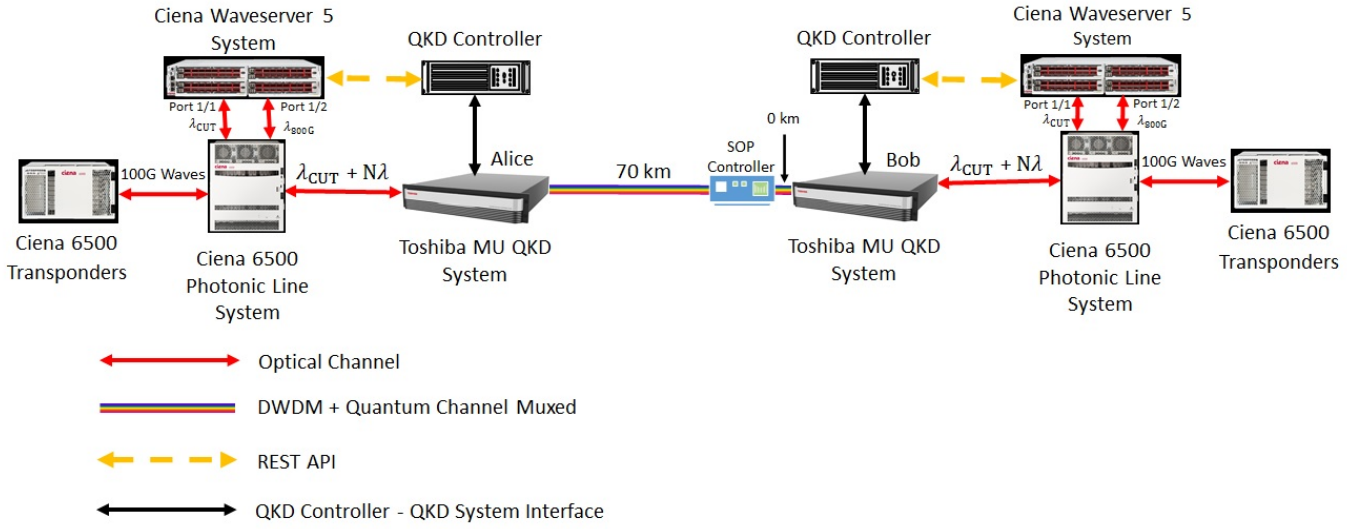

Fig. 8. SOP Fluctuation Study Test-Bed Configuration

between the two blockchain nodes Alice and Bob, including Peer Discovery, consensus and transaction propagation, were conducted over the quantum-secured optical channel. Upon initiating a transaction by node Alice, a listener process on node Bob confirmed the receipt of the transaction along with its addition into the block. Once included in the block, the transaction was considered confirmed via the consensus mechanism. During this experiment, the application did not encrypt the JSON payload in the transaction that it published on blockchain since protection was provided by the quantum-secured channel.

Without the quantum-secured channel, the Liink protocol must use standard public-key cryptographic schemes to secure the confidentiality of the information in transaction payloads against eavesdroppers. Such encryption schemes rely on the standard assumptions necessary for public key cryptography, which are known to be vulnerable to attacks realizable on powerful quantum computers expected to become available in the future. By routing the traffic over the quantum-secured channel, we replaced the public-key cryptographic schemes with QKD-enabled symmetric-key cryptography and ensured that a quantum-equipped eavesdropper cannot decrypt the traffic, including sensitive transaction data. As a result, we achieve the first of our discussed guarantees: confidentiality against a non-permissioned attacker. Ensuring that a non-permissioned party cannot introduce forged messages into the network can be done through the use of symmetric-key based information-theoretic message authentication codes [19] thereby achieving our second guarantee: message integrity. As a result, we achieve both of the previously discussed guarantees: confidentiality and integrity against a non-permissioned attacker.

Given the above changes to the Liink application, it is crucial that the participants of the blockchain network are still able to achieve consensus regarding the state of the ledger, even in the presence of some number of misbehaving participants with access to less than 51% of the total stake in the network. As a necessary step of the Liink protocol, some subset of the participants, referred to as *validators*, all receive, separately, a given transaction. For them to validate the transaction and update the ledger, they must first ensure that they all received the same transaction, reaching consensus on it. This is achieved through byzantine agreement schemes [20], which commonly make use of broadcast protocols, which enable all of the participants to verify that they have received the same message. A natural extension of our proof of concept to more nodes encrypts the payloads via QKD-generated keys, making the construction and use of a broadcast channel costly due to the necessary cross-comparisons of a byzantine agreement protocol, but the use of optimally resilient verifiable secret-sharing schemes [21], [22] can increase the efficiency, in a fully connected graph, and still allow the participants to reach consensus. In this approach, a transaction is split into n shares according to a k-out-of-n (optionally verifiable) secret-sharing scheme, with these n shares being distributed over the QKD-secured links to the n participants in the network, under the assumption that the network is fully connected. When it is their turn to validate a transaction, some k participants can then form a quorum and recover the transaction from the shares. In doing so, they all necessarily agree on the same transaction, ensuring consensus [23].

