Asset tokenisation in the Quantum Age:

Future-proofing gold tokens with post-quantum security

HSBC

Authors:

Prashant Malik,
Technology Strategy and
Partnerships, Digital Assets
and Currencies Technology
Markets & Securities Services
HSBC

Mark Williamson,
Global Head of FX & Commodities
Partnerships & Propositions
Markets & Securities Services
HSBC

Philip Intallura,
Global Head of Quantum
Technologies
Group Innovation
HSBC

Del Rajan,
Quantum Computing
Research Scientist
Group Innovation
HSBC

Duncan Jones,
Head of Cybersecurity
Quantinuum

Ben Merriman,
Solutions Architect
Quantinuum

Kimberley Fewell,
Project Manager
Quantinuum

Executive summary

Asset tokenisation is not just an emerging trend, but a transformative force already reshaping the financial services industry. This application of distributed ledger technology (DLT) allows for the digital representation of assets on a distributed ledger, enabling transactions and the 'carrying' of assets over computer networks.

HSBC has been at the forefront of this revolution, being the first global bank to offer tokenised physical gold to institutional investors using DLT. Further extending this innovative approach, HSBC launched the HSBC Gold Token for retail investors in Hong Kong SAR, providing them with the

Recognising the potential cyber threats posed by the development of powerful quantum computers, HSBC is assessing ways to future-proof its technology systems using quantum-secure technologies. This approach is aimed at protecting the cryptographic systems that underpin asset tokenisation, thereby mitigating the risk of security and integrity compromise of tokenised assets.

In a significant milestone HSBC in collaboration with Quantinuum, a 3rd party integrated quantum company, successfully trialled the first application of quantum-secure technology for distributing tokenised physical gold. This achievement underscores HSBC's FX and commodities businesses commitment to safeguarding critical applications from potential future quantum computing attacks. It also presents a cost-effective approach to protecting existing production DLT in the short and medium term, without the need for re-architecting the DLT.

HSBC has also demonstrated the interoperability of its gold tokens by using post-quantum cryptography (PQC) to move digital assets safely across distributed ledgers, via secure networks. This includes the capability to convert HSBC's gold tokens into ERC-20 fungible tokens, thereby enhancing distribution and interoperability with other DLTs and digital wallets. This approach addresses clients' evolving needs and regulations, further cementing HSBC's position as a leader in the asset tokenisation space.

opportunity to acquire fractional ownership of physical gold. Both these initiatives leverage the technology of the HSBC Orion digital assets platform.

Table of contents

Introduction

The business case for enhancing cybersecurity in financial services and banking is clear. The industry has seen transformative changes with the adoption of distributed ledger technology (DLT), which has improved transparency, efficiency, and security. A key application of DLT is asset tokenisation, where assets like bonds and gold are digitally represented on a distributed ledger, facilitating easier trading and fractional ownership.

The central view of this whitepaper is that tokenisation allows value, in the form of asset tokens, to be 'carried' across computer networks as opposed to data alone. Consequently, the cybersecurity protocols around these assets need to be critically considered from the context of futureproofing. Thus, it is crucial to not only maintain but also continue to enhance the security measures surrounding distributed ledgers, ensuring that they remain resilient against both current and emerging cryptographic threats.

At present, it remains largely unfeasible to break public key cryptosystems like RSA (Rivest–Shamir–Adleman) and ECC (Elliptic-curve cryptography) with a digital computer. However, the unfortunate case for cybersecurity professionals is that the state-of-the-art for technological code breaking continues to advance. A pressing issue is the emerging development of powerful quantum computers. These future large-scale general-purpose quantum computers would be capable of rendering current public key technologies ineffective, thus introducing a critical vulnerability. Despite distributed ledger technology being highly secure, this threat may impact them in the future since some cryptography currently used may be threatened by the advances in quantum computing. The consensus is that the development of cryptanalytically relevant quantum computers (CRQCs) may still be a decade or more away. However, there is an emerging view that it could occur sooner, thus providing compelling reasons to start preparing now [1]. Firstly, modernising the cryptographic infrastructure of a global organisation will take considerable time and effort.

Secondly, there is a risk of "store now, decrypt later" cyberattacks, where encrypted data is collected now with the intention of decrypting it in the future using CRQCs. This is particularly concerning for sensitive financial information, which could be intercepted and stockpiled by malicious actors.

To mitigate these threats, organisations are planning their migration to "quantum-safe" cryptography, also known as post-quantum cryptography (PQC). These algorithms, standardised by the National Institute of Standards and Technology (NIST) [2], are believed to be secure even in the event of a CRQC attack. However, the migration to these standards is a complex task that will span multiple years. Given PQC is only computationally secure, further steps such as cryptographic agility need to be considered.

Whilst DLT and asset tokenisation offer significant benefits, it is crucial to enhance and future-proof the security measures surrounding these technologies. This involves preparing for the advent of CRQCs and migrating to quantum-safe cryptography to ensure the continued resilience of our financial systems against both current and emerging cryptographic threats.

Explainer box: Cryptographic agility and QRNGs

Cryptographic agility is the ability to rapidly and safely change cryptographic algorithms and keys in the case of compromise. This capability will continue to grow in importance.

Alongside the migration to new quantum-resistant algorithms, leading organisations are looking to quantum technology as a new form of defence. One such area involves the generation of the random numbers that underpin encryption keys. Normally these are generated programmatically, using entropy from highly unpredictable sources. Quantum random number generators (QRNGs) provide a new, stronger source of random numbers, which helps ensure cryptographic keys are completely, rather than highly, unpredictable.

In this whitepaper, we explore a first step in that journey for protecting sensitive financial data in a real-world banking application: HSBC's gold tokenisation platform.

HSBC was the first global bank to offer tokenised physical gold to institutional investors using DLT. It also achieved another first with the launch of HSBC Gold Token for retail investors in Hong Kong SAR, allowing them to acquire fractional ownership of physical gold. Both launches use the technology of the HSBC Orion digital assets platform.

