QUANTUM INTERNET ALLIANCE

D4.1 Quantum Applications and Use Case Report

Document History

Revision Nr	Description	Author	Review	Date
1.0	Final Version	Mina Doosti, Marc Kaplan		22/12/2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 820445.

Index

1. Abstract

This document presents applications for future quantum networks. These applications were obtained by interviewing potential end-users in various fields: security, banking, payment, blockchain, distributed computing, quantum machine learning and telecommunications. Our goal was to investigate potential uses of some selected quantum communication tasks. After selecting a few tasks that we believe can have an impact on end-users applications, the interview process aimed to identify the problems for which these tasks could offer a solution. This document does not solve the identified problems, but rather matches current problems with potential solutions. The design of precise solutions to these problems would be the topic of subsequent research.

We have classified the areas of applications in five categories: new threats on authentication, secure data aggregation, cross-platform finance, regulations of security and privance, and quantum machine learning. In each category, we present some problems that stakeholders have identified, and match them with quantum tasks. In particular, we selected a number of problems as challenges.

We expect these interviews to pave the way to future relations between research and industries within the Quantum Internet Alliance. By identifying future end-users, we expect to stimulate more involvement from potential stakeholders. Ultimately, this could be a crucial step toward a large adoption of the technologies related to the quantum internet.

2. Introduction

Quantum technologies bear the promise of a revolution in information processing. Many areas will be impacted, from sensing with high-sensitivity gravimeters and high-precision atomic clocks, to quantum computation who will solve problems that are out of reach of current computing technology. In this report, we focus specifically on quantum communication, which is based on the ability to prepare and send quantum states of light from one point to another where it is detected.

Quantum communication networks already exist. The best example is in China, who has built a fully-operational quantum network connecting more than 30 nodes over more than 2000km between Beijing and Shanghai. Currently, such networks have very limited capabilities but can nevertheless execute a well-defined task: quantum key distribution. This task allows two connected parties to share a secret key which can then be used to establish secure communication channels.

The theory of quantum key distribution was established in the early 80's by Charles Bennet and Gilles Brassard (Bennett & Brassard, 1984). Originally, their work showed that it is possible, using quantum states of light, to realize a task that cannot be achieved using only classical information. A commercial activity spun out of academia in the early 2000's, with several companies over the world proposing operational QKD systems.

Since then, it has been shown that as quantum networks will gain new abilities, using more elaborate hardware to process quantum information, new quantum communication tasks, beyond quantum key distribution, will be enabled (Wehner, Elkouss, & Hanson, 2018). Far from limited to key establishment, future quantum networks will have many applications in areas ranging from cybersecurity to distributed computing or metrology.

The early developments of quantum network developments have showed that a well-defined application with a provable advantage over existing technologies does not suffice to address the market. Criticism over QKD remains vivid today, even from national security agencies. The American National Security Agency, for example, made the following public statement in October 2020: "*NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems*" (National Security Agency Central Security Service, 2020).

We interpret this as a discrepancy between what the technology offers and the user needs. Our goal, in this report, is to bridge this gap, not for quantum key distribution, but for the future tasks that quantum networks will be able to run. For this purpose, we have worked with potential stakeholders to sketch future evolutions and how they will be used in practical problems that end-users are facing with today's technology. Based on a few selected tasks, we identified the stakeholders that could be involved and discussed the applications they would run.

The ambition of this report is to demonstrate how, in the field of quantum communication, new hardware leads to executing new protocols, which in turn increases the number of potential end-users interested in new applications. The link between hardware and protocols is investigated in the academic world. In parallel, industrial actors are identifying end-users and the applications they need. We draw a line between these two approaches to sketch the practical use of future of quantum communication networks.

2.1. Stages of quantum networks

Quantum key distribution networks are using a very limited set of abilities. One party prepares and sends single qubit systems encoded into single photons or coherent states of light; the other party receives and measures the quantum state of the qubits. These operations require several pieces of hardware, which are already developed by various industries in the world: lasers, light modulators, single photon detectors, etc…

This state of technology forms the first stage of quantum networks. A classification of quantum networks depending on the hardware that they use was developed by the Technical University of Delft (Wehner, Elkouss, & Hanson, 2018). Each stage extends the previous one by integrating new hardware. As mentioned, this new integration allows the network to execute more tasks. A classification of the tasks available at each stage can be found in the Quantum Protocol Zoo (VeriQloud, n.d.). In this section, we briefly describe each stage to sketch the foreseen technological evolution of quantum networks.

In current quantum communication networks, nodes can generate and measure single qubit quantum states. This is sufficient for quantum key distribution. The communication distance, however, remains strongly limited by fiber losses. The usual solution to extend the distance is to add trusted nodes whose role is to route keys between distant parties. Quantum key distribution is thus available without end-to-end security.

