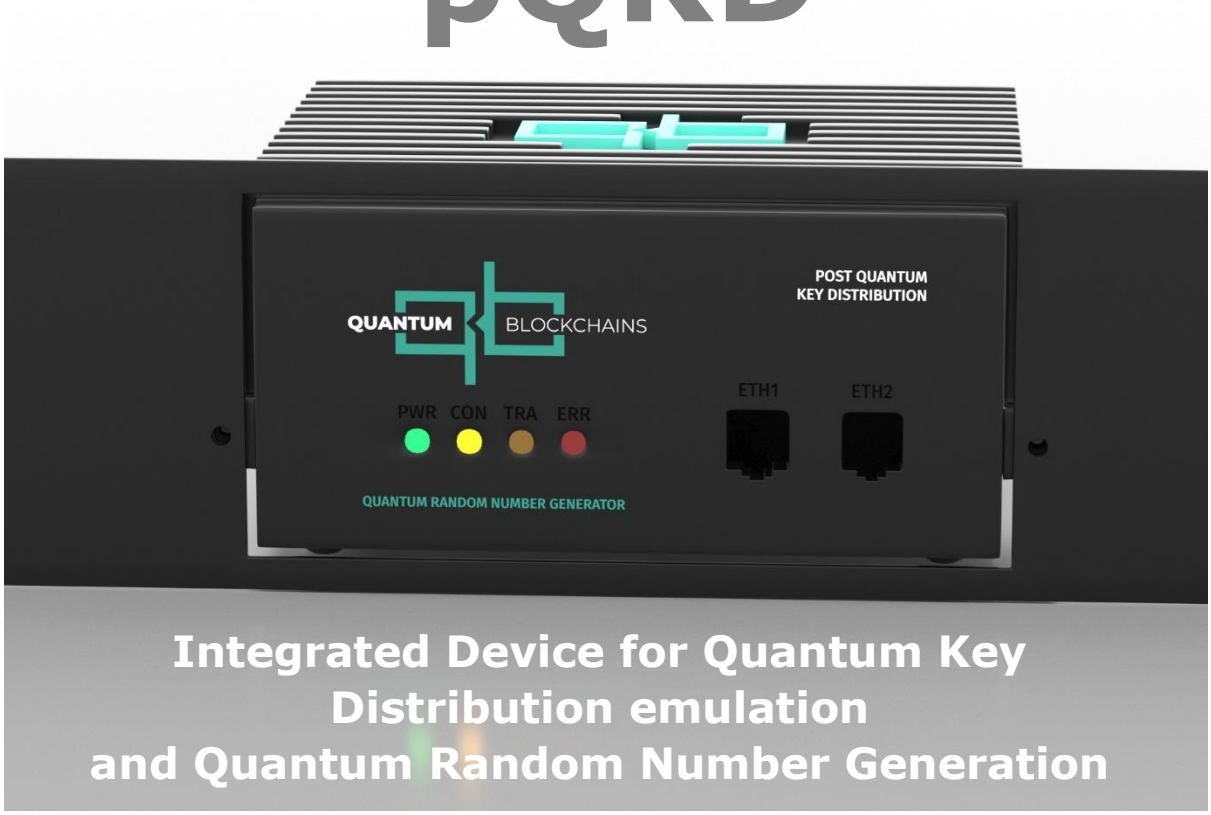
pQKD



pQKD is a groundbreaking cybersecurity product designed by Quantum Blockchains, Inc. Its chief objective is to expedite the transition towards quantum-resistant cryptographic systems. This is accomplished by meticulously simulating QKD protocols in accordance with the global communication standards established for QKD technology by ETSI.

For its operation, pQKD does not rely on dedicated fiber optic links, but rather utilizes **an out-of-band network channel for the distribution of cryptographic keys.** This distribution **is safeguarded by the Kyber key encapsulation mechanism** (KEM), a post-quantum method engineered to withstand cryptanalytic attacks from potent future quantum computers. Kyber is projected to be incorporated into forthcoming NIST standards, ensuring its resilience and reliability in the cybersecurity landscape.

pQKD utilizes **a genuine on-chip Quantum Random Number Generator** (QRNG) supplied by the industry leader, ID Quantique. The QRNG operates independently of the QKD emulation function, serving as a high-grade local source of entropy for any cryptographic application. This integral feature further strengthens the robustness and versatility of the pQKD system in the field of advanced cybersecurity.

pQKD is highly versatile, capable of interfacing with **any network-layer encryption device** that supports key exchange using ETSI QKD protocols. Furthermore, it's compatible with various hardware and software solutions such as VPN applications and appliances. Broadly speaking, pQKD provides secure key exchange for any quantum-resistant systems. While it doesn't assure the physical security provided by true QKD devices, it does guarantee a level of security that is at least on par with that of post-quantum key distribution mechanisms.

pQKD also offers functionality **as a straightforward encryptor** for network communication applications. In this capacity, it employs highly secure, long-key AES algorithms and the provably secure OTP (one-time pad) methods, delivering enhanced protection in a user-friendly package.

Due to a number of innovations incorporated in the device design it is the subject of the company's **patent application titled "A method and a device for encryption key distribution and communication".**

Device specification

Post-Quantum Key Distribution - pQKD
QKD (Quantum Key Distribution) emulator with QRNG (Quantum Random Number Generator)

Minimum setup

Two devices (“Alice” and “Bob” pair).

Physical form

Stand alone casing with rack mounted option
Dimensions (LWH): 90mm * 65mm * 33mm.

Interfaces

2 * LAN RJ-45 ports: Simulated Quantum Channel, Service/Data channel.

Power Supply

Via USB C connector or 19” rack-mounted case connector: 5V, Max Current 2A.

Control elements

Reset button, Shutdown button.

Diagnostic

LEDs: State, QKD active, QRNG active.

Protocols

QKD ETSI – 004, ETSI – 014.
QRNG API (proprietary Rest API) via HTTPS.

Cryptographic algorithms

Post-Quantum KYBER Key Encapsulation mechanism.
AES with key lengths: 128,256,512,1024, 2048
AES modes of operation: : GCM256, CBC256, ECB from 256 to 4096.

Encryptor functionality

OTP (One-Time-Pad) or AES algorithms.

Management interfaces

Comprehensive Web Interface for interactive setup and configuration.
SNMP protocol (with v1,v2 and v3 authentication).

Quantum Random Number Generator

Quantis IDQ6MC1 by ID Quantique.

Availability

Availability:

Fully-functional pre-production (CE certified) versions are presently in the shipping phase. Certification for fully-secured versions is in progress.