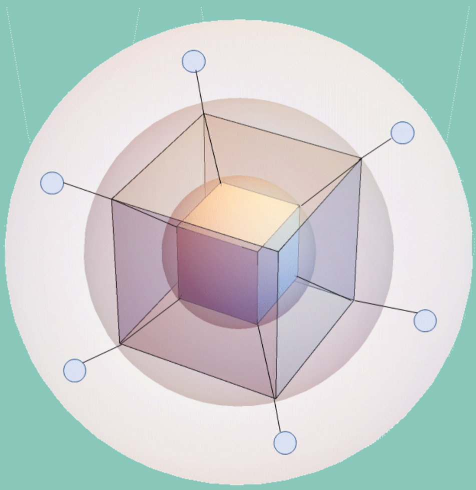
The QSB



Quantum Secured Blockchain

A Whitepaper
by

Marta Misiaszek-Schreyner, Łukasz Kujawski,
Miriam Kosik, Piotr Kulicki, Mirek Sopek,
and others

QUANTUM BLOCKCHAINS

Contents

Executive Summary

In this whitepaper, we introduce Quantum Secured Blockchain (QSB), which was invented, developed, and is currently being implemented by Quantum Blockchains Inc. The aim of Quantum Secured Blockchain is to establish a blockchain that can withstand anticipated attacks from cryptographically relevant quantum computers.

QSB has been designed as a system that enhances the cryptographic foundations of blockchains by incorporating three fundamental components of modern quantum-resistant technologies: Quantum Cryptography, exemplified by QKD technology (Quantum Key Distribution) for securing communication between blockchain nodes; Post-Quantum Cryptography (PQC) for generating private and public keys, as well as digital signatures; and Quantum Random Number Generators (QRNG) for producing unbiased and unpredictable randomness (entropy) within the blockchain.

After successfully conducting initial tests using QKD for a simple model blockchain implemented as a Node.js system, Quantum Blockchains company decided in mid-2022 to adopt Substrate as the foundational framework for building QSB. This decision was driven by practical considerations and is not fundamental in nature. Given the availability of resources, Quantum Blockchains can construct a quantum blockchain, with varying levels of difficulty, on top of many existing blockchains.

Upon completion, QSB will represent the first blockchain that capitalizes on state-of-the-art scientific and technological developments in quantum information technologies and post-quantum cryptography. This innovative approach will enable the creation of a provably secure blockchain network resistant to various forms of attacks. Furthermore, it will implement cutting-edge post-quantum cryptographic methods to generate a new, more secure class of private and public keys, while maximizing entropy through the utilization of inherently unpredictable quantum processes.

The invention of the pQKD, a QKD emulator, has been a critical breakthrough that has enabled the implementation of Quantum Secured Blockchain systems in the present day, without the need for a fully developed quantum communication network. By effectively mitigating the challenges associated with setting up QKD networks, the QKD emulator provides post-quantum level security. This innovation allows blockchains that rely on quantum cryptography for security to transition seamlessly from the emulator to real QKD devices, without any alterations to the code. The QKD emulator has thus accelerated the deployment and adoption of quantum-resistant blockchains and demonstrated the potential of integrating quantum cryptography in contemporary systems.

In its current form, QSB can then be utilized in a conventional manner, just like any other blockchain built using Substrate, such as Polkadot parachains.

Following a detailed exposition of QSB's fundamental concepts and pertinent implementation details, we conclude our paper with a vision of the future of quantum blockchains. In this future landscape, we anticipate an increasingly significant role of fundamental quantum technology in shaping key aspects of blockchain systems, notably consensus protocols. Our company's ongoing scientific research endeavors to explore the potential of quantum information science for blockchains in general and QSB in particular, thereby pushing the boundaries of what is possible in this burgeoning field.

A Brief History of Quantum Secured Blockchain Development

The development of quantum blockchains originated from the pure scientific research of three future founders of the company: Dr. Xin Sun, Dr. Mirek Sopek, and Prof. Piotr Kulicki. Between 2019 and 2022, a series of peer-reviewed papers [SSK] laid the theoretical groundwork for the basic architecture, operations, and theoretical use cases of quantum blockchains, such as lotteries, auctions, and voting. Two key features of this research stand out: the strict scientific rigor demonstrated through mathematical proofs of the proposed protocols, and the practical possibility of implementing the proposed systems. The authors did not assume their quantum blockchain would require quantum computers; instead, they focused on the use of secure quantum channels (e.g. QKD links) between blockchain nodes.

By the end of 2021, the company had been established as a European startup headquartered in Poland, and the first practical implementation was developed. This simple model blockchain (called QKDBase) was implemented in Node.js, and the company began evolving it into a system compatible with commercially available QKD devices. Quantum communication technology supplier QNU Labs, a cybersecurity company based in Bengaluru, India, provided these devices. QNU Labs and Quantum Blockchains have been in partnership since the fall of 2021.

A dedicated pair of QNU Labs' Armos QKD systems was made available to Quantum Blockchains developers. To minimize infrastructure costs, the pair was installed in QNU Labs' laboratory in Bangalore, India, with communication facilitated by classically secured proxy servers. Two such servers for the fictional cryptographic couple "Alice" and "Bob" were made available via the ETSI QKD protocol.

After conducting long-term tests with QNU Labs' Armos devices [QNU] (over four months), Quantum Blockchains was able to replace its previous software-simulated quantum channels with real QKD devices operating in the company offices. The company later tested the blockchain's operation on devices made by ID Quantique (Clavis XG QKD system) [IDQ], which were made available remotely by the Poznań Supercomputing and Networking Center (PSNC) – a leader in QKD networks in Central and Eastern Europe.

The second quantum device used was a Quantum Random Number Generator (QRNG), which provided a high-entropy source of randomness. The physical devices were produced by ID Quantique.

To the best of our knowledge, QKDBase was the first model blockchain to utilize both QKD and QRNG for securitization and consensus protocol. Blockchain security was enhanced using Toeplitz Hash MACs and a solution called Toeplitz Group Signature. The QSYAC consensus protocol, inspired by the Iroha blockchain's YAC consensus, was also employed. In test runs, the blockchain operated on four nodes and performed thousands of transactions, generating several thousand cryptographic keys using QNU Labs' Armos QKD devices [QNU] and Clavis XG QKD devices [IDQ] installed at PSNC.
For a detailed report on this initial work, interested readers are referred to the respective communication [QB].

The next phase of development was made possible when Quantum Blockchains received its first seed funding in the second half of 2022. This allowed the company to hire new developers and create an entirely new development model. The company opted to use the respected blockchain development framework, Substrate. As one of the most powerful frameworks for creating future blockchains, Substrate also serves as the technological foundation for the Polkadot system. The details of the implementation on Substrate will be described in the following chapters of this white paper.

Preparing for the Quantum Era

Understanding the implications and navigating the general risks to cryptography

There is a widely accepted belief that the cryptographic foundations of our digital infrastructure are under threat. Quantum computers, which derive their power from the ability to control individual quantum objects, can execute algorithms specifically designed for them, demonstrating significantly higher efficiency than their classical counterparts for traditional computers.

One such algorithm, developed by Peter Shor in 1994 [PS], is capable of performing integer factorization and solving the discrete logarithm problem exponentially faster. Both of these mathematical properties underpin existing asymmetric cryptography, which in turn forms the basis for modern digital signatures and most secure key exchange protocols.

Another algorithm, developed by Lov Grover in 1996, is capable of performing unstructured searches quadratically faster. While Grover's algorithm cannot break symmetric cryptographic protocols or successfully attack hash functions, it can certainly weaken these classes of cryptographic primitives.

Although it is uncertain when exactly Cryptographically Relevant Quantum Computers (CRQCs) will become available, their current capacity (figuratively measured by the number of qubits) and the pace of development leave no doubt that the risk is real. This arises from the fact that the combined time needed for migration and for maintaining secrecy in all realistic measurements exceeds the expected arrival time of CRQCs. This effect, described by Mosca's Theorem [MT], has led to numerous recommendations, and recently, legal regulations and clear directives to replace or amend existing cryptography – both in the United States and the European Union [LR].

In the United States, the most significant legal action to date is the *"Quantum Computing Cybersecurity Preparedness Act"*, enacted by the US Congress as a public law through the well-known bill H.R.7535 [QCC]. In essence, the act requires the phased adoption of post-quantum cryptography.
In the EU, there are also regulations and directives related to the threat, but the most substantial initiative is the EuroQCI (European Quantum Communication Infrastructure) programme [EQ]. Among other things, thanks to this, the EU is in the process of creating a large-scale Quantum Key Distribution network to enable secure cryptographic key exchange across the continent.

Although it is impossible to definitively conclude that the US is focused on post-quantum cryptography while the EU emphasizes quantum cryptography, there is undoubtedly a noticeable difference between the two regions in the Western world.

Risks specific to blockchains

The importance of cryptography for blockchains is paramount. Blockchains could not have been invented nor could they exist without asymmetric cryptography. These are the statements of the obvious. However, with a few notable exceptions, such as TheQRL project [QRL] and the QAN platform [QN], awareness of the imminent risks is limited. According to recent reports by Deloitte, both Bitcoin [DB] and Ethereum [DE] are, to a certain degree, at risk. For Bitcoin, it is estimated that about 4 million BTC (representing approximately 25% of all coins in circulation) are under direct threat due to the use of older forms of addresses (the "p2pk" type). Deloitte states that Ethereum could suffer from both "transit attacks" and "storage attacks," and they estimate that about 60% of all Ether coins are exposed to attack.

While it is generally assumed that symmetric algorithms and hash functions are safe even in the quantum era, the author of the highly professional report *"The Quantum Threat to Blockchain"* [IQT], Dr. Robert Campbell, the senior analyst at Inside Quantum Technology, claims that:

> *"Grover's algorithm, which can dramatically speed up unstructured search, allows generation of a modified pre-image from a given hash, permitting a signed data block to be modified, devastating standardized blockchain cryptography and cybersecurity."*

The predicted weakening of hash functions by Grover's algorithm is by 50%.

Risk mitigation - Quantum resistant cryptography

It is quite a paradoxical fact in the development of cryptography that the two most fundamental methods with the power to mitigate the risks of quantum computers were discovered and largely developed almost a decade before the quantum algorithms for breaking cryptography were invented. These two methods rely on two drastically different approaches to create strong ciphers.

The first method doesn't stray far from the way modern cryptography was developed – it is algorithmic. It relies on the existence of algorithms that are believed to be unbreakable. Such a feature stems from the fact that they are built around special mathematical objects – one-way functions – i.e., functions that are easy to compute in one direction but extremely difficult to reverse. The first known protocol of this kind was the McEliece cryptosystem, introduced by Robert McEliece in 1978. The second one was developed by Harald Niederreiter in 1986.

The second method is revolutionary in its nature – it assumes that it is possible to create a cryptosystem based on certain physical properties of matter at the quantum level. Two fundamental protocols of this type were created by Charles Bennett and Gilles Brassard in 1984 (BB84 protocol) and by Artur Ekert in 1991 (E91 protocol). Both gave rise to what today is known as QKD – Quantum Key Distribution.