The second stage of the hierarchy is reached when it becomes possible to send single-qubit states between arbitrary nodes of the network. This can be achieved, for example, using quantum repeaters which distill entangled states used for quantum teleportation. At this stage, quantum key distribution becomes possible with end-to-end security, and quantum protocols for secure identification can be executed.

At the third stage, entangled states can be distributed between arbitrary sets of points of the network. This allows a new form of cryptography called *device independent* in which security can be achieved even using untrusted devices.

When reaching the fourth stage, the nodes receiving quantum states can store them in their internal memory and process them later. This can be used to distribute unforgeable tokens that can be used, for example, as electronic cash.

The fifth stage allows nodes to execute limited computation by operating on the quantum states stored in the quantum memories. The number of qubits is limited but the computation is fault-tolerant. At this stage, quantum networks can perform distributed computation with higher efficiency than their classical counterparts. They can also be used for very accurate clock synchronization.

Finally, at the sixth stage, full-scale quantum computers are connected to quantum networks, and can exchange arbitrary quantum states. It becomes possible to securely delegate quantum computation to distance servers, without the server learning the computation it is performing.

Stage	Applications
VI.Quantum Internet	Distributed machine learning, leader election, byzantine agreement
V. Few qubits fault-tolerant computing networks	Clock synchronization, distributed computing
IV. Memory networks	Quantum coins, quantum tokens
III. Entanglement distribution networks	Anonymous transmission, certified randomness expansion, randomness amplification, device-independent quantum key distribution
II. Prepare and measure networks	Secure communication with point-to-point security, Digital signature
I. QKD networks	Secure communications

Table 1: Stages of quantum networks

2.2. Interviews of potential end-users

Our work focuses on a small number of identified tasks that we believe could have a high impact on the applications developed by end-users. A task describes a functionality that the parties involved are trying to achieve. A protocol is a sequence of operations that the parties apply in order to realize a task. Some tasks can be realized by multiple protocols with different resources or different levels of security.

Our goal is to exhibit matchings between the tasks we have selected and the applications that end-users might need. With this respect, the selected tasks can be considered as primitives that are used to build more elaborate processes integrated into the application developed and used by end-users.

After reviewing the literature and selecting promising quantum communication tasks, we have interviewed potential end-users to discuss, within the applications they use, the problems that they have identified regarding the security, performance or robustness, and how these could be addressed using the tasks we have selected. These potential end-users have expertise in various areas of network software engineering such as cybersecurity, banking, blockchain or IoT.

Designing solutions to their problem is a difficult research and development or engineering problem. At this stage, we only focus on exhibiting matchings between the properties of quantum communication tasks and the properties desired by end-users for their applications. To summarize, the contributions of this report are:

1. To identify new stakeholders who could be involved in the future developments of quantum communication networks at later stages than QKD networks;
2. To match end-user's problems and quantum information processing tasks developed in the academic world for quantum communication networks;
3. To characterize the new types of services available at each stage of the development of the quantum communication networks.

Altogether, this contributes to sketching the future evolution of quantum communication networks from the point of view of end-users.

3. Quantum communication tasks

In this section, we describe the tasks that we believe will have a significant importance for quantum network users. While we keep the descriptions brief, interested readers can refer to the Quantum Protocol Zoo to learn more about the quantum protocols that realize these tasks.

3.1. Quantum key distribution

Quantum key distribution is a task that enables two parties to establish a classical secret key using quantum communication. A classical secret key is a random string of bits known to only the legitimate parties, and completely unknown to any third party. Such a secret key can be used with a classical encryption algorithm to encrypt a classical message sent over a public and classical communication channel. Quantum key distribution addresses encryption, the first pillar of network security.

Classical key exchange protocols are usually based on asymmetric cryptography. The most commonly used classical encryption system is RSA, whose security is based on the hardness of factoring. This makes RSA vulnerable to quantum computers which, when available, will be able to factor large numbers efficiently. Other popular asymmetric cryptosystems suffer similar weaknesses.

In recent years, the area of post-quantum cryptography has substantially grown. In this area, the hardness of breaking an encryption algorithm relies on a mathematical problem that is assumed to be hard for quantum computers.

While our present work aims to go beyond quantum key distribution, it is interesting to recall that it leads to a security model that differs radically from classical systems. Quantum key distribution is *unconditionally secure*, which means that it does not rely on some hardness assumption. Moreover, it can be shown that an attack on quantum key distribution can only be successful if it happens at the moment of its execution. Unlike classical cryptosystems, it is not possible to record execution of quantum key distribution protocols to decrypt secret data later in time, when more computational power becomes available. In other words, *quantum cryptography can make data as secure in the future as they are today*. This notion is usually referred to as *everlasting security* and cannot be achieved with classical cryptosystems.

In addition, quantum cryptography offers two strong security properties. Firstly, QKD has forward-secrecy, which means that the leakage of a recent secret does not lead to compromising previously completed sessions. Secondly, QKD sessions have post-compromise security, which means that the leakage of a past secret does not lead to compromise secrets of future sessions.