In the following sections we will describe the gold tokenisation platform, its underlying distributed ledger, as well as the threats it faces from future CRQCs.

We will proceed to outline the technical approach taken to minimise these risks, and thereby provide first steps towards quantum safety. Our solution will involve deploying PQC algorithms and QRNGs in an effective manner to address part of the problem.

To the best of our knowledge, this is the first application of PQC to gold tokenisation.

This whitepaper is aimed at a non-technical audience. Citations are provided for the more technically curious who wish to explore further.
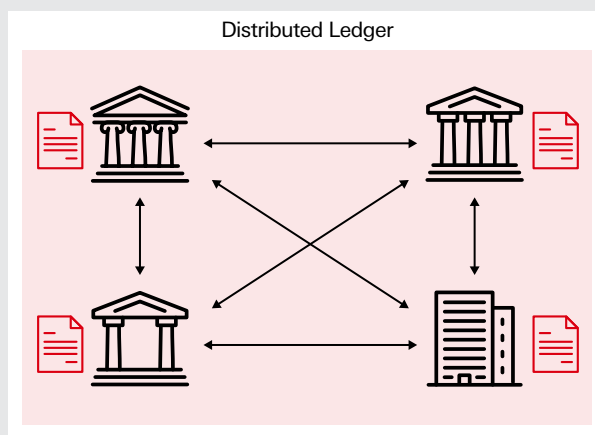
Asset tokenisation

Distributed Ledger Technology
Distributed ledger technology enables the operation and use of distributed ledgers shared across a computer network [3].

In financial services, the technology enables institutions to gain operational and capital efficiency, improve accessibility and liquidity, and decrease costs, while simultaneously providing a secure and immutable record of transactions. By embracing distributed ledgers, banks are also creating innovative investment opportunities that ultimately open new markets, thereby reshaping the financial landscape.

Explainer box: How does DLT work?

- Distributed ledgers are designed as a peer-to-peer distributed system composed of several participants. They use hash functions, digital signatures, and cryptographic keys to secure and authenticate the data and transactions recorded on the distributed ledger.

- Hash functions are used to create a unique digital fingerprint of transactions. The resulting output is known as a 'hash'. The inability to tamper with the distributed ledger is based on the cryptographic properties of the hash function.

- Digital signatures are used to authenticate and verify the identity of participants in the network. Each participant has a unique public-private key pair, and transactions are signed with the private key and verified using the corresponding public key.

- Distributed ledger technology enables each participant to propagate transactions to all other nodes and achieve simultaneous consensus amongst the nodes on what transactions to include in the ledger.

- Various consensus methods exist (e.g., proof of work for Bitcoin, proof of stake for Ethereum, etc.).

- Once consensus is reached, a new set of transactions is included in the ledger by all nodes.

Distributed Ledger

One such prominent change is the emerging practice of asset tokenisation which uses distributed ledgers as a technological backbone. In this application, assets (such as bonds, gold, real estate, art, etc.) are digitally represented on the distributed ledger, making them easier to trade and fractionalise among multiple owners. They allow assets to be securely carried across the network.

It is widely argued that tokens have the potential to transform the financial services industry. The tokenisation of assets promises to enhance investment strategies by providing liquid and fractionalised ownership of assets. Not only does this approach open new investment opportunities, it also improves liquidity in markets that used to be considered illiquid or semi-liquid. Boston Consulting Group (BCG) estimates that tokenised assets will become a $16 trillion business by 2030 [4]. Notable comments include ones made by the CEO of BlackRock, Larry Fink, who stated that tokenisation will be "the next generation for markets" [5]. Robin Vince, CEO of BNY Mellon, has said that "With a majority of institutional investors interested in tokenisation, distributed ledger technology may represent the next financial frontier."[25]

We believe that strengthening the relationship between tokenisation and cybersecurity will become part of the best practice for this emerging industry. The irreversibility and immutability of distributed ledger technology is predicated on state-of-the-art security protocols to prevent unauthorised transactions. As tokens represent assets which can be digitally transferred over distributed ledger networks, an important point to consider is ensuring robust security capabilities against emerging cyber threats.

HSBC's journey in asset tokenisation

HSBC has established itself as a leader in the asset tokenisation space, leveraging its expertise in implementing DLT solutions to drive significant advancements. The bank's journey of implementing production DLT solutions began in 2018 with the launch of FX Everywhere, a ground-breaking platform for settlement of foreign exchange trades using DLT. FX Everywhere has facilitated over 150 million trades worth **$10 trillion** to date, underscoring HSBC's capability in using DLT to enhance operational efficiency and transparency.

In 2019, HSBC introduced the Digital Vault, a custody solution that leveraged DLT to digitise the records of private placement investments, furthering HSBC's commitment to for digital transformation.

2023 marked another important year for HSBC with the issuance of the European Investment Bank (EIB) digital bond on its bond tokenisation platform, HSBC Orion. This milestone demonstrated how HSBC's DLT infrastructure brought efficiency to traditional bond issuance processes. The same year also saw HSBC furthering its leadership position in the precious metals market with the launch of gold tokenisation, offering investors a new, secure way to own and trade gold digitally. This was followed by the Hong Kong Monetary Authority (HKMA) issuing HKD 6bn multi-currency bonds on HSBC Orion in 2024. HSBC also expanded its gold tokenisation product to retail investors in Hong Kong SAR in 2024, providing them with a secure and accessible way to invest in gold digitally, marking another significant step in its journey of innovation in digital assets.

Post-quantum security

The need for post-quantum cryptography (PQC). The progressing developments toward a large-scale quantum computer has driven the need to migrate to quantum-safe technologies. These are designed to withstand attacks from a CRQC, and the most prominent of these solutions is PQC.