These two fields belong to distinct branches of cryptography. Quantum Cryptography emerged from the latter method, while Post-Quantum Cryptography originated from the former.

From this historical paradox, we can plausibly conclude that the genius of Charles Bennett, Gilles Brassard, and Artur Ekert laid the groundwork for security that was shattered much later in the history of cryptology.

Let’s now review both of these fundamental approaches.

Post-Quantum Cryptography (PQC)

The most significant cryptographic attack vector on blockchains by emerging quantum computers involves their ability to break asymmetric cryptography using Shor's algorithm. This attack vector could potentially reveal users' private keys from their public keys. Although the extent of the threat varies depending on the specific blockchain and its exposure to "raw" public keys, there is a general consensus that traditional asymmetric cryptography used on blockchains, such as ECDSA (Elliptic Curve Digital Signature Algorithm), RSA (Rivest, Shamir, and Adleman algorithm based on the multiplication of large prime numbers), DH (Diffie-Hellman) Algorithm (used for key exchange), and DSA (DH used for signatures), should not be employed in modern blockchains.

Ideally, traditional asymmetric cryptographic primitives should be replaced with equivalent quantum cryptography counterparts. However, at the current stage of quantum cryptography development, there are no practical alternatives to such asymmetric algorithms, necessitating the exploration of an area known as Post-Quantum Cryptography (PQC).

PQC encompasses the definition and development of quantum-safe (quantum-resistant) algorithms. There is no precise definition of what characterizes a PQC algorithm, other than its purported inability to be broken by any known methods implemented on a quantum computer.

There are five classes of algorithms classified today as post-quantum: lattice-based, multivariate, hash-based, code-based, and supersingular elliptic curve isogeny algorithms. A detailed explanation of these classes is beyond the scope of this whitepaper. In brief, they are based on various mathematical theories that yield systems much more robust than existing asymmetric cryptosystems based on prime number multiplication or elliptic curves.

For those interested in this topic, it is recommended to familiarize with presentations created by scientists who have significantly contributed to PQC development: Daniel J. Bernstein and Tanja Lange [PQC]. For a basic understanding of the technology, there is also an entertaining introduction called "Post Quantum Crypto for dummies" [PQD].

Currently, the development of new cryptosystems is in the standardization phase by both NIST in the US and ETSI in the EU. In July 2022, NIST published algorithms selected for forthcoming standardization:

- Public-key Encryption and Key-establishment Algorithms: CRYSTALS-KYBER.
- Digital Signature Algorithms: CRYSTALS-DILITHIUM, FALCON, and SPHINCS+.

As outlined in the subsequent sections of the whitepaper, we have chosen to use the CRYSTALS-DILITHIUM Digital Signature Algorithm, specifically the "Dilithium2" version, for QSB development. For implementation on the Substrate blockchain, CRYSTALS-DILITHIUM has been developed in the Rust language.

One issue with post-quantum algorithms is that we cannot definitively prove their security against attacks from quantum computers. This problem is best exemplified by the fact that shortly after NIST announced the fourth and final-round candidate for PQC standards, the SIKE algorithm, it was cracked by two Belgian cryptoanalysts from KU Leuven research university using a conventional Intel Xeon-based computer [PQH].

However, the situation is not entirely bleak. Recently, scientists from Technion University in Haifa, Israel, and Yan Liu from Cornell have identified a "master problem" that guarantees the existence of true one-way functions [OWF], which are essential for the existence of secure asymmetric cryptographic algorithms. The master problem is one of the oldest and most central issues in complexity theory. Known as Kolmogorov complexity, it concerns the difficulty of distinguishing random strings of numbers from strings containing some information. Liu and Pass demonstrated that if a specific version of Kolmogorov complexity is hard to compute in a certain sense, then one-way functions truly exist, and there should be a method to construct them. At this point, things become more challenging – while we now know that such functions exist, this discovery has not yet been transformed into a computationally feasible algorithm. Nevertheless, this research marks significant progress towards secure algorithmic cryptographic algorithms, even though the path to achieving them may be long and arduous.

The aforementioned and still potentially genuine vulnerability of PQC cryptography prompted our decision to adopt a hybrid solution for QSB. In this approach, PQC is complemented by QKD (Quantum Key Distribution) and QRNG (Quantum Random Number Generator) technologies.

Quantum cryptography

Considering the potential vulnerability, it is undoubtedly essential to guarantee blockchain security in the advent of the quantum computing era by upgrading existing blockchain protocols. This can be achieved by incorporating state-of-the-art quantum cryptographic technologies, which cannot be broken and whose security can be proven, into their core. This confidence stems from the fact that only quantum cryptography can deliver ultimate and everlasting security.

To quote Simon Singh, author of "The Code Book":

> *"Quantum cryptography would mark the end of the battle between codemakers and codebreakers, and the codemakers emerge victorious. Quantum cryptography is an unbreakable system of encryption. (…) The claim that quantum cryptography is secure is qualitatively different from all previous claims. Quantum cryptography is not just effectively unbreakable, it is absolutely unbreakable."*

Everlasting security provides protection against computationally unlimited attackers once a protocol with such a feature is implemented. We assert that designing and constructing a blockchain based on quantum cryptography will result in an everlastingly secure blockchain capable of withstanding attacks from future quantum computers.

This statement is derived from the fact that quantum cryptography relies on the quantum properties of matter, rather than specific mathematical algorithms, for its security. Consequently, it provides information-theoretic security, which is more robust than computational security.

However, not all cryptographic primitives crucial for blockchains can be achieved using quantum cryptography as it currently exists. For instance, despite significant research on quantum digital signatures [QDS] and quantum hashing [QHS], these two cannot be easily realized with existing technology. Due to the current state of technology, we can protect two modalities of blockchain data using quantum cryptography: data-in-transit and data-at-rest. To create resilient keys, addresses, and signatures, we need to utilize algorithms from the family of PQC algorithms, as previously described.

Designing a blockchain with secured data-in-transit involves using quantum cryptography in a manner that was pioneered in numerous papers by various authors [QKI] and evolved into practical implementations due to our research that predates the creation of our startup [SSK].

In today's practice, quantum cryptography is implemented through Quantum Key Distribution (QKD) systems, as described below, and Quantum Random Number Generators (QRNGs), which are discussed in the subsequent section.

QKD is the most crucial component of quantum cryptography. It offers several secure communication protocols based on quantum mechanics, distinguishing itself from algorithmic cryptography of any kind, as its security is founded on the physical properties of matter, rather than mathematical characteristics of specific algorithms. Essentially, QKD enables two communicating nodes to create a shared random secret key known only to them, which can then be used for algorithmic encryption and decryption of messages. When encryption and decryption are performed using the One Time Pad (OTP) algorithm, it is possible to prove that the resulting cryptosystem is absolutely unbreakable, providing everlasting security.
This strong statement can be traced back to Claude Shannon and his proof developed during WWII and published in 1949 [SH]. One Time Pad is "information-theoretically secure" and remains secure even against adversaries with infinite computational power. This is because the encrypted message provides not enough information about the original message that could be used in cryptanalysis.

The use of QKD for blockchains was first analyzed from a theoretical perspective. The pioneer of this research was Evgeniy Olegovich Kiktenko, who published a paper titled *"Quantum-secured blockchain"* in 2018. Our papers referenced in the respective section of our website [QBW] introduced improvements over the original concept formulated by Kiktenko.

The most significant findings from this development history are that QKD can indeed protect network traffic in a blockchain system and offers an unbreakable communication layer for its network communication. This is achieved through the use of single photons in fiber-optic cables under proven protocols such as BB84 [BB] or E91 [AK]. The security of these protocols relies on the physical properties of single photons. Any attempt to intercept a photon's state irreversibly changes its quantum state, allowing for the detection of such attempts and the subsequent termination or restart of communication.

QRNGs are utilized by QKD to generate random secret keys and also facilitate the creation of high-entropy streams of random data, which are essential for numerous blockchain operations.

As QKD networks, which are ultimately intended to enable the creation of the Quantum Internet, are currently in their infancy, it is unrealistic to assume that globally distributed QKD-enhanced blockchains can replace existing blockchains in the near future. The challenge lies not only in the technological immaturity of QKD networks, but also in a fundamental problem: to guarantee the absolute security, we cannot have something akin to a "router" that would allow the construction of a global Quantum Internet from existing QKD links, similar to how the current Internet has been built from copper wires, fiber-optic cables, or radio waves. The same rules of physics that ensure the unbreakable nature of quantum cryptography protocols prohibit the creation of a router. Fortunately, the situation will change when "free-space" QKD becomes available, realized by satellite-based communication, and when research on processes that use entanglement to create a quantum analogue for classical routing matures.

What is possible and technically feasible today is the creation of a QKD-based quantum blockchain in a specific locality or geography, where it is possible to connect a certain number of blockchain nodes with QKD links – perhaps employing a solution based on "trusted nodes," where keys from one fiber link are transmitted to another. Assuming that the trusted nodes are not accessible by an attacker, we can maintain the security of data-in-transit between nodes.

Another possibility is the implementation of what we call the "Quantum Cryptography Migration System", invented by our company, which is compatible with QKD at the protocol level, does not require dedicated fiber-optic channels, and offers security no lesser than the best Post-Quantum Cryptography (PQC). We will describe this system in a separate chapter.

Why building Quantum Secured blockchain with QKD is difficult?

The design of any Blockchain assumes peer-to-peer connectivity (with exception to systems using DAG – Directed Acyclic Graphs). In a network of N nodes, full peer-to-peer connectivity requires N*(N-1)/2 links (full mesh network). In other words, the number of QKD links would scale quadratically with the number of nodes. With the current high cost to setup QKD links, it would be technically and economically infeasible to design such a network.

What we propose in the subsequent sections of this paper is the quantum secured blockchain with standard classical networks in a peer-to-peer mode, and QKD network created using specific network topologies, that reduce the number of required QKD links. Various such network topologies were popular in the early days of parallel computing, and they allow for much better scalability than “full mesh” – characteristic of peer-to-peer networks.

Deep analysis of various topologies [MK] finally led us to consider a hypercube topology. The hypercube network topology, also known as a binary n-cube or n-dimensional cube, is an interconnection topology invented for parallel and distributed computing systems. It is particularly useful for organizing a large number of nodes in a distributed system due to its regular structure and low diameter (i.e. the maximum number of "hops" or edges that must be traversed to travel between any two nodes in the network). See references [HC] for more information. Figure 1 illustrates hypercubes of dimension 1 to 5, which can serve as network topologies for 2,4,8,16 and 32 nodes.