Quantum key distribution can also be combined with classical cryptography to ensure the security of stored data. The idea is to use classical cryptography algorithms to split the data into a number of shares and distribute those over different servers using quantum key distribution. This can be pushed further by constantly re-encrypting the shares, which ensures that an eavesdropper that wants to learn the secret has to attack several servers at the same time.

There exist various protocols for quantum key distribution. The simplest, based on preparing single qubits systems and measuring their states, can be implemented using commercially available systems.

3.2. Quantum Digital signatures

Digital Signatures allow the exchange of messages from sender to multiple recipients, with a guarantee that the signature has come from a genuine sender. This can be used to authenticate the sender of a message. Authentication, after encryption, is the second pillar of network security.

The security of classical digital signatures relies on *authentication* (the message comes from the claimed party), *integrity* (the message has not been altered) and *non-repudiation* (the sender cannot deny having sent a signed message).

Quantum digital signatures slightly differ from their classical counterparts. In the quantum case, we usually consider the properties of *transferability* (a signature can be transferred to a third party), *non-repudiation* (same as classical) and *unforgeability* (a signature cannot be forged by a third party). These schemes are used to sign classical messages but not quantum messages.

Classical digital signature protocols are well understood and commonly used. The encryption algorithm RSA can be turned into a signing algorithm. XMSS is a quantum-resistant analogue. As it was mentioned in the description of the protocol, the natures of classical and quantum digital signatures differ slightly. However, the two protocol families can be compared for tasks such as preserving data integrity, or to authenticating the sender of a message.

Quantum digital signatures are unconditionally secure, which ensures long-term security and quantum resistance. Moreover, Quantum Digital Signatures scenario usually involves three parties. In a typical scenario, Bob proves to Charlie that some data were signed by Alice.

Most protocols for quantum digital signatures require quantum memories, although less efficient protocols exist for the prepare-and-measure network stage. These can be implemented with current technology at a small scale.

3.3. Quantum anonymous transmission

Anonymous transmission is a task that enables two nodes to communicate in a network anonymously. More specifically, one of the nodes of the network, the sender, communicates a quantum state to the receiver in a way that their identities remain completely hidden throughout the protocol. In particular, it implies that the sender's identity remains unknown to all the other nodes, whereas for the receiver it implies that no one except the sender knows her identity. The main goal of anonymous transmission is to fully hide the identities of the sender and the receiver; it does not aim at guaranteeing the reliability of the transmitted message.

Several classical protocols for anonymous transmission were proposed since the late 1980's. The most widely-spread practical solutions are proxy anonymizers, which are trusted third parties, and networks based on computationally-secure problems and a chain of forwarding. Famous examples of the latter include MixMaster, PipeNet, OnionRouting and its best-known implementation, Tor.

Quantum protocols are traceless: the sender cannot be reconstructed afterwards. They do not rely on a trusted third party, nor use computational assumptions. Moreover, they seem well-suited for small scale infrastructures since they do not require a chain of servers.

Various protocols for quantum anonymous transmission were introduced, which differ in the hardware they require. State-of-the-art protocol simplified the problem and can be implemented with current technologies and distributed entangled states. This means that, considering the existing hardware, they currently cannot scale to a large number of parties. Progresses on the generation and distribution of entangled states are expected to occur in the next ten years. This would allow scaling quantum anonymous transmission to a larger number of parties.

3.4. Quantum money

The concept of quantum Money was first introduced by Wiesner in 1983. Informally, the quantum money object is a unique (i.e. based on a public classical serial number) and unforgeable physical object that is created by a third party called *Mint*. Then, it is circulated among potentially untrusted parties called *Holders* who might attempt to forge it for double spending. A Merchant, however, upon receiving it, should be able to verify that the money has not been forged and originated from Mint. There exist many verification schemes based on different types of communication and types of encryption used by Mint.

Classical digital currencies are usually based on the use of a ledger called a blockchain. Operations such as token emission and spending are reported to the public ledger. The ledger is publicly verifiable and copied on several nodes of the network, which ensures that no minority of agents can alter the history of operations.

Quantum money realizes a different task to classical digital currencies. Quantum resources lead to tokens whose integrity can be easily verified by anyone, but that can only be spent once. The security of these tokens is unconditional. Moreover, since there is no need for a ledger, the quantum solution has a better scaling. While classical digital currencies are decentralized, Quantum money is emitted by a Mint which is a central authority.

In most applications, quantum tokens need to be stored. This implies the use of quantum memories, a device that can store a quantum system and release it on demand. These devices do not exist yet, but they are an intense research topic in the field of quantum information processing. There are multiple proposals to implement them, and they could be available in five to ten years from now.

3.5. Secure Client-server delegated quantum computing

Delegated Computation is the task of assigning computation on hidden data to a powerful untrusted party - the *Server* - by a party with weak computational power – the *Client* - while maintaining privacy of data from the server.