Governments and regulators are taking steps to upgrade cybersecurity standards and regulations to PQC. We highlight several examples below:
- Quantum Computing Cybersecurity Preparedness Act 2022 [6] for US federal agencies to migrate to PQC.
- The White House Memorandum on Migration to Post-Quantum Cryptography [7].
- The UK National Cyber Security Centre released guidance on migration to PQC [8].
- More specific to financial services are the documents on Addressing the Cybersecurity Risks with Quantum by the Monetary Authority of Singapore [9], as well as Quantum Security for Financial Sector report by the World Economic Forum and the Financial Conducts Authority [10].
- Along with these actions, there have also been milestones on implementing PQC on commercial use cases, most notable by Apple on iMessage [11] and Zoom [12].
- Project Leap [13] was a line of work to show a first step for central banks to transition towards quantum-safe security. A PQC-encrypted Virtual Private Network (VPN) connection was set up between the Bank of France and Deutsche Bundesbank to accomplish the transmission of payment messages [13].

Challenges with PQC implementation for DLTs

The need for PQC also extends to the specific case of distributed ledger technology.

Despite the robust security offered by distributed ledgers and blockchain through encryption and decentralised consensus mechanisms, the rapid advancement of the quantum computing cyber threats necessitates a proactive approach to future-proofing these systems. It is crucial to not only maintain but also continue to enhance the security measures surrounding distributed ledgers, ensuring that they remain resilient against both current and emerging cyber threats. This line of thought is important for the emerging trend of asset tokenisation, where assets are carried across the network.

Previous investigations on implementing PQC in distributed ledger technology can be found in academic research[14, 15] and in various industry work [16, 17, 18].

However, the major concern of implementing PQC into distributed ledgers is the potential impact on performance. These new algorithms have larger key sizes for the cryptography [19], and may have significant effect on the operational use of distributed ledgers. It has been argued that the signatures and larger key sizes used in PQC systems would cause an increase in block size [20] and signature time [24].

This has the unfortunate consequence of affecting the performance, efficiency, and execution speed of the whole distributed network. Therefore, an appropriate solution to integrate PQC algorithms into distributed ledgers needs to consider performance. We aim to provide a first step towards this direction by applying a PQC-VPN tunnel.

Proof of Concept:

Implementation approach by HSBC-Quantinuum

HSBC in collaboration with Quantinuum, a 3rd party integrated quantum company, has conducted a PoC to test PQC to a gold tokenisation platform, underpinned by QRNG technology. It represents a first step in future-proofing gold tokens and more broadly distributed ledgers against a CRQC.

Our approach aligns with Project Leap [13], which involved the construction of a PQC-VPN tunnel. A major outcome of that project was the observation of minimal impact on performance levels when sending data through the tunnel, irrespective of the size of the data. The only exception was that the performance was impacted initially when setting up the tunnel. However, it did not affect the data transfer itself. The authors emphasised that in a realistic scenario, the initial tunnel would be set up once or twice during a day.

HSBC in collaboration with Quantinuum have used this insight to develop a transition plan with implementation for deploying PQC-VPN in a gold tokenisation environment. The priority is to close security gaps without impacting performance. For the tokenisation platforms, the greatest near-term risks from quantum attacks are related to confidentiality. Transaction data, even if encrypted, could be stored and attacked in the future using a powerful quantum computer. To resolve this future threat, the data communications that underpin the gold tokens must be protected using PQC. This closes the door on threat to confidentiality, without impacting the integrity of the transactions. The use of a QRNG further strengthens the keys.

The ultimate end-state of a quantum-safe gold tokenisation platform is to embed PQC algorithms throughout the system, especially for transaction signing. However, provided such a migration is completed before powerful quantum computers exist, nothing is lost from a security perspective. For this reason, the project has focused on upgrading communication security to PQC.

The benefits of deploying QRNGs

QRNGs provide a critical raw ingredient for cryptography: high-quality random numbers. While attention is often paid to the cryptographic algorithms themselves, the underlying randomness is just as important for security [21]. The secrecy and unpredictability of an encryption key is the cornerstone of cybersecurity. In fact, according to Kerckhoffs' principle, it should be assumed an attacker knows everything about a given system, except for the cryptographic keys themselves [22].

Unlike legacy approaches to randomness generation that use traditional computing hardware, QRNGs offer a method of generating randomness that can be proven to be unpredictable. The unique properties of quantum physics ensure the randomness generated is exceptionally high-quality. This future-proofed approach to strengthening keys helps deepen cyber resilience.

Solution

Our solution, involving a PQC-VPN, is embedded in customer journey where an asset manager creates and transfers simulated HSBC Gold Tokens.

Customer Journey
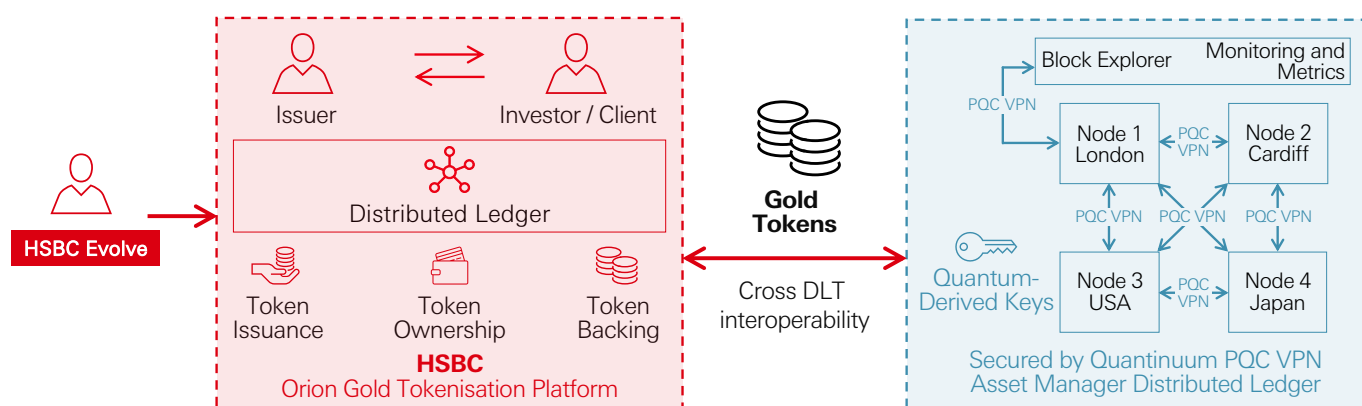
Here are the scenario steps:
1. Asset Manager signs into Evolve Single Dealer Platform (SDP).
2. Asset Manager buys 4 million HSBC Gold Tokens XGT/USD at $2,300 per troy ounce; 10 gold bars, notional $9.2 million.
3. With the PQC VPN secured network, the 4 million tokens are moved from private HSBC Orion Gold DLT to public permissioned DLT run by the asset manager.
4. Tokens can now be distributed into asset manager portfolios and wallets, and further transacted on asset manager DLT secured by PQC VPN.

