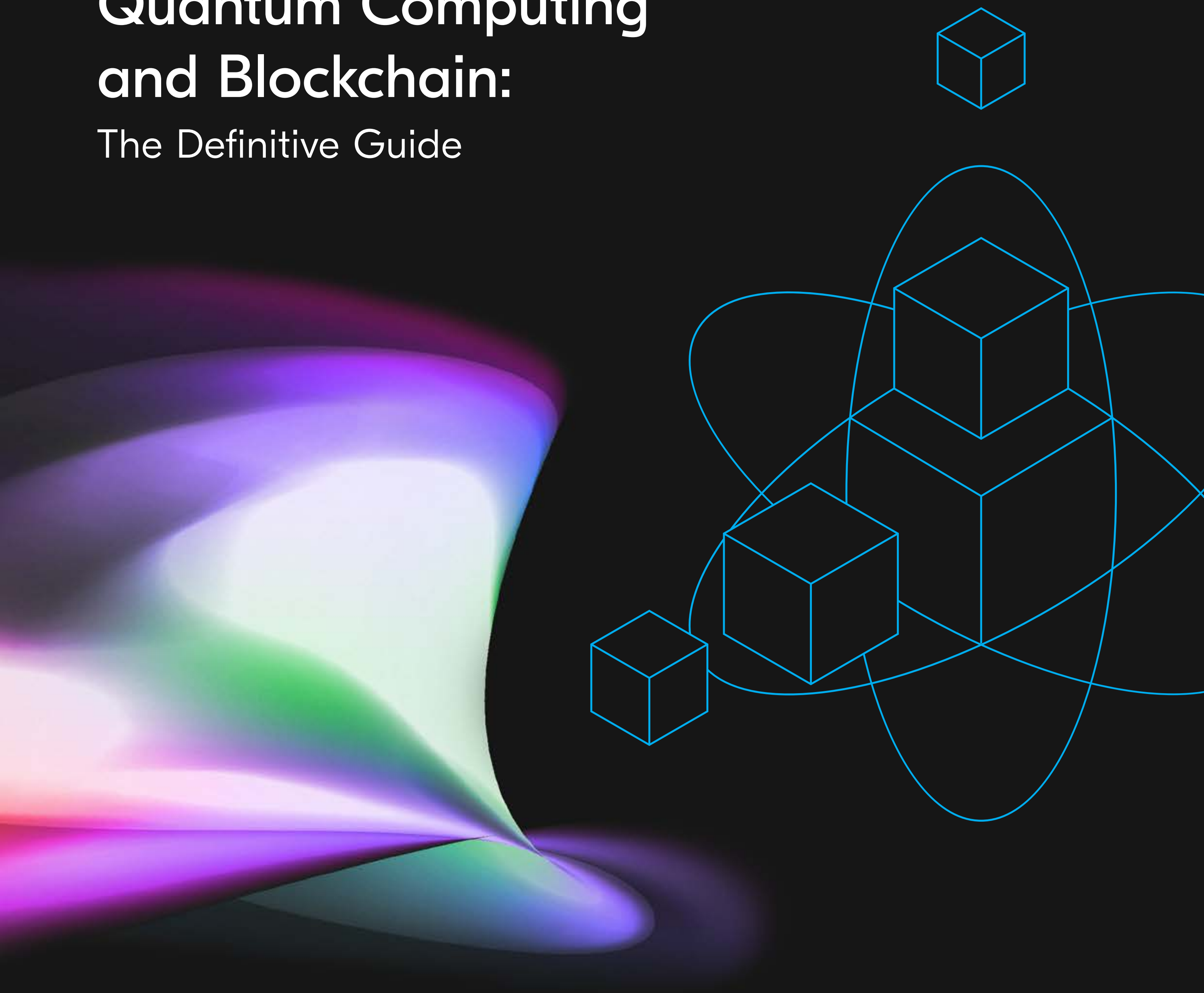
QAN

BLOCKCHAIN PLATFORM

Quantum Computing and Blockchain:

The Definitive Guide

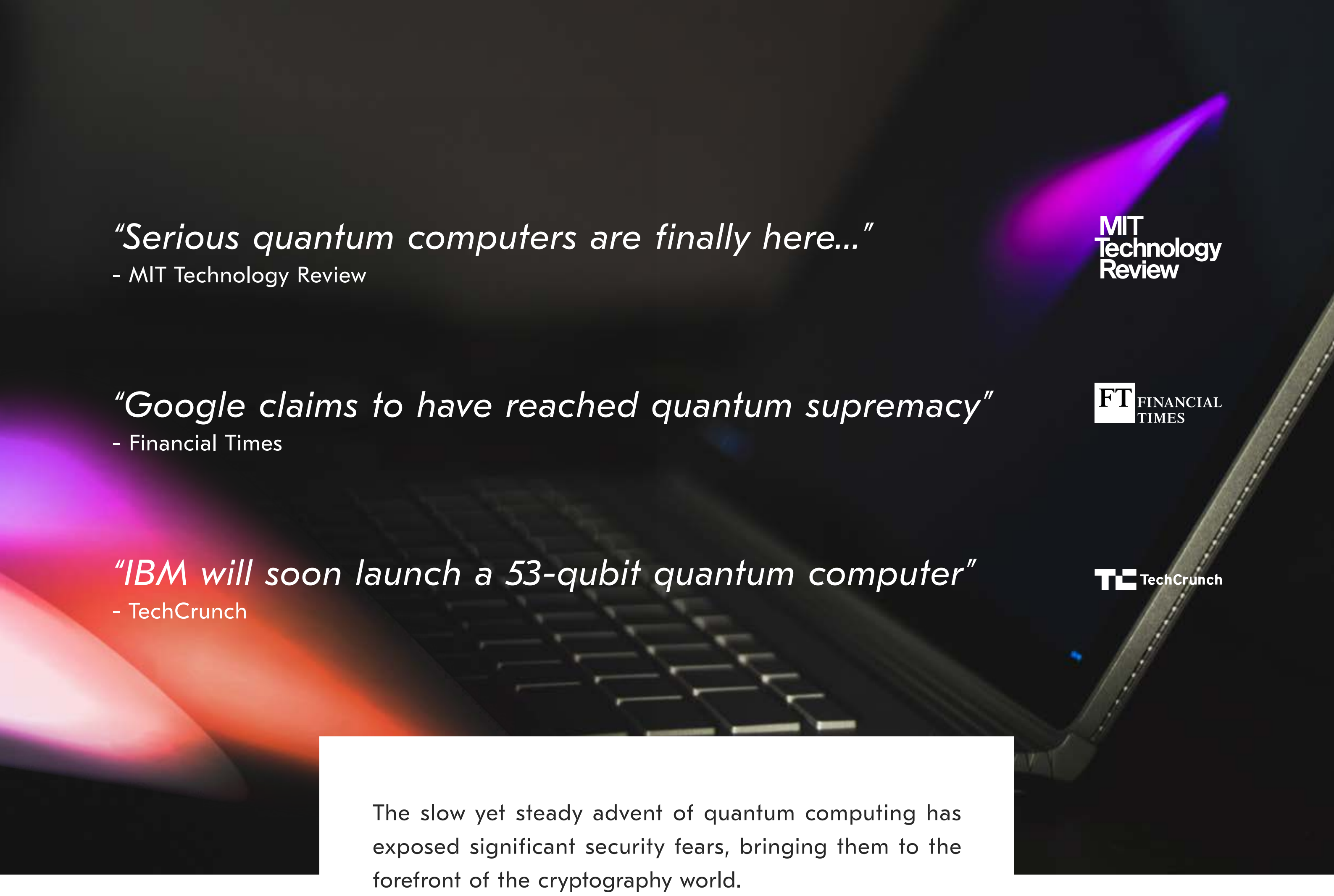


powered by

centrum circle

QANPLATFORM.COM

Contents List



“Serious quantum computers are finally here...”
- MIT Technology Review

“Google claims to have reached quantum supremacy”
- Financial Times

“IBM will soon launch a 53-qubit quantum computer”
- TechCrunch

The slow yet steady advent of quantum computing has exposed significant security fears, bringing them to the forefront of the cryptography world.

Due to the fact that cryptography is an essential foundation of much of our lives as we know them, quantum computers pose a threat to a wide array of industries.

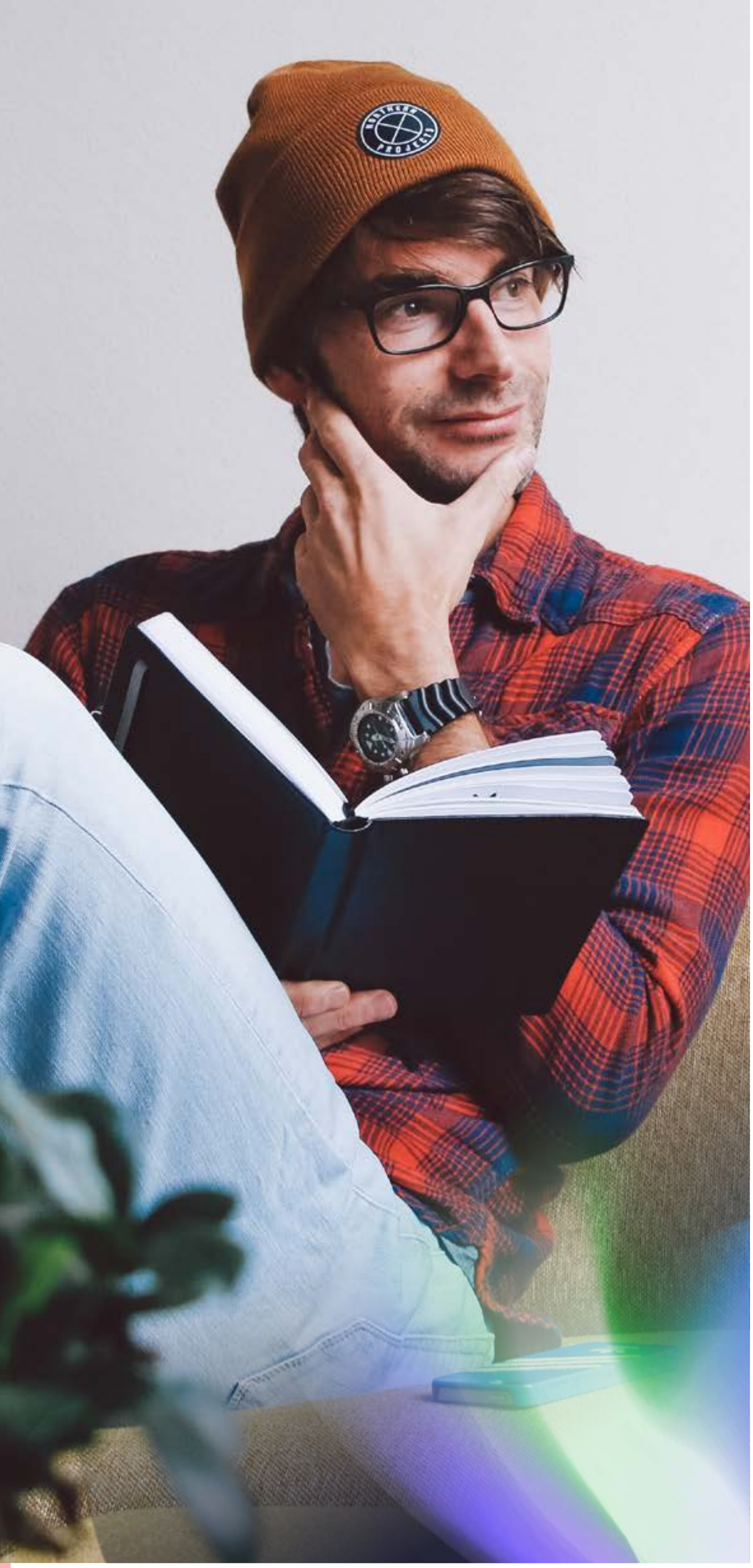
But do we really need to worry today?