Secure Delegated Computation was an open problem in classical computation until Gentry's work in 2009 on Homomorphic Encryption using Lattice-Based Cryptography. This solution offers a high security and in particular, it is resistant to attacks by quantum computers. The consortium HomomorphicEncryption.org issues standard for homomorphic encryption libraries. Currently, there exists a dozen of publicly-available implementations.

The main problem of homomorphic encryption is that it is currently inefficient. They typically have very high overheads limiting their practical use.

In the quantum setting, a quantum computation is delegated to a quantum computer. This implies a larger computational power and the possibility to address a larger set of problems. Moreover, protocols for delegated quantum computing usually have very little overheads. The amount of data that needs to be communicated to the server is of a comparable size with the program that is delegated. Finally, their security is unconditional.

Delegated quantum computing requires a quantum computer. These devices are not supposed to be available in near future. Experts predict that they will be available in twenty to forty years.

In most protocols for delegated quantum computing, the client used for the protocol is very simple. Although it performs quantum operations, these operations are similar to the ones performed in quantum key distribution. Such a client can thus be built with current technologies.

Another constraint is that the client and the server need to be able to exchange quantum states. This requires a quantum communication channel. In general, clients are simple enough to directly operate optical quantum states, which are convenient for the transport of qubits. They are thus well suited to be connected to quantum communication networks. On the other hand, connecting quantum computers might require converting optical qubits to the qubit used for computing. The complexity of this operation highly depends on the underlying technology, ranging from straightforward for optical quantum computing to extremely challenging for superconducting or silicon-based quantum computing.

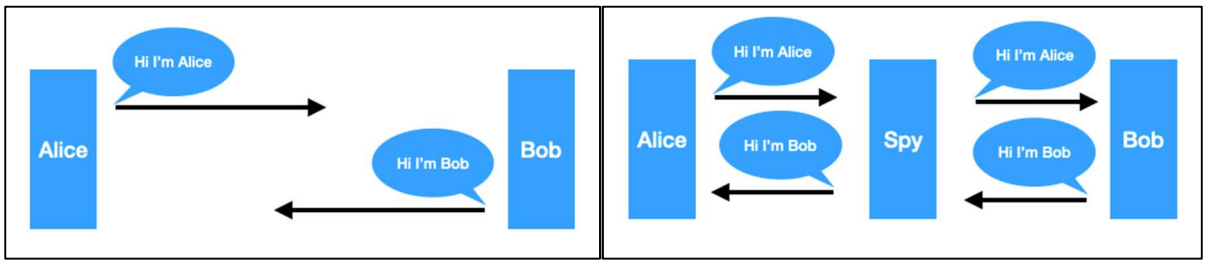
There exist alternative solutions to implement delegated quantum computation using only classical communication. These typically use classical cryptography techniques that induce large overheads, which in turn require larger quantum computers to be executed.

4. Security and privacy challenges

In this section, we introduce the problems that are either mentioned in the literature or that were raised by the potential end-users we have interviewed. We have grouped these problems in general categories. We also mention explicit challenges that require further research and development, or engineering. These challenges aim at developing applications that would match the needs expressed by end-users.

4.1. New threat models on authentication

Authentication is, with encryption, one of the most important tasks to secure network. Without authentication, any participant in a network could impersonate any other. No security could ever be possible in such a context. The impersonation attack, called *man-in-the-middle,* is very general, and can even be used to break quantum key distribution protocols.



Legitimate protocol execution

Man-in-the-middle attack

Authenticating network nodes and their communication is crucial for many network applications: online banking, software updating or e-commerce are common operations that use authentication to establish trustful communication channels. Due to this importance, there exist various mature solutions for authentication. The most common ones use Public Key Infrastructures (PKI), and use trusted authorities to emit certificates that can be used by users to prove their identity.

This solution is based on centralized certificates and lead to heavy processes to emit, update or revoke identity credentials. It can be scaled with intermediate authorities, but this inherent centralization limits its range of application.

Recent evolutions in network topologies are pushing to reconsider the authentication problem. With the increase of *Internet of things* (IoT), more and more devices are being connected to networks. Beside the visible development of consumer's devices, IoT is spreading in many industries such as transport, maritime, oil and gas, mining or agriculture. These devices may contain critical information, and their security needs to be carefully assessed.

One solution to manage the identity of such devices is to hardcode a master key in them. This key can be used directly, or to derive session keys, but in any case, the security of the device reduces to securing the key stored in the device. While this may be considered a good solution due to the limited computational power of such devices, it does not face well the new threats arising in the world of IoT. Such devices are assumed to be light, and their security should consider situations where their identity credentials

get stolen or copied. Handling security in a manner that takes into account this threat model and in such networks is considered a challenge by security experts.

This situation could benefit from the power of quantum networks. The challenge is to create a system to manage identity credentials that cannot be cloned, forged and can be revoked instantaneously by a central authority. *Quantum money* protocols seem to offer the desired properties. The various proposals for quantum money protocols are all based on the idea of producing unforgeable tokens. The security of these construction is derived from the unclonability of quantum states, a physical property that ensures the security of many quantum tasks. Moreover, quantum tokens are, like standard money, issued by a central authority which can revoke them easily. One difference, however, is that when quantum tokens are consumed, they are not available anymore while authentication may be performed several times.