The Proof of Concept achieved the following objectives:
- Proved the interoperability of tokenised gold between 2 different blockchains.
- Secured using Post-Quantum Cryptography, future proofing security between 2 distributed ledgers.

The distributed ledger associated with the simulated asset manager involved nodes placed in the UK, USA, and Japan. The PQC-VPN service was used to securely connect the various nodes in this distributed network. A diagrammatic representation of this setup is shown below:
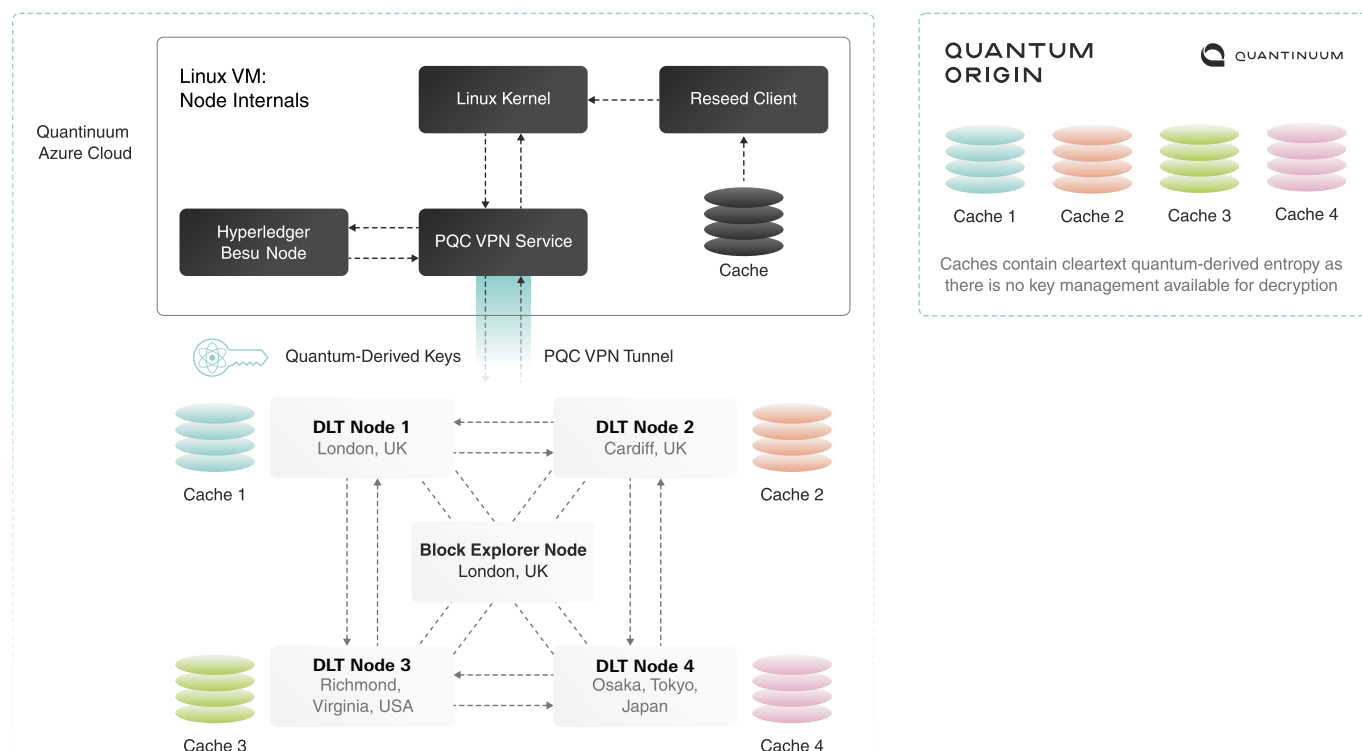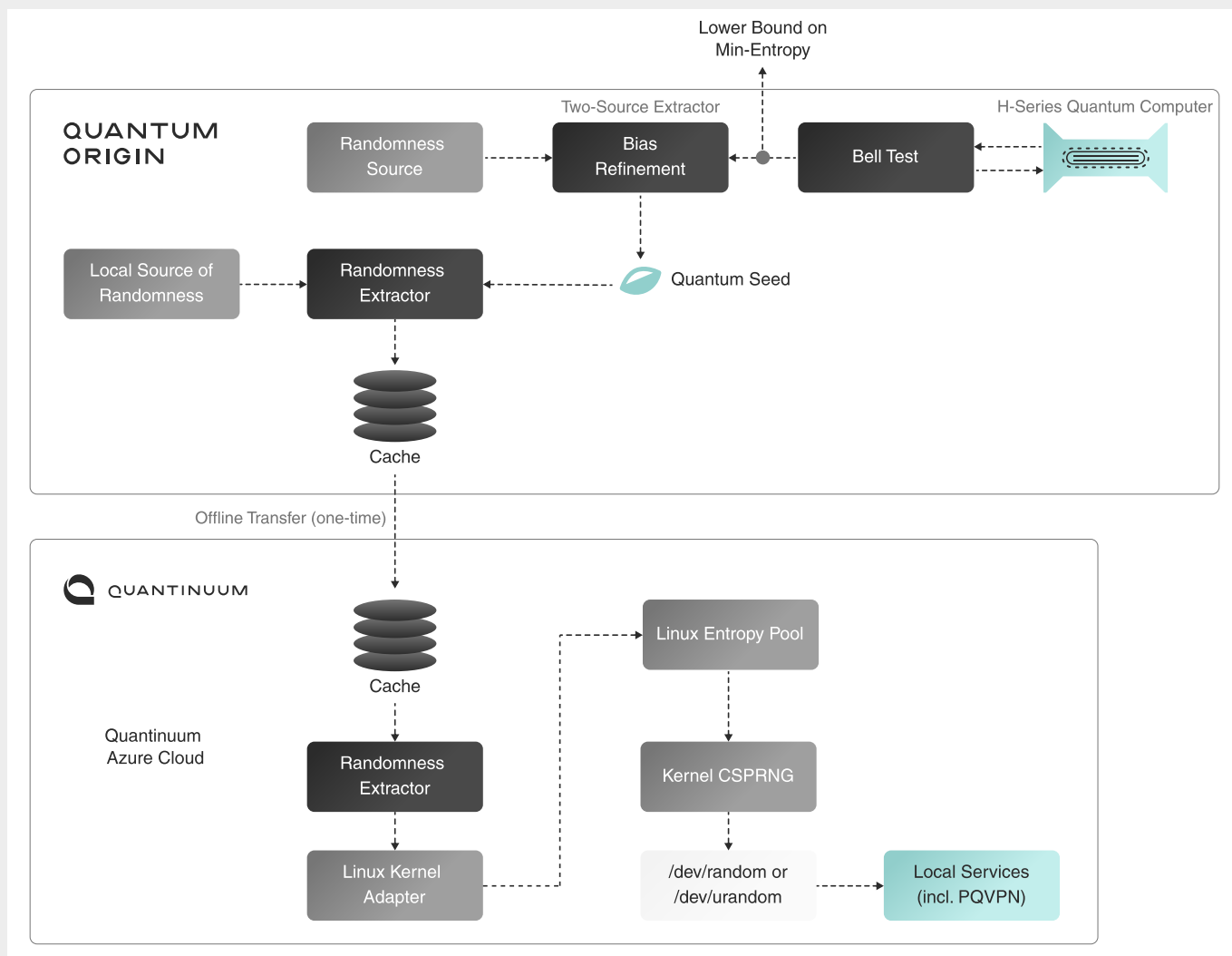