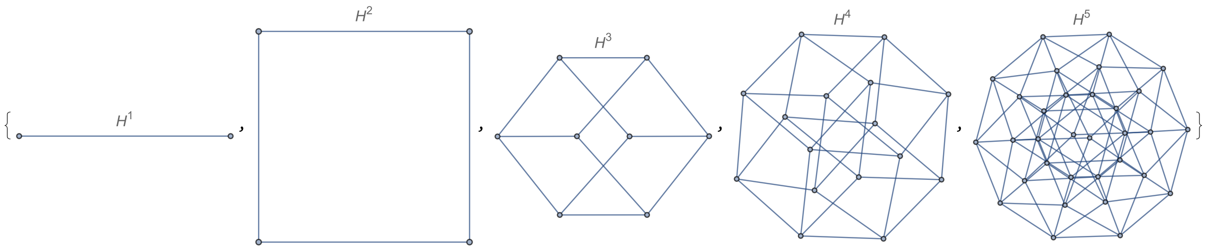


Figure 1. *Hypercubes of dimension 1 to 5.*

Adoption of hypercube topology for blockchains requires modification of the underlying key-exchange protocols so that they need lower number of QKD links than in the “full mesh” network topology. Essentially, it means that not every pair of nodes is directly connected by a QKD link, thus, for its secured communication and consensus protocol we must use some special mechanisms for the transmission of keys which we will describe in the following sections of this paper.

However, due to the current QKD technology limits, such mechanisms alone would not permit quantum blockchains to be deployed globally today. To make it possible for the period of time from now to the full availability of QKD networks, we have proposed the aforementioned "Quantum

Cryptography Migration System" based on QKD emulators. We will describe them in the subsequent chapters.

Quantum randomness

Cryptography focuses on confidentiality, integrity, and authentication, necessitating unpredictable and highly random cipher keys. Although cryptographic algorithms are public, the strength of their application depends on the keys. Cryptanalysis of encrypted ciphers may significantly contribute to revealing the cipher key. Thus, to ensure the high security of applications, improving the randomness of keys is crucial when developing any cryptography dependent systems.

Quantum technologies play a leading role in advancing randomness generation technology. Unlike the pseudo-randomness of Pseudo Random Number Generators (PRNGs) or the biased, usually non-uniform, and difficult-to-verify randomness of True Random Number Generators (TRNGs), they can provide true randomness. There is a fundamental difference between the randomness offered by quantum technologies and that of any classical technology. Classically generated randomness is founded on the stochasticity and indeterminacy based on our lack of full knowledge about the underlying physical or algorithmic processes. Consequently, it is always theoretically possible to create a device that would enable an attacker to acquire such knowledge and discover, replicate, or simulate these processes. However, such an attack is absolutely impossible if measurements of single quantum objects serve as a source of true randomness.

Quantum Random Number Generators (QRNGs) exploit this property by utilizing quantum processes that involve the measurement of single quantum objects. Since these processes are governed by the inherently unpredictable nature of quantum mechanics, the resulting random numbers can be considered truly random and independent of any prior events or knowledge. Moreover, there is a fundamental impossibility to perform an attack on such a system because any attack is, in fact, also a measurement, which destroys the possibility of repeating it.

Various approaches exist for constructing QRNGs, such as the radioactive decay of atoms, photon polarization, electron tunneling, and heterodyne detection, to generate random numbers. The principles of the design of our own QRNG are presented in one of the subsequent sections.

Role of randomness in Blockchains

Blockchains require a high level of randomness for various reasons, all of which are related to security, fairness, and decentralization. For instance, in traditional blockchains with Proof-of-Work (PoW) -based consensus mechanisms, randomness ensures that no single miner can consistently dominate the process. In Proof-of-Stake (PoS) mechanisms, validators are chosen randomly to create new blocks and validate transactions, reducing the risk of centralization and manipulation.

Many smart contracts and decentralized applications (DApps) running on blockchains require a reliable source of randomness for their functionality. For example, decentralized lotteries, gambling platforms, and DApps often necessitate random number generation to ensure absolutely fair and unpredictable results. However, since blockchain networks are deterministic in nature, generating true randomness is quite challenging. Consequently, many chains use various techniques, such as off-chain oracles [RND], on-chain commit-reveal schemes [CR], or cryptographic accumulators [CA] to generate random numbers.

A particularly important solution for providing randomness in blockchains is the Verifiable Random Function (VRF) [VRF]. VRF is a cryptographic primitive that generates a unique random value for a given input, along with a proof that the value was generated correctly. As a result, it is used today in PoS-based consensus protocols, randomness beacons (sources of public randomness on blockchains), decentralized identity systems, and secure multi-party computations, to name a few.

There are significant benefits to combining VRFs and QRNGs, all of which are related to the certainty that the generated randomness (sometimes imprecisely called 'entropy') is both unpredictable and verifiable. The general approach involves feeding the VRF with a random seed generated by the QRNG.

In conclusion, QRNG technology plays a crucial role in generating entropy for blockchains. Enabling blockchains to use the truly unpredictable entropy offered by QRNGs is a reasonable goal for future secure blockchains.

State of the Art of Quantum Resistant Blockchains – studies, analyses, and implementations

Studies and Analyses

Despite progress in quantum cryptography and post-quantum cryptography, the number of realistic solutions designed to protect blockchains from the risk of being compromised in the quantum computing era is unsatisfactory. A 2020 review [BR] lists just a few realistic blockchains based on quantum resistant PQC algorithms. A 2021 paper [BRQ] proposes a PQC-based mechanism for securitizing the Ethereum Blockchain but falls short in referring to existing realistic solutions.

We have already referred to July 2022 report, *"The Quantum Threat to Blockchain: Emerging Business Opportunities"* by Dr. Robert Campbell [IQT] and published by Inside Quantum Technology Research. As was previously noted, the report demonstrates that risks extend beyond the impact of Shor's algorithm on asymmetric cryptographic algorithms.

Many intriguing aspects of Quantum Blockchains have been recently explored in the book *"Quantum and Blockchain for Modern Computing Systems: Vision and Advancements"* by Adarsh Kumar, Ajith Abraham, and Sukhpal Singh Gill [QBB]. However, the majority of the potential systems described therein are not yet feasible for implementation today.

Implementations

The most advanced proposal for constructing a quantum resistant blockchain to date comes from TheQRL [TQR]. TheQRL utilizes Post-Quantum Cryptography on its running mainnet. However, since the post-quantum algorithms employed by TheQRL were not selected by NIST in its latest recommendations, it is difficult to determine if TheQRL has truly created a quantum-resistant ledger, at least from the recommended algorithm perspective.

QAN Platform also makes bold claims about quantum resistance. The company alleges to use post-quantum cryptographic algorithms and a Proof-of-Randomness consensus algorithm. However, as QAN Platform does not openly share its source code, it is hard to evaluate its actual level of security.

A significant effort to address the threats posed by quantum computers to blockchain has been undertaken by the Canadian company BTQ [BTQ], which has offices in Taiwan, Liechtenstein, and Australia. BTQ has developed four categories of solutions to tackle this threat: post-quantum digital signature algorithms, zero-knowledge proof solutions implemented in both software and hardware, and hardware-based post-quantum cryptography processors.

Perhaps the most advanced and significant blockchain, Ethereum, acknowledges the necessity of upgrading its network to guard against the threats posed by quantum cryptography [EPQ]. However, its founder believes that such an upgrade will be required in "a few decades." Contrary to this view, we, along with the cited studies, do not share this level of optimism.

In addition to modified and upgraded blockchains, there is a high-level reference to the indirect application of Quantum Cryptography for Blockchains – a project by JPMorgan, Toshiba, and Ciena [JPT] involving routing a blockchain application over a single quantum-secured optical channel.

There have also been attempts to create quantum-secured blockchains using just one of the three pillars of quantum cryptography, namely QRNG. To learn more about that, check out the Quantum Assets [QA] project.

In conclusion, although there are genuine efforts to develop or modify existing blockchains with Post-Quantum Cryptography, no realistic blockchain based on quantum cryptography could protect itself from imminent threats before our work. It is also debatable whether solutions based only on PQC can provide a sustainable option for the future. PQC algorithms depend on computational security, and while no known quantum algorithms can break PQC algorithms currently, it is uncertain if rapid advancements in quantum algorithms might jeopardize these types of algorithms in the future.

Recognizing these limitations has motivated us to propose a blockchain that utilizes all three pillars of quantum-resistant technology. By integrating Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), and Post-Quantum Cryptography (PQC) within the blockchain framework, we aim to create a more robust and future-proof solution that can withstand the potential threats posed by advancements in quantum computing.

Quantum Secured Blockchain Defined

A Quantum Secured Blockchain (QSB) is a blockchain that employs three fundamental technologies to achieve quantum resistance:

- Quantum Key Distribution (QKD) to protect blockchain network communication,
- Quantum Random Number Generator (QRNG) to provide the highest possible entropy for various randomness requirements on the blockchain,
- Post-Quantum Cryptography (PQC) for signatures, keys, and addresses.

We have incorporated all these technologies to create a QSB using the Substrate based blockchain platform. In the following section, we will examine how these elements are integrated into the architecture of the Quantum Secured Blockchain (QSB).

Use of Substrate framework for QSB development

Substrate [SB] is a sophisticated, modular, adaptable, and expandable blockchain framework, designed for the creation and deployment of customized blockchain systems. Developed by Parity Technologies, Substrate offers a comprehensive suite of tools, libraries, and runtimes that streamline the process of crafting a blockchain solution tailored to specific requirements. Implemented using the Rust programming language, Substrate was employed in the development of the Polkadot network and supports a variety of consensus algorithms, rendering it a versatile option for an extensive array of blockchain projects.

Considering these attributes, we've chosen this platform as the foundation for the first practical Quantum-Secured Blockchain. By leveraging it, we've successfully integrated all three core quantum technologies: Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), and Post-Quantum Cryptography (PQC) into an existing, state-of-the-art blockchain system.

QKD as a Mechanism to Protect data-in-transit on the Blockchain

In general, the idea of using QKD to protect communication on a blockchain seems straightforward: QKD is utilized for distributing encryption keys among blockchain nodes. These keys are then employed to encrypt standard peer-to-peer communication using classical networks. However, as previously noted (see “Why building Quantum Secured blockchain with QKD is difficult?” subsection), QKD networks cannot assume peer-to-peer communication due to fundamental restrictions on point-to-point communication. This necessitates the application of a specific QKD network topology for Quantum Secured Blockchains (QSBs).

It is also possible to use real QKD communication only in the most secure part of the network, which can play a special role in the QSB network. In other parts of the network, the use of QKD emulators is accepted (described in the "Quantum Cryptography Migration System" chapter). While they do not offer absolute security like true QKD, their security level is as high as that of Post-Quantum Cryptography, but they are much less costly and do not require dedicated fiber optic connections.

QSB Network Topology

The QSB topology features a dual-modality design, consisting of both a classical plane and a quantum plane. In the classical plane, the design adheres to a typical peer-to-peer network structure and, within the context of the Substrate framework, utilizes the widely recognized modular network stack, libp2p [LB]. In the quantum plane, a hypercube topology is adopted, which minimizes the number of links required for communication between any two nodes, assuming point-to-point, direct connections that are characteristic of current QKD networks.