Challenge nº1: Design an authentication system using unclonable quantum tokens.

Mobile devices are also used for a lot of transactions that require authentication, such as payment. The main issue here is that the devices are not trusted and the mobile manufacturer may not be willing to collaborate with security companies.

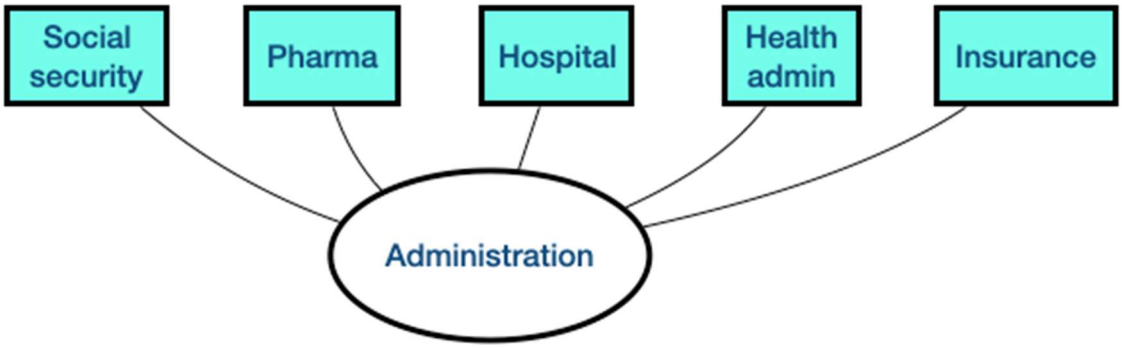
Quantum protocols may also offer solutions to these problems. In particular, Quantum Digital Signatures could be helpful to get long-term security. More advanced concepts, such as Quantum Physically Unclonable Functions (Doosti, Kumar, Delavar, & Kashefi, 2020) are also investigated as potential solutions to identification problems.

Quantum networks will offer new solutions to various challenges related to authentication. Known protocols can be used to develop more secure solutions thanks to the unclonability and unforgeability of quantum tokens, as well as the long-term security that naturally follows from the use of quantum resources.

4.1. Aggregation of sensitive data from mistrustful parties

When Diffie and Hellman introduced public-key cryptography in the mid-nineteen seventies, it was clear that beyond its mathematical interest, it would have a huge effect on real-world data processing (Diffie & Hellman, 1976). This intuition was largely proven to be true. As information flows in networks, the security of the data deeply affects the trust relationship between the communicating participants. For example, online payment would not exist if the buyer did not trust that its data are correctly secured. It is not exaggerating to state that cryptography is a key ingredient of the modern information society.

These issues became more and more important since we have realized the value of data. Collecting data securely requires careful application of cryptographic techniques. But data owners also want to be able to capitalize on them, and computing over data while maintaining privacy requires techniques that are at the forefront of modern cryptographic research.



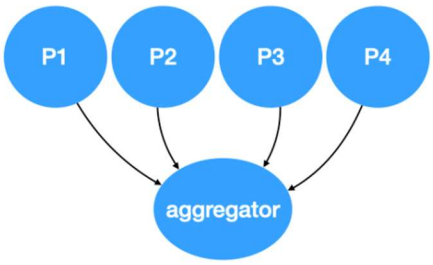
An administration wants to extract statistics from distributed data

Issues arise even from simple problems such as extracting statistics from distributed data. The data might be too valuable or regulated in a way that prevents sending them directly to a third party.

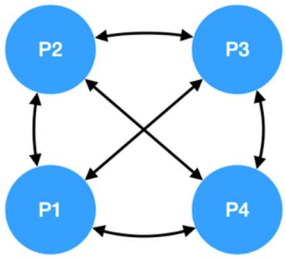
Classical cryptography offers solutions to perform these operations. In particular, secure multiparty computing allows mistrustful parties to compute over their inputs while maintaining privacy. Some secure computing solutions also involve third parties but the theory ensures that they will not get any information during the process.

The two main security models considered for secure computing are participatory trust and delegated trust. In the participatory trust model, data owners perform a collective computation which is private by-design. The participants thus bear the responsibility for the privacy. In the delegated trust model, a third party aggregates the data from various participants and runs the computation. He is responsible for the privacy of the process.

Various security issues arise from these situations. In the delegated trust model, the first step is to centralize the data. This requires to secure data in-transit as well as stored data. The second step is to compute over the securely stored data. In the participatory trust model, the protocol executed by the participants should be private by-design.



Delegated trust



Participatory trust

In both cases, quantum networks can increase security. In the example developed above, the aggregation is performed on healthcare data. These are very sensitive data that require carefully designed security. In particular, the long-term security that is inherent to quantum cryptography could strengthen the security of communication and storage in the case of delegated trust, and privacy by-design in the case of participatory trust.