The PQC-VPN was configured as a site-to-site VPN to allow a demonstration of traditional network traffic, such as a web browsing session, flowing across Azure networks and transparently enhancing the security to quantum-secure.

We proceed to describe the PQC-VPN component in more detail below. PQC-VPN implementations are already being prototyped ahead of standardisation and have been deployed in a hybrid mode, especially on cloud platforms. It will similarly be based on the existing work done publicly by the Open Quantum Safe [23] (OQS) project. OQS has developed an OpenSSL implementation and an OpenVPN integration that supports the PQC algorithms from the NIST competition.

However, the keys are only as strong as the process used to generate them, where a significant element to that generation is the entropy used to seed the generator and ensure the keys are unpredictable. This is where Quantinuum's Quantum Origin product comes into play. Let us first explain this process, before diving into the PQC-VPN solution.

Quantinuum has developed a method of delivering quantum-computing-hardened entropy directly into the Linux kernel, thus upscaling the quality of all keys generated by the operating system. No code changes or updates are required for any applications that generate keys through the kernel, as they pull natively from the API on the system.

QUANTUM ORIGIN

Lower Bound on Min-Entropy

Two-Source Extractor

H-Series Quantum Computer

Randomness Source → Bias Refinement → Bell Test

Local Source of Randomness → Randomness Extractor ← Quantum Seed

Cache

Offline Transfer (one-time)

QUANTINUUM

Cache

Quantinuum Azure Cloud

Randomness Extractor

Linux Entropy Pool

Kernel CSPRNG

Linux Kernel Adapter

/dev/random or /dev/urandom → Local Services (incl. PQVPN)

The PQC-VPN is configured as a site-to-site VPN. The initial algorithms used are p384_kyber768 as the key encapsulation mechanism (KEM) and p384_dilithium3 as the signature algorithm. The encryption agreed by the PQC-VPN once setup is AES-256-GCM, this encryption algorithm will not change as AES is considered quantum-safe today; doubling its key length provides sufficient security.

These algorithms have been chosen to support the parallel use of classic and quantum-safe cryptography. By combining classic and quantum-safe methods, one achieves the highest available security today, without interrupting legacy systems.

The algorithms can be swapped out for any of the algorithms supported by the underlying liboqs library, documented by the OQS Project on their GitHub page [23]. As shown in the graphs below, we chose different algorithms and generated new certificates and keys to be used by the VPN after deployment, to demonstrate comparative benchmarks.

