Be it a new product design we wish to hide from competitors, or our credit card credentials when purchasing flowers for Mother's Day – we all have secrets we wish to protect from prying eyes. From ancient Mesopotamia to block-chain currency, humanity has been using cryptography to defend its valuable information, but a new threat to these classic solution has emerged in the form of quantum computing.

The rise of quantum computers casts a shadow on modern encryption schemes, threatening to shatter internet and communication security. In this document we will introduce an encryption technology like none before it, relaying on the same physical properties of quantum computing to safeguard against it – Quantum Cryptography. While sometimes portraited as a cryptographic "silver bullet", Quantum Cryptography is not without its own disadvantages, and is suited mostly for organizations with highly sensitive, long-term information the such of banking, finance and defence industries. Before we can dive deeper into Quantum Cryptography however, we must consider something more basic – what is cryptography?

Cryptography encapsulates methods and procedures used to protect information with the use of code. One such method is encryption. Encryption is a general term used to describe masking of information using a secret - one side hides the information, and only those with the appropriate knowledge of a specific secret can access this information. The term used to describe this secret is "key", as encrypting of information is paralleled to locking it in a safe. The key used to encrypt the information and the key used to decrypt the information are not necessarily identical. When both keys are the same, we refer to the process as "symmetric encryption" and when they are different "asymmetric encryption". A major issue in encryption is securely exchanging these keys between both parties, without leaking them to any illegitimate third party.

The exchange of secure encryption keys between two parties whilst not sharing an initial secret is crucial in many fields, including internet communication and banking. Currently this problem is mostly addressed using asymmetric encryption algorithms, the like of RSA or Diffie-Hellman. These algorithms use hard to solve problems to enable the exchange of secrets between two parties. An adversary that wishes to eavesdrop on our communication must work extremely hard to crack these asymmetric algorithms, the longer our encryption key is, the harder such opponents must work.

The stronger our adversary's computers are – the faster and easier it is for them to find our key and gain access to our secret information.

This brings us to Quantum Cryptography - an umbrella term describing many protocols used to exchange encryption keys between two parties, without these two parties sharing an initial secret. The more accurate term used to describe Quantum Cryptography is Quantum Key Distribution (QKD). These protocols do not encrypt the information that we try to protect, but rather enable the two parties to securely exchange encryption keys that may then be used to encrypt the protected information.

It is easy to fall into the false pretense of encapsulating Quantum Cryptography and Quantum Computing together. While the two fields share many basic ideas, such as the use of Qubits instead of classical bits, and both fields heavily relay on fundamental principles of quantum mechanics, they have inherently different purposes. While quantum computing aims at enabling new, different, and more efficient approach to solve certain problems, Quantum Cryptography offers us a way to protect information form unwanted onlookers. Classical asymmetric encryption algorithms are vulnerable to quantum computing. If we imagine the problem of finding our encryption key as lifting a weight off the ground, then classic computers are trying to lift the weight using their (metaphorical) hands and back, while quantum computers use leverages and

pullies. Doubling the weight might make the challenge much harder of classical computers, but for quantum computers - not as much.

Unlike the classical asymmetric algorithms, QKD utilizes some of the fundamental principles of quantum mechanics to secure the exchanged keys. This physical security ensures that no matter how advanced our adversaries are, they could not extract information of our encryption keys without being detected. Since the encryption key itself is of no value until we use it for encrypting information, we can discard exposed keys, and could therefore prevent an adversary from accessing the encrypted information.

Quantum computers rapidly become more advanced and has already left the academic domain and entered the hands of major industrial powers such as IBM and Google which will further haste the field's development. Once a sufficiently strong quantum computer is available, classical asymmetric encryption scheme will be compromised. NIST (The US National Institute of Standards and Technology) is currently working on post-quantum encryption standards, meant to address the risk quantum computing poses to present-day encryption. These post-quantum algorithms maintain security through the same methods as the other classical algorithms – a very hard problem, to which quantum computing does not **currently** have a good solution. There is no guarantee that an appropriate quantum-algorithm, able to break these post-quantum cryptographic algorithms, be discovered or developed in the future.

In many ways, quantum computing is the driving force behind developments in QKD. Since QKD offer physical protection, it is secure against classical computers and quantum computers alike – physics itself obfuscate our secrets. We no longer place the weight on the floor, we now merge it completely with the ground.

In classical encryption, changing encryption keys requires delivery of key across the channel, or sharing instruction on how to arrive at the required key. This means that an adversary who records our communication, and at some point in the future manages to figure out our initial key, now has all our encryption keys from that point forward. In QKD however, the key itself is never transferred across a classical channel, but only through a physically secure quantum channel. This means that if we exchange encryption keys via QKD, even if somehow a key is leaked to an opponent, once we replace it our communication is once again secured. The information itself is still transferred on a classical channel, but without information of our key, even quantum computers can't decipher it.

The physical nature of protection provided by QKD ensure secrecy regardless of technological and algorithmic progress – as long as it does not shake the foundation of quantum mechanics to their core.

While all this is true and good, migration to QKD security is not trivial, nor is it an absolute necessity. The migration to QKD requires dedicated infrastructure, and is therefore applicable mostly to highly sensitive industries such as banking, data centers, communications, defence contractors etc. For many organizations post-quantum cryptography will supply sufficient protection, and the deployment of QKD systems does not justify the expensive overhead.

However, if your information secrecy's lifetime is long, QKD is currently the only cryptographic method offering complete forward protection. Once a link has been established, the keys are grunted to be completely secured by physics, regardless of algorithmic and computing advancements – quantum, classical or otherwise.