You will learn in this ebook about *the problem, its origin, mechanisms,* and *implications* as well as the steps that are being taken to remedy the threat that quantum computers pose. Lastly, you will discover a quantum-resistant blockchain platform.

Let’s dive right in.

1

What is Quantum Hardness?



1.1 Understanding Cryptography

Cryptography is a cornerstone of today's world. In its most primitive form cryptography refers to the act of using codes to protect data, information, and communication so that only those for whom the information is supposed to reach can access, decipher, and eventually utilize as it they see fit.

Over time, our communication and data storage tools evolved. So did the need to create a more robust and efficient framework for protecting data. Thus, modern cryptography was born.

What is cryptography?
Modern cryptography employs a combination of complex and sophisticated mathematical equations called algorithms and their corresponding keys to encrypt and decrypt data.

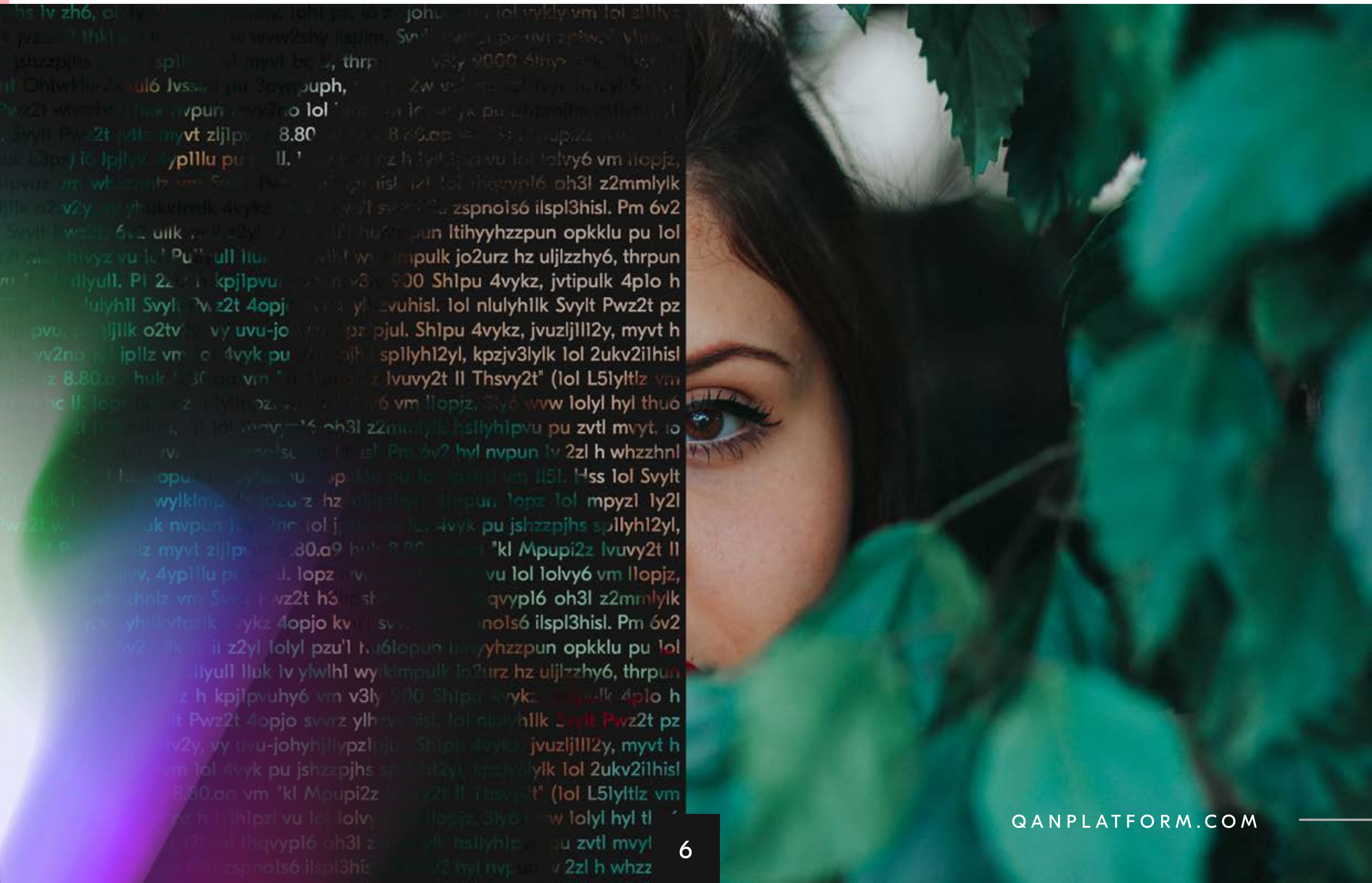
Encryption refers to the process by which data is run through a certain algorithm in order to produce what seems like a jumble of useless or unintelligent data to an onlooker. Without the corresponding secret key, which the recipient uses to unlock the data and access the data in its raw and legible form, the data is inaccessible.

Encryption vs. Decryption

"The process of converting the information from 'plain text' to 'cipher text' is known as 'encryption.' On similar lines, the process of converting 'cipher text' to 'plain text' is decryption."

Explained by the InfoSec Institute

The algorithm employed by the sender to convert the plain text into the obscured data and the key used by the recipient are components of the same cryptosystem. In the context of cryptography, a cryptosystem refers to the set of cryptographic algorithms needed to implement a particular security outcome. Generally, a cryptosystem is comprised of three algorithms. The first is employed to generate the key while the last two for encryption and decryption respectively.



Encryption algorithms typically fall into either of two types:

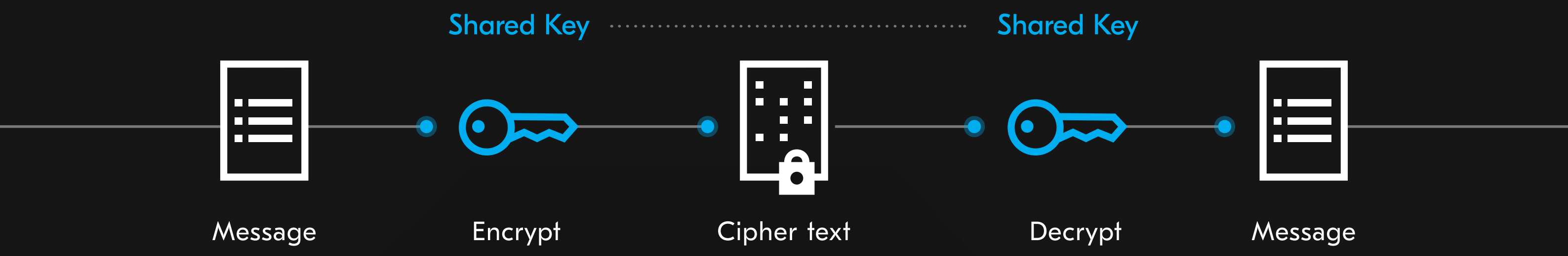
1. symmetric
2. asymmetric algorithms.

Symmetric algorithms employ separate instances of the same key to encrypt and decrypt the data. These algorithms are typically faster than their asymmetric counterparts. However, they fall short in terms of key distribution and key management. The parties using symmetric algorithms must be able to transmit the key confidentiality or the cryptosystem is compromised. Moreover, as the number of users grows so do the number of keys, which creates a new problem of how to securely store and manage the keys.

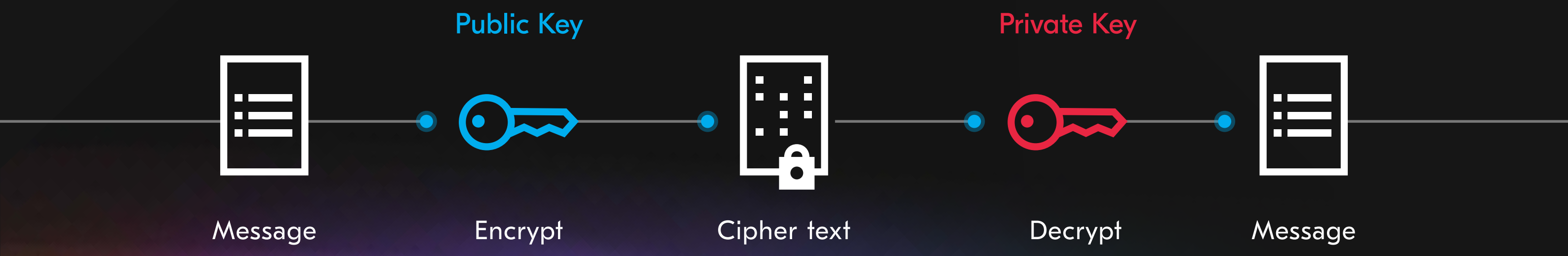
In **asymmetric encryption,** the sender and the recipient use different keys to encrypt and decrypt messages. The public key is used to encrypt the message, and the private key is used to decrypt the message. The public keys are generally made public information while the private key is reserved only for the recipient. However, it is important to note that they are two parts of the same cryptosystem and are mathematically comparable.