PQC VPN: Balancing enhanced security with operational practicality

There are several potential benefits that were observed in this work:

- **Cost-effectiveness:** PQC VPNs offer a cost-effective solution for securing digital communications, particularly when compared to the direct implementation of PQC algorithms in core DLT systems. Implementing PQC algorithms directly often requires substantial investment in new hardware and software, along with significant resources for testing and validation. Conversely, a PQC VPN can leverage existing network infrastructure, requiring only minimal adjustments. This means organisations can achieve quantum-resistant security, without the need for expensive overhauls of their current systems, making PQC VPNs a more budget-friendly option.
- **Seamless integration with existing DLT systems:** One of the most significant advantages of PQC VPNs is their ability to integrate seamlessly into existing DLT systems, without necessitating a redesign of the distributed ledger architecture or costly IT hardware upgrades. The PQC VPN operates as an overlay on the existing network, providing quantum-resistant encryption for data in transit without altering the underlying DLT structure. This compatibility ensures that businesses can enhance the security of their blockchain applications, while preserving their current investments in infrastructure and technology.
- **Minimal changes required for deployment:** PQC VPNs can be deployed on an existing production DLT infrastructure with minimal changes, which is a key factor in their practicality. Unlike more invasive security upgrades that might disrupt operations or require significant downtime, PQC VPNs can be implemented with lower changes, allowing for a smooth transition to a quantum-resistant state. This minimal disruption is particularly beneficial for organisations that rely on continuous operation of their DLT systems and cannot afford extended downtime or significant changes to their operational processes.
- **Low latency impact:** One of the critical concerns when implementing PQC in DLT systems is the potential for increased latency in transaction processing and block validation. Directly embedding PQC algorithms into the core architecture of DLTs can introduce significant delays due to the computational complexity of these algorithms. In contrast, using a PQC VPN approach mitigates this risk, as the encryption process occurs outside the core DLT system, thereby maintaining the speed and efficiency of transaction processing. This ensures that the DLT's relative performance remains robust while still benefiting from enhanced security against quantum threats.
- **Practical security** for the short and medium term.

As quantum computing technology evolves, so too will the methods for integrating PQC into core DLT architectures. However, until those methods are fully developed, tested, and ready for prime-time, PQC VPNs provide an interim solution that balances enhanced security with operational practicality. This approach allows organisations to protect their digital assets against emerging quantum threats, without waiting for more complex solutions to become feasible.
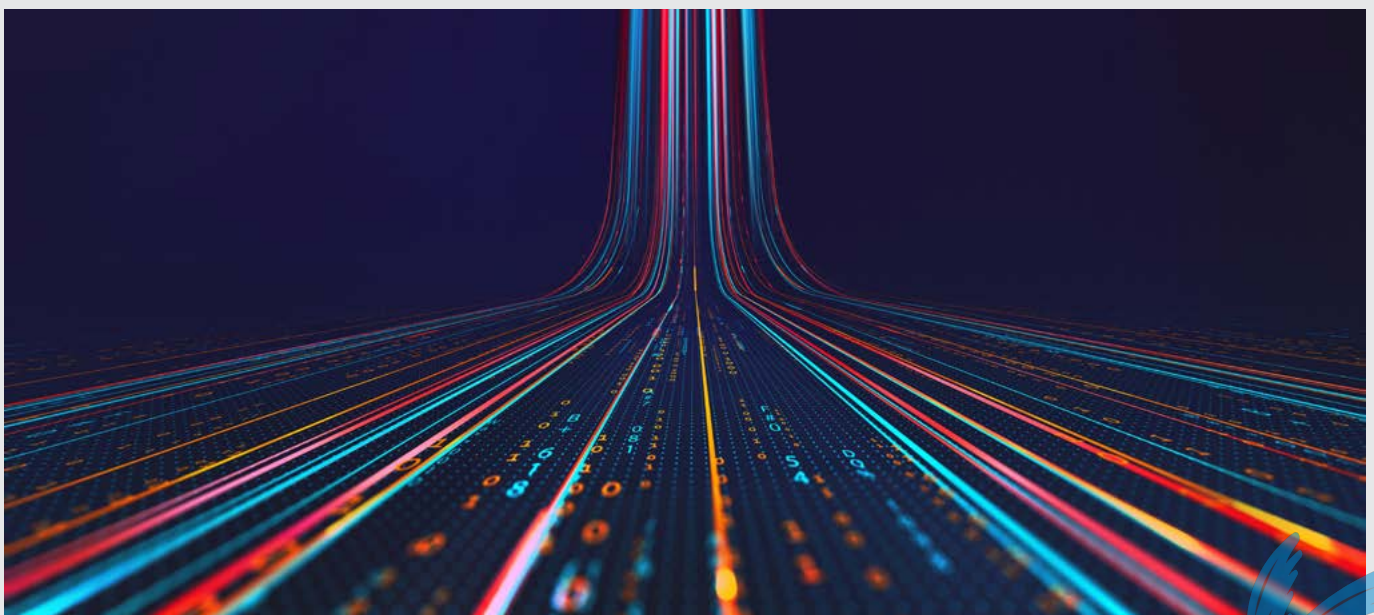
We recorded various performance metrics on securing a distributed ledger with a PQC-VPN, as opposed to without it. The results below show minimal performance impact on latency and throughput.

As described in the 'Solution' section, the measurements were taken on the Azure network, and as such, fit expected patterns for data traversing the Internet, with the peaks and troughs associated with other traffic on their fibre.