Finally, we note that it is necessary that participants of the network are confident that a transaction originates from the participant it purports to originate from. In our case, where the underlying QKD network is complete, and all parties therefore share pairwise secret keys, the participants may make use of group message-authentication codes that are information-theoretic secure to ensure integrity [24]. With a complete network we are then able to achieve consensus as well as efficiently achieve transaction integrity without the

use of some underlying computational assumptions. In the case of incomplete networks, the design of methods that allow validators to verify the origin of the transactions they reach consensus on without the use of such additional assumptions will be part of future work.

VIII. Related Work

Although experimental trials have been previously conducted to investigate QKD technology, they have been done on a limited scale or under conditions that do not represent real-world, high-capacity operational environments. In this section, some of these efforts are discussed. For a more extensive survey of previous experimental results regrading real world QKD networks, see [6], [25].

In 2005 researchers at DARPA deployed the first real world QKD network in which they achieved 1 kbps SKR at 10 km distance over a non-muxed dedicated quantum channel [26]. In [27], a SKR of 3.1 kbps with QBER of 2.6% over 33 km of non-muxed dedicated quantum channel was achieved as part of the SECOQC project which realized a multi-platform QKD network operating in Vienna. Further, researchers in [28] achieved 18 kbps at 90 km on a non-muxed dedicated quantum channel on a link in the Tokyo QKD network in 2011. As pointed out before, the ability to multiplex both DWDM optical channels and quantum channel are of utmost importance in the real-world operational environments. Therefore, these works cannot be considered for such deployments.

Indeed there have also been previous efforts to multiplex the optical channels with the quantum channel. It was first shown that it was possible to do so in [29], where a quantum channel was multiplexed with a 1.2 Gbps classical channel over 28 km. In [30] researchers followed up on this work by multiplexing 4 DWDM channels with a quantum channel, in which those 4 channels were used for key distillation and 1 Gbps encrypted communication. This work resulted into a SKR of 11 bps at a maximum distance of 50 km. In [31] a CV-QKD channel multiplexed with one DWDM channel was demonstrated. In this demonstration the single DWDM channel was run at -3 dBm and at 75 km a key rate of 0.49 kbps was achieved. In [32] two 100 Gbps DWDM channels (at 1529.55 and 1529.94 nm) were multiplexed with the QKD quantum channel on 1547.72 nm. In [33] multiple 200 Gbps and 100 Gbps channels were multiplexed with quantum channel running at 1310 nm. For this experiment, the polarization encoding decoy-state BB84 protocol QKD was utilized. During this trial, a 3 kbps SKR at 66 km of G652 fiber was achieved.

IX. Conclusion

To the best of our knowledge, in this research study, for the first time an 800-Gbps quantum-secured optical channel along with several other DWDM channels on the C-band and multiplexed with the QKD quantum channel on the O-band at distances up to 100 km with secure key rates relevant for use in real-world mission-critical applications has been established. At 70 km distance over Corning SMF-28 fiber, this system was able to provide a secure key rate of 66.16 Kpbs, which would be able to support 258 quantum-secured DWDM data channels using AES-256-GCM encryption with the key refresh rate of 1/sec. In addition, during the course of these trials, transporting a blockchain application over this established channel was utilized as a demonstration of securing a financial transaction in transit over a quantum-secured optical channel. This experimental research was conducted purely based on real-world operational equipment and no simulation or emulation was used to replace them.

Deployment of such high-capacity quantum-secured optical channels while multiplexed with the quantum channel in the real-world mission-critical operational environments would introduce challenges due to some strict requirements such as high launch powers and polarization fluctuations that would have negative impact on the performance of the quantum channel. Therefore, in the course of this research, experimental studies were conducted on the impact of several degradation factors present in the real-world operational environment on the quantum channel, including inter-channel interference (due to effects such as Raman scattering and nonlinear effects), attenuation, polarization fluctuations and distance dependency. During the course of this investigation, the entire system under test exhibited resiliency against most degradation factors. However, based on our findings, some recommendations are made towards meeting the strict requirements for deployment in a mission-critical operational environments. These include future research into quantifying the exact impact of extreme SOP transients on quantum channels and QKD systems and introducing quantum channel performance degradation alarms for proactive diagnosis by the network operators to prevent outages.

The findings of this research pave the way towards the deployment of quantum-secured optical channels based on QKD technology in high-capacity metro-scale mission-critical operational environments, such as Inter-Data Center Interconnects.