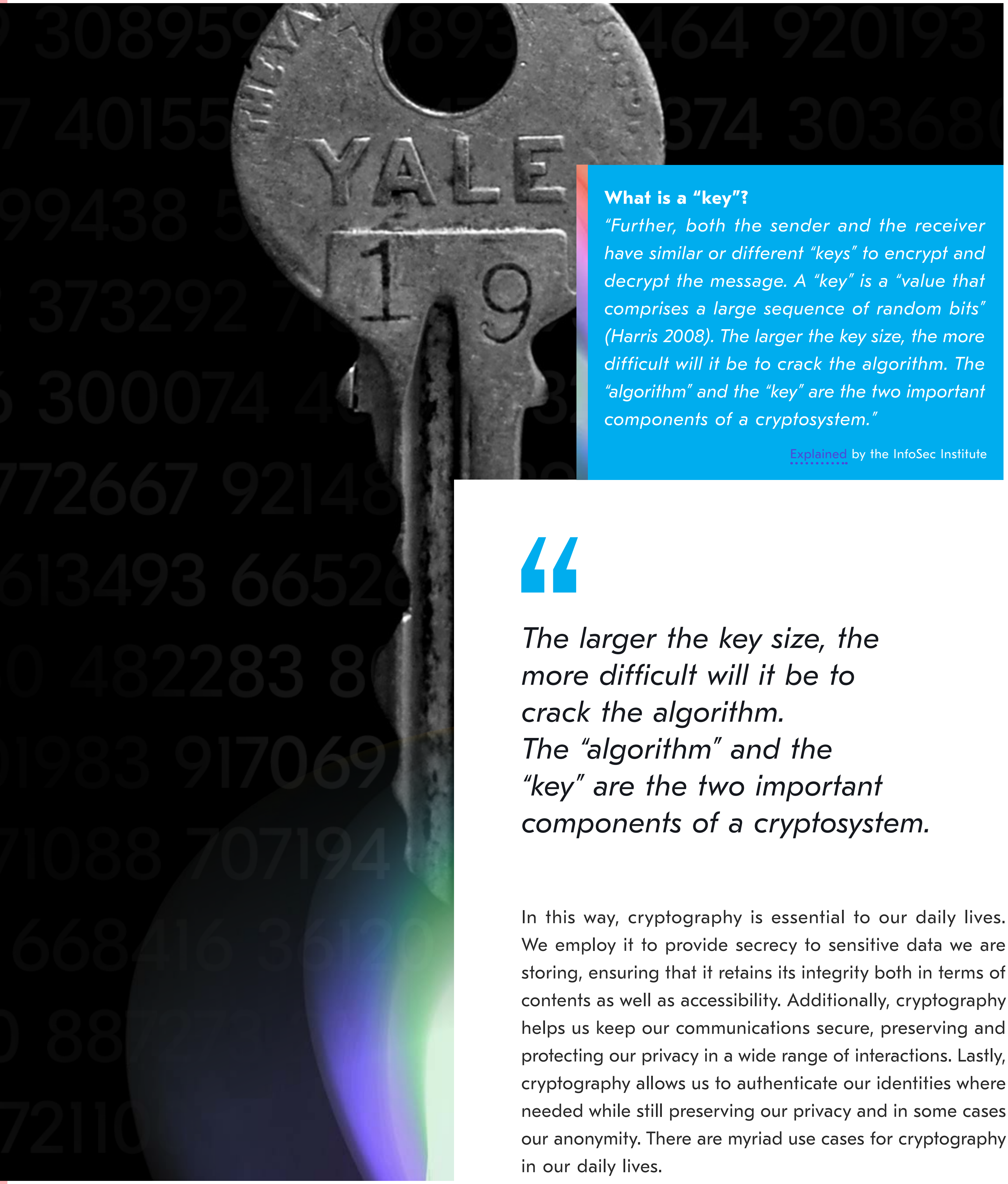
Despite its relative slowness in comparison to symmetric cryptography, asymmetric cryptography upholds the security tenets of authenticity and non-repudiation. It is important to note that the recipient and sender generally have access to two different keys as a generally accepted security standard. Because the sender's key is usually made public as a tool through which it is possible to authenticate the identity of the source as well as the integrity of the data, the recipient usually has a private key which they use to "unlock" the data which simultaneously serves to authenticate his identity.

Symmetric Encryption



Asymmetric Encryption





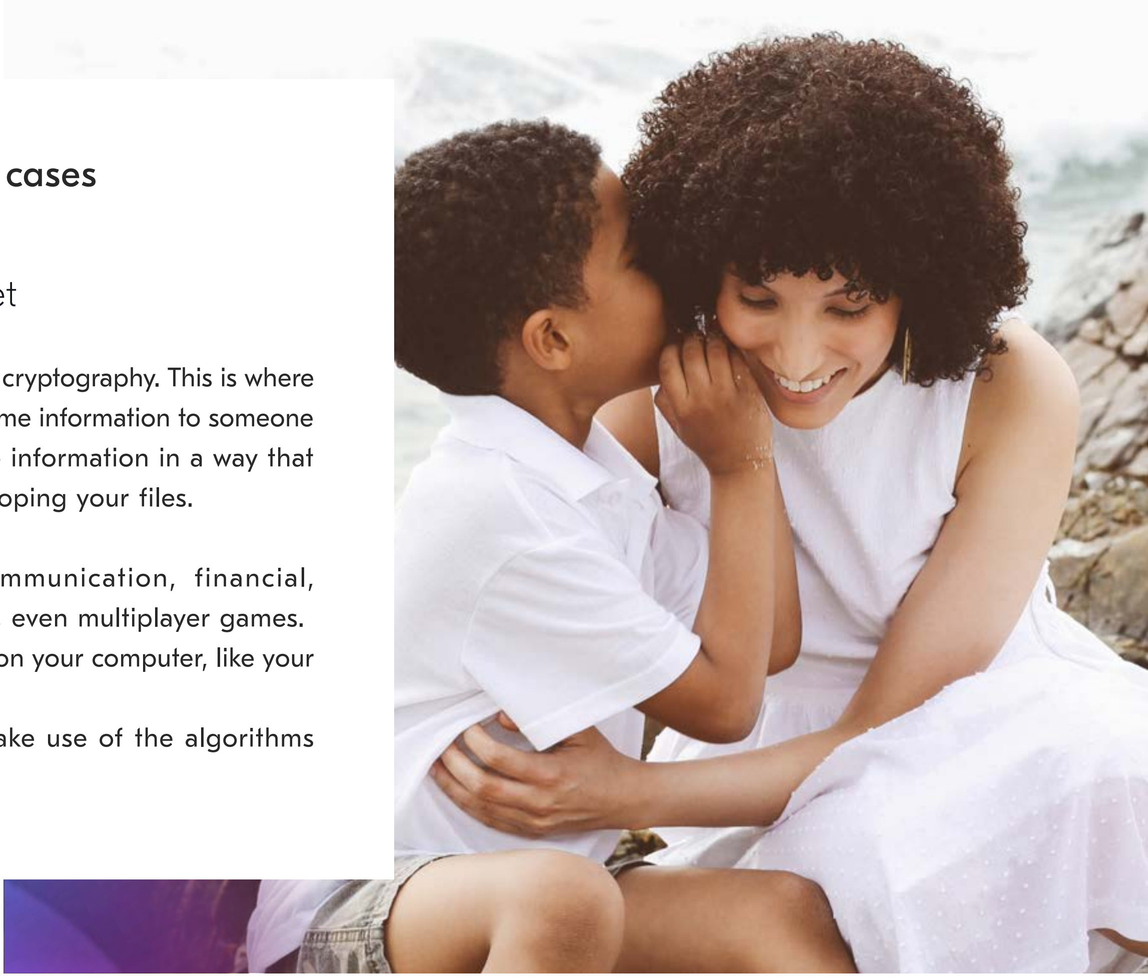
What is a "key"?

"Further, both the sender and the receiver have similar or different "keys" to encrypt and decrypt the message. A "key" is a "value that comprises a large sequence of random bits" (Harris 2008). The larger the key size, the more difficult will it be to crack the algorithm. The "algorithm" and the "key" are the two important components of a cryptosystem."

Explained by the InfoSec Institute

> *The larger the key size, the more difficult will it be to crack the algorithm. The "algorithm" and the "key" are the two important components of a cryptosystem.*

In this way, cryptography is essential to our daily lives. We employ it to provide secrecy to sensitive data we are storing, ensuring that it retains its integrity both in terms of contents as well as accessibility. Additionally, cryptography helps us keep our communications secure, preserving and protecting our privacy in a wide range of interactions. Lastly, cryptography allows us to authenticate our identities where needed while still preserving our privacy and in some cases our anonymity. There are myriad use cases for cryptography in our daily lives.



Cryptography use cases in our daily lives:

1. Keeping a secret

This is the standard use of cryptography. This is where you want to either send some information to someone else, or you want to store information in a way that prevents others from snooping your files.

a. Secure network communication, financial, government, medical, even multiplayer games.
b. Securely storing data on your computer, like your password keeper.
c. Crypto-currencies make use of the algorithms for digital wallets.

2. Proving Identity

With public-key encryption, also called asymmetric encryption, it is possible to digitally "sign" some content in a way that proves to others who created the content. Or another way identity is proven is when you attempt to connect to a server, such as your bank.

a. Digital certificates that are used to sign programs that you run on your computer and apps that you run on your phone. It lets you know that the app you are running is what the developer created, and has not been modified.
b. Digital certificates are used by websites to verify that they are in fact your bank, or your companies secure VPN login portal.

Great interpretation from Paul M Watt, MS Cybersecurity
from Johns Hopkins University

1.2 Security in Cryptography

In symmetric cryptography, the type of cryptography that is heavily in use across the world due to its superior security considerations, security is related or relies on "hard" problems.

As explained earlier, algorithms are simply complex mathematical equations through which information is fed to create another set of data.

Hard problems are central to symmetric cryptography because they are practical to compute with the right key but are infeasible to crack in the absence of the corresponding private key.

A "hard" problem, one that is ideal for use within the context of cryptography, should take the best computers available a long time to solve without the corresponding key. On the contrary, an "easy" problem is one that can be solved very quickly and, thus, is ineffective and unsuitable for use within a cryptosystem.

> *The most widely used form of cryptography for laypeople and daily use, public-key cryptography, is heavily dependent on integer factorization and discrete log problems. These are hard problems. They are difficult for classical computers to break.*

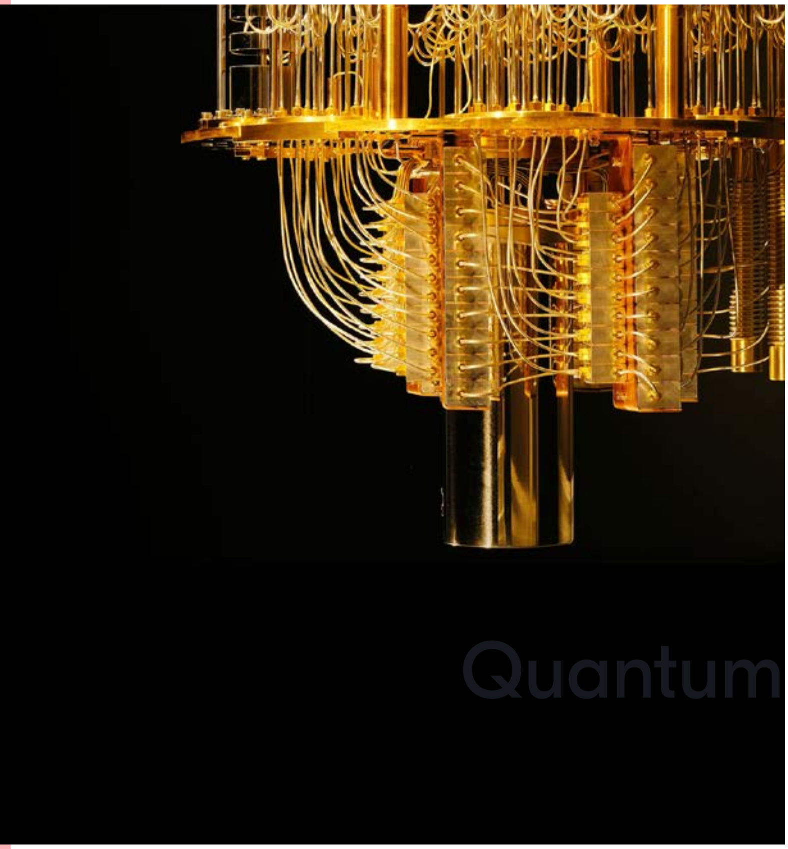
1.3 Quantum Hardness

Unfortunately, most hard problems, on which public-key cryptography is currently based on, are easy for quantum computers to solve. Thus, you may have inferred that quantum hardness refers to a problem that is just as hard for quantum computers to solve.

The most widely used PKC systems, including RSA, Diffie-Hellman, and ECDSA are hard for classical computers to solve but easy for quantum computers. They are quantum easy.

To understand why quantum computers seemingly do not follow the rules that classical computers adhere to, it is important to understand how they function.

A quantum computers are a relatively new type of computer that utilizes the different quantum states of subatomic particles to store information. In quantum computers, calculations are determined by examining the behavior of particles at the atomic and sub-atomic level, hence the name quantum.