Securing a distributed ledger with PQC VPN - Proof of Concept solution

Secured by PQC VPN

Without PQC VPN
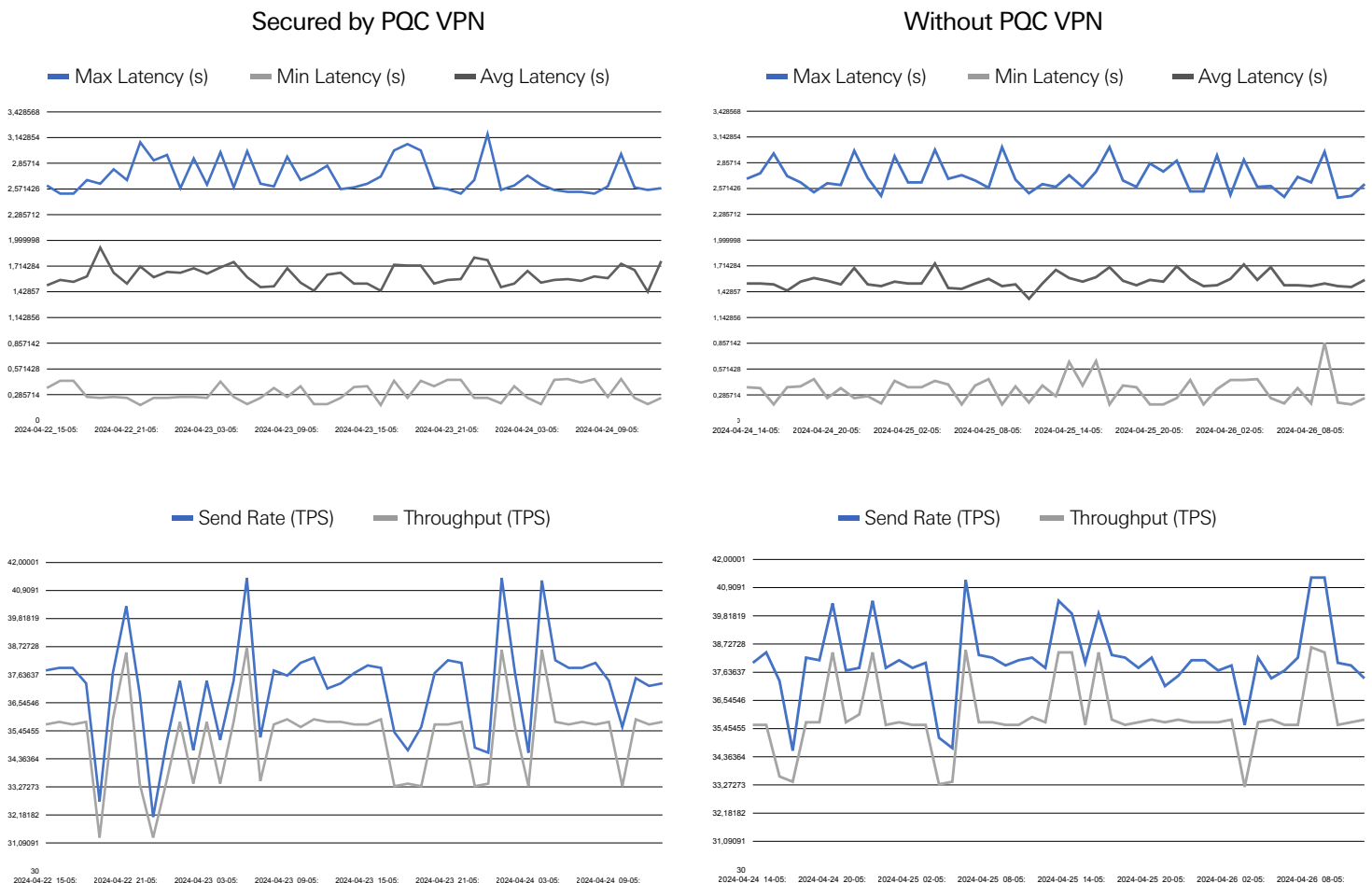
From the graphs above, when measuring the maximum, minimum and average latency there is no noticeable impact from using PQC with a VPN. Both graphs are similar shapes and fit the same scale, with the maximum being 3.1 seconds and minimum below 0.2 seconds.

Equally, the send rate and throughput are within the same bounds of between 31 and 40 transactions per second (TPS), and show negligible performance impact to upgrading to PQC on a VPN.

Conclusion

In this work, HSBC in collaboration with Quantinuum has successfully trialled the first application of quantum-secure technology for distributing tokenised physical gold.
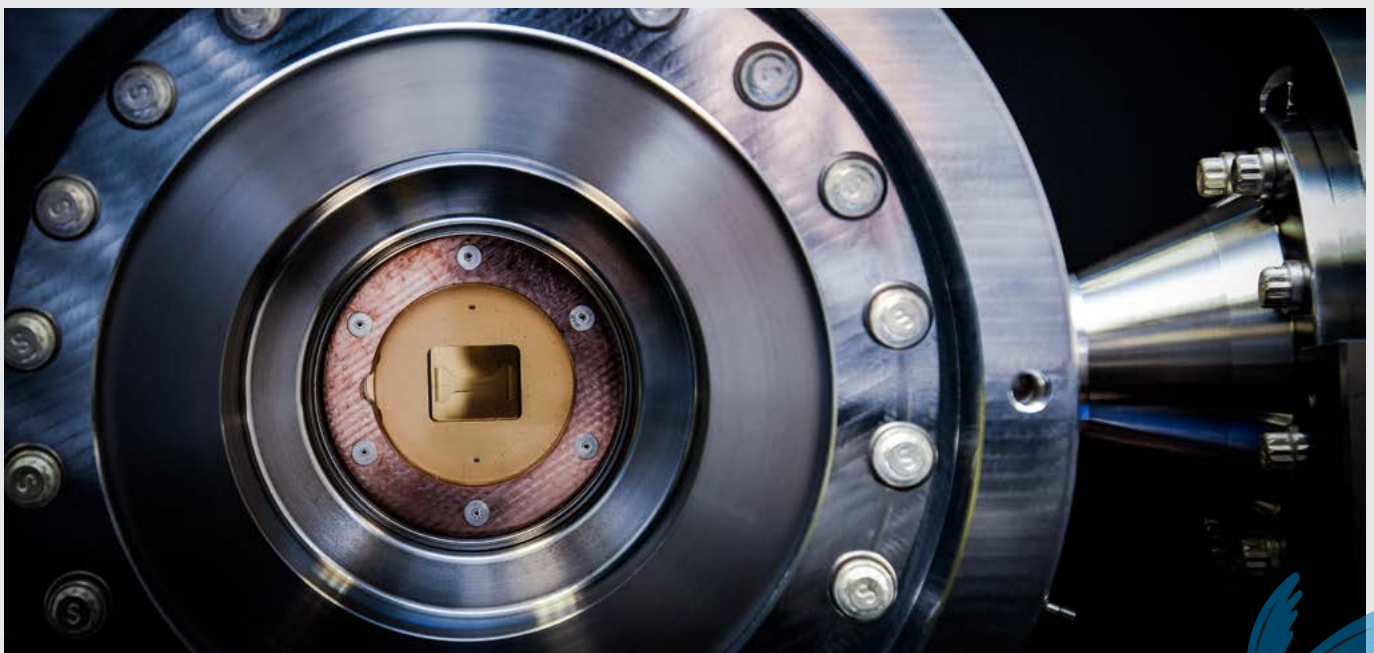
This achievement marks the latest step by HSBC in pioneering the protection of critical applications from potential future quantum computing attacks. This also presents a cost-effective approach of protecting existing production DLT in the short and medium term, without needing to rearchitect the DLT.