Challenge nº2: Make privacy by-design long-term secure with the help of quantum resources.

In some cases, the only information that needs to remain private is the sender's identity. For example, monitoring car traffic can lead to a better management. Drivers, however, might not be willing to share their speed to avoid being caught over the speed limit for example. *Quantum anonymous transmission* could be used to hide the drivers' identities while collecting valuable data.

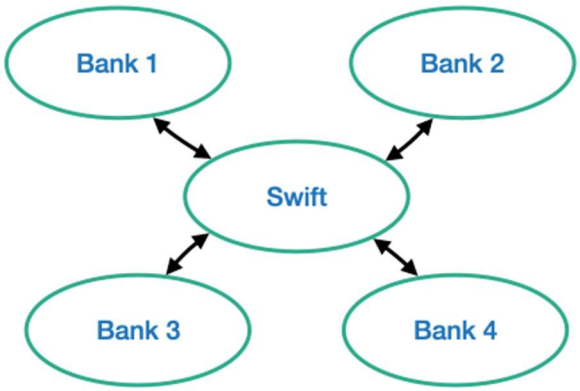
Cryptography can be used to make mistrustful parties collaborate to reach a common goal. While the amount of data is increasing, the responsibility of data's owners is increasing as well. Quantum networks could help making better use of data, without sacrificing privacy and security.

4.2. Cross-platform finance

The banking industry always needs more security. Breaches in bank's security make them lose money either because of theft or because they get find by regulators. The care on data security in banking stems from the fact that, to some extent, the world's economy relies on the bank's security.

A specific set of tasks that requires high levels of security is the operations between banks. The SWIFT system, designed for this purpose, is presented as "The global provider of secure financial messaging services". In practice, SWIFT is used to emit messages for international financial operations.

In 2015, a spectacular attack on SWIFT led to a $101 million theft from the central bank of Bangladesh. This attack was based on the emission of unauthorized money transfer orders. These orders were then erased from transaction databases to erase any trace of illegal money movement.



Messaging service between banks

Quantum cryptography could be useful to strengthen the security around the breaches that were exploited for these attacks. Properties such as non-repudiation, i.e. the impossibility for a bank to deny having sent a message received by another bank, can be found in quantum digital signatures, and quantum tokens could be used for a better tracing of messages.

In this case, the assets that are moving between banks represent money. For this reason, a quantum SWIFT system based on quantum money and quantum digital signatures could offer very high security guarantees.

Challenge nº3: Design a Quantum SWIFT system.

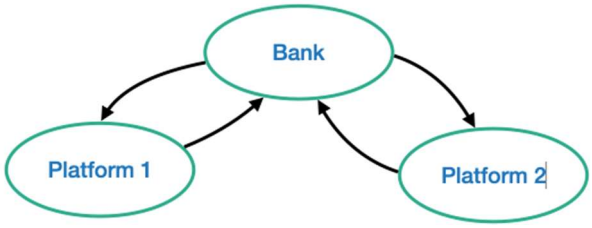
Quantum networks is one of the many transformations that the banking industry is experiencing. Another important transformation is that money is turning more and more into a purely digital asset. Beyond the mathematical challenges regarding the security of those digital assets, there is a deeper question on how to maintain trust in this new situation. Once again, cryptography can help to bring trustfulness to end-users. Two paradigms epitomize the digital transform of financial assets: platform money and blockchain.

In the digital world, supply and demand are handled by *digital platforms*. While their original role was to manage *the multitude* of users and data, the services they offer have widely diversified over the last twenty years. Platforms like Amazon, Microsoft, PayPal or Facebook are building ecosystems rather than just servicing customers.

With this respect, it is not surprising that Facebook announced in June 2019 that it was working on its own money, Libra. Although this project has not been deployed yet, this is a trend that banks are looking at seriously, trying to anticipate what their role will be in such an economic environment. It is clear that a systemic bank is also building an ecosystem rather than servicing customers. Anticipating changes for such institutions means they should understand not only their business, but also what their main values are. *What is the value of a systemic bank in a quantum world?*

Quantum technologies are an opportunity for banks to push further the trust relationship with their customers. As we mentioned, cryptography can be used to build trust between users of digital systems, which explains its wide adoption by the financial sector. In fact, systemic banks are more than financial operators. They also establish a deep trustful relationship with their customers. We trust banks to keep our money stored in their vaults, and to ensure the stability of the world's economy.

In a world of platform money, banks would have to maintain and expand this trust relationship to platforms. The strong security guarantees of quantum money and quantum digital signatures could be an asset to establish trustful relationship between platforms.