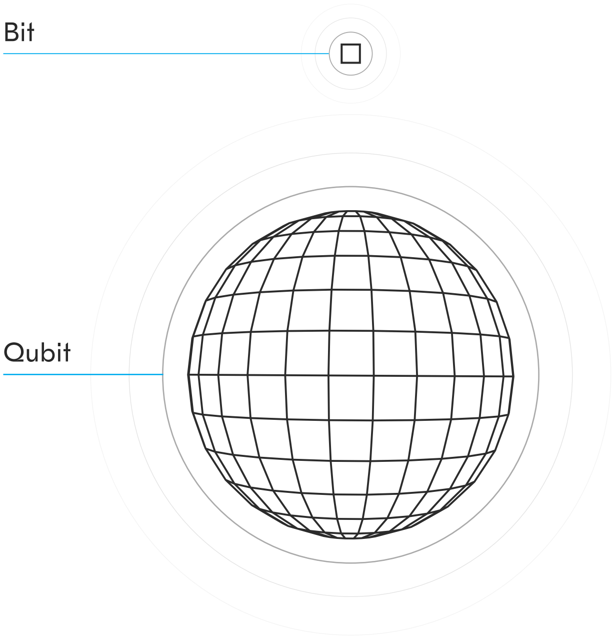
Quantum computer vs classic computer

To further understand the difference between quantum and classical computers, consider that classical computers, such as your PC, are binary in nature. In other terms, classical computers utilize bits in the form of transistors which can exist in either of two values — 0 or 1. Contrastingly, quantum Computers use Qubits which can either take a value of 0 or 1 or both simultaneously in a state of superposition.

Quantum vs Classic

Thus, theoretically speaking, quantum computers are capable of efficiently handling a much greater number of instructions per second than their classical counterparts. Data in a quantum computer is stored in qubits, where it can exist in more than one state, and because of this, there is an exponential increase in the millions of instructions per second (MIPS).

Data in quantum computers is denoted in Qubits, which are similar to normal bits, except that they can take on more than one value, sometimes many, simultaneously.
Furthermore, due to the fact that information in quantum computers is not stored or processed in a binary manner, the machine is able to "think" different "thoughts" at the same time. This simultaneous consideration of varying end states from the same set of particles/variables/data allows quantum computers to have much faster processing capabilities.



Based on their impressive processing capabilities, quantum computers represent a risk for cryptography as we know it. Robert Schoelkopf, a Yale professor and founder of a company called Quantum Circuits, reiterates the danger posed by the emergence of quantum computing.

Robert Schoelkopf | Picture via Weforum

Schoelkopf says:

> *"If you had 50 or 100 qubits and they really worked well enough, and were fully error-corrected— you could do unfathomable calculations that can't be replicated on any classical machine, now or ever. The flip side to quantum computing is that there are exponential ways for it to go wrong."*

Johann Polecsak, CTO of quantum-resistant blockchain platform QAN, said in a Forbes.com interview:

“In cryptography, it’s best to prepare for the worst, and one can observe in recent literature that past skeptics now instantiate their crypto protocols in a post-quantum setting - just in case. Users shouldn’t worry now, but experts should prepare before it’s too late.”

Quantum computers have long been considered a theoretical threat due to the difficulty involved in developing the machines. To effectively function as a quantum computer, their data sets, qubits must stay in the quantum state. However, they are notoriously prone to abandoning their quantum state over the slightest disturbance. Examples of these disturbances are tiny electrical discharge, heat, stray electromagnetic fields or even slight physical activity.

Quantum hardness is related to post-quantum cryptography. This is a relatively new school of cryptography dedicated to creating cryptographic algorithms that are thought to be able to withstand an attack by quantum computers.

> *“The focus of post-quantum cryptographic study is currently centered on public-key algorithms due to their essentiality in a wide array of use cases across industries globally. These algorithms can also be referred to as quantum-proof, quantum-safe or quantum-resistant algorithms.*

2

Why Do We Need Quantum Safety At All?

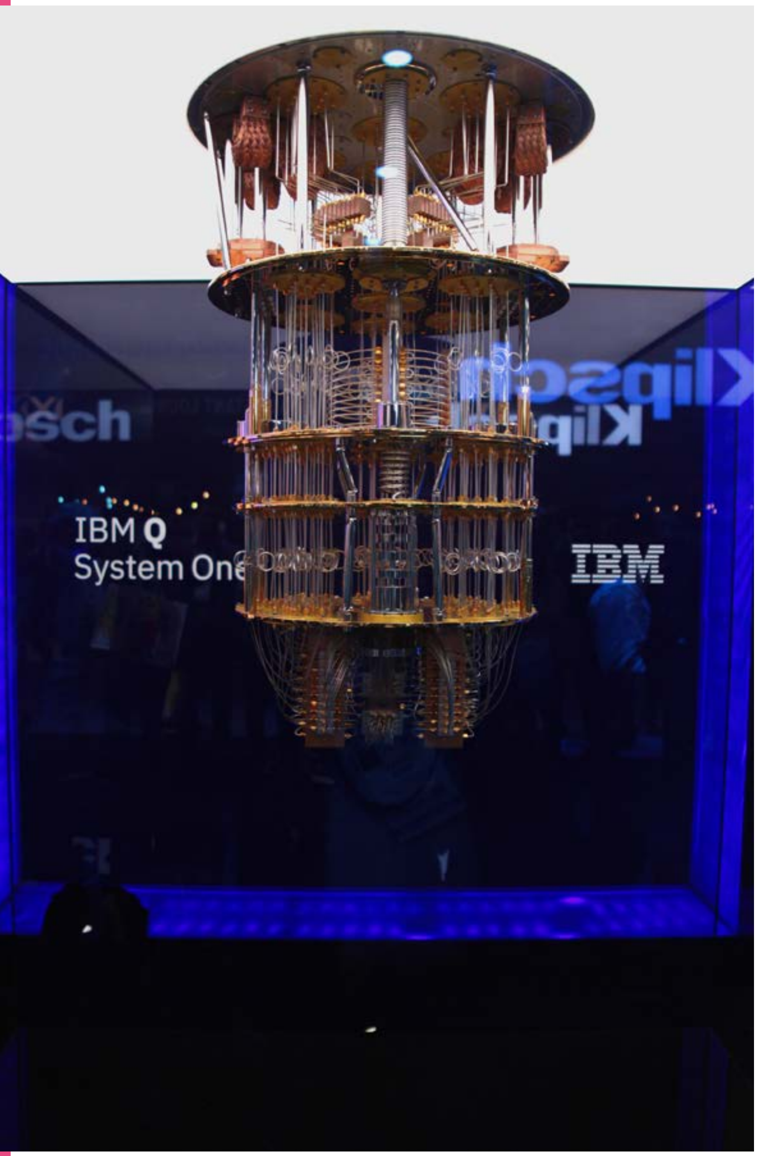
2.1
A Short History

Edward Snowden | Picture via Shifter

Fears regarding the threat that quantum computing represent began to grow in magnitude following Snowden's leak of a substantial amount of classified materials in 2014. In Snowden's data leak, he revealed that the NSA was working on developing a quantum computer within a project called "Penetrating Hard Targets (PHT)," which was allocated a $79.7 million budget.

The worries surrounding the PHT project died down relatively quickly due to the fact that the budget allocated to the program was considered paltry and that within the leaked documents were clues that pointed to a project still in its initial stages. However, in 2015, the NSA reignited these concerns when it updated its guidelines for contractors who worked with the agency. In the new set of guidelines, the NSA strongly advised other US government agencies as well as private sector parties to begin making plans for the transition to post-quantum cryptography.

> The NSA explained:
> *"Our ultimate goal is to provide cost-effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms."*



Moreover, in news that is rocking the computing world, The Financial Times was able to grab a hold of a research paper that briefly appeared on the NASA website which appears to confirm that Google has 'achieved quantum supremacy.' Google's quantum computer reportedly solved a problem, which would have taken the world's fastest supercomputer about 10,000 years to successfully compute, in only three minutes and 20 seconds.

At the time speculations were centered around whether the NSA had successfully developed a quantum computer or that the agency had knowledge of a functional one.

The threat of quantum computing is now turning into a reality as opposed to a far-away nightmare. Last year, tech giant IBM announced that it had developed a quantum computer. IBM's earliest quantum computer was a 20-qubit machine, with in-house computer scientists working on upgrading it to a 50 qubit capability.

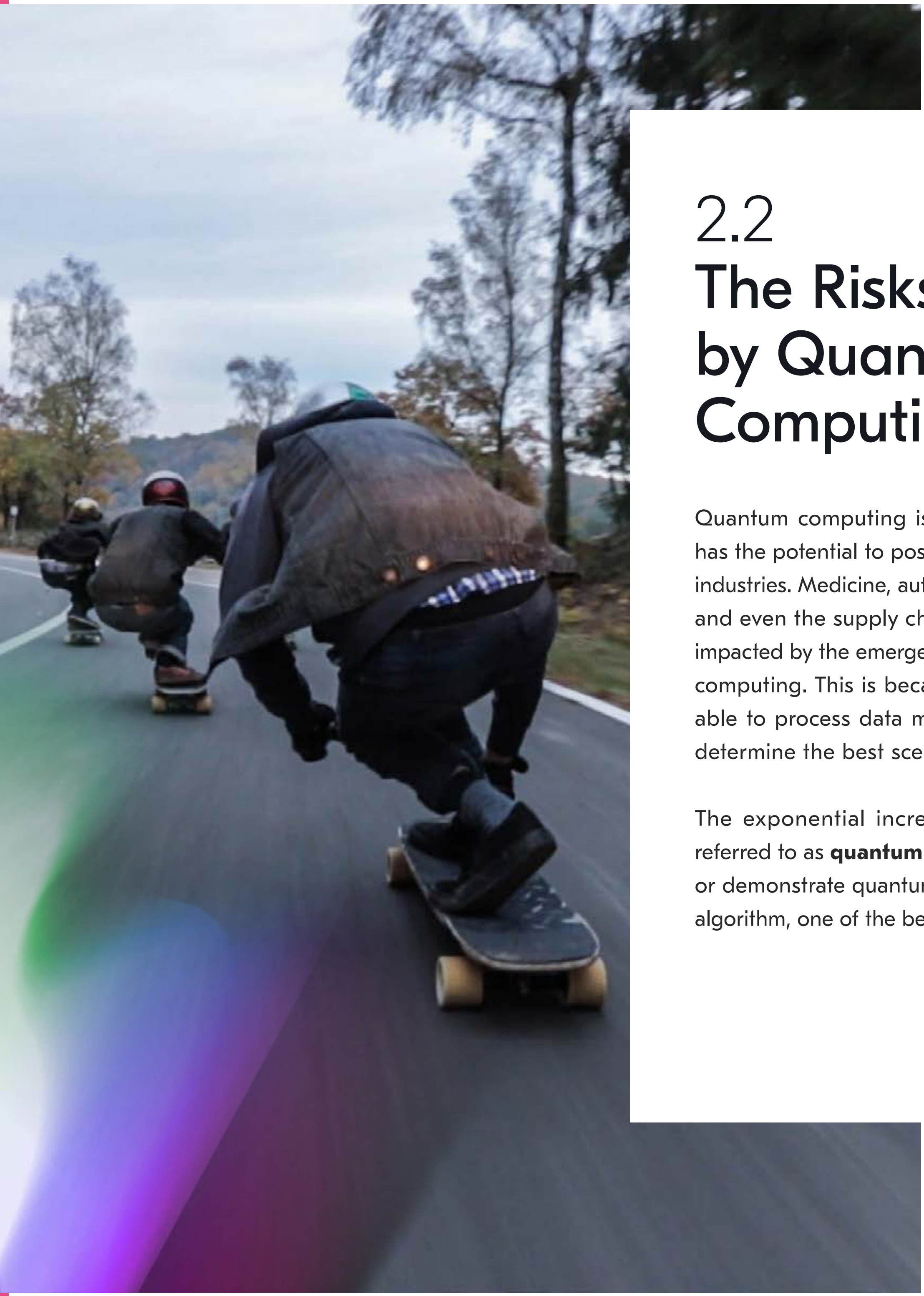
However, in September 2019, IBM revealed that it was making a number of quantum computing systems available commercially, including a 53 Qubit quantum computer. IBM reiterated that the move represented the ushering in of a new age stating:

> *"This milestone represents a paradigm shift in quantum computing, marking the first large-scale deployment of quantum computing systems. One of the systems to be released next month has 53 qubits, which will make it the largest commercially available universal gate-model quantum computing system to date."*

In the paper titled **"Quantum supremacy using a programmable superconducting processor,"** published on September 23, 2019, Google stated: *"To our knowledge, this experiment marks the first computation that can only be performed on a quantum processor."* By demonstrating that quantum computing is indeed superior, Google has ushered in a new age where everything which relied on older non-quantum safe cryptographic systems must adapt or be left behind.