By having a comprehensive view of both technologies and business needs, the approach taken in this work serves as a thought leadership strategy in future-proofing asset tokenisation for the Quantum Age.
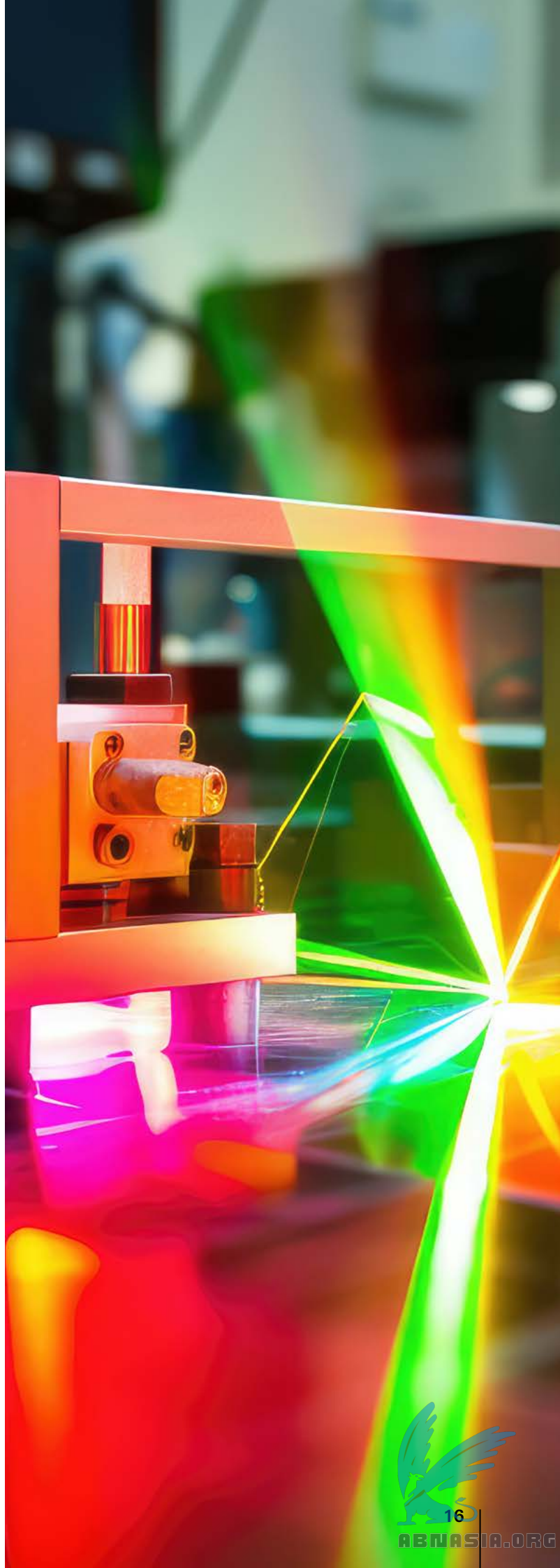
References

1. [2021 Quantum Threat Timeline Report: Global Risk Institute - Global Risk Institute](#)

2. [Post-Quantum Cryptography | CSRC (nist.gov)](#)

3. [https://www.gbm.hsbc.com/en-gb/insights/innovation/distributed-ledger-technology](#)

4. [https://www.bcg.com/publications/2022/relevance-of-on-chain-asset-tokenization](#)

5. [https://www.forbes.com/sites/davidbirch/2023/03/01/larry-fink-says-tokens-are-the-next-generation-for-markets/](#)

6. [https://www.congress.gov/bill/117th-congress/house-bill/7535](#)

7. [https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf](#)

8. [https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc](#)

9. [https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum](#)

10. [https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/](#)

11. [https://security.apple.com/blog/imessage-pq3/](#)

12. [https://news.zoom.us/post-quantum-e2ee/](#)

13. [https://www.bis.org/about/bisih/topics/cyber_security/leap.htm](#)

14. [https://www.nature.com/articles/s41598-023-32701-6](#)

15. [https://www.nature.com/articles/s41598-023-47331-1](#)

16. [https://www.qanplatform.com/en](#)

17. [https://www.theqrl.org/](#)

18. [https://www.nature.com/articles/s41598-023-32701-6](#)

19. [https://blog.cloudflare.com/sizing-up-post-quantum-signatures/](#)

20. [https://www2.deloitte.com/nl/nl/pages/risk/articles/quantum-risk-to-the-ethereum-blockchain.html](#)

21. [https://ieeexplore.ieee.org/document/1366239](#)

22. [https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle](#)

23. [https://github.com/open-quantum-safe](#)

24. [https://eprint.iacr.org/2024/1206](#)

25. [https://www.ft.com/content/5568bd6b-99df-4c8b-91bc-e0b49011da80](#)

HSBC