While designing the quantum plane, we have made the assumption that within a timeframe of several years starting from 2023, it will not be feasible to construct an entire quantum plane using real QKD devices (or further details, refer to the section "Why Building a Quantum Secured Blockchain with QKD is Difficult?"). Due to this limitation, we have assumed that the most secure portion of the QSB, consisting of 2, 4, or 8 nodes, will utilize real QKD, while all remaining nodes will employ a QKD emulator. This has led to the division of the entire network topology into two parts: the "core" and the "mantle," which are described below.

As a result, the QSB network topology is constructed based on the following principles:

- All blockchain nodes participate in a classical peer-to-peer network based on the existing TCP/IP network. This network is referred to as the classical plane.
- All blockchain nodes have a certain number of QKD connections to other nodes. These connections provide a means for delivering encryption keys to the nodes, which are later used to protect classical peer-to-peer communication. This network is called the quantum plane. The quantum network is organized as a hypercube graph network.
- The entire QSB network is divided into three layers:
  - **Core** – This is the most secure layer of the QSB. On the quantum plane, all connections are made of actual quantum Key Distribution links using fiber optic-based QKD (in the future, these could also be realized with free space links when they become available [EQC]). The number of nodes in the core is always equal to a power of 2. With current limitations, the practical number of nodes in the core is 4, 8, or 16 (hypercubes of dimension 2, 3, or 4).
  - **Mantle** – This is a secure layer of the QSB. From a communication protocol perspective, on the quantum layer, this layer is also protected by QKD; however, it is possible to use QKD emulators on that layer (for example, our pQKD system described in the chapter "Quantum Cryptography Migration System"). The use of QKD emulators in the mantle quantum plane allows for global deployment, provided that every node is equipped with a hardware QKD emulator.
  - **Crust** – This is the outer layer of the QSB, which exists only on the classical plane and does not use QKD or QKD emulators. It provides very restricted API-like access to the QSB and does not participate in transaction processing and consensus. The nodes in the crust are called “Relays” as they do not have copies of the QSB blocks. Depending on the application of QSB crust is optional and is not mandatory for the functioning of QSB.

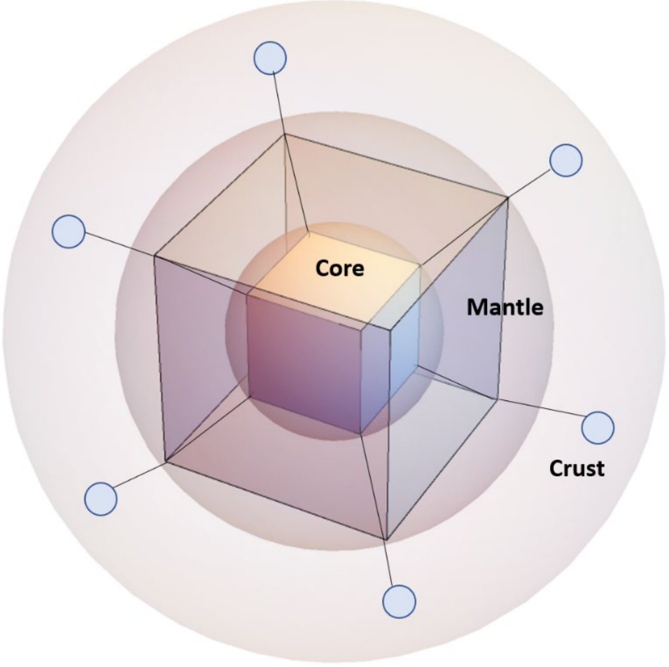


Figure 2. *Visualization of QSB quantum plane topology with 16 validating nodes. In the layer named "Core" QKD is used, in the layer named "Mantle" pQKD (QKD emulators), and in the optional “Crust” layer there are only QSB Blockchain APIs.*

The QSB topology is illustrated in Figure 2. in the subsequent section, we discuss the design of communication between nodes within this topology.

Function of the nodes in QSB layers

Core nodes

The nodes located in the QSB core are the most secure, as they utilize real QKD to protect communication, and must be situated in regions where QKD links are available. Consequently, they can have special privileges in the QSB, depending on the specific use case. For example, it is possible to limit the privilege of being a validator and block creator node exclusively to the nodes in the core. However, such an architecture can be overly centralized, particularly for networks with a small number of nodes (i.e., with hypercube graphs of dimension lower than 4).

It is also possible that nodes in the core can have access to our off-chain Quantum-Gapped Custody subsystem (which will be described in a separate whitepaper in the near future). The nodes in the core also have full access to the archive nodes of the blockchain.

On the contrary, even in scenarios where block creation and validation are permitted for nodes in the mantle, nodes in the core consistently experience a more robust governance model over the QSB. Furthermore, with the tokenization of the QSB, nodes in the core will be entitled to substantial rewards.

Mantle nodes

The nodes in the mantle use QKD emulators (i.e., the pQKD devices described in the "Quantum Cryptography Migration System" section below). As such, they can be installed at any location worldwide with a regular network connection. For higher security, it is recommended that the location has two independent network connections (for out-of-band simulated quantum channel). A single pQKD device can establish multiple links needed to fulfill the requirements of the actual network topology. In most cases, the nodes in the mantle enjoy validator and block creator status, unless these functionalities are restricted to the core.

Mantle nodes can also participate in interoperability communication with other blockchain networks. This can be achieved using modified bridges, similar to those in the Polkadot system. The need for modification arises from the necessity to maintain the security of the QSB without compromising it.

Crust Relays

The “nodes” in the crust are not standard Substrate-compliant nodes. They are custom-made software modules, called “relays”, as they can receive and retransmit data between the mantle and core, and the outer world. They expose only specific Web API methods (analogous to the Polkadot API) and, as such, allow for a subset of restricted actions specific to the QSB use case. In some designs, they can have access to tokens and smart contracts or to mechanisms for their creation. The crust layer is optional – for the most secure blockchains, due to security reasons, it is not even recommended.

Crust relays can also be utilized in interoperability strategies with other blockchains. These strategies can be simpler than those involving mantle nodes, as they don't require pQKD devices. However, this leads to less secure connectivity, which may restrict the scope of interoperable interactions between the QSB and other blockchains.

Guidelines for constructing the QSB topology

To uniquely identify a vertex or point within the hypercube, we can address its nodes using a binary code. In a hypercube in *n* dimensions, each vertex can be represented using *n* bits, where each bit represents the coordinate along one of the *n* dimensions. For example, in a 3D cube each vertex can be represented using three bits, where the first bit represents the x-coordinate, the second bit represents the y-coordinate, and the third bit represents the z-coordinate, as shown in Figure 4 below.

It is crucial that in hypercubes, the addresses of neighboring nodes differ in precisely one bit position. For instance, in a 3D cube, the node "100" has three neighbors: "000," "110," and "101." This characteristic enables the immediate determination of a given node's neighbors based on its address.

An *n*-dimensional hypercube is built recursively from two hypercubes of dimension *n−1,* by linking corresponding vertices. For example, one-dimensional hypercube is just a line segment connecting two points (labeled “0” and “1”). To create a two-dimensional hypercube, another line segment parallel to the first line is taken and connected to analogous endpoints (“0” to “0”, and “1” to “1”).

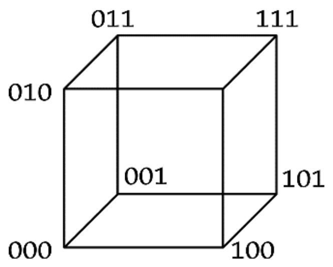


Figure 3. *Node addresses in a three-dimensional hypercube. The addresses of direct neighbours always differ only by one bit.*

Finally, to distinguish the nodes coming from two different lines, the label needs to be extended. It is done through adding a “0” before every node in the first line and “1” before the address of every node in the lower line.
Similarly, to construct a 3D hypercube, two squares are taken and connected to their corresponding vertices. This process can be further expanded to higher dimensions. Figure 5 illustrates the outcome of combining two 3D cubes to create a 4D hypercube.

By applying these rules for constructing hypercube graph network topologies, QKD connections can be established within the Quantum Secured Blockchain.

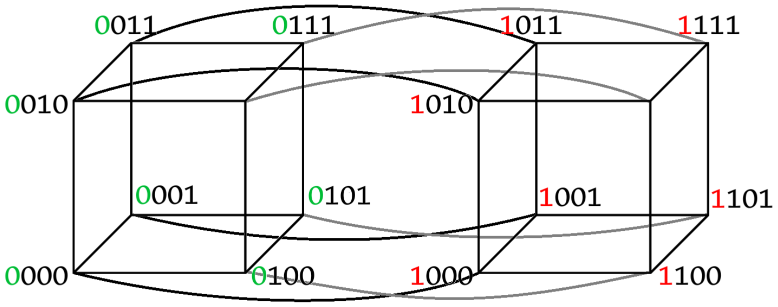


Figure 4. *Combining two cubes to create a 4D hypercube. The green and red numbers extend labels from the 3D cubes to represent the fourth dimension.*

QKD protected communication in QSB

Use of the PSK feature

To ensure the security of communication between nodes within the QSB, we employ two technologies: Quantum Key Distribution (QKD) for symmetric key distribution and key rotation. These symmetric keys are subsequently utilized to encrypt the communication. Despite the difference between the core and the mantle layer, nodes in both layers use exactly the same protocol, i.e., ETSI 014, to obtain the keys.

We have made modifications to the default network client module of Substrate, which interfaces with the libp2p networking stack, to incorporate Pre-Shared Key (PSK) feature. This feature enables the use of 32-byte symmetric keys, known as pre-shared keys, to secure peer-to-peer communication. Prior to node initialization, the PSK must be supplied, loaded, and decrypted. Subsequently, the PSK is loaded into Substrate's memory and promptly deleted. The ongoing updates of the PSK, referred to as key rotations, are managed by a separate Python module called "Runner."

The mechanism of key rotation

Key rotation is a procedure that facilitates the generation and distribution of a PSK symmetric key among all nodes in the network. The QSB network can operate when there are at least two nodes. According to the QBS network architecture of the QSB, the core adopts a hypercube topology, allowing for 2^N nodes. In other parts of the network, such as the mantle, this number is more flexible, as described in the "QSB network topology" section.

For every block received from outside the network (via the off-chain worker module), a new PSK creator is chosen based on a predetermined difficulty and uniform entropy across all nodes. The entropy is determined based on the previous blocks, ensuring consistency throughout the network. In QSB, since the nodes are required to know all other nodes in the network, when exactly one PSK creator is selected for a new block, all nodes send a message to the Runner, requesting a key rotation.

The selected node, referred to as Alice, generates the new PSK using a Quantum Random Number Generator and signs it with her private key. The remaining nodes, referred to as Bobs, query other nodes with whom they have QKD connections, based on the given network topology, to obtain the symmetric key. Subsequently, Alice encrypts the PSK using the symmetric key obtained through QKD. Along with the block number and her signature, Alice sends the encrypted PSK to the Bobs. Upon receiving the key, each Bob decrypts it using the shared symmetric key obtained earlier through QKD, verifies the signature, and stores the new encrypted PSK. Finally, under control of the runner, Alice and Bob restart the QSB node with the new PSK key.