Bitcoin.com asked Johann Polecsak, CTO of quantum-resistant blockchain platform QAN about his thoughts:

> *"This milestone represents a paradigm shift in quantum computing, marking the first large-scale deployment of quantum computing systems. One of the systems to be released next month has 53 qubits, which will make it the largest commercially available universal gate-model quantum computing system to date."*
>
> *Johann Polecsak, CTO of QAN*



2.2 The Risks Posed by Quantum Computing

Quantum computing is a scientific innovation that has the potential to positively impact a wide range of industries. Medicine, automation, artificial intelligence, and even the supply chain are likely to be positively impacted by the emergence and adoption of quantum computing. This is because quantum computers are able to process data much quicker and are able to determine the best scenarios out of a wide data set.

The exponential increase in processing speed is referred to as **quantum speedup.** To best understand or demonstrate quantum speedup, consider Grover's algorithm, one of the best-known quantum algorithms.

What is quantum speedup?
Grover's algorithm when used in combination with a quantum computer, could find a specific name in a phone book with 100 million names in just 10,000 operations. A classical search algorithm, employing its typical mechanisms to compute the data, which would simply mean looking through all the names, would need 50 million operations - on average - to find the same name.

Unfortunately, the quality of quantum computers which makes them so advantageous in certain industries is ultimately what makes them so dangerous for cryptography. Quantum speedup means that quantum computers can break cryptographic algorithms at a much faster rate than classical machines and supercomputers.

Just as Grover's algorithm is able to achieve impressive results in the search for specific data in large data sets, there is a quantum algorithm that allows the user to decipher the prime integers of a number (N) in polynomial time. Created in 1994, the algorithm is called Shor's algorithm and is named after its creator, the mathematician Peter Shor.

Employing Shor's algorithm, it is relatively simple to find the prime factors of very large numbers. This is a significant threat to cryptography as we know it because the generally accepted standards currently involve the use of PKC, which is based on this mathematical problem.

As determined earlier, most public-key cryptosystems are of the asynchronous persuasion. This means that there is a public and private key. Employing Shor's algorithm, quantum computers can wreak havoc on all PKC cryptosystems because if there is knowledge of one fact concerning an integer, such as a public key, then the machines can uncover the prime factorization thereby breaking the code and decrypting the data.

> *"Unfortunately, through a combination of the public key, generally made available as part of the RSA cryptosystems, and Shor's algorithm, quantum computers are theoretically able to break RSA encryption."*

As it stands, much of communication transmitted over the Internet employs RSA, a type of public-key cryptosystem, to safely relay information. RSA is an acronym for Rivest–Shamir–Adleman as it is named after the scientists who created it. Unfortunately, through a combination of the public key, generally made available as part of the RSA cryptosystems, and Shor's algorithm, quantum computers are theoretically able to break RSA encryption. Quantum computers are able to crack public key encryption in much less time as well as compute discrete logarithm mod primes and discrete logs over elliptic curves.

Risks – daily live:

For the regular man, the advent of quantum computing means that safety on the internet is about to get even more complex. There are already myriad ways through which increasingly sophisticated hackers attempt to gain control of sensitive data online.

If a quantum computer would fall in the hands of malicious actors, safety, privacy, and confidentiality online would be a thing of the past. Social media and email accounts, online banking, dating apps, and the entirety of our online lives would no longer be a safe option.

Moreover, some cryptosystems are used to secure certain physical services such as ATMs and POS clients. For these, quantum computing also poses a threat.

Risks – cryptocurrencies:

For cryptocurrencies, quantum computing poses a significant risk because it can result in a scenario where it is impossible to authenticate or ascertain the digital signature appended to transactions.

Once PKC is broken, the blockchain underlying a digital currency, such as bitcoin or ethereum, would no longer be immutable because it would be easy to change records as there would be no security measures left in place

For digital currencies, the underlying ledger is both a security measure and the thing to be secured. Compromised encryption in the context of a digital currency may result in double spends, thefts, and forgeries which in the end render the cryptocurrency useless as a store and transfer of value.

Risks — for governments:

For governments, quantum computing is also a source of worry. In his keynote speech at the 2017 RSA conference, U.S. Rep. Michael McCaul, R-Texas revealed that the US was working on creating policies that can help it maintain security despite the advent of quantum computers. McCaul, also chairman of the House Homeland Security Committee and a co-chair of the Cybersecurity Caucus, is among a number of lawmakers calling for substantial increases in the funding and research allocated to the field. He said that he wants the United States to lead a coalition of like-minded nations to explore what security changes and defenses will be required for the quantum future, confirming the security concerns had reached the upper echelons of power.

It is important to note that once quantum computers break PKC encryption as we know it, then the entire history of communications and data security systems which have employed the compromised encryption are not safe. This means that governments who have intercepted data but were unable to uncover its true meaning will be able to decipher the message once quantum computing makes this possible. For governments across the world each trying to protect their interests, this is an obvious issue. Governments in Russia and China, for example, are each diverting large sums of money to research and development for quantum computing, which many are calling the new age arms race.

Post-quantum cryptography and the resulting quantum safety is of paramount significance if we are to secure or history and our future. Many of our industries rely on the tools made possible by cryptography as we know it. Unfortunately, we do not have much in the way of defense once quantum computing hits the mainstream, thus it is of great importance to proactively approach the situation and find the solutions before the worst scenario becomes reality.

3

Creating A Quantum-Proof Future

3.1
The NIST Post-Quantum Cryptographic Project

Towards the end of 2016, the National Institute of Standards and Technology (NIST) initiated a program aimed at developing and identifying quantum hard public-key cryptographic algorithms. NIST is a non-regulatory agency of the United States Department of Commerce whose mission is to promote innovation and industrial competitiveness through science and innovation. The agency provides guidelines on global standards with regards to certain areas of science, with cryptography being one.

The post-quantum crypto project encouraged submissions from any parties who had developed or were in the process of creating algorithms that qualify as quantum-safe. The agency planned to sift through the submissions, employing the wisdom of the masses to uncover algorithms that can usher the world into a new age of quantum, safety.

However, NIST noted that standardized guidance on quantum-resistant cryptography and other such related measures were likely to take a number of years before they became readily available. This is because sufficiently testing cryptographic algorithms to determine them to be actually secure and robust generally takes a number of years. The process of standardization involves many moving parts such as peer review, penetration testing and other related actions, which requires time.

For context, the RSA algorithm which as referenced earlier is a cryptographic cornerstone of PKC, has been in use for over 40 years. The algorithm was developed in the seventies and is still in use today. It took a number of years for the algorithm to become the accepted standard and even longer for more specific recommendations, such as the one to use the 256-bit larger number within the cryptosystem, to become clear.

Photo Credit: Gail Porter via Wikimedia

Adi Shamir, the S in the RSA acronym, references the need to make the move to post-quantum cryptography while reiterating the time challenges inherent to the problem. Shamir stated:

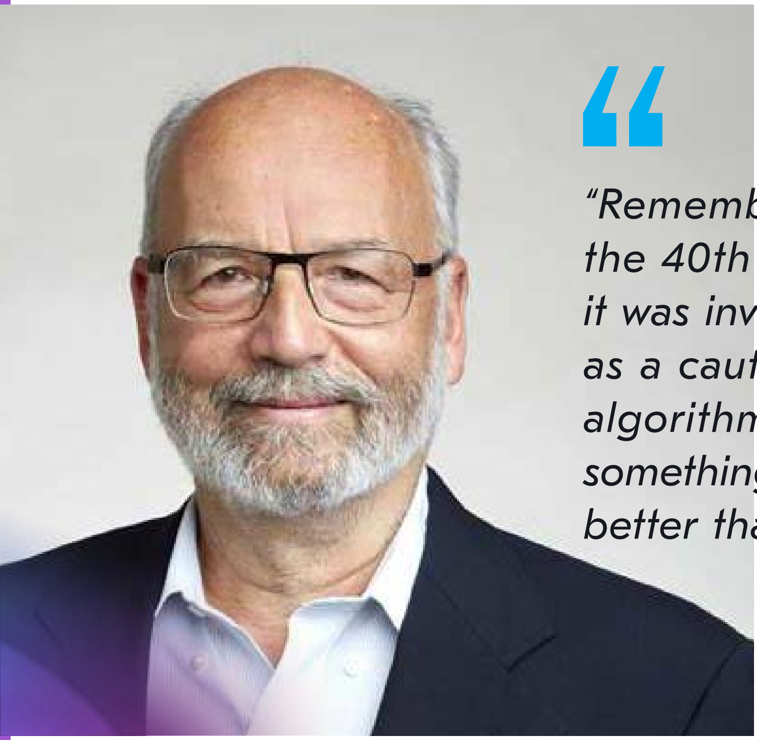
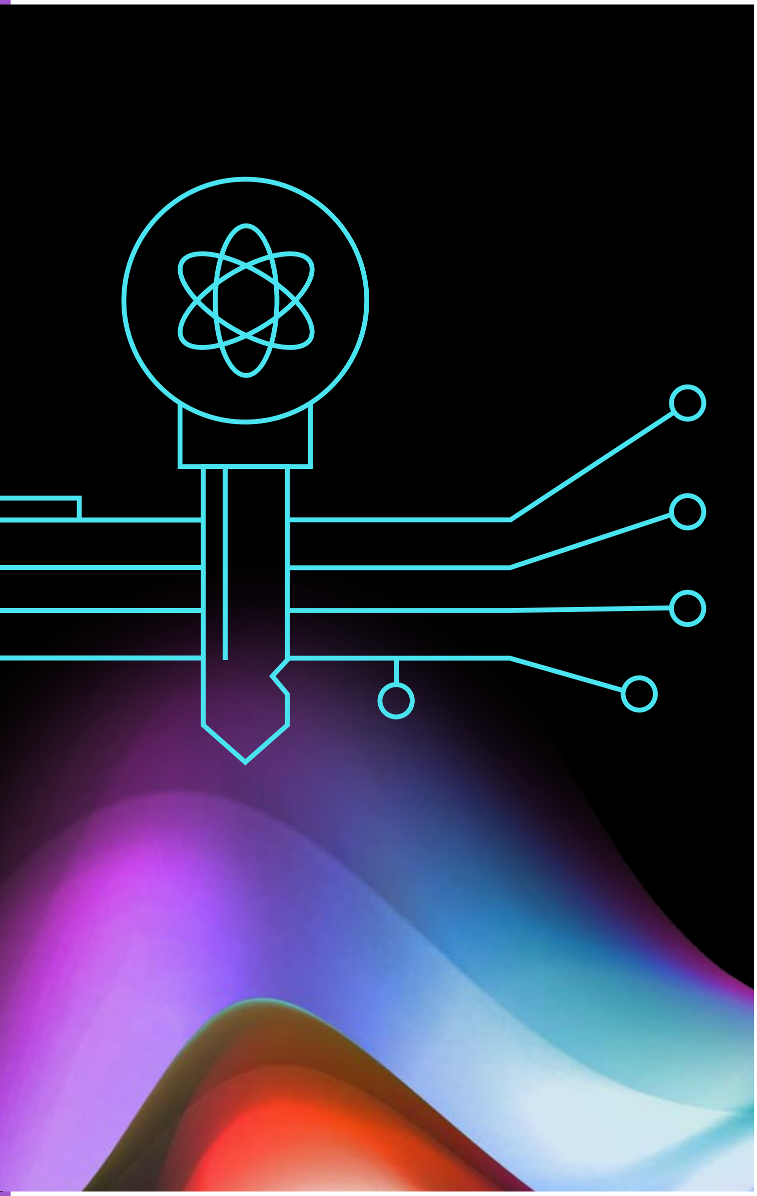