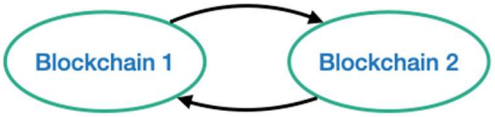


Banks as an intermediate between platform

Decentralized finance is an extreme case in which all the trust is put into cryptography while fully removing third parties such as banks. This area is growing based on the progress of the blockchain technology, the key technical element behind bitcoin and other cryptocurrencies.

The main reason for this development is clear. On the one hand, third parties are weak links in the security chain. Most of the security measures should be concentrated there, which may be difficult to achieve when addressing, for example, emerging financial markets. Decentralization is a way to mitigate the risks while developing new financial tools. On the other hand, increasing the liquidity of digital assets implies having various blockchain technologies that are compatible one with another. This allows to have tools to connect markets one to the other and avoid isolation.

In the case of cryptocurrencies, the most important role of the blockchain is to avoid double spending. How can this security goal be achieved in a world with multiple blockchains? This question is can be phrased in general terms as designing *secure cross-chain operations*.



Operations across blockchains

The potential consequences of quantum communications on blockchain have been widely studied (Aggarwal, Brennen, Lee, Santha, & Tomamichel; Kiktenko, et al., 2018; Ikeda, 2018). One obvious reason is that most implemented blockchains are not secure against attacks by quantum computers. It is possible to design quantum-secure cryptocurrencies using quantum key distribution and quantum digital signatures. More interestingly, quantum money can be used to get better scaling for blockchain, a crucial problem for the sustainability of this technology (Coladangelo & Sattath, 2020).

The unforgeability and unclonability of quantum money could be helpful to design secure cross-chain operations. Quantum coins can only be spent once, which seems to offer a solution to the double-spending problem. That would require sending those quantum tokens on quantum networks.

Challenge nº4: Design secure cross-chain operations using unforgeable quantum tokens.

4.3. Toward regulation for security and privacy

A massive amount of data is being collected every day. The exploitation of these data is a central question of the digital strategy in any major company. The effects of these strategies can already be seen: big data is one of the key factors that enabled the rise of machine learning over the last fifteen years. This is one of the reasons why, over the same period, the value of data has been soaring.

Collecting data also implies responsibilities. Companies in areas such as banking or payments are collecting and storing a lot of *personal data*. They are thus responsible for putting sufficient security measures to ensure their security. To some extent, the trust relationship established between these industries and their clients also stands on their responsibility on the data they collect.

Banking and payment are heavily regulated industries. One aspect of this regulation is the duration of data's security. The value of data obviously evolves over time. The images of a football game have a very high value for a short time, whereas the value of personal, healthcare or classified data remains high for at least thirty years. For banking data, ten or twenty years of security is standard, and in some cases, it tends to evolve toward thirty years.

Considering the value of data over time has very different consequences in the classical and quantum case. In classical cryptography, the mathematical security follows from the conjectured hardness of some computational problem. For example, the security of RSA encryption follows from the hardness of factoring large numbers. Therefore, in order to set the size of encryption keys (a large number in the case of RSA), it is necessary not only to consider current computational power, but also anticipate its increase during all the lifetime of the data. These previsions are usually done by governments through either IT security Agencies (BSI in Germany, ANSSI in France) or standardization institutions (NIST in the US). These previsions are obviously more relevant for the short term than the long term, which makes the question of long-term security very complex in the case of classical cryptography.

As we mentioned already, quantum cryptography can make data as secure in the future as they are at the moment they are encrypted. This could completely change the way we approach security over time. In particular, the question of the long-term security of data should be reconsidered in this setting. Quantum key distribution and its applications to secure storage is opening new doors for the regulation of the security of the most sensitive data.

The general framework for data privacy in Europe is GDPR. This regulation lays down the people's right regarding the processing and movement of their personal data. This puts stringent limitations on how collected data can be used. Data aggregation, introduced earlier, is a case in which cryptography can be used to enforce trust between mistrustful parties. Similar approaches can be developed for regulated data.

Using cryptography to design *GDPR-compliant applications* is already being considered in the classical case. Quantum cryptography can offer more tools for such designs. Anonymous transmission and secure delegated quantum computation can be used to hide some selected information to the recipients of quantum communication. These tools seem relevant in even more complex contexts such as the protection of free speech or whistleblowers.

Beyond the economic consequences that we have already reviewed, cryptography can be used to enforce the application of human rights. Quantum networks will offer more options for regulating security in the long term, personal data protection, and more.

4.4. Quantum machine learning

Quantum computers, when available, are expected to have a great impact on various computational problems. In particular, quantum machine learning is a very active research field in both academia and industry. A large number of quantum machine learning research groups were created in large companies, as well as a number of startups. Their goal is to develop a portfolio of algorithms in various areas such as finance or healthcare to be ready to use when quantum computers will be available.

Similar to their classical counterparts, quantum machine learning algorithms need to be trained on data. This paradigm raises two main security issues that already exist for classical machine learning. On the one hand, the algorithms themselves are produced by

investments in research and development. Companies working in the area might not want to make these algorithms public. On the other hand, data required to train those algorithms might be subject to regulation that prevents sharing them.