Disclaimer

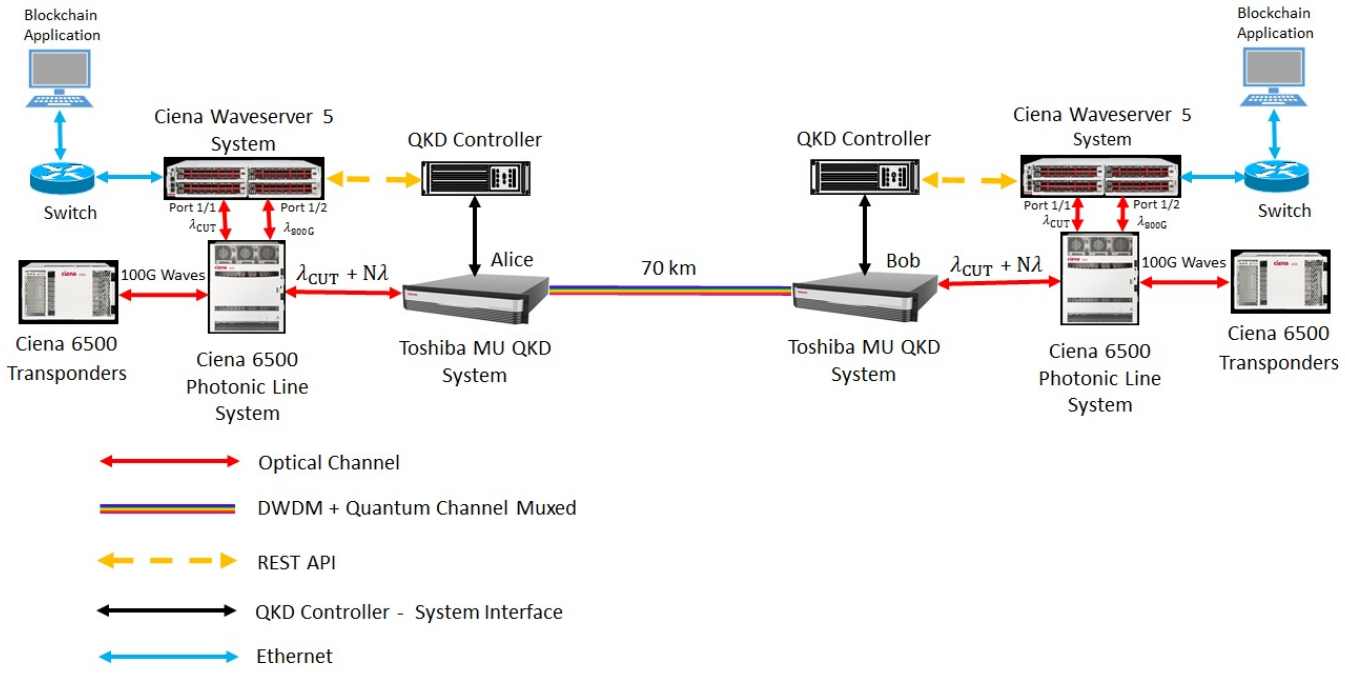

Fig. 9. Blockchain Application Transport Test-Bed Configuration

ACKNOWLEDGEMENTS

The authors would like to thank the following people for their invaluable contributions and support to this project: Lori Beer, George A. Sherman, Andrew J. Lang, Patrick P. Opet, Umar Farooq, Christine Moy, Matthew Tice, Beata Shahriari, Myron Wieneke, Stephen Gannon, Charles Carley, Douglas B. David, Michael P. Lombardi, Mike Rutigliano, Paula Varas, Stephen I. Winer, Jennifer H. Lavoie, Daniel Cantor, Hargun Kalsi, Michael Hattery, Alejandro Poggi, Chaddy Huussin and Emily Mullins from JPMorgan Chase; Terry Cronin from Toshiba; and Patrick Skully, Daniel McCarthy, Chris Howard, John P. Ferrel, Sebastien Gareau and Yves Cayer from Ciena.

REFERENCES

[1] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[2] H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[3] M. Koashi, "Unconditional Security of Quantum Key Distribution and the Uncertainty Principle," in *Journal of Physics: Conference Series*, IOP Publishing, vol. 36, 2006, p. 016.

[4] R. Alléaume, C. Branciard, J. Bouda, *et al.*, "Using Quantum Key Distribution for Cryptographic Purposes: A Survey," *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.

[5] L. Gyöngyösi, L. Bacsardi, and S. Imre, "A Survey on Quantum Key Distribution," *Infocommunications Journal*, vol. 11, no. 2, pp. 14–21, 2019.

[6] O. Amer, V. Garg, and W. O. Krawec, "An Introduction to Practical Quantum Key Distribution," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 30–55, 2021. DOI: 10.1109/MAES.2020.3015571.