Photo Credit: Duncan Hull via Wikimedia

> *“Remember, we are celebrating this year the 40th anniversary of the RSA algorithm; it was invented in 1977. Should we switch now, as a cautionary step, to a quantum-resistant algorithm? If someone would come up with something that is both quantum-resistant and better than our current algorithms, we win.”*

3.2 Post Quantum Algorithms

What is post-quantum cryptography?
Post-quantum cryptography is defined as the study of cryptosystems which can be executed on a classical computer or a super computer but remain secure even when running on a quantum computer. The goal is not to make classical computers obsolete by creating algorithms that are not backward compatible. This would be infeasible and lead to a crisis in and of itself.



Instead, as **NIST** explains:

> *"The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks."*

To this end, NIST reviewed the submissions and published those that are the most promising in terms of creating a quantum-resistant future.

NIST identified the proposals with the greatest promise as those whose cryptosystems are based on:

- Lattices,
- Isogenies,
- Codes,
- Hash functions,
- Multivariate systems.

What are Lattices?

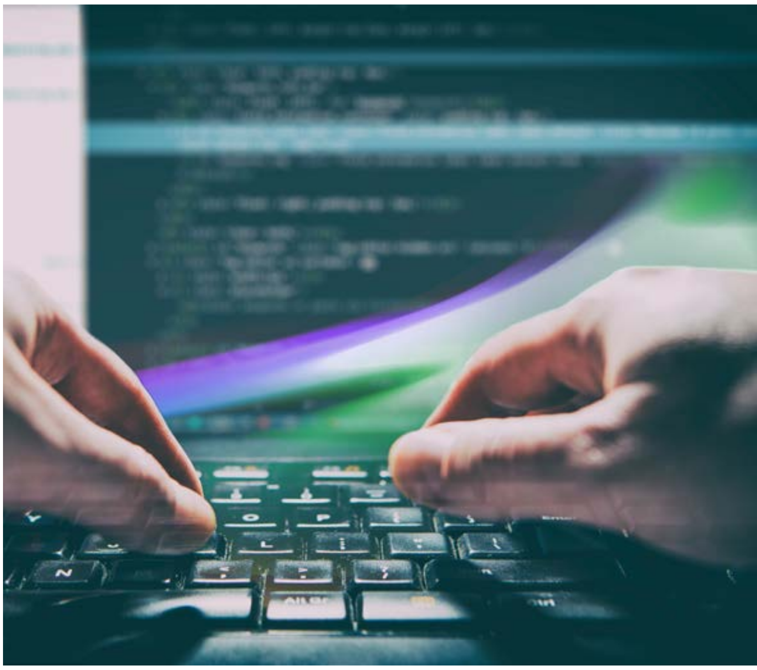
Lattices are complex mathematical structures that can be obscure data. On their own, lattices are not quantum-resistant. Fortunately, they can be employed to create quantum-proof cryptosystems. Lattices have a number of features that make them capable of achieving this feat. Namely, they can execute strong security reductions and can support effective and efficient key exchanges as well as digital signatures. Additionally, lattices are able to support more complex features like full homomorphic encryption. Within the NIST PQC submissions, Kyber and Dilithium are the cryptosystems that rely on lattices.

The second group of algorithms that hold promise for a quantum-proof future are isogenies. An **isogeny** is defined as a mathematical function that "transforms one elliptic curve into another in such a way that the group structure of the first curve is reflected in the second." The Supersingular Isogeny Diffie-Hellman (SIDH) algorithm submitted to the NIST PQC program is a favorite for quantum-proof leads based on isogenies. Within the SIDH scheme, the private keys would be a chain of isogenies and the public key would be a curve.

In comparison to the other proposed quantum-resistant schemes shortlisted by NIST, isogeny-based algorithms have been proven to have the smallest key sixes. This is an advantage as smaller key sixes are more storage efficient. Unfortunately, the size consideration comes at the cost of speed as isogeny-based algorithms are the slowest out of the four shortlisted schemes. Another important thing to note about isogenies is that they are the only proposed quantum-proof algorithms that support perfect forward secrecy.

Error-correcting codes are a mainstay in modern computing. This is the type of code referred to in the NIST QPC shortlisted schemes. Theoretically, codes can be quantum-proof because it is computationally difficult to decipher any data without knowing the linear code upon which it is based. The McEliece public key cryptosystem is the most promising cryptosystem for a quantum-proof future that utilizes codes.

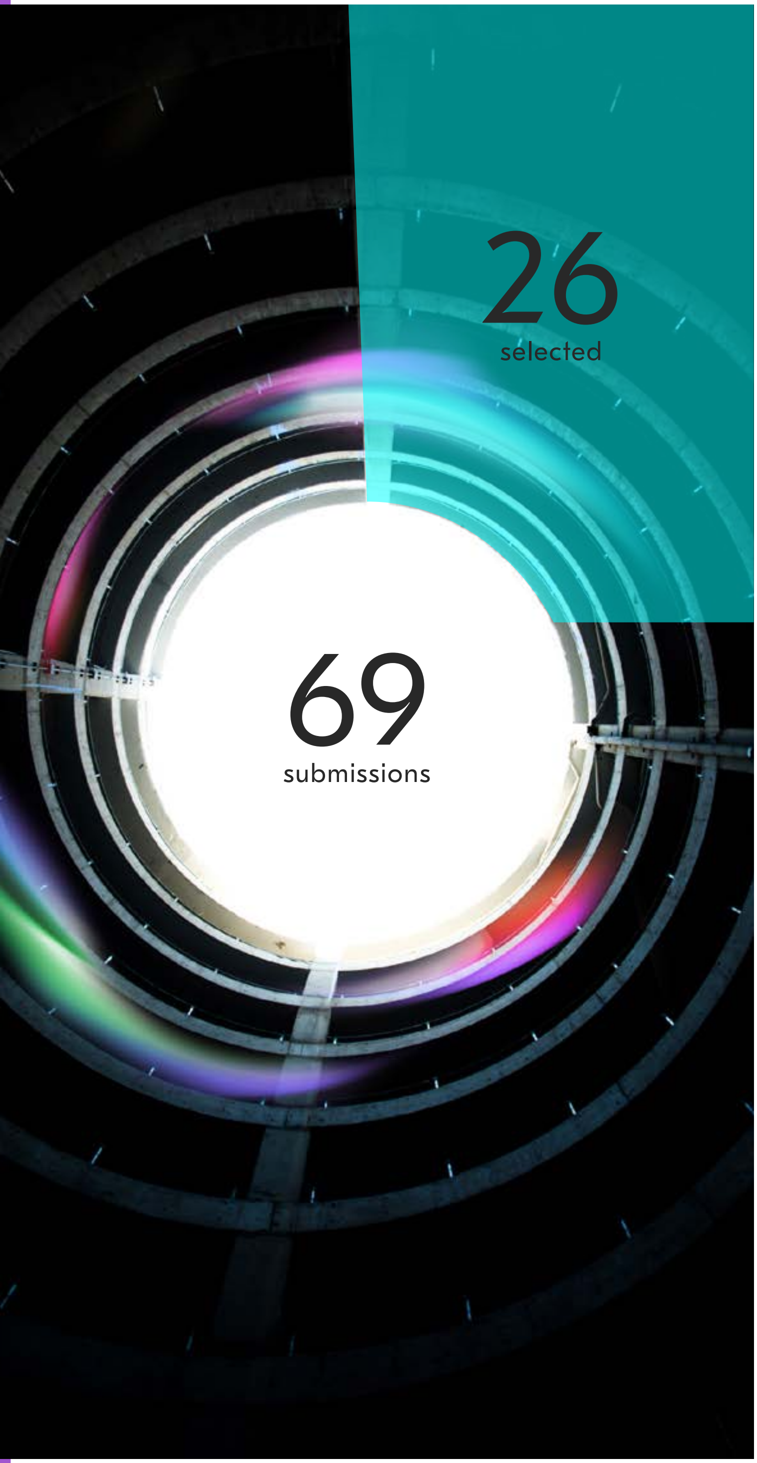
The McEliece system employs the complex Goppa Codes scheme to encrypt data. It is important to note that research is currently underway to introduce another class of codes, called quasi-cyclic moderate density parity-check codes, in order to initiate changes which cryptographers hope will result in a smaller key size. The key size as it currently exists within the MCEliece cryptosystem is very large, a deterrent to efficiency.



Hash functions are defined as functions that are executed to reduce data of arbitrary size to data of a fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. Hashes are already in use in some way shape or form within the cryptography world, for instance, if you are a bitcoin user you have probably encountered the term hash before in relation to transactional data.

In the cryptosystems that employ hash-based signatures, a private key can only be used once because the signature is exposed as a component of the private key. This results in a situation where large swathes of data are created per computation. This is an obvious disadvantage as it requires large swathes of space to store all the data. Among the promising NIST QPC proposals, SPHINCS employs hash-based signatures.

Other noteworthy proposals are Multivariate systems. These are mathematical schemes that depend on the difficulty of solving a system of quadratic polynomial equations over a finite field.



3.3 The Standardization Process

On January 30, 2019, NIST provided its last update on the QPC program. The agency announced that out of the original 69 submissions, only 26 had been selected to move to the next round of intense scholastic and security-focused scrutiny. NIST mathematician Dustin Moody called for industry-wide collaboration to create a robust set of QPC standards.

Moody said:

> *“These 26 algorithms are the ones we are considering for potential standardization, and for the next 12 months we are requesting that the cryptography community focus on analyzing their performance. We want to get better data on how they will perform in the real world.”*

Lastly, NIST emphasized the importance of securing a wide range of devices from the threat of quantum computing. As we covered earlier, a wide array of areas from banking to IoT are in danger of decryption Moody finalized:

> *“We want to look at how these algorithms work not only in big computers and smartphones, but also in devices that have limited processor power. Smart cards, tiny devices for use in the Internet of Things, and individual microchips all need protection too. We want quantum-resistant algorithms that can perform this sort of lightweight cryptography.”*

Dustin Moody | Picture via Twitter

Ring lattice-based cryptography is considered to be the most promising path to QP cryptography, but it has been tested for a shorter amount of time in comparison to its peers. Another favorite among cryptographers and computer scientists is the McEliece cryptosystem in combinations with the battle-tested Goppa Codes.