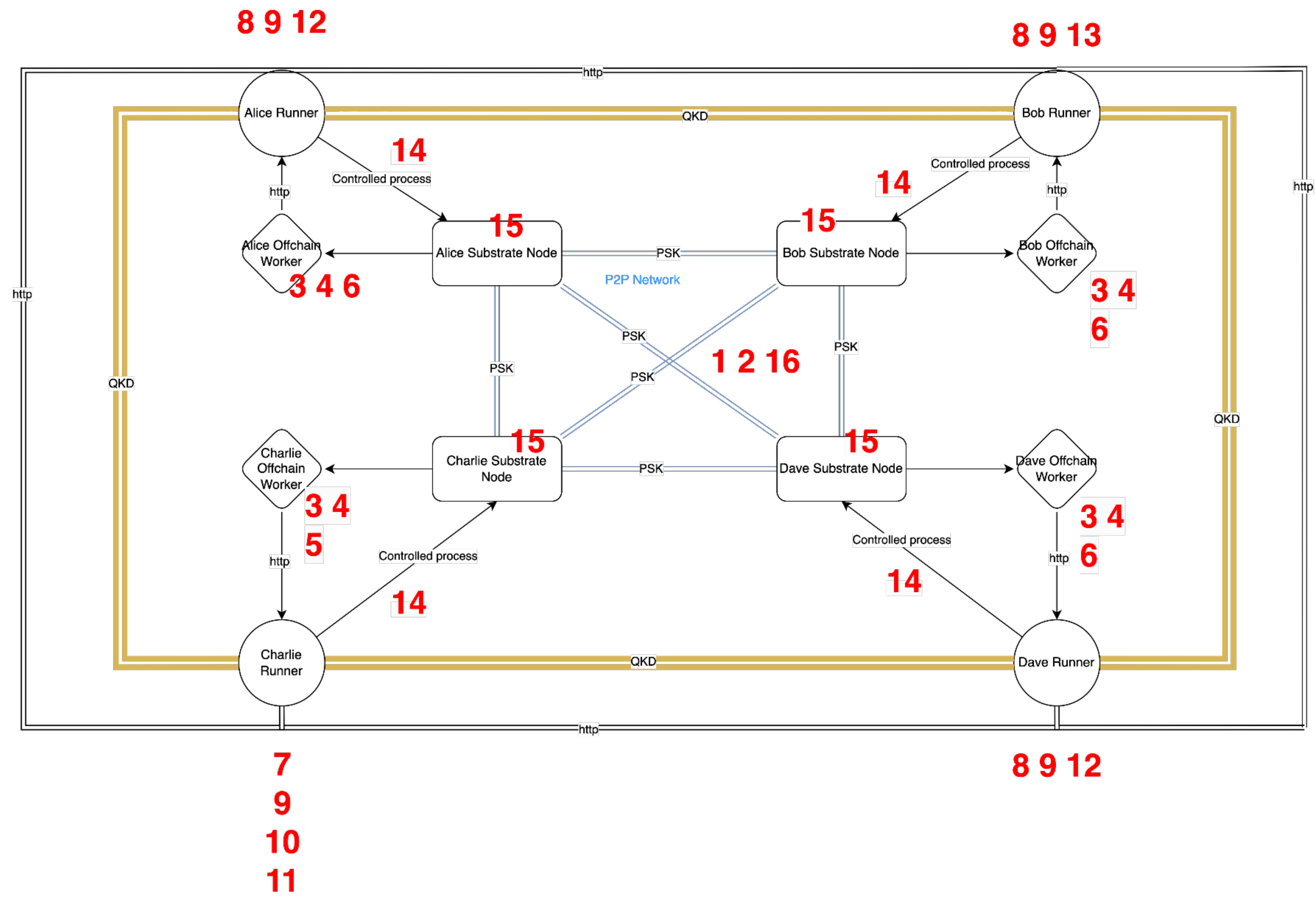


Figure 5. The mechanism of key rotation illustrated for a 2D hypercube network architecture. All labels are defined and elaborated in the text below.

The mechanism of key rotation is illustrated in the above diagram for four nodes in a square topology. The red labels have the following meaning:

1. QSB classical (P2P) network operates on a predefined PSK.
1. When a new block is mined:
2. off-chain workers of all nodes take randomness from the chain, and based on that, check which node is chosen as the new PSK creator.
3. All nodes notice that Charlie is chosen as the new PSK creator.
4. Charlie's off-chain worker sends information to its runner that he is the new PSK creator.
5. The rest of the nodes send information to their runners that Charlie is the new PSK creator.
6. Charlie generates the new PSK from QRNG in its runner, signs it, and saves it.
7. The rest of the nodes ask (through HTTP) the runners which have a QKD connection to get the new PSK.
8. The asked nodes check if they contain the new PSK; if not, they ignore the request.
9. Charlie has the PSK, so he generates a QKD encryption key for Alice and Dave.
10. Charlie encrypts the PSK with the QKD key and sends it to Alice and Dave with the PSK signature and QKD key ID.
11. Alice and Dave fetch the QKD key by key ID they get from Charlie, decrypt the PSK with the QKD key, validate the signature, and save the PSK.

12. Bob calls Alice and Dave's runners for a new PSK again - now they have the PSK, so his request is not ignored; he gets the encrypted PSK, decrypts it with the corresponding QKD keys, validates the signature, and saves the PSK.
13. After some arbitrary time set in the Runner configuration (depending on the network size, this time must be sufficient to spread the new PSK over the entire network), all Runners restart the Substrate node processes.
14. Nodes are restarted with the new PSK, and they immediately remove it as they put it in memory.
15. QSB network operates on the new PSK.

This mechanism allows for the distribution of the new PSK symmetric keys across the network.

QRNG as a source of entropy for QSB

In QSB, quantum entropy is generated by utilizing a Quantum Random Number Generator (QRNG) embedded within the pQKD devices (see the "Quantum Cryptography Migration System" section) present at each node.

The primary purpose of the QRNG is to generate secure PSK-type keys for communication within the QSB, as elaborated in the previous section. Additionally, we incorporated QRNG-generated randomness into a Substrate pallet as an analog of the RANDAO solution, which is well-known in Ethereum networks. Each node possessing an embedded pQKD device participates in the RANDAO campaign for every block. Then, all the numbers are combined, and one random number is generated at runtime. We use this number for the selection of nodes responsible for PSK creation, but it can also be used for various applications in other pallets or smart contracts within the QSB blockchain.

Furthermore, quantum entropy plays a crucial role in the signature algorithm (CRYSTALS-Dilithium).

It also has the potential to contribute to the consensus algorithm. As the QSB is built upon the Substrate framework, its consensus algorithms utilize Verifiable Random Functions (VRF), as introduced in the "Role of Randomness in Blockchains" subsection, particularly in the Proof-of-Stake (PoS) algorithm and its variants. A Verifiable Random Function (VRF) does not rely on a source of randomness to produce its output. Instead, it uses a cryptographic algorithm that generates an output that appears random to anyone who doesn't possess the private key. The algorithm is deterministic: given the same input and the same private key, it will always produce the same output. Because of this, we plan to replace VRF with our RANDAO implementation in the future to utilize QRNG in the QSB consensus model. At the time of writing, the integration of RANDAO into the Substrate consensus has not yet been implemented. This feature is planned for inclusion in the next iteration of the QSB development. Despite this, we are also planning the use of QRNG, particularly form the pQKD local devices as a source of high entropy seed for VRFs.

Post-Quantum Signatures for QSB

Following NIST July 2022 announcement of candidates for post-quantum cryptography standards, we have decided to implement CRYSTALS-Dilithium algorithm as the fundamental digital signature algorithm for Quantum Secured Blockchain.

CRYSTALS-Dilithium is a cutting-edge digital signature algorithm that serves as a crucial component of the CRYSTALS (Cryptographic Suite for Algebraic Lattices) framework. This groundbreaking scheme has been developed by a consortium of esteemed scientists and cryptographers in response to the NIST post-quantum cryptography standardization project. The primary objective of this project is to identify and standardize cryptographic protocols capable of withstanding potential attacks from quantum computing technology.

The foundation of CRYSTALS-Dilithium lies in lattice cryptography, an advanced subdomain of cryptography that leverages the intricate mathematical properties of network structures. Lattice-based cryptography has garnered significant interest owing to its presumed resilience against known quantum threats, such as the potent Shor algorithm, which can compromise widely utilized cryptographic systems like RSA and ECC. Its cryptographic strength stems from the complexity of individual lattice problems, such as Learning-With-Errors (LWE) and Short-Integer-Solutions (SIS), which are believed to be challenging for both classical and quantum computing systems.

The distinguishing attributes of CRYSTALS-Dilithium from other algorithms are:

- Post-quantum protection: Designed with quantum resistance in mind, CRYSTALS-Dilithium is a solid candidate for crypto applications in the post-quantum era.
- Computational Efficiency: Compared to alternative post-quantum digital signature algorithms, Dilithium boasts higher performance, featuring streamlined key and signature dimensions and fast signing and verification processes.
- Use as digital signatures: As a digital signature scheme, Dilithium facilitates message authentication, integrity assurance and non-repudiation. This allows the recipient to confirm the authenticity of the message, confirm the sender's identity, and ensure that the message remains unchanged.

Implementation of CRYSTALS-Dilithium in RUST programming language

The RUST code was ported from the original reference source code [CD] provided by the authors of the algorithm. Our implementation [QCR] leverages almost all of RUST's features, particularly its clean and secure memory management. The code is considerably cleaner and shorter in comparison to the original implementation.

The implementation was verified in two separate ways:

- Cross-verification with the reference implementation – signatures generated by the RUST implementation were successfully verified by the reference C-implementation; signatures generated by the reference implementation were verified by the RUST implementation.
- Self-verification – signatures generated by the RUST implementation were verified by the RUST implementation itself.

The verification was performed using the Monte Carlo methodology for random keys and random messages.

In QSB, we utilize the Dilithium2 variant, which has the following key lengths:

- Public: 1312 bytes,
- Private: 2528 bytes,
- Signature: 2420 bytes.

Use of CRYSTALS-Dilithium in Substrate framework

Within the Substrate ecosystem, elliptic curve-based keys are used by default for account management, signing, and verifying block proposals in PoS consensus.

Given the potential threat posed by quantum computers, it becomes crucial to replace these applications with Post-Quantum Cryptography (PQC). Fortunately, the modular and flexible design of Substrate allows for the replacement of cryptographic schemes, making it feasible to transition to PQC.