Although these two security issues are similar for classical and quantum machine learning, these two setups have different constraints and which will lead to different solutions. Classical machine learning algorithms are resource consuming, and their execution is usually performed on specialized hardware. This hardware can be bought by big enough companies, but in the quantum case, this seems largely unrealistic because of the expected price of quantum computers. For this reason, most companies building quantum computers are also developing – or already propose (IBM, n.d.) – a cloud access to their hardware. How can the secret of the algorithm be maintained in such a setting?

Fortunately, there exists a solution coined as *blind quantum computing*, which can be achieved by connecting the quantum computer to a quantum communication network. In this setup, it is well-known that quantum programs can be efficiently and securely delegated to the server. The server then runs an encrypted version of the program and returns the answer without learning the computation it is running.

In the classical setting, this task is known as homomorphic encryption. Surprisingly, the quantum version is much more efficient than the classical one, and only induces a minor overhead on the computation as long as a quantum communication channel allows the client to drive the computation remotely. Moreover, it only requires a very light client which can be built with currently existing technology, and a conversion from the qubits used for transport to the qubits used for computing.

While blind quantum computing is often recognized as a killer-feature for quantum networks, we want to stress that it also fits well with the planned development of quantum computers and quantum networks. Quantum computers will be expensive and probably mutualized through HPC facilities accessible to multiple users. Creating quantum communication networks between those users and the facility will bring security for the algorithms.

The second issue that needs to be considered is the security of data. While startups may be developing quantum machine learning algorithms today, and get cloud access to quantum computers, getting access to sensitive data may not be possible today or in the future.

A solution to this problem for classical machine learning is to add noise to the data to preserve privacy. Machine learning algorithms are naturally resistant to noise (an algorithm that recognizes a cat on a picture should be able to recognize a cat on a noisy picture). Quantum networks being inherently noisy and lossy, we might be able to take advantage of that feature to enhance security and privacy.

Challenge nº5: Use the noise of quantum networks to make quantum machine learning algorithms private by-design.

5. Conclusion

The goal of this report is to give examples of the impact that quantum networks will have in the long-term. While the impact of quantum key distribution is studied in WP1, we are going beyond this task. We have selected a limited number of potential quantum tasks that we consider could have a high impact. This already allowed us to identify a wide range of applications in a number of different areas.

Concretely, it shows that a quantum key distribution network is only a first step toward the ambitious goal of building a global quantum internet. Researchers have identified several steps that will lead us from current technologies to this final goal, each step unlocking new tasks for quantum networks. We have shown that each step will also bring new potential end-users that could use quantum communication for their information processing tasks.

The classical internet has changed all aspects of data processing. This has led people to realize the importance of data, and consequently of data protection. With its deep impact on cryptography, a global quantum network will pursue this story. Better control of connected devices, longer data security, better privacy protection, collaboration between mistrustful parties, many aspects of data processing will be impacted at all the different stages of quantum network developments.

6. Acknowledgements

We would like to thank all the people that accepted to discuss the potential uses of future quantum networks: thank Tommaso Gagliardoni and Ryan Spanier (Kudelski security), Kurt Nielsen (Partisia), Vincent Danos (Giri), Aisling Connolly (Ingenico), Vincent Deslandes and Jean-Gabriel Krieg (Airbus), Laurent Poupon, Marc-Michel Stack and Thierry Moineau (BNP), Adam Ouorou and Sebastien Canard (Orange), Iordanis Kerenidis (QC Ware France).

7. References

Aggarwal, D., Brennen, G., Lee, T., Santha, M., & Tomamichel, M. (s.d.). *Quantum attacks on Bitcoin, and how to protect against them.* ArXiv.org.

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, (pp. volume 175, page 8).

Coladangelo, A., & Sattath, O. (2020). A Quantum Money Solution to the Blockchain Scalability Problem. *Quantum, 4*(297).

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 644 - 654.

Doosti, M., Kumar, N., Delavar, M., & Kashefi, E. (2020). *Client-Server Identification Protocols with Quantum PUF.* Obtido de https://arxiv.org/abs/2006.04522

IBM. (s.d.). *IBM Quantum Experiment*. Obtido de https://quantum-computing.ibm.com/

Ikeda, K. (2018). Security and Privacy of Blockchain and Quantum Computation. Em *Blockchain Technology: Platforms, Tools and Use Cases.* Pethuru Raj and Ganesh Chandra Deka.

Kiktenko, E., Pozhar, N., Anufriev, M., Trushechkin, A., Yunusov, R., Kurochkin, Y., & Lvovsky, A. a. (2018). Quantum-secured blockchain. *Quantum Science and Technology , 3*(3).

National Security Agency Central Security Service. (October de 2020). *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)* . Obtido de https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/

VeriQloud. (s.d.). *Quantum Protocol Zoo*. Obtido de wiki.veriqloud.com

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science, 362*(6412).