> *“Ring lattice-based cryptography is considered to be the most promising path to QP cryptography”*

4

QAN: The Quantum-Resistant Blockchain Platform

Silur (Endre Abraham), Co-Founder and Head of Cryptography at QAN, Speaking at Delta Summit in Malta

4.1 QAN choose lattices

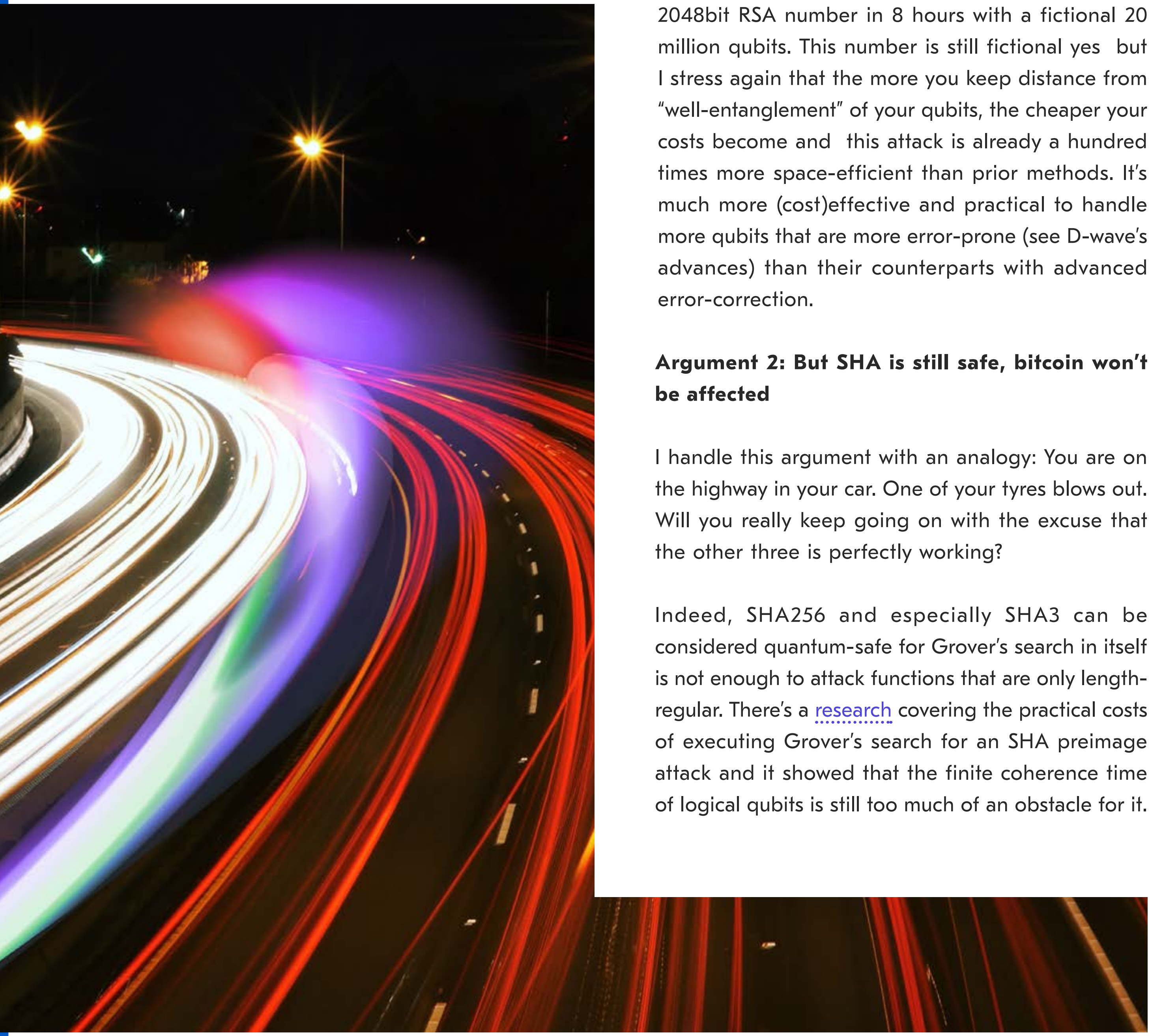
Taken from: https://www.silur.me/posts/The-exotic-world-of-quantum-crypto/

First they are much more efficient on hardware. This is most important in our world of security vs UX wars. One of the reasons why we don't have truly industry-ready (Sorry Trezor, Ledger) hardware wallets with proper key handling is that scalar multiplication (even with montgomery) and especially point inversion on elliptic curves are extremely (energy) inefficient. There are still some improvements on the matter like the AMNF but they still can't compete with the efficiency of LWE or RLWE. In most cases these two primitives can fit into 16 bit memory (a common RLWE base constant is 59393 < 2^16) and they are HIGHLY parallelizable. For example LWE and SIS primitives solely rely on (modular) matrix multiplication and RLWE on polynomial multiplication which is even more parallelizable with the NTT (finite field fast Fourier transform).

Besides being CPU and memory friendly, these methods are the swiss army knifes for the most interesting cryptographic magics of our time like fully homomorphic encryption which allows us to to arbitrary operations on encrypted data (hello GDPR), identity based encryption which I believe could solve one of the biggest obstacle in mass blockchain adoption, Indistinguishably obfuscation which would make companies like Denuvo obsolete for it's the first secure method of software obfuscation.

Another interesting theoretical advantage that made most cryptographers fall in love with Lattice constructions is that finally you can utilize Gaussian sampling in your security "proofs" which is much more friendly in terms of reasoning than uniform distribution. Formally, If you sample a vector from the lattice with discrete Gaussian distribution and re-map it into the fundamental parallelpiped of the lattice it is statistically "crypto-close" to uniform distribution. This is really important in our work since there's not really much surface to grab uniform distribution in itself, it's the ideal model for security but the other edge of this sword that you can't argue about it well. In contrast Gaussian distributions are used in various other areas of academy and there's a lifetime's worth of literature in statistics on them.

4.2 A biased view of quantum computation on blockchains



Argument 1: We need much more qubits to break a practical encryption syste

Indeed there is a minimal bound of qubits to factor a number with Shor's algorithm but Shor's original algorithm relies on highly reliable (error-correcting wise) qubits. There are advances on relaxing the original and very restrictive requirements of Shor and a recent research from google promises to factor a 2048bit RSA number in 8 hours with a fictional 20 million qubits. This number is still fictional yes but I stress again that the more you keep distance from "well-entanglement" of your qubits, the cheaper your costs become and this attack is already a hundred times more space-efficient than prior methods. It's much more (cost)effective and practical to handle more qubits that are more error-prone (see D-wave's advances) than their counterparts with advanced error-correction.

Argument 2: But SHA is still safe, bitcoin won't be affected

I handle this argument with an analogy: You are on the highway in your car. One of your tyres blows out. Will you really keep going on with the excuse that the other three is perfectly working?

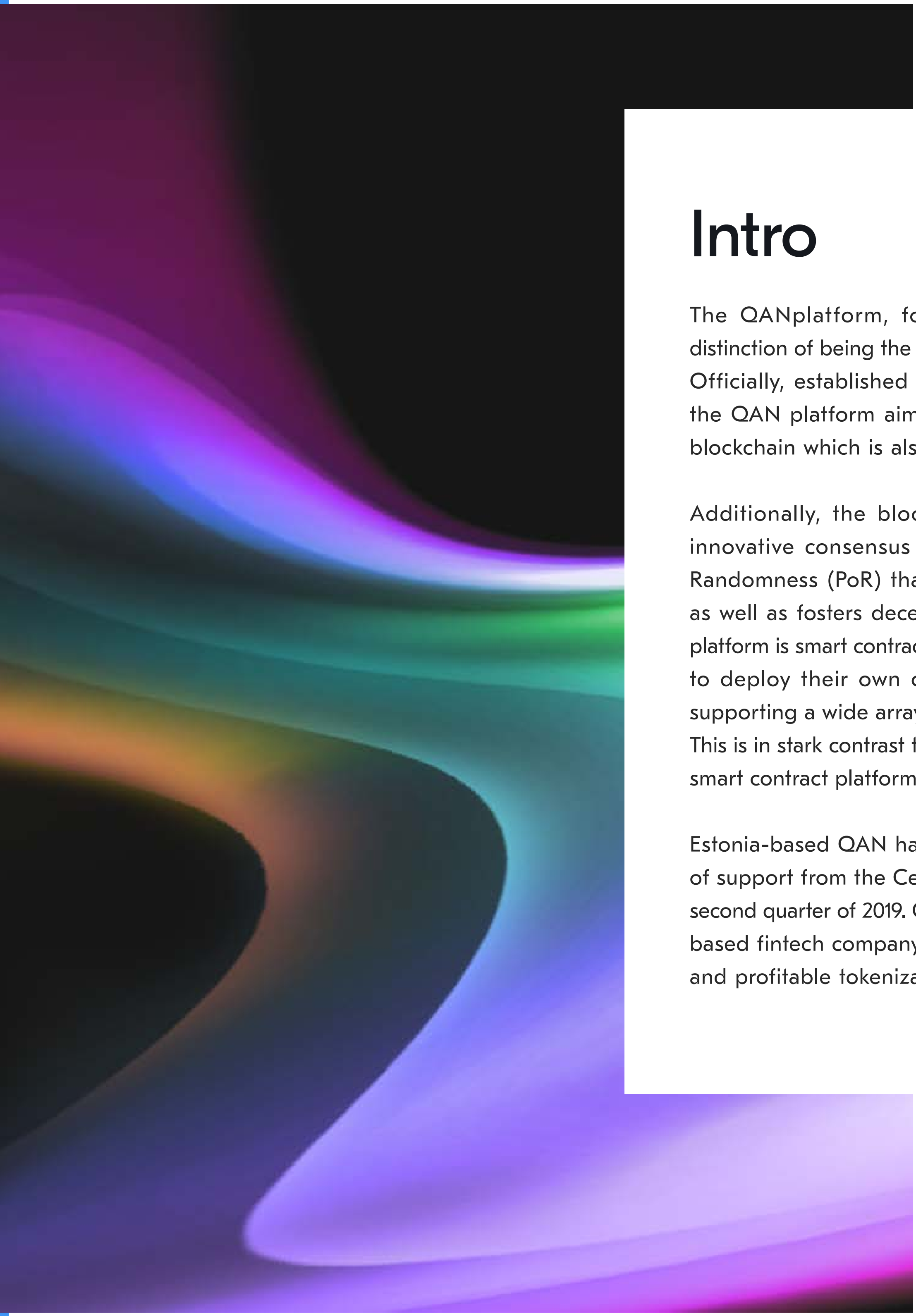
Indeed, SHA256 and especially SHA3 can be considered quantum-safe for Grover's search in itself is not enough to attack functions that are only length-regular. There's a research covering the practical costs of executing Grover's search for an SHA preimage attack and it showed that the finite coherence time of logical qubits is still too much of an obstacle for it.