Keys Controlling User Accounts in Runtime

To replace the underlying algorithm, a new "Pair" trait implementation was introduced in Substrate, with Dilithium2 keys being designated as the primary algorithm for managing user accounts. Notably, generating new keys from a seed phrase does not require any modifications, as both the elliptic curve-based algorithm Ed25519 and Dilithium2 utilize 32-byte entropy to generate a new key pair. Therefore, BIP-39 mnemonics can still be relied upon in this context. However, it is important to acknowledge that as other variants of Dilithium with longer keys or different PQC algorithms are employed in the future, the need for higher entropy during key generation may arise, potentially necessitating a departure from BIP-39 mnemonics.

Furthermore, there are no hindrances to utilizing PQC with Substrate SS58 encoded format addresses, and Dilithium2 keys are compatible in this aspect.

Keys Controlling Block Proposals in Consensus and GRANDPA Finality

Since QSB is not designed as a trustless blockchain, we made the decision to adopt the Aura consensus mechanism with the GRANDPA finality gadget instead of PoS. However, our proprietary consensus algorithm, described in theoretical papers [SSK], which utilizes secure quantum communication capabilities, is being considered for future implementation.

Aura (Authority Round) is a consensus algorithm employed in some Substrate-based blockchains. It operates as a round-robin-style consensus mechanism in which pre-selected validators take turns creating and validating blocks. While Ed25519 keys can be used for account keys in Substrate, the Aura consensus algorithm typically employs a separate set of keys for block authoring and finality.

In the Aura consensus, validator nodes use two primary types of keys:

- **Block Authoring Keys**: Validators use these keys to sign the blocks they produce during their designated slots. In Substrate, block authoring keys are typically generated using the Schnorrkel (sr25519) cryptographic scheme. Although this scheme differs from Ed25519, it shares certain similarities, such as providing relatively strong classical security guarantees and facilitating efficient signature generation and verification.

- **Finality Keys**: In addition to block authoring, Aura features a finality gadget called GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement), which ensures block finalization. GRANDPA utilizes its own set of keys, known as finality keys or GRANDPA keys, to sign and validate block finality messages. These keys can be generated using the Ed25519 or sr25519 cryptographic schemes.

Integrating PQC for consensus in Substrate requires replacing the existing cryptographic scheme with Dilithium in both the Aura pallet and the Grandpa pallet. In the current stage of development, we have chosen to maintain the original Aura rules. However, our future plans may involve implementing a quantum-secured Aura using our theoretical algorithms or exploring entirely new quantum-enhanced communication methods (refer to the "Future of quantum communication for Blockchains" section).

Quantum Cryptography Migration System

As explained in earlier chapters, the utilization of QKD guarantees unparalleled security for data-in-transit on blockchains. Unfortunately, QKD technology is expensive and constrained by the limitations imposed by the distance of fiber optic cables, and thus, incorporating QKD into a project is a complex task. Nevertheless, ongoing investments in this technology are expected to lead to significant advancements in the near future, thanks to both private and public investments, such as the EU's EuroQCI project [EQ].

To facilitate the development of Quantum Secured Blockchain in the present day, Quantum Blockchains Inc. has introduced a system known as the "Quantum Cryptography Migration System." This system accelerates the progress of quantum cryptography through the utilization of a patent-pending hardware device called pQKD (post-Quantum Key Distribution). The device incorporates several key features, including:

- **Complete compatibility** with ETSI QKD protocols, specifically ETSI 004 and ETSI 0014: Consequently, a pair of devices can be seamlessly replaced by actual QKD devices currently implementing these protocols (which constitutes the majority of devices in production).
- **Versatility in application**: pQKD can be utilized outside of blockchain systems. In such cases, it facilitates secure key exchanges for routers, network encryptors, VPNs, and other security systems, as illustrated in Figure 6.
- **Quantum entropy**: The generation of genuine quantum entropy is achieved through a QRNG chip embedded in the devices. At present, the utilized chip is ID Quantique's "Quantis" QRNG [QR], which is the most compact commercially available quantum entropy chip.

Furthermore, efforts are being made to develop a substantially more advanced QRNG based on our own proprietary design.

While pQKD cannot provide ultimate security comparable to real QKD, it does offer a post-quantum key establishment mechanism (KEM) and an out-of-band communication channel for key exchange.

At the time of writing this paper, both the final design and functional prototypes of the device exist (see Figure 7).

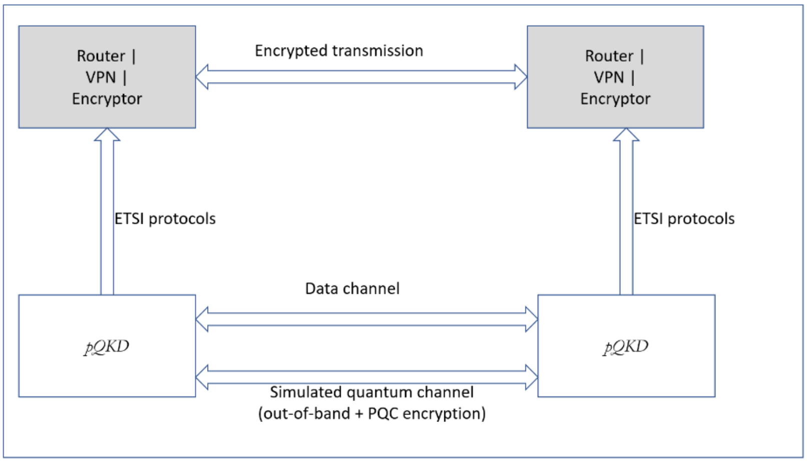


Figure 6. *Utilization of pQKD in the Quantum Cryptography Migration System.*

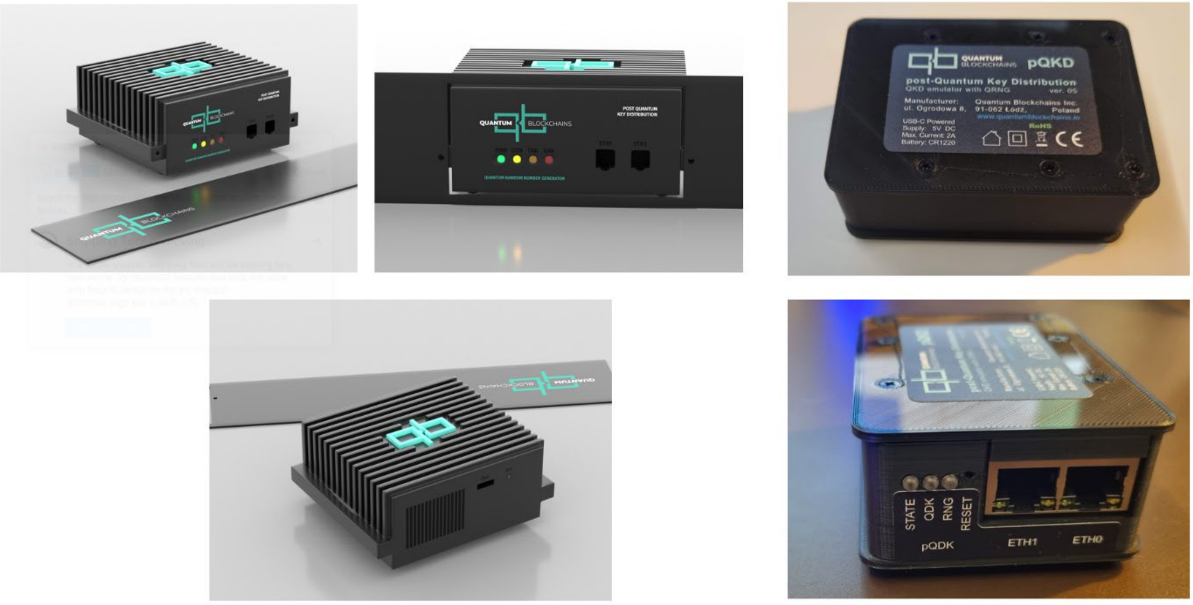


Figure 7. *pQKD devices: design of the final product (left), the functioning prototype (right).*

From a deployment standpoint, each QSB node is equipped with pQKD devices, enabling the establishment of multiple point-to-point links for secure key exchanges, as described in "QKD-protected communication in QSB" section.

The invention of pQKD facilitates the deployment of QKD-compatible communication in the present day, without the need for substantial investments in fiber optics infrastructure.

Future of quantum communication for Blockchains

In the preceding sections, we have presented the implementation of Quantum Secured Blockchain at Quantum Blockchains labs, incorporating quantum-resistant technologies such as QKD, QRNG, and PQC. In this section, we introduce another patent-pending invention that holds the potential to revolutionize future blockchain technologies through the utilization of quantum mechanics.

Time-Bin Quantum Conference Key Agreement for Blockchain Consensus Algorithms

As highlighted in earlier sections, Quantum Key Distribution (QKD) offers significant advantages, such as, i.e. information-theoretic security. However, it also comes with certain limitations, one of which poses a challenge for blockchain technology: the inability to create a quantum-safe network in various shapes, particularly beyond point-to-point connections. This limitation can be considered a substantial drawback.

On the other hand, there is a possibility of multiparty quantum key exchange using the Conference Key Agreement protocol [CKA]. This protocol was experimentally demonstrated in 2021. Unfortunately, due to the specifics of its implementation, the obtained performance of key generation has been insufficient for practical use.

In order to address these limitations, significant modifications were required. As a result, a new variant of the previous protocol emerged, called the time-bin conference key agreement (TB CKA).

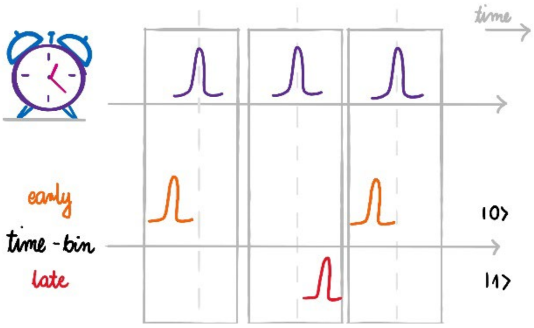


Figure 8. *Scheme of time-bin encoding. Early- and late- time-bin in relation to the external clock.*

The concept behind Time-Bin Conference Key Agreement (TB CKA) is elegantly simple. Similar to CKA, it utilizes GHZ states for key exchange. The key distinction lies in the encoding of the qubit, where instead of the polarization of single photons, it is encoded in time-bins. Such qubits may be simply created by single photons traveling paths of different lengths. As a result, photons' arrival time, compared to external clock, differ, and may be assigned as the early- and late-time-bin, as presented in Figure 6 above.