[7] M. Lucamarini, K. Patel, J. Dynes, *et al.*, "Efficient decoy-state quantum key distribution with quantified security," *Optics express*, vol. 21, no. 21, pp. 24 550–24 565, 2013.

[8] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *International Conference on Computers, Systems & Signal Processing, Bangalore, India*, 1984.

[9] Z. Yuan, A. Plews, R. Takahashi, *et al.*, "10-Mb/s Quantum Key Distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[10] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf.

[11] D. Charlton, S. Clarke, D. Doucet, *et al.*, "Field Measurements of SOP Transients in OPGW, with Time and Location Correlation to Lightning Strikes," *Optics Express*, vol. 25, no. 9, pp. 9689–9696, 2017.

[12] *International Telecommunications Union, Optical fibres, cables and systems*, 2009.

[13] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[14] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, *Quantum Computers Put Blockchain Security at Risk*, 2018.

[15] B. Rodenburg and S. P. Pappas, "Blockchain and Quantum Computing," The Mitre Corporation, Tech. Rep., 2017.

[16] N. Kappert, E. Karger, and M. Kureljusic, "Quantum Computing—The Impending End for the Blockchain?" *Quantum*, vol. 7, pp. 12–2021, 2021.

[17] *Liink*, Accessed on Jan 31, 2022. [Online]. Available: https://www.jpmorgan.com/onyx/liink.

[18] ConsenSys, *Consensys/Quorum: A Permissioned Implementation of Ethereum Supporting Data Privacy*, Accessed on Jan 31, 2022. [Online]. Available: https://github.com/ConsenSys/quorum.

[19] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of computer and system sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[20] J. Katz and C.-Y. Koo, "On Expected Constant-Round Protocols for Byzantine Agreement," in *Annual International Cryptology Conference*, Springer, 2006, pp. 445–462.

[21] A. Choudhury, A. Patra, *et al.*, "A Survey on Perfectly-Secure Verifiable Secret-Sharing," *arXiv preprint arXiv:2112.11393*, 2021.

[22] A. Beimel, "Secret-Sharing Schemes: Survey," in *International conference on coding and cryptology*, Springer, 2011, pp. 11–46.

[23] R. Canetti and T. Rabin, "Fast asynchronous byzantine agreement with optimal resilience," in *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*, ser. STOC '93, San Diego, California, USA: Association for Computing Machinery, 1993, pp. 42–51, ISBN: 0897915917. DOI: 10.1145/167088.167105. [Online]. Available: https://doi.org/10.1145/167088.167105.

[24] R. Amiri, A. Abidin, P. Wallden, *et al.*, "Efficient Unconditionally Secure Signatures Using Universal Hashing," in *Applied Cryptography and Network Security*, B. Preneel and F. Vercauteren, Eds., Cham: Springer International Publishing, 2018, pp. 143–162, ISBN: 978-3-319-93387-0.

[25] P. Sharma, A. Agrawal, V. Bhatia, *et al.*, "Quantum Key Distribution Secured Optical Networks: A Survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2049–2083, 2021. DOI: 10.1109/OJCOMS.2021.3106659.

[26] C. Elliott, A. Colvin, D. Pearson, *et al.*, *Current Status of the DARPA Quantum Network*, 2005. arXiv: quant-ph/0503058.

[27] M. Peev, C. Pacher, R. Alleaume, *et al.*, "The SECOQC Quantum Key Distribution Network in Vienna," eng, *NEW JOURNAL OF PHYSICS*, vol. 11, ?–? 2009, ISSN: 1367-2630.

[28] M. Sasaki, M. Fujiwara, H. Ishizuka, *et al.*, "Field Test of Quantum Key Distribution in the Tokyo QKD Network," *Optics express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[29] P. D. Townsend, "Simultaneous Quantum Cryptographic Key Distribution and Conventional Data Transmission over Installed Fibre Using Wavelength-Division Multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, 1997.

[30] P. Eraerds, N. Walenta, M. Legre, *et al.*, "Quantum Key Distribution and 1 Gbps Data Encryption over a Single Fibre," *New Journal of Physics*, vol. 12, p. 063 027, 2010.

[31] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of Continuous Variable QKD with Intense DWDM Classical Channels," *New Journal of Physics*, vol. 17, no. 4, p. 043 027, 2015.

[32] J. F. Dynes, W. W. Tam, A. Plews, *et al.*, "Ultra-high bandwidth quantum secured data transmission," *Scientific reports*, vol. 6, no. 1, pp. 1–6, 2016.

[33] Y. Mao, B.-X. Wang, C. Zhao, *et al.*, "Integrating Quantum Key Distribution with Classical Communications in Backbone Fiber Network," *Optics express*, vol. 26, no. 5, pp. 6010–6020, 2018.