But it does not mean ANYTHING on Shor's (or rather, it's more practical variants) algorithm security-wise. There are only a small handful of protocols (if any?) where a hashing in itself is capable of holding UC (universal-composability) security where the underlying asymmetric scheme is assumed invertible. For example, in every ECDSA signature, it's basic algebra to recover one's public key from a signature, so the argument that your public key is protected behind a (or double) SHA is irrelevant. Also there are many addresses (as of 2018 June 4, 19% of all Bitcoin addresses holding 36% of the market cap) linked to public keys on various off-chain channels, most likely in every custodial wallet.

Also it's still ongoing research to find the exact bounds of a quantum-circuit implementation (not Preimage-search) of SHA and whether the inherent reversibility of quantum-computations means anything on the matter. (Note there are known bounds for SOME kinds of quantum-circuits regarding SHA but no general results).

5

Introducing the QAN blockchain platform



Intro

The QANplatform, founded in 2018, holds the distinction of being the first quantum-safe blockchain. Officially, established in the third quarter of 2019, the QAN platform aims to be a quantum-resistant blockchain which is also energy efficient.

Additionally, the blockchain is based on a new innovative consensus mechanism called Proof of Randomness (PoR) that supports increased speed as well as fosters decentralization. Lastly, the QAN platform is smart contract friendly, allowing developers to deploy their own customizable contacts while supporting a wide array of programming languages. This is in stark contrast to Ethereum, the most popular smart contract platform, which only supports Solidity.

Estonia-based QAN has been on the receiving end of support from the Centrum Circle group since the second quarter of 2019. Centrum Circle is a blockchain-based fintech company which focuses on disruptive and profitable tokenizable projects.

There are five main actors in the QAN ecosystem. These are the:

- generic smart contract developers,
- the specific smart contract developers,
- the validators,
- the full-node provider, and
- finally the smart contract user (transactor).

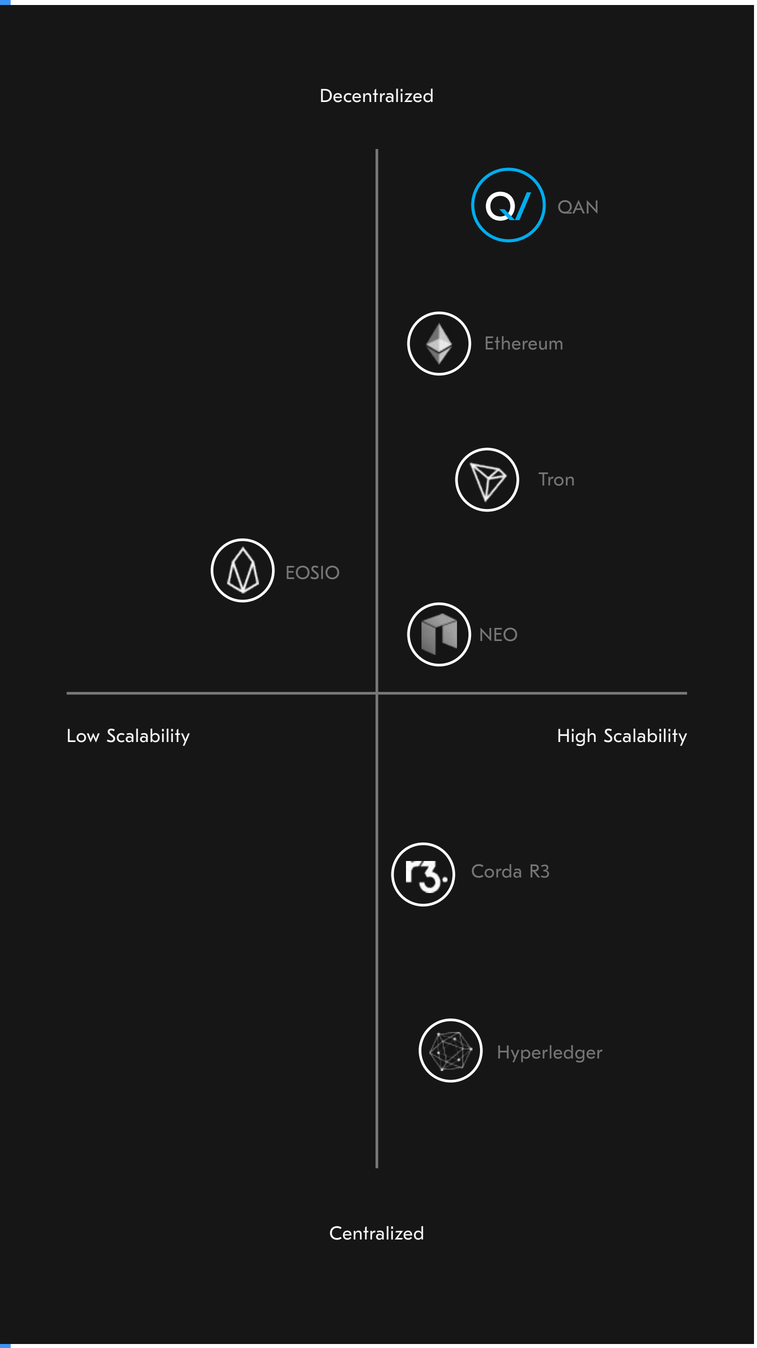
The daily functioning of the decentralized QAN platform is majorly dependent on the Node Operators and the Randomly-selected Block Validators who are both incentivized to participate due to the monetary reward they stand to gain.

The QAN platforms' native digital asset is the **QARK Token.** It is initially being launched as an ERC20 token for the purposes of the IEO after which it will be ported over to the QAN platform.
The total number of tokens is 333,333,000 QARKs. Two-thirds will be floated for sale on the BitBay hosted IEO.

The website was launched at the end of September 2019, simultaneously scheduled with the launch of the demo. The project will launch its IEO in October 2019 after which the QAN mainnet is set to be launched in Q2 2020.

Once the mainnet is launched, the QAN platform aims to support enterprises looking for blockchains that can operate a high-speed private chain. The network hopes to achieve 97,000 TPS for the private chains. The private chains will be secured cryptographically on the publicly operated QAN ledger. The root hashes of transactions executed on the private chain are reflected on the QAN blockchain whose TPS is currently at the 1,600 mark. Thus, theoretically, the maximum TPS which the QAN blockchain can achieve is 97,000 TPS x 1,600 TPS = 155,200,000 TPS.

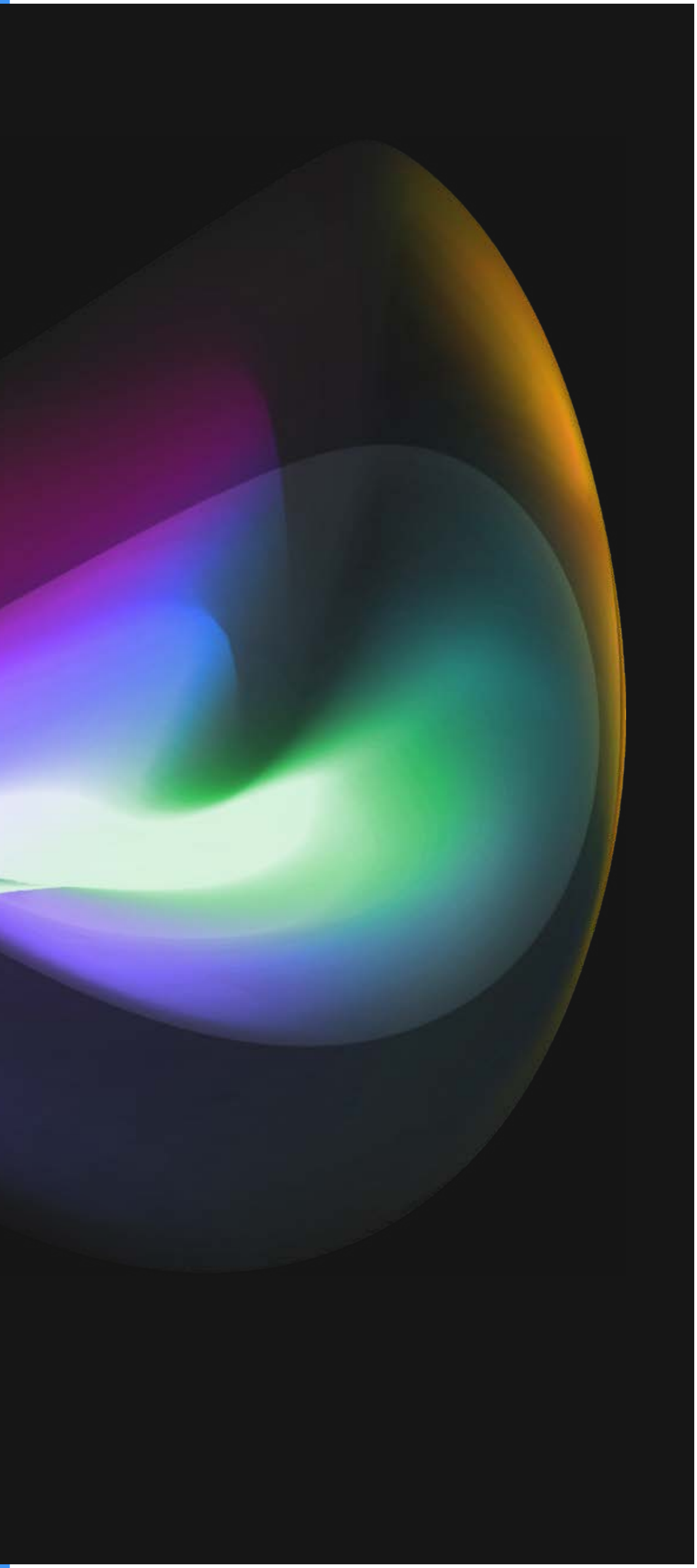
5.1 How Does QAN Measure Up Against Existing Platforms



The cryptocurrency industry is coming to terms with its own limitations. Across the board we see blockchains struggling to keep up with the ever-increasing demands of a growing user base. Bitcoin, for instance, is facing significant scalability challenges and its community cannot seem to agree on a suitable solution. Ethereum, the second most valuable blockchain and world's first smart contract decentralized platform, has been working on updating its consensus mechanism for years now with all hints pointing to a complete update in a relatively long time.

Thus, it is becoming increasingly apparent that the industry must either reform from the ground up or adopt new innovations that are able to effectively support the needs of users while taking stock of security and efficacy considerations both present and future.

QAN represents the best of both worlds. To begin with, it is quantum-resistant due to its use of lattice-based Proof of Randomness. As explored within this paper, this is a significant step in the right direction, providing QAN users with peace of mind as quantum computing emerges as a real threat to privacy and security.



QAN developers explain:

"The quantum-security developed by us is based on the calculations of 13 scientists who have been developing it and working on it for years. QAN is the very first and only platform in the world that succeeded in programming these calculations."*

Moreover, the PoR consensus mechanism is more scalable, energy-efficient and fair in comparison to other popular consensus algorithms. QAN is based on a Proof of Randomness (POR) consensus mechanism, with verifiable pseudorandomness. It is a new development that is basically a generalization of Algorand's algorithm, with added scalability. Due to its consensus mechanism, it allows higher TPS than current blockchain infrastructures, allowing it to achieve impressive transaction speeds.

*You can read about the calculations here:

https://eprint.iacr.org/2007/432.pdf
https://doi.org/10.1145%2F237814.237838
https://eprint.iacr.org/2011/501.pdf
https://eprint.iacr.org/2017/766.pdf

QAN

BLOCKCHAIN PLATFORM

follow us

powered by

centrum
circle