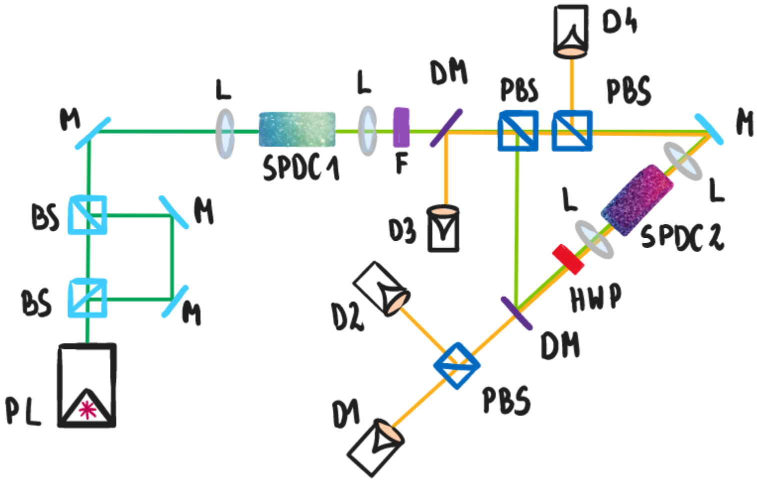


Figure 9. *Proposal of the experimental setup for implementation of time-bin CKA protocol. Symbols: PL – pulsed laser , BS – beamsplitter, M – mirror, L – lens, F – filter, DM – dichroic mirror, PBS –polarization beamsplitter, SPDC1, SPDC2 – nonlinear crystals, D1,D2,D3,D4 – single-photon detectors. Converted photon beams are marked with different color lines.*

Figure 9 presents a proposed experimental setup for implementing the TB CKA protocol in a four-node network [TB CKA], with the nodes designated as detectors (D1, D2, D3, D4). The experimental arrangement can be effectively categorized into two main sections, each fulfilling a specific function. The initial component, symbolized by the dark green beam, is responsible for generating time bins. In contrast, the second component, consisting of the light green and orange beams, engages in a two-stage down-conversion process to establish the entangled state. Consequently, the nodes successfully share a time-bin GHZ state, which can be written as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0_{\leftrightarrow}0_{\updownarrow}0_{\leftrightarrow}0_{\updownarrow}\rangle + |1_{\leftrightarrow}1_{\updownarrow}1_{\leftrightarrow}1_{\updownarrow}\rangle\right) ,$$

where arrows serve as symbolic representations of the polarization of each respective beam. Such photon state shows so-called hyperentanglement, where in correlation between photons various properties (degrees of freedom) are engaged.

Let us also check the kind of photon state that are prepared for detection by respective detectors:

$$\begin{aligned} &\mathrm{D1}: \ |0_{\leftrightarrow}\rangle + |1_{\leftrightarrow}\rangle \ , \\ &\mathrm{D2}: \ |0_{\updownarrow}\rangle + |1_{\updownarrow}\rangle \ , \\ &\mathrm{D3}: \ |0_{\leftrightarrow}\rangle + |1_{\leftrightarrow}\rangle \ , \\ &\mathrm{D4}: \ |0_{\updownarrow}\rangle + |1_{\updownarrow}\rangle \ . \end{aligned}$$

Since single-photon detectors are not usually sensitive to the photon polarization state (they are more sensitive to photon wavelength), it may be concluded that in all detectors the same shared time-bin qubit is measured. Thanks to this it is possible to establish the key simultaneously with all four nodes.

The TB CKA protocol offers an additional benefit as it effectively addresses the challenges encountered in distributed systems, which are outlined by the CAP theorem [CAP] and FLP impossibility [FLP].

The CAP theorem establishes a fundamental principle for distributed systems, stating that it is impossible for any system to simultaneously possess all three of the following properties:

- **Consistency** (C): Ensuring that every read operation receives the most recent write.
- **Availability** (A): Guaranteeing that each request will eventually receive a response.
- **Partition tolerance** (P): Allowing the system to continue operating even in the presence of arbitrary message loss between nodes, caused by communication breakdowns or other factors.

Regrettably, the CAP theorem oversimplifies the delicate balance between the properties it describes. As a result, its formulation is not entirely accurate. The theorem merely states that achieving perfect availability and consistency in the presence of partitions is not possible. Consequently, when designing distributed systems, there is no need to make an absolute choice between consistency and availability when partitions are involved. Instead, the objective is to find a suitable trade-off between these two properties.

The FLP impossibility result, named after its authors Fischer, Lynch, and Patterson, pertains to achieving consensus in distributed systems. It demonstrates that in an asynchronous setting, there is no distributed algorithm that can consistently solve the consensus problem, even if only a single node in the system is faulty.

The implications of both the CAP and FLP theorems give rise to a phenomenon known as the blockchain trilemma. In the realm of classical blockchains, it becomes impossible to simultaneously guarantee security, scalability, and decentralization. Various consensus algorithms in blockchain have attempted to strike a balance among these three features, much like the trade-offs made by designers of conventional distributed systems. One approach to mitigate the negative effects of the trilemma is to prioritize data availability (i.e., scalability) and acknowledge that the data may not be consistent across all nodes simultaneously, but still demand eventual consistency over time during the system's lifespan.

Given the significance of these challenges in the realm of blockchain technology, it is vital to carefully analyze new proposals and explore innovative algorithms. Fortunately, recent research [GHZ] has indicated that leveraging the principles and mechanisms of quantum mechanics can offer valuable insights for mitigating the adverse effects of the blockchain trilemma. In essence, the utilization of GHZ states presents a promising opportunity to achieve consensus within the blockchain network, surpassing the limitations imposed by the FLP and CAP theories. This breakthrough offers a pathway towards a consensus mechanism that defies the conventional constraints, enabling a more robust and reliable blockchain ecosystem.

By employing the TB CKA protocol, every node within a network is provided with a single qubit and proceeds to measure it. If the resulting state is determined to be $|0\rangle$, the node selects "0"; otherwise, it chooses "1". Notably, this act of measurement induces a collapse of the qubit state not solely for the node conducting the measurement, but also for all other participants involved in the communication. This fascinating phenomenon allows consensus to be achieved regarding a single bit of information across multiple nodes.

A protocol designed to achieve consensus over a data block can be outlined as follows:

1. All nodes share two random but identical bits, denoted as b_1 and b_2.
2. Each node calculates the XOR of the two bits: $b_1\ XOR\ \ b_2 = b_3$.
3. All nodes share the value of b_3 with one another.
   a) Nodes that have the same value for b_3(the majority) perform an operation on a data block d_1: $b_1\ XOR\ \ d_1 = d_2$(or $b_2\ XOR\ \ d_1 = d_2$).
   b) Nodes with a different value for b_3 take no action and are temporarily excluded from adding data to the blockchain.
4. Nodes share the value of d_2 with one another, and if it is the same, an agreement is reached on the data block d_1.
5. Steps 1-4 are repeated iteratively.

It is important to note that only the initial step of the protocol requires access to the quantum channel, as the bits $b_1$and b_2 are obtained from the measurement of a shared quantum state. All subsequent steps can be performed using classical communication layers.

The presented consensus method encompasses all the essential properties of distributed consensus:

- **Agreement**: Quantum mechanics ensures agreement, as the measurement of any entangled qubit causes all other qubits to collapse into an identical state.
- **Validity**: Each node proposes either "0" or "1" after performing the measurement, thereby ensuring the validity of the consensus.
- **Wait-free processing**: The entanglement of the qubits allows for the simultaneous collapse of their quantum states, guaranteeing wait-free processing.

It is worth noting that faulty nodes do not hinder the achievement of consensus because the consensus is reached after any measurement performed by any node.

Conclusion and future work

Quantum information technologies offer remarkable opportunities for blockchains. First, quantum cryptography, based on physical properties of matter, and its counterpart, post-quantum cryptography, based on difficult mathematical problems, provide a hybrid mechanism to protect blockchains from attacks by forthcoming quantum computers and AI-aided attackers.

We have demonstrated how key components of Quantum Cryptography, such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG), can be used to protect blockchains by securing data-in-transit between nodes and generating unpredictable, high-entropy randomness. The third pillar of hybrid security, post-quantum cryptography (PQC), was used to replace classical asymmetric cryptography. In these demonstrations, we utilized state-of-the-art solutions: real QKD devices, patent-pending QKD emulators to accelerate quantum cryptography adoption, and the NIST-recommended CRYSTALS-Dilithium post-quantum algorithm implemented in Rust language. All these implementations were conducted using the cutting-edge blockchain framework Substrate to create a functioning demonstrator blockchain.

We have also described our patent-pending invention, which directly employs quantum information processes to propose a novel consensus algorithm based on quantum entanglement, with the potential to overcome fundamental challenges in blockchains and other distributed systems. While the implementation of a Quantum Secured Blockchain has been demonstrated as feasible today, the implementation of this new kind of consensus algorithm will require experimental verification and will become implementable when quantum networks beyond the QKD paradigm become available.

Our near-future work includes perfecting the QSB demonstrator and developing it to the state of testnet by the end of the first quarter of 2024 and mainnet in third quarter of 2024. Since QSB is a permissioned blockchain, these networks will be accessible to operators with QKD devices or those who acquire our QKD emulator. We plan to issue specific utility tokens to facilitate the purchase and use of these devices. The corresponding token economy will also be a part of our future work. In addition to developing QSB as a strictly infrastructural blockchain project, we will be building use cases. For example, we plan to create a prototype of our Quantum-Gapped technology for custody-like system, which could rival existing solutions based on MPC technology. In another use case, we aim to demonstrate how SSI-based (Self-Sovereign Identity) systems can be safeguarded against quantum computer threats.

As for our infrastructural work plan, we intend to explore the possibility of making a networking protocol like libp2p quantum-secure by employing QKD protocols. By doing this, we aim to realize our vision of "quantomizing" a more extensive range of blockchain systems.

Bibliography

[AE] A.K. Ekert, *“Quantum cryptography based on Bell's theorem”*, Physical Review Letters **67**(6), 661-663 (1991).

[BB] C.H. Bennett, G. Brassard, *“Quantum cryptography: Public key distribution and coin tossing”*, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 175-179 (1984).

[BR] T. M. Fernández-Caramès, P. Fraga-Lamas, *"Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks",* in IEEE Access **8**, 21091-21116, (2020).

[BRQ] M. Allende et al., *"Quantum-resistance in blockchain networks"*, arXiv:2106.06640 (2021).

[BTQ] BTQ webpage, https://www.btq.com/ (access: May 13th, 2023)

[CA] D. Derler, C. Hanser, D. Slamanig, *“Revisiting Cryptographic Accumulators, Additional Properties and Relations to Other Primitives”,* In: Topics in Cryptology –- CT-RSA 2015, edited by K. Nyberg, Springer, Cham, Lecture Notes in Computer Science vol. 9048 (2015).

[CAP] S. Gilbert, N.A. Lynch, *“Perspectives on the CAP Theorem”,* Computer **45**(2), 30 (2012).

[CD] Repository containing the official reference implementation of the Dilithium signature scheme: https://github.com/pq-crystals/dilithium (access: May 13th, 2023).

[CKA] F. Grasselli, *“Quantum Cryptography: from Key Distribution to Conference Key Agreement”,* PhD thesis from the Institute for Theoretical Physics III at the Heinrich-Heine-Universität Düsseldorf (2020).

M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, A. Fedrizzi, *“Experimental quantum conference key agreement”*, Science Advances 7, 23 (2021).

[CR] K. Zipfel, *“Exploring Commit-Reveal Schemes on Ethereum”,* Medium (2020), https://medium.com/swlh/exploring-commit-reveal-schemes-on-ethereum-c4ff5a777db8 (access: May 13th, 2023).

[DB] I. Barmes, B. Bosch, *“Quantum computers and the Bitcoin blockchain”*, Delloite, https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html (access: May 13th, 2023).

[DE] I. Barmes, B. Bosch, O. Haalstra, *“Quantum risk to the Ethereum blockchain - a bump in the road or a brick wall?”*, Delloite, https://www2.deloitte.com/nl/nl/pages/risk/articles/quantum-risk-to-the-ethereum-blockchain.html (access: May 13th, 2023).

[EPQ] J. Oliver, C. Williams, “Crypto "Has to Transform Into Something Useful" by 2032: Vitalik Buterin”, Cryptobriefieng, https://cryptobriefing.com/crypto-has-to-transform-into-something-useful-vitalik-buterin/ (access: May 13th, 2023).

[EQ] European Commision webpage, *“The European Quantum Communication Infrastructure (EuroQCI) Initiative”*, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (access: May 13th, 2023).

[EQC] The European Space Agency webpage, *"European quantum communications network takes shape*", https://www.esa.int/Applications/Telecommunications_Integrated_Applications/European_quantum_communications_network_takes_shape (access: May 13th, 2023).

[FLP] M.J. Fischer, N.A. Lynch, M.S. Paterson, *"Impossibility of Distributed Consensus with One Faulty Process"*, Journal of the ACM **32**(2), 374 (1985).

[GHZ] E. D'Hondt, P. Pamamgaden, *"The Computational Power of the W and GHZ states"*, Journal of Quantum Information and Computation **6**(2), 173 (2005).

M. Marcozzi, L. Mostarda, "*Quantum Consensus: an overview"*, arXiv: 2101.04192 (2021).

[HC] G. Ostrouchov, *"Parallel computing on a hypercube: an overview of the architecture and some applications"*, conference paper, 19th Symposium on the Interface of Computer Science and Statistics (1987).

A. Grama, A. Gupta, G. Karypis, V. Kumar, "Introduction to Parallel Computing", ISBN: 0201648652,9780201648652, Pearson (2003).

F. Harary, J.P. Hayes, H.J. Wu, *"A survey of the theory of hypercube graphs"*, Computers & Mathematics with Applications **15**(4), 277-289 (1998).

[IDQ] ID Quantique Clavis XG QKD System: https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/

[IQT] Inside Quantum Technology, "The Quantum Threat to Blockchain: Emerging Business Opportunities", Report IQT-BLOCKCHAIN2022-0722, https://www.insidequantumtechnology.com/product/the-quantum-threat-to-blockchain-emerging-business-opportunities/ (access: May 13th, 2023).

[JPT] M. Pistoia et al., *"Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment in Mission-Critical Environments"*, arXiv:2202.07764 (2022).

[LB] Libp2p - A modular network stack: https://libp2p.io/ (access: May 13th, 2023).

[LR] USA Legal Regulations and advises related to quantum resistance;

December 21, 2022 - The US Congress "Quantum Computing Cybersecurity Preparedness Act", https://www.congress.gov/bill/117th-congress/house-bill/7535/text (access: May 13th, 2023).

National Cybersecurity strategy, Strategic Objective 4.3 therein: "Prepare for the post-quantum future": https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (access: May 13th, 2023).

National Security Memorandum 10 (NSM-10): https://crsreports.congress.gov/product/pdf/IN/IN11921 (access: May 13th, 2023).

[MK] M. Kosik, *"Network Topologies for QKD secured blockchains"*, Quantum Blockchains Inc. internal paper, http://quantumblockchains.io/reports/network-topology.pdf (access: May 13th, 2023).

[MT] M. Mosca, *"Quantum Computer Algorithms"*, PhD thesis from Wolfson College at the University of Oxford (1999).

[OWF] Y. Liu, R. Pass, *"On One-way Functions and Kolmogorov Complexity",* arXiv:2009.11514 (2009).

[PQC] D.J. Bernstein, T. Lange, *"PQCHacks: a gentle introduction to post-quantum cryptography",* presentation slides (2015), https://cr.yp.to/talks/2015.12.27/slides-dan+tanja-20151227-16x9.pdf (access: May 13th, 2023).

D.J. Bernstein, T. Lange, *"Introduction to post-quantum cryptography",* presentation slides (2022), https://hyperelliptic.org/tanja/vortraege/20220825-qsancus.pdf (access: May 13th, 2023).

[PQD] M. Waidner, R. Niederhagen, T. Groetker, P. Reinelt, *"Post-Quantum Crypto for dummies"* Utimaco Special Edition, Wiley (2018).

[PQH] D. Geer, "NIST Post-Quantum Cryptography Candidate Cracked", Communications of ACM, https://cacm.acm.org/news/269080-nist-post-quantum-cryptography-candidate-cracked/fulltext (access: May 13th, 2023).

[PS] P.W. Shor, *"Algorithms for Quantum Computation: Discrete Logarithms and Factoring"*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, IEEE Computer Society Press (1994).

[QA] Quantum Assets webpage, https://www.quantumassets.vg (access: May 13th, 2023).

[QB] M. Sopek, *"Quantum Blockchain's „QKDBase" – the first QKD and QRNG based quantum blockchain model completed"*, Quantum Blockchains Inc. internal report, https://www.quantumblockchains.io/wp-content/uploads/2022/04/QKDBase-report_final.pdf (access: May 13th, 2023).

[QBB] A. Kumar, A. Abraham, S. Singh Gill, *"Quantum and Blockchain for Modern Computing Systems: Vision and Advancements"* Springer, Cham, Lecture Notes on Data Engineering and Communications Technologies vol. 133 (2022).

[QBW] Quantum Blockchains Inc. Foundational papers: https://www.quantumblockchains.io/our-papers/ (access: May 13th, 2023).

[QCC] Official regulations and recommendations;

Quantum Computing Cybersecurity
Preparedness Act: https://www.congress.gov/bill/117th-congress/house-bill/7535/text (access: May 13th, 2023).

NSM-10 act: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (access: May 13th, 2023).

A webinar about the obligations: https://www.protiviti.com/us-en/podcast-transcript/real-date-quantum-computing-apocalypse-and-what-white-house-says-well and the related video: https://www.youtube.com/watch?v=niZ7b0bqvOo (access: May 13th, 2023).

IQT report on Blockchains' security: https://www.prnewswire.com/news-releases/iqt-research-predicts-blockchain-and-quantum-threat-will-quickly-spread-beyond-cybercurrencies-surge-in-new-product-and-services-opportunities-to-come-301593893.html (access: May 13th, 2023).

CitiBank Global Insights: Quantum Computing and Finance (2021): https://www.citivelocity.com/rendition/eppublic/public/documentService/dXNlcl9pZD1mczY0enMxbTIxaz0/ZG9jX2lkPTMwMDUwOTc2JnBsYXRmb3JtSWQ9Nzg (access: May 13th, 2023).

World Bank recommendation: https://www.weforum.org/agenda/2022/09/organizations-protect-quantum-computing-threat-cybersecurity/ (access: May 13th, 2023).

[QCR] Pure RUST implementation of CRYSTALS-Dilithium digital signature scheme: https://github.com/Quantum-Blockchains/dilithium

[QDS] P. Wallden, V. Dunjko, A. Kent, E. Andersson, *"Quantum digital signatures with quantum key distribution components"*, Physical Review A **91,** 042304 (2015).

R.J. Collins at al., "Experimental demonstration of quantum digital signatures over 43 dB channel loss using *differential phase shift quantum key distribution*", Scientific Reports **7**, 3235 (2017).

[QHS] Y.-G. Yang, P. Xu, R. Yang, Y.-H. Zhou, W.-M. Shi, *"Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption",* Scientific Reports **6**, 19788 (2016).

[QKI] E.O. Kiktenko et al., *"Quantum-secured blockchain",* Quantum Science and Technology **3**(3), 035004 (2018).

[QN] QAN platform webpage: https://www.qanplatform.com/en (access: May 13th, 2023).

[QNU] QNu's Armos QKD devices: https://www.qnulabs.com/armos-quantum-key-distribution/

[QR] Quantis QRNG Chips: https://www.idquantique.com/random-number-generation/products/quantis-qrng-chips/ (access: May 13th, 2023).

[QRL] QRL webpage: https://www.theqrl.org/ (access: May 13th, 2023).

[RND] Chainlink docs, *"Introduction to Chainlink VRF",* https://docs.chain.link/vrf/v2/introduction (access: May 13th, 2023).

API3 webpage: https://api3.org/QRNG (access: May 13th, 2023).

[SB] Substrate - an open, flexible, interoperable blockchain framework: https://substrate.io/ (access: May 13th, 2023).

[SS] Substrate, address formats: https://docs.substrate.io/reference/address-formats/ (access: May 13th, 2023).

[SH] C.E. Shannon, "*Communication Theory of Secrecy Systems",* Bell System Technical Journal **28**(4), 656-715 (1949).

[SSK] Papers by Quantum Blockchains founders:

X. Sun, F. He, M. Sopek, M. Guo, *"Schrödinger's Ballot: Quantum Information and the Violation of Arrow's Impossibility Theorem*", Entropy **23**(8), 1083 (2021).

X. Sun, P. Kulicki, M. Sopek,"*Logic Programming with Post-Quantum Cryptographic Primitives for Smart Contract on Quantum-Secured Blockchain"*, Entropy **23**(9), 1120 (2021).

X. Sun, P. Kulicki, M. Sopek," *Lottery and Auction on Quantum Blockchain"*, Entropy **22**(12), 1377 (2020).

X. Sun, M. Sopek, Q. Wang, P. Kulicki," *Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic"*, Entropy **21**(9), 887 (2019).

X. Sun, F. He, D. Qiu, P. Kulicki, M. Sopek, M. Guo, *"Distributed Quantum Vote Based on Quantum Logical Operators, a New Battlefield of the Second Quantum Revolution",* arXiv:2202.00147 (2022).

X. Sun, P. Kulicki, M. Sopek, "*Bit Commitment for Lottery and Auction on Quantum Blockchain",* arXiv: 2004.10312 (2020).

X. Sun, Q. Wang, P. Kulicki, M. Sopek, *"A Simple Voting Protocol on Quantum Blockchain",* International Journal of Theoretical Physics **58,** 275–281 (2019).

[TB CKA] M. Misiaszek-Schreyner, M. Sopek, *"CKA as a tool for blockchain technology"*, Quantum Blockchains' internal paper, https://www.quantumblockchains.io/our-papers/cka-as-a-tool-for-blockchain-technology/ (access: May 13th, 2023).

[VRF] Verified random function, Wikipedia webpage, https://en.wikipedia.org/wiki/Verifiable_random_function (access: May 13th